

# Konstruktibilnost u planimetriji

---

Filipović, Glorija

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:217:293491>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-07-17**



Repository / Repozitorij:

[Repository of the Faculty of Science - University of Zagreb](#)



**SVEUČILIŠTE U ZAGREBU**  
**PRIRODOSLOVNO–MATEMATIČKI FAKULTET**  
**MATEMATIČKI ODSJEK**

Glorija Filipović

**KONSTRUKTIBILNOST U**  
**PLANIMETRIJI**

Diplomski rad

Voditelj rada:  
doc. dr. sc. Igor Ciganović

Zagreb, rujan, 2022.

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. \_\_\_\_\_

*Jednom malom zlatu...*

*Hvala dragom Bogu što je uvijek sa mnom.*

*Hvala mojim roditeljima, sestrama i bratu koji su mi na svaki moj "ne mogu" pokazali da "mogu"!*

*Hvala mom mentoru, profesoru Igoru Ciganoviću, koji je imao razmišljanja za mene.  
Hvala svim profesorima jer su na ovaj ili onaj način utjecali na smjer u kojem će se moj život razvijati.*

*Hvala mojoj bebi Lori što mi je dala vremena da napišem ovaj rad.  
I na kraju hvala mom suprugu Goranu što me kroz cijeli studij bodrio i vjerovao u mene više nego sam sama ikada, ali najviše mu hvala što je bio moj partner u vrijeme pisanja ovog rada. Bez njega ovo ne bih uspjela.*

*Još jednom, znate tko ste, hvala vam!*

# Sadržaj

<b>Sadržaj</b>	<b>iv</b>
<b>Uvod</b>	<b>1</b>
<b>1 Osnovne konstrukcijske metode ravnalom i šestarom</b>	<b>2</b>
1.1 Temeljne operacije ravnalom i šestarom . . . . .	3
1.2 Temeljne konstrukcije ravnalom i šestarom . . . . .	3
<b>2 Izvodljivost konstrukcija ravnalom i šestarom</b>	<b>13</b>
2.1 Algebarska metoda konstrukcije . . . . .	13
2.2 Proširenje polja racionalnih brojeva . . . . .	19
<b>3 Klasični geometrijski problemi</b>	<b>27</b>
3.1 Kvadratura kruga . . . . .	27
3.2 Duplikacija kocke . . . . .	32
3.3 Trisekcija kuta . . . . .	35
<b>4 Rješivost konstrukcija pravilnih mnogokuta</b>	<b>41</b>
<b>Bibliografija</b>	<b>47</b>

# Uvod

U ovom diplomskom radu raspravljat ćemo o elementarnim, tj. euklidskim konstrukcijama jednobridnim ravnalom i šestarom u planimetriji te ćemo opisati i vizualno prikazati neke od konstrukcija. Neke geometrijske situacije opisat ćemo koristeći se analitičkom geometrijom jer su na taj način često zadovoljeni polinomijalni uvjeti pa se egzistencija same konstrukcije ravnalom i šestarom može povezati s tipom proširenja polja racionalnih brojeva, koje sadrži korijene odgovarajućih polinoma. Tim pristupom pokazat ćemo da se ne mogu svi geometrijski objekti dobiti konstrukcijom ravnalom i šestarom. Tu su najpoznatiji takozvani klasični problemi, odnosno kvadratura kruga, duplikacija kocke i trisekcija kuta, ali i neki polinomi. Na kraju ćemo se posvetiti rješivosti konstrukcija pravilnih mnogokuta.

Ovaj diplomski rad podijeljen je u četiri poglavlja. U prvom poglavlju opisane su temeljne operacije i temeljne konstrukcije ravnalom i šestarom, iz kojih proizlaze sve ostale konstrukcije, popraćene odgovarajućim ilustracijama napravljenim u *Geogebra*. U drugom poglavlju bavimo se izvodljivošću konstrukcija ravnalom i šestarom. Opisujemo sve primjere algebarske metode konstrukcije ponovno uz ilustracije napravljene u *Geogebra*. Također, definiramo konstruktibilnost realnog broja te se bavimo proširenjem polja racionalnih brojeva kroz niz propozicija i teorema popraćenih dokazima. U trećem poglavlju opširno se bavimo trima klasičnim geometrijskim problemima, spominjemo starogrčke matematičare koji su ih pokušavali riješiti i na koji način. Također, priložili smo i dokaze o neizvedivosti njihovih konstrukcija koristeći isključivo ravnalo i šestar. I na kraju, u četvrtom poglavlju uz niz definicija i teorema obrađujemo rješivost konstrukcija pravilnih mnogokuta.

# Poglavlje 1

## Osnovne konstrukcijske metode ravnalom i šestarom

U ovom poglavlju uvodimo osnovne pojmove i konstrukcije pri čemu pratimo [5]. Pod osnovnim konstrukcijama ravnalom i šestarom u Euklidskoj ravnini smatrat ćemo sve konstrukcije koje su izvedive jednobridnim ravnalom (bez njegove paralelne strane i bez oznaka bilo kakve mjerne jedinice) te šestarom u konačno mnogo koraka. Ravnalom možemo povući spojnicu dviju točaka, odnosno pravac koji prolazi kroz dvije točke, a šestarom možemo oko svake točke opisati kružnicu proizvoljnog polumjera. Točke mogu biti ili unaprijed zadane ili dobivene presjekom dvaju pravaca, pravca i kružnice ili dviju kružnica. Dakle, točku smatramo konstruiranom ako je dobivena kao presjek dvaju pravaca, pravca i kružnice ili dviju kružnica; pravac smatramo konstruiranim ako mu možemo konstruirati bilo koje dvije točke, a kružnicu smatramo konstruiranom ako možemo konstruirati njezino središte i bilo koju njenu točku.

Osnovne konstrukcijske metode ravnalom i šestarom još nazivamo euklidskim konstrukcijama jer prva tri Euklidova postulata očigledno dopuštaju njihovo korištenje. Nabrojimo prva tri Euklidova postulata:

1. od svake točke do svake točke može se povući dužina
2. ograničena dužina produžuje se neograničeno
3. svakim središtem i udaljenošću opisuje se krug.

Prije nego krenemo dalje, definirajmo još jediničnu dužinu:

**Definicija 1.0.1.** *Pretpostavimo da su dane dvije različite točke  $O$  i  $E$  u danoj ravnini. Dužinu  $\overline{OE}$  smatramo **jediničnom dužinom**.*

## 1.1 Temeljne operacije ravnalom i šestarom

Svaka konstrukcija ravnalom i šestarom počiva na temeljnim operacijama i moguća je samo njihovom uporabom. Temeljnim operacijama ravnalom i šestarom smatramo:

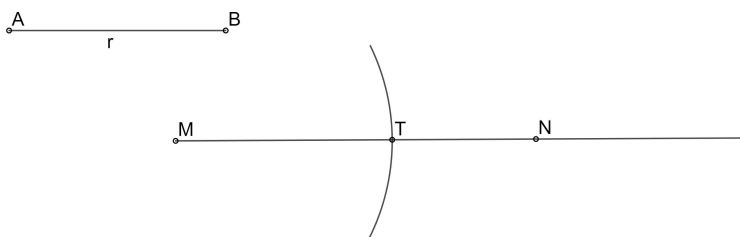
1. konstrukciju pravca kroz dvije dane točke,
2. konstrukciju sjecišta dvaju neparalelnih pravaca,
3. konstrukciju kružnice poznatog središta koja prolazi zadanom točkom,
4. konstrukciju sjecišta dane kružnice (zadane središtem i jednom točkom) i pravca (zadanog dvijema točkama),
5. konstrukciju sjecišta dviju kružnica (zadanih središtem i po jednom svojom točkom).

Ovako opisane konstrukcije točaka srž su rješavanja konstruktivnih problema. Svaki složeniji konstruktivni zadatak rješavat će se uporabom temeljnih konstrukcija.

**Definicija 1.1.1.** *Svaki slijed od konačno mnogo izvedenih osnovnih operacija zvat ćemo konstrukcijom pomoću ravnala i šestara, odnosno euklidskom konstrukcijom.*

## 1.2 Temeljne konstrukcije ravnalom i šestarom

1. PRIJENOS DUŽINE Zadana je dužina  $\overline{AB}$  i polupravac  $MN$ . Potrebno je dužinu  $\overline{AB}$  prenijeti na polupravac  $MN$ .



Slika 1.1: Prijenos dužine



OPIS KONSTRUKCIJE:

Konstruiramo kružnicu sa središtem u točki  $M$  polumjera  $r = |AB|$ . Ta kružnica polupravac  $MN$  siječe u točki  $T$ . Dužina  $\overline{MT}$  je jednaka dužini  $\overline{AB}$ .

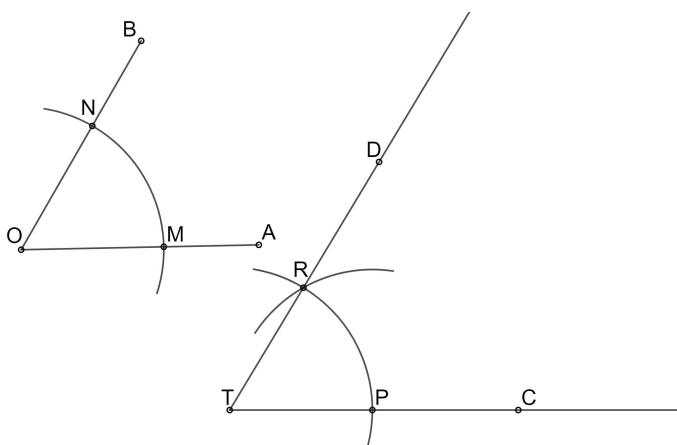
2. PRIJENOS KUTA

Zadan je kut  $\angle AOB$  i polupravac  $TC$ . Potrebno je konstruirati kut  $\angle CTD$  takav da je njegova mjera jednaka mjeri zadanog kuta.

OPIS KONSTRUKCIJE:

Oko točke  $O$  konstruiramo kružni luk proizvoljnog polumjera te ponovimo isto oko točke  $T$ . Kružni luk oko točke  $O$  siječe krakove kuta  $\angle AOB$  u točkama  $M$  i  $N$ , a kružni luk oko točke  $T$  siječe polupravac  $TC$  u točki  $P$ . Sada oko točke  $P$  konstruiramo kružni luk polumjera  $r = |MN|$ . Ti kružni lukovi sijeku se u točki  $R$ .

Luk  $\widehat{MN}$  jednak je luku  $\widehat{PR}$  pa je i  $\angle AOB = \angle MON = \angle PTR = \angle CTD$ .



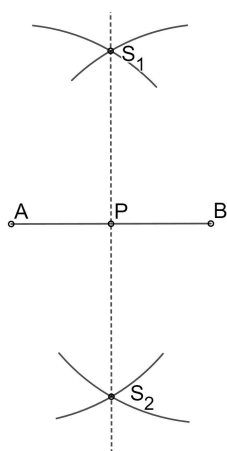
Slika 1.2: Prijenos kuta

3. SIMETRALA DUŽINE I POLOVIŠTE DUŽINE

Zadana je dužina  $\overline{AB}$  svojim krajevima  $A$  i  $B$ . Potrebno je konstruirati simetralu dane dužine i njezino polovište  $P$ .

OPIS KONSTRUKCIJE:

Oko točke  $A$  konstruiramo kružnicu polumjera  $r = |AB|$  te oko točke  $B$  konstruiramo kružnicu polumjera  $r = |AB|$ . U presjeku tih dviju kružnica nalaze se dvije točke  $S_1$  i  $S_2$ . Konstruiramo li pravac kroz  $S_1$  i  $S_2$  dobili smo simetralu dužine  $\overline{AB}$ . Točka koja se dobije presjekom dužine  $\overline{AB}$  i njezine simetrale je traženo polovište  $P$ .



Slika 1.3: Simetrala dužine i polovište dužine

#### 4. OKOMICA IZ DANE TOČKE NA DANI PRAVAC

Zadan je pravac  $p$  i točka  $T$ . Potrebno je konstruirati pravac  $n$  okomit na pravac  $p$ , a koji prolazi točkom  $T$ .

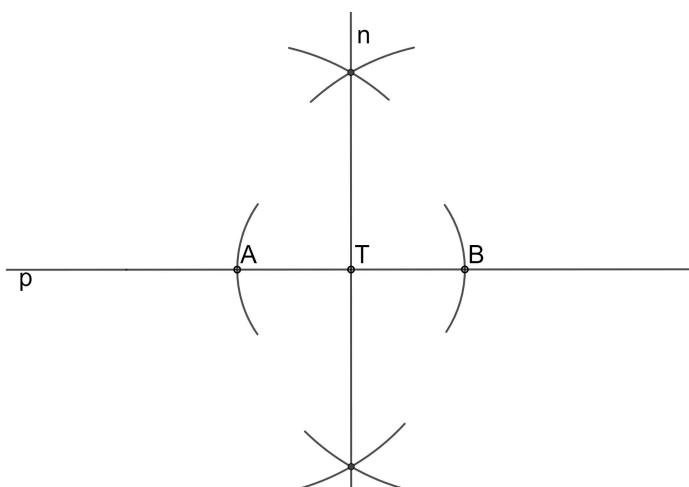
Razlikujemo dva slučaja:

- a) Točka  $T$  je na pravcu  $p$ .
- b) Točka  $T$  nije na pravcu  $p$ .

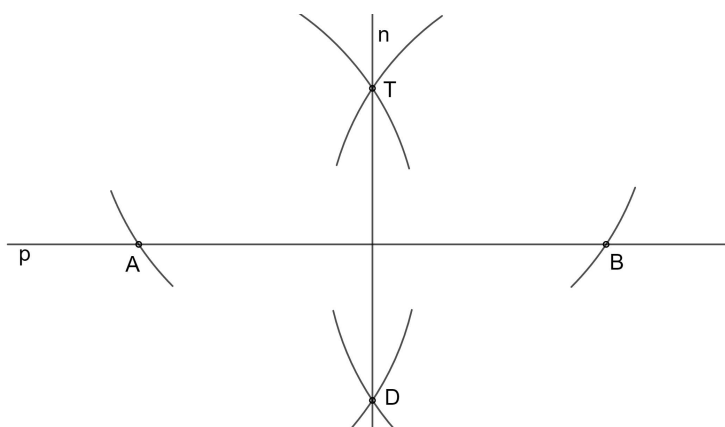
OPIS KONSTRUKCIJE:

- a) Konstruiramo kružni luk sa središtem u točki  $T$  proizvoljnog polumjera. Taj kružni luk siječe pravac  $p$  u točkama  $A$  i  $B$ . Tada je točka  $T$  polovište dužine  $\overline{AB}$ . Sada traženu okomicu dobivamo konstrukcijom simetrale dužine opisanom u točki 1 i ta okomica prolazi točkom  $T$ .
- b) Konstruiramo kružni luk sa središtem u točki  $T$  dovoljno velikog radijusa tako da ta kružnica siječe pravac  $p$ . Dakle, ta kružnica siječe pravac  $p$  u točkama  $A$  i  $B$ . Sada traženu okomicu dobivamo konstrukcijom simetrale dužine  $\overline{AB}$  opisanom u točki 1 i ta okomica prolazi točkom  $T$  jer je točka  $T$  jednako udaljena od točaka  $A$  i  $B$ .

NAPOMENA: Ovaj postupak ne uči se u školi, nego se okomice dobivaju korištenjem dva trokuta.



Slika 1.4: Okomica iz dane točke na dani pravac kada je ta točka dio danog pravca



Slika 1.5: Okomica iz dane točke na dani pravac kada ta točka nije dio danog pravca

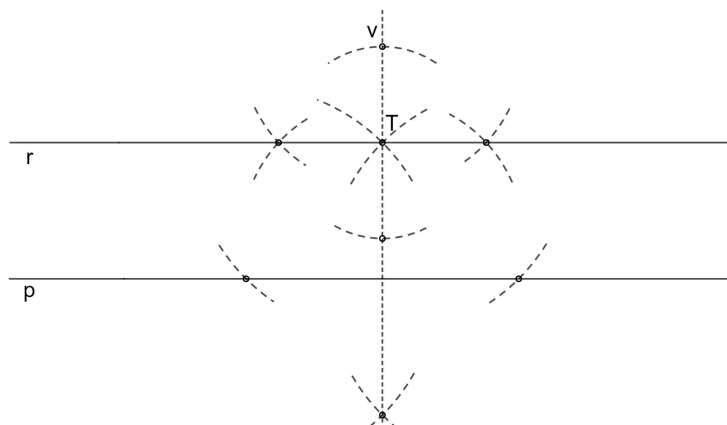
### 5. PRAVAC KROZ DANU TOČKU PARALELAN S DANIM PRAVCEM

Zadan je pravac  $p$  i točka  $T$  koja ne pripada pravcu  $p$ . Potrebno je konstruirati pravac  $r$  koji prolazi točkom  $T$  i paralelan je zadanom pravcu.

#### OPIS KONSTRUKCIJE:

*Konstrukciju možemo provesti na više načina, a ovdje ćemo pokazati jedan od njih.* Konstruirajmo pravac  $v$  koji prolazi točkom  $T$  i okomit je na zadani pravac  $p$ . Sada konstruiramo pravac okomit na pravac  $v$  koji prolazi točkom  $T$ . Dobili smo traženi

pravac  $r$ .



Slika 1.6: Pravac kroz danu točku paralelan s danim pravcem

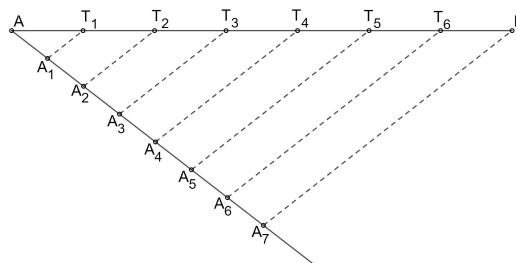
NAPOMENA: Ovaj postupak ne uči se u školi, nego se paralele povlače korištenjem dva trokuta.

6. DIJELJENJE DUŽINE NA JEDNAKE DIJELOVE I U DANOM OMJERU  
Zadana je dužina  $\overline{AB}$ . Potrebno ju je podijeliti:

- a) na jednake dijelove
- b) u danom omjeru.

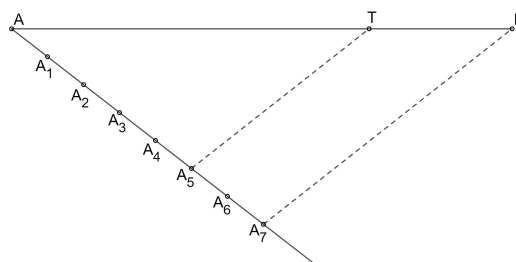
OPIS KONSTRUKCIJE:

- a) Iz točke  $A$  povučemo bilo koji polupravac koji nema drugih zajedničkih točaka s  $\overline{AB}$ . (Isto smo mogli napraviti i iz točke  $B$ ). Sada šestarom na polupravac nanesemo istu dužinu, krenuvši iz točke  $A$ , onoliko puta na koliko dijelova želimo podijeliti dužinu. Na taj način dobijemo točke  $A_1, A_2, A_3, \dots, A_n$ , gdje je  $n$  broj željenih dužina, takve da je  $|AA_1| = |A_1A_2| = |A_2A_3| = \dots = |A_{n-1}A_n|$ . Spojimo  $A_n$  sa  $B$ , a zatim kroz točke  $A_1, A_2, A_3, \dots, A_{n-1}$  napravimo paralele s  $\overline{A_nB}$  (opisano u prethodnoj točki). Presjekom paralela i  $\overline{AB}$  dobivamo točke  $T_1, T_2, T_3, \dots, T_{n-1}$  i one dužinu dijele na  $n$  jednakih dijelova.
- b)  $\overline{AB}$  podijelit ćemo u omjeru  $m : n$  tako da ju na gore opisan način podijelimo na  $m + n$  dijelova i tako dobijemo točke  $A_1, A_2, A_3, \dots, A_{m-1}, A_m, A_{m+1}, A_{m+2}, \dots$



Slika 1.7: Dijeljenje dužine na sedam jednakih dijelova

,  $A_{m+n-1}$ ,  $A_{m+n}$ . Kroz točku  $A_m$  povučemo paralelu sa  $A_{m+n}B$  te ona  $\overline{AB}$  siječe u točki  $T$  takvoj da je  $|AT| : |TB| = m : n$ .



Slika 1.8: Dijeljenje dužine u omjeru 5:2

## 7. SIMETRALA KUTA

Zadan je kut  $\angle ATB$ . Potrebno je konstruirati njegovu simetralu.

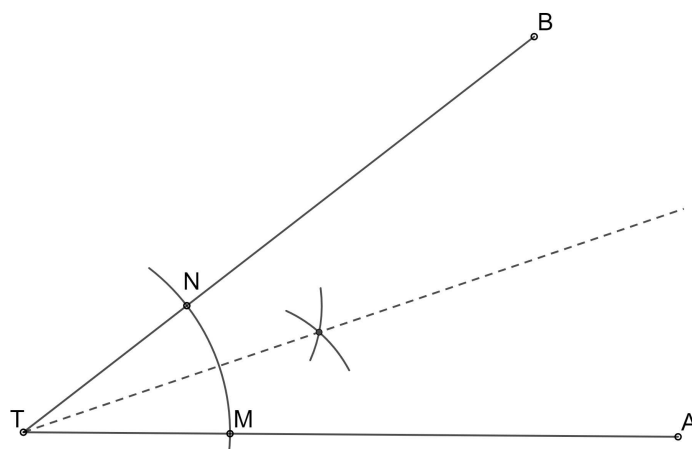
### OPIS KONSTRUKCIJE:

Šestarom konstruiramo kružni luk proizvoljnog polumjera s centrom u točki  $T$ . Taj kružni luk siječe krakove kuta u točkama  $M$  i  $N$ . Simetralu kuta  $\angle ATB$  dobit ćemo konstruiramo li simetralu  $\overline{MN}$  (opisano u 1. točki).

NAPOMENA: Dovoljno je konstruirati točku unutar kuta  $\angle ATB$  jer simetrala prolazi točkom  $T$ .

## 8. KRUŽNI LUK IZ ČIJIH SE TOČAKA VIDI NEKA DUŽINA POD DANIM KUTOM

Zadana je dužina  $\overline{AB}$  i kut  $\angle XOY$ . Potrebno je konstruirati kružni luk iz čijih se

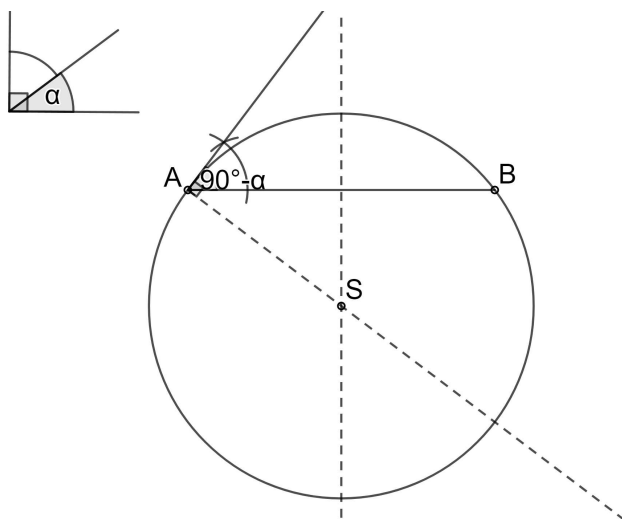


Slika 1.9: Simetrala kuta

točkaka vidi dužina  $\overline{AB}$  pod kutom  $\angle XOY$ .

**OPIS KONSTRUKCIJE:**

Po teoremu o obodnom i središnjem kutu zaključujemo da se središte traženog kružnog luka mora nalaziti na simetrali tetive  $\overline{AB}$ .



Slika 1.10: Kružni luk iz čijih se točkaka vidi neka dužina pod danim kutom

Dakle, konstruiramo simetralu dužine  $\overline{AB}$ . Prenesemo kut  $\angle XOY$  u položaj tako da mu jedan krak bude na dužini  $\overline{AB}$ , a vrh u jednoj od točaka  $A$  i  $B$ . Konstruiramo okomicu u vrhu kuta na njegov drugi krak. Ta okomica i simetrala tetive  $\overline{AB}$  sijeku se u središtu traženog kružnog luka.

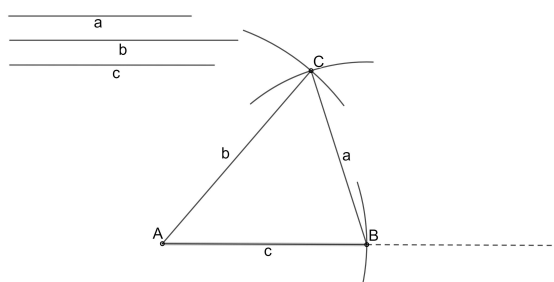
## 9. ELEMENTARNE KONSTRUKCIJE TROKUTA

- *SSS*

Zadane su dužine duljina  $a$ ,  $b$  i  $c$  tako da vrijedi:  $a + b > c$ ,  $a + c > b$  i  $b + c > a$ . Potrebno je konstruirati trokut  $ABC$  sa stranicama duljina  $a$ ,  $b$  i  $c$ .

OPIS KONSTRUKCIJE:

Neka je  $|AB| = c$ ,  $|AC| = b$  i  $|BC| = a$ . Fiksirajmo u ravnini bilo koju točku, nazovimo je  $A$ . Sada kroz točku  $A$  povučemo bilo koji polupravac te konstruiramo kružnicu sa središtem u točki  $A$  polumjera  $c$ . Ta kružnica siječe polupravac u točki  $B$ . Sada oko točke  $A$  opišemo kružnicu polumjera  $b$  te oko točke  $B$  opišemo kružnicu polumjera  $a$ . Jedno od sjecišta tih dviju kružnica je točka  $C$ . Dobili smo traženi trokut  $ABC$ .



Slika 1.11: *SSS* konstrukcija trokuta

- *SKS*

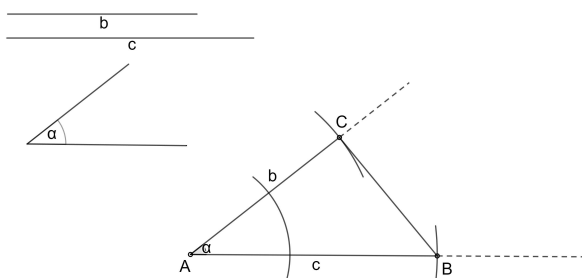
Zadane su dvije dužine duljina  $b$  i  $c$  i jedan kut  $\angle BAC$ . Potrebno je konstruirati trokut kojem su zadane dužine stranice, a dani kut je između njih.

OPIS KONSTRUKCIJE:

Bez smanjenja općenitosti, neka su zadane stranice  $\overline{AB}$  i  $\overline{AC}$  duljina  $|AB| = c$  i  $|AC| = b$  te kut  $\angle BAC = \alpha$ .

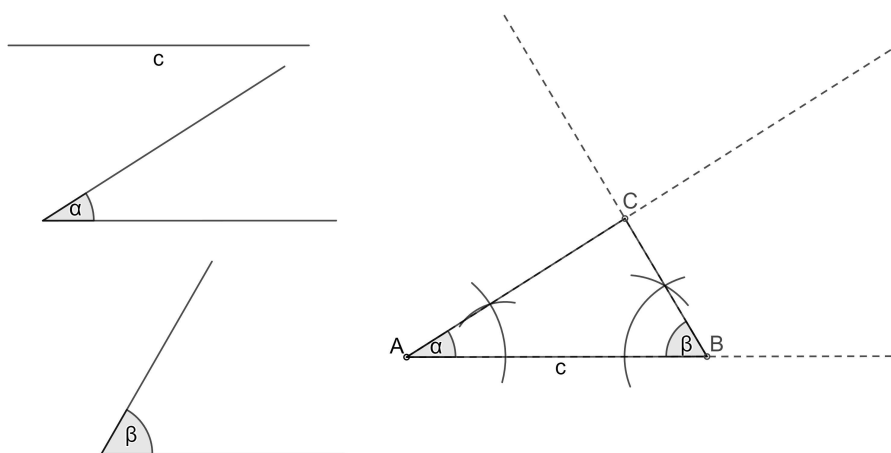
Fiksirajmo u ravnini bilo koju točku  $A$ , kroz nju povučemo bilo koji polupravac te konstruiramo kružnicu sa središtem u točki  $A$  polumjera  $c$ . Ta kružnica siječe

polupravac u točki  $B$ . Zadani kut  $\angle BAC$  prenesemo u položaj  $\angle BAX$ . Oko točke  $A$  konstruiramo kružnicu polumjera  $b$ . Ta kružnica siječe polupravac  $AX$  i točki  $C$ . Dobili smo trokut  $ABC$ .



Slika 1.12: *SKS* konstrukcija trokuta

- *KSK*  
 Zadana je dužina duljine  $c$  i dva kuta  $\angle BAC$  i  $\angle ABC$ . Potrebno je konstruirati trokut kojemu je zadana dužina stranica, a zadani kutovi su uz tu stranicu.



Slika 1.13: *KSK* konstrukcija trokuta

OPIS KONSTRUKCIJE:

Bez smanjenja općenitosti, neka je zadana stranica  $\overline{AB}$  duljine  $|AB| = c$  te kutovi  $\angle BAC = \alpha$  i  $\angle ABC = \beta$ .



Fiksirajmo u ravnini bilo koju točku  $A$ , kroz nju povučemo bilo koji polupravac te konstruiramo kružnicu sa središtem u točki  $A$  polumjera  $c$ . Ta kružnica siječe polupravac u točki  $B$ . Zadani kut  $\angle BAC$  prenesemo u položaj  $\angle BAX$ , a zadani kut  $\angle ABC$  prenesemo u položaj  $\angle ABY$ . Polupravci  $AX$  i  $BY$  sijeku se u točki  $C$ . Dobili smo trokut  $ABC$ .

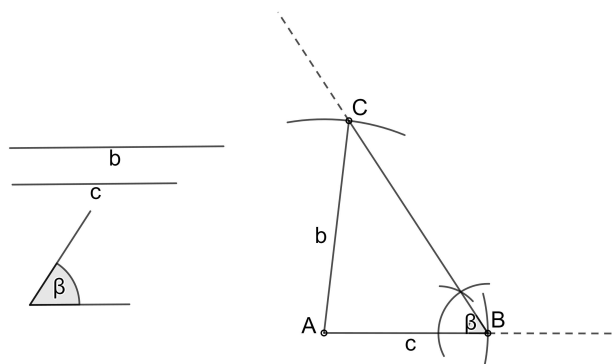
•  $SSK^>$

Zadane su dvije dužine duljina  $b$  i  $c$  i jedan kut  $\angle BAC$ . Potrebno je konstruirati trokut kojem su zadane dužine stranice, a dani kut je nasuprot dulje od njih.

OPIS KONSTRUKCIJE:

Bez smanjenja općenitosti, neka su zadane stranice  $\overline{AB}$  i  $\overline{AC}$  duljina  $|AB| = c$  i  $|AC| = b$  takve da je  $b < c$  te kut  $\angle ABC = \beta$ .

Fiksirajmo u ravnini bilo koju točku  $A$ , kroz nju povučemo bilo koji polupravac te konstruiramo kružnicu sa središtem u točki  $A$  polumjera  $c$ . Ta kružnica siječe polupravac u točki  $B$ . Zadani kut  $\angle ABC$  prenesemo u položaj  $\angle ABX$ . Oko točke  $A$  konstruiramo kružnicu polumjera  $b$ . Ta kružnica siječe polupravac  $BX$  u točki  $C$ . Dobili smo trokut  $ABC$ .



Slika 1.14:  $SSK^>$  konstrukcija trokuta

## Poglavlje 2

# Izvodljivost konstrukcija ravnalom i šestarom

### 2.1 Algebarska metoda konstrukcije

U ovom odlomku bavit ćemo se algebarskom metodom konstrukcije kao što je dano u [5] i [6] jer parametri kojima su opisane geometrijske situacije u planimetriji, često zadovoljavaju neke polinomijalne uvjete. Zato se egzistencija konstrukcije ravnalom i šestarom može povezati s tipom proširenja polja racionalnih brojeva, koje sadrži korijene odgovarajućih polinoma. Konkretnije, pokazat ćemo kako konstruirati duljine dužina:

1.  $x = a + b$ ,  $x = a - b$ ,  $a > b$ ,
2.  $x = n \cdot a$ ,  $x = \frac{a}{n}$ ,
3.  $x = \frac{a \cdot b}{c}$ ,  $x = \frac{a}{c}$ ,  $x = a \cdot b$ ,
4.  $x = \sqrt{a \cdot b}$ ,  $x = \sqrt{a}$ ,
5.  $x = \sqrt{a^2 + b^2}$ ,  $x = \sqrt{a^2 - b^2}$ ,  $a > b$ ,

gdje su  $1$ ,  $a$ ,  $b$  i  $c$  duljine zadanih dužina i  $n$  prirodan broj  $> 1$ .

Kažemo još da smo konstruirali navedene izraze.

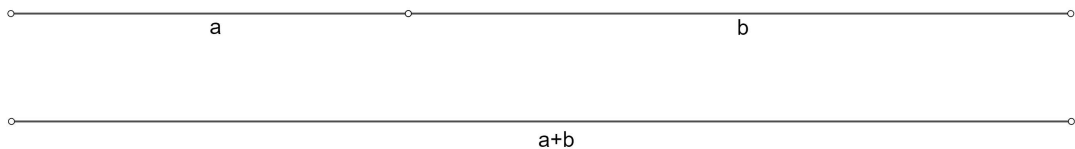
Pokažimo sada konstrukcije izraza 1. – 5.:

1. zbrajanje i oduzimanje dužina

a)  $x = a + b$

Dvije dužine kojima su duljine  $a$  i  $b$  zbrajamo tako da na istom pravcu nanese prvo dužinu duljine  $a$ , a zatim odmah do nje dužinu duljine  $b$  tako da

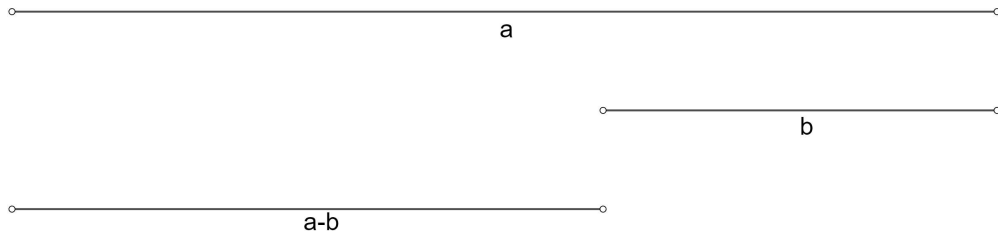
imaju zajedničku krajnju točku. Njihov zbroj je dužina kojoj je jedna krajnja točka krajnja točka dužine duljine  $a$ , a druga krajnja točka joj je krajnja točka dužine duljine  $b$ .



Slika 2.1: Zbroj dužina

**b)  $x = a - b$**

Dvije dužine kojima su duljine  $a$  i  $b$ , gdje je  $a > b$ , oduzimamo tako da na istom pravcu naneseemo prvo dužinu duljine  $a$ , a zatim unutar te dužine naneseemo dužinu duljine  $b$  tako da imaju zajedničku krajnju točku. Njihova razlika je dužina koja preostane od dužine duljine  $a$ .



Slika 2.2: Razlika dužina

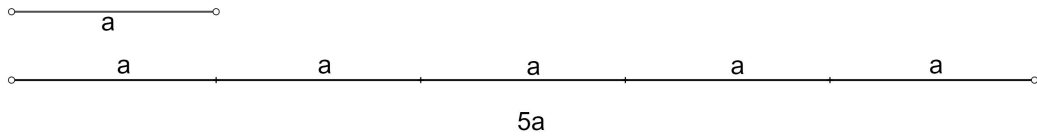
2. množenje i dijeljenje prirodnim brojem

**a)  $x = n \cdot a$**

Kako je množenje uzastopno zbrajanje istog broja  $n$  puta, tako dužinu  $x$  dobijemo ako  $n$  puta pribrojimo dužinu duljine  $a$  kako je opisano u 1. a).

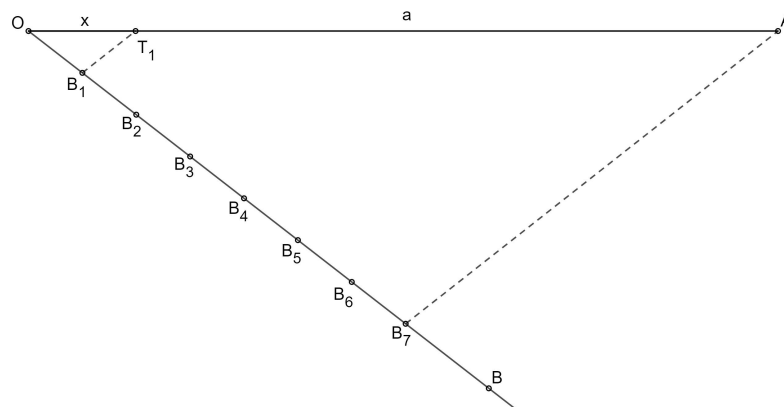
**b)  $x = \frac{a}{n}$**

Neka je dužina  $\overline{OA}$  takva da je njezina duljina jednaka  $|OA| = a$ . Povučemo polupravac  $OB$  iz točke  $O$  različit od  $OA$  i na njega uzastopno naneseemo  $n$  jediničnih dužina počevši od točke  $O$ . Tako dobijemo točke  $B_1, B_2, \dots, B_n$ . Kroz



Slika 2.3: Množenje dužine prirodnim brojem

točku  $B_1$  povučemo paralelu sa dužinom  $\overline{AB_n}$ . Ta paralela siječe dužinu  $\overline{OA}$  u točki  $A_1$ . Dužina  $\overline{OA_1}$  je tražena dužina duljine  $x$ .



Slika 2.4: Dijeljenje dužine prirodnim brojem

### 3. konstrukcija četvrte proporcionalne

**a)**  $x = \frac{a \cdot b}{c}$

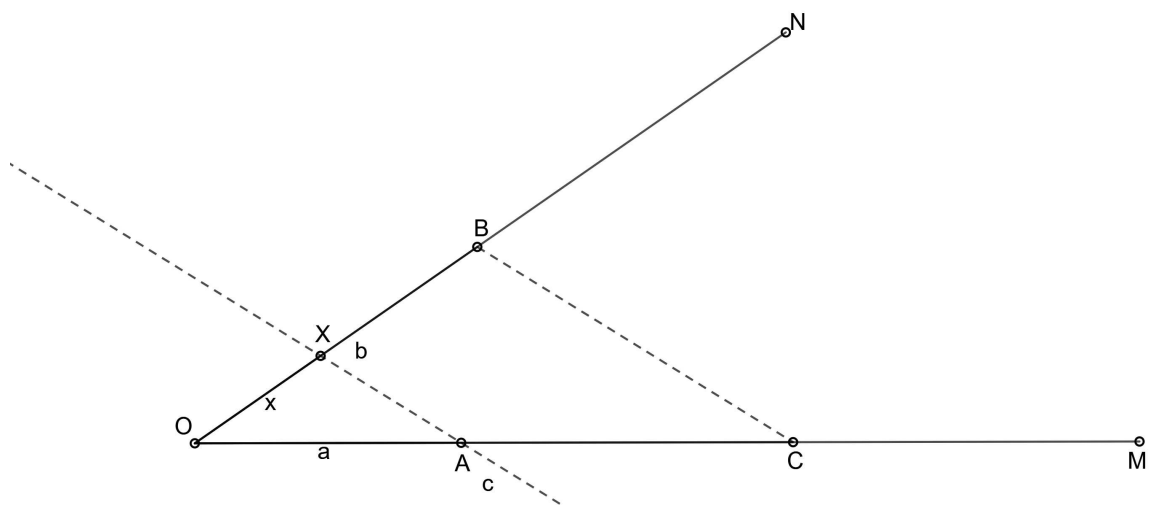
Ovu konstrukciju provest ćemo pomoću Talesovog teorema o proporcionalnosti. Kako je zadano  $x = \frac{a \cdot b}{c}$ , slijedi da je  $x : b = a : c$ .

Na krak  $OM$  kuta  $\angle MON$  nanesimo dužine  $\overline{OA}$  i  $\overline{OC}$  duljina  $|OA| = a$  i  $|OC| = c$ . Na krak  $ON$  nanesimo dužinu  $\overline{OB}$  duljine  $|OB| = b$ . Tada točkom  $A$  povučemo paralelu s dužinom  $\overline{BC}$ . Ta paralela siječe krak  $OB$  u točki  $X$ , tj.  $x = |OX|$ . Time smo konstruirali mjerni broj  $x = \frac{a \cdot b}{c}$ .

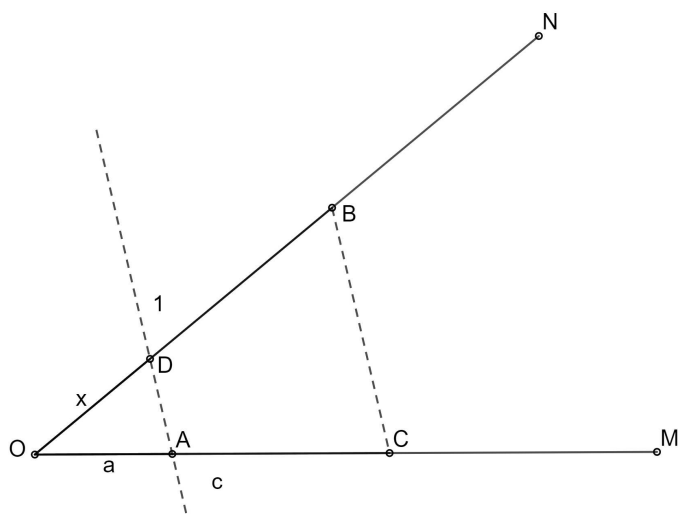
**b)**  $x = \frac{a}{c}$

Specijalni slučaj primjera  $x = \frac{a \cdot b}{c}$  gdje je  $b = 1$ .

Konstrukcija se provodi analogno.



Slika 2.5: Konstrukcija četvrte proporcionalne

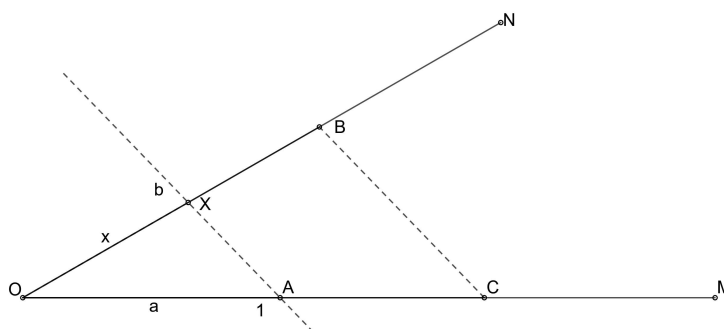


Slika 2.6: Konstrukcija četvrte proporcionalne kada je jedna od zadanih dužina jedinična

c)  $x = a \cdot b$

Specijalni slučaj primjera  $x = \frac{a \cdot b}{c}$  gdje je  $c = 1$ .

Konstrukcija se provodi analogno.

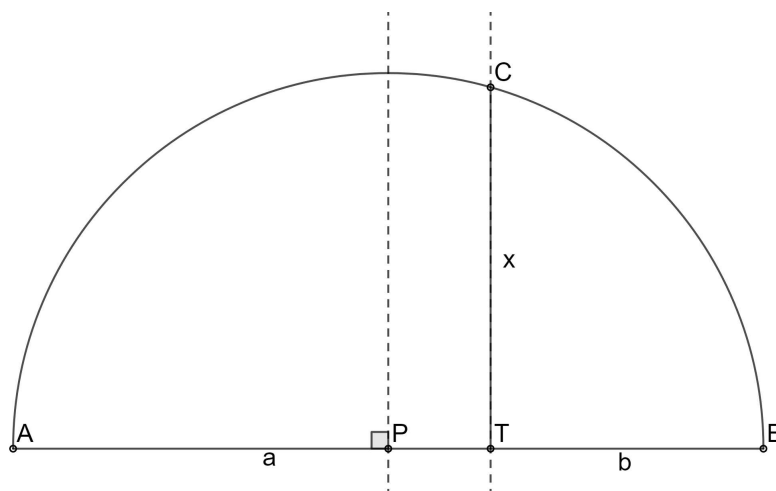


Slika 2.7: Konstrukcija četvrte proporcionalne kada je jedna od zadanih dužina jedinična

4. geometrijska sredina

a)  $x = \sqrt{a \cdot b}$

Ovu konstrukciju provest ćemo pomoću Euklidovog poučka i Talesovog te-



Slika 2.8: Konstrukcija geometrijske sredine

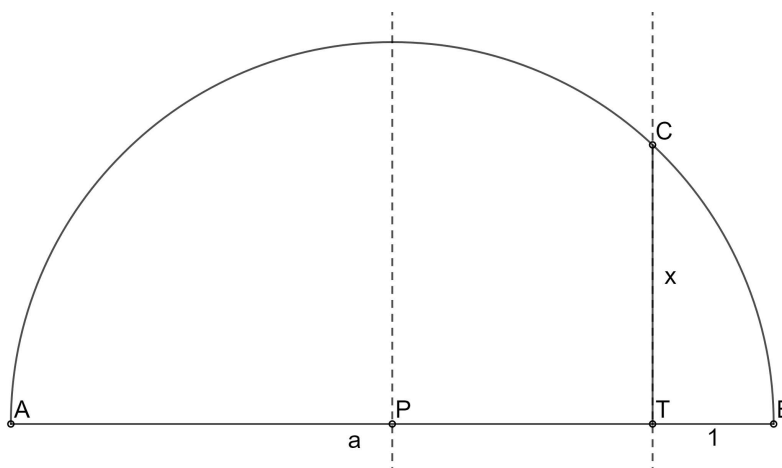
orema o obodnom kutu nad promjerom kružnice.

Konstruiramo dužinu  $\overline{AB}$  duljine  $|AB| = |AT| + |TB| = a + b$ . Sada konstruiramo polovište  $P$  dužine  $\overline{AB}$  i kružnicu oko točke  $P$  polumjera  $r = |AP|$ . Dakle, dužina  $\overline{AB}$  promjer je te kružnice. Odabirom bilo koje točke  $C$  na kružnici obodni kut nad promjerom  $\overline{AB}$  u točki  $C$  bit će pravi, a samim time i trokut  $ABC$  bit će pravokutan.

Povucimo okomicu iz točke  $T$  na dužinu  $\overline{AB}$ . Presjek okomice i kružnice označimo točkom  $C$ . Sada iz Euklidovog poučka slijedi da je  $|CT| = \sqrt{a \cdot b} = x$ .

b)  $x = \sqrt{a}$

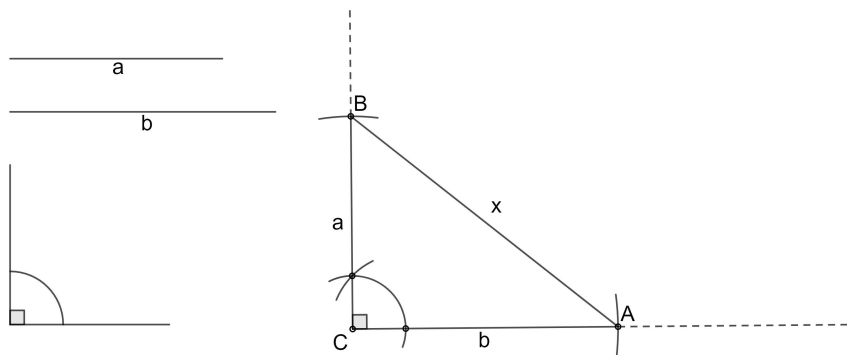
Specijalni slučaj primjera  $x = \sqrt{a \cdot b}$  gdje je  $b = 1$ .



Slika 2.9: Konstrukcija geometrijske sredine kada je jedna od zadanih dužina jedinična

5. a)  $x = \sqrt{a^2 + b^2}$

Prema Pitagorinom poučku slijedi da je dužina duljine  $x$  hipotenuza pravokut-



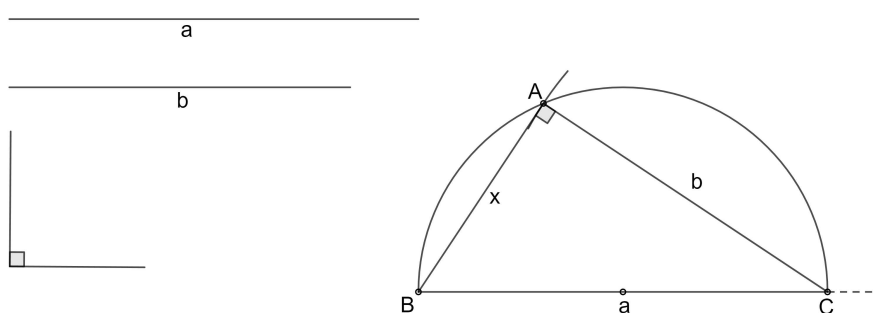
Slika 2.10: Konstrukcija korijena zbroja kvadrata

nog trokuta kojemu su katete duljina  $a$  i  $b$ . Dakle, potrebno je konstruirati trokut

kojem su poznate stranice duljina  $a$  i  $b$  te kut među njima ( $SKS$  konstrukcija trokuta).

b)  $x = \sqrt{a^2 - b^2}$

Prema Pitagorinom poučku slijedi da je dužina duljine  $x$  jedna od kateta pravokutnog trokuta kojem je druga kateta duljine  $b$ , a hipotenuza duljine  $a$ . Dakle, potrebno je konstruirati trokut kojem su zadane duljine dviju stranica  $a$  i  $b$  te mjera kuta nasuprot dulje od njih ( $SSK^>$  konstrukcija trokuta).



Slika 2.11: Konstrukcija korijena razlike kvadrata

Nakon što smo pokazali kako konstruirati izraze 1. – 5. možemo konstruirati bilo koji izraz koji se može dobiti iz zadanih dužina kombinacijom racionalnih operacija i vađenjem kvadratnih korijena.

## 2.2 Proširenje polja racionalnih brojeva

U prethodnom odlomku pokazali smo kako od zadanih dužina konstruirati dužine kojima je duljina jednaka zbroju, razlici, umnošku ili kvocijentu zadanih dužina, kako im izvaditi kvadratni korijen te još nekoliko kombinacija ovih računskih operacija.

Zaključujemo da je moguće konstruirati dužine čije su duljine jednake korijenima zadane kvadratne jednadžbe. Drugim riječima, zadanim dužinama izvodimo racionalne operacije, ali i proširujemo polje racionalnih brojeva, koje sadrži korijene odgovarajućih polinoma. U ovom poglavlju osim o proširenju polja racionalnih brojeva, govorit ćemo i o konstruktibilnosti realnog broja, pri čemu pratimo [6], a kako bismo to ostvarili moramo uvesti pojmove algebarskog i transcendentalnog broja.



**Definicija 2.2.1.** Neka je  $P$  potpolje od  $\mathbb{C}$ . Neka je  $\alpha \in \mathbb{C}$ . Ako je  $\alpha$  korijen neke algebarske jednadžbe s koeficijentima iz  $P$ , onda kažemo da je  $\alpha$  **algebarski broj** nad poljem  $P$ . Ako takva algebarska jednadžba ne postoji, onda kažemo da je  $\alpha$  **transcendentan broj** nad poljem  $P$ .

Primjetimo da je svaki  $a \in P$  algebarski nad poljem  $P$  jer je  $a$  rješenje jednadžbe  $x - a = 0$ .

**Propozicija 2.2.2.** Ako je  $\alpha$  algebarski broj nad poljem  $P$ , onda je  $P[\alpha]$  polje i vrijedi  $P[\alpha] = P(\alpha)$ .

*Dokaz.* Kako je  $\alpha$  algebarski, slijedi da postoji polinom  $p(x) \in P[x]$ ,  $p(x) = p_0 + p_1x + p_2x^2 + \dots + p_nx^n$ ,  $p_n \neq 0$ , tako da je  $p(\alpha) = 0$ . Bez smanjenja općenitosti možemo pretpostaviti da je  $p$  ireducibilan nad  $P$ . Očito uvijek vrijedi  $P[\alpha] \subseteq P(\alpha)$ .

Dokažimo obrnutu inkluziju. Neka je  $\beta \in P[\alpha]$ . Tada postoji polinom  $f(x) \in P[x]$ ,  $f(x) = c_0 + c_1x + c_2x^2 + \dots + c_kx^k$ ,  $k \in \mathbb{N}$ ,  $c_i \in P$ , takav da je  $\beta = f(\alpha)$ . Tvrdimo da se  $\beta$  može napisati u obliku  $\beta = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1}$ , gdje je  $n$  stupanj polinoma  $p$ .

Zaista, podijelimo li  $f(x)$  sa  $p(x)$ , neka je  $r(x)$  ostatak pri tom dijeljenju, tj.  $f(x) = p(x)q(x) + r(x)$ , gdje je  $r(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$ . Za  $x = \alpha$  slijedi  $f(\alpha) = r(\alpha)$ , tj.

$$\beta = f(\alpha) = r(\alpha) = a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1},$$

čime je tvrdnja dokazana.

Neka je sada  $\frac{f(\alpha)}{g(\alpha)} \in P(\alpha)$ . Prema upravo dokazanoj tvrdnji vrijedi

$$\frac{f(\alpha)}{g(\alpha)} = \frac{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}}{b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1}}, \quad g(\alpha) \neq 0.$$

Pokažimo da je  $\frac{f(\alpha)}{g(\alpha)} \in P[\alpha]$ . U tu svrhu promotrimo polinom  $g(x) = b_0 + b_1x + \dots + b_{n-1}x^{n-1}$ .  $g$  nije nul-polinom jer je  $g(\alpha) \neq 0$ . Polinom  $g$  nije djeljiv s  $p$  jer je  $\text{st } g < \text{st } p$ . No  $p$  je po pretpostavci ireducibilan pa su stoga  $g$  i  $p$  relativno prosti polinomi. Stoga prema teoremu o najvećoj zajedničkoj mjeri postoje polinomi  $\varphi(x), \psi(x) \in P[x]$ , takvi da je  $g(x)\varphi(x) + p(x)\psi(x) = 1$ . Stavimo li ovdje  $x = \alpha$  onda zbog  $p(\alpha) = 0$  slijedi  $g(\alpha) \cdot \varphi(\alpha) = 1$ . Dakle, postoji polinom  $\varphi(x) \in P[x]$ , takav da je

$$\varphi(\alpha) = \frac{1}{g(\alpha)}.$$

Stoga je  $\frac{f(\alpha)}{g(\alpha)} = f(\alpha) \cdot \varphi(\alpha)$ , pa je  $\frac{f(\alpha)}{g(\alpha)} \in P[\alpha]$  čime je propozicija dokazana.  $\square$

**Korolar 2.2.3.** Dimenzija od  $P[\alpha]$  kao vektorskog prostora nad  $P$  jednaka je stupnju ireducibilnog polinoma iz  $P[x]$  koji poništava  $\alpha$ .

Posljedica konstrukcija iz podpoglavlja 2.1 je sljedeći teorem:

**Teorem 2.2.4.** *Ako je  $x$  neki nenegativni realni broj koji možemo dobiti pomoću konačno mnogo racionalnih operacija i konačno mnogo vađenja kvadratnih korijena, iz mjernih brojeva konačno mnogo danih dužina, tada možemo iz danih dužina pomoću ravnala i šestara konstruirati dužinu čiji mjerni broj je jednak  $x$ .*

Ovaj teorem nam govori da je prikaz broja  $x$  pomoću konačno mnogo racionalnih operacija i konačno mnogo vađenja kvadratnog korijena iz mjernih brojeva konačno mnogo danih dužina dovoljan uvjet za mogućnost konstruiranja dužine sa mjernim brojem  $x$  iz konačno mnogo danih dužina pomoću ravnala i šestara.

Obratom teorema 2.2.4 dokazat ćemo nužan uvjet za mogućnost konstruiranja dužine sa mjernim brojem  $x$  iz konačno mnogo danih dužina pomoću ravnala i šestara.

**Teorem 2.2.5.** *Ako se iz danih dužina s mjernim brojevima  $m_1, m_2, \dots, m_n$  može pomoću ravnala i šestara konstruirati dužina mjernog broja  $x$ , tada se ta dužina  $x$  može izračunati iz mjernih brojeva  $m_1, m_2, \dots, m_n$  pomoću konačno mnogo racionalnih operacija i konačno mnogo vađenja kvadratnih korijena.*

*Dokaz.* Svaku konstrukciju možemo provesti u konačno mnogo koraka nizom temeljnih operacija. Pokažimo da je moguće temeljne operacije provesti analitičkom metodom:

1. Pravac kroz dvije dane točke  $T_1(a_1, b_1), T_2(a_2, b_2)$ .

Jednadžba pravca koji prolazi kroz dvije točke glasi:

$$y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)$$

Uvrštavanjem točaka  $T_1$  i  $T_2$  te sređivanjem izraza dobivamo:

$$(b_1 - b_2)x + (a_2 - a_1)y + a_1b_2 - a_2b_1 = 0.$$

Odnosno:

$$ax + by + c = 0,$$

gdje je:

$$a = b_1 - b_2,$$

$$b = a_2 - a_1,$$

$$c = a_1b_2 - a_2b_1.$$

2. Sjecište  $S(x_s, y_s)$  dvaju neparalelnih pravaca  $a_1x + b_1y + c_1 = 0$  i  $a_2x + b_2y + c_2 = 0$  Rješavanjem sustava jednađžbi dobijemo koordinate sjecišta:

$$x_s = \frac{b_2c_1 - b_1c_2}{a_2b_1 - a_1b_2} \quad y_s = \frac{a_1c_2 - a_2c_1}{a_2b_1 - a_1b_2}$$

Uz uvjet da pravci nisu paralelni:  $a_2b_1 - a_1b_2 \neq 0$

3. Kružnica poznatog središta  $S(p, q)$  koja prolazi točkom  $T(x_1, y_1)$ . Kružnica je skup točaka  $(x, y)$  jednako udaljenih od jedne čvrste točke  $(p, q)$  koju nazivamo središtem. Dakle, jednađžba kružnice glasi:

$$(x - p)^2 + (y - q)^2 = r^2,$$

gdje je  $r$  udaljenost tih točaka od čvrste točke. Tj.

$$r = \sqrt{(x_1 - p)^2 + (y_1 - q)^2}.$$

Dakle, uvrštavanjem i sređivanjem izraza dobivamo:

$$x^2 + y^2 + ax + by + c = 0,$$

gdje je

$$a = -2p,$$

$$b = -2q,$$

$$c = p^2 + q^2 - (x_1 - p)^2 - (y_1 - q)^2.$$

4. Sjecišta dane kružnice  $x^2 + y^2 + a_1x + b_1y + c_1 = 0$  i pravca  $a_2x + b_2y + c_2 = 0$ . Rješavanjem sustava jednađžbi dobijemo

$$x_s = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}, \quad y_s = -\frac{a_1}{b_1}x_s - \frac{c_1}{b_1},$$

gdje je

$$A = a_1^2 + b_1^2,$$

$$B = b_1^2a_2 + 2a_1c_1 - a_1b_1b_2,$$

$$C = c_1^2 - b_1c_1b_2 + b_1^2c_2,$$

uz uvjet da je  $b_1 \neq 0$ .

Za  $b_1 = 0$  i  $a_1 \neq 0$  rješenje sustava je:

$$x_s = -\frac{c_1}{a_1}, \quad y_s = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A},$$

gdje je

$$\begin{aligned} A &= a_1^2, \\ B &= a_1^2 b_2, \\ C &= c_1^2 - a_1 c_1 a_2 + a_1^2 c_2. \end{aligned}$$

U oba slučaja je  $A > 0$  i  $B^2 - 4AC > 0$  ako tražena sjecišta postoje.

5. Sjecište dviju kružnica  $x^2 + y^2 + a_1x + b_1y + c_1 = 0$  i  $x^2 + y^2 + a_2x + b_2y + c_2 = 0$ . Rješavanje ovog sustava svodi se na rješavanje sustava jednačbi bilo koje od ovih dviju kružnica i pravca  $(a_1 - a_2)x + (b_1 - b_2)y + c_1 - c_2 = 0$ . Taj pravac je potencijala tih dviju danih kružnica. Dakle, problem sjecišta dviju kružnica svodi se na problem sjecišta kružnice i pravca prikazan u točki 4.

Dakle, sve temeljne operacije ravnalom i šestarom moguće je analitičkom metodom dobiti u konačno mnogo koraka primjenom osnovnih racionalnih operacija i vađenjem kvadratnog korijena čime je teorem dokazan. □

Prethodna dva teorema dokazuju da je mogućnost prikaza broja  $x$  iz brojeva  $m_1, m_2, \dots, m_n$  s konačno mnogo racionalnih operacija i konačno mnogo vađenja kvadratnih korijena nužan i dovoljan uvjet za mogućnost konstruiranja dužine čiji je mjerni broj  $x$  iz danih dužina s mjernim brojevima  $m_1, m_2, \dots, m_n$  pomoću ravnala i šestara.

**Definicija 2.2.6.** *Kažemo da je realni broj  $x$  moguće **elementarno konstruirati** (ili da je **konstruktibilan**) ako je  $x \in \mathbb{Q}$  ili  $x \in \mathbb{Q}(q_1, q_2, \dots, q_k)$ , gdje je  $q_i = \sqrt{A_i}$ ,  $A_i \in \mathbb{Q}(q_1, q_2, \dots, q_{i-1})$ ,  $i = 1, 2, \dots, k$ , a  $q_i \notin \mathbb{Q}(q_1, q_2, \dots, q_{i-1})$  (pri čemu uzimamo  $\mathbb{Q}(q_0) = \mathbb{Q}$ ). Kompleksan broj  $z$  je moguće **elementarno konstruirati** ako je moguće elementarno konstruirati njegov realni dio  $\text{Re}z$  i imaginarni dio  $\text{Im}z$ .*

**Definicija 2.2.7.** *Ako se korijeni algebarske jednačbe s racionalnim koeficijentima mogu elementarno konstruirati, onda kažemo da je ta jednačba **rješiva u kvadratnim radikalima**.*

Ako točke ravnine identificiramo sa  $\mathbb{C}$ , gdje točka  $O$  odgovara broju 0, a točka  $E$  broju 1, iz dokaza prethodna dva teorema slijedi:

**Teorem 2.2.8.** *Točka  $z \in \mathbb{C}$  se može konstruirati ako i samo ako je broj  $z$  konstruktibilan.*

Uočimo, kut  $\alpha$  se može konstruirati ako i samo ako se mogu konstruirati  $|\cos \alpha|$  i  $|\sin \alpha|$ , odnosno  $e^{i\alpha} = \cos \alpha + i \sin \alpha$  je konstruktibilan.

Ako su  $\alpha \in \mathbb{Q}(q_1, q_2, \dots, q_n)$ ,  $\alpha \neq 0$ ,  $\beta \in \mathbb{Q}(q'_1, q'_2, \dots, q'_m)$  konstruktibilni, tada su  $\alpha\beta$ ,  $\alpha - \beta$ ,  $\alpha + \beta$ ,  $\frac{1}{\alpha} \in \mathbb{Q}(q_1, q_2, \dots, q_n, q'_1, \dots, q'_m)$  pa zaključujemo da konstruktibilni brojevi čine polje.

**Teorem 2.2.9.** *Ako neka kubna jednadžba*

$$x^3 + a_2x^2 + a_1x + a_0 = 0$$

*s cjelobrojnim koeficijentima ima racionalno rješenje  $x_1$ , tada je taj  $x_1$  cijeli broj i djelitelj je broja  $a_0$ .*

*Dokaz.* Neka je  $x_1$  jedno racionalno rješenje jednadžbe. To rješenje možemo pisati u obliku  $x_1 = \frac{l}{m}$  ( $l, m \in \mathbb{Z}, m > 0$ , najveći zajednički djelitelj od  $l$  i  $m$  je 1). Kako je  $x_1$  rješenje, slijedi

$$l^3 + a_2l^2m + a_1lm^2 + a_0m^3 = 0$$

odakle dalje slijedi

$$l^3 = -m \cdot (a_2l^2 + a_1lm + a_0m^2)$$

i odatle  $m = 1$ . Iz prethodne jednakosti slijedi također

$$a_0m^3 = -l \cdot (l^2 + a_2lm + a_1m^2)$$

i odatle izlazi da je  $l$  djelitelj od  $a_0$ . Napokon na temelju prikaza  $x_1 = \frac{l}{m}$  slijedi neposredno tvrdnja teorema.  $\square$

**Teorem 2.2.10.** *Jednadžba trećeg reda s racionalnim koeficijentima rješiva je u kvadratnim radikalima ako i samo ako ima racionalni korijen.*

*Dokaz.* Najprije ako jednadžba trećeg reda s racionalnim koeficijentima ima racionalni korijen  $\frac{p}{q}$  ( $q \neq 0$ ), onda se ona može faktorizirati kao  $(qx - p)(rx^2 + sx + t) = 0$ , gdje su svi koeficijenti racionalni pa odatle odmah slijedi tvrdnja.

Obratno, pođimo od jednadžbe

$$f(x) = x^3 + ax^2 + bx + c = 0. \quad (2.1)$$

Treba pokazati ako je 2.1 rješiva u kvadratnim radikalima, onda ona ima racionalan korijen. Pretpostavimo suprotno.

Jednadžba 2.1 ima bar jedan realan korijen. Neka je to  $x_1$  (po pretpostavci nije racionalan). Kako je jednadžba 2.1 rješiva u kvadratnim radikalima, to postoje iracionalni brojevi  $\varrho_1 = \sqrt{A_1}, \dots, \varrho_k = \sqrt{A_k}$ ,  $k \geq 1$ ,  $A_j \in \mathbb{Q}(\varrho_1, \dots, \varrho_{j-1})$ ,  $j = 1, \dots, k$ , takvi da je

$$x_1 \in \mathbb{Q}(\varrho_1, \dots, \varrho_k).$$

Bez smanjenja općenitosti možemo pretpostaviti da  $\varrho_k \notin \mathbb{Q}(\varrho_1, \dots, \varrho_{k-1})$ , jer bi u suprotnom u našoj konstrukciji  $\varrho_k$  bio suvišan i mogli bismo stati kod  $\varrho_{k-1}$ .

Analogno možemo pretpostaviti da  $x_1 \notin \mathbb{Q}(\varrho_1, \dots, \varrho_{k-1})$ . Pokazat ćemo najprije da su svi korijeni od 2.1 realni i konstruktibilni.

Pretpostavka  $x_1 \in \mathbb{Q}(\varrho_1, \dots, \varrho_k)$  povlači da je  $x_1$  oblika

$$x_1 = p + q\varrho_k, \quad p, q \in \mathbb{Q}(\varrho_1, \dots, \varrho_{k-1}), \quad q \neq 0.$$

Pokazat ćemo da je  $x_2 = p - q\varrho_k$  također korijen od 2.1 koji je očito realan i konstruktibilan. U tu svrhu uvrstimo  $x_1 = p + q\varrho_k$  u 2.1. Dobijemo

$$f(x) = P + Q\varrho_k = 0,$$

gdje je  $P = p^3 + 3pq^2A_k + ap^2 + aq^2A_k + bp + c$ ,  $Q = 3p^2q + q^3A_k + 2apq + bq$ . Dakle,  $P, Q \in \mathbb{Q}(\varrho_1, \dots, \varrho_{k-1})$ . Ako bi vrijedilo  $Q \neq 0$ , onda bi bilo  $\varrho_k = -\frac{P}{Q}$ , tj.  $\varrho_k \in \mathbb{Q}(\varrho_1, \dots, \varrho_{k-1})$ , suprotno pretpostavci. Dakle,  $Q = 0$ , što povlači  $P = 0$ .

Ako sada u 2.1 uvrstimo  $x_2 = p - q\varrho_k$  lakim računom dobivamo da je

$$f(x_2) = P - Q\varrho_k,$$

pa  $P = Q = 0$  povlači  $f(x_2) = 0$ . Dakle,  $x_2$  je korijen jednadžbe 2.1 i  $x_2 \neq x_1$  (jer je  $q \neq 0$ ). Neka je  $x_3$  treći korijen od 2.1. Prema Vièteovoj formuli  $x_1 + x_2 + x_3 = -a$  slijedi  $x_3 = -a - 2p$ . Odavde zbog  $a \in \mathbb{Q}$ ,  $p \in \mathbb{Q}(\varrho_1, \dots, \varrho_{k-1})$  slijedi da je  $x_3 \in \mathbb{Q}(\varrho_1, \dots, \varrho_{k-1})$ . Dakle,  $x_3$  je realan i konstruktibilan.

Kontradikcija koja dokazuje tvrdnju teorema sastojat će se u tome da iz naših pretpostavki slijedi  $x_2 \in \mathbb{Q}(\varrho_1, \dots, \varrho_{k-1})$  i tada  $x_1 \in \mathbb{Q}(\varrho_1, \dots, \varrho_{k-2})$ . To se sada dobije tako da se ponovi prethodni postupak na korijen  $x_3$ .  $\square$

Sljedeći teorem govori nam o jednadžbama četvrtog stupnja, tj. o njihovoj rješivosti u kvadratnim radikalima. Za dokaz tog teorema bit će nam potrebna njezina rezolventa.

Za jednadžbu

$$f(x) = x^4 + ax^3 + bx^2 + cx + d = 0, \quad a, b, c, d \in \mathbb{Q}, \quad (2.2)$$

njena rezolventa je jednadžba trećeg stupnja

$$(ay - c)^2 = 4 \left( \frac{a^2}{4} - b + 2y \right) (y^2 - d). \quad (2.3)$$

Rezolventa nam je potrebna da bi izraz u uglatoj zagradi u zapisu

$$f(x) = (x^2 + \frac{a}{2}x + y)^2 - [(\frac{a^2}{4} - b + 2y)x^2 + (ay - c)x + y^2 - d]$$

bio kvadrat nekog linearnog polinoma  $Ax + B$ . Stoga su veze među korijenima  $x_i$  jednadžbe 2.2 i korijenima  $y_1$  rezolvente 2.3 kvadratne, tj. vrijedi

$$x_i^2 + \frac{a}{2}x_i + y_i = \pm(Ax_i + B).$$

Odavde neposredno slijedi teorem.

**Teorem 2.2.11.** *Jednadžba četvrtog stupnja 2.2 je rješiva u kvadratnim radikalima ako i samo ako je u kvadratnim radikalima rješiva njezina rezolventa 2.3.*

Iz Teorema 2.2.10 i 2.2.11 dobivamo kriterij za konstruktibilnost korijena jednadžbe četvrtog stupnja.

**Korolar 2.2.12.** *Korijeni jednadžbe 2.2 se mogu elementarno konstruirati ako i samo ako njezina rezolventa 2.3 ima racionalni korijen.*

Pokažimo primjenu ovih teorema na konkretnom primjeru.

**PRIMJER.** Unutar danog kuta zadana je točka. Pokažite da se elementarno ne može tom točkom konstruirati dužina zadane duljine, kojoj su krajevi na krakovima kuta.

**Rješenje.** Uzmimo posebni slučaj da je kut pravi i promotrimo u koordinatnom sustavu točku  $(1, 2)$  kroz koju treba prolaziti pravac koji siječe osi u točkama čija je udaljenost jednaka 6. Taj pravac ima jednadžbu  $y - 2 = k(x - 1)$ . Taj pravac možemo elementarno konstruirati ako i samo ako možemo konstruirati koeficijent smjera  $k$ . No, iz uvjeta da je navedena udaljenost 6 i  $k \neq 0$  slijedi  $(\frac{k-2}{k})^2 + (k-2)^2 = 36$ , tj.

$$k^4 - 4k^3 - 31k^2 - 4k + 4 = 0.$$

Rezolventa te jednadžbe je jednadžba

$$f(y) = 2y^3 + 31y^2 - 144 = 0.$$

Kandidati za racionalni korijen te jednadžbe su brojevi  $\frac{p}{q}$ , gdje su

$$p = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 9, \pm 12, \pm 16, \pm 18, \pm 24, \pm 36, \pm 48, \pm 72, \pm 144,$$

i  $q = \pm 1, \pm 2$ . Lako se vidi da niti jedan od ovih nije korijen.

U stvari, zbog  $f(2) < 0, f(3) > 0, f(-3) > 0, f(-2) < 0, f(-12) > 0, f(-16) < 0$ , dovoljno je ispitati samo one kandidate koji su u uniji  $[-16, -12] \cup [-3, -2] \cup [2, 3]$ .

Prema 2.2.12,  $k$  nije moguće elementarno konstruirati te stoga nije moguće konstruirati ni traženi pravac.

## Poglavlje 3

# Klasični geometrijski problemi

U prethodnim poglavljima pokazali smo mnogo konstrukcija koje su izvedive ravnalom i šestarom. No, postavlja se pitanje je li svaki geometrijski problem moguće riješiti konstrukcijom ravnalom i šestarom? S tim pitanjem suočili su se već u vremenu Antičke Grčke. Njihovi problemi poznati su pod zajedničkim nazivom "klasični problemi", a radi se o kvadraturi kruga, duplikaciji kocke i trisekciji kuta.

Kvadratura kruga podrazumijeva konstrukciju kvadrata čija površina je jednaka površini danog kruga. Duplikacija kocke pak podrazumijeva konstrukciju brida kocke koja ima dvostruko veći volumen od dane kocke, a trisekcija kuta, kao što samo ime govori, podrazumijeva podijelu kuta na tri jednaka dijela.

Mnogi starogrčki matematičari bavili su se njihovim rješavanjem, ali do rezultata ravnalom i šestarom nisu došli. Neki od njih uspjeli su doći do rješenja, ali problemu su pristupali na drugačiji način.

U ovome poglavlju čitat ćemo o nekim pokušajima konstrukcije tih i takvih problema, navedenim u [2] i [10], ali i o njihovoj ne rješivosti ravnalom i šestarom.

### 3.1 Kvadratura kruga

Kaže se da je na problem kvadrature kruga tijekom vremena potrošeno više intelektualnog napora nego za slanje čovjeka na Mjesec. To nam govori da je ovaj problem bio važan mnogim matematičarima kroz povijest.

Smatra se da je na jednom od najstarijih sačuvanih matematičkih tekstova, Rhindovom papirusu iz oko 1650. g. pr. Kr., prvi put spomenut problem kvadrature kruga. Pisar Ahmes opisuje kako konstruirati kvadrat čija površina je gotovo jednaka površini nekog kruga.

Mnogi matematičari još od vremena antičke Grčke bavili su se ovim problemom. Mnogi od njih došli su do različitih rješenja, ali ni jedno od njih nije dobiveno konstrukcijom



ravnalom i šestarom, već su dobivena mehaničkim metodama. Neke od dobivenih rješenja ćemo detaljnije opisati.

## **Matematičari koji su pokušavali riješiti problem kvadrature kruga**

### **Antifont**

Antifont (oko 480.–411. pr. Kr.) za rješenje predlaže upisivanje pravilinih mnogokuta u krug. Njegova zamisao bila je upisivati pravilne mnogokute, krenuvši od kvadrata, u krug. Nakon kvadrata išao bi osmerokut pa šesnaesterokut. Smatrao je da proces može ponavljati udvostručujući broj stranica mnogokuta sve dok razlika između površine mnogokuta i površine kruga nebi nestala.

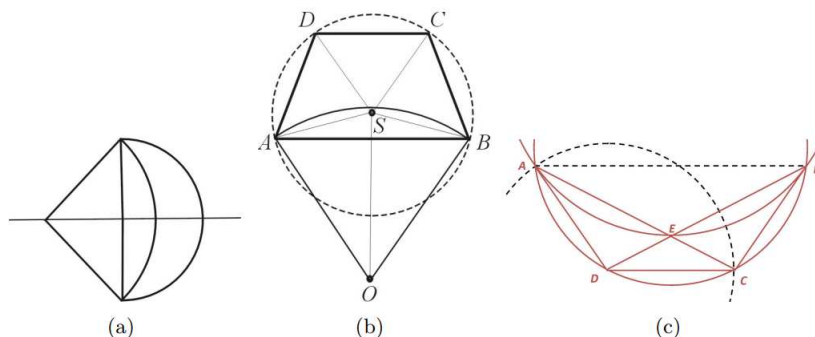
### **Brison**

Antifontovu ideju nadgradio je Brison (oko 450.–390. pr. Kr.). On je osim što je upisivao mnogokute unutar kruga, opisivao mnogokute oko kruga, a onda promatrao mnogokut između njih. Kao i Antifont, krenuo bi od kvadrata pa povećavao broj stranica. Kako se broj stranica povećavao, tako je razlika između upisanog i opisanog mnogokuta postajala sve manja, a samim time je i mnogokut između njih bivao sve sličnije površine njihovima. Povećanjem broja stranica mnogokuta površine tog mnogokuta i kruga, prema Brisonu, postaju jednake. Nije pronađen podatak kako je određivao mnogokut između upisanog i opisanog mnogokuta. Nama je poznato da takvih ima beskonačno mnogo.

### **Hipokrat**

Hipokrat (oko 470.–410. pr. Kr.) je shvatio da bi kvadriranjem krivocrtnog lika lakše razumio problem kvadrature kruga pa se počeo baviti takozvanim mjesecima. Mjesec je geometrijski lik omeđen kružnim lukovima dviju kružnica koje imaju različita središta i različite polumjere.

Hipokrat je prvi koji je ravnalom i šestarom kvadrirao neke mjesece i točno odredio njihove površine i zato takve mjesece danas zovemo Hipokratovim mjesecima. Danas je poznato da takvih mjesececa ima 5 dok je Hipokrat znao njih 3. Bio je svijestan da time nije riješio problem kvadrature kruga. Međutim, otkrio je, a vjerojatno i dokazao, da se površine krugova odnose kao površine kvadrata nad njihovim polumjerima.

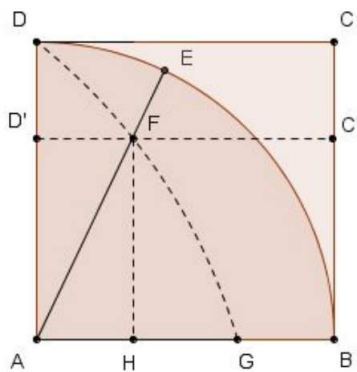


Slika 3.1: Slika Hipokratovih mjeseca preuzeta iz knjige Povijest matematike I (izmijenjeno i dopunjeno izdanje) Franke Miriam Brückler

**Dinostrat**

Dinostrat (oko 390.-320. pr. Kr.) je za rješavanje problema kvadrature kruga koristio Hippijnu kvadratisu.

Hippija (oko 460.-400. pr. Kr.) je važan zbog otkrića kvadratise, krivulje kojom se može



Slika 3.2: Slika Hippijine kvadratise preuzeta iz diplomskog rada Tri klasična problema Marine Musa

riješiti problem kvadrature kruga (ali i trisekcije kuta). Kvadratisa je krivulja koju dobijemo kao geometrijsko mjesto točkaka  $F$  koje su sjecišta stranice  $\overline{DC}$  kvadrata  $ABCD$  (koja jednoliko pada na stranicu  $\overline{AB}$ ) i stranice  $\overline{AD}$  (koja jednoliko rotira oko točke  $A$  prema stranici  $\overline{AB}$ ). Te stranice "gibaju" se jednoliko tako da u isto vrijeme stranica  $\overline{DC}$  padne

na stranicu  $\overline{AB}$  i stranica  $\overline{AD}$  rotacijom padne na stranicu  $\overline{AB}$ . Dakle, kvadratisa je krivulja koju nije moguće dobiti konstrukcijom isključivo ravnalom i šestarom. Takve krivulje nazivamo **mehaničkima**.

Dinostrat je pokazao da kada kvadratisa siječe stranicu  $\overline{AB}$  u točki  $G$  vrijedi:

$$\widehat{DB} : |AB| = |AB| : |AG|.$$

Ova jednakost koristi se za dokaz da je površina kruga jednaka površini pravokutnog trokuta čija je jedna kateta duljine jednake duljini polumjera tog kruga, a druga kateta duljine opsega tog kruga. Taj dokaz dao je Arhimed.

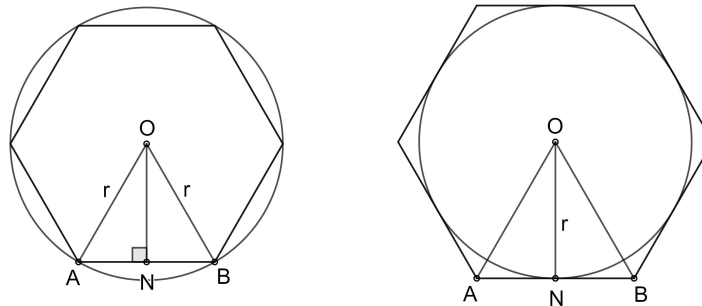
### Arhimed

Najveći napredak u rješenju problema kvadrature kruga dao je Arhimed iz Sirakuze (oko 287.–212. pr. Kr.). On je dokazao da je površina kruga jednaka površini pravokutnog trokuta kojem je jedna kateta jednaka polumjeru, a druga opsegu tog kruga. Da bi dokazao tu tvrdnju koristio je sljedeće pretpostavke i teoreme:

1. Krug i kružni odsječak imaju površinu.
2. Površina skupa u parovima disjunktih trokuta i kružnih odsječaka jednaka je zbroju njihovih površina. Specijalno, ako krug rastavimo na disjunktne trokute i kružne odsječke, površinu kruga možemo dobiti kao zbroj njihovih površina. Također, površina kruga veća je od zbroja površina bilo kojeg pravog podskupa tih trokuta i odsječaka.
3. Za svaki krug postoji duljina veća od opsega bilo kojeg tom krugu upisanog poligona i manja od opsega bilo kojeg tom krugu opisanog poligona: to je opseg kruga (ime  $\pi$  za opseg kruga promjera  $r = 1$  potječe od Williama Jonesa, 1706.).
4. Arhimedov aksiom: za svake dvije površine  $P$  i  $S$  postoji prirodan broj  $m$  takav da je  $mP > S$ .
5. Pravilni  $2^n$ -terokut upisan u krug pokriva više od  $1 - 2^{-(n-1)}$  njegove površine, a pravilni  $2^n$ -terokut opisan krugu ima površinu manju od  $1 + 2^{-(n-2)}$  površine kruga.
6. Površina kruga razmjerna je kvadratu njegova promjera.

Arhimed kaže:

Neka je  $P$  površina danog kruga, a  $S$  površina pravokutnog trokuta kojem je jedna kateta jednaka polumjeru  $r$ , a druga opsegu  $O$  tog kruga. Tada:


 Slika 3.3: Površina upisanog i opisanog  $2^n$ -terokuta na primjeru šesterokuta

- Ako je  $P > S$ , onda prema točkama 4 i 5 postoji  $n \in \mathbb{N}$  takav da je površina upisanog  $2^n$ -terokuta veća od  $S$ . Neka je  $\overline{AB}$  stranica tog upisanog  $2^n$ -terokuta i  $N$  njeno polovište. Tada je  $|ON| < r$  jer je  $\overline{ON} \perp \overline{AB}$ . Prema točki 3 slijedi da je površina upisanog  $2^n$ -terokuta jednaka

$$2^n \frac{|AB| \cdot |ON|}{2} = |ON| \frac{2^n |AB|}{2} < \frac{r \cdot o}{2} = S,$$

gdje je  $o$  opseg danog kruga.

- Ako je  $P > S$ , onda prema točkama 4 i 5 postoji  $n \in \mathbb{N}$  takav da je površina opisanog  $2^n$ -terokuta manja od  $S$ . Neka je  $\overline{AB}$  stranica tog opisanog  $2^n$ -terokuta i  $N$  njeno polovište. Tada je  $|ON| = r$ . Prema točki 3 slijedi da je površina opisanog  $2^n$ -terokuta jednaka

$$2^n \frac{|AB|r}{2} > \frac{r \cdot o}{2} = S.$$

Dakle, kako ne vrijedi ni  $P < S$ , ni  $P > S$ , prema Aristotelovom principu isključenja trećeg slijedi da je  $P = S$ .

### Dokaz o neizvedivosti konstrukcije kvadrature kruga ravnalom i šestarom

Postoje egzaktna rješenja koja nisu dobivena konstrukcijom ravnalom i šestarom. Ravnalom i šestarom je moguće napraviti približnu konstrukciju, sa određenom pogreškom.

Problem kvadrature kruga objasniti ćemo algebarski. Neka je zadan krug polumjera  $r$ . Površina toga kruga jednaka je  $P = r^2\pi$ . Budući da je

$$r^2\pi = \left( \sqrt{2r\pi \cdot \frac{r}{2}} \right)^2,$$

zaključujemo da traženi kvadrat ima stranicu duljine  $a = \sqrt{2r\pi \cdot \frac{r}{2}}$ .

Dakle, stranicu  $a$  traženog kvadrata možemo konstruirati kao geometrijsku sredinu između  $2r\pi$  i  $\frac{r}{2}$ . Za  $r = 1$ , problem kvadrature kruga svodi se na konstrukciju dužine čija je duljina  $2\pi$ .

Kako je broj  $\pi$  transcendentan broj, slijedi da njegova konstrukcija ravnalom i šestarom nije izvediva.

## 3.2 Duplikacija kocke

Problem duplikacije ili udvostručenja kocke bio je jako popularan u vrijeme starih Grka. Priča koju je zapisao Teon iz Smirne, a izvorno je pismo Eratostena kralju Egipta, kaže da su se Atenjani za vrijeme epidemije kuge oko 430. pr. Kr. obratili proročištu na otoku Delosu. Tražili su savjet što učiniti kako bi stala epidemija. Proročište im je savjetovalo da udvostruče oltar bogu Apolonu. Atenjani su izgradili oltar kockastog oblika, ali nisu udvostručili volumen u odnosu na postojeći oltar, nego su udvostručili duljinu stranice oltara čime su dobili oltar volumena osam puta većeg od postojećeg. Legenda kaže da je gradom nastavila harati kuga jer Atenjani nisu poslušali savjet proročišta. Toj legendi u čast, ovaj problem poznat je i pod imenom Delski problem.

Postoji još jedna priča o nastanku ovog problema. Zapisao ju je Eutocius u komentaru Arhimedova djela O kugli i valjku i ona kaže da je kralj Minos bio nezadovoljan veličinom grobnice pjesnika Glaukusa pa ju je odlučio udvostručiti. Na kraju je i on dobio osam puta veću grobnicu jer je zapravo udvostručio duljinu stranice grobnice.

Dakle, nismo sigurni kako je ovaj problem nastao, ali može se pretpostaviti da je ipak nastao kao generalizacija dupliciranja kvadrata. Odnosno, kako se radi o stereometrijskom problemu, da bi ga riješili prvo su ga sveli na problem u ravnini. Sa sigurnošću možemo reći da su stari Grci znali duplicirati kvadrat.

## Matematičari koji su pokušavali riješiti problem duplikacije kocke

### Arhita

Arhita (oko 428. – 350. pr. Kr.) je srednje geometrijske proporcionalne između  $a$  i  $2a$  odredio korištenjem presjeka cilindra, konusa i torusa. (Torus je rotaciono tijelo koje nastaje rotacijom kružnice oko osi koja leži u ravnini kružnice.)

Radi lakšeg razumijevanja, problem ćemo opisati koristeći analitičku geometriju.

Dakle, imamo presjek ploha s jednadžbama

$$\begin{aligned}x^2 + y^2 + z^2 &= 4x^2, \\x^2 + y^2 &= 2ax, \\x^2 + y^2 + z^2 &= 2a\sqrt{x^2 + y^2}.\end{aligned}$$

gdje prva jednadžba predstavlja cilindar polumjera  $a$  kojemu je os pravac kroz točku  $(a, 0, 0)$  paralelan  $z$ -osi. Druga jednadžba predstavlja konus s vrhom u ishodištu kojem je os  $x$ -os koordinatnog sustava i koji ima vršni kut od  $120^\circ$ . Treća jednadžba predstavlja torus kojem je  $a$  polumjer poprečnog presjeka, a rupa je polumjera  $0$ .

Rješavanjem i sređivanjem sustava dobivamo

$$a : \sqrt{x^2 + y^2} = \sqrt{x^2 + y^2} : \sqrt{x^2 + y^2 + z^2} = \sqrt{x^2 + y^2 + z^2} : 2a.$$

Dobivena jednakost vrijedi za koordinate točke dobivene presjekom tih triju ploha. Primjetimo da rješenje sustava daje tražene geometrijske proporcionalne.

### Hipokrat

Hipokrat je dokazao da ako za brojeve  $a, x, y$  vrijedi odnos

$$a : x = x : y = y : 2a, \tag{3.1}$$

tada kocka s bridom duljine  $x$  ima volumen dvostruko veći od kocke s bridom duljine  $a$ . Tada su duljine  $x$  i  $y$  srednje geometrijske proporcionalne između duljina  $a$  i  $2a$ .

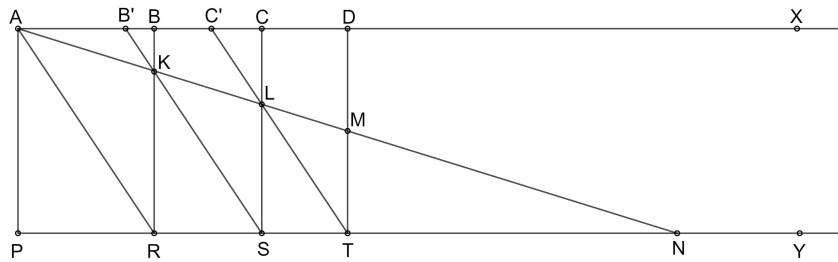
Zaista, iz izraza 3.1 vidimo da vrijedi  $x^3 = 2a^3$ .

Nakon Hipokrata, svi pokušaji konstrukcije duplikacije kocke svodili su se na određivanje srednjih geometrijskih proporcionala između  $a$  i  $2a$ .

### Eratosten

Eratosten (oko 275. - 195. pr. Kr.) je dao jedno od najpoznatijih mehaničkih rješenja problema duplikacije kocke. Njegov mezolabij je mehanizam koji određuje srednje geometrijske proporcionalne. Sastoji se od dvije letve postavljene paralelno tako da su im

spojnice koje povezuju njihove rubove okomite na letve. Na njih su postavljena tri sukkladna pravokutna trokuta na način da je po jedna njihova kateta naslonjena na jednu od dviju letvi, a nasuprotni vrh je na drugoj letvi. Prvi trokut je fiksiran uz rub letve, a preostala dva pomičemo. Modelirajmo situaciju kako bi lakše objasnili postupak:



Slika 3.4: Eratostenov mezolabij

Dvije letve prikazimo dvama paralelnim polupravcima  $AX$  i  $BY$ . Neka su trokuti  $ABR$ ,  $BCS$ ,  $CDT$  tri sukkladna pravokutna trokuta kojima su katete  $\overline{AB}$ ,  $\overline{BC}$ ,  $\overline{CD}$  na polupravcu  $AX$ , a vrhovi  $R$ ,  $S$ ,  $T$  na polupravcu  $BY$ . Prvi trokut je fiksiran, a preostala dva pomičemo tako da se preklapaju. Time dobivamo nove točke, tj. trokute  $B'CS$  i  $C'DT$ . Neka je tada  $BR \cap B'S = K$  i  $CS \cap C'T = L$ . Dužina  $\overline{AB}$  okomita je na polupravce. Potrebno je fiksirati polovište  $M$  dužine  $\overline{DT}$ . Trokute  $B'CS$  i  $C'DT$  je potrebno pomicati sve dok točke  $A$ ,  $K$ ,  $L$  i  $M$  ne postanu kolinearne. Neka je  $BY \cap AM = N$ .

Lako se dokaže da su trokuti  $APN$ ,  $KRN$ ,  $LSN$  i  $MTN$  slični:

- $\angle APN = \angle KRN = \angle LSN = \angle MTN = 90^\circ$
- $\angle ANP = \angle KNR = \angle LNS = \angle MNT$

Dakle, prema  $KK$  teoremu o sličnosti trokuta slijedi da su trokuti  $APN$ ,  $KRN$ ,  $LSN$  i  $MTN$  slični.

Iz toga možemo zaključiti da vrijedi:

$$|AP| : |KR| = |KR| : |LS| = |LS| : |MT|.$$

Stoga su  $|KR|$  i  $|LS|$  tražene srednje geometrijske proporcionalne između  $|AP|$  i  $|MT|$ . Kako je  $|MT| = \frac{1}{2}|AP|$  slijedi da je za duplikaciju kocke brida  $a = |MT|$  potreban brid duljine  $|LS|$ .

### Dokaz o neizvedivosti konstrukcije duplikacije kocke ravnalom i šestarom

Zadana je kocka s bridom duljine  $a$ . Potrebno je konstruirati brid kocke čiji je volumen jednak dvostrukom volumenu zadane kocke.

Duljinu brida tražene kocke označimo s  $x$ , a duljinu brida zadane kocke s  $a$ . Kako volumen kocke računamo po formuli  $V = a^3$ , slijedi da je  $x^3 = 2a^3$ .

Dakle, trebamo konstruirati dužinu duljine  $x = a\sqrt[3]{2}$  iz zadane duljine  $a$ . Ovaj zadatak je rješiv ako je moguće konstruirati ravnalom i šestarom dužinu duljine  $\sqrt[3]{2}$ .

Transformacijama formule  $x^3 = 2a^3$  i uvrštavanjem  $y = \frac{x}{a}$  dobivamo  $y^3 - 2 = 0$ . Kada bi taj zadatak bio rješiv, prema teoremu 2.2.6. broj  $x = a\sqrt[3]{2}$  bio bi konstruktibilan iz broja 1 te bi jednadžba

$$y^3 - 2 = 0 \tag{3.2}$$

imala jedno rješenje, konstruktibilno iz racionalnih brojeva. Jednadžba 3.1. nema racionalnih rješenja jer prema teoremu 2.2.7. rješenja moraju biti djelitelji broja 2, a jedini kandidati su brojevi  $\pm 1, \pm 2$ , koji nisu rješenja te jednadžbe. Zaključujemo da nije moguće konstruirati ravnalom i šestarom brid kocke čiji je volumen duplo veći od zadane.

### 3.3 Trisekcija kuta

Problem trisekcije kuta je, za razliku od preostala dva klasična problema, rješiv u nekim slučajevima konstrukcijom ravnalom i šestarom. Smatra se da je nastao iz želje za konstrukcijom pravilnog deveterokuta. Stari Grci trebali su kružnicu podijeliti na devet jednakih dijelova. To su pokušali tako da su najprije konstruirali jednakostranični trokut i time kružnicu podijelili na tri jednaka dijela. Problem je nastao kada je središnji kut od  $120^\circ$  trebalo podijeliti na tri jednaka dijela. Konstrukcijom ravnalom i šestarom to nisu uspjeli. Međutim, neke kutove ipak je moguće podijeliti na tri jednaka dijela. Na primjer, moguće je konstruirati trećinu pravog kuta jer znamo konstruirati kut od  $60^\circ$  pa je preostali dio do pravog kuta zapravo njegova trećina. Ovdje ćemo promatrati trisekciju samo šiljastih kutova jer se tupi kut svodi na zbroj pravog i šiljastog kuta.

#### Matematičari koji su pokušavali riješiti problem trisekcije kuta

Mnogi matematičari pokušavali su raznim metodama doći do konstrukcije trisekcije kuta. Međutim, ravnalom i šestarom to nisu uspjeli u svakom slučaju pa su se okrenuli drugačijim metodama. Prikazat ćemo neke od njih.

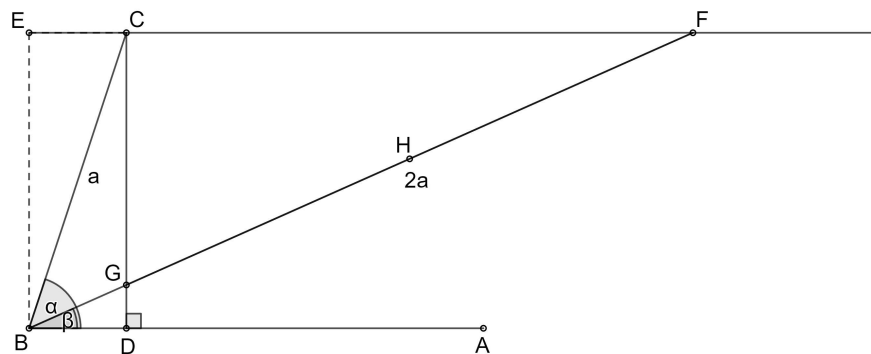


### Hipokrat

Hipokratovo mehaničko rješenje trisekcije kuta glasilu je:

Zadan je kut  $\angle ABC$  mjere  $\alpha$ . Konstruiramo okomicu iz vrha  $C$  na krak  $AB$ . Nožište te okomice označimo točkom  $D$ . Konstruiramo točku  $E$  tako da mnogokut  $BDCE$  bude pravokutnik. Sada stranicu  $\overline{EC}$  produžimo u polupravac  $EC$ . Na ravnalu označimo dužinu  $\overline{BC}$  i ravnalo namjestimo tako da prolazi točkom  $B$  i polupravcem  $EC$  te da odsječak između polupravca  $EC$  i okomice  $CD$  bude jednak duljini dužine  $\overline{BC}$ . Neka je tada  $F$  točka na polupravcu  $EC$  i  $G$  točka na okomici  $CD$ . Dakle,  $|GF| = 2|BC|$ . Sada je kut  $\angle ABF$  jednak trećini kuta  $\alpha$ .

Zaista, označimo li kut  $\angle ABF = \beta$ , slijedi da je i kut  $\angle BFC = \beta$  zbog transversale paralelnih pravaca. Pogledajmo trokut  $HFC$ . On je jednakokrčan s krakovima  $\overline{HF}$  i  $\overline{HC}$  pa je  $\angle HFC = \angle HCF = \beta$ , odnosno kut  $\angle CHF = 180^\circ - 2\beta$ . Dakle, kut  $\angle CHB = 2\beta$ . Kako je i trokut  $BHC$  također jednakokrčan s krakovima  $HC$  i  $BC$  slijedi da je i kut  $\angle HBC = 2\beta$ . Dakle, kut  $\alpha = \angle ABC = \angle ABF + \angle FBC = \beta + 2\beta = 3\beta$  čime smo dokazali trisekciju kuta  $\alpha$ .



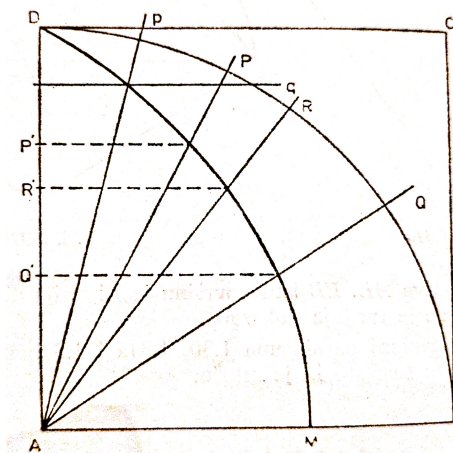
Slika 3.5: Hipokratova trisekcija kuta

### Hipija

Najpoznatiju ideju rješenja ovog problema dao je Hipija, a u rješavanju mu je pomogla već spomenuta krivulja kvadratisa. Njegova ideja bila je trisekciji dužine pridružiti trisekciju kuta.

Pokažimo kako je Hipija podijelio kut na tri jednaka dijela:

Neka točke  $P$  i  $Q$  pripadaju kružnom luku  $\widehat{BD}$ . Izvršimo trisekciju kuta  $\angle PAQ$ . Pomoću kvadratise točkama  $P$  i  $Q$  pronađemo pridružene točke  $P'$  i  $Q'$  na dužini  $\overline{AD}$ . Sada dužinu  $\overline{P'Q'}$  podijelimo na tri jednaka dijela, tj. nađemo točku  $R'$  takvu da dužinu  $\overline{P'Q'}$  dijeli u omjeru  $1 : 2$ . Nadalje, pomoću kvadratise pronađemo točku  $R$  na kružnom luku  $\widehat{BD}$ . Kako se stranice  $\overline{AD}$  i  $\overline{DC}$  gibaju jednoliko, slijedi da dužini  $\overline{DC}$  da dođe od točke  $P'$  do točke  $R'$  treba trećina vremena potrebnog da dođe od točke  $P'$  do točke  $Q'$ . Također, isto vrijedi i za rotaciju dužine  $\overline{AD}$  pa slijedi da je kut  $\angle PAR$  trećina kuta  $\angle PAQ$ .



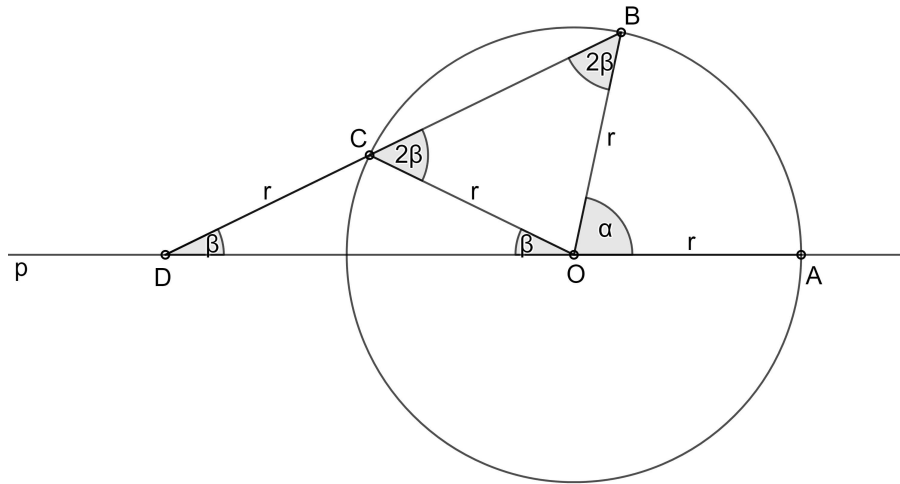
Slika 3.6: Hipijina trisekcija kuta preuzeta iz knjige Pogled u povijest matematike Štefana Znama

### Arhimed

Arhimedovo mehaničko rješenje vrlo je slično Hipokratovom.

Zadan je kut mjere  $\alpha$  s vrhom  $O$ . Otvorimo šestar po volji i nacrtamo kružnicu sa središtem u točki  $O$ . Sjecište kružnice i krakova kuta označimo s  $A$  i  $B$ . Krak  $\overline{OA}$  produljimo u pravac  $p$ . Označimo na ravnalu polumjer kružnice  $r$  i namjestimo ravnalo tako da prolazi točkom  $B$ , siječe pravac  $p$  i odsječak između pravca i kružnice bude jednak označenom polumjeru  $r$ . Neka je tada  $C$  točka na pravcu, a  $D$  točka na kružnici. Dakle,  $|CD| = r$ . Sada je kut  $\angle COD$  jednak trećini kuta  $\alpha$ .

Zaista, trokut  $OCD$  je jednakokravan pa je  $\angle COD = \angle CDO = \beta$ . Iz toga slijedi da je kut  $\angle OCD = 180^\circ - 2\beta$  pa je kut  $\angle OCB = 180^\circ - \angle OCD = 2\beta$ . Kako je trokut  $OBC$  također jednakokravan, slijedi da je i kut  $\angle OBC = 2\beta$  pa je kut  $\angle BOC = 180^\circ - 4\beta$ . Kako je kut



Slika 3.7: Arhimedova trisekcija kuta

$\angle AOD$  ispruženi, slijedi

$$180^\circ = \angle AOD = \angle AOB + \angle BOC + \angle COD = \alpha + 180^\circ - 4\beta + \beta$$

iz čega slijedi da je  $\alpha = 3\beta$  čime smo dokazali trisekciju kuta  $\alpha$ .

### Papus

Papus (oko 290. - 350.) je problem trisekcije kuta riješio pomoću krivulje konhoide. Neka je dan kut  $\angle AOB$  s vrhom u točki  $O$ . Konstruiramo okomicu  $p$  na krak  $OA$  kuta  $AOB$ . Ta okomica siječe krak  $OB$  u točki  $L$ . Označimo duljinu dužine  $|OL| = a$ . Kroz točku  $L$  konstruiramo okomicu na pravac  $p$  i njezino sjecište s konhoidom označimo točkom  $C$ . Tada je kut  $\angle AOC$  trećina kuta  $\angle AOB$ .



Odnosno

$$\begin{aligned}\cos \varphi &= \cos^3 \frac{\varphi}{3} - 3 \cos \frac{\varphi}{3} (1 - \cos^2 \frac{\varphi}{3}) \\ &= \cos^3 \frac{\varphi}{3} - 3 \cos \frac{\varphi}{3} + 3 \cos^3 \frac{\varphi}{3} \\ &= 4 \cos^3 \frac{\varphi}{3} - 3 \cos \frac{\varphi}{3}\end{aligned}$$

Uvrstimo li da je

$$\begin{aligned}\cos \varphi &= d \\ \cos \frac{\varphi}{3} &= x\end{aligned}$$

možemo zaključiti da se problem trisekcije kuta  $\varphi$  svodi na pitanje da li jednadžba

$$4x^3 - 3x - d = 0$$

ima barem jedno iz racionalnih brojeva konstruktibilno rješenje.

Uvrstimo li još  $y = 2x$  i sredimo li izraz, dobivamo:

$$y^3 - 3y - 2d = 0.$$

Dakle, kad bi ova konstrukcija bila rješiva tada bi dobivena jednadžba trećeg stupnja prema teoremu 2.2.10 morala imati barem jedno iz racionalnih brojeva konstruktibilno rješenje i to bi rješenje prema teoremu 2.2.9 moralo biti djeliteľ od  $2d$ .

Kako možemo pronaći neograničeni broj vrijednosti od  $d$  za koje jednadžba 3.3 nema rješenja, slijedi da postoji nebrojeno kuteva kod kojih konstrukcija trisekcije nije izvediva ravnalom i šestarom.

Konkretno, želimo li konstruirati trisekciju kuta od  $60^\circ$ , slijedi da je  $d = \frac{1}{2}$  jer je  $\cos 60^\circ = \frac{1}{2}$ . Dakle, dobivamo jednadžbu oblika

$$y^3 - 3y - 1 = 0.$$

Jedini kandidati za racionalna rješenja ove jednadžbe su brojevi  $-1$  i  $1$ . Kako ni  $-1$  ni  $1$  nisu rješenja dobivene jednadžbe, slijedi da se kut od  $60^\circ$  ne može podijeliti na tri jednaka dijela.

S druge strane, kutu od  $90^\circ$  za kojeg smo već opisali postupak trisekcije, pridružujemo jednadžbu

$$y^3 - 3y = 0$$

jer je  $\cos 90^\circ = 0$  pa je i  $d = 0$ .

Dakle, ova jednadžba je trivijalna i ima racionalni korijen ( $y = 0$  pa je i  $x = 0$ ). Zaključujemo da zaista možemo konstruirati trisekciju kuta od  $90^\circ$ .

## Poglavlje 4

# Rješivost konstrukcija pravilnih mnogokuta

U ovom poglavlju dajemo definicije i teoreme kojima dokazujemo konstruktibilnost pravilnih mnogokuta pri čemu pratimo [6].

**Definicija 4.0.1.** *Pravilni mnogokut ili  $n$ -terokut je konveksan lik ravnine omeđen s  $n$  međusobno jednakih dužina, takvih da su mu i svi kutovi koji zatvaraju uzastopne stranice jednaki.*

**Definicija 4.0.2.** *Ciklotomski polinom (ili polinom dijeljenja kružnice)*

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ M(k,n)=1}} (x - \varepsilon_k),$$

je polinom čiji su svi korijeni primitivni  $n$ -ti korijeni iz jedinice.

Dakle,  $\Phi_n(x) \in \mathbb{C}[x]$  i  $\text{st}\Phi_n(x) = \varphi(n)$ .

Možemo zaključiti da poznavanje bilo kojeg korijena  $\varepsilon_k$  od  $\Phi_n$  potenciranjem daje kutove  $r \cdot \frac{2\pi}{n}$ , tj. kutove pravilnog  $n$ -terokuta upisanog u jediničnu kružnicu  $|z| = 1$  u kompleksnoj ravnini. Dakle, konstrukcija pravilnog  $n$ -terokuta ekvivalentna je konstrukciji jednog primitivnog  $n$ -tog korijena iz jedinice.

**Teorem 4.0.3.** *Ako je  $n = p \cdot q$ , gdje su  $n, p, q$  prirodni brojevi i  $p$  i  $q$  relativno prosti, to je konstrukcija dijeljenja kružnice na  $n$  jednakih dijelova rješiva točno onda kada je i konstrukcija dijeljenja kružnice na  $p$  i  $q$  jednakih dijelova također rješiva.*

*Dokaz.* Ako kružnica može biti podijeljena na  $n$  jednakih dijelova, tada te dijelove možemo uvijek grupirati u  $p$  grupa od po  $q$  dijelova ili u  $q$  grupa od po  $p$  dijelova.

Ako obrnuto kružnica može biti podijeljena na  $p$  odnosno na  $q$  dijelova, tada promotrimo jednadžbu

$$qx - py = 1.$$

Takvu jednadžbu je uvijek moguće riješiti s rješenjima  $x$  i  $y$  cijelim brojevima. Neka su dakle  $x$  i  $y$  cijeli brojevi i rješenja gornje jednadžbe. Slijedi

$$\frac{x}{p} - \frac{y}{q} = \frac{1}{n},$$

tako da je

$$x \cdot \frac{2\pi}{p} - y \cdot \frac{2\pi}{q} = \frac{2\pi}{n}.$$

Dakle, da se dobije  $\frac{1}{n}$ -ti dio kružnice treba od  $x$  puta  $\frac{1}{p}$ -tog dijela oduzeti  $y$  puta  $\frac{1}{q}$ -ti dio kružnice.

Na primjer, neka je  $n = 21, p = 3, q = 7$ . Rješenja sada mogu biti  $x = 4, y = 9$ . Da se razdijeli kružnica na 21 dijelova potrebno je od četverostruke trećine kružnice odbiti deveterostruku sedminu.  $\square$

**Lema 4.0.4.**  $x^n - 1 = \prod_{d|n} \Phi_d(x)$ .

*Dokaz.* Promotrimo grupu  $G = \{\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}\}$ . Neka je red elementa  $\varepsilon_k$  jednak  $d$  (tj. red podgrupe generirane sa  $\varepsilon_k$ ). Tada zbog Lagrangeovog teorema da red podgrupe dijeli red grupe, slijedi  $d|n$ . Stoga, ako je  $\varepsilon_k \in G$  primitivni  $d$ -ti korijen iz jedinice, onda  $d|n$ .

Obratno, ako  $d|n$ ,  $n = kd$ , a  $\varepsilon$   $d$ -ti primitivni korijen iz jedinice, onda je  $\varepsilon^d = 1$ , pa je  $\varepsilon^{kd} = \varepsilon^n = 1$  i stoga  $\varepsilon \in G$ . Prema tome se grupa  $G$  sastoji iz svih primitivnih  $d$ -tih korijena iz jedinice za sve  $d$  za koje je  $d|n$ .  $\square$

**Lema 4.0.5.**  $\Phi_n(x) \in \mathbb{Z}[x]$ , tj.  $\Phi_n$  je polinom s cjelobrojnim koeficijentima.

*Dokaz.* Indukcijom po  $n$ .  $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$ ,  $\Phi_2(x) = x + 1 \in \mathbb{Z}[x]$ . Pretpostavimo da je  $\Phi_r(x) \in \mathbb{Z}[x]$ , za  $r < n$ . Prvo, polinom  $\Phi_n(x)$  je očito normiran. Po pretpostavci indukcije je

$$f(x) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)$$

normirani polinom iz  $\mathbb{Z}[x]$ . Prema Lemi 4.0.4 je

$$\Phi_n(x) = \frac{x^n - 1}{f(x)},$$

a prema teoremu o dijeljenju polinoma s ostatkom slijedi da je i  $\Phi_n(x)$  polinom s cijelim koeficijentima, jer su i  $x^n - 1$  i  $f(x)$  takvi, a  $f(x)$  je i normiran.  $\square$

**Lema 4.0.6.** Polinomi  $\Phi_p(x)$  i  $\Phi_{p^a}(x)$  su ireducibilni nad  $\mathbb{Q}$ .

*Dokaz.* Prema Eisensteineovom kriteriju ireducibilnosti nad  $\mathbb{Q}$ , ako je

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$$

za kojeg postoji prost broj  $p$  takav da je  $p \nmid a_n$ ,  $p \mid a_{n-1}$ ,  $p \mid a_{n-2}$ , ...,  $p \mid a_0$ , ali  $p^2 \nmid a_0$ , onda je  $f(x)$  ireducibilan nad  $\mathbb{Q}$ . Stavimo li sada  $x = y + 1$  u  $\Phi_p(x)$ , dobivamo

$$\begin{aligned} \Phi_p(x) &= \frac{x^p - 1}{x - 1} = \frac{(y + 1)^p - 1}{y} = \\ &= y^{p-1} + \binom{p}{1} y^{p-2} + \binom{p}{2} y^{p-3} + \dots + \binom{p}{k} y^{k-1} + \dots + \binom{p}{p-2} y + p. \end{aligned}$$

Kako  $p \mid \binom{p}{k}$ ,  $1 \leq k \leq p - 1$ , slijedi da je  $\Phi_p(x)$  ireducibilan nad  $\mathbb{Q}$ . Koristeći gornju formulu za  $\Phi_{p^a}(x)$  i Eisensteinov kriterij slijedi opet uz  $x = y + 1$  slično ireducibilnost za  $\Phi_{p^a}(x)$ .  $\square$

**Definicija 4.0.7.** Prost broj  $p$  oblika  $p = 2^{2^k} + 1$ ,  $k \geq 0$ , zove se *Fermatov prost broj*.

**Teorem 4.0.8.** (i) Neka je  $p \geq 3$  prost broj. Ako je moguće elementarno konstruirati pravilni  $p$ -terokut, onda je  $p$  Fermatov prost broj.

(ii) Ako je moguće konstruirati pravilni  $p^a$ -terokut onda je  $p^{a-1}(p - 1)$  potencija od 2, tj. ili je  $p = 2$  ili je pak  $a = 1$  i  $p$  je Fermatov prost broj.

*Dokaz.* (i) Broj  $\varepsilon = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}$  je  $p$ -ti primitivni korijen iz jedinice.

Kako je prema Lemi 4.0.6  $\Phi_p(x)$  ireducibilan i  $\text{st}\Phi_p(x)\varphi(p) = p - 1$ , onda mora biti  $p - 1 = 2^k$ , tj.  $p = 2^k + 1$  za neki  $k \in \mathbb{N}$ . Da bi prirodan broj  $2^k + 1$  bio prost broj mora  $k$  biti potencija od 2, tj.  $k = 2^l$  ( $l \geq 0$ ). U protivnom bi naime bio  $k = ab$ ,  $a \neq 1$  neparan, pa bi  $2^k + 1 = (2^b)^a + 1$  imao netrivialan faktor  $2^b + 1$ . Dakle,  $p$  mora biti Fermatov prost broj.

(ii) Kako je  $\text{st}\Phi_{p^a}(x) = p^{a-1}(p - 1)$  to iz istih razloga mora biti  $p^{a-1}(p - 1) = 2^k$ , odakle slijedi tvrdnja.  $\square$

Oдавде slijedi teorem:

**Teorem 4.0.9.** Ako se pravilni  $n$ -terokut može konstruirati, onda je  $n$  ili potencija od 2 ili je rastav na proste faktore od  $n$  oblika  $2^r p_1 p_2 \dots p_k$ , gdje je  $r \geq 0$ , a  $p_i$  su različiti Fermatovi prosti brojevi.

**Teorem 4.0.10.** (Gauss, 1796.) Pravilni  $n$ -terokut se može konstruirati ravnalom i šestarom ako i samo ako je  $n$  potencija od 2 ili je  $n = 2^r p_1 p_2 \dots p_k$ , gdje je  $r \geq 0$ ,  $k \in \mathbb{N}$ ,  $p_i$  su različiti Fermatovi prosti brojevi.



*Dokaz.* Potrebno je dokazati da se može konstruirati pravilni  $n$ -terokut, gdje je  $n = p$  Fermatov prost broj, tj.  $p = 2^{2^N} + 1$ . Drugim riječima, treba pokazati da je primitivni  $p$ -ti korijen iz jedinice  $\omega$  konstruktibilan.

Svi  $p$ -ti primitivni korijeni iz jedinice su tada  $\omega, \omega^2, \omega^3, \dots, \omega^{p-1}$ . Tada je  $\omega$  korijen jednadžbe  $x^{p-1} + x^{p-2} + \dots + x + 1 = 0$  (a i svi ostali  $p$ -ti primitivni korijeni jedinice). Iz Vièteove formule slijedi da je  $\sum_{k=1}^{p-1} \omega^k = -1$ . Iz definicije  $\omega$  se odmah vidi  $\omega^i = \omega^j \iff i \equiv j \pmod{p}$ . Vidi se da nekongruentnih primitivnih  $p$ -tih korijena iz jedinice ima  $\varphi(p) = p-1$ . Neka je  $g$  neki eksponent nekog primitivnog  $p$ -tog korijena iz jedinice modulo  $p$ . Tada su brojevi  $g, g^2, g^3, \dots, g^{p-1}$  nekongruentni i svaki je  $\not\equiv 0 \pmod{p}$  pa se svi primitivni  $p$ -ti korijeni iz jedinice mogu reprezentirati kao  $\omega^g, \omega^{g^2}, \dots, \omega^{g^{p-1}}$ . Neka je zbog jednostavnosti  $[k] = \omega^k$ . Neka je  $S = \{[g], [g^2], \dots, [g^{p-1}]\}$ .  $S$  je skup svih  $p$ -tih primitivnih korijena jedinice. Svaki član od  $S$  (u navedenom poretku) je  $g$ -ta potencija prethodnog, a prvi je  $g$ -ta potencija posljednjeg. Dakle, sve primitivne  $p$ -te korijene iz jedinice možemo dobiti tako da startamo od bilo kojeg i tada ih redom podižemo na  $g$ -tu potenciju; npr. startamo li od  $[g^j]$ , onda redom dobivamo  $[g^j], [g^{j+1}], [g^{j+2}], \dots, [g^{p-1}], [g], \dots, [g^{j-1}]$ .

Označimo  $S_1 = \{[g], [g^3], [g^5], \dots, [g^{p-2}]\}$ ,  $S_2 = \{[g^2], [g^4], [g^6], \dots, [g^{p-1}]\}$ . Uočimo da svaki od njih dobijemo uzastopnom  $g^2$ -tom potencijom nekog od elemenata, ili pak možemo smatrati da  $S_1$  i  $S_2$  dobijemo tako da uzmemo "svaki drugi" element od  $S$ . Za  $i = 1, 2$ , raspolovimo  $S_i$  u dva skupa  $S_{i,1}, S_{i,2}$  na analogan način. Tako je  $S_{i,1}$  generiran uzastopnim potenciranjem s  $g^4$  prvog elementa od  $S_i$  (ili uzimajući "svaki drugi" element od  $S_i$  startajući s prvim elementom), a  $S_{i,2}$  uzastopnim potenciranjem sa  $g^4$  počev s drugim elementom od  $S_i$ .

Sada nastavimo raspolavljanje skupova dok ne dođemo do jednočlanih skupova. Opišimo taj proces induktivno:  $m$ -skupom ćemo zvati skup dobiven iz  $m$  raspolavljanja, pa će takav skup imati  $m$  indeksa:  $S$  je 0-skup,  $S_1$  i  $S_2$  su 1-skupovi,  $S_{1,1}, S_{1,2}, S_{2,1}, S_{2,2}$  su 2-skupovi itd. Svaki  $m$ -skup je generiran potenciranjem  $g^{2^m}$ -tom potencijom nekog elementa i svaki takav skup sadrži  $\frac{p-1}{2^m}$  elemenata. Svaki  $m$ -skup  $S_{i_1, i_2, \dots, i_m}$  daje dva  $(m+1)$ -skupa  $S_{i_1, i_2, \dots, i_m, 1}$  i  $S_{i_1, i_2, \dots, i_m, 2}$ . Prvi je generiran sukcesivnim potenciranjem  $g^{(2^{m+1})}$ -tim potenciranjem prvog elementa, a drugi tim istim potenciranjem drugog elementa od  $S_{i_1, i_2, \dots, i_m}$ . Konačni efekt je opet uzimanje svakog drugog elementa. Takva dva dobivena  $(m+1)$ -skupa zvat ćemo **komplementarni**.

Uočimo da je ovdje važno da je  $p-1$  potencija od 2. Kad  $p-1$  nebi bilo potencija od 2, onda opetovana podjela na dva jednaka skupa nebi bila moguća, a niti bi tada skup mogao biti dobiven sukcesivnim potenciranjem sa  $g^{2^m}$ . No, u našem slučaju, nakon  $m = 2^N$  podjela, svaki skup sadrži jedan jedini element i to neki primitivni  $p$ -ti korijen iz jedinice.

Nazovimo sumu elemenata skupa **periodom**, tj.  **$m$ -periodom** ako se radio i periodu nekog  $m$ -skupa. Dva perioda su **komplementarna** ako su periodi komplementarnih skupova. Stoga svaki  $m$ -period je suma nekih  $\frac{p-1}{2^m}$  primitivnih  $p$ -tih korijena iz jedinice i posebno za  $m = 2^N$ , svaki takav  $m$ -period je točno jedan takav primitivni  $p$ -ti korijen jedinice. Teorem

će biti dokazan ako pokažemo da je za svako  $0 \leq m \leq 2^N$ , svaki  $m$ -period konstruktibilan. To ćemo pokazati indukcijom po  $m$ . Srž postupka je da će  $(m + 1)$ -period biti korijen kvadratne jednadžbe čiji koeficijenti su linearne kombinacije  $m$ -perioda (čiji korijeni će biti komplementarni periodi).

Podsjetimo se da vrijedi  $x^2 - Ax + B = 0$  ako je  $A = x_1 + x_2$  i  $B = x_1x_2$  gdje su  $x_1, x_2$  korijeni te jednadžbe. Ako su  $A$  i  $B$  konstruktibilni, onda su i  $x_1$  i  $x_2$  konstruktibilni.

Dokažimo dakle da su svi  $m$ -periodi konstruktibilni,  $0 \leq m \leq 2^N$ . Za  $m = 0$ , jedini 0-period je suma svih primitivnih  $p$ -tih korijena, a ta suma jednaka je  $-1$ , što je konstruktibilan broj. Pretpostavimo da su svi do  $(m - 1)$ -perioda konstruktibilni. Neka je  $\alpha$   $m$ -period, a  $\beta$  njemu komplementarni  $m$ -period. Dokažimo da su  $\alpha + \beta$  i  $\alpha\beta$  konstruktibilni. Kako je  $\alpha + \beta$  točno jedan od  $(m - 1)$ -perioda, slijedi da je zbog induktivne pretpostavke taj konstruktibilan. Konstruktibilnost  $\alpha\beta$  će slijediti iz sljedeće tvrdnje.

**TVRDNJA.**  $\alpha\beta$  se može izraziti kao linearna kombinacija s nenegativnim cijelim koeficijentima svih  $m$ -perioda,  $1 \leq m \leq 2^N - 1$ . U toj linearnoj kombinaciji komplementarni periodi imaju iste koeficijente. Za  $m = 2^N$ ,  $\alpha\beta = 1$ .

**Dokaz Tvrdnje.**  $\alpha$  i  $\beta$  su sume elemenata u dva komplementarna  $m$ -skupa  $S'$  i  $S''$ . Ta dva  $m$ -skupa su dobivena iz jednog  $(m - 1)$ -skupa, a generirana su uzastopnim potenciranjem sa  $g^{(2^{m-1})}$  nekog elementa  $\omega^k$ . Stavimo li  $h = g^{(2^{m-1})}$  i  $f = 1 + \frac{p-1}{2^{m-1}}$ , onda je taj  $(m - 1)$ -skup  $[k], [kh], [kh^2], \dots, [kh^{f-2}]$ . Daljnjim potenciranjem od  $h$  ne dobivamo ništa novo, jer je

$$h^{f-1} = \left(g^{(2^{m-1})}\right)^{\frac{p-1}{2^{m-1}}} \equiv g^{p-1} \equiv 1 \pmod{p}$$

(tu smo koristili Fermatov teorem). Stoga je

$$\alpha = [k] + [kh^2] + \dots + [kh^{f-3}], \quad \beta = [kh] + [kh^3] + \dots + [kh^{f-2}].$$

Za  $m = 2^N$ ,  $h = g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ , pa je  $\alpha\beta = \omega^k \omega^{-k} = 1$ . Za  $m < 2^N$ , grupiramo članove ovako (podsjetimo  $[kh^i][kh^j] = [kh^i + kh^j]$ , jer  $[t]$  znači  $\omega^t$ ):

$$\begin{aligned} \alpha\beta &= [k + kh] + [kh^2 + kh^3] + \dots + [kh^{f-3} + kh^{f-2}] + \\ &+ [k + kh^3] + [kh^2 + kh^5] + \dots + [kh^{f-3} + kh] + \\ &\vdots \\ &+ [k + kh^{f-4}] + [kh^2 + kh^{f-2}] + \dots + [kh^{f-3} + kh^{f-6}] + \\ &+ [k + kh^{f-2}] + [kh^2 + kh] + \dots + [kh^{f-3} + kh^{f-4}]. \end{aligned}$$

Svaki redak je suma generirana potenciranjem sa  $h^2$  nekog od elemenata. Nadalje, nijedan od eksponenata nije kongurentan 0 modulo  $p$ . Zaista, dovoljno je pogledati prvi stupac.

Pretpostavimo da je  $k + kh^{2j+1} \equiv 0 \pmod{p}$  gdje je  $1 \leq 2j+1 \leq f-2$ . Tada je  $h^{2j+1} \equiv -1 \pmod{p} \Rightarrow h^{4j+2} \equiv 1 \pmod{p} \Rightarrow g^{(2^{m-1})(4j+2)} \equiv 1 \pmod{p}$ , pa kako je  $g$  primitivni korijen modulo  $p$ , to mora  $p-1 \mid (2^{m-1})(4j+2)$ . No,

$$2 \leq 4j+2 \leq 2f-4 = \frac{p-1}{2^{m-2}} - 2 \Rightarrow (2^{m-1})(4j+2) \leq 2(p-1) - 2^m < 2(p-1).$$

Stoga bi bilo  $p-1 = 2^{m-1}(4j+2) = 2^m(2j+1)$ . No, kako  $p-1$  nema neparnih faktora, jedini slučaj koji može nastupiti je  $j=0$ , ali bi tada imali  $p-1 = 2^m \leq 2^{2^{m-1}} = \frac{p-1}{2}$ , što je nemoguće. Dakle, svaki redak je neki  $m$ -period, no ne nužno  $\alpha\beta$ . Ukupno ima  $2^m$   $m$ -skupova, svaki s odgovarajućim periodom. Nadalje, prvi i posljednji redak su komplementarni  $m$ -periodi, jer uzmemo li  $h$ -tu potenciju nekog elementa prvog retka dobijemo element posljednjeg retka. Tako npr. uzmemo li  $h$ -tu potenciju prvog elementa prvog retka, dobijemo

$$[k + kh]^h = [kh + kh^2] = [kh^2 + kh],$$

što je drugi element zadnjeg retka. Na isti način se vidi da je svaki  $i$ -ti redak odozgo komplementaran  $i$ -tom retku odozdo. Broj redaka je paran i iznosi  $\frac{f-1}{2}$ , pa se svi reci mogu tako spariti pa se svaki  $m$ -period javlja kao i njegov komplement. Time je tvrdnja dokazana.

Prema tvrdnji  $\alpha\beta$  je suma članova oblika  $a(\gamma + \tilde{\gamma})$ , gdje je  $a \in \mathbb{N}_0$ , a  $\gamma$  i  $\tilde{\gamma}$  komplementarni  $m$ -periodi. Kako su  $\gamma$  i  $\tilde{\gamma}$  komplementarni, to je  $\gamma + \tilde{\gamma}$  neki  $(m-1)$ -period, pa stoga konstruktibilan prema induktivnoj pretpostavci. Kao suma konstruktibilnih brojeva slijedi da je  $\alpha\beta$  i sam konstruktibilan. Ranije smo već pokazali da je  $\alpha + \beta$  konstruktibilan pa su konačno i  $\alpha$  i  $\beta$  konstruktibilni.  $\square$

# Bibliografija

- [1] A. Bogdanović, *Pogled u povijesni razvoj geometrije do renesanse*, dostupno na: <https://repozitorij.mathos.hr/islandora/object/mathos:554/datastream/PDF/view> (lipanj 2022.)
- [2] F. M. Brückler, *Povijest matematike 1 (izmijenjeno i dopunjeno izdanje)*, dostupno na: <http://www.mathos.unios.hr/images/uploads/714.pdf> (kolovoz 2022.)
- [3] M. Murat, *Predeuklidsko razdoblje grčke matematike*, dostupno na: <https://repozitorij.pmf.unizg.hr/islandora/object/pmf%3A5344/datastream/PDF/view> (srpanj 2022.)
- [4] M. Musa, *Tri klasična problema*, dostupno na: <http://www.mathos.unios.hr/mdjumic/uploads/diplomski/MUS05.pdf> (studeni 2021.)
- [5] D. Palman, *Geometrijske konstrukcije*, Element, Zagreb, 1996.
- [6] B. Pavković, D. Veljan, *Elementarna matematika 1*, Tehnička knjiga, Zagreb, 1992.
- [7] I. Smrk, *Starogrčka geometrijska algebra*, dostupno na: <https://repozitorij.pmf.unizg.hr/islandora/object/pmf:8439/datastream/PDF/view> (studeni 2021.)
- [8] S. Škarica, *Kvadratura kruga*, Školska knjiga, Zagreb, 1951.
- [9] E. Vrban, *Konstrukcije ravnalom i šestarom*, dostupno na: <http://www.mathos.unios.hr/mdjumic/uploads/diplomski/VRB01.pdf> (studeni 2021.)
- [10] Š. Znam, L. Bukovský, M. Hejný, J. Hvorecký, B. Riečan, *Pogled u povijest matematike*, Tehnička knjiga, Zagreb, 1989.

# Sažetak

U ovom diplomskom radu raspravljali smo o konstruktibilnosti u planimetriji. U prvom poglavlju prikazali smo euklidske konstrukcije jednobridnim ravnalom i šestarom. U drugom poglavlju, bavili smo se algebarskim metodama konstrukcija i proširenjem polja racionalnih brojeva jer se konstrukcije ravnalom i šestarom mogu povezati s tipom proširenja polja racionalnih brojeva, koje sadrži korijene odgovarajućih polinoma. Kroz nekoliko teorema smo pokazali da se ne mogu svi geometrijski objekti dobiti konstrukcijama ravnalom i šestarom. Treće poglavlje bilo je o trima klasičnim problemima, kroz tri podpoglavlja smo opisali kako su oni nastali, naveli smo neke od pokušaja njihovog rješavanja i dokazali nemogućnost konstrukcije uporabom samo ravnala i šestara. Na kraju, u četvrtom poglavlju, kroz nekoliko teorema dokazali smo konstruktibilnost pravilnih mnogokuta.

# Summary

In this master's thesis we shall analyse the issue of constructibility pertaining to planimetry. In the first chapter we will display euclidean constructions using a straight edge ruler and a (regular) divider. In the second chapter we examined the algebraic methods of construction and widening of the field of rational numbers since constructions derived from the utilisation of a ruler and a divider can be associated with the type of expansion of the field of rational numbers that includes the roots of proper polynomials. The employed theorems demonstrate that not all geometric objects can be obtained by constructions using a straight edge ruler and a divider. The third chapter deals with the classical problems whose emergence is discussed in three subheadings, and some attempts at their solution are presented as well, and we demonstrated the impossibility of their construction by using solely a ruler and a divider. Finally, in the fourth chapter we employ certain theorems in order to prove the constructibility of regular polygons.

# Životopis

Rođena 1.8.1994. u Zagrebu kao Glorija Čavar. Osnovnu školu kao i osnovnu glazbenu školu te gimnaziju završila sam u Vrbovcu gdje živim čitav svoj život. Kroz čitavo osnovnoškolsko i srednješkolosko obrazovanje pratio me ples u Vrbovečkim mažoretkinjama s kojima sam obišla mnogo europskih gradova. Godine 2013. upisujem Prometni fakultet Sveučilišta u Zagrebu, smjer Inteligentni transportni sustavi i logistika, od kojeg odustajem već sredinom prvog semestra shvaćajući da to nije moj put. Do ponovnog upisa radim studentske poslove i pripremam se za studij matematike, smjer nastavnički, na Prirodoslovno - matematičkom fakultetu Sveučilišta u Zagrebu kojeg upisujem u srpnju sljedeće godine. Preddiplomski studij završavam 2018. godine te iste godine upisujem diplomski sveučilišni studij Matematika, smjer nastavnički. Paralelno sa diplomskim studijem radim u Osnovnoj školi Špansko Oranice u Zagrebu, a zatim u Osnovnoj školi Marije Jurić Zagorke Vrbovec (osnovnoj školi koju sam i sama pohađala) gdje odlučujem i ostati. 2021. godine u srpnju se udajem i postajem gospođa Filipović, a 16. travnja 2022. godine moj život mijenja se iz temelja jer postajem majka jedne predivne djevojčice imena Lora.