

# Primitivni tetraedri u trodimenzionalnoj cjelobrojnoj rešeci

---

**Marin, Nataša**

**Master's thesis / Diplomski rad**

**2015**

*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:217:816990>

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

*Download date / Datum preuzimanja:* **2025-02-27**



*Repository / Repozitorij:*

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



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

Nataša Marin

**PRIMITIVNI TETRAEDRI U**  
**TRODIMENZIONALNOJ**  
**CJELOBROJNOJ REŠECI**

Diplomski rad

Voditelj rada:  
prof. dr. sc. Juraj Šiftar

Zagreb, srpanj 2015.

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. \_\_\_\_\_

# Sadržaj

<b>Sadržaj</b>	<b>iii</b>
<b>Uvod</b>	<b>1</b>
<b>1 Osnovne definicije</b>	<b>2</b>
<b>2 Unimodularna preslikavanja</b>	<b>7</b>
<b>3 Primitivni poligoni u rešeci <math>\mathbb{Z}^2</math></b>	<b>11</b>
<b>4 Primitivni tetraedri u rešeci <math>\mathbb{Z}^3</math></b>	<b>22</b>
<b>Bibliografija</b>	<b>32</b>

# Uvod

Primitivni politop u  $n$ -dimenzionalnom euklidskom prostoru  $E^n$  je politop čiji vrhovi pripadaju cjelobrojnoj rešeci  $\mathbb{Z}^n$ , ali nema drugih točaka rešetke u unutrašnjosti ili na rubu.

U radu su prikazani neki rezultati o primitivnim tetraedrima u rešeci  $\mathbb{Z}^3$ , a posebno prebrojavanje klasa ekvivalencije primitivnih tetraedara zadanog volumena.

Osim toga, u radu je pokazano da se rezultati koji vrijede u trodimenzionalnoj rešeci bitno razlikuju od ravninskog slučaja. Primitivan politop u rešeci  $\mathbb{Z}^2$  ima najviše 4 vrha pa iz Pickovog teorema slijedi da to može biti ili trokut površine  $\frac{1}{2}$  ili paralelogram površine 1. Dakle, površina primitivnih politopa u  $\mathbb{Z}^2$  je ograničena. Za volumen primitivnih politopa u  $\mathbb{Z}^3$  ne postoji gornja granica pa stoga ne možemo poopćiti Pickov teorem.

Bitnu ulogu u radu ima unimodularno preslikavanje. U ravnini vrijedi da su svaka dva primitivna trokuta unimodularno ekvivalentna, ali u tri dimenzije odgovarajuća tvrdnja za tetraedre ne vrijedi. No, za dani volumen primitivnog tetraedra možemo izračunati broj klasa ekvivalencije.

# Poglavlje 1

## Osnovne definicije

Promatrat ćemo neke posebne skupove točaka u euklidskom prostoru  $E^n$ , dakle realnom unitarnom prostoru  $\mathbb{R}^n$  sa standardnom metrikom.

Podskup  $\mathbb{Z}^n \subseteq \mathbb{R}^n$  nazivamo cjelobrojna rešetka u  $\mathbb{R}^n$ . Algebarski, to je modul nad prstenom  $\mathbb{Z}$  cijelih brojeva.

**Definicija 1.1.** *Neka je  $m \in \mathbb{N}$  proizvoljan prirodan broj i neka su  $x_1, \dots, x_m \in \mathbb{R}^n$ . Linearnu kombinaciju  $\sum_{i=1}^m \lambda_i x_i = \lambda_1 x_1 + \dots + \lambda_m x_m$  gdje su  $\lambda_1, \dots, \lambda_m \geq 0$  i  $\sum_{i=1}^m \lambda_i = 1$  zovemo konveksna kombinacija točaka  $x_1, \dots, x_m$ .*

Podsjetimo da se podskup  $K$  euklidskog prostora naziva konveksnim skupom ako je za svake dvije točke  $v_1, v_2 \in K$  cijeli segment  $[v_1, v_2] = \{\lambda v_1 + (1 - \lambda) v_2 : \lambda \in [0, 1]\}$  sadržan u  $K$ . Presjek bilo koje familije konveksnih skupova također je konveksan skup.

Ako je  $S$  bilo koji podskup euklidskog prostora, skup svih konveksnih kombinacija točaka iz  $S$  naziva se konveksna ljuska skupa  $S$  i označava se s  $\text{conv}(S)$ . Konveksna ljuska je najmanji konveksni podskup koji sadrži  $S$ , to jest to je presjek svih konveksnih podskupova prostora  $\mathbb{R}^n$  koji sadrže  $S$ .

**Definicija 1.2.** *Neka je  $S = \{v_1, \dots, v_m\} \subseteq \mathbb{R}^n$  konačan skup. Skup*

$$P = \text{conv}(S) = \left\{ \lambda_1 v_1 + \dots + \lambda_m v_m : v_1, \dots, v_m \in S, \lambda_1, \dots, \lambda_m \geq 0, \sum_{i=1}^m \lambda_i = 1 \right\}$$

*zovemo politop razapet točkama  $v_1, \dots, v_m$ .*

**Napomena.** *U skladu s ovom definicijom, promatrat ćemo samo konveksne politope.*

**Definicija 1.3.** *Točka  $v$  politopa  $P$  je vrh tog politopa ako se ne može prikazati kao konveksna kombinacija preostalih točaka skupa  $P$ .*

U našem razmatranju politopa u rešetkama  $\mathbb{Z}^2$  i  $\mathbb{Z}^3$  možemo bez gubitka općenitosti pretpostaviti da je skup točaka koje razapinju politop upravo skup njegovih vrhova. Zato ćemo daljnje definicije iskazati uzimajući tu pretpostavku.

Točka  $v = \lambda_1 v_1 + \dots + \lambda_m v_m$  nalazi se na rubu politopa  $P$  ako postoji barem jedan  $i \in \{1, \dots, m\}$  takav da je  $\lambda_i = 0$ , tj.

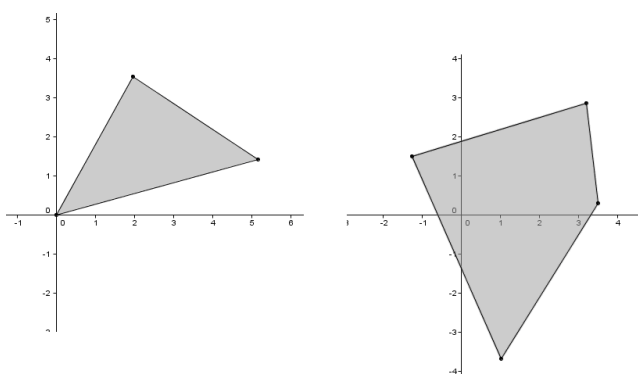
$$\partial P = \left\{ \lambda_1 v_1 + \dots + \lambda_m v_m : v_1, \dots, v_m \in \mathbb{Z}^n, \lambda_1, \dots, \lambda_m \geq 0, \sum_{i=1}^m \lambda_i = 1, \lambda_i = 0 \text{ za neko } i \in \{1, \dots, m\} \right\}$$

Točka  $v = \lambda_1 v_1 + \dots + \lambda_m v_m$  nalazi se u unutrašnjosti politopa  $P$  ako je  $\lambda_i > 0$  za svako  $i \in \{1, \dots, m\}$ . Drugim riječima,

$$\text{int}(P) = \left\{ \lambda_1 v_1 + \dots + \lambda_m v_m : v_1, \dots, v_m \in \mathbb{Z}^n, \lambda_1, \dots, \lambda_m > 0, \sum_{i=1}^m \lambda_i = 1 \right\}$$

**Definicija 1.4.** *Za politop  $P = \left\{ \lambda_1 v_1 + \dots + \lambda_m v_m : v_1, \dots, v_m \in \mathbb{Z}^n, \lambda_1, \dots, \lambda_m \geq 0, \sum_{i=1}^m \lambda_i = 1 \right\}$  kažemo da se nalazi u cjelobrojnoj rešetci. Takav politop je primitivan ako osim vrhova  $v_1, \dots, v_m$  ne sadrži niti jednu drugu točku iz  $\mathbb{Z}^n$  niti na rubu niti u unutrašnjosti.*

**Primjer 1.1.** *Politopi razapeti s tri i četiri točke u  $\mathbb{R}^2$ .*



Slika 1.1: Primjeri politopa

**Teorem 1.1.** *Primitivan politop u  $\mathbb{R}^n$  ima najviše  $2^n$  vrhova.*

*Dokaz.* Pretpostavimo da primitivan politop  $P$  u  $\mathbb{R}^n$  ima više od  $2^n$  vrhova.

S obzirom da svaku koordinatu  $n$ -dimenzionalne točke možemo izabrati na dva načina (paran ili neparan broj) slijedi da postoji točno  $2^n$  različitih mogućnosti za odabir vrha ovisno o parnosti njegovih koordinata.

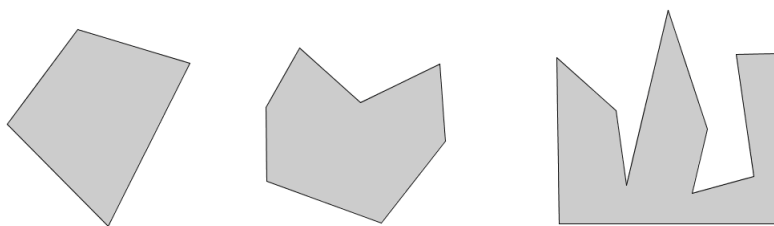
Stoga ako primitivan politop ima više od  $2^n$  vrhova onda postoje vrhovi  $v = \{v_1, \dots, v_n\}$ ,  $w = \{w_1, \dots, w_n\}$  takvi da je  $v_i + w_i \equiv 0 \pmod{2}$  za svako  $i = 1, \dots, n$ .

No politop  $P$  sadrži točku  $\frac{1}{2}(v + w)$  koja nije vrh jer se može prikazati kao linearna kombinacija dva vrha. Vrijedi  $\frac{1}{2}(v + w) \in \mathbb{Z}^n$  pa slijedi da  $P$  nije primitivan što je kontradikcija.

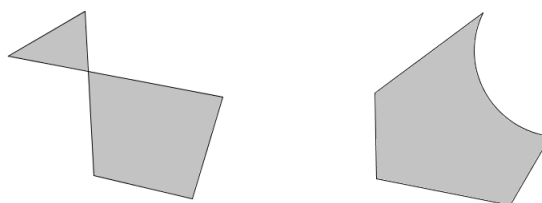
Dakle,  $P$  ima najviše  $2^n$  vrhova. □

**Definicija 1.5.** *Poligon u  $\mathbb{R}^2$  je unija zatvorene izlomljene linije i njene unutrašnjosti.*

**Primjer 1.2.** *Na prvoj slici su prikazani likovi koji su poligoni, a na drugoj nisu poligoni.*



Slika 1.2: Poligoni



Slika 1.3: Nisu poligoni



Podsjetimo da se skup točaka  $\{T_0, T_1, \dots, T_m\}$  prostora  $E^n$  naziva linearno nezavisnim ako je skup vektora  $\{\overrightarrow{T_0T_1}, \dots, \overrightarrow{T_0T_m}\}$  linearno nezavisan u vektorskom prostoru  $\mathbb{R}^n$ .

**Definicija 1.6.** Neka su  $T_0, T_1, \dots, T_m \in \mathbb{R}^n$  linearno nezavisne točke te za svako  $j = 1, \dots, m$  označimo sa  $v_j = \overrightarrow{T_0T_j}$ . Tada skup

$$P = P(v_1, \dots, v_m) = \{T_0 + \lambda_1 v_1 + \dots + \lambda_m v_m : 0 \leq \lambda_1, \dots, \lambda_m \leq 1\}$$

zovemo  $m$ -dimenzionalni paralelotop prostora  $\mathbb{R}^n$  razapet vektorima  $v_1, \dots, v_m$ .

**Napomena 1.1.**  $n$ -dimenzionalni paralelotop  $P \subseteq \mathbb{R}^n$  je konveksan skup jer se može prikazati kao presjek zatvorenih poluprostora, koji su konveksni skupovi, pa je i njihov presjek konveksan.

**Definicija 1.7.** Neka su  $T_0, T_1, \dots, T_m \in \mathbb{R}^n$  linearno nezavisne točke. Konveksno zatvorenje skupa  $\{T_0, T_1, \dots, T_m\}$  zovemo  $m$ -dimenzionalni simpleks razapet vrhovima  $T_0, T_1, \dots, T_m$ .

**Napomena 1.2.**  $n$ -dimenzionalni simpleks  $S \subseteq \mathbb{R}^n$  je konveksan skup jer se može prikazati kao presjek  $n + 1$  zatvorenih poluprostora.

Tetraedar  $T \subseteq \mathbb{R}^3$  je konveksno zatvorenje skupa svojih vrhova, dakle zapravo je 3-simpleks.

(vidi [9], 55 - 59)

**Definicija 1.8.** Preslikavanje  $L : \mathbb{R}^m \rightarrow \mathbb{R}^n$  je linearno ako za proizvoljne vektore  $x, y \in \mathbb{R}^m$  te za skalar  $a \in \mathbb{R}$  vrijedi  $L(x + y) = L(x) + L(y)$  i  $L(ax) = aL(x)$ .

Linearno preslikavanje nam je poznato i kao linearni operator. Svaki linearni operator  $L : \mathbb{R}^m \rightarrow \mathbb{R}^n$  u potpunosti je određen djelovanjem na (bilo kojoj) bazi prostora  $\mathbb{R}^m$ . Iz toga slijedi da postoji matrica  $M \in M_{m,n}(\mathbb{R})$  koja u potpunosti određuje linearni operator  $L$ . Matricu  $M$  zovemo matrica operatora.

**Definicija 1.9.** Preslikavanje  $A : \mathbb{R}^m \rightarrow \mathbb{R}^n$  je afino ako postoje linearno preslikavanje  $L : \mathbb{R}^m \rightarrow \mathbb{R}^n$  i vektor  $b \in \mathbb{R}^n$  takvi da za svako  $x \in \mathbb{R}^m$  vrijedi  $A(x) = L(x) + b$ .

Afino preslikavanje je kompozicija linearnog preslikavanja i translacije. Ako je  $A : \mathbb{R}^m \rightarrow \mathbb{R}^n$  afino, onda postoje matrica operatora  $M$  koja u potpunosti određuje linearno preslikavanje i vektor  $b \in \mathbb{R}^n$  takvi da za svako  $x \in \mathbb{R}^m$  vrijedi  $A(x) = Mx + b$ .

## Poglavlje 2

# Unimodularna preslikavanja

Volumen paralelotopa  $P$  u  $\mathbb{R}^n$  razapetog točkama  $v_1, \dots, v_n \in \mathbb{R}^n$  definiramo s

$$\text{vol}(P) = |\det [v_1 \ v_2 \ \dots \ v_n]|$$

pri čemu je  $[v_1 \ v_2 \ \dots \ v_n]$  kvadratna matrica reda  $n$  čije stupce čine  $n$ -torke koordinata vrhova paralelotopa.

Ova definicija volumena preko determinante proizlazi iz toga što se pokazuje da je determinanta jedinstvena funkcija s  $\mathbb{R}^n$  u  $\mathbb{R}$  koja ispunjava uobičajena svojstva volumena u euklidskom prostoru.

Volumen simpleksa jednak je  $\frac{1}{n!}$  volumena pripadnog paralelotopa jer se svaki  $n$ -dimenzionalni paralelotop može rastaviti na  $\frac{1}{n!}$  simpleksa.

(vidi [9], 100 - 108)

Ako je  $g : \mathbb{R}^n \rightarrow \mathbb{R}^n$ ,  $g(u) = Mu$  linearno preslikavanje određeno matricom  $M \in M_n(\mathbb{R})$  tada vrijedi

$$\text{vol}(g(P)) = |\det M| \cdot \text{vol}(P) \tag{2.1}$$

Naime, primjenom Binet - Cauchyjevog teorema dobivamo

$$\begin{aligned} \text{vol}(g(P)) &= |\det [Mv_1 \ Mv_2 \ \dots \ Mv_n]| = |\det (M \cdot [v_1 \ v_2 \ \dots \ v_n])| = \\ &= |\det M| \cdot |\det [v_1 \ v_2 \ \dots \ v_n]| = |\det M| \cdot \text{vol}(P) \end{aligned}$$

Volumen paralelotopa  $P$  bit će jednak volumenu njegove slike pod djelovanjem preslikavanja  $g$  ako i samo ako vrijedi  $\det M = \pm 1$ , tj.

$$\text{vol}(P) = \text{vol}(g(P)) \iff \det M = \pm 1 \tag{2.2}$$

**Definicija 2.1.** Preslikavanje  $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$  je unimodularno ako vrijedi

- (u1)  $f$  je afino
- (u2)  $f$  čuva volumen
- (u3)  $f(\mathbb{Z}^n) \subseteq \mathbb{Z}^n$

**Napomena 2.1.** Skup  $M_n(\mathbb{Z})$  svih kvadratnih matrica reda  $n$  s cjelobrojnim koeficijentima asocijativan je grupoid s jedinicom s obzirom na množenje matrica. Podskup svih regularnih matrica iz  $M_n(\mathbb{Z})$  kojima se i inverz nalazi u  $M_n(\mathbb{Z})$  očito je grupa.

Nužan i dovoljan uvjet da bi za  $A \in M_n(\mathbb{Z})$  postojala inverzna matrica  $A^{-1}$  koja se također nalazi u  $M_n(\mathbb{Z})$  dobivamo pomoću determinante. Iz  $\det(AA^{-1}) = \det A \cdot \det A^{-1} = 1$  i pretpostavke da  $A$  i  $A^{-1}$  imaju cjelobrojne koeficijente slijedi da je  $\det A = \det A^{-1} \in \{-1, 1\}$ . Uvjet  $\det A \in \{-1, 1\}$  također je dovoljan da bi  $A^{-1}$  imala cjelobrojne koeficijente jer  $A^{-1} = \frac{1}{\det A} \tilde{A} = \pm \tilde{A}$ , a očito je adjunkta  $\tilde{A} \in M_n(\mathbb{Z})$ .

Dakle, skup  $\{A \in M_n(\mathbb{Z}) : \det A \in \{-1, 1\}\}$  je grupa svih cjelobrojnih regularnih matrica čiji su inverzi također cjelobrojne matrice. Tu grupu označavat ćemo s  $GL_n(\mathbb{Z})$ .

**Teorem 2.1.** Neka je  $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$  i neka je  $P$  politop u rešeci  $\mathbb{Z}^n$ . Tada vrijedi

- (i)  $f$  je unimodularno ako i samo ako je  $f(u) = Mu + v$  gdje su  $v \in \mathbb{Z}^n$  i  $M \in GL_n(\mathbb{Z})$ , tj.  $M$  je cjelobrojna  $n \times n$  matrica i  $\det(M) = \pm 1$
- (ii) ako je  $f$  unimodularno onda je  $f$  invertibilno i  $f^{-1}$  je unimodularno
- (iii) ako je  $f$  unimodularno onda su  $f(P)$  i  $f^{-1}(P)$  politopi u rešeci. Osim toga,  $f$  preslikava točke iz unutrašnjosti od  $P$  u unutrašnjost od  $f(P)$  i vrhove od  $P$  u vrhove od  $f(P)$
- (iv) ako je  $P$  primitivan politop onda su i  $f(P)$  i  $f^{-1}(P)$  primitivni

*Dokaz.* (i) Ako je  $f$  afino slijedi  $f(u) = Mu + v$  gdje su  $u, v \in \mathbb{R}^n$  i  $M \in M_n(\mathbb{R})$ .

Obratno, ako je  $f(u) = Mu + v$  onda je  $f$  afino jer je vektor  $v$  translacija, a preslikavanje  $u \mapsto Mu$ ,  $M \in M_n(\mathbb{R})$  je linearno.

Iz definicije preslikavanja  $f$  slijedi  $f(\mathbb{Z}^n) \subseteq \mathbb{Z}^n$  ako i samo ako je  $v \in \mathbb{Z}^n$  i  $M \in M_n(\mathbb{Z})$ . Neka je  $S \subseteq \mathbb{R}^n$  izmjeriv skup i  $g : \mathbb{R}^n \rightarrow \mathbb{R}^n$ ,  $g(u) = Mu$  linearno preslikavanje određeno matricom  $M \in M_n(\mathbb{R})$ .

Iz formule (2.2) te zato što translacija ne utječe na volumen slijedi da preslikavanje  $f$  čuva volumen ako i samo ako je  $\det M = \pm 1$ .

(ii) Neka je  $f$  unimodularno,  $f(u) = Mu + v$ ,  $v \in \mathbb{Z}^n$ ,  $M \in GL_n(\mathbb{Z})$ ,  $\det M = \pm 1$ . Preslikavanje  $f$  je invertibilno jer je matrica  $M$  regularna i vrijedi  $f^{-1}(u) = M^{-1}u - w$ , gdje je  $w = M^{-1}v$ . Dakle,  $w \in \mathbb{Z}^n$ ,  $\det M^{-1} = \pm 1$ ,  $M^{-1} \in GL_n(\mathbb{Z})$  pa je  $f^{-1}$  unimodularno.

(iii) Neka je  $P = \left\{ \lambda_1 v_1 + \dots + \lambda_m v_m : v_1, \dots, v_m \in \mathbb{Z}^n, \lambda_1, \dots, \lambda_m \geq 0, \sum_{i=1}^m \lambda_i = 1 \right\}$  politop u rešeci  $\mathbb{Z}^n$  i neka je  $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$  unimodularno preslikavanje,  $f(u) = Mu + v$ ,  $v \in \mathbb{Z}^n$ ,  $M \in GL_n(\mathbb{Z}^n)$ ,  $\det M = \pm 1$ .

Tada je  $f(\lambda_1 v_1 + \dots + \lambda_m v_m) = M(\lambda_1 v_1 + \dots + \lambda_m v_m) + v = \lambda_1(Mv_1) + \dots + \lambda_m(Mv_m) + v$ . Označimo s  $s_i = Mv_i \in \mathbb{Z}^n$ .

Tada je  $f(P)$  politop  $\left\{ \lambda_1 s_1 + \dots + \lambda_m s_m : s_1, \dots, s_m \in \mathbb{Z}^n, \lambda_1, \dots, \lambda_m \geq 0, \sum_{i=1}^m \lambda_i = 1 \right\}$  transliran za vektor  $v \in \mathbb{Z}^n$ . Dakle,  $f(P)$  je politop u rešeci.

Točke  $v_1, \dots, v_m \in \mathbb{Z}^n$  su vrhovi politopa  $P$ .

Vrijedi  $f(v_i) = Mv_i + v = s_i + v$  za svako  $i = 1, \dots, m$ .

Dakle,  $f$  preslikava vrhove politopa  $P$  u vrhove politopa  $f(P)$ .

Neka je  $z \in \mathbb{Z}^n$  točka iz unutrašnjosti politopa  $P$ . Tada se  $z$  može prikazati kao linearna kombinacija točaka  $v_1, \dots, v_m$ , tj.  $z = \lambda_1 v_1 + \dots + \lambda_m v_m$  pri čemu je  $\sum_{i=1}^m \lambda_i = 1$  i  $\lambda_i > 0$  za svako  $i = 1, \dots, m$ . Vrijedi  $f(z) = \lambda_1(Mv_1) + \dots + \lambda_m(Mv_m) + v$  pri čemu je  $\sum_{i=1}^m \lambda_i = 1$  i  $\lambda_i > 0$  za svako  $i = 1, \dots, m$ , tj.  $f(z)$  se nalazi u unutrašnjosti politopa  $f(P)$ .

Ako je  $f$  unimodularno preslikavanje onda iz (ii) slijedi da je i  $f^{-1}$  unimodularno pa stoga vrijedi tvrdnja za  $f^{-1}$ .

(iv) Neka je  $P = \left\{ \lambda_1 v_1 + \dots + \lambda_m v_m : v_1, \dots, v_m \in \mathbb{Z}^n, \lambda_1, \dots, \lambda_m \geq 0, \sum_{i=1}^m \lambda_i = 1 \right\}$  primitivan politop i neka je  $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$  unimodularno preslikavanje,  $f(u) = Mu + v$ ,  $v \in \mathbb{Z}^n$ ,  $M \in GL_n(\mathbb{Z})$ ,  $\det M = \pm 1$ .

Iz (iii) slijedi da je  $f(P)$  politop i pretpostavimo da nije primitivan. Tada postoji točka iz cjelobrojne rešetke  $f(z) \in f(P)$  koja nije vrh politopa  $f(P)$ , tj.  $f(z) = \lambda_1(Mv_1) + \dots + \lambda_m(Mv_m) + v \in \mathbb{Z}^n$ ,  $0 \leq \lambda_1, \dots, \lambda_m < 1$ ,  $\sum_{i=1}^m \lambda_i = 1$ . Vrijedi  $M \in GL_n(\mathbb{Z}^n)$ ,

$v \in \mathbb{Z}^n$  iz čega slijedi  $z = \lambda_1 v_1 + \dots + \lambda_m v_m \in \mathbb{Z}^n$ ,  $0 \leq \lambda_1, \dots, \lambda_m < 1$ ,  $\sum_{i=1}^m \lambda_i = 1$ . Dakle,  $z \in \mathbb{Z}^n$  je točka politopa  $P$  koja nije vrh, a to je kontradikcija s primitivnošću politopa  $P$ . Slijedi da je  $f(P)$  primitivan politop.

Ako je  $f$  unimodularno preslikavanje, iz (ii) slijedi da je  $f^{-1}$  unimodularno pa je  $f^{-1}(P)$  primitivan politop.

□

**Definicija 2.2.** Politopi  $P_1, P_2 \subseteq \mathbb{R}^n$  su unimodularno ekvivalentni ako postoji unimodularno preslikavanje  $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$  takvo da je  $f(P_1) = P_2$ . Ako su  $P_1$  i  $P_2$  unimodularno ekvivalentni pišemo  $P_1 \cong P_2$ .

**Primjer 2.1.** Neka je  $P_1$  politop razapet točkama  $(3, 1)$ ,  $(-4, 0)$  i  $(-1, 2)$  te neka je  $P_2$  politop razapet točkama  $(28, 5)$ ,  $(-39, -10)$  i  $(-4, -2)$ . Tada su  $P_1$  i  $P_2$  unimodularno ekvivalentni, a unimodularno preslikavanje  $f$  takvo da je  $f(P_1) = P_2$  dano je sa

$$f((v_1, v_2)) = \begin{pmatrix} 9 & 4 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} + \begin{pmatrix} -3 \\ -2 \end{pmatrix}$$

Pokažimo da je  $\cong$  relacija ekvivalencije.

- Refleksivnost

Neka je  $P \subseteq \mathbb{R}^n$  politop. Identiteta  $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ ,  $f(u) = u$  je unimodularno preslikavanje pa je  $P \cong P$ .

- Simetričnost

Neka su  $P_1, P_2 \subseteq \mathbb{R}^n$  politopi takvi da je  $P_1 \cong P_2$ . Tada postoji unimodularno preslikavanje  $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$  takvo da je  $f(P_1) = P_2$ . No,  $f^{-1}$  je također unimodularno i vrijedi  $f^{-1}(P_2) = P_1$ . Dakle,  $P_2 \cong P_1$ .

- Tranzitivnost

Neka su  $P_1, P_2, P_3 \subseteq \mathbb{R}^n$  politopi takvi da je  $P_1 \cong P_2$  i  $P_2 \cong P_3$ . Tada postoje unimodularna preslikavanja  $f, g : \mathbb{R}^n \rightarrow \mathbb{R}^n$  takva da je  $f(P_1) = P_2$  i  $g(P_2) = P_3$ . Kompozicija unimodularnih preslikavanja je unimodularno preslikavanje pa vrijedi  $g(f(P_1)) = g(P_2) = P_3$ . Dakle,  $P_1 \cong P_3$ .

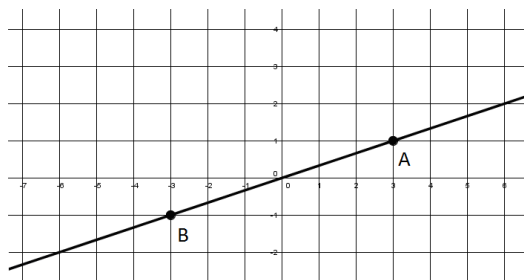
## Poglavlje 3

### Primitivni poligoni u rešeci $\mathbb{Z}^2$

U ovome poglavlju koristeći vidljive točke u rešeci pokazujemo da su svaka dva primitivna trokuta unimodularno ekvivalentna. Pomoću tog rezultata dokazat ćemo Pickov teorem koji nam daje vrlo elegantan način za izračunati površinu poligona u rešeci  $\mathbb{Z}^2$ . Iz teorema 1.1 slijedi da primitivan politop u ravnini može imati najviše 4 vrha, a iz Pickovog teorema zaključujemo da je primitivan politop u rešeci  $\mathbb{Z}^2$  ili trokut površine  $\frac{1}{2}$  ili paralelogram površine 1. Nakon toga slijede još neki interesantni rezultati dobiveni prebrojavanjem točaka rešetke koje poligon sadrži na rubu ili u unutrašnjosti.

**Definicija 3.1.** *Pravac u cjelobrojnoj rešeci je pravac koji prolazi kroz barem dvije točke rešetke. Segment u cjelobrojnoj rešeci je segment kojemu su početna i krajnja točka točke rešetke.*

**Definicija 3.2.** *Neka je dan pravac u cjelobrojnoj rešeci koji prolazi kroz ishodište. Točke rešetke koje se nalaze na danom pravcu i čija udaljenost od ishodišta je minimalna zovemo vidljive točke.*



Slika 3.1: Točke A i B su vidljive

U dokazima nekoliko sljedećih teorema koristit ćemo poznatu tvrdnju iz elementarne teorije brojeva.

**Lema 3.1.** *Neka su  $m, n \in \mathbb{Z}$  i neka je  $g = m(m, n)$ . Tada postoje  $s, t \in \mathbb{Z}$  takvi da je  $g = sm + nt$ . Posebno, ako su  $m$  i  $n$  relativno prosti tada vrijedi  $sm + nt = 1$ .*

**Teorem 3.1.** *Točka rešetke  $T = (m, n) \in \mathbb{Z}^2$  je vidljiva ako i samo ako su  $m$  i  $n$  relativno prosti.*

*Dokaz.* Pretpostavimo da je  $T = (m, n)$  vidljiva točka. Iz definicije vidljive točke slijedi da segment  $[0, T]$  ne sadrži niti jednu drugu točku rešetke.

Pretpostavimo da  $m$  i  $n$  nisu relativno prosti i neka je  $k > 1$  njihova mjera. Slijedi  $\frac{m}{k}, \frac{n}{k} \in \mathbb{Z}$ . Jednadžba pravca koji sadrži segment  $[0, T]$  jednaka je  $y = \frac{n}{m}x$  pa slijedi da segment  $[0, T]$  sadrži točku  $(\frac{m}{k}, \frac{n}{k})$  koja je bliže ishodištu od točke  $(m, n)$  što je kontradikcija s time da je  $(m, n)$  vidljiva točka. Dakle,  $k = 1$ , tj.  $m$  i  $n$  su relativno prosti.

Obratno, pretpostavimo da su  $m$  i  $n$  relativno prosti. Neka je  $T' = (m', n')$  točka rešetke koja se nalazi na segmentu  $[0, T]$  i različita je od ishodišta. Treba pokazati da je  $T = T'$ . Promatramo tri slučaja:

- (i) Neka je  $m' = 0$ . Tada  $[0, T]$  leži na  $y$ -osi pa je  $T = (0, n)$ . No,  $m = 0$  i  $n$  su relativno prosti pa slijedi  $n = 1$ . S obzirom da je točka  $T'$  različita od ishodišta i jer se nalazi na segmentu  $[0, T]$  slijedi  $T = T'$ .
- (ii) Neka je  $n' = 0$ . Tada  $[0, T]$  leži na  $x$ -osi pa je  $T = (m, 0)$ . Opet,  $m$  i  $n = 0$  su relativno prosti pa slijedi  $m = 1$ . S obzirom da je točka  $T'$  različita od ishodišta i jer se nalazi na segmentu  $[0, T]$  slijedi  $T = T'$ .
- (iii) Neka su sada  $m', n' \neq 0$ . S obzirom da točke  $T$  i  $T'$  leže na istom pravcu koji prolazi kroz ishodište slijedi  $\frac{n}{m} = \frac{n'}{m'}$  pa je  $nm' = n'm$  iz čega zaključujemo da  $m|m'n$ . Jer su  $m$  i  $n$  relativno prosti te  $m|m'n$  slijedi  $m|m'$ . Na isti način dobijemo da  $n|n'$ . Točka  $T$  se nalazi na segmentu  $[0, T]$  pa mora vrijediti  $|m'| < |m|$  i  $|n'| < |n|$ . Slijedi  $T = T'$ .

□

**Propozicija 3.1.** *Površina primitivnog paralelograma jednaka je 1.*

*Dokaz.* Neka je dan primitivan paralelogram. Translatiramo ga tako da dobijemo paralelogram  $P$  u prvom kvadrantu čiji vrhovi su točke  $(0, 0)$ ,  $A = (m, n)$ ,  $B = (i, j)$  i  $A + B = (m + i, n + j)$ .

$P$  je primitivan pa je točka  $A$  vidljiva. Iz teorema 3.1 slijedi da su  $m$  i  $n$  relativno prosti.



Stoga postoje  $p, q \in \mathbb{Z}$  takvi da je  $mp + nq = 1$ .

Stavimo da je  $M = \begin{pmatrix} p & q \\ -n & m \end{pmatrix} \in M_2(\mathbb{Z})$ .

Definiramo  $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ ,  $f(x) = Mx$ . Vrijedi  $\det M = mp + nq = 1$  pa je  $f$  unimodularno preslikavanje.

$f$  preslikava vrhove paralelograma  $P$  u točke  $(0, 0)$ ,  $(pi + qj, -ni + mj)$ ,  $(1, 0)$  i  $(pi + qj - 1, -ni + mj)$ .

Neka su  $u = pi + qj$ ,  $v = -ni + mj$ . Tada su vrhovi paralelograma  $f(P)$  točke  $(0, 0)$ ,  $(u, v)$ ,  $(1, 0)$ ,  $(u + 1, v)$ .

Ako je  $v = 0$  onda su vrhovi od  $f(P)$  kolinearni pa  $f(P)$  nije paralelogram. Dakle,  $|v| \geq 1$ . Pretpostavimo da je  $|v| > 1$  i da je  $v$  pozitivan. Tada dvije stranice paralelograma  $f(P)$  sijeku pravac  $y = 1$  u točkama  $p_1, p_2 \notin \mathbb{Z}^2$ . Udaljenost točaka  $p_1$  i  $p_2$  jednaka je 1. Osim toga, one leže na pravcu  $y = 1$  pa slijedi da postoji točka rešetke koja se nalazi na pravcu  $y = 1$  i između točaka  $p_1$  i  $p_2$ . No, ta točka rešetke se nalazi u unutrašnjosti paralelograma  $f(P)$  što je kontradikcija s primitivnošću paralelograma  $f(P)$ .

Analognim zaključivanjem dobije se kontradikcija ako pretpostavimo  $|v| > 1$ ,  $v$  negativan (promatramo pravac  $y = -1$ ).

Dakle,  $v = 1$ .

Slijedi da su vrhovi paralelograma  $f(P)$  točke  $(0, 0)$ ,  $(u, 1)$ ,  $(1, 0)$ ,  $(u + 1, 1)$ . Duljina jedne stranice jednaka je 1, isto kao i duljina visine na tu stranicu pa je površina paralelograma  $f(P)$  jednaka 1. Preslikavanje  $f$  je unimodularno pa čuva volumen.

Dakle, površina primitivnog paralelograma  $P$  je 1.

□

**Propozicija 3.2.** Svaka dva primitivna trokuta u rešeci  $\mathbb{Z}^2$  unimodularno su ekvivalentna.

*Dokaz.* Dokazat ćemo da je svaki primitivan trokut unimodularno ekvivalentan trokutu  $T_{0,e_1,e_2}$  čiji su vrhovi točke  $(0, 0)$ ,  $(0, 1)$ ,  $(1, 0)$  i koji je primitivan.

Neka je dan proizvoljan primitivan trokut i neka je  $T$  taj trokut translatican tako da mu se jedan vrh nalazi u ishodištu. Neka su točke  $(0, 0)$ ,  $(s_1, s_2)$ ,  $(t_1, t_2)$  vrhovi trokuta  $T$ .

Neka je  $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ ,  $f(u) = Mu$ ,  $M \in GL_2(\mathbb{R})$  takvo da je  $f((0, 0)) = (0, 0)$ ,  $f((0, 1)) = (s_1, s_2)$ ,  $f((1, 0)) = (t_1, t_2)$ .

Ako stavimo da je  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  tada slijedi  $b = s_1$ ,  $d = s_2$  i  $a = t_1$ ,  $c = t_2$ . Dakle, matrica  $M$

je dana s  $M = \begin{pmatrix} t_1 & s_1 \\ t_2 & s_2 \end{pmatrix}$  i  $\det M = t_1 s_2 - s_1 t_2$ .

No, vektori stupci matrice  $M$  razapinju paralelogram i površina tog paralelograma je jednaka  $\det M$ . Osim toga, taj paralelogram je primitivan pa mu je površina jednaka 1, tj.  $\det M = 1$ . Slijedi da je  $f$  unimodularno preslikavanje.

Dakle, za svaki primitivan trokut  $T$  vrijedi  $T \cong T_{0,e_1,e_2}$  pa zbog toga što je  $\cong$  relacija ekvi-

valencije slijedi da su svaka dva primitivna trokuta unimodularno ekvivalentna.  $\square$

**Teorem 3.2 (Pick).** *Neka je  $P$  poligon u rešeci  $\mathbb{Z}^2$ . Ako  $P$  u unutrašnjosti ima  $I$  točaka iz  $\mathbb{Z}^2$ , te ako  $P$  na rubu ima  $B$  točaka iz  $\mathbb{Z}^2$ , tada je površina poligona  $P$  jednaka*

$$\text{area}(P) = I + \frac{1}{2}B - 1$$

*Dokaz.* Dokaz provodimo indukcijom po broju  $n = I + B$ , tj. po broju točaka rešetke koje poligon  $P$  sadrži.

Baza indukcije:  $n = I + B = 3$

Tada je  $B = 3, I = 0$ , tj.  $P$  je primitivan trokut. No, svaki primitivan trokut unimodularno je ekvivalentan trokutu  $T((0, 0), (1, 0), (0, 1))$  čija je površina jednaka  $\frac{1}{2}$ . Stoga formula vrijedi za  $n = 3$ .

Pretpostavka indukcije: pretpostavimo da formula vrijedi za sve  $B + I < n$  i dokažimo da vrijedi za  $B + I = n$ .

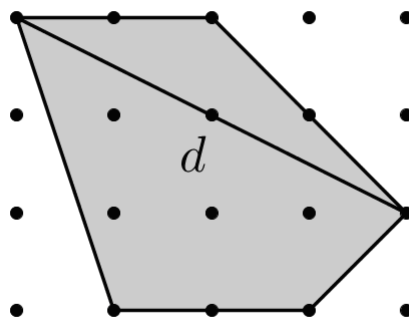
Promatramo sljedeća dva slučaja:

(i)  $B \geq 4$

(ii)  $B = 3, I \geq 1$

Neka je  $B \geq 4$ . Tada  $P$  možemo podijeliti na dva poligona.

Neka je  $d$  dužina koja spaja dva vrha od  $P$  i dijeli ga na poligone  $Q_1$  i  $Q_2$ . Primjer takve podjele prikazan je na sljedećoj slici.



Slika 3.2

Označimo s  $area(Q_j)$  površinu poligona  $Q_j$ , s  $B_j$  broj točaka rešetke na rubu od  $Q_j$  te s  $I_j$  broj točaka rešetke u unutrašnjosti od  $Q_j$ , za  $j = 1, 2$ .

Za  $d$  neka je  $I_d$  broj točaka rešetke na dužini te  $B_d = 2$ .

Za poligone  $Q_j$  vrijedi  $B_j + I_j < n$  pa po pretpostavci indukcije za  $j = 1, 2$  vrijedi

$$area(Q_j) = I_j + \frac{1}{2}B_j - 1$$

Osim toga, vrijedi

$$I = I_1 + I_2 + I_d$$

te

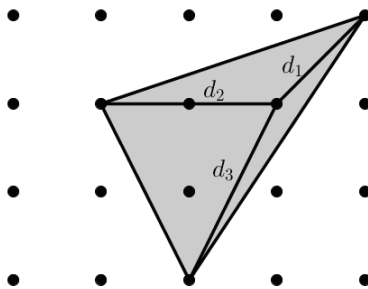
$$B = B_1 + B_2 - 2I_d - 2$$

Dakle,

$$\begin{aligned} area(P) &= area(Q_1) + area(Q_2) = I_1 + I_2 + \frac{1}{2}(B_1 + B_2) - 2 = \\ &= I - I_d + \frac{1}{2}(B + 2I_d + 2) - 2 = I - I_d + \frac{1}{2}B + I_d + 1 - 2 = \\ &= I + \frac{1}{2}B - 1 \end{aligned}$$

pa vrijedi Pickova formula.

Neka je sada  $B = 3$ ,  $I \geq 1$ . Odaberemo jednu točku rešetke iz unutrašnjosti od  $P$  te tu točku spojimo s tri proizvoljna vrha od  $P$ . Na taj način pomoću tri dužine koje označimo s  $d_1, d_2, d_3$  poligon  $P$  podijelimo na poligone  $Q_1, Q_2$  i  $Q_3$ . Primjer takve podjele prikazan je na sljedećoj slici.



Slika 3.3

Ta tri novodobivena poligona sadrže manje točkaca rešetke od  $P$  pa zadovoljavaju pretpostavku indukcije.

Označimo s  $area(Q_j)$  površinu poligona  $Q_j$ , s  $B_j$  broj točkaca rešetke na rubu od  $Q_j$  te s  $I_j$  broj točkaca rešetke u unutrašnjosti od  $Q_j$ ,  $j = 1, 2, 3$ . Za  $d_j$  neka je  $I_{d_j}$  broj točkaca rešetke na dužini te  $B_{d_j} = 2$ ,  $j = 1, 2, 3$ .

Za politope  $Q_j$  vrijedi  $B_j + I_j < n$  pa po pretpostavci indukcije za  $j = 1, 2, 3$  vrijedi

$$area(Q_j) = I_j + \frac{1}{2}B_j - 1$$

Osim toga, vrijedi

$$I = I_1 + I_2 + I_3 + I_{d_1} + I_{d_2} + I_{d_3} + 1$$

te

$$B = B_1 + B_2 + B_3 - 2I_{d_1} - 2I_{d_2} - 2I_{d_3} - 3 - 3$$

Dakle,

$$\begin{aligned} area(P) &= area(Q_1) + area(Q_2) + area(Q_3) = I_1 + I_2 + I_3 + \frac{1}{2}(B_1 + B_2 + B_3) - 3 = \\ &= I - I_{d_1} - I_{d_2} - I_{d_3} - 1 + \frac{1}{2}(B + 2(I_{d_1} + I_{d_2} + I_{d_3}) + 6) - 3 = \\ &= I + \frac{1}{2}B - 1 \end{aligned}$$

□

Neka je  $P$  primitivan politop u  $\mathbb{Z}^2$ . Tada  $P$  može imati najviše 4 vrha, tj.  $P$  je ili trokut ili paralelogram. Iz Pickovog teorema slijedi da je površina primitivnog trokuta jednaka  $\frac{1}{2}$  ( $I = 0$ ,  $B = 3$ ), a površina primitivnog paralelograma je jednaka 1 ( $I = 0$ ,  $B = 4$ ).

**Teorem 3.3** (Scott). *Neka je  $P \subseteq \mathbb{R}^2$  poligon u rešeci koji sadrži  $I \geq 1$  točkaca rešetke u unutrašnjosti, te neka je  $area(P)$  površina tog poligona. Tada vrijedi jedna od sljedeće dvije tvrdnje*

$$(1) P = T((0, 0), (3, 0), (0, 3)) \text{ pri čemu je } I = 1 \text{ te je } area(P) = \frac{9}{2}$$

$$(2) area(P) \leq 2(I + 1)$$

*Dokaz.* Ako je  $I = 1$  i  $P = T((0, 0), (3, 0), (0, 3))$  tada je  $B = 9$  i  $area(P) = \frac{9}{2}$ .

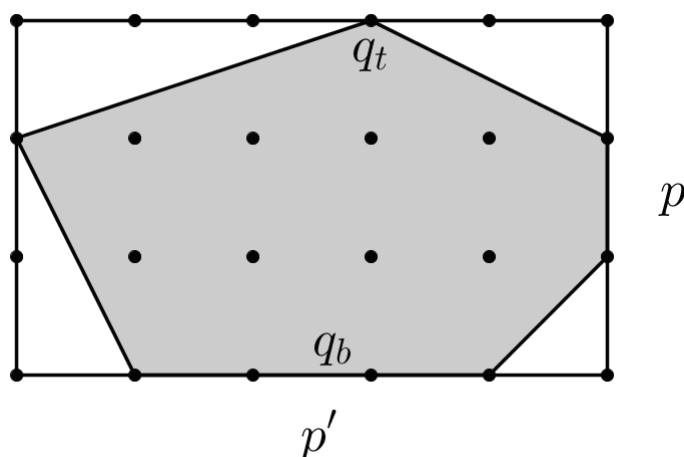
U suprotnom, treba pokazati  $area(P) \leq 2(I + 1)$  za  $I \geq 1$ .

Iz Pickove formule imamo  $I = area(P) - \frac{1}{2}B + 1$  pa je  $area(P) \leq 2(I + 1)$  ekvivalentno s

$B \leq \text{area}(P) + 4$ .

Poligon  $P$  transliramo tako da bude sadržan u pravokutniku s vrhovima  $(0, 0)$ ,  $(p', 0)$ ,  $(0, p)$ ,  $(p', p)$  pri čemu su  $p, p' \in \mathbb{N}$  minimalni.

Zbog  $I \geq 1$  bez smanjenja općenitosti možemo pretpostaviti da je  $2 \leq p \leq p'$ . Primjer takvog poligona sadržanog u pravokutniku prikazan je na sljedećoj slici.



Slika 3.4

Označimo s  $q_b$  duljinu presjeka poligona  $P$  i donje stranice pravokutnika, te s  $q_t$  duljinu presjeka poligona  $P$  s gornjom stranicom pravokutnika. Tada vrijedi

$$B \leq q_b + q_t + 2p \quad (3.1)$$

$$\text{area}(P) \geq \frac{p(q_b + q_t)}{2} \quad (3.2)$$

Ako u Pickovoj formuli  $\text{area}(P) = I + \frac{1}{2}B - 1$  uzmemo u obzir  $I \geq 1$  dobivamo  $\text{area}(P) \geq \frac{1}{2}B$ .

Promatramo sljedeća četiri slučaja:

(i)  $p = q_b + q_t = 3$

Tada iz (3.1) slijedi  $B \leq 9$ .

Ako je  $B \leq 8$  tada je  $\frac{1}{2}B \leq 4$  i znamo da vrijedi  $\frac{1}{2}B \leq \text{area}(P)$  pa zbrajanjem te dvije nejednakosti dobivamo  $B \leq \text{area}(P) + 4$ .

Pretpostavimo sada da je  $B = 9$ . Tada je  $\text{area}(P) \geq \frac{9}{2}$ . Ako je  $\text{area}(P) \geq 5$  onda odmah slijedi  $B \leq \text{area}(P) + 4$ . Ako je  $\text{area}(P) = \frac{9}{2}$  onda slijedi da je  $I = 1$ .

Do na unimodularno preslikavanje, jedini poligon koji zadovoljava  $B = 9$ ,  $I = 1$ ,  $p = q_b + q_t = 3$  je  $T((0, 0), (3, 0), (0, 3))$ .

- (ii)  $p = 2$  ili  $q_b + q_t \geq 4$   
Iz (3.1) i (3.2) slijedi

$$\begin{aligned} 2B - 2\text{area}(P) &\leq 2q_b + 2q_t + 4p - pq_b - pq_t = \\ &= 2(q_b + q_t - 4) + 8 - p(q_b + q_t - 4) = \\ &= (2 - p)(q_b + q_t - 4) + 8 \end{aligned}$$

Ako je  $p = 2$  onda je  $2B - 2\text{area}(P) \leq 8$  pa vrijedi  $B \leq \text{area}(P) + 4$ .

Ako je  $q_b + q_t \geq 4$  onda je  $(2 - p)(q_b + q_t - 4) \leq 0$  zbog  $p \geq 2$  pa opet vrijedi  $2B - 2\text{area}(P) \leq 8$ , tj.  $B \leq \text{area}(P) + 4$ .

- (iii)  $p = 3$  i  $q_b + q_t \leq 2$   
Iz (3.1) slijedi  $B \leq 8$  pa tvrdnja slijedi kao i u (i).

- (iv)  $p \geq 4$  i  $q_b + q_t \leq 2$   
Izaberemo točke  $P(x_b, 0)$  i  $R(x_t, p)$  koje se nalazi u presjeku poligona i donje, odnosno gornje stranice pravokutnika i to tako da je  $u = |x_b - x_t|$  najmanji mogući.  
Promatramo preslikavanje

$$f : \mathbb{R}^2 \rightarrow \mathbb{R}^2, f((x, y)) = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} (x, y)^T = (x + ky, y), \text{ gdje je } k \in \mathbb{Z}.$$

$f$  je unimodularno preslikavanje.

Slijedi da je površina poligona  $f(P)$  jednaka  $\text{area}(P)$ , te je broj točaka rešetke koje se nalaze na rubu poligona  $f(P)$  jednak  $B$ .

Osim toga,  $f$  ne mijenja drugu koordinatu vektora na kojeg djeluje pa sve točke na pravcu  $y = p$  oblika  $(x, p)$  translata u  $(x + kp, p)$ , a one na  $x$ -osi ostanu iste.

Stoga  $q_b + q_t$  nakon djelovanja preslikavanja  $f$  ostane nepromijenjen.

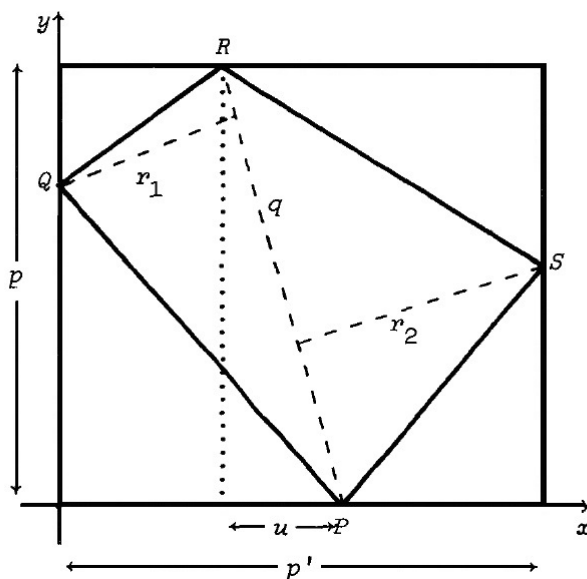
Može se desiti da  $p'$  postane manji od  $p$ , ali u tom slučaju im zamijenimo uloge.

Dakle, možemo pretpostaviti da vrijedi

$$u \leq \frac{p - q_b - q_t}{2} \quad (3.3)$$

(ako ta nejednakost ne vrijedi za poligon  $P$  onda postoji  $k \in \mathbb{Z}$  takav da vrijedi za  $f(P)$ ).

Sada izaberemo točke  $Q$  i  $S$  iz presjeku poligona i lijeve, odnosno desne stranice pravokutnika. Označimo s  $r_1$  visinu iz vrha  $Q$  na stranicu  $\overline{PR}$ , s  $r_2$  visinu iz vrha  $S$  na stranicu  $\overline{PR}$ , te neka je  $q = |PR|$ .



Slika 3.5

Četverokut  $PQRS$  je sadržan u poligonu  $P$  i vrijedi

$$\text{area}(PQRS) = \frac{1}{2}q(r_1 + r_2)$$

Redom koristeći da vrijedi  $q \geq p$ ;  $u = 0 \Rightarrow r_1 + r_2 = p' = p' - u$ ;  $p' \geq p$ ; te (3.3) dobivamo

$$\begin{aligned} \text{area}(P) &\geq \text{area}(PQRS) = \frac{1}{2}q(r_1 + r_2) \geq \frac{1}{2}p(r_1 + r_2) \geq \frac{1}{2}p(p' - u) \geq \\ &\geq \frac{1}{2}p(p - u) \geq \frac{1}{2}p\left(p - \frac{p - q_b - q_t}{2}\right) = \frac{1}{4}p(p + q_b + q_t) \end{aligned}$$

Vrijedi  $4\text{area}(P) \geq p(p + q_b + q_t)$  pa iz toga i iz (3.1) slijedi

$$\begin{aligned} 4(b - \text{area}(P)) &\leq 4(q_b + q_t + p) - p(p + q_b + q_t) = \\ &= p(8 - p) + (q_b + q_t)(4 - p) \leq p(8 - p) \leq 16 \end{aligned}$$

jer je  $(q_b + q_t)(4 - p) \leq 0$  zbog pretpostavke, a  $p(8 - p) \leq 16$  jer je  $p(8 - p)$  konkavna parabola s tjemenom u točki  $(4, 16)$ .

Dakle,  $b \leq \text{area}(P) + 4$  što je i trebalo dokazati.

□

Neka je  $k \in \mathbb{N}$ , neka su  $P$  i  $kP = \{kx : x \in P\}$  poligoni u rešeci  $\mathbb{Z}^2$ , te označimo s

$$L(P) = |P \cap \mathbb{Z}^2|, \quad L(kP) = |kP \cap \mathbb{Z}^2|$$

Iz Pickovog teorema dobivamo

$$I(P) = \text{area}(P) - \frac{1}{2}B(P) + 1, \quad I(kP) = \text{area}(kP) - \frac{1}{2}B(kP) + 1$$

pa slijedi

$$L(P) = \text{area}(P) + \frac{1}{2}B(P) + 1, \quad L(kP) = \text{area}(kP) + \frac{1}{2}B(kP) + 1$$

Pretpostavimo da znamo vrijednosti  $I(P)$  i  $B(P)$  te želimo izračunati  $L(P)$  i  $L(kP)$ .

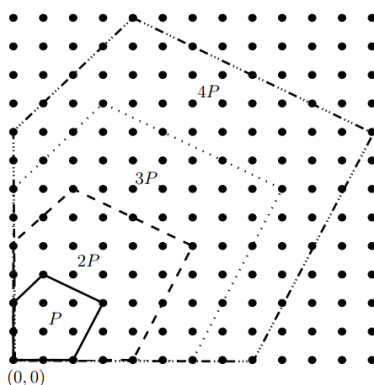
Očito je  $L(P) = I(P) + B(P)$ , ali da bismo izračunali  $L(kP)$  moramo odrediti  $\text{area}(kP)$  i  $B(kP)$ , a to može biti poprilično komplicirano.

No, postoji puno jednostavnije rješenje opisanog problema, a ono je dato sljedećim teoremom. (J. Garbett, Lattice Point Geometry: Pick's Theorem and Minkowski's Theorem, Kenyon College (2010), 28)

**Teorem 3.4** (Ehrhartov teorem za dimenziju dva). *Neka je  $P$  poligon u rešeci  $\mathbb{Z}^2$ ,  $k \in \mathbb{N}$  i  $kP = \{kx : x \in P\}$ . Ako s  $L(kP)$  označimo broj točaka rešetke sadržane u poligonu  $kP$  tada je*

$$L(kP) = \text{area}(P) \cdot k^2 + \frac{1}{2}B(P) \cdot k + 1$$

**Primjer 3.1.** *Neka je  $P$  peterokut prikazan na slici i neka je  $k = 2, 3, 4$ . Ovim primjerom ćemo prikazati način računanja vrijednosti  $L(kP)$  tako da odredimo  $\text{area}(kP)$  i  $B(kP)$ , te pomoću teorema 3.4.*



Slika 3.6



Sa slike lako vidimo da je  $I(P) = 4$  i  $B(P) = 7$ .

Iz Pickovog teorema slijedi  $\text{area}(P) = 4 + \frac{7}{2} - 1 = \frac{13}{2}$ .

- (1) Računamo  $L(kP)$  određivanjem  $\text{area}(kP)$  i  $B(kP)$ . No, da bismo pomoću Pickovog teorema izračunali površinu poligona  $kP$  trebamo odrediti  $I(kP)$ , tako da zapravo  $L(kP) = I(kP) + B(kP)$  dobijemo prebrojavanjem točaka rešetke koje poligon  $kP$  sadrži. Dobiveni rezultati su

$$L(2P) = 34, L(3P) = 70, L(4P) = 119$$

- (2) Računamo  $L(kP)$  pomoću teorema 3.4. Slijedi  $L(kP) = \frac{13}{2}k^2 + \frac{7}{2}k + 1$ . Uvrštavanjem vrijednosti broja  $k$  dobivamo

$$L(2P) = \frac{13}{2} \cdot 4 + \frac{7}{2} \cdot 2 + 1 = 34$$

$$L(3P) = \frac{13}{2} \cdot 9 + \frac{7}{2} \cdot 3 + 1 = 70$$

$$L(4P) = \frac{13}{2} \cdot 16 + \frac{7}{2} \cdot 4 + 1 = 119$$

Iako je ovaj primjer poprilično jednostavan, ipak ilustrira eleganciju računanja vrijednosti  $L(kP)$  dobivenu teoremom 3.4.

## Poglavlje 4

### Primitivni tetraedri u rešeci $\mathbb{Z}^3$

U trodimenzionalnoj rešeci promatramo primitivne tetraedre. Na početku navodimo nužan i dovoljan uvjet da bi tetraedar bio primitivan. Svaki tetraedar s vrhovima  $(0, 0, 0)$ ,  $(1, 0, 0)$ ,  $(0, 1, 0)$  i  $(1, 1, n)$  je primitivan za svako  $n \in \mathbb{Z} \setminus \{0\}$ . Stoga ne postoji gornja granica za volumen primitivnog tetraedra pa generalizacija Pickovog teorema nije moguća. No, pomoću unimodularnog preslikavanja, za dani volumen možemo odrediti broj klasa ekvivalencije primitivnih tetredara.

U daljnjem tekstu ćemo s  $T_{a,b,n}$  označavati tetraedar čiji su vrhovi  $(0, 0, 0)$ ,  $(1, 0, 0)$ ,  $(0, 1, 0)$  i  $(a, b, n) \in \mathbb{Z}^3$ ,  $n \neq 0$ .

**Teorem 4.1.** *Tetraedar  $T$  je primitivan ako i samo ako vrijedi  $T \cong T_{0,0,1}$  ili  $T \cong T_{1,b,n}$  pri čemu je  $1 \leq b < n$ ,  $(b, n) = 1$ .*

S obzirom da unimodularno preslikavanje čuva volumen slijedi da je broj klasa ekvivalencija primitivnih tetraedara beskonačan.

**Teorem 4.2.** *Neka su  $b, b^{-1}, n, x \in \mathbb{Z}$  takvi da je  $1 \leq x, b, b^{-1} < n$ ,  $(b, n) = (x, n) = 1$  i  $bb^{-1} \equiv 1 \pmod{n}$ . Primitivni tetraedri  $T_{1,b,n}$  i  $T_{1,x,n}$  su unimodularno ekvivalentni ako i samo ako je  $x \in \{b, n - b, b^{-1}, n - b^{-1}\}$ .*

**Napomena 4.1.**  $b^{-1}$  je cijeli broj i ne označava multiplikativni inverz broja  $b$  u polju  $\mathbb{Q}$ .

*Dokaz.* Pretpostavimo da su  $T_{1,b,n}$  i  $T_{1,x,n}$  unimodularno ekvivalentni. Tada postoji unimodularno preslikavanje koje preslikava  $T_{1,b,n}$  u  $T_{1,x,n}$ , te to preslikavanje možemo promatrati

kao preslikavanje između vrhova ta dva tetraedra. Slijedi da postoji  $4! = 24$  različitih unimodularnih preslikavanja koja preslikavaju tetraedar  $T_{1,b,n}$  u  $T_{1,x,n}$ .

- (1) Pretpostavimo da vrijedi  $(0, 0, 0) \mapsto (1, 0, 0)$ ,  $(1, 0, 0) \mapsto (0, 0, 0)$ ,  $(0, 1, 0) \mapsto (0, 1, 0)$  i  $(1, b, n) \mapsto (1, x, n)$ . Tada slijedi da je djelovanje unimodularnog preslikavanja na točku  $(v_1, v_2, v_3)$  dano s

$$\begin{pmatrix} -1 & -1 & \frac{1+b}{n} \\ 0 & 1 & \frac{x-b}{n} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Slijedi  $b \equiv -1 \pmod{n}$  i  $x - b \equiv 0 \pmod{n}$  pa zbog  $1 \leq x < n$  dobivamo  $x = b$ .

- (2) Pretpostavimo da vrijedi  $(0, 0, 0) \mapsto (0, 1, 0)$ ,  $(1, 0, 0) \mapsto (0, 0, 0)$ ,  $(0, 1, 0) \mapsto (1, x, n)$  i  $(1, b, n) \mapsto (1, 0, 0)$ . Tada slijedi da je djelovanje unimodularnog preslikavanja na točku  $(v_1, v_2, v_3)$  dano s

$$\begin{pmatrix} 0 & 1 & \frac{1-b}{n} \\ -1 & x-1 & \frac{b(1-x)}{n} \\ 0 & n & -b \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

Slijedi  $b \equiv 1 \pmod{n}$  i  $b(x-1) \equiv 0 \pmod{n}$  pa zbog  $1 \leq x < n$  dobivamo  $x = b^{-1}$ .

- (3) Pretpostavimo da vrijedi  $(0, 0, 0) \mapsto (1, 0, 0)$ ,  $(1, 0, 0) \mapsto (1, x, n)$ ,  $(0, 1, 0) \mapsto (0, 1, 0)$  i  $(1, b, n) \mapsto (0, 0, 0)$ . Tada slijedi da je djelovanje unimodularnog preslikavanja na točku  $(v_1, v_2, v_3)$  dano s

$$\begin{pmatrix} 0 & -1 & \frac{b-1}{n} \\ x & 1 & \frac{-x-b}{n} \\ n & 0 & -1 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Slijedi  $b \equiv 1 \pmod{n}$  i  $x + b \equiv 0 \pmod{n}$  pa zbog  $1 \leq x < n$  dobivamo  $x = n - b$ .

- (4) Pretpostavimo da vrijedi  $(0, 0, 0) \mapsto (1, 0, 0)$ ,  $(1, 0, 0) \mapsto (0, 1, 0)$ ,  $(0, 1, 0) \mapsto (1, x, n)$  i  $(1, b, n) \mapsto (0, 0, 0)$ . Tada slijedi da je djelovanje unimodularnog preslikavanja na točku  $(v_1, v_2, v_3)$  dano s

$$\begin{pmatrix} -1 & 0 & 0 \\ 1 & x & \frac{-1-bx}{n} \\ 0 & n & -b \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Slijedi  $bx \equiv -1 \pmod{n}$  pa zbog  $1 \leq x < n$  dobivamo  $x = n - b^{-1}$ .

Raspisivanjem preostalih preslikavanja dolazimo do zaključka da mora vrijediti  $x \in \{b, n - b, b^{-1}, n - b^{-1}\}$ .

Obratno, pretpostavimo da vrijedi  $x \in \{b, n - b, b^{-1}, n - b^{-1}\}$ .

Da bi dokazali da su  $T_{1,b,n}$  i  $T_{1,x,n}$  unimodularno ekvivalentni treba dokazati da postoji unimodularno preslikavanje koje  $T_{1,b,n}$  preslikava u  $T_{1,x,n}$ .

Promatramo svaki od četiri moguća slučaja.

- (1) Neka je  $x = b$ . Tada je identiteta traženo unimodularno preslikavanje te vrijedi  $T_{1,b,n} \cong T_{1,b,n}$ .

- (2) Neka je  $x = n - b$ .  
Tada je s

$$\begin{pmatrix} 1 & 0 & 0 \\ -1 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

definirano traženo unimodularno preslikavanje i ono redom vrhove  $(0, 0, 0)$ ,  $(1, 0, 0)$ ,  $(0, 1, 0)$ ,  $(1, b, n)$  preslikava u  $(0, 1, 0)$ ,  $(1, 0, 0)$ ,  $(0, 0, 0)$ ,  $(1, x, n)$ .

- (3) Neka je  $x = b^{-1}$ .  
Tada je s

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & b^{-1} & \frac{1-bb^{-1}}{n} \\ 0 & n & -b \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

definirano traženo unimodularno preslikavanje i ono redom vrhove  $(0, 0, 0)$ ,  $(1, 0, 0)$ ,  $(0, 1, 0)$ ,  $(1, b, n)$  preslikava u  $(1, 0, 0)$ ,  $(0, 0, 0)$ ,  $(1, x, n)$ ,  $(0, 1, 0)$ .

- (4) Neka je  $x = n - b^{-1}$ .  
Tada je s

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & n - b^{-1} & \frac{b(b^{-1}-n)+1}{n} \\ 0 & n & -b \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

definirano traženo unimodularno preslikavanje i ono redom vrhove  $(0, 0, 0)$ ,  $(1, 0, 0)$ ,  $(0, 1, 0)$ ,  $(1, b, n)$  preslikava u  $(1, 0, 0)$ ,  $(0, 0, 0)$ ,  $(1, x, n)$ ,  $(0, 1, 0)$ .

□

Neka je  $n \in \mathbb{N}$  proizvoljan. Tada iz teorema 4.1 slijedi da je tetraedar  $T_{1,b,n}$  primitivan ako i samo ako je  $1 \leq b < n$  te  $(b, n) = 1$ . Volumen tog tetraedra jednak je  $\frac{n}{6}$ .

Primjenom teorema 4.2 za proizvoljan  $n \in \mathbb{N}$  možemo odrediti broj klasa ekvivalencije primitivnih tetraedara čiji volumen je upravo  $\frac{n}{6}$ .

**Primjer 4.1.** Za različite vrijednost broja  $n \in \mathbb{N}$ , koristeći teorem 4.2, odredimo broj klasa ekvivalencije primitivnih tetraedara čiji volumen je jednak  $\frac{n}{6}$ .

(1) Neka je  $n = 5$ .

Slijedi da je  $b \in \{1, 2, 3, 4\}$  pa promatramo tetraedre  $T_{1,1,5}, T_{1,2,5}, T_{1,3,5}, T_{1,4,5}$ .

- Ako je  $b = 1$  onda iz uvjeta  $bb^{-1} \equiv 1 \pmod{5}$  te  $1 \leq b^{-1} < 5$  slijedi  $b^{-1} = 1$ .  
Dakle,  $x \in \{1, 4\}$ .  
Dobili smo  $T_{1,1,5} \cong T_{1,4,5}$
- Ako je  $b = 2$  onda iz uvjeta  $bb^{-1} \equiv 1 \pmod{5}$  te  $1 \leq b^{-1} < 5$  slijedi  $b^{-1} = 3$ .  
Dakle,  $x \in \{2, 3\}$ .  
Dobili smo  $T_{1,2,5} \cong T_{1,3,5}$

Dakle, postoje dvije klase ekvivalencije primitivnih tetraedara volumena  $\frac{5}{6}$ .

(2) Neka je  $n = 6$ .

Slijedi da je  $b \in \{1, 5\}$  pa promatramo tetraedre  $T_{1,1,6}, T_{1,5,6}$ . Ako je  $b = 1$  onda iz uvjeta  $bb^{-1} \equiv 1 \pmod{6}$  te  $1 \leq b^{-1} < 6$  slijedi  $b^{-1} = 1$ .

Dakle,  $x \in \{1, 5\}$ .

Dobili smo  $T_{1,1,6} \cong T_{1,5,6}$ . Dakle, postoji samo jedna klasa ekvivalencije primitivnih tetraedara čiji volumen je jednak 1. Drugim riječima, svi primitivni tetraedri volumena 1 su međusobno unimodularno ekvivalentni.

(3) Neka je  $n = 13$ .

Slijedi da je  $b \in \{1, 2, \dots, 11, 12\}$  pa promatramo tetraedre  $T_{1,1,13}, T_{1,2,13}, \dots, T_{1,12,13}$ .

- Ako je  $b = 1$  onda iz uvjeta  $bb^{-1} \equiv 1 \pmod{13}$  te  $1 \leq b^{-1} < 13$  slijedi  $b^{-1} = 1$ .  
Dakle,  $x \in \{1, 12\}$ .  
Dobili smo  $T_{1,1,13} \cong T_{1,12,13}$
- Ako je  $b = 2$  onda iz uvjeta  $bb^{-1} \equiv 1 \pmod{13}$  te  $1 \leq b^{-1} < 13$  slijedi  $b^{-1} = 7$ .  
Dakle,  $x \in \{2, 6, 7, 11\}$ .  
Dobili smo  $T_{1,2,13} \cong T_{1,6,13} \cong T_{1,7,13} \cong T_{1,11,13}$
- Ako je  $b = 3$  onda iz uvjeta  $bb^{-1} \equiv 1 \pmod{13}$  te  $1 \leq b^{-1} < 13$  slijedi  $b^{-1} = 9$ .  
Dakle,  $x \in \{3, 4, 9, 10\}$ .  
Dobili smo  $T_{1,3,13} \cong T_{1,4,13} \cong T_{1,9,13} \cong T_{1,10,13}$
- Ako je  $b = 4$  onda iz uvjeta  $bb^{-1} \equiv 1 \pmod{13}$  te  $1 \leq b^{-1} < 13$  slijedi  $b^{-1} = 10$ .  
Dakle,  $x \in \{3, 4, 9, 10\}$ .  
Dobili smo  $T_{1,3,13} \cong T_{1,4,13} \cong T_{1,9,13} \cong T_{1,10,13}$
- Ako je  $b = 5$  onda iz uvjeta  $bb^{-1} \equiv 1 \pmod{13}$  te  $1 \leq b^{-1} < 13$  slijedi  $b^{-1} = 8$ .  
Dakle,  $x \in \{5, 8\}$ .  
Dobili smo  $T_{1,5,13} \cong T_{1,8,13}$

Dakle, postoje četiri klase ekvivalencije primitivnih tetraedara volumena  $\frac{13}{6}$ .

(4) Neka je  $n = 30$ .

Slijedi da je  $b \in \{1, 7, 11, 13, 17, 19, 23, 29\}$  pa promatramo tetraedre  $T_{1,1,30}$ ,  $T_{1,7,30}$ ,  $T_{1,11,30}$ ,  $T_{1,13,30}$ ,  $T_{1,17,30}$ ,  $T_{1,19,30}$ ,  $T_{1,23,30}$ ,  $T_{1,29,30}$ .

- Ako je  $b = 1$  onda iz uvjeta  $bb^{-1} \equiv 1 \pmod{30}$  te  $1 \leq b^{-1} < 30$  slijedi  $b^{-1} = 1$ .  
Dakle,  $x \in \{1, 29\}$ .  
Dobili smo  $T_{1,1,30} \cong T_{1,29,30}$
- Ako je  $b = 7$  onda iz uvjeta  $bb^{-1} \equiv 1 \pmod{30}$  te  $1 \leq b^{-1} < 30$  slijedi  $b^{-1} = 13$ .  
Dakle,  $x \in \{7, 13, 17, 23\}$ .  
Dobili smo  $T_{1,7,30} \cong T_{1,13,30} \cong T_{1,17,30} \cong T_{1,23,30}$
- Ako je  $b = 11$  onda iz uvjeta  $bb^{-1} \equiv 1 \pmod{30}$  te  $1 \leq b^{-1} < 30$  slijedi  $b^{-1} = 11$ .  
Dakle,  $x \in \{11, 19\}$ .  
Dobili smo  $T_{1,11,30} \cong T_{1,19,30}$

Dakle, postoje tri klase ekvivalencije primitivnih tetraedara volumena 5.

No, što je  $n$  veći to je teže izračunati broj klasa ekvivalencije, tako da ovaj način baš i nije operativan.

**Definicija 4.1.** Neka je  $n \in \mathbb{N}$ ,  $n \geq 1$ . Eulerova funkcija  $\phi(n)$  je broj pozitivnih cijelih brojeva koji su relativno prosti s  $n$ .

**Napomena 4.2.** Ako je  $n \in \mathbb{N}$  prost, onda je  $\phi(n) = n - 1$ .

**Teorem 4.3.** Eulerova funkcija je multiplikativna, tj.  $\phi(1) = 1$  te za sve  $a, b \in \mathbb{N}$  takve da je  $(a, b) = 1$  vrijedi  $\phi(ab) = \phi(a)\phi(b)$ .  
(vidi [8], 18)

**Definicija 4.2.** Neka grupa  $G$  djeluje na skup  $X$  i neka je  $x \in X$ . Stabilizator elementa  $x$  je skup  $G_x = \{g \in G : gx = x\} \subseteq G$ . Orbita elementa  $x$  je skup  $x^G = \{gx : g \in G\} \subseteq X$ .

**Korolar 4.1.** Neka grupa  $G$  djeluje na skup  $X$  i neka je  $x \in X$ . Tada je  $|x^G| \cdot |G_x| = |G|$ .

**Lema 4.1** (Cauchy-Frobenius-Burnside). *Neka grupa  $G$  djeluje na skup  $X$ . Označimo s  $f(g) = |\{x \in X : gx = x\}|$  broj točaka iz  $X$  fiksiranih elementom  $g \in G$ . Broj orbita pri djelovanju  $G$  na  $X$  jednak je prosječnom broju točaka koje fiksiraju elementi iz  $G$ ,*

$$\frac{1}{|G|} \sum_{g \in G} f(g)$$

*Dokaz.* Na dva načina prebrojimo parove  $\{(g, x) \in G \times X : gx = x\}$ .

Za fiksni  $g \in G$  broj parova je  $f(g)$  pa je ukupan broj parova  $\sum_{g \in G} f(g)$ .

Za fiksni  $x \in X$  broj parova jednak je redu stabilizatora  $|G_x|$  koji je prema korolaru 4.1 jednak  $\frac{|G|}{|x^G|}$ .

Ukupan broj parova je stoga  $|G| \sum_{x \in X} \frac{1}{|x^G|}$ .

Rezultat slijedi izjednačavanjem, ako primijetimo da suma  $\sum_{x \in X} \frac{1}{|x^G|}$  daje broj orbita pri djelovanju  $G$  na  $X$ .

Za svaki  $x$  sumiramo recipročnu vrijednost veličine orbite kojoj pripada, pa u sumi dobivamo po jednu jedinicu za svaku orbitu.

□

**Definicija 4.3.** *S  $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots, n - 1 + n\mathbb{Z}\}$  označavamo prsten ostataka modulo  $n$ .*

**Definicija 4.4.** *Neka je  $n \in \mathbb{N}$  i  $f(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ . Tada s  $N(f(x) \equiv 0 \pmod{n})$  označavamo broj rješenja kongruencije  $f(x) \equiv 0 \pmod{n}$  u  $\mathbb{Z}/n\mathbb{Z}$ .*

U daljnjem radu će nam značajan biti broj rješenja kongruencija  $f(x) \equiv 0 \pmod{n}$  za  $f(x) = x^2 - 1$  i  $f(x) = x^2 + 1$ . Sljedeći teorem iz teorije brojeva daje nam vrijednosti  $N(x^2 \pm 1 \equiv 0 \pmod{n})$ . Osim toga, za primjenu teorema potrebno je samo rastaviti broj  $n$  na proste faktore što ga čini lako primjenjivim te nam je njegov značaj samim time još i veći. (vidi [10], poglavlja 2 i 3)

**Teorem 4.4.** *Neka je  $n = 2^k m$ , pri čemu je  $n \geq 2$  i  $(m, 2) = 1$ . Ako je  $m > 1$  onda s  $p_1, \dots, p_t$  označimo proste faktore od  $m$ , a u suprotnom stavimo  $t = 0$ . Tada je*

$$N(x^2 - 1 \equiv 0 \pmod{n}) = \begin{cases} 2^t & , \text{ za } k = 0, 1 \\ 2^{t+1} & , \text{ za } k = 2 \\ 2^{t+2} & , \text{ za } k \geq 3 \end{cases}$$

$$N(x^2+1 \equiv 0 \pmod{n}) = \begin{cases} 2^t & , \text{ ako je } k \leq 1 \text{ i } p_i \equiv 1 \pmod{4} \text{ za svako } i \in \{1, \dots, t\} \\ 0 & , \text{ ako je } k \geq 2 \text{ ili postoji } i \in \{1, \dots, t\} \text{ takav da je } p_i \equiv 3 \pmod{4} \end{cases}$$

**Teorem 4.5.** Neka je  $n \in \mathbb{N}$ ,  $n \geq 2$  te označimo s  $T(n)$  broj različitih klasa ekvivalencije primitivnih tetraedara volumena  $\frac{n}{6}$ . Neka je  $f(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$  i neka je  $N(f(x) \equiv 0 \pmod{n})$  broj rješenja kongruencije  $f(x) \equiv 0 \pmod{n}$  u  $\mathbb{Z}/n\mathbb{Z}$ . Tada je

$$T(n) = \frac{\phi(n) + N(x^2 - 1 \equiv 0 \pmod{n}) + N(x^2 + 1 \equiv 0 \pmod{n})}{4} \quad (4.1)$$

Ako je  $n$  prost, onda je

$$T(n) = \begin{cases} \frac{n+3}{4} & , \text{ za } n \equiv 1 \pmod{4} \\ \frac{n+1}{4} & , \text{ za } n \equiv 3 \pmod{4} \end{cases}$$

*Dokaz.* Neka je  $U = \{x : 1 \leq x < n, (x, n) = 1\}$  i neka je  $G = \{g_1, g_2, g_3, g_4\}$  skup bijekcija na  $U$ , gdje su  $g_1(x) = x$ ,  $g_2(x) = n - x$ ,  $g_3(x) = x^{-1}$  i  $g_4(x) = n - x^{-1}$ , pri čemu je  $x^{-1}$  takav da je  $xx^{-1} \equiv 1 \pmod{n}$ , za svaki  $x \in U$ .

Iz definicije funkcije  $\phi$  slijedi  $|U| = \phi(n)$ .

Po lemi 4.1 slijedi da je  $T(n)$  jednak broju orbita od  $U$  pod djelovanjem grupe  $G$ .

Neka je  $U_i = \{x \in U : g_i(x) = x\}$ , za  $i = 1, 2, 3, 4$ .

- $g_1$  je identiteta pa su sve točke iz  $U$  fiksne, tj. vrijedi  $|U_1| = |U| = \phi(n)$ .
- Iz  $g_2(x) = x$  slijedi  $n - x = x$  pa je  $x = \frac{n}{2}$ . Ako je  $n$  neparan onda  $x \notin \mathbb{N}$ , a ako je  $n$  paran onda je  $(x, n) \neq 1$ . Dakle, funkcija  $g_2$  nema fiksnih točaka pa je  $|U_2| = 0$ .
- Ako je  $g_3(x) = x$  onda je  $x^{-1} = x$  pa slijedi  $x^2 = xx^{-1} \equiv 1 \pmod{n}$ . Stoga je  $|U_3| = N(x^2 - 1 \equiv 0 \pmod{n})$ .
- Množenjem  $g_4(x) = x$  s  $x$  dobivamo  $x^2 = nx - xx^{-1} \equiv 0 - 1 \pmod{n}$  pa je  $x^2 + 1 \equiv 0 \pmod{n}$ . Dakle,  $|U_4| = N(x^2 + 1 \equiv 0 \pmod{n})$ .

Sada, primjenom leme 4.1 dobivamo  $T(n) = \frac{1}{|G|} \sum_{g_i \in G} |\{x \in U : g_i(x) = x\}|$ , tj.

$$T(n) = \frac{\phi(n) + N(x^2 - 1 \equiv 0 \pmod{n}) + N(x^2 + 1 \equiv 0 \pmod{n})}{4}$$



Posebno, ako je  $n$  prost tada je  $\phi(n) = n - 1$  te iz teorema 4.3 slijedi  $N(x^2 - 1 \equiv 0 \pmod{n}) = 2$ . Osim toga, također iz teorema 4.3 slijedi  $N(x^2 + 1 \equiv 0 \pmod{n}) = 2$  ako je  $n \equiv 1 \pmod{4}$  tj.  $N(x^2 + 1 \equiv 0 \pmod{n}) = 0$  ako je  $n \equiv 3 \pmod{4}$ . Dakle, vrijedi i druga tvrdnja.

□

**Primjer 4.2.** Koristeći teoreme 4.3 i 4.4 izračunajmo broj klasa ekvivalencije primitivnih tetraedara čiji volumen je  $\frac{n}{6}$ . Za  $n \in \mathbb{N}$  uzet ćemo iste brojeve kao i u primjeru 4.1.

- (1) Neka je  $n = 5$ . Tada je  $\phi(5) = 4$ . Iz teorema 4.3, za  $k = 0$  i  $t = 1$ , slijedi  $N(x^2 - 1 \equiv 0 \pmod{5}) = 2$  i  $N(x^2 + 1 \equiv 0 \pmod{5}) = 2$ . Iz teorema 4.4 slijedi  $T(n) = 2$ .
- (2) Neka je  $n = 6$ . Tada je  $\phi(6) = 2$ . Iz teorema 4.3, za  $k = 1$  i  $t = 1$ , slijedi  $N(x^2 - 1 \equiv 0 \pmod{6}) = 2$  i  $N(x^2 + 1 \equiv 0 \pmod{6}) = 0$ . Iz teorema 4.4 slijedi  $T(n) = 1$ .
- (3) Neka je  $n = 13$ . Tada je  $\phi(13) = 12$ . Iz teorema 4.3, za  $k = 0$  i  $t = 1$ , slijedi  $N(x^2 - 1 \equiv 0 \pmod{13}) = 2$  i  $N(x^2 + 1 \equiv 0 \pmod{13}) = 2$ . Iz teorema 4.4 slijedi  $T(n) = 4$ .
- (4) Neka je  $n = 30$ . Tada je  $\phi(30) = 8$ . Iz teorema 4.3, za  $k = 1$  i  $t = 2$ , slijedi  $N(x^2 - 1 \equiv 0 \pmod{30}) = 4$  i  $N(x^2 + 1 \equiv 0 \pmod{30}) = 0$ . Iz teorema 4.4 slijedi  $T(n) = 3$ .
- (5) Neka je  $n = 3640$ . Tada je  $\phi(3640) = \phi(8)\phi(5)\phi(7)\phi(13) = 4 \cdot 4 \cdot 6 \cdot 12 = 1152$ . Iz teorema 4.3, za  $k = 3$  i  $t = 3$ , slijedi  $N(x^2 - 1 \equiv 0 \pmod{3640}) = 2^5 = 32$  i  $N(x^2 + 1 \equiv 0 \pmod{3640}) = 0$ . Iz teorema 4.4 slijedi  $T(n) = \frac{1152+32+0}{4} = 296$ .

Kao što vidimo, puno je jednostavnije izračunati broj klasa primitivnih tetraedara koristeći teoreme 4.3 i 4.4 nego koristeći teorem 4.2. No, ovako smo izračunali samo broj klasa ekvivalencije, a ne i koji tetraedar se nalazi u kojoj od klasa. Osim što je ovaj način jednostavniji za računanje, probleme nam ne stvara niti veća vrijednost broja  $n$ .

Iako ne možemo generalizirati Pickov teorem na tetraedre u  $\mathbb{Z}^3$  postoji način kako možemo povezati volumen tetraedra i broj točaka rešetke.

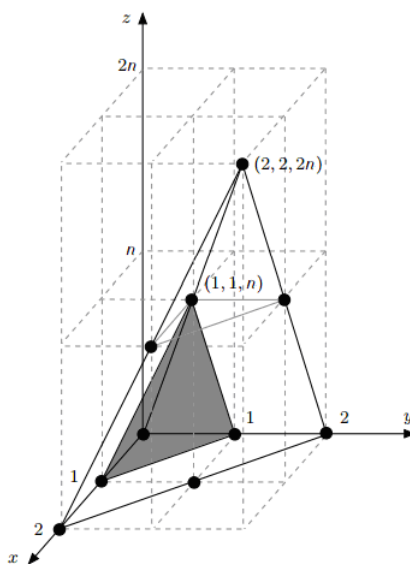
Neka je  $T$  primitivan tetraedar u trodimenzionalnoj cjelobrojnoj rešeci, neka je  $k \in \mathbb{N}$ ,  $kT = \{kx : x \in T\}$  te označimo s  $L(kT) = |kT \cap \mathbb{Z}^3|$ . Tada postoje  $a_1, a_2, a_3 \in \mathbb{R}$  takvi da je

$$L(kT) = a_3 k^3 + a_2 k^2 + a_1 k + 1 \quad (4.2)$$

pri čemu je  $a_3 = \text{vol}(T)$ .

Postoji generalizacija formule (4.2) koja se odnosi na politope u  $d$ -dimenzionalnoj rešeci, no mi se u ovome radu nećemo baviti tom tzv. Ehrhartovom teorijom. (J. Kepler, Counting Lattice Points in Polytopes: The Ehrhart Theory)

**Primjer 4.3.** Neka je  $T$  primitivan tetraedar u trodimenzionalnoj cjelobrojnoj rešeci čiji su vrhovi točke  $(0, 0, 0)$ ,  $(1, 0, 0)$ ,  $(0, 1, 0)$ ,  $(1, 1, n)$ . U ovome primjeru odredit ćemo koeficijente  $a_1, a_2, a_3 \in \mathbb{R}$  tako da za tetraedar  $T$  vrijedi formula (4.2). Za  $k = 1$  i  $k = 2$ , pomoću sljedeće slike odredit ćemo  $L(T)$  i  $L(2T)$ .



Slika 4.1

Vrijedi

$$L(T) = 4 = a_3 + a_2 + a_1 + 1$$

$$L(2T) = 9 + n = 8a_3 + 4a_2 + 2a_1 + 1$$

No, znamo da je  $a_3 = \text{vol}(T) = \frac{n}{6}$  pa slijedi

$$4 = \frac{n}{6} + a_2 + a_1 + 1$$

$$9 + n = \frac{8n}{6} + 4a_2 + 2a_1 + 1$$

Rješavajući gornji sustav dobivamo  $a_2 = 1$  i  $a_1 = 2 - \frac{n}{6}$ .

Dakle, za tetraedar  $T$  vrijedi

$$L(kT) = \frac{n}{6}k^3 + k^2 + \left(2 - \frac{n}{6}\right)k + 1$$

# Bibliografija

1. M. R. Khan, A Counting Formula for Primitive Tetrahedra in  $\mathbb{Z}^3$ , Amer. Math. Monthly 106 (6) (1999), 515-533.
2. B. Reznick, Lattice Point Simplices, Discrete Math. 60 (1986), 219-242.
3. C. Haase, B. Nill, A. Paffenholz, Lecture Notes on Lattice Polytopes, TU Darmstadt (2012), 20-26.
4. J. Garbett, Lattice Point Geometry: Pick's Theorem and Minkowski's Theorem, Kenyon College (2010), 12-14
5. P.R. Scott, On convex lattice polygons, Bull. Austral. Math. Soc., Vol. 15 (1976), 395-399.
6. J. Šiftar, V. Krčadinac, Konačne geometrije, skripta, PMF-Matematički odsjek, 2013.
7. B. Pavković, D. Veljan, Elementarna matematika 1, Tehnička knjiga, 1992
8. A. Dujella, Uvod u teoriju brojeva, skripta, PMF-Matematički odsjek
9. M. Polonijo i ostali, Euklidski prostori, skripta, PMF-Matematički odsjek
10. H. Loo Keng, Introduction to Number Theory, translated from the Chinese by Peter Shiu, Springer-Verlag, 1982

# Sažetak

U ovome radu promatramo primitivne tetraedre u trodimenzionalnoj cjelobrojnoj rešeci. Tetraedar je primitivan ako su mu vrhovi točke rešetke, ali se sadrži niti jednu drugu točku rešetke, niti na rubu niti u unutrašnjosti. Koristimo unimodularno preslikavanje kao glavni alat pomoću kojeg ćemo dokazati većinu rezultata, a naročito je bitno za klasifikaciju primitivnih tetraedara, koja se temelji na unimodularnoj ekvivalenciji.

Zatim, radi potpunosti i usporedbe s trodimenzionalnim slučajem, razmatramo poligone u rešeci  $\mathbb{Z}^2$ . Ovdje ključnu ulogu za karakterizaciju primitivnih poligona ima glasoviti Pickov teorem koji daje vezu između površine poligona i broja točaka rešetke koje taj poligon sadrži na rubu, odnosno u unutrašnjosti.

U trodimenzionalnoj rešeci najprije dajemo karakterizaciju primitivnih tetraedara u terminima unimodularne ekvivalencije. S obzirom da volumen primitivnog tetraedra nije ograničen, ne možemo generalizirati Pickov teorem u tri dimenzije, ali možemo naći formulu za prebrojavanje klasa ekvivalencije primitivnih tetraedara danog volumena.

# Summary

In this paper we study primitive tetrahedra in a three dimensional integer lattice. A tetrahedron is primitive if its vertices are lattice points but it does not contain any other lattice points in its interior or on its boundary. We use unimodular maps as a main mathematical tool to prove most of the results, and especially for classification of primitive tetrahedra, based on unimodular equivalence.

Further, we investigate primitive polygons in  $\mathbb{Z}^2$  so that a comparison could be made with the three dimensional case. A crucial part in this chapter belongs to the famous Pick's theorem, which gives the relationship between the area of a lattice polygon and the number of lattice points on its boundary and in its interior.

In the three dimensional integer lattice, first of all we state a characterization of primitive tetrahedra in terms of unimodular equivalence. Considering that there is no boundary on the volume of a primitive tetrahedron, a generalization of Pick's theorem to dimension three is impossible, but there is a simple formula that counts the number of equivalence classes of primitive tetrahedra of a given volume.

# Životopis

Rođena sam 27. travnja 1989. godine u Zagrebu. Od 1996. do 1998. godine pohađala sam OŠ Ivana Cankara, a od 1998. do 2004. godine OŠ Otona Ivekovića. Nakon završene osnovne škole upisala sam V. gimnaziju u Zagrebu, te 2008. godine maturirala s odličnim uspjehom. Te iste godine upisala sam Preddiplomski sveučilišni studij Matematika na Prirodoslovno - matematičkom fakultetu u Zagrebu. Nakon završetka Preddiplomskog studija 2013. godine upisala sam Diplomski sveučilišni studij Matematička statistika na istom fakultetu.