МАТЕМАТИЧКА ГИМНАЗИЈА

МАТУРСКИ РАД

из предмета Анализа са алгебром

МНОУГОУГЛОВИ СА ТЕМЕНИМА У ЦЕЛОБРОЈНИМ ТАЧКАМА

Ученик:
Ђорђе Жикелић, 4д,

Ментор:
Др Ђорђе Баралић

Београд, Јун 2014.

Садржај

1 Увод

При решавању разних математичких проблема, није реткост да нам сама поставка делује одбојна и неприступачна, да једноставно немамо идеју о томе како приступити проблему. Тада се трудимо да, представљањем проблема на неки други, еквивалентан начин, стекнемо бољу слику о томе шта заправо треба доказати, што често резултује и неком идејом која води ка решењу. У том смислу, решетке су врло погодне као математички апарат зато што их је једноставно замислити и одређени проблем интерпретирати помоћу одговарајућих елемената решетке.

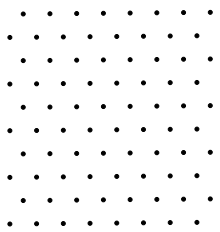
Решетке се не могу назвати математичком облашћу. Оне више представљају математичко оруђе које има бројне примене у комбинаторици, геометрији, криптографији, информатици, али и неким неочекиваним математичким областима, као што је теорија бројева (леп пример једне такве примене је интерпретација проблема Фробениусових бројева, коју ћемо навести на крају овог рада). Међутим, то не значи да иза ове наизглед једноставне конфигурације не постоји сложена теорија која нам у многоме може помоћи у решавању интерпретираног проблема. Због тога је јако корисно знати понешто о овој теми.

Ми ћемо се у овом раду пре свега бавити целобројним решеткама у еуклидским просторима (и то највише у $\mathbb{R}^2$). Најпре дефинишемо решетку уопште, а затим у овом делу представићемо тврђења Пикове теореме, теореме Минковског, као и неколико тврђења које су поставили Аркинштал, Скот, Рабиновитз, а која су новијег века. Затим ћемо се бавити неким основним својствима политопа уписаним у целобројну решетку у еуклидском простору $\mathbb{R}^n$, да бисмо сам рад завршили већ наведеним Фробениусовим проблемом и његовом интерпретацијом помоћу целобројних решетки.

2 Решетка и многоугао уписан у њу

2.1 Шта је заправо решетка?

Дефиниција 2.1. *Скуп L тачака у $\mathbb{R}^n$ назива се **решетком** ако задовољава следеће услове:*
1. $(V,+)$ је дискретна група, где је V скуп свих вектора са крајњим тачкама у тачкама решетке L.
2. Свака тачка у L је центар лопте која не садржи ни једну другу тачку из L.



Слика 1. Решетка

Приметимо да, на први поглед, није интуитивно зашто ова дефиниција одговара нашем неформалном схватању решетке. Међутим, како из другог услова имамо да, на пример, решетка не може садржати скуп повезаних тачака (иначе лопта произвољно малог пречника са центром у некој од ових тачака садржи још неку тачку решетке), примећујемо да су тачке из L, што се тога тиче, одговарају нашем неформалном дефинисању решетке. Такође, из првог услова ($(V,+)$ је група) интуитивно је јасно зашто ће решетка бити симетрична у односу на сваку тачку из L, па ова дефиниција заиста одговара неформалном доживљавању решетке.

Пример 2.1. *$\mathbb{Q}^n$ је подгрупа $\mathbb{R}^n$, али није дискретна, тако да $\mathbb{Q}^n$ није решетка.*

Пример 2.2. *Скуп $\mathbb{Z}^n$ јесте решетка, зато што задовољава претходну дефиницију.*

Овде наводимо још једну, еквивалентну дефиницију решетке.

Дефиниција 2.2. *Нека су $B = [b_1, b_2, \ldots, b_k] \in \mathbb{R}^{n\times k}$ линеарно независни вектори у $\mathbb{R}^n$. Тада се **решетка** дефинише помоћу B као*

$$L(B) = \left\{Bx | x \in \mathbb{Z}^k\right\} = \left\{\sum_{i=1}^{k} x_i b_i | x_i \in \mathbb{Z}\right\}.$$

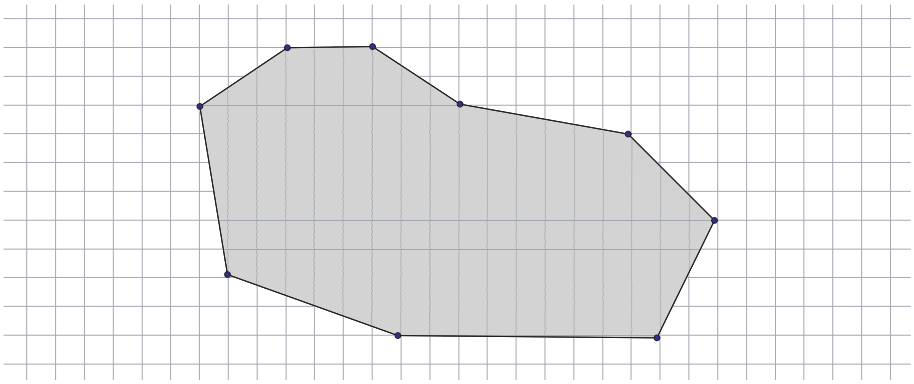
Дефиниција 2.3. *Сваку тачку подскупа L скупа $\mathbb{R}^n$ који је решетка називамо и* ***теменом (чвором) решетке*** *L.*

Дефинишимо сада и целобројну решетку, која ће нас, заправо, и највише интересовати у овом раду.

Дефиниција 2.4. *Тачка $(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ је* ***целобројна*** *ако x_1, x_2, …, $x_n \in \mathbb{Z}^n$. Решетка је* ***целобројна*** *ако су сви њени чворови целобројне тачке.*

Дефиниција 2.5. *Многоугао је уписан у решетку $L \subset \mathbb{R}^2$ ако су сва његова темена чворови те решетке.*

Дефиниција 2.6. ***Прост многоугао*** *P је многоугао чија је граница једна излом-љена линија, која не сече саму себе. Прост многоугао је уписан у решетку ако су сва његова темена чворови ове решетке.*



Слика 2. Прост многоугао

У наставку овог поглавља бавићемо се неким својствима уписаних многоуглова, и сматраћемо да су све решетке целобројне и у $\mathbb{R}^2$.

2.2 Пикова теорема

Пошто смо се упознали са неким основним терминима, прећи ћемо на нека од најважнијих својстава многоуглова уписаних у решетке. Вероватно најпознатија је *Пикова теорема* (1899, Џорџ Александер Пик), која нам омогућава да израчунамо површину многоугла само пребројавањем одређених чворова решетке. Интерестантно је да је Џон Реви показао да не постоји еквивалент Пиковој теореми у екулидским просторима $\mathbb{R}^n$, $n \geq 3$.

Дефиниција 2.7. *За прав многоугао P уписан у целобројну решетку $L \subset \mathbb{R}^2$, са $u(P)$ означимо број чворова у унутрашњости многоугла, са $v(P)$ број чворова на самој граничној линији, а са $S(P)$ означимо његову површину.*

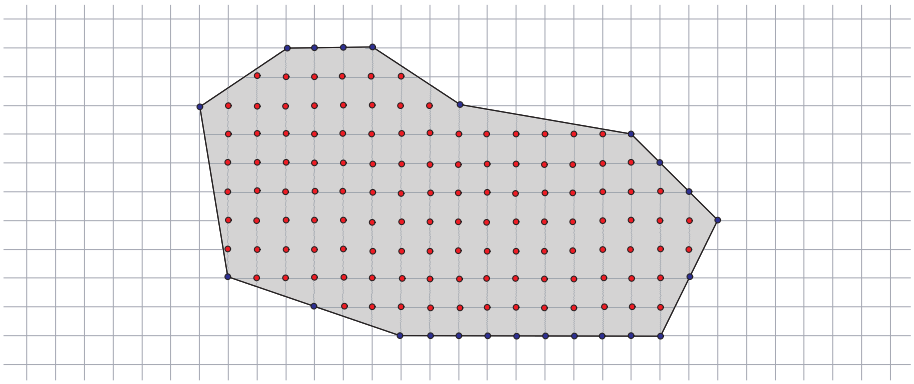
Теорема 2.1. *Ако је P прав многоугао уписан у целобројну решетку $L \subset \mathbb{R}^2$, важи:*

$$S(P) = u(P) + \frac{v(P)}{2} - 1.$$

Пикова теорема има више доказа. Представићемо два, један добијен триангулацијом на примитивне троуглове, а други помоћу Ојлерове теореме из теорије графова. За сваки од њих потребно нам је више помоћних тврђења.

Дефиниција 2.8. *Подела многоугла P на дисјунктне троуглове назива се **триангулација** многоугла P.*

Лема 2.1. *Сваки n-тоугао P_n могуће је поделити на $n-2$ дисјунктних троуглова помоћу његових дијагонала које се међусобно не секу.*



Слика 3. Пикова теорема

Доказ. Тврђење ћемо доказати потпуном индукцијом по n. Случај $n = 3$ је тривијалан, па ћемо претпоставити да оно важи за све $n = 3, 4, \ldots, k$ и доказати га за $n = k + 1$. Уочимо дијагоналу овог $(k+1)$-тоугла. Она дели овај многоугао на два дисјунктна многоугла, са по m и l темена, редом. Како свако теме полазног многоугла припада тачно једном од два добијена, осим крајњих тачака уочене дијагонале које су присутне у оба многоугла, имамо да је $m + l = n + 2$. Према индуктивној претпоставци могуће је извршити триангулацију добијених многоуглова и тако добити $m - 2$ и $l - 2$ троугла, редом, а како се дијагонале из различитих многоуглова међусобно не секу јер су они дисјунктни, добили смо триангулацију на $k-2+l-2 = n-2$ троугла, чиме је доказ завршен. □

Последица 1. *Сваки n-тоугао уписан у решетку може се поделити на $n-2$ дисјунктна троугла уписана у решетку.*

Дефиниција 2.9. *Многоугао уписан у решетку је* ***примитиван*** *ако нема темена решетке у својој унутрашњости и на ободу, са изузетком самих темена многоугла.*

Лема 2.2. *Сваки многоугао уписан у решетку може се поделити на примитивне троуглове уписане у решетку.*

Доказ. На основу претходно доказане леме, могуће је дати многоугао триангулисати на троуглове уписане у решетку. Дакле, довољно је показати да је могуће извршити триангулацију троугла на примитивне троуглове. Ово показујемо индукцијом по r, где је r број чворова решетке унутар овог троугла.

Ако је $r = 0$, и ако је троугао примитиван, тврђење је доказано. У супротном, постоји страница троугла са бар једним чвором у унутрашњости. Тада троугао делимо тако што све чворове на тој страници спајамо са наспрамним теменом троугла, и тиме се смањује максималан број чворова на ободу свих ових троуглова. Како је овај број ненегативан и цео, у једном тренутку мора достићи 0, чиме је извршена описана триангулација. Ако је $r = 1$, поделићемо дати троугао на 3 мања тако да је свакоме теме ова једна тачка у унутрашњости, а преостала два су темена троугла. Тиме смо добили три троугла која се по индуктивној хипотези могу триангулисати на описани начин. Напокон, ако је $r > 1$ уочавањем неког од чворова унутар троугла и сличном поделом на 3 троугла добијемо да максимум броја чворова у унутрашњости троуглова опада, па по индуктивној хипотези за мање r поново можемо извршити триангулацију, чиме је доказ завршен. □

Лема 2.3. *Површина примитивног троугла уписаног у целобројну решетку је* $\frac{1}{2}$.

Ова лема може се доказати на много начина, али због изразите елеганције бирамо следећи, иако можда мање интуитиван.

Доказ. Уведимо координатни систем, и транслирајмо посматрани примитивни троугао тако да му се теме оштрог угла нађе у координатном почетку (како је ово прави троугао мора постојати бар један оштар угао). Приметимо да тада координатне осе не секу странице троугла у унутрашњости, иначе троуагао не би био примитиван. Како је угао код координатног почетка оштар, закључујемо да се цео троугао налази у једном квадранту. Без губљења на општости, у првом.

Нека су темена посматраног троугла $O(0,0)$, $P(p_x, p_y)$ и $Q(q_x, q_y)$. Приметимо да је $(p_x, p_y) = (q_x, q_y) = 1$, јер би у супротном постојао чвор решетке на OP или OQ, па троугао не би био примитиван. Такође, P и Q са исте стране праве $y = x$, јер би у супротном нека тачка осе или тачка $(1,1)$ припадали троуглу. То значи да је $0 \leq \frac{p_x}{p_y}, \frac{q_x}{q_y} \leq 1$.

Уочимо сада све тачке које су *видљиве* из O, такве да за њихов аргумент важи $\phi \in [0, \pi/4]$. За сваку тачку редом посматрамо количник апсцисе и ординате. Није тешко приметити да ове тачке чине *Фарејев низ* за подесно изабран максималан именилац (овде би то био максимум координата P, Q), и то у растућем поретку. Како је $\triangle OPQ$ примитиван, P и Q су суседне у овом низу, па на основу познатог тврђења за Фарејев низ важи $p_y q_x - p_x q_y = 1$, па како је $O = O(0, 0)$, из аналитичке формуле за површину троугла имамо да је површина примитивног троугла заиста $\frac{1}{2}$. □

Вратимо се сада доказу Пикове теореме. Као што смо већ рекли, извешћемо га на два начина.

Доказ 1. Како смо већ показали, могуће је дати многоугао P поделити на примитивне троуглове. Ако је број ових троуглова N, сума углова у свим троугловима је

$$T = N\pi. \tag{1}$$

Са друге стране, како је сума углова чије је теме у фиксираној унутрашњој тачки једнака 2π, сума углова код свих чворова на ободу (а која нису темена многоугла) једнака π, а сума свих углова у теменима многоугла је $(n-2)\pi$, имамо да важи

$$T = 2\pi u(P) + \pi v(P) - 2\pi, \tag{2}$$

па изједначавањем (1) и (2) добијамо

$$N\pi = 2\pi u(P) + \pi v(P) - 2\pi,$$

односно

$$N = 2u(P) + v(P) - 2.$$

На крају, како је површина примитивног троугла $\frac{1}{2}$, имамо $S(P) = \frac{N}{2}$, па одатле следи

$$S(P) = u(P) + \frac{v(P)}{2} - 1.$$

□

Доказ 2. Доказ се такође може завршити применом Ојлерове теореме у теорији графова. Наиме, дефинишемо планарни граф $G(V, E)$ чији су чворови темена примитивних троуглова, ивице странице троуглова, а стране сами троуглови уз још једну страну, остатак равни. Како је већ показано да је површина примитивног троугла $\frac{1}{2}$, имамо да је $S(P) = \frac{1}{2}(f-1)$. Са друге стране, ако са e_v означимо број ивица које спајају чворове на ободу, а са e_u обележимо број осталих, унутрашњих ивица, мора важити $3(f-1) = 2e_u + e_v$ (ово се добије пребројавањем страница свих примитивних троуглова). Такође, из дефиниције се види

да је $v(P) = e_v$ и $u = u(P) + v(P)$. Како из Ојлерове теореме имамо да је $v - e + f = 2$, паметном манипулацијом израза добијамо следеће:

$$\begin{aligned} f &= 3(f-1) - 2f + 3 \\ &= 2e_u + e_v - 2f + 3 \\ &= 2e - e_v - 2f + 3 \\ &= 2(e-f) - e_v + 3 \\ &= 2(u-2) - e_v + 3 \\ &= 2(u(P) + v(P) - 2) - v(P) + 3 \\ &= 2u(P) + v(P) - 1. \end{aligned}$$

Дакле, $S(P) = \frac{1}{2}(f-1) = u(P) + \frac{1}{2}v(P) - 1$, па је доказ завршен. □

Постоје многа уопштења Пикове теореме. Ми ћемо овде издвојити два најпознатија, Пикову теорему за многоуглове који нису прости, и Пикову теорему за $kP = \{kx | x \in P\}$, где је k природан број, а P многоугао уписан у решетку. Пошто докази користе већ наведене идеје, овде их нећемо наводити.

Теорема 2.2 (О многоуглу који није прост)**.** *Нека је P многоугао уписан у решетку, са m рупа. Многоугао P могуће је триангулисати на примитивне троуглове. Ако се држимо већ уведених ознака, површину многоугла P рачунамо као*

$$S(P) = u(P) - \frac{1}{2}v(P) + m - 1.$$

Теорема 2.3 (О многоуглу kP)**.** *Нека је P многоугао уписан у решетку, k природан број, и $kP = \{kx | x \in P\}$. Ако са $L(kP)$ означимо број чворова унутар и на ободу многоугла kP, важи*

$$L(kP) = S(P)k^2 + \frac{1}{2}v(P)k + 1.$$

2.3 Теорема Минковског

Дефиниција 2.10. *За $S \subset \mathbb{R}^2$ кажемо да је **конвексан**, ако за сваке две тачке $P = P(p_x, p_y)$ и $Q = Q(q_x, q_y)$ које припадају S, важи*

$$\{tP + (1-t)Q | t \in [0,1]\} \subset S.$$

Дефиниција 2.11. *За тачку $P \in \mathbb{R}^2$, $P = P(p_x, p_y)$, дефинишемо њој **супротну тачку** $-P$ као $(-p_x, -p_y)$.*

Дефиниција 2.12. *За скуп тачака $S \subset \mathbb{R}^2$ кажемо да је **симетричан у односу на координатни почетак**, ако за сваку тачку $P = P(p_x, p_y)$ која припада скупу S важи и $-P \in S$.*

Теорема 2.4. *Ако је S конвексан скуп тачака у $\mathbb{R}^2$ који је симетричан у односу на координатни почетак, и чија је површина већа од 4, тада он садржи бар једну целобројну тачку различиту од координатног почетка.*

Доказ. Уочимо функцију $f : S \to \mathbb{R}^2$, која тачку (x, y) слика у $(x \mod 2, y \mod 2)$. Интуитивно, јасно нам је да ово пресликавање дели раван на квадрате 2×2, па их затим слаже један на други. Тако ћемо и ми посматрати ово пресликавање. Докажимо да ће се овако неке две тачке из S "преклапати", то јест да ће се неке две тачке из S сликати у исту тачку. Претпоставимо супротно, да је функцијс f икнјективна. Како је површина сваког од добијених квадрата 4, пошто нема преклапања површина S може бити највише 4, па имамо контрадикцију. Дакле, f није инјективна, па постоје тачке P_1 и P_2 из S такве да је $f(P_1) = f(P_2)$.

Како је $f((x,y)) = (x \mod 2, y \mod 2)$, из претходно наведеног закључујемо да постоје P_1, $P_2 \in S$ такве да је $P_1 = P_2 + (2i, 2j)$, $i, j \in Z$, $(i,j) \neq (0,0)$. Даље, како је S симетричан у односу на координатни почетак важи и $-P_2 \in S$, па из услова конвексности добијамо да

$$\frac{1}{2}(-P_2 + P_2 + (2i, 2j)) \in S,$$

односно $(i,j) \in S$, па S садржи целобројну тачку различиту од координатног почетка, што је и требало доказати. □

Интересантно је да се ова теорема може уопштити на решетке које не морају бити целобројне, као и на еуклидске просторе димензије веће од 2. Дефиниције *конвексности* и *супротне тачке* су аналогне, па их нећемо наводити (конвексност за више димензије ћемо дефинисати у наредном поглав-љу). *Запремину* скупа у $\mathbb{R}^n$ могуће је природно дефинисати. Овде представљамо оригиналну формулацију теореме Минковског.

Теорема 2.5 (Теорема Минковског)**.** *Нека је L решетка детерминанте $d(L)$ у n-димензионалном векторском простору $\mathbb{R}^n$, и нека је S конвексан подскуп скупа $\mathbb{R}^n$, који је симетричан у односу на координатни почетак. Ако је запремина скупа S строго већа од $2^n d(L)$, онда S садржи бар један чвор решетке различит од координатног почетка.*

Овде се *детерминанта решетке* $d(L)$ дефинише као запремина *фундаменталног паралелепипеда* решетке. Из дефиниције тривијално је да је за целобројну решетку та запремина једнака 1, па одатле и следи специјалан случај који смо овде доказали.

2.4 Још нека својства целобројне квадратне решетке

Теорема 2.6. *У целобројну квадратну решетку од правилних многоуглова могуће је уписати само правилан четвороугао.*

Доказ 1. Посматрајмо неко $n \in \mathbb{N}$ за које је могуће конструисати овакав n-тоугао. Како многоуглове уписујемо у квадратну решетку, скуп дужина страница је пребројив, па можемо уочити правилан n-тоугао најмање површине који се може уписати у квадратну решетку, нека је то $A_1A_2 \dots A_n$.

Означимо са O координатни почетак, и нека је $B_i, i \in \{1, 2, \dots, n\}$ дефинисано као $\overrightarrow{OB_i} = \overrightarrow{A_iA_{i+1}}$, $A_{n+1} = A_1$. Приметимо да, како су O, A_i, A_{i+1} темена решетке, то мора бити и B_i, па је $B_1B_2 \dots B_n$ такође уписан у решетку. Шта више, он је правилан зато што су углови $\angle B_iOB_{i+1}$ и $\angle A_iA_{i+1}A_{i+2}$ суплементни. Како је из дефинисаности $A_iA_{i+1} \leq B_iB_{i+1}$, имамо да је $A_iA_{i+1} \leq 2A_iA_{i+1} \sin \frac{\pi}{n}$, па је $n \leq 6$, чиме смо показали да за све правилне многоуглове са 7 или више страница овакво уписивање није могуће.

Посматрајмо сада $n \leq 6$. Из аналитичке формуле за тежиште видимо да су координате центра овог правилног многоугла рационалне, па хомотетијом овог многоугла са неким целобројним коефицијентом добијамо правилан многоугао уписан у решетку чији центар такође има целобројне координате. Сада, ако ротирамо овај многоугао око његовог центра редом за углове $\frac{\pi}{2}$, π и $\frac{3\pi}{2}$ добићемо нове тачке, које ће из централне симетрије око центра такође бити целобројне и заједно са почетним тачкама чинити неки нови правилан многоуао. У случају правилног троугла и шестоугла имаћемо 12 тачака, а у случају правилног петоугла 20 тачака, па из претходног дела овакви правилни многоуглови не постоје. Са друге стране, за правилан четвороугао имаћемо само 4 тачке.

Како за квадрат постоји пример са теменима у $(0, 1)$, $(1, 1)$, $(1, 0)$ и $(0, 0)$, овиме смо показали да се од свих правилних многоуглова само квадрат може уписати у квадратну целобројну решетку. □

Доказ 2. Опет, посматрајмо неко $n \in \mathbb{N}$ за које је могуће конструисати овакав n-тоугао. Из Пикове теореме имамо да је његова површина $S(P) = u(P) + \frac{1}{2}v(P) - 1$, па је $2S(P) \in \mathbb{N}$. Са друге стране, знамо да је површина правилног n-тоугла странице дужине L једнака $\frac{1}{4}nL^2 \operatorname{ctg} \frac{\pi}{n}$, па из свега наведеног имамо да $\operatorname{ctg} \frac{\pi}{n}$ мора бити рационалан. Сада није тешко извести да је ово могуће једино за $n = 4$, односно само квадрат се може уписати у целобројну квадратну решетку. □

Први математичар који је приметио неке класе многоуглова које морају садржати бар једну целобројну тачку у унутрашњости је J. P. Аркинштал. Овде наводимо неке од његових резултата.

Став 2.1. *Конвексан трапез уписан у целобројну квадратну решетку мора садржати бар једну целобројну тачку у својој унутрашњости.*

Доказ овог става ћемо прескочити, зато што је идејно сличан доказу следећег тврђења.

Став 2.2. *Конвексан петоугао уписан у целобројну квадратну решетку мора садржати бар једну целобројну тачку у својој унутрашњости.*

Доказ. Нека је конвексан петоугао $ABCDE$ уписан у решетку. Збир његових унутрашњих углова је 3π, па је збир парова узастопних унутрашњих углова једнак 6π. То значи да је збир нека два суседна угла већи од π. Нека је без губљења на општости $\angle A + \angle B > \pi$. Такође, нека је без губљења на општости $d(E, AB) \geq d(C, AB)$. Ако конструишемо паралелограм $ABCX$, јасно је да ће тачка X бити целобројна. Из претходно наведеног имамо да је $\angle BAX < \angle BAE$, а како је $d(E, AB) \geq d(C, AB)$, закључујемо да је тачка X унутар овог петоугла, а како је она целобројна тврђење је доказано. □

Теорема 2.7 (Скотова граница)**.** *За конвексан многоугао уписан у целобројну квадратну решетку важи $v(P) \leq 2u(P) + 7$. Ако P има више од три темена, важи $v(P) \leq 2u(P) + 6$.*

Због опширности и компликованости доказа одлучили смо да га овде не наводимо. Један од начина је да се многоугао упише у правоугаоник и да се разматра низ случајева по броју темена на страницама правоугаоника, а други је индукција по $u(P)$, с тим што базни случај уопште није тривијалан.

Став 2.3 (Колманова лема)**.** *Нека је $ABCDE$ конвексан петоугао уписан у целобројну квадратну решетку. Ако $\triangle ACE$ нема целобројних тачака у унутрашњости, онда дужи AC или CE садрже целобројну тачку у унутрашњости. Специјално, ако AE садржи целобројну тачку у својој унутрашњости, онда тврђење важи и за AC и за CE.*

Доказ. Нека је X чвор решетке у троуглу $\triangle ABC$ најближи страници AC (ако не постоји, узимамо $X = B$). Аналогно за $\triangle CDE$ и страницу CE дефинишемо тачку Y. Из конвексности петоугла $ABCDE$ имамо да је конвексан и петоугао $AXCYE$, па на основу једног од претходно наведених примера закључујемо да он садржи једну тачку у својој унутрашњости. Из дефинисаности X и Y закључујемо да нема целобројних тачака у $\triangle ACX$ и $\triangle CYE$, а како из услова задатка целобројне тачке нема ни у унутрашњости $\triangle ACE$, закључујемо да мора постојати цеобројна тачка на некој од дужи AC и CE.

Докажимо сада други део тврђења, и нека је P целобројна тачка у унутрашњости AE. Без губљења на општости, нека је сада X тачка која се налази на AC, а тачку Y дефинишемо као мало пре, односно као целобројну тачку унутар троугла $\triangle CDE$ која је најближа страници CE (ако таква тачка не постоји, узећемо $Y = D$). Како је петоугао $ABCDE$ конвексан, то мора бити и петоугао $CXPEY$, па на сличан начин као у првом делу доказа закључујемо да мора постојати целобројна тачка и унутар странице CE, чиме је доказ завршен. $\square$

3 Политопи и решетке у просторима димензија већих од 2

Након што смо се упознали са разним својствима многоуглова уписаних у целобројну квадратну решетку, логично је поставити питање да ли се неко од тих тврђења може уопштити и на више димензије, као и шта би био пандам за многоугао у $\mathbb{R}^n$, $n > 2$. Навели смо уопштење теореме Минковског, док је, на пример, показано да се Пикова теорема не може уопштити на еуклидски простор произвољне димензије. Међутим, постоји низ других теорема које се баве овим проблемом. Ми овде представљамо неке од њих, али за почетак уводимо неопходне термине.

Политоп није лако дефинисати, и постоје многе дефиниције. Све је почело од Лудвига Шлафлија, швајцарског математичара који је рекао да је тачка *0-политоп*, права *1-политоп*, раван *2-политоп*, а n-*политоп* је природни наставак овог низа. Међутим, конвексни политоп је много лакше дефинисати. Како ће једино он и бити предмет нашег изучавања, прескачемо дефиницију политопа.

Дефиниција 3.1. ***Хиперраван*** *H је потпростор векторског простора V, такав да ако су n и p вектори из V, важи $H = \{y | n \cdot (y - p) = 0\}$.*

Дефиниција 3.2. ***Конвексни политоп*** *је скуп тачака у $\mathbb{R}^n$ чије су координате решења система једначина*

$$mx \leq b,$$

где је m реална матрица димензија $s \times n$, а b представља s вектор са реалним координатама.

Јасно је да ова дефиниција представља пресек s скупова, где је сваки скуп заправо скуп тачака са исте стране једне хиперравни одређене одговарајућом једначином у систему. Такође, конвексан политоп се може дефинисати на већ познат начин, то јест за дат скуп вектора $\{v_1, v_2, \ldots, v_s\}$ конвексан политоп дефинишемо као

$$P = \{\lambda_1 v_1 + \lambda_2 v_2 + \cdot + \lambda_s v_s | \lambda_i \geq 0, \lambda_1 + \lambda_2 + \cdot + \lambda_s = 1\}.$$

Дефиниција 3.3. ***Димензија*** *политопа P дефинише се као димензија најмањег афиног простора који садржи P. Ако је димензија политопа d, пишемо $\dim P = d$.*

Из дефиниције димензије очито је да политоп у $\mathbb{R}^n$ не мора имати димензију d, већ само мора важити $\dim P \leq n$.

Дефиниција 3.4. ***Страна*** *конвексног политопа представља пресек хиперравни која одређује политоп и самог политопа.*

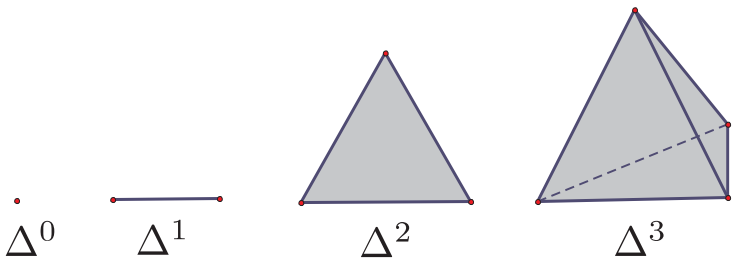
Очито, и страна има своју димензију, а у зависности од те димензије уводимо још два термина.

Дефиниција 3.5. ***Ивица*** *или* ***страница*** *конвексног политопа је страна политопа димензије* 1.

Дефиниција 3.6. ***Теме*** *конвексног политопа је страна политопа димензије* 0.

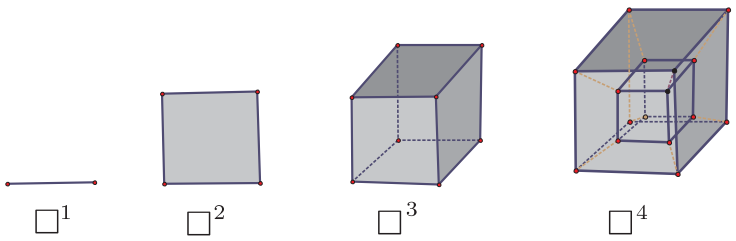
Дефиниција 3.7. *Ако политоп P има димензију d, за њега кажемо да је d-политоп.*

Није тешко показати да d-политоп мора имати бар $d+1$ темена. Конвексан d-политоп који има тачно $d+1$ темена назива се *d-симплекс*. Специјално, *стандардни n-симплекс* дефинишемо као $\triangle = \operatorname{conv}\{0, e_1, e_2, \ldots, e_n\}$.



Слика 4. Симплекси

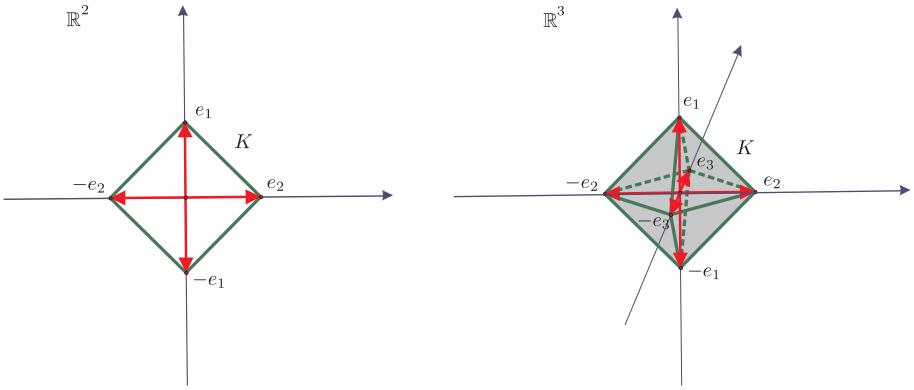
Још један специфичан политоп је *јединична коцка*. Јединичну коцку дефинишемо као $\square = \operatorname{conv}\{x \in \mathbb{R}^n | x \in \pm 1^n\}$. Напокон, *ортоплекс* дефинишемо као $\diamondsuit = \operatorname{conv}\{\pm e_1, \pm e_2, \ldots, \pm e_n\}$, где су $e_1, e_2, \ldots, e_n$ јединични вектори.



Слика 5. Коцке

3.1 Пребројавање целобројних тачака у конвексним политопима

Проблем пребројавања чворова целобројне решетке у конвексном n-политопу знатно је компликованији него што је то био случај код многоуглова. У општем случају, није могуће донети закључке о неким



Слика 6. Ортоплекси

особинама политопа само на основу броја чворова у њему, као што је био случај у равни (на пример, помоћу Пикове теореме лако смо могли израчунати површину многоугла, међутим, овај број нам није довољан да бисмо одредили запремину n-политопа).

Међутим, француски математичар Еуген Ерхарт је дошао на једну другу идеју. Свестан значаја овог податка, он је полазни политоп прво транслирао тако да му координатни почетак постане теме, а затим посматрао политопе које добијамо хомотетичним пресликавањем добијеног политопа у односу на координатни почетак, са целобројним коефицијентима хомотетије. Закључио је да се многе особине политопа могу изразити у функцији од броја целобројних чворова унутар свих добијених политопа, што је управо идеја ове теорије.

Ерхартова теорија је тренутно популарна и веома изучавана област. Готово сви резултати захтевају значајан теоријски увод и предзнање из одговарајућих области, тако да ћемо се ми у овом раду задржати само на основним идејама и терминима ове теорије, као и на неколико најједноставнијих примера.

Дефиниција 3.8. *За посматрани политоп P у $\mathbb{R}^n$, његову t-**дилатацију**, односно tP, дефинишемо као*

$$tP = \{(tx_1, tx_2, \ldots, tx_n) | (x_1, x_2, \ldots, x_n) \in P\}.$$

Дефиниција 3.9. *За дати политоп P уписан у целобројну решетку $\mathbb{Z}^n$ и ненегативан цео број t, са $L_P(t)$ означаваћемо број чворова решетке у tP, односно*

$$L_P(t) = \#(tP \cap \mathbb{Z}^n).$$

Пример 3.1. *Израчунајмо $L_\square(t)$. Како је $\square = \text{conv}\{x \in \mathbb{R}^n | x \in \pm 1^n\} = \{x \in \mathbb{R}^n | -1 \leq x \cdot e_i \leq 1, 1 \leq i \leq n\}$, закључујемо да је $t\square = \{x \in \mathbb{R}^n | -t \leq x \cdot e_i \leq t, 1 \leq i \leq n\}$. Одатле је тривијално да је $L_\square(t) = (2t+1)^n$.*

Пример 3.2. *Слично, за ортоплекс* $\diamondsuit = \{x \in \mathbb{R}^n | \sum_{i=1}^{n} |x \cdot e_i| \leq 1\}$ *је* $t\diamondsuit = \{x \in \mathbb{R}^n | \sum_{i=1}^{n} |x \cdot e_i| \leq t\}$. *Одавде видимо да се проблем своди на налажење броја целобројних решења неједначине* $|x_1| + |x_2| + \cdots + |x_n| \leq t$. *Овај број није тешко наћи, јер ако број оних* i*-ова за које је* $x_i \geq 0$ *и означимо га са* j*, није тешко приметити да је број решења једначине за фиксно* j *заправо* $\binom{t+n-j}{n}$ *(збир* n *природних бројева не сме бити већи од* $t+n-j$*, па распоређујемо* n *преграда на* $t+n-j$ *места). Из свега наведеног закључујемо* $L_{\diamondsuit}(t) = \sum_{j=1}^{n} \binom{n}{j}\binom{t+n-j}{n}$.

Пример 3.3. *За стандардни* n*-симплекс важи* $\triangle = \operatorname{conv}\{0, e_1, e_2, \ldots, e_n\} = \{x \in \mathbb{R}^n | x \times e_i \geq 0, \sum_{i=1}^{n} x \times e_i \leq 1\}$, *па је* $t\triangle = \{x \in \mathbb{R}^n | x \times e_i \geq 0, \sum_{i=1}^{n} x \times e_i \leq t\}$. *Сада се проблем своди на налажење броја решења неједначине* $x_1 + x_2 + \cdots + x_n \leq t$, *што се може израчунати слично као у претходном примеру, па је* $L_{\triangle}(t) = \binom{t+n}{n}$.

Теорема 3.1 (Ерхартова теорема)**.** *Ако је* $P \subset \mathbb{R}^n$ d*-политоп уписан у целобројну решетку одговарајуће димензије, и ако посматрамо политоп* tP *за неко ненегативно цело* t*,* $L_P(t)$ *се може представити као полином степена* d *по* t*, односно* $L_P(t) = c_0 + c_1 t + \cdots + c_d t^d$. *Овај полином назива се* ***Ерхартовим полиномом*** *политопа* P *за цео ненегативан број* t.

Доказ ове теореме је веома захтеван. Пре него што пређемо на њега, докажимо једну лему:

Лема 3.1. *Нека је* $f : Z_{\geq 0} \to C$*, и* d *ненегативан цео број. Тада су следећа тврђења еквивалентна:*

1. *За све* $t \geq 0$, $\sum_{k=0}^{d+1} (-1)^{d+1-k} \binom{d+1}{k} f(t+k) = 0$.
2. *Постоји полином степена* $\leq d$ *који узима исте вредности као* $f(t)$ *у свим ненегативним целим тачкама.*

Доказ. Тврђење доказујемо индукцијом по d. Ако је $d = 0$, тврђење је очито тривијално ($f(t+1) - f(t) = 0$ у целобројним тачкама). Претпоставимо да је $d > 0$, и да тврђење важи за $d - 1$.
Претпоставимо да важи друга ставка. Нека је $g(t) = f(t+1) - f(t)$

полином степена $d-1$, и на основу индуктивне хипотезе важи:

$$0 = \sum_{k=0}^{d} (-1)^{d-k} \binom{d}{k} (f(t+1+k) - f(t+k))$$

$$= \sum_{k=1}^{d+1} (-1)^{d-k+1} \binom{d}{k-1} f(t+k) + \sum_{k=0}^{d} (-1)^{d-k+1} \binom{d}{k} f(t+k)$$

$$= f(t+d+1) + (-1)^{d+1} f(t) + \sum_{k=1}^{d} (-1)^{d-k+1} \binom{d+1}{k} f(t+k)$$

$$= \sum_{k=0}^{d+1} (-1)^{d-k+1} \binom{d+1}{k} f(t+k).$$

За други смер, претпоставимо да важи прва ставка. Слично као малопре, видимо да функција $g(t) = f(t+1) - f(t)$ задовољава први услов (сада смо гледали $d-1$ уместо d, остатак извођења је исти), па на основу индуктивне хипотезе закључујемо да постоји полином степена $\leq d-1$ који се поклапа са $g(t)$ у свим целобројним тачкама. Како је $f(t+1) = f(t) + g(t)$, а индукцијом тривијално показујемо да је онда $f(t+1) = f(0) + \sum_{k=0}^{t} g(k)$, видимо да и за $f(t)$ постоји одговарајући полином, па је довољно показати да је степен тог полинома $\leq d$. Ако разбијемо претходно наведену суму на мономе, видимо да се задатак своди на доказивање да је $\sum_{k=0}^{t} k^r$ полином $r+1$-вог степена. □

Вратимо се сада на доказ Ерхартове теореме. Показаћемо да је за све $t \geq 0$

$$L_P(t+d+1) = \sum_{k=0}^{d} (-1)^{d-k} \binom{d+1}{k} L_P(t+k).$$

На основу претходне леме тиме бисмо показали да је $L_P(t)$ заправо полином по t. Ако извршимо триангулацију политопа P на симплексе, применом принципа укључења-искључења $L_P(t)$ постаје сума полинома са одговарајућим знацима, дакле полином, па без губљења на општости можемо претпоставити да је P симплекс.

Нека су $\{v_0, v_1, \ldots, v_d\}$ темена P и t фиксан ненегативан цео број. За свако теме v_i дефинишемо $Q_i := (t+d)P + v_i$. Дефинишимо и $Q := \bigcup_i Q_i$. Прво, покажимо да је $Q = (t+d+1)P$. Јасан је смер $Q \subset P$. Како је $(t+d+1)P = \{\sum_{i=0}^{d} a_i v_i | a_i \geq 0, \sum_{i=0}^{d} a_i = t+d+1\}$, за свако $p = a_0 v_0 + a_1 v_1 + \cdot + a_d v_d \in (a+d+1)P$ мора постојати неко j такво да је $a_j \geq 1$ (овде користимо претпоставку да је P симплекс). Дакле, $p \in Q_j$, па је и $p \in Q$, из чега закључујемо $P \subset Q$. Коначно, показали смо да је $P = Q$.

Са друге стране, пребројмо целобројне тачке унутар Q.

$$\begin{aligned} Q_j &= (t+d)P + v_j \\ &= \left\{ v_j + \sum_{i=0}^{d} (t+d)c_i v_i | c_i \geq 0, \sum_{i=0}^{d} c_i = 1 \right\} \\ &= \left\{ \sum_{i=0}^{d} a_i v_i | a_i \geq 1 \text{ ако } i \in I, \sum_{i=0}^{d} a_i = t+d+1 \right\}. \end{aligned}$$

Како је за свако $I \subset D, D := \{0, 1, \ldots, d\}$,

$$\bigcap_{i \in I} Q_i = \left\{ \sum_{i=1}^{d} a_i v_i | a_i \geq 1 \text{ ако } i \in I, \sum_{i=0}^{d} a_i = t+d+1 \right\} = (t+d+1-\#I)P + \sum_{i \in I} v_i,$$

принципом укључења-искључења закључујемо:

$$\begin{aligned} \#(Q \cap \mathbb{Z}^n) &= \sum_{k=1}^{d+1} (-1)^{k+1} \sum_{I \subset D, \#I = k} \#(\bigcap_{i \in I} Q_i \cap \mathbb{Z}^n) \\ &= \sum_{k=1}^{d+1} (-1)^{k+1} \binom{d+1}{d+1-k} L_P(t+d+1-k) \\ &= \sum_{k=0}^{d} (-1)^{d-k} \binom{d+1}{k} L_P(t+k). \end{aligned}$$

Дакле, показали смо тврђење са почетка доказа, па смо тиме доказали и да је $L_P(t)$ полином по t степена $\leq d$. Дакле, потребно је још доказати да је степен полинома тачно d. Можемо претпоставити да је једно теме политопа координатни почетак (транслирамо га по потреби). Како је P d-политоп, његова темена $v_1, v_2, \ldots, v_d$ су линеарно независна. За природне бројеве $k_1, k_2, \ldots, k_d \leq t$, тачке $k_1 v_1 + \cdot + k_d v_d$ су све унутар $dtP \cap \mathbb{Z}^n$, и све оне су различите за различите изборе k-ова. Дакле, $L_P(dt) \geq t^d$, па посматрањем довољно великог t закључујемо да је степен полинома бар d, односно да из претходног мора бити тачно d. Овиме је Ерхартова теорема доказана. □

Интересантно је да би слично тврђење важило и ако посматрани политоп не би био уписан у решетку, већ је довољно да му све координате буду рационални бројеви. Тада, међутим, $L_P(t)$ постаје квазиполином по t, односно уместо коефицијената c_i, $1 \leq i \leq n$, имамо периодичне функције $c_i(t), c_i : \mathbb{Q} \to \mathbb{Z}$. Међутим, у овом раду ће нас занимати искључиво целобројни политопи, тако да се на овоме нећемо задржавати.

3.2 Дискретна и непрекидна запремина политопа

Овде ћемо представити крајње неформалну дефиницију запремине политопа, која је као појам ипак интуитивно јасна.

Дефиниција 3.10. *Запремина политопа дефинише се као ненегативан реалан број* $\mathrm{vol}(P) = \int_P dV$.

Ово се може замислити као попуњавање политопа малим d-коцкама странице $\frac{1}{t}$, где је запремина овакве коцке $\frac{1}{t^d}$. Како смањујемо страницу коцке, ово можемо замислити и као рачунање $\#(P \cap (\frac{1}{t}\mathbb{Z})^n)$ и множење тог броја са запремином једне коцке. Дакле, одавде видимо да би следећа дефиниција запремине политопа била еквивалентна оној нама познатој.

Дефиниција 3.11. *Запремина d-политопа $P \subset \mathbb{R}^n$ је ненегативан реалан број* $\mathrm{vol}(P) = \lim_{t\to+\infty} \frac{1}{t^d}\#(P \cap (\frac{1}{t}\mathbb{Z})^n)$.

Дефиниција 3.12. *Релативна запремина d-политопа $P \subset \mathbb{R}^n$ је ненегативан реалан број* $\mathrm{relvol}\, P = \lim_{t\to+\infty} \frac{1}{t^{d-1}}\#(tP \cap \mathbb{Z}^n)$.

Теорема 3.2. *Нека је $P \subset \mathbb{R}^n$ d-политоп, $\mathbb{Z}^d$ целобројна решетка, и нека је $L_P(t) = c_0 + c_1 t + \cdot + c_d t^d$ Ерхартов полином политопа P. Тада важи:*

1. $c_d = \mathrm{vol}(P)$.
2. $c_{d-1} = \frac{1}{2}\sum_F \mathrm{relvol}(F)$, *где се врши сумирање по странама F политопа P.*
3. $c_0 = 1$.

Доказ. Како важи

$$\begin{aligned}\mathrm{vol}(P) &= \lim_{t\to+\infty} \frac{1}{t^d}\#(P \cap (\frac{1}{t}\mathbb{Z})^n) \\ &= \lim_{t\to+\infty} \#(tP \cap \mathbb{Z}^n) \\ &= \lim_{t\to+\infty} L_P(t),\end{aligned}$$

а $\lim_{t\to+\infty} L_P(t) = c_d$, прва ставка је доказана. Како је $1 = L_P(0) = c_0$, и трећа ставка је доказана, док ћемо доказ друге ставке навести касније. □

Често се уместо Ерхартовог полинома користи и Ерхартов ред, а чијим се посматрањем такође могу добити наведени резултати.

Дефиниција 3.13. *Ерхартов ред за дати политоп $P \subset \mathbb{R}^n$ дефинише се као $Ehr_P(x) = 1 + \sum_{t=1}^{+\infty} L_P(t)x^t$.*

Пример 3.4. *За стандардни n-симплекс је*

$$Ehr_{\triangle}(x) = 1 + \sum_{t=1}^{+\infty} \binom{t+n}{n} x^t = \frac{1}{(1-x)^{d+1}}.$$

3.3 Ерхарт-Мекдоналдов реципроцитет

Дефиниција 3.14. *Нека је $P \subset \mathbb{R}^n$ политоп. Ако је P дефинисан помоћу низа неједнакости $mx \leq b$, тада са P° дефинишемо његову унутрашњост, односно све тачке $x \in P$ за које се ни у једној од наведених неједнакости не достиже једнакост. Дефинишемо и $L_{P^\circ}(t) = \#(P^\circ \cap \mathbb{Z}^n)$ Ерхартов полином и одговарајући Ерхартов ред $Ehr_{P^\circ}(x) = 1 + \sum_{t=1}^{+\infty} L_{P^\circ}(t)x^t$.*

Теорема 3.3. *(Ерхарт-Мекдоналдов реципроцитет) Ако је $P \subset \mathbb{R}^n$ политоп, важи*

$$L_{P^\circ}(t) = (-1)^d L_P(-t)$$

и

$$Ehr_P(\frac{1}{x}) = (-1)^{d+1} Ehr_{P^\circ}(x).$$

Због дужине и комплексности доказа, овде ћемо га прескочити. Помоћу овог тврђења можемо доказати и другу ставку у Теореми 3.2. Наиме, ако приметимо

$$\begin{aligned}
\sum_F \mathrm{vol}(F) &= \mathrm{relvol}(P) - \mathrm{relvol}(P^\circ) \\
&= \lim_{t\to+\infty} \frac{1}{t^{d-1}} \#(tP \cap \mathbb{Z}^n) - \lim_{t\to+\infty} \frac{1}{t^{d-1}} \#(tP^\circ \cap \mathbb{Z}^n) \\
&= \lim_{t\to+\infty} \frac{1}{t^{d-1}} (L_P(t) - (-1)^d L_P(-t)) \\
&= 2 \lim_{t\to+\infty} \frac{1}{t^{d-1}} (c_{d-1}t^{d-1} + c_{d-3}t^{d-3} + \cdot) \\
&= 2c_{d-1},
\end{aligned}$$

видимо да тврђење одмах следи.

4 Фробениусов проблем

У уводу смо рекли да се многи проблеми могу интерпретирати помоћу елемената целобројне решетке. Овде дајемо један такав пример на решавању Фробениусовог проблема (или Проблема новчића). Навешћемо тврђење Фробениусовог проблема у општем случају:

Дефиниција 4.1. *Нека је $A = \{a_1, a_2, \ldots, a_n\}$ скуп природних бројева, и нека је $m \in \mathbb{N}$. Тада за број m кажемо да се може **репрезентовати** помоћу елемената скупа A ако постоје ненегативни цели бројеви x_1, x_2,..., x_n такви да је $m = x_1a_1 + x_2a_2 + \cdots + x_na_n$, и тада се овај израз назива **репрезентацијом броја** m **помоћу бројева из** A.*

Теорема 4.1 (Фробениусов проблем)**.** *Дат је скуп $A = \{a_1, a_2, \ldots, a_n\}$ природних бројева, таквих да је $NZD(a_1, a_2, \ldots, a_n) = 1$. Ако је $R(A)$ скуп свих природних бројева који се могу репрезентовати помоћу бројева из A, тада постоји $g(a_1, a_2, \ldots, a_n) = \max\{m | m \in \mathbb{Z}\backslash R(A)\}$. Овај број називамо **Фробениусовим бројем скупа A**, а сам скуп A **скупом генератора**.*

Дефиниција 4.2. *За скуп генератора $A = \{a_1, a_2, \cdot, a_n\}$ и неки природан број k функцију $p_A : \mathbb{N} \to \mathbb{N} \cup \{0\}$ дефинишемо као*

$$p_A(k) = \#\left\{(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n | (\forall i) x_i \geq 0, x_1 + x_2 + \cdot + x_n = k\right\}.$$

Иако није тешко показати да овај број постоји, показано је да не постоји општа формула за рачунање Фробениусовог броја за фиксан број генератора $n \geq 3$. Постоји метода која користи генераторне функције и помоћу које се (често само уз помоћ рачунара) може одредити за дате генераторе.

Овде ћемо показати једну занимљиву интерпретацију овог проблема помоћу решетки, као и решење проблема и још нека лепа својства за $n = 2$. На крају, дајемо и најпознатији доказ самог проблема за произвољно n.

4.1 Геометријски приступ

Нека је $A = \{a_1, a_2, \ldots, a_n\}$, $NZD(a_1, a_2, \ldots, a_n)$, $a_i > 1$ скуп генератора (ако је неко $a_i = 1$, очито постоји репрезентација за сваки природан број). Посматрајмо следећи скуп:

$$P = \{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n | x_1a_1 + x_2a_2 + \cdots + x_na_n = 1\}.$$

Јасно је да је овај скуп један политоп. Како је за неко природно k, $p_A(k) = \#\left\{(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n | (\forall i) x_i \geq 0, x_1 + x_2 + \cdot + x_n = k\right\}$,

видимо да је
$p_A(k)$ заправо број чворова решетке $\mathbb{R}^n$ у политопу kP, односно важи $p_A(k) = L_P(k)$. Дакле, овиме смо повезали Фробениусов број за произвољни скуп генератора са Ерхартовом теоријом. Тако за дат скуп генератора пребројавањем целобројних чворова у одређеном политопу можемо одредити да ли се тај број може репрезентовати или не. Управо овом методом су добијена решења проблема за одређене класе скупова генератора, што се стандардним методама за решавање Диофантских једначина не може урадити.

4.2 Фробениусов број за два генератора

Пошто смо већ споменули овај проблем, наводимо и најпознатије резултате за $n = 2$. Оба резулата се приписују Силвестеру.

Теорема 4.2. *Нека су a и b узајамно прости природни бројеви. Тада важи $g(a, b) = ab - a - b$ (специјално, ако је неки од ових бројева -1 добијамо $g(a, b) = -1$, што значи да су сви природни бројеви репрезентативни).*

Доказ. Како је $NZD(a, b) = 1$, сваки природан број c може се представити као $c = xa + yb$, $x, y \in \mathbb{Z}$. Такође, приметимо да, ако је $0 \leq x \leq b-1$, ово представљање мора бити јединствено (ово је потпун систем остатака по модулу b, па не могу постојати два оваква представљања). Дакле, за сваки цео број c постоје $x, y \in \mathbb{Z}$ такви да важи $c = xa + yb, 0 \leq x \leq b - 1$.

Приметимо сада да број није репрезентативан ако и само ако у последњем представљању важи $y < 0$. Како су a и b природни бројеви, одавде следи да је највећи број који није репрезентативан заправо

$$g(a, b) = (b - 1)a + (-1)b = ab - a - b,$$

што је и требало доказати. □

Теорема 4.3 (Силвестерова теорема)**.** *За скуп генератора $A = (a, b)$, где су a и b узајамно прости природни бројеви, тачно пола од бројева из скупа $\{1, 2, \ldots, ab - a - b + 1\}$ није репрезентативно.*

Доказ. Већ смо показали да је $ab - a - b + 1$ репрезентативан, а да $ab - a - b$ није. Од осталих бројева, доказаћемо да је тачно један од бројева z и $ab - a - b - z$ репрезентативан (z је природан број мањи од $ab - a - b$). Јасно је да ако је један од ова два броја репрезентативан, онда други не може бити (иначе је и њихов збир, односно $ab - a - b$ репрезентативан). Дакле, довољно је показати да је бар један од бројева z и $ab - a - b - z$ репрезентативан.

Претпоставимо да неки природан број $z < ab-a-b$ није репрезентативан. Тада га на јединствени начин можемо представити као $z = xa + yb$, где је $0 \leq x \leq b-1$, $x, y \in \mathbb{Z}$. Како z није репрезентативан, мора важити $y < 0$. Одатле имамо да је $ab - a - b - z = (b-x-1)a + (-y-1)b$, а како из дефиниције x и y важи $b-x-1 \geq 0$ и $-y-1 \geq 0$, закључујемо да је $ab-a-b-z$ репрезентативан, чиме је доказ завршен. □

За крај, представљамо и доказ самог Фробениусовог проблема:

Тврђење доказујемо индукцијом по n, $n \geq 2$. База следи директно из Силвестерове теореме. Претпоставимо да тврђење важи за неких n генератора и докажимо га за $n+1$. Нека је $A = \{a_1, a_2, \ldots, a_{n+1}\}$ скуп генератора таквих да је $NZD(a_1, a_2, \ldots, a_{n+1}) = 1$ и нека је $NZD(a_1, a_2, \ldots, a_n) = d$. Очито је $NZD(a_{n+1}, d) = 1$. Из индуктивне хипотезе примењене на скуп генератора $B = \{\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\}$, постоји $u = g(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d})$. Нека је $v > u$ најмањи природан број узајамно прост са a_{n+1}. Тада је из претходно наведеног број dv репрезентативан помоћу $a_1, a_2, \ldots, a_n$, па како је $NZD(a_{n+1}, dv) = 1$, постоји $g(a_{n+1}, dv)$. Одатле следи да се након неког природног броја сви могу репрезентовати помоћу бројева из A, односно природних бројева који се не могу репрезентовати има коначно много, па је тиме показано да и $g(a_1, a_2, \ldots, a_{n+1}$ постоји. Овиме је доказ индукцијом завршен. □

Литература

[1] M. Beck, S. Robins, *Computing the Continuous Discretely*, Springer Science+Business Media, LLC ISBN 978-0-387-29139-0

[2] Stanley Rabinowitz, *On the Number of Lattice Points Inside a Convex Lattice n-gon*, Congressus Numerantium, 73(1990)99-124

[3] M. Berger, *Geometry Revealed*, Springer-Verlag Berlin Heidelberg 2010, ISBN 978-3-540-70997-8

[4] Steven V. Sam, Kevin M. Woods, *A finite calculus approach to Ehrhart polynomials*, Electron. J. Combin. 17 (2010), no. 1, Research Paper 68, 13pp.

[5] Steven V. Sam, *A bijective proof for a theorem of Ehrhart*, Amer. Math. Monthly 116 (2009), no. 8, 688-701

[6] B. J. Braun, *Ehrhart Theory for Lattice Polytopes*, Washington University 2007

[7] Paul Yiu, *Recreational Mathematics*, Florida Atlanitc University 2003

[8] J. Garbett, *Lattice Point Geometry: Pick's Theorem and Minkowski's Theorem*, Kenyon College 2010