Pravokutni trokuti s racionalnim stranicama zadane površine

Petek, Elena

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Elena Petek

PRAVOKUTNI TROKUTI S RACIONALNIM STRANICAMA ZADANE POVRŠINE

Diplomski rad

Voditelj rada:
prof. dr. sc. Juraj Šiftar

Zagreb, rujan, 2019.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Svima koji su bili uz mene na mom životnom putu, sudjelovali u mom obrazovanju, bili materijalna i moralna potpora, davali mi snage za svaki korak u mom životu.

Posebna zahvala mentoru prof. dr. sc. Jurju Šiftaru, dečku Marku, mami i tati.
Neizmjerna zahvala obitelji Krstić na potpori tijekom studiranja.
Hvala dragom Bogu što mi je dao radost uspjeha.

Sadržaj

Uvod

Pravokutni trokut čije su duljine stranica prirodni brojevi zovemo Pitagorin[1] trokut. Uređenu trojku prirodnih brojeva (x, y, z) zovemo Pitagorina trojka, ako su x i y duljine kateta, a z duljina hipotenuze nekog Pitagorinog trokuta, odnosno ako zadovoljavaju jednakost

$$x^2 + y^2 = z^2, \tag{1}$$

koja predstavlja algebarski zapis dobro poznatog Pitagorinog poučka. Ukoliko su brojevi x, y i z relativno prosti, kažemo da je (x, y, z) primitivna Pitagorina trojka, a trokut s takvim duljinama stranica naziva se primitivni Pitagorin trokut. Još od Euklida[2] poznate su formule kojima su duljine stranica bilo kojeg Pitagorinog trokuta izražene u obliku m^2-n^2, $2mn$ i $m^2 + n^2$, za neka dva prirodna broja m i n.

Jedno od najstarijih pitanja u povijesti matematike, od antičkog doba i Diofantovih[3] radova, preko arapskih matematičara u 10. stoljeću, Fibonaccija[4] u 13. stoljeću i dalje, sve do suvremene aritmetičke geometrije i teorije brojeva, odnosi se na pronalaženje svih pravokutnih trokuta s racionalnim duljinama stranica čija površina ima zadanu cjelobrojnu vrijednost. Prirodni broj $\mathcal{A}$ sa svojstvom da postoji pravokutni trokut s racionalnim duljinama stranica čija površina iznosi $\mathcal{A}$ uobičajeno se naziva *kongruentnim brojem*. Iako su proučavanjem kongruentnih brojeva dobiveni mnogi zanimljivi rezultati, još uvijek je otvoren problem općenitog postupka kojim bi se u konačno mnogo koraka ispitalo je li neki prirodni broj kongruentan.

U ovom radu prikazana je jedna geometrijska metoda kojom se za pojedini kongruentni broj $\mathcal{A}$, počevši od jednog pripadnog pravokutnog trokuta s racionalnim duljinama stranica, može iterativno konstruirati niz trokuta s istim svojstvima, površine oblika $\mathcal{A}r^2$, pri čemu je r racionalan broj. U takvom nizu nema sličnih trokuta. Kako je u proučavanju

[1] Pitagora (Samos, oko 570.pr.Kr. – Tarent, oko 495.pr.Kr.), starogrčki filozof i matematičar.
[2] Euklid (oko 340.pr.Kr. – oko 287.pr.Kr.), starogrčki matematičar.
[3] Diofant (Aleksandrija, 3.st.), grčki matematičar.
[4] Leonardo iz Pise - Fibonacci (1170. – 1240.), talijanski matematičar.

kongruentnih brojeva ključna ideja povezivanje s eliptičkim krivuljama i njihovom strukturom grupe, dalje se pokazuje kako se parametrizacijom i preslikavanjem na eliptičku krivulju $E : y^2 = x^3 - \mathcal{A}^2 x$ dobivaju nove racionalne točke i njima pridruženi trokuti.

Prikladnom parametrizacijom skupa $T_{\mathcal{A}}$ racionalnih pravokutnih trokuta površine $\mathcal{A}$ na tom skupu uvodi se algebarska struktura u kojoj je $T_{\mathcal{A}}$ konačno generiran. To je zapravo varijanta Mordellovog teorema, u okviru geometrijski konstruiranog skupa $T_{\mathcal{A}}$. Ostaje otvoreni problem efektivnog pronalaženja tog konačnog skupa generatora. Na primjerima su prikazani skupovi generatora za neke vrijednosti kongruentnog broja $\mathcal{A}$ i pripadne particije skupa $T_{\mathcal{A}}$.

Poglavlje 1

Povijesni pregled i pojam kongruentnog broja

1.1 Euklidova parametrizacija pravokutnih trokuta s cjelobrojnim stranicama

Postojanje Pitagorinih trojki koje zadovoljavaju jednadžbu (1) poznato je već preko dvije tisuće godina. Euklid je pronašao formule koje za bilo koja dva prirodna broja m i n, $m > n$ daju Pitagorine trojke:

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ z &= m^2 + n^2 \end{aligned} \tag{1.1}$$

([6], Lema 1. uz Propoziciju 29., Knjiga 10.). Svi pravokutni trokuti s cjelobrojnim duljinama stranica mogu se dobiti iz formule (1.1). Svaka Pitagorina trojka višekratnik je neke primitivne trojke, koje su u izravnoj korelaciji s relativno prostim parovima (m, n) na način da je točno jedan od (m, n) paran [4].

Teorem 1.1.1. *Sve primitivne Pitagorine trojke (x, y, z) u kojima je y paran, dane su formulama:*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2, \tag{1.2}$$

gdje je $m > n$ i $m, n \in \mathbb{N}$ su relativno prosti brojevi različite parnosti.

Dokaz. Jednadžbu (1) možemo zapisati u obliku:

$$y^2 = (z + x)(z - x).$$

Nadalje, neka je $y = 2c$. Brojevi $z + x$ i $z - x$ su parni pa postoje prirodni brojevi a i b takvi da je $z + x = 2a$, $z - x = 2b$. Tada je:

$$c^2 = ab. \tag{1.3}$$

Budući da je $z = a + b$, $x = a - b$, zaključujemo da su brojevi a i b relativno prosti, jer u suprotnom x i z ne bi bili relativno prosti. Prema tome, iz (1.3) slijedi da postoje relativno prosti prirodni brojevi m i n takvi da je $a = m^2$, $b = n^2$. Odavde je:

$$x = m^2 - n^2, \quad z = m^2 + n^2, \quad y = 2mn.$$

Brojevi m i n ne mogu biti oba parni jer su relativno prosti i ne mogu biti oba neparni jer je $x = m^2 - n^2$ neparan. Dakle, brojevi m i n su različite parnosti.
Nadalje, brojevi x, y i z definirani u (1.1) zadovoljavaju jednadžbu (1), odnosno vrijedi:

$$(m^2 - n^2)^2 + (2mn)^2 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2.$$

Provjerimo jesu li brojevi x, y i z relativno prosti. Pretpostavimo suprotno, odnosno da brojevi x i z imaju zajednički djelitelj $d > 1$. Tada je d neparan, $d \mid (m^2+n^2)+(m^2-n^2)$ tj. $d \mid 2m^2$ i $d \mid (m^2+n^2)-(m^2-n^2)$ tj. $d \mid 2n^2$. No, ovo je u kontradikciji s pretpostavkom da su m i n, pa stoga i m^2 i n^2, relativno prosti. □

Možemo, dakle, ustvrditi da su primitivne Pitagorine trojke (x, y, z) u kojima je y paran, parametrizirane parom (m, n), pri čemu su $m, n \in \mathbb{N}$ relativno prosti brojevi različite parnosti i $m > n$.

Iz teorema 1.1.1 slijedi da su sve Pitagorine trojke dane identitetom:

$$[k(m^2 - n^2)]^2 + (2kmn)^2 = [k(m^2 + n^2)]^2,$$

gdje su $m, n, k \in \mathbb{N}$, $m > n$ i m, n različite parnosti.

Nije teško pokazati da se svi pravokutni trokuti s racionalnim duljinama stranica mogu dobiti množenjem duljina stranica pravokutnih trokuta s cjelobrojnim stranicama racionalnim skalarom.

1.2 Diofant i arapski zapisi

Petstotinjak godina nakon Euklida, Diofant je zapazio da pravokutni trokut s cjelobrojnim duljinama stranica x, y, z i cjelobrojnom vrijednosti površine $\mathcal{A}$ postoji ako i samo ako su $z^2 + 4\mathcal{A}$ i $z^2 - 4\mathcal{A}$ oba kvadrati prirodnog broja, uz uvjet $\mathcal{A} > 0$.
Jedan smjer je očigledan, jer ako postoji takav trokut, onda vrijedi $x^2+y^2 = z^2$ i $4\mathcal{A} = 2xy$, pa je $z^2 \pm 4\mathcal{A} = (x \pm y)^2$.

Obratno, ako vrijedi $z^2 + 4\mathcal{A} = u^2$ i $z^2 - 4\mathcal{A} = v^2$, pri čemu su u i v cijeli brojevi, lako je uočiti da su $x = \frac{u+v}{2}$ i $y = \frac{u-v}{2}$ također cijeli brojevi (jer $(u + v)(u - v) = 8\mathcal{A}$), za koje vrijedi $x^2 + y^2 = z^2$ i $2xy = 4\mathcal{A}$, pa su x, y duljine kateta pravokutnog trokuta površine $\mathcal{A}$.

Promatramo li pitanje postojanja Pitagorinog trokuta na taj način, može se krenuti od zadane vrijednosti površine $\mathcal{A}$ i tražiti sve Pitagorine trojke (x, y, z) za taj prirodni broj $\mathcal{A}$.

U Poglavlju XVI., *History of the Theory of Numbers* [3], spominje se kako anonimni arapski zapis, napisan prije 972. godine, sadrži sljedeći problem (kongruentnih brojeva): Za zadani $k \in \mathbb{Z}$ treba pronaći kvadrat z^2 takav da su $z^2 \pm k$ oba kvadrati. U tim zapisima navedena su neka svojstva i primjeri kongruentnih brojeva te tablica s preko trideset takvih brojeva, počevši od $5, 6, 14, \ldots$, itd. do 10374. I ovdje su kongruentni brojevi eksplicitno povezani s pravokutnim trokutima, no nema jasnih naznaka da je ta tematika bila izravno potaknuta Diofantovim radovima, premda su neki od tih radova prevedeni na arapski jezik u drugoj polovici 10. stoljeća i imali su veliki utjecaj na arapsku matematiku. Mohammed Ben Alhocain u jednom arapskom rukopisu iz 10. stoljeća kao glavni cilj teorije pravokutnih trokuta s racionalnim stranicama navodi traženje kvadrata, kojem kada mu se pribroji ili oduzme cijeli broj k opet daje kvadrat. Izveden je i geometrijski dokaz gore spomenutog Diofantovog zapažanja da kvadrat hipotenuze ima traženo svojstvo jer je $z^2 \pm 2xy = (x \pm y)^2$.

Mnoge arapske, a i druge matematičare srednjega vijeka zanimalo je postojanje rješenja za zadani prirodni broj $\mathcal{A}$, i ako ono postoji, pronaći Pitagorine trojke koje zadovoljavaju zadanu vrijednost površine $\mathcal{A}$. Više o tome može se pronaći u [3].

1.3 Fibonacci i kvadrati brojeva

Fibonaccijev prvi rad, po pitanju pronalaska pravokutnih trokuta zadane površine, bio je odgovoriti Johnu od Palerma[1] na postavljeno pitanje:

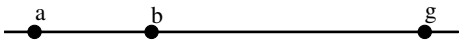
> Pronađi kvadrat broja iz kojeg, kada mu se pridoda ili oduzme broj 5, u oba slučaja se dobije kvadrat broja ([7], str. 3.).

U matematičkoj notaciji to znači pronaći brojeve u, v i w takve da vrijedi: $w^2 + 5 = u^2$ i $w^2 - 5 = v^2$. Jednostavno je pronaći iracionalna rješenja, no Fibonacci je tražio racionalna rješenja za navedeni problem. Lako se pokaže da su cjelobrojna rješenja nemoguća.

Rješenje navedenog problema zahtijeva nekoliko koraka. U prvom koraku Fibonacci konstatira da ako su dva broja relativno prosti i zbroj im je paran te ako je trostruki umnožak dva broja i njihovog zbroja pomnožen brojem od kojeg veći broj sadrži manji broj, tada je rezultat broj koji je višekratnik broja 24 ([7], str. 48.).

[1] John od Palerma, prevoditelj na dvoru rimskog cara Fredericka II. (1194. – 1250.)

Fibonacci je često brojeve prikazivao kao duljine. Smjestio je točke a, b i g na pravac zajedno s dva broja ab, bg koja predstavljaju udaljenosti između a i b te između b i g.



Vrijedi:

$$ab \cdot bg \cdot (ab + bg) \cdot (bg - ab), \tag{1.4}$$

gdje su ab i bg relativno prosti brojevi, $bg > ab$. Pažljivo je provjerio sve slučajeve i dokazao da je umnožak iz (1.4) višekratnik broja 24, a brojeve dobivene iz tog umnoška nazvao je *kongruentni brojevi*. Postojanje kongruentnih brojeva odnosi se na sljedeći problem:

> Pronađi broj koji kada se pribroji kvadratu nekog broja i oduzme od kvadrata tog istog broja uvijek rezultira kvadratom nekog broja ([7], str. 53.).

Uočimo da je ovo zapravo problem Johna od Palerma, samo što se ne zahtijeva da traženi broj bude broj 5.

Fibonaccijeva metoda pretpostavlja sljedeće. Neka je $bg \cdot (bg - ab) < ab \cdot (ab + bg)$ te neka je broj uzastopnih neparnih brojeva koji se nalaze oko broja $ab \cdot (ab + bg)$ oblika $bg \cdot (bg - ab)$ i neka je broj uzastopnih neparnih brojeva koji se nalaze oko broja $bg \cdot (bg - ab)$ oblika $ab \cdot (ab + bg)$. U primjeru iz knjige [7], za $ab = 3$ i $bg = 5$, ubacivanjem u prethodne pretpostavke dobivamo 10 uzastopnih neparnih brojeva smještenih oko broja 24:

$$15, 17, 19, 21, 23, 25, 27, 29, 31, 33.$$

Također, postoji 6 uzastopnih neparnih brojeva smještenih oko broja 40:

$$35, 37, 39, 41, 43, 45.$$

Uočimo povezanost prethodna dva niza: drugi niz se nastavlja na prvi niz u nizu svih neparnih brojeva i oba niza imaju jednaku sumu, 240. Nadalje, broj 240 je kongruentan broj jer zadovoljava relaciju (1.4). Također, broj 240 je i rješenje problema jer vrijedi:

$$17^2 - 240 = (1 + 3 + \ldots + 33) - (15 + 17 + \ldots + 33) = 1 + 3 + \ldots + 13 = 7^2,$$

odnosno

$$17^2 + 240 = (1 + 3 + \ldots + 33) + (35 + 37 + \ldots + 45) = 1 + 3 + \ldots + 45 = 23^2.$$

Međutim, ovo nije rješenje problema kojeg je postavio John od Palerma, jer treba broj 240 na neki način zamijeniti brojem 5. Fibonacci je zaključio da treba pronaći kongruentan broj oblika $5 \cdot kvadrat$, jer na taj način može dijeliti dobiveni kongruentan broj s

kvadratom i dobiti broj 5 ([7], str. 76.). Brojevi $ab = 4$ i $bg = 5$ ne zadovoljavaju u potpunosti relaciju (1.4), jer $4 + 5$ nije paran broj, što je nužno kod kongruentnih brojeva. Stoga ne postoji 5 uzastopnih neparnih brojeva smještenih oko broja 36, kao ni 4 uzastopna neparna broja smještena oko broja 45. Međutim, udvostručene navedene vrijednosti zadovoljavaju relaciju (1.4). Zaista postoji 10 uzastopnih neparnih brojeva smještenih oko broja 72: $63, 65, \ldots, 81$, a postoji i 8 uzastopnih neparnih brojeva smještenih oko broja 90: $83, 85, \ldots, 97$. Zbroj oba niza je 720, što je jednako $5 \cdot 12^2$. Na ovaj način dobili smo:

$$41^2 - 720 = (1 + 3 + \ldots + 81) - (63 + 65 + \ldots + 81) = 1 + 3 + \ldots + 61 = 31^2,$$

odnosno

$$41^2 + 720 = (1 + 3 + \ldots + 81) + (83 + 85 + \ldots + 97) = 1 + 3 + \ldots + 97 = 49^2.$$

Konačno, Fibonacci je odgovorio Johnu od Palerma:

> Za prvi kvadrat imamo $6\frac{97}{144}$, s korijenom $2\frac{7}{12}$, koji nastaje dijeljenjem broja 31 s korijenom od 144, odnosno s 12. Za drugi kvadrat, koji je traženi kvadrat, imamo $11\frac{97}{144}$, s korijenom $3\frac{5}{12}$, koji je rezultat dijeljenja broja 41 s 12. Za zadnji korijen imamo $16\frac{97}{144}$ s korijenom $4\frac{1}{12}$ ([7], str. 78.).

Fibonaccijev odgovor možemo matematički zapisati na sljedeći način:

$$\left(\frac{41}{12}\right)^2 - 5 = \left(\frac{31}{12}\right)^2 \quad \text{i} \quad \left(\frac{41}{12}\right)^2 + 5 = \left(\frac{49}{12}\right)^2.$$

Lako možemo vidjeti da broj $w = \frac{41}{12}$ odgovara Pitagorinom trokutu s duljinama stranica: $\frac{3}{2}$, $\frac{20}{3}$ i $\frac{41}{6}$, površine 5, jer je $\frac{49}{12} - \frac{31}{12} = \frac{3}{2}$, $\frac{49}{12} + \frac{31}{12} = \frac{20}{3}$.

Uočimo sada vezu ovog Fibonaccijevog rješenja s problemom postojanja Pitagorinih trokuta sa zadanom cjelobrojnom površinom. Uzmemo li pravokutni trokut s duljinama stranica $a = \frac{3}{2}$, $b = \frac{20}{3}$ i $c = 2w = \frac{41}{6}$ $\left(\text{jer po Pitagorinom poučku vrijedi: } \left(\frac{3}{2}\right)^2 + \left(\frac{20}{3}\right)^2 = \frac{9}{4} + \frac{400}{9} = \left(\frac{41}{6}\right)^2\right)$, nalazimo da je njegova površina $\mathcal{A} = \frac{1}{2} \cdot \frac{3}{2} \cdot \frac{20}{3} = 5$.

Međutim, duljine stranica tog trokuta nisu cijeli, nego racionalni brojevi. Općenito, bit će lakše promatrati pravokutne trokute s racionalnim duljinama stranica kako bi se istražilo postojanje Pitagorinih trokuta sa zadanom cjelobrojnom površinom, pa ćemo u nastavku tako i postupati.

U prethodnom primjeru, racionalna trojka $\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$ množenjem sa 6 daje Pitagorinu trojku (9, 40, 41), za trokut površine $\mathcal{A} = 180 = 5 \cdot 6^2$.

Pokazat ćemo kako se u tom i u svim primjerima te vrste povezuju zadana vrijednost $\mathcal{A} \in \mathbb{N}$ i određena rješenja $w \in \mathbb{Q}$ s odgovarajućim pravokutnim trokutom racionalnih duljina stranica. Najprije uvodimo sljedeću definiciju (iz [8]) za vrijednost prirodnog broja $\mathcal{A}$, koja pritom ima ključnu ulogu.

Definicija 1.3.1. *Za prirodan broj n kažemo da je kongruentan broj ako je jednak površini nekog pravokutnog trokuta s racionalnim stranicama.*

Cilj će, dakle, biti pronalaženje svih kongruentnih brojeva, a time i racionalnih pravokutnih trokuta. Za tu svrhu bit će nam važna sljedeća karakterizacija kongruentnih brojeva iz [8].

Propozicija 1.3.2. *Prirodan broj n je kongruentan ako i samo ako postoji racionalan broj x sa svojstvom da su x, $x-n$ i $x+n$ kvadrati racionalnih brojeva.*

Vidjet ćemo da je dokaz ove propozicije usko povezan s prije navedenom Diofantovom karakterizacijom pravokutnih trokuta s cjelobrojnim duljinama stranica. Riječ je zapravo o maloj modifikaciji istog računa, čime će ujedno biti prikazano kako se u primjeru Fibonaccijevog problema određuje pripadni pravokutni trokut.

Dokaz. Napišimo prvo sljedeće relacije:

$$z^2 + 4\mathcal{A} = u^2,$$
$$z^2 - 4\mathcal{A} = v^2$$

i pomnožimo ih s $\frac{1}{4}$. Dobivamo:

$$\left(\frac{z}{2}\right)^2 + \mathcal{A} = \left(\frac{u}{2}\right)^2,$$
$$\left(\frac{z}{2}\right)^2 - \mathcal{A} = \left(\frac{v}{2}\right)^2.$$

Ako postoji pravokutni trokut s racionalnim duljinama stranica x, y, z i površinom $\mathcal{A} \in \mathbb{N}$, onda je $w = \frac{z}{2}$ takav racionalan broj da su w, $w+\mathcal{A}$, $w-\mathcal{A}$ kvadrati racionalnih brojeva. Obratno, ako imamo $w \in \mathbb{Q}$ i $\mathcal{A} \in \mathbb{N}$ takve da su w, $w+\mathcal{A}$, $w-\mathcal{A}$ kvadrati racionalnih brojeva, stavimo $\frac{z}{2} = w$, tj. $z = 2w$, te $x = \frac{u+v}{2}$ i $y = \frac{u-v}{2}$, pa će to biti racionalne duljine stranica pravokutnog trokuta površine $\mathcal{A}$.
Naime,

$$x^2 + y^2 = \frac{(u+v)^2 + (u-v)^2}{4} = \frac{u^2+v^2}{2} = z^2$$

i

$$2xy = \frac{u^2 - v^2}{2} = 8\mathcal{A} \iff \frac{xy}{2} = A.$$

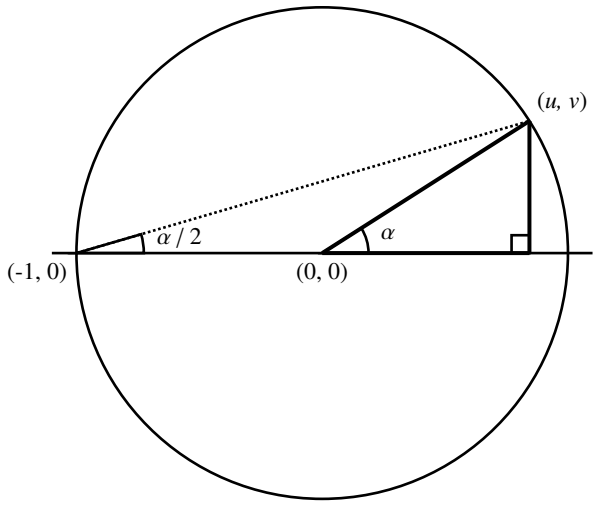
□

Poglavlje 2

Geometrijski pristup

2.1 Geometrijski pristup parametrizaciji pravokutnih trokuta

Pravokutni trokut s racionalnim duljinama stranica x, y i z te kutom α nasuprot stranici duljine y, možemo smjestiti u koordinatni sustav i opisati mu jediničnu kružnicu takvu da se vrh s kutom α nalazi u ishodištu, a duljina hipotenuze jednaka je radijusu kružnice, kao na slici 2.1.



Slika 2.1: Parametrizacija pravokutnog trokuta

Neka su $u = \frac{x}{z}$ i $v = \frac{y}{z}$. Zbog hipotenuze duljine 1, $u = \cos\alpha$ i $v = \sin\alpha$ su racionalni brojevi. Produživanjem pravca na osi x, na način da siječe kružnicu u točki

$(-1, 0)$, dobivamo kut pri tom vrhu mjere $\frac{\alpha}{2}$ (po teoremu o obodnom i središnjem kutu). Nadalje, neka je $t = \operatorname{tg}\frac{\alpha}{2}$ nagib pravca koji prolazi točkama $(-1, 0)$ i (u, v). Tada je $t = \frac{v}{u+1} \in \langle 0, 1\rangle$ racionalan broj. Zanimaju nas apscisa i ordinata točke (u, v) izražene preko t. S obzirom da je pravac oblika $y = tx + l$, gdje je l odsječak na osi y, i prolazi točkom $(-1, 0)$, slijedi da je $l = t$, odnosno jednadžba danog pravca je $y = tx + t$. Uvrštavanjem u jednadžbu kružnice $x^2 + y^2 = 1$ dobivamo dva rješenja: $x_1 = -1$ i $y_1 = 0$, što nam je već poznato, i $x_2 = \frac{1-t^2}{1+t^2}$ i $y_2 = \frac{2t}{1+t^2}$. Uočimo da smo na ovaj način dobili formulu za univerzalnu supstituciju, gdje je $u = \cos\alpha = \frac{1-t^2}{1+t^2}$, $v = \sin\alpha = \frac{2t}{1+t^2}$, $t = \operatorname{tg}\frac{\alpha}{2}$.

Istu parametrizaciju možemo dobiti i na algebarski način, bez korištenja trigonometrijskih funkcija. Neka je $t = \frac{m}{n}$, gdje su m, n relativno prosti prirodni brojevi. Skaliranjem duljina stranica danog trokuta faktorom m^2+n^2 dobivamo Euklidovu parametrizaciju danu u (1.1).

Ako zamijenimo uloge od x i y, tada će trokut biti parametriziran s vrijednošću $\frac{1-t}{1+t}$. Naime, tražimo funkciju $f(t)$ koja udovoljava zahtijevu $u(f(t)) = \frac{2t}{1+t^2}$. Supstituirajući t s $f(t)$ u izrazu $u = \frac{1-t^2}{1+t^2}$ dobivamo da je $f(t) = \frac{1-t}{1+t}$. S obzirom da preslikavanje $t \mapsto \frac{1-t^2}{1+t^2}$ ima inverz, postoje točno dva parametra iz intervala $\langle 0, 1\rangle$ za svaki trokut. Ipak, postoji primitivni izbor parametra za svaki trokut, i on je jedinstven s brojnikom i nazivnikom različite parnosti. Zaista, parametre zadanog trokuta možemo napisati kao $t = \frac{m}{n}$ i $\frac{1-t^2}{1+t^2} = \frac{M}{N} = \frac{n-m}{n+m}$, gdje su brojevi m, n i M, N relativno prosti prirodni brojevi. Jedini mogući zajednički faktor brojeva $n - m$ i $n + m$ je broj 2, stoga razlikujemo dva slučaja:

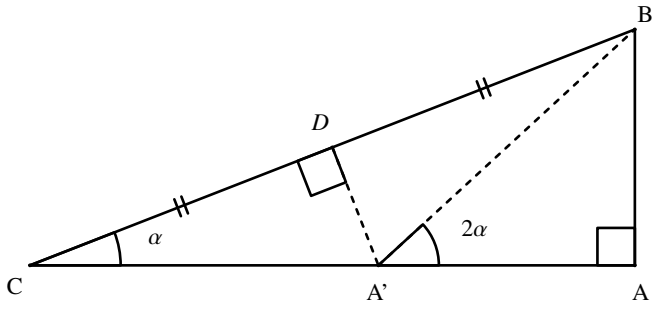
- m, n različite parnosti: $M + N = (n - m) + (n + m) = 2n$ – paran broj,
- m, n neparni: $M + N = \frac{n-m}{2} + \frac{n+m}{2} = n$ – neparan broj.

Dakle, u točno jednom od parametara t i $\frac{1-t^2}{1+t^2}$, brojnik i nazivnik imaju različitu parnost. Takvi parametri odgovaraju primitivnom trokutu iz (1.1). U suprotnom su sve tri stranice trokuta djeljive s 2.

2.2 Konstrukcija novog trokuta

Za zadani pravokutni trokut ABC s racionalnim duljinama stranica zadane površine $\mathcal{A}$, cilj je geometrijski konstruirati pravokutni trokut $A'B'C'$ površine $r^2\mathcal{A}$, za neki racionalan broj r.

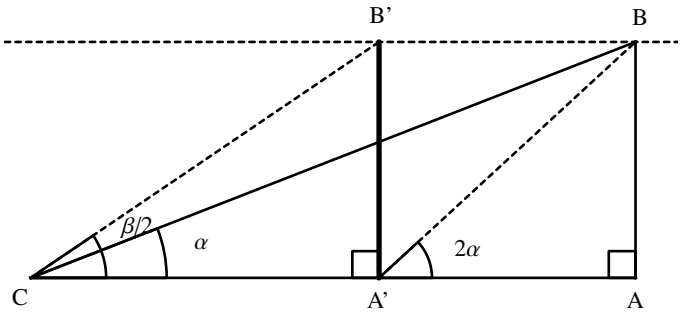
Neka je α šiljasti kut trokuta ABC, tako da su $\sin\alpha$, $\cos\alpha$ i $\operatorname{tg}\alpha$ racionalni brojevi. Simetrala hipotenuze $\overline{BC}$ siječe dužu katetu trokuta u nekoj točki A', kao na slici 2.2.



Slika 2.2: Udvostručeni kut α početnog trokuta ABC

Trokuti $\triangle A'CD$ i $\triangle A'BD$ su sukladni po S-K-S teoremu o sukladnosti. Stoga, $|A'C| = |A'B|$ i $\angle AA'B$ je dvostruki kut $\angle ACB$, odnosno $\angle AA'B = 2\alpha$. Štoviše, $\sin 2\alpha$, $\cos 2\alpha$ i $\operatorname{tg} 2\alpha$ racionalni su izrazi od $\operatorname{tg}\alpha$, pa su također racionalni brojevi. S obzirom da je duljina stranice $\overline{AB}$ racionalan broj, zaključujemo da trokut $A'AB$ ima racionalne duljine stranica, pa je $|A'C| = |AC| - |A'A|$ racionalna.

Translacijom stranice $\overline{AB}$ za vektor $\overrightarrow{AA'}$ dobivamo stranicu $\overline{A'B'}$ novog trokuta $A'B'C$. Označimo $\angle A'CB'$ s $\frac{\beta}{2}$ (vidi sliku 2.3).



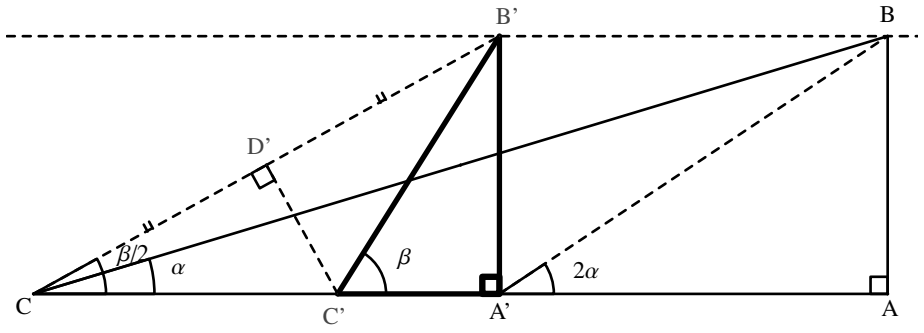
Slika 2.3: Dobivanje parametra $\tan\frac{\beta}{2} = \sin 2\alpha$ od novog trokuta

Nadalje,

$$\operatorname{tg}\frac{\beta}{2} = \frac{|A'B'|}{|A'C|} = \frac{|AB|}{|A'B|} = \sin 2\alpha,$$

što je racionalan broj.

Budući da je $|A'C| = |A'B| > |AB| = |A'B'|$, vidimo da je $\overline{A'C}$ duža kateta pravokutnog trokuta $A'B'C$. Nadalje, simetrala hipotenuze $\overline{B'C}$ mora sjeći stranicu $\overline{A'C}$ u nekoj točki C', kao na slici 2.4.



Slika 2.4: Novi trokut $A'B'C'$ s kutom β

Slijedi, $\angle A'C'B' = \beta$. S obzirom da je $\operatorname{tg}\frac{\beta}{2}$ racionalan, zaključujemo da su i $\sin\beta$, $\cos\beta$ i $\operatorname{tg}\beta$ racionalni brojevi, zbog formule dvostrukog kuta. Štoviše, $|A'B'| = |AB|$ je racionalan broj pa zaključujemo da su sve stranice u trokutu $A'B'C'$ racionalnih duljina. Kateta $\overline{A'B'}$ pravokutnog trokuta $A'B'C'$ i kateta $\overline{AB}$ pravokutnog trokuta ABC jednakih su duljina, stoga je omjer površina ta dva trokuta jednak:

$$\begin{aligned}
\frac{|A'C'|}{|AC|} &= \frac{\frac{|AB|}{|AC|}}{\frac{|A'B'|}{|A'C'|}} \\
&= \frac{\operatorname{tg}\alpha}{\operatorname{tg}\beta} \\
&= \frac{1-\operatorname{tg}^2\frac{\beta}{2}}{2\operatorname{tg}\frac{\beta}{2}} \cdot \frac{\sin\alpha\cos\alpha}{\cos^2\alpha} \\
&= \frac{1-\sin^2 2\alpha}{2\sin 2\alpha} \cdot \frac{\sin 2\alpha}{2\cos^2\alpha} \\
&= \frac{\cos^2 2\alpha}{4\cos^2\alpha} \\
&= \left(\frac{\cos 2\alpha}{2\cos\alpha}\right)^2 \\
&= \left(\frac{|A'A|\cdot|BC|}{2\cdot|A'B|\cdot|AC|}\right)^2,
\end{aligned} \tag{2.1}$$

što je kvadrat racionalnog broja, kao što smo i zahtijevali.

U prethodnom odjeljku 2.1 pokazali smo da je $t = \operatorname{tg}\frac{\alpha}{2}$ parametar za trokut ABC.

Analogno, za novi trokut $A'B'C'$ parametar je:

$$T = \operatorname{tg}\frac{\beta}{2} = \sin 2\alpha = 2\sin\alpha\cos\alpha = 2uv = \frac{4t(1-t^2)}{(1+t^2)^2} \in \langle 0, 1\rangle. \tag{2.2}$$

Ako zamijenimo parametar t s parametrom $\frac{1-t}{1+t}$ u formuli 2.2, dobit ćemo istu vrijednost za T.

Poglavlje 3

Iterativna konstrukcija niza pravokutnih trokuta

Danom pravokutnom trokutu s racionalnim duljinama stranica površine $\mathcal{A}$ možemo pridružiti parametar t, kao u odjeljku 2.1. Zatim, poistovjećujući $t_1 = t$ i koristeći metodu iz odjeljka 2.2 možemo konstruirati novi pravokutni trokut s racionalnim duljinama stranica površine $\mathcal{A}r_2^2$, za neki $r_2 \in \mathbb{Q}$, s parametrom $t_2 = T$. Ponavljajući navedenu konstrukciju stvara se beskonačan niz racionalnih brojeva $t_1, t_2, \ldots$, gdje je t_k parametar pravokutnog trokuta s racionalnim duljinama stranica površine $\mathcal{A}r_k^2$, za neki racionalni broj r_k, $k \in \mathbb{N}$, i $t_{k+1} = \frac{4t_k(1-t_k^2)}{(1+t_k^2)^2}$ (vidi jednadžbu (2.2)).

Prema [2], počevši s Pitagorinom trojkom (3, 4, 5), sljedeća trojka je (49, 1200, 1201), nakon koje slijedi (339252715200, 2066690884801, 2094350404801). Uočavamo brzi rast brojeva, stoga je nemoguće iteriranjem konstrukcije iz odjeljka 2.2 dobiti slične trokute.

racionalan broj t_k, $k \in \mathbb{N}$, možemo zapisati kao $t_k = \frac{m_k}{n_k}$, gdje su m_k, n_k relativno prosti prirodni brojevi. Za utvrđivanje da su svi t_j, $j \in \mathbb{N}$, međusobno različiti te da stvaraju trokute među kojima nema sličnih, treba dokazati da vrijedi: $n_1 < n_2 < n_3 < \ldots$.

Teorem 3.0.1. *Ako postoji jedan pravokutan trokut s racionalnim duljinama stranica površine $\mathcal{A}$, tada postoji beskonačno mnogo takvih trokutova.*

Dokaz. Neka je $t = \frac{m}{n}$, gdje su m i n relativno prosti prirodni brojevi različite parnosti, $m < n$. Neka je $T = \frac{M}{N}$, gdje su $M = 4mn(n^2 - m^2)$ i $N = (n^2 + m^2)^2$ relativno prosti prirodni brojevi, pri čemu je M paran, a N neparan (vidi odjeljak 2.1 i formulu (2.2)). Za svaki $k \in \mathbb{N}$, vrijedi $n_{k+1} = (m_k^2 + n_k^2)^2$ i $n_k^4 < n_{k+1} < 4n_k^4$, $m_k < n_k$, $t_k \in \langle 0, 1\rangle$. Naime, za parametre t_k u nizu $t_1, t_2, \ldots$ dovoljno je gledati samo nazivnike pa da svi budu različiti. Uočimo da su parametri prikazani kao skraćeni razlomci $\frac{m_k}{n_k}$, a zbog toga što su međusobno različiti slijedi da trokuti nisu međusobno slični. Pretpostavimo da su jednaki

neki t_j i t_k, $j,k \in \mathbb{N}$. Tada je $\frac{m_j}{n_j} = \frac{m_k}{n_k}$ i odatle imamo jednakost umnožaka prirodnih brojeva $m_j \cdot n_k = m_k \cdot n_j$. Sada iskoristimo da su relativno prosti m_j i n_j te m_k i n_k. Kako m_j dijeli lijevu stranu, mora dijeliti i desnu, a budući da je relativno prost s n_j, mora biti i djelitelj od m_k. Analogno, kako m_k dijeli desnu stranu, mora dijeliti i lijevu, ali relativno je prost s n_k te mora dijeliti od m_j. Dakle, imamo dva prirodna broja koji su uzajamno djeltelji pa moraju biti jednaki. Slijedi da su jednaki i n_j i n_k. Zaključujemo, ako su ovakvi skraćeni razlomci jednaki, onda su jednaki posebno brojnici i posebno nazivnici.

Budući da smo dokazali da je niz nazivnika strogo rastući, nema podudaranja među nazivnicima pa onda ni među cijelim razlomcima, to jest vrijednostima parametara. □

Proučavanjem jednostavnog primjera Pitagorinih trojki (3, 4, 5), iz kojih su konstruirani pravokutni trokuti s cjelobrojnim duljinama stranica, koristeći metodu danu u odjeljku 2.2, uočavamo da su duljine kateta redom jednake 7^2 i $3 \cdot 20^2$, zatim $3 \cdot 336280^2$ i 1437599^2. U svakom primjeru duljina jedne katete je *kvadrat* nekog broja, a duljina druge katete je oblika $2\mathcal{A} \cdot$ *kvadrat*. Generalizirajući navedeno opažanje, Chan u [2] daje formule za cjelobrojne i relativno proste duljine kateta novog pravokutnog trokuta, dobivenog iz pravokutnog trokuta s cjelobrojnim i relativno prostim duljinama stranica x, y i z:

$$(x^2 - y^2)^2 \quad \text{i} \quad 4xyz^2 = 2\mathcal{A} \cdot (2z)^2. \tag{3.1}$$

Izrazi u (3.1) jednaki su redom izrazima:

$$(1 - T^2) \cdot z^4 \quad \text{i} \quad 2T \cdot z^4.$$

Zaključujemo da je izraz $1 - T^2$ kvadrat nekog racionalnog broja. Štoviše, izrazi

$$1 - T = 1 - 2uv = (u - v)^2 \quad \text{i} \quad 1 + T = 1 + 2uv = (u + v)^2$$

kvadrati su racionalnih brojeva. Uočavamo da novi trokuti konstruirani na ovakav način imaju vrlo specifičan oblik.

Teorem 3.0.2. *Za dani pravokutni trokut s duljinama stranica* $(1-T^2, 2T, 1+T^2)$*, gdje su* $1-T$ *i* $1+T$ *kvadrati racionalnih brojeva, postoji pravokutni trokut s duljinama stranica* $(u, v, 1)$ *takav da je* $T = 2uv$*, gdje su* $u, v \in \mathbb{Q}$*. Omjer njihovih površina kvadrat je racionalnog broja.*

Dokaz. Neka su $1 - T = r^2$ i $1 + T = s^2$, gdje su r i s racionalni brojevi. Nadalje, neka su $u = \frac{r+s}{2}$ i $v = \frac{s-r}{2}$. Slijedi, $u^2 + v^2 = \frac{1}{2}(r^2 + s^2) = 1$ i $2uv = \frac{1}{2}(s^2 - r^2) = T$.
Za dani pravokutni trokut s duljinama stranica $(u, v, 1)$ možemo konstruirati originalni trokut metodom iz odjeljka 2.2, i pri tome je omjer njihovih površina kvadrat racionalnog broja. □

Međutim, teoremom 3.0.2 ne mogu se pronaći svi pravokutni trokuti s cjelobrojnim duljinama stranica. Na primjer, za trokut s duljinama stranica 9, 40, 41, parametar $t = \frac{4}{5}$. Iako je $1 - t^2 = \left(\frac{3}{5}\right)^2$ kvadrat racionalnog broja, $1 - t = \frac{1}{5}$ i $1 + t = \frac{9}{5}$ nisu kvadrati niti jednog racionalnog broja. Stoga se nameće pitanje kako pronaći sve takve pravokutne trokute, a odgovor se nalazi u sljedećem poglavlju.

Poglavlje 4

Kongruentni brojevi i eliptičke krivulje

Cilj ovoga poglavlja je pokazati da pravokutni trokuti s racionalnim duljinama stranica x, y, z zadane površine $\mathcal{A}$ daju racionalne točke na eliptičkoj krivulji. Pojmovi „racionalna točka“ i „eliptička krivulja“ bit će definirani u nastavku (vidi definicije 4.2.2 i 4.3.1).

4.1 Od kongruentnih brojeva do eliptičkih krivulja

Kao u dokazu propozicije 1.3.2 imamo $x^2 + y^2 = z^2$, $\mathcal{A} = \frac{1}{2}xy$ te je $w = \frac{z}{2}$. Malim modifikacijama dobivamo

$$w^2 + \mathcal{A} = \left(\frac{u}{2}\right)^2, \quad w^2 - \mathcal{A} = \left(\frac{v}{2}\right)^2.$$

Nadalje,

$$\begin{aligned}\left(w \cdot \frac{u}{2} \cdot \frac{v}{2}\right)^2 &= w^2(w^2 + \mathcal{A})(w^2 - \mathcal{A}) \\ &= w^6 - \mathcal{A}^2 w^2.\end{aligned}$$

Na lijevoj strani je kvadrat racionalnog broja. Uvedimo supstituciju $w = X$, $w \cdot \frac{u}{2} \cdot \frac{v}{2} = Y$, pa imamo

$$Y^2 = X^3 - \mathcal{A}^2 X.$$

Vidimo da $\left(w^2, \frac{wuv}{4}\right)$ čini jedno racionalno rješenje jednadžbe $Y^2 = X^3 - \mathcal{A}^2 X$.

Krivulju s jednadžbom $Y^2 = X^3 - \mathcal{A}^2 X$ označit ćemo s $E_{\mathcal{A}}$. To je primjer tzv. *eliptičke krivulje*. Odsad ćemo jednadžbu krivulje pisati u uobičajenom obliku

$$E_{\mathcal{A}}: \quad y^2 = x^3 - \mathcal{A}^2 x. \tag{4.1}$$

Zaključujemo da postojanje kongruentnog broja $\mathcal{A}$ implicira postojanje točke s racionalnim koordinatama, ukratko racionalne točke, na krivulji $E_{\mathcal{A}}$, takve da je $y \neq 0$. U nastavku ćemo promatrati navedenu krivulju, no za sada je važno uočiti da za prethodni postupak dobivanja racionalne točke na krivulji $E_{\mathcal{A}}$ može postojati i obrnuti postupak. Stoga je potrebno otkriti koja svojstva trebaju imati točke (x, y), $x, y \in \mathbb{Q}$ na eliptičkoj krvulji oblika $E_{\mathcal{A}}$ za dokazivanje da je $\mathcal{A}$ kongruentan broj, odnosno da postoji pravokutni trokut s racionalnim duljinama stranica zadane površine $\mathcal{A}$ [1].

Propozicija 4.1.1. *Neka su $x_0, y_0 \in \mathbb{Q}$ takvi da je $y_0^2 = x_0^3 - \mathcal{A}^2 x_0$. Pretpostavimo da x_0 zadovoljava sljedeće uvjete:*

(1) *x_0 je kvadrat racionalnog broja*

(2) *nazivnik od x_0 je paran*

(3) *brojnik od x_0 je relativno prost s $\mathcal{A}$.*

Tada postoji pravokutni trokut s racionalnim duljinama stranica površine $\mathcal{A}$, koji je povezan s x_0.

Dokaz. Dokaz ćemo provesti unatrag, nizom koraka kojim smo došli do jednadžbe $y^2 = x^3 - \mathcal{A}^2 x$. Neka je $x_0 = w^2$, $w \in \mathbb{Q}$. Nadalje, neka je $v = \frac{y_0}{w}$ takav da $v^2 = \frac{x_0^3 - \mathcal{A}^2 x_0}{x_0} = x_0^2 - \mathcal{A}^2$. Tada je

$$x_0^2 = \mathcal{A}^2 + v^2. \tag{4.2}$$

Neka je t nazivnik od w. S obzirom da je $w^2 = x_0$ i po pretpostavci t je paran, mora vrijediti $2 \mid t$. Uočimo da v^2 i x_0^2 imaju isti nazivnik, t^4, jer je $\mathcal{A} \in \mathbb{N}$ i $\mathcal{A}^2 + v^2 = x_0^2$. Množenjem jednadžbe (4.2) s t^2 dobivamo primitivnu Pitagorinu trojku $t^2 v$, $t^2\mathcal{A}$, $t^2 x_0$, gdje je $t^2\mathcal{A}$ paran. Brojnik od x_0 i $\mathcal{A}$ nemaju zajedničkih faktora pa zaključujemo da je $gcd(t^2 v, t^2\mathcal{A}, t^2 x_0) = 1$. Primjenom teorema 1.1.1 zaključujemo da postoje prirodni brojevi m, n takvi da je $t^2 v = m^2 - n^2$, $t^2\mathcal{A} = 2mn$ i $t^2 x_0 = m^2 + n^2$.

Primitivnom Pitagorinom trojkom $x = \frac{2n}{t}$, $y = \frac{2m}{t}$, $z = 2w$ određen je pravokutni trokut

$$\begin{aligned} x^2 + y^2 &= \frac{4}{t^2}(m^2 + n^2) \\ &= \frac{4}{t^2}(t^2 x_0) \\ &= 4x_0 \\ &= (2w)^2 \\ &= z^2. \end{aligned}$$

Površina dobivenog trokuta dana je s

$$\begin{aligned}\frac{1}{2}xy &= \frac{1}{2}\frac{4mn}{t^2}\\ &= \frac{2mn}{t^2}\\ &= \mathcal{A}.\end{aligned}$$

Dakle, dobili smo pravokutni trokut s racionalnim duljinama stranica površine $\mathcal{A}$, kao što smo i tvrdili. □

Prethodna propozicija 4.1.1 koristit će nam za dokazivanje sljedeće, koja ima veću primjenu u pridruživanju točaka $x_0,\ y_0 \in \mathbb{Q}$ na krivulji $y_0^2 = x_0^3 - \mathcal{A}^2 x_0$ pravokutnim trokutima s racionalnim duljinama stranica i površinom $\mathcal{A}$ [1].

Propozicija 4.1.2. *Neka su skupovi A i B dani s*

$$\begin{aligned}A &= \left\{(X,Y,Z) \in \mathbb{Q}^3 : \frac{1}{2}XY = \mathcal{A},\ X^2 + Y^2 = Z^2\right\}\\ B &= \left\{(x,y) \in \mathbb{Q}^2 : y^2 = x^3 - \mathcal{A}^2 x,\ y \neq 0\right\}.\end{aligned}$$

Tada je bijekcija između skupova A i B dana sljedećim preslikavanjima:

$$f(X,Y,Z) = \left(-\frac{\mathcal{A}Y}{X+Z}, \frac{2\mathcal{A}^2}{X+Z}\right)$$

i

$$g(x,y) = \left(\frac{\mathcal{A}^2 - x^2}{y}, -\frac{2x\mathcal{A}}{y}, \frac{\mathcal{A}^2 + x^2}{y}\right).$$

Dokaz. Želimo dokazati sljedeće:

$$f\left(\frac{\mathcal{A}^2 - x^2}{y}, -\frac{2x\mathcal{A}}{y}, \frac{\mathcal{A}^2 + x^2}{y}\right) = (x,y)$$

i

$$g\left(-\frac{\mathcal{A}Y}{X+Z}, \frac{2\mathcal{A}^2}{X+Z}\right) = (X,Y,Z)\,.$$

Pokažimo prvo da je preslikavanje f dobro definirano.

$$\begin{aligned}-\frac{\mathcal{A}\cdot\left(-\frac{2x\mathcal{A}}{y}\right)}{\frac{\mathcal{A}^2-x^2}{y} + \frac{\mathcal{A}^2+x^2}{y}} &= \frac{\frac{2x\mathcal{A}^2}{y}}{\frac{2\mathcal{A}^2}{y}}\\ &= x.\end{aligned}$$

Analogno se pokaže za y.
Nadalje, pokažimo da je preslikavanje g dobro definirano,

$$\begin{aligned}\frac{\mathcal{A}^2 - \left(-\frac{\mathcal{A}Y}{X+Z}\right)^2}{\frac{2\mathcal{A}^2}{X+Z}} &= \frac{1 - \frac{Y^2}{(X+Z)^2}}{\frac{2}{X+Z}} \\ &= \frac{(X+Z)^2 - Y^2}{2(X+Z)} \\ &= \frac{X^2 + 2XZ + X^2}{2(X+Z)} \\ &= \frac{2X(X+Z)}{2(X+Z)} \\ &= X.\end{aligned}$$

Analogno se pokaže za Y i Z.
Dakle, postoji bijekcija između skupova A i B. □

U nastavku ćemo dati jednu drugu karakterizaciju točke $P = (x, y)$ na eliptičkoj krivulji $y^2 = x^3 - \mathcal{A}^2 x$, koja odgovara pravokutnom trokutu s racionalnim duljinama stranica zadane površine $\mathcal{A}$.

4.2 Osnovno o projektivnoj ravnini

Uzmimo trojku kompleksnih brojeva (x, y, z) takvih da je $(x, y, z) \neq (0, 0, 0)$. Definirajmo relaciju ekvivalencije na takvim trojkama: $(x, y, z) \sim (a, b, c)$ ako $x = \lambda a$, $y = \lambda b$, $z = \lambda c$, za neki $\lambda \in \mathbb{C}\backslash\{0\}$. Označimo klasu ekvivalencije koja sadrži (x, y, z) s $(x : y : z)$. Skup klasa ekvivalencije trojki naziva se *projektivna ravnina* $\mathbb{P}^2_{\mathbb{C}}$, odnosno:

$$\mathbb{P}^2_{\mathbb{C}} = \left\{(x : y : z) : x, y, z \in \mathbb{C}, (x, y, z) \neq (0, 0, 0)\right\}.$$

Napomena 4.2.1. *Projektivna ravnina ne mora se konstruirati preko skupa kompleksnih brojeva. Na primjer, projektivne ravnine $\mathbb{P}^2_{\mathbb{R}}$ i $\mathbb{P}^2_{\mathbb{Q}}$ definiraju se analogno projektivnoj ravnini $\mathbb{P}^2_{\mathbb{C}}$.*

Projektivna ravnina je proširenje afine ravnine nad poljem $\mathbb{K}$. Točki (x, y) afine ravnine odgovara točka $(x : y : 1)$ projektivne ravnine, dok obratno, ako je $(x_0 : y_0 : z_0)$ točka projektivne ravnine sa $z_0 \neq 0$, njoj odgovara točka (x, y) s $x = \frac{x_0}{z_0}$, $y = \frac{y_0}{z_0}$ euklidske ravnine. Klase $(x : y : z)$ za koje je $z = 0$ nazivaju se *točkama u beskonačnosti*, a geometrijski odgovaraju klasama paralelnih pravaca euklidske ravnine. Klasi skupa $k \in \mathbb{R}$, dakle, pravcima oblika $y = kx + l$, pridružena je točka $(1 : k : 0)$, dok je pravcu $x = c = const.$

pridružena beskonačno daleka točka $(0 : 1 : 0)$. Točku $(0 : 1 : 0)$ označit ćemo s O i ta zajednička točka svih vertikalnih pravaca, paralelnih s osi y, pripada svakoj eliptičkoj krivulji.

Definicija 4.2.2. *Za točku $P = (x_0 : y_0 : z_0)$ kažemo da je na eliptičkoj krivulji $F(x, y, z) = 0$ ako $F(x_0, y_0, z_0) = 0$. Kažemo da je P racionalna točka na krivulji $F(x, y, z) = 0$ ako se P nalazi na krivulji i $x_0, y_0, z_0 \in \mathbb{Q}$. Ako krivulju označimo sa $C : F(x, y, z) = 0$, tada je skup racionalnih točaka dan s $C(\mathbb{Q})$.*

4.3 Općenito o eliptičkim krivuljama

Definicija 4.3.1. *Eliptička krivulja nad poljem $\mathbb{K}$ je nesingularna projektivna kubna krivulja nad $\mathbb{K}$ s barem jednom $\mathbb{K}$-racionalnom točkom.*

Prema [5], eliptička krivulja ima afinu jednadžbu oblika

$$F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0,$$

gdje su $a, b, \ldots, j \in \mathbb{K}$. Nesingularnost označava da je u svakoj točki na krivulji u projektivnoj ravnini $\mathbb{P}^2(\overline{\mathbb{K}})$ nad algebarskim zatvorenjem od $\mathbb{K}$ barem jedna parcijalna derivacija funkcije F različita od 0. Svaka takva jednadžba može se biracionalnim transformacijama (racionalna transformacija čiji je inverz također racionalna transformacija) svesti na oblik

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{4.3}$$

koji nazivamo *Weierstrassova forma*.

Nadalje, ako je karakteristika polja $\mathbb{K}$ različita od 2 i 3, tada se jednadžba (4.3) može transformirati u oblik

$$y^2 = x^3 + ax + b, \tag{4.4}$$

koji nazivamo *kratka Weierstrassova forma*. U jednadžbi (4.4) uvjet nesingularnosti je da kubni polinom $f(x) = x^3 + ax + b$ nema višestrukih nultočaka u $\overline{\mathbb{K}}$, što je ekvivalentno uvjetu da je diskriminanta $D = -4a^3 - 27b^2 \neq 0$.

U nastavku ćemo pod pojmom *eliptička krivulja* podrazumijevati skup točaka $(x, y) \in \mathbb{K} \times \mathbb{K}$ koje zadovoljavaju jednadžbu

$$E: \quad y^2 = x^3 + ax + b, \tag{4.5}$$

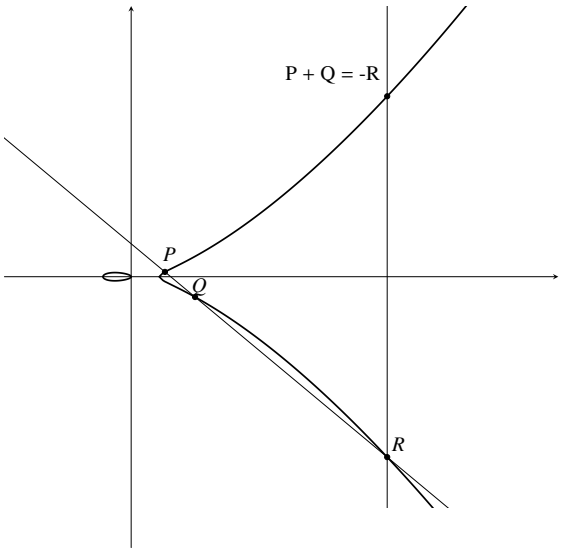
gdje su $a, b \in \mathbb{K}$ i $4a^3 + 27b^2 \neq 0$. Točke (x, y) zajedno s točkom u beskonačnosti O označavamo s $E(\mathbb{K})$. U slučaju racionalnih točaka (x, y) oznaka je $E(\mathbb{Q})$.

4.4 Struktura grupe na eliptičkoj krivulji

Važno svojstvo eliptičkih krivulja je da one uz operaciju zbrajanja čine Abelovu grupu (Teorem 2.1 u [12], str. 15.). Poincaré (1908.) je pokazao da kompleksne točke na eliptičkoj krivulji $E : y^2 = x^3 + ax + b$ čine grupu, čija je podgrupa $E(\mathbb{Q})$. Pri tome je operacija zbrajanja na $E(\mathbb{Q})$ definirana na sljedeći način ([11], str. 18.): Neka su $P = (x_P, y_P)$, $Q = (x_Q, y_Q) \in E(\mathbb{Q})$. Pravac kroz točke P i Q siječe krivulju E u tri točke. Označimo treću točku s $R = (x_R, y_R)$ i neka pravac ima jednadžbu $y = mx + c$. Uočimo da jednadžba ima racionalne koeficijente, jer su točke P, Q racionalne. Tada x-koordinate točaka P, Q, R moraju zadovoljavati jednadžbu:

$$x^3 - (mx + c)^2 + ax + b = x^3 + ax + b - y^2 = 0. \tag{4.6}$$

Stoga postoje tri korijena (rješenja) jednadžbe (4.6): x_P, x_Q i x_R, koji u zbroju daju m^2. Slijedi, x_R je racionalan. S obzirom da se točka R nalazi na pravcu $y = mx + c$, zaključujemo da je $R \in E(\mathbb{Q})$. Točku $P + Q$ definiramo kao osnosimetričnu točku točke R s obzirom na os x, $(x_R, -y_R)$, kao na slici 4.1.



Slika 4.1: Struktura grupe na eliptičkoj krivulji $y^2 = x^3 - 6^2x$

U slučaju $P = Q$, pravac je tangenta kroz točku P. Još uvijek vrijedi da pravac siječe krivulju u tri točke, ali sada moramo uzeti u obzir kratnost tih presjeka, stoga kažemo da pravac siječe krivulju dva puta u točki P. Točku $2P = P + P$ konstruiramo na analogan način, koristeći treću točku R presjeka pravca i krivulje, te primjenom osne simetrije na točku R s obzrom na os x. Detaljnija pojašnjanja navedenih izjava moguće je pronaći u [1].

Proširenjem do projektivne ravnine, svakoj eliptičkoj krivulji pridružena je i *točka u beskonačnosti*, $O = (0 : 1 : 0)$, kako je i navedeno u odjeljku 4.2. Naime, prijelazom na projektivne koordinate $\left(x \to \frac{x}{z}, y \to \frac{y}{z}\right)$ jednadžba $y^2 = x^3 + ax + b$ prelazi u oblik $y^2z = x^3 + axz^2 + bz^3$. Za $z = 0$ dobiva se $x^3 = 0$, stoga $x = 0$. Vidimo da je točka $O = (0 : 1 : 0)$ jedina točka u beskonačnosti ove krivulje, a pripada svakoj eliptičkoj krivulji. Nadalje, ako dvije točke na eliptičkoj krivulji leže na istom vertikalnom pravcu, njihov zbroj je O. Uočimo da je $O + P = P$, jer je pravac kroz O i P zapravo vertikalni pravac kroz P, koji siječe krivulju treći put i osnosimetrično preslikava točku P s obzirom na os x. Stoga sljedeća definicija objedinjuje ideje zbrajanja točaka na eliptičkoj krivulji.

Definicija 4.4.1. *Neka pravac p kroz točke $P = (x_P, y_P)$ i $Q = (x_Q, y_Q)$ na eliptičkoj krivulji E siječe krivulju u trećoj točki, $R = (x_R, y_R)$. Zbroj $P + Q$ definiramo kao osnosimetričnu sliku točke R preko osi x, $(x_R, -y_R)$.*
U slučaju tangente p na eliptičku krivulju E u jednoj njezinoj točki P, definiramo osnosimetričnu sliku točke presjeka p i E preko osi x kao zbroj $P + P$.

Primjer 4.4.2. *Jednadžba tangente u točki $P = (12, 36) \in E_6(\mathbb{Q})$ na krivulji E_6 dana je s $y = \frac{11}{2}x - 30$. Vrijedi, $x_R + 2x_P = \frac{121}{4}$, pa je $x_R = \frac{121}{4} - 24 = \frac{25}{4}$. Nadalje, $y_R = \frac{11}{2} \cdot \frac{25}{4} - 30 = \frac{35}{8}$. Stoga je $2P = \left(\frac{25}{4}, -\frac{35}{8}\right)$.*

4.5 Eliptičkom krivuljom do novog trokuta

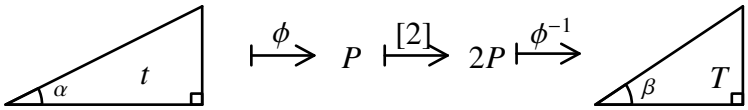
U odjeljku 2.1 vidjeli smo da skup pravokutnih trokuta s racionalnim duljinama stranica zadane vrijednosti površine $\mathcal{A}$ može biti prikazan skupom:

$$T_{\mathcal{A}} := \{t \in \mathbb{Q} : t(1 - t^2) = \mathcal{A}r^2, r \in \mathbb{Q}\}.$$

Definirajmo preslikavanje $\Phi : T_{\mathcal{A}} \to E_{\mathcal{A}}(\mathbb{Q})$ takvo da $\Phi(t) = \left(\frac{\mathcal{A}}{t}, \frac{r\mathcal{A}^2}{t^2}\right)$. Uočimo da je njegov inverz $\Phi^{-1}(x, y) = \frac{\mathcal{A}}{x}$. Stoga možemo prikazati bilo koji negativni element $\frac{-1}{t} \in \langle -\infty, -1\rangle$ u ovom skupu poistovjećujući ga s $t \in \langle 0, 1\rangle$. U ovom slučaju negativni dio $T_{\mathcal{A}} \cap \langle -\infty, -1\rangle$ može se prikazati samo kao kopija od $T_{\mathcal{A}} \cap \langle 0, 1\rangle$.

Jedan način za pronalazak novog trokuta u $T_{\mathcal{A}}$ iz danog $t \in T_{\mathcal{A}}$ je da prvo odredimo $P = \Phi(t)$, a zatim izračunamo $2P$ i na kraju postavimo $T = \Phi^{-1}(2P) \in T_{\mathcal{A}}$, kao na slici 4.2.

Primjer 4.5.1. *Počevši s pravokutnim trokutom čije su duljine stranica 3, 4, 5, imamo $t = \frac{1}{2} \in T_6$. Zatim, $P = \Phi(t) = (12, 36) \in E_6(\mathbb{Q})$. U primjeru 4.4.2 dobili smo da je $2P = \left(\frac{25}{4}, -\frac{35}{8}\right)$, pa je $T = \Phi^{-1}(2P) = \frac{24}{25} \in T_6$. Uočimo da je ovo ista vrijednost koju smo dobili iz geometrijske konstrukcije.*



Slika 4.2: Novi trokut pomoću udvostručavanja

Općenito, imamo $x(P) = \frac{\mathcal{A}}{t}$, zatim $x(2P) = \left(\frac{1+t^2}{2r}\right)^2$ i na kraju $T = \frac{4\mathcal{A}r^2}{(1+t^2)^2} = \frac{4t(1-t^2)}{(1+t^2)^2}$.

Prisjetit ćemo se dva teorema iz Poglavlja 3 i primijeniti ih u kontekstu eliptičkih krivulja. Pri tom je važno da se za svaku točku $P \in E_{\mathcal{A}}(\mathbb{Q})$, gdje je $x_P \neq 0, \mathcal{A}, -\mathcal{A}$, može dobiti $t = \Phi^{-1}(P) \in T_{\mathcal{A}}$.

Primjer 4.5.2. *Iz teorema 3.0.1 slijedi da su svi elementi iz niza $t_1 = t, t_2, \ldots \in T_{\mathcal{A}}$ različiti. Definiranjem $P_n = \Phi(t_n)$ dobivamo beskonačan niz različitih točaka $P_1 = P, P_2, \ldots \in E_{\mathcal{A}}(\mathbb{Q})$, gdje je $P_n = 2^n P$. Za točku P grupe $E_{\mathcal{A}}(\mathbb{Q})$ kažemo da je reda m u toj grupi ako je m najmanji prirodni broj takav da vrijedi $mP = 0$. Ako takav prirodni broj ne postoji, kažemo da je točka P beskonačnog reda u grupi. U grupi $E_{\mathcal{A}}(\mathbb{Q})$ jedine točke konačnog reda su točka O reda 1 i tri točke $(0, 0)$, $(\mathcal{A}, 0)$, $(-\mathcal{A}, 0)$ reda 2. Sve točke krivulje za koje je $x_P \neq 0, \mathcal{A}, -\mathcal{A}$ beskonačnog su reda u $E_{\mathcal{A}}(\mathbb{Q})$.*

Primjer 4.5.3. *Teorem 3.0.2 možemo reinterpretirati kao tvrdnju da je $P \in 2E_{\mathcal{A}}(\mathbb{Q})$ ako i samo ako $1 - T$ i $1 + T$ su oba kvadrati nekog broja, gdje je $T = \Phi^{-1}(P)$. Zapravo, teorem 3.0.2 pokazuje kako odrediti točku $R = \Phi\left(\frac{v}{u+1}\right) \in E_{\mathcal{A}}(\mathbb{Q})$, za koju vrijedi $P = 2R$. Sada svako rješenje jednadžbe $2Q = P$ mora biti oblika $Q = R + S$, gdje je $2S = O$. Dakle, $Q = R$, $R + (0, 0)$, $R + (\mathcal{A}, 0)$ ili $R + (-\mathcal{A}, 0)$. Ove točke odgovaraju četirima rješenjima $(\pm u, \pm v, 1)$ iz teorema 3.0.2, ali da bi odgovarali konkretnom trokutu trebamo ograničiti rješenja samo na ona u kojima su u i v oba pozitivni.*

Napomena 4.5.4. *Fermat*[1] *je dokazao da broj* 1 *nije kongruentan broj koristeći metodu zvanu* beskonačni spust*, koju možemo zamisliti kao uzastopno primjenjivanje teorema 3.0.2 kako bismo dobili sve manje i manje trokute i u konačnici došli do kontradikcije. Više o Fermatovoj metodi može se pronaći u Poglavlju II, §X, u [13]. Upravo je ta Fermatova metoda inspirirala Mordellov*[2] *dokaz ključnog teorema (1922.) da je za bilo koju eliptičku krivulju*

[1] Pierre de Fermat (1601. – 1665.), francuski matematičar i pravnik.

[2] Louis Joel Mordell (1888. – 1972.), britanski matematičar rođen u SAD-u.

E grupa $E(\mathbb{Q})$ konačno generirana (vidi [9], Poglavlje 16.). Šest godina kasnije Weil[3] je u svojoj disertaciji značajno poopćio taj rezultat, primjenom novih ideja koje su pridonijele boljem razumijevanju i pojednostavljenju Mordellova dokaza. Više o tome može se pronaći u [13].

4.6 Konstrukcija kompozicijom različitih preslikavanja

U Poglavlju 1., odjeljak 1.2, dokazali smo Diofantov rezultat o postojanju pravokutnih trokuta s cjelobrojnim duljinama stranica x, y, z i zadanom cjelobrojnom vrijednosti površine $\mathcal{A}$. Fibonacci je promatrao pravokutne trokute racionalnih duljina stranica i pokazao istinitost relacija:

$$z^2 + 4\mathcal{A} = (x+y)^2 \quad \text{i} \quad z^2 - 4\mathcal{A} = (x-y)^2.$$

Njihovim međusobnim množenjem i dijeljenjem sa 16 dobivamo:

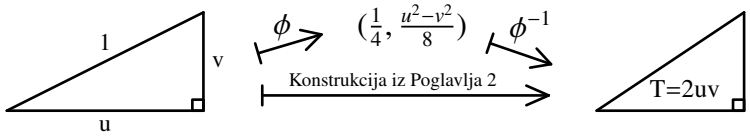
$$\left(\frac{z}{2}\right)^4 - \mathcal{A}^2 = \left(\frac{x^2-y^2}{4}\right)^2,$$

odnosno

$$r^4 - \mathcal{A}^2 = s^2,$$

gdje je $r = \frac{z}{2}$ i $s = \frac{x^2-y^2}{4}$.
Ovo daje racionalnu točku (r^2, rs) na krivulji kongruentnog broja $E_A : y^2 = x^3 - A^2x$. Preslikavanje $(x, y, z) \to (r^2, rs)$ označimo sa Ψ.

U odjeljku 4.5 pokazali smo da je preslikavanje Φ, koje koristi parametar t, dajući racionalnu točku $\left(\frac{\mathcal{A}}{t}, \frac{r\mathcal{A}^2}{t^2}\right)$, jednostavno invertirati na način da uvrstimo $t = \frac{\mathcal{A}}{x}$.
Pokušajmo povezati ova dva preslikavanja. Počinjemo s trokutom koji ima parametar t konstruirajući trokut s duljinama stranica u, v, 1 površine $\mathcal{A}$. Preslikavanje Ψ daje racionalnu točku $\left(\frac{1}{4}, \frac{u^2-v^2}{8}\right)$ na $E_{\mathcal{A}}$, a invertiranjem drugog preslikavanja dobivamo $T = 4\mathcal{A} = 2uv$, kao i prije (vidi sliku 4.3).



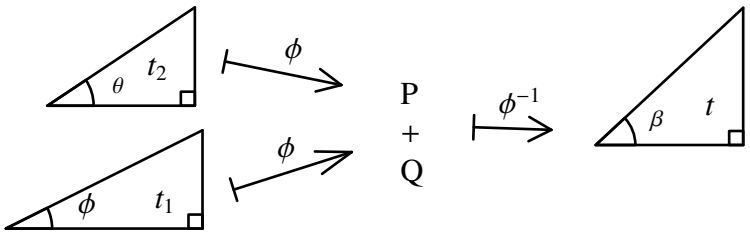
Slika 4.3: Kompozicija dva različita preslikavanja

[3] André Weil (1906. – 1998.), francuski matematičar.

Izračunajmo još što se dobiva djelovanjem preslikavanja Φ na drugu moguću vrijednost parametra. Označimo $\psi(t) := \frac{1-t}{1+t}$ na intervalu $\langle 0, 1\rangle$. Sada je $\psi(t)(1-\psi(t)^2) = \mathcal{A}\left(\frac{2r}{(1+t)^2}\right)^2$, pa je $\Phi(\psi(t)) = \left(\frac{\mathcal{A}(1+t)}{1-t}, 2r\left(\frac{\mathcal{A}}{1-t}\right)^2\right)$.

4.7 Zbrajanje dvije različite točke

Zbrajanje dvije različite točke P i Q na $E_{\mathcal{A}}(\mathbb{Q})$ treba na neki način odgovarati kombiniranju dva trokuta s racionalnim duljinama stranica površine $\mathcal{A}$ za konstruiranje još jednog takvog trokuta površine $\mathcal{A}$. Prikazat ćemo geometrijsku konstrukciju navedenoga, koja izravno daje traženi trokut, kao na slici 4.4.



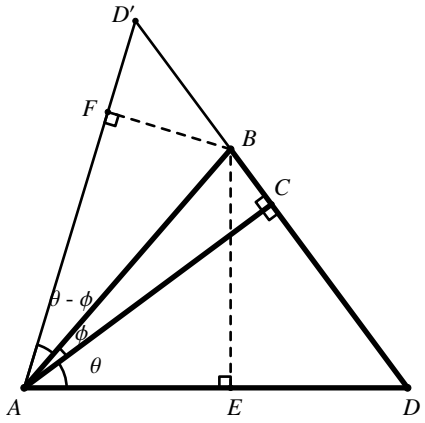
Slika 4.4: Dodavanje točaka koje odgovaraju nesličnim trokutima na krivulji kongruentnog broja

Počinjemo s dva različita trokuta racionalnih duljina stranica jednake površine. Skaliramo početne trokute tako da njihove duže katete imaju istu duljinu, a zatim ih poravnamo kao na slici 4.5. Dva trokuta su trokut ABC s kutom ϕ i trokut ACD s kutom θ, gdje je $|AB| = 1$. Nadalje, preslikavamo točku D preko pravca AC tako da dobijemo osnosimetričnu točku D' od točke D i kutove $\theta - \phi$ i $\theta + \phi$ (vidi sliku 4.5).

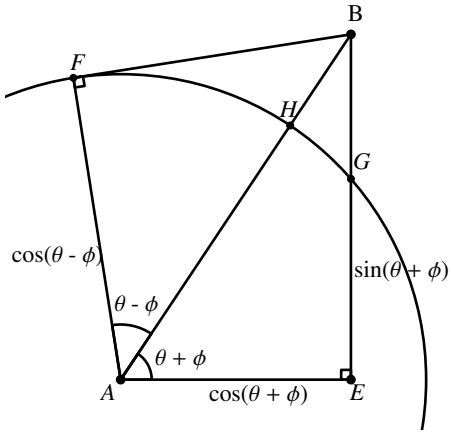
Kako je $|AB| = 1$, možemo zaključiti da su $\sin\phi = |BC|$, $\cos\phi = |AC|$, a tako i $|CD| = \operatorname{tg}\theta\cos\phi$, $|AD| = \frac{\cos\phi}{\cos\theta}$ svi racionalni brojevi. Primjenom funkcija sin, cos i tg na kutove $\theta - \phi$ i $\theta + \phi$, također dobivamo racionalne brojeve.

Trokut ABC ima površinu $\frac{1}{2}\cdot AC\cdot BC = \frac{1}{2}\sin\phi\cos\phi = \frac{1}{4}\sin 2\phi$, a trokut ACD ima površinu $\frac{1}{2}\cdot AC\cdot CD = \frac{1}{2}\cos^2\phi\operatorname{tg}\theta = \frac{1}{4}\left(\frac{\cos\phi}{\cos\theta}\right)^2\sin 2\theta$. Naša je pretpostavka da je omjer ovih površina kvadrat racionalnog broja. Stoga njihov umnožak mora biti kvadrat, iz čega slijedi da je $\sin 2\phi\sin 2\theta$ kvadrat racionalnog broja. Nazovimo ga R^2.

Spustimo okomicu iz točke B na stranice $\overline{AD}$ i $\overline{AD'}$. Redom dobivamo točke presjeka E i F. Promotrimo sada trokute ABE i ABF. Kružnica sa središtem u točki A radijusa $|AF|$ presijeca stranicu $\overline{AB}$ u točki H i stranicu $\overline{BE}$ u točki G, kao na slici 4.6.



Slika 4.5: Dobivanje kutova $\theta \pm \phi$



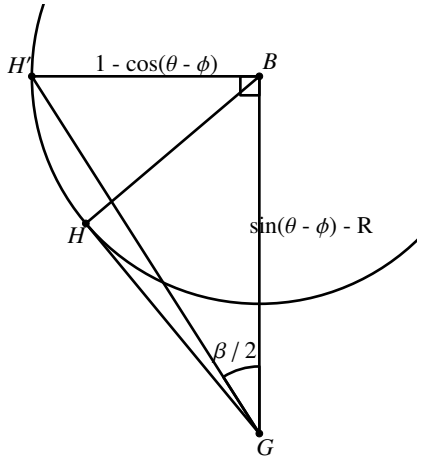
Slika 4.6: Konstruiranje duljina $|AH| = \cos(\theta - \phi)$ i $|EG| = R$

Sada neka je $|AH| = |AG| = |AF| = \cos(\theta - \phi)$ i $|BH| = |AB| - |AH| = 1 - \cos(\theta - \phi)$. Povrh toga,

$$|EG| = \sqrt{AG^2 - AE^2} = \sqrt{\cos^2(\theta - \phi) - \cos^2(\theta + \phi)} = \sqrt{\sin 2\theta \sin 2\phi} = R,$$

tako da $|BG| = |BE| - |GE| = \sin(\theta + \phi) - R$.

Trokut BGH sadrži informaciju koju trebamo, posebno duljine $|BH|$ i $|BG|$. Rotirajmo stranicu $\overline{BH}$ u $\overline{BH'}$ tako da je $\overline{BH'}$ okomita na $\overline{BG}$ (vidi sliku 4.7).



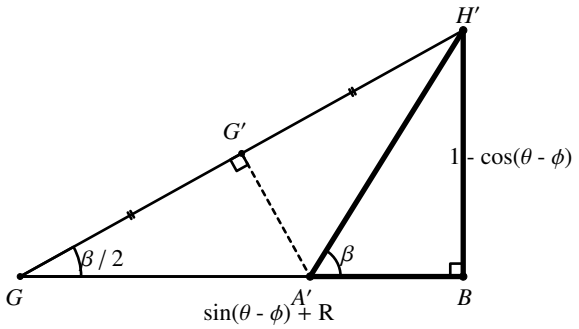
Slika 4.7: Rotiranje stranice BH za dobivanje pravokutnog trokuta

Neka je $\angle BGH' = \frac{\beta}{2}$. Vrijedi

$$\operatorname{tg}\left(\frac{\beta}{2}\right) = \frac{1 - \cos(\theta - \phi)}{\sin(\theta + \phi) - R}.$$

Slijedi da je $\operatorname{tg}\frac{\beta}{2}$ racionalan broj.

Simetrala stranice $\overline{GH'}$ siječe stranicu $\overline{BG}$ u točki A', dajući novi trokut $A'BH'$ s kutom β, kao što je prikazano na slici 4.8.



Slika 4.8: Konstruiranje trokuta iz parametra $\operatorname{tg}\frac{\beta}{2}$

Novi trokut $A'BH'$ bit će racionalan sve dok ima racionalne duljine stranica $|BH'| = 1 - \cos(\theta - \phi)$, $|A'B| = \frac{BH'}{\operatorname{tg}\beta}$ i $|A'H'| = \frac{BH'}{\sin\beta}$, gdje su $\sin\beta$ i $\operatorname{tg}\beta$ racionalne

funkcije od $\operatorname{tg}\frac{\beta}{2}$, tako da i oni moraju biti racionalni. Parametar za trokut $A'BH'$ je

$$\begin{aligned} t = \operatorname{tg}\left(\frac{\beta}{2}\right) &= \frac{(t_1 - t_2)^2}{t_2(1-t_1^2) + t_1(1-t_2^2) - 2\sqrt{t_1 t_2 (1-t_1^2)(1-t_2^2)}} \\ &= \left(\frac{t_1 - t_2}{\sqrt{t_2(1-t_1^2)} - \sqrt{t_1(1-t_2^2)}}\right)^2 = \left(\frac{\sqrt{t_2(1-t_1^2)} + \sqrt{t_1(1-t_2^2)}}{1 + t_1 t_2}\right)^2, \end{aligned} \tag{1}$$

gdje je t_1 parametar trokuta ABC i t_2 parametar trokuta ADC, tako da do na kvadrat ti trokuti imaju površine $T_1 = \frac{4t_1(1-t_1^2)}{(1+t_1^2)^2} = \sin 2\phi$ i $T_2 = \frac{4t_2(1-t_2^2)}{(1+t_2^2)^2} = \sin 2\theta$. Stoga je $R^2 = T_1 T_2$. Lako se pokaže da su brojnik i nazivnik od t_1 i od t_2 različite parnosti.

Površina novog trokuta je

$$\begin{aligned} \frac{4 \cdot P(A'BH')}{|A'H'|^2} = T &= \frac{4t(1-t^2)}{(1+t^2)^2} \\ &= \left(\frac{(4t_1 t_2 - (1-t_1^2)(1-t_2^2))(\sqrt{T_1} + \sqrt{T_2})}{4t_1 t_2 + (1-t_1^2)(1-t_2^2) + 2(1-t_1 t_2)(t_1 + t_2)\sqrt{T_1 T_2}}\right)^2. \end{aligned}$$

Dakle, ako je $T_1 = \mathcal{A}r_1^2$ i $T_2 = \mathcal{A}r_2^2$, tada $T = \mathcal{A}r^2$, gdje je

$$r = \frac{(4t_1 t_2 - (1-t_1^2)(1-t_2^2))(r_1 + r_2)}{4t_1 t_2 + (1-t_1^2)(1-t_2^2) + 2(1-t_1 t_2)(t_1 + t_2)\mathcal{A}r_1 r_2}.$$

Oduzimanje dvije različite točke

Oduzimanjem točke P od točke Q na $E_{\mathcal{A}}(\mathbb{Q})$ dobivamo drugačije trokute. Dva različita trokuta s parametrima t_1 i t_2 dat će novi trokut s parametrom

$$t = \left(\frac{\sqrt{t_2(1-t_1^2)} - \sqrt{t_1(1-t_2^2)}}{1 + t_1 t_2}\right)^2, \tag{2}$$

površine $T = \frac{4t(1-t^2)}{(1+t^2)^2} = \mathcal{A}r^2$, gdje je

$$r = \frac{(4t_1 t_2 - (1-t_1^2)(1-t_2^2))(r_1 - r_2)}{4t_1 t_2 + (1-t_1^2)(1-t_2^2) - 2(1-t_1 t_2)(t_1 + t_2)\mathcal{A}r_1 r_2}.$$

Isti parametar dobije se ako prvo zbrojimo trokute, uzimajući u obzir parametre $\Psi(t_1) = \frac{1-t_1}{1+t_1}$ i t_2 te oznaku θ za drugi kut trokuta ACD kao u prethodno izloženoj geometrijskoj konstrukciji, a zatim primijenimo Ψ na rezultirajući parametar. Ovaj proces

također je geometrijska konstrukcija, koju nazivamo oduzimanje, zato što, ako su nam dani parametri t_1 i t_2 i rezultat je t_3 u jednadžbi (1), možemo ponovno dobiti t_1 tako da primijenimo jednadžbu (2) na t_3 i t_2.

Poglavlje 5

Skup pravokutnih trokuta s racionalnim stranicama zadane površine $\mathcal{A}$

Neka $T_{\mathcal{A}}$ označava skup svih pravokutih trokuta racionalnih duljina stranica i zadane vrijednosti površine $\mathcal{A}$. Skup $T_{\mathcal{A}}$ u bijekciji je sa skupom parametara $t = \frac{m}{n} \in T_{\mathcal{A}}$, gdje su m i n relativno prosti prirodni brojevi različite parnosti. Definirajmo zbrajanje i oduzimanje na $T_{\mathcal{A}}$, kao što smo geometrijski opisali u prethodnom poglavlju (odjeljak 4.7), tako da novi trokuti imaju parametre redom dane s (1) i (2). Može se pokazati da ako krenemo s parametrima čiji su brojnici i nazivnici različite parnosti, tada će novi parametar dobiven iz (1) i (2) imati isto svojstvo. U nastavku ćemo se ograničiti na takve parametre u $T_{\mathcal{A}}$. Uočimo pritom da su $\triangle_1 - \triangle_2$ i $\triangle_2 - \triangle_1$ jedan te isti trokut.

5.1 Konačan skup generatora

Definirajmo preslikavanje $W : T_{\mathcal{A}} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$ s $W(t) = (1 - t, 1 + t)$. Dva racionalna broja jednaka su u $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ ako je njihov omjer kvadrat racionalnog broja. Ovo preslikavanje je homomorfizam, jer ako $\triangle_1 + \triangle_2 = \triangle_3$ redom odgovara pripadajućim parametrima t_1, t_2 i t_3, iz izraza za t_3 u (1) dobivamo

$$\begin{aligned}(1 + t_1)(1 + t_2)(1 + t_3) &= \left(\frac{(1 + t_1)(1 + t_2) + \sqrt{t_1 t_2 (1 - t_1^2)(1 - t_2^2)}}{1 + t_1 t_2} \right)^2 \\ &= \left((1 + t_1)(1 + t_2) + \frac{1}{4} \mathcal{A} r_1 r_2 (1 + t_1^2)(1 + t_2^2) \right)^2 \\ &= 1\end{aligned}$$

u $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Slično $(1 - t_1)(1 - t_2)(1 - t_3) = 1$ u $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

Iz teorema 3.0.2 slijedi da je $2T_{\mathcal{A}}$ jezgra od W, odnosno $t \in 2T_{\mathcal{A}}$ ako i samo ako $W(t) = (1,1)$. Ako t pripada skupu $2T_{\mathcal{A}}$, to znači da t odgovara trokutu dobivenom postupkom iz odjeljka 2.2, to jest da u skladu s relacijom (2.2) vrijedi

$$t = \frac{4s(1-s^2)}{(1+s^2)^2},$$

za neki s iz $T_{\mathcal{A}}$. Izravnim računom vidi se da su tada $1-t$, $1+t$ oba kvadrati racionalnih brojeva:

$$1 - t = \frac{(s^2+2s-1)^2}{(1+s^2)^2}$$

i

$$1 + t = \frac{(s^2-2s+1)^2}{(1+s^2)^2}.$$

Stoga je $W(t) = (1,1)$ u $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

Obrnuto, neka su $1-t$ i $1+t$ oba kvadrati racionalnih brojeva. Po Teoremu 3.0.2 tada vrijedi da je $t = 2uv$, pri čemu su u i v racionalni brojevi takvi da je $u^2 + v^2 = 1$. Tada umnožak uv ima oblik $\frac{2s(1-s^2)}{(1+s^2)^2}$ pa $t = 2uv$ ima oblik iz relacije (2.2). Zato se t nalazi u $2T_{\mathcal{A}}$. Naime, omjer površina trokuta za trojku $(u,v,1)$ i trokuta za trojku $(1-t^2, 2t, 1+t^2)$, koji se iz $(u,v,1)$ može dobiti postupkom iz 2.2, jednak je kvadratu nekog racionalnog broja. Nadalje, klase ekvivalencije $T_{\mathcal{A}}/2T_{\mathcal{A}}$ dane su s $\{t \in T_{\mathcal{A}} : W(t) = w\}$, za svaki $w \in W(T_{\mathcal{A}})$, i slika su od $T_{\mathcal{A}}$ dobivena preslikavanjem W.

Ako je $t = \frac{m}{n}$, gdje su m, n relativno prosti prirodni brojevi, onda $mn(m+n)(n-m) = n^4 t(1-t^2) = \mathcal{A}(rn^2)^2$. Ova četiri faktora m, n, $m+n$, $n-m$ u parovima su međusobno relativno prosti. Dakle, $m, n, m+n, n-m = a, b, c, d$ u $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, gdje je $abcd = \mathcal{A}$ u $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, te $W(t) = (bd, bc)$ za neke relativno proste brojeve b, c, d koji nisu kvadrati, gdje je bcd djelitelj od $\mathcal{A}$. Naime, kad znamo da je $(1-t_1)(1-t_2)(1-t_3)$ kvadrat racionalnog broja, dakle $(1-t_1)(1-t_2)(1-t_3) = 1$ u $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, onda je $(1-t_1)(1-t_2)(1-t_3)^2 = 1-t_3$ u istoj kvocijentnoj grupi, pa je odatle $(1-t_1)(1-t_2) = 1-t_3$ i, analogno, $(1+t_1)(1+t_2) = 1+t_3$. Ovo ograničava $W(T_{\mathcal{A}})$ na konačan skup mogućnosti, a iz toga slijedi da je $T_{\mathcal{A}}/2T_{\mathcal{A}}$ konačan.

Uzmimo cijeli skup $\mathcal{R}$ koji se sastoji od predstavnika klasa ekvivalencije u $T_{\mathcal{A}}/2T_{\mathcal{A}}$. Ako fiksiramo bilo koji t u $T_{\mathcal{A}}$, tada t mora biti u istoj klasi ekvivalencije s T u $\mathcal{R}$. Primijetimo da su pripadajući trokuti od t i T redom $\triangle$ i $\triangle'$. Slijedi, $\triangle + \triangle'$ je u jezgri od W pa postoji neki $\triangle_1$ s parametrom t_1 u $T_{\mathcal{A}}$ takav da

$$\triangle + \triangle' = 2\triangle_1.$$

Za dane $t = \frac{m}{n}$, $t_1 = \frac{m_1}{n_1}$ i $T = \frac{M}{N}$, gdje su m, n, m_1, n_1, M, N u parovima međusobno relativno prosti, trokut $\triangle + \triangle'$ ima parametar

$$\left(\frac{\sqrt{NM(n^2-m^2)} + \sqrt{nm(N^2-M^2)}}{nN+mM} \right)^2.$$

Nazivnik dijeli pa je stoga i manji od $(nN + mM)^2 < 4n^2N^2$. S druge strane, znamo da parametar od $2\triangle_1$ ima nazivnik veći od n_1^4, iz Poglavlja 3. Kombiniranje dvije nejednakosti daje $n_1^4 < 4n^2N^2$.

Nadalje, neka je C najveći od nazivnika svih elemenata iz $\mathcal{R}$. Tada, ako je $n \geqslant 2C$, imamo nejednakost $n_1 < \sqrt{2nN} \leqslant \sqrt{2Cn} \leqslant n$. Ponavljanjem navedenog postupka na t_1 induktivno dobivamo niz parametara $t_2, t_3, \ldots$ koji redom definiraju trokute $\triangle_2, \triangle_3, \ldots$ tako da za svaki $k \geqslant 1$ vrijedi

$$\triangle_k + \triangle_k' = 2\triangle_{k+1},$$

gdje $\triangle_k'$ ima parametar u $\mathcal{R}$ i t_k ima nazivnik n_k. Uz uvjet $n_k \geqslant 2C$, nazivnici formiraju strogo padajući niz cijelih brojeva $n_{k+1} < n_k < \ldots < n_1 < n$. Nakon konačnog broja koraka navedeni postupak mora dati t_K s nazivnikom $n_K < 2C$, pa iz toga slijedi relacija

$$\triangle + \triangle' + 2\triangle_1' + \ldots + 2^{K-1}\triangle_{K-1}' = 2^K\triangle_K.$$

Ovo se dobiva tako da se jednakosti $\triangle_k + \triangle_k' = 2\triangle_{k+1}$ najprije redom pomnože s 2^k pa se zatim zbroje. Parametri u $T_{\mathcal{A}}$ s nazivnicima manjim od $2C$ čine konačan skup koji sadrzi $\mathcal{R}$ i generira sve trokute u $T_{\mathcal{A}}$.

Time smo dokazali valjanost sljedećeg teorema.

Teorem 5.1.1. *Postoje trokuti $\triangle_1, \ldots, \triangle_r$ u $\mathcal{T}_{\mathcal{A}}$ takvi da za svaki trokut $\triangle \in \mathcal{T}_{\mathcal{A}}$ postoje cijeli brojevi $a_1, \ldots, a_r$ za koje vrijedi*

$$\triangle = a_1\triangle_1 + \ldots + a_r\triangle_r.$$

Ovime je zapravo pokazana varijanta Mordellovog teorema, samo u okviru geometrijske konstrukcije skupa trokuta. U originalnoj verziji Mordellovog teorema tvrdi se da je $E_{\mathcal{A}}(\mathbb{Q})$ konačno generirana Abelova grupa ranga r. Postoji baza $P_1, \ldots, P_r$ za $E_{\mathcal{A}}(\mathbb{Q})$ pa stoga i odgovarajuća baza koju sačinjavaju neki trokuti $\triangle_1, \ldots, \triangle_r$ u $\mathcal{T}_{\mathcal{A}}$. Preslikavanje W poseban je slučaj Weilovog preslikavanja na $E_{\mathcal{A}} : y^2 = x^3 - \mathcal{A}^2x$, što je homomorfizam

$$\begin{aligned} &E_{\mathcal{A}}(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \\ &(x, y) \mapsto (x, x - \mathcal{A}, x + \mathcal{A}), \end{aligned}$$

i dobro je poznato da ima jezgru $2E_{\mathcal{A}}(\mathbb{Q})$ (vidi Poglavlje X.1 u *The Arithmetic of Elliptic Curves* [10]). Weilovo preslikavanje nadahnuto je Fermatovom metodom spusta, a to je analogno preslikavanju W u izvođenju spusta u dokazu Mordellovog teorema.

Ostaje otvoreno pitanje efektivnog određivanja konačnog skupa generatora $\mathcal{R}$. Premda postoji eksplicitno zadan konačni skup mogućnosti za $W(T_{\mathcal{A}})$, time i za $T_{\mathcal{A}}/2T_{\mathcal{A}}$, u praksi se često mogu riješiti konkretni zadani primjeri, ali nije poznat algoritam koji bi

sigurno dovodio do rezultata općenito. Riječ je o jednom od istaknutih otvorenih problema u računarskoj aritmetičkoj geometriji, određivanju ranga grupe $E(\mathbb{Q})$ zadane eliptičke krivulje E.

5.2 Particija $T_{\mathcal{A}}$ s obzirom na parametar t

Primijetimo da kako su $\triangle_1, \ldots, \triangle_r$ nezavisni, slijedi da

$$a_1\triangle_1 + \ldots + a_r\triangle_r \ : \ 0 \leq a_1, \ldots, a_r \leq 1$$

daje potpuni skup predstavnika od $\mathcal{T}_{\mathcal{A}}/2\mathcal{T}_{\mathcal{A}}$ i $|\mathcal{T}_{\mathcal{A}}/2\mathcal{T}_{\mathcal{A}}| = 2^r$.

Kod $\frac{1}{2^r}$ trokuta $1-t$ i $1+t$ su oba kvadrati, tako da barem $\frac{1}{2^r}$ trokuta ima $1-t^2$ jednak kvadratu. To u formuli (1.1) odgovara da je $m^2 - n^2 = m^2(1-t^2)$ kvadrat. Stoga, najmanje $\frac{1}{2^r}$ primitivnih trokuta imaju jednu katetu duljine jednake kvadratu nekog racionalnog broja.

Primjer 5.2.1. *Neka je površina trokuta $\mathcal{A} = 6$. Tada je $E_6(\mathbb{Q})$ generiran točkom $P = (12, 36)$, koja odgovara trokutu $\triangle_P$ sa stranicama $(3, 4, 5)$ i parametrom $\frac{1}{2}$. Parni višekratnici od $\triangle_P$ imaju $(1-t, 1+t) = (1, 1) \mod (\mathbb{Q}^*)^2$, a neparni višekratnici od $\triangle_P$ imaju $(1-t, 1+t) = (2, 6) \mod (\mathbb{Q}^*)^2$. Skup $\mathcal{R}$ je $\left\{0, \frac{1}{2}\right\}$ pa je $C = 2$. Stoga postoje samo tri moguća razlomka s nazivnikom manjim od $2C = 4$: to su $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$ pa je $\triangle_P$ jedini trokut od ovih parametara koji je u $\mathcal{T}_6$.*

Primjer 5.2.2. *Površina trokuta $\mathcal{A} = 34$ najmanji je cijeli broj takav da je $r > 1$. Grupa $E_{34}(\mathbb{Q})$ ima $r = 2$, generiran točkama $P = \left(\frac{289}{4}, \frac{4335}{8}\right)$ i $Q = (578, 13872)$, što redom odgovara trokutima $\triangle_P = (225, 272, 353)$ i $\triangle_Q = (17, 144, 145)$. Skup trokuta $\mathcal{T}_{34}$ može se particionirati u četiri podskupa s predstavnicima prikazanim u sljedećoj tablici:*

Predstavnici	t	$W(t)$
0	0	$(1, 1)$
$\triangle_P = (225, 272, 353)$	$\frac{8}{17}$	$(17, 17)$
$\triangle_Q = (17, 144, 145)$	$\frac{8}{9}$	$(1, 17)$
$\triangle_P + \triangle_Q = (1377, 3136, 3425)$	$\frac{32}{49}$	$(17, 1)$

Skup $\mathcal{R} = \left\{0, \frac{8}{17}, \frac{8}{9}, \frac{32}{49}\right\}$ i $C = 49$. Provjerom svih mogućih razlomaka pronalazimo da su $\triangle_P$, $\triangle_Q$, $\triangle_P + \triangle_Q$ jedini trokuti iz $\mathcal{T}_{34}$ koji imaju parametre s nazivnicima manjim od $2C = 98$.

5.3 Daljnje primjene geometrijske metode

Geometrijska metoda može se primijeniti i na druge slučajeve.

Pretpostavimo da se promatra eliptička krivulja nad poljem $\mathbb{Q}(\sqrt{d})$ kao proširenjem polja racionalnih brojeva. Elementi tog polja su oblika $a + b\sqrt{d}$, pri čemu je d prirodni broj koji nije kvadrat prirodnog broja, dok su $a,\ b \in \mathbb{Q}$. Elementi $a + b\sqrt{d}$ i $a - b\sqrt{d}$ uzajamno su konjugirani, njihov zbroj je racionalni broj, a razlika im je $2b\sqrt{d}$. Za odgovarajuće točke na krivulji $E_{\mathcal{A}}(\mathbb{Q}(\sqrt{d}))$ tada vrijedi, analogno, da je zbroj konjugiranih točaka racionalna točka krivulje, to jest točka krivulje $E_{\mathcal{A}}(\mathbb{Q})$. Ako ta točka nije trivijalna, njome je određen pravokutni trokut s racionalnim stranicama. Opisani geometrijski postupak omogućuje izravnu konstrukciju tog novog trokuta.
Dakle, vrijedi:

Teorem 5.3.1. *Ako postoji pravokutan trokut s duljinama stranica u polju $\mathbb{Q}(\sqrt{d})$ i zadane racionalne vrijednosti površine $\mathcal{A}$, takav da racionalni dio od njegove hipotenuze nije jednak nuli, tada postoji pravokutan trokut s racionalnim stranicama površine $\mathcal{A}$.*

Nadalje, oduzimanjem točaka koje odgovaraju uzajamno konjugiranim brojevima $a + b\sqrt{d}$ i $a - b\sqrt{d}$ dobiva se točka P koja je konjugirana s točkom $-P$ na krivulji $E_{\mathcal{A}}(\mathbb{Q}(\sqrt{d}))$. Točka P može se tada interpretirati kao točka krivulje $E_{\mathcal{A}d}(\mathbb{Q})$ pomoću koje je određen pravokutni trokut s racionalnim stranicama površine $\mathcal{A}d$. Taj novi trokut također se može izravno konstruirati našim geometrijskim postupkom, čime se dobiva sljedeći rezultat:

Teorem 5.3.2. *Ako postoji pravokutan trokut s duljinama stranica u polju $\mathbb{Q}(\sqrt{d})$ i iracionalne duljine hipotenuze, sa zadanom racionalnom vrijednosti površine $\mathcal{A}$, onda postoji pravokutan trokut s racionalnim stranicama površine $\mathcal{A}d$.*

Vjerojatno su moguće i druge primjene ove geometrijske metode, koje bi dovele do drukčijeg pristupa i potpunijeg razumijevanja rezultata i otvorenih problema u području kongruentnih brojeva.

Bibliografija

[1] J. Brown, *Congruent Numbers and Elliptic Curves*, Clemson University (2007), http://www.math.caltech.edu/~jimlb/congruentnumberslong.pdf.

[2] S. Chan, *Rational Right Triangles of a Given Area*, The American Mathematical Monthly **125** (2018), br. 8, 689–703.

[3] L. E. Dickson, *History of the Theory of Numbers*, Chelsea Publishing Co., 1966.

[4] A. Dujella, *Uvod u teoriju brojeva*, PMF-Matematički odjel, Sveučilište u Zagrebu (skripta) (2006), https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf.

[5] ———, *Eliptičke krivulje u kriptografiji*, PMF-Matematički odjel, Sveučilište u Zagrebu (skripta) (2013), https://web.math.pmf.unizg.hr/~duje/elkript/elkripto2.pdf.

[6] Euklid, *Euclid's Elements: all thirteen books complete in one volume: the Thomas L. Heath translation*, Green Lion Press, 2002, Ed. by Densmore, D.

[7] L. P. Fibonacci, *The Book of Squares*, Academic Press, 1987, Translated by Sigler, L. E.

[8] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, sv. 97, Springer-Verlag, 1984.

[9] L. J. Mordell, *Diophantine Equations*, sv. 30, Academic Press, 1969.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, sv. 106, Springer Science & Business Media, 2009.

[11] J. H. Silverman i J. T. Tate, *Rational Points on Elliptic Curves*, Springer, 2015.

[12] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman and Hall/CRC, 2008.

[13] A. Weil, *Number Theory: An approach through history from Hammurapi to Legendre*, Springer Science & Business Media, 2006.

Sažetak

Jedan od najstarijih poznatih matematičkih problema odnosi se na određivanje pravokutnih trokuta čije su duljine stranica racionalni brojevi, a površina je jednaka zadanom prirodnom broju $\mathcal{A}$. U suvremenoj terminologiji takav broj $\mathcal{A}$ naziva se kongruentnim brojem. U ovom radu prikazana je geometrijska metoda kojom se za pojedini kongruentni broj $\mathcal{A}$, počevši od jednog pripadnog pravokutnog trokuta s racionalnim duljinama stranica, može iterativnim postupkom konstruirati niz trokuta s racionalnim stranicama i površinom oblika $\mathcal{A}r^2$, pri čemu je r racionalan broj.

Opis skupa $T_{\mathcal{A}}$ svih pravokutnih trokuta površine $\mathcal{A}$, s racionalnim duljinama stranica, blisko je povezan s grupom $E_{\mathcal{A}}(\mathbb{Q})$ racionalnih točaka eliptičke krivulje $E : y^2 = x^3 - \mathcal{A}^2 x$. Prikladnom parametrizacijom skupa $T_{\mathcal{A}}$ i primjenom geometrijske konstrukcije dobivaju se nove racionalne točke na krivulji. Na skupu $T_{\mathcal{A}}$ uvodi se algebarska struktura u kojoj se taj skup pokazuje konačno generiranim. U pojedinim primjerima na temelju toga moguće je potpuno opisati skup $T_{\mathcal{A}}$, no problem efektivnog algoritma za pronalaženja skupa generatora ostaje otvoren.

Summary

One of the oldest known problems in mathematical research is to determine all right-angled triangles with rational sidelengths such that their area equals a given positive integer $\mathcal{A}$. In modern terminology such a number $\mathcal{A}$ is called a congruent number. In this thesis, a geometric method of producing new rational-sided right triangles with area $\mathcal{A}$, starting from one given triangle, is exhibited. Iterating this construction, an infinite sequence of nonsimilar triangles with the same property may be obtained.

A description of the set $T_{\mathcal{A}}$ of all right-angled triangles with rational sidelengths and area $\mathcal{A}$ is closely related to the group $E_{\mathcal{A}}(\mathbb{Q})$ of rational points of the elliptic curve $E : y^2 = x^3 - \mathcal{A}^2 x$. By a suitable parametrization of $T_{\mathcal{A}}$ and application of the geometric construction, new rational points on E are obtained. An algebraic structure is introduced on $T_{\mathcal{A}}$, in which this set is shown to be finitely generated. Using that fact, in some specific examples it is possible to give a complete description of $T_{\mathcal{A}}$, but the problem of an effective algorithm for finding the set of generators remains open.

Životopis

Rođena sam u Zagrebu 29.9.1994. Osnovnu i srednju školu pohađala sam u Požegi. Preddiplomski sveučilišni studij Matematika; smjer: nastavnički upisala sam 2013., a Diplomski sveučilišni studij Matematika i informatika; smjer: nastavnički 2016. godine na Prirodoslovno-matematičkom fakultetu u Zagrebu.