NYILATKOZAT

Név: Tiderenczl Dániel

ELTE Természettudományi Kar, szak: Matematika Bsc

NEPTUN azonosító: DNJ1LW

Szakdolgozat címe:
A rácsok geometriája

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2023.06.01.

Tiderenczl Dániel

a hallgató aláírása

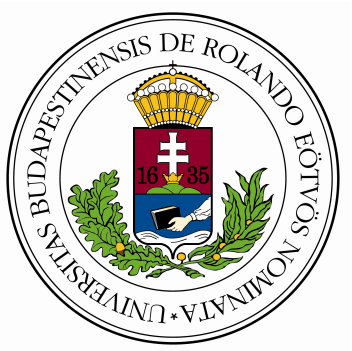
Eötvös Loránd Tudományegyetem
Természettudományi Kar

Tiderenczl Dániel

A rácsok geometriája

Szakdolgozat
Matematika BSc

Témavezető:
Csikós Balázs
egyetemi docens



Budapest, 2023

Tartalomjegyzék

Köszönetnyilvánítás

Szeretnék köszönetet mondani témavezetőmnek, Csikós Balázsnak, aki ezt a rendkívül érdekes témát ajánlotta a szakdolgozatom megírásához, és útmutatásaival segítette munkámat.

Továbbá szeretném megköszönni egyetemi oktatóimnak és középiskolai tanáraimnak, hogy matematikai tudásuk átadásával hozzájárultak az előrehaladásomhoz.

Nem utolsó sorban pedig szeretném kifejezni hálámat a családomnak, akik egyetemi tanulmányaim alatt is mindvégig támogattak.

1. Bevezetés

A középkortól kezdődően sok neves matematikus foglalkozott olyan problémákkal, amelyek a rácsok geometriájához fűződnek. Azonban a matematika ezen ágának valódi kezdetét 1891-re teszik, amikor Hermann Minkowski publikálta híres tételét. Ezt az eredményt a rácsok geometriájának alappilléreként szokás említeni. Azóta számos szép rácsgeometriai és számelméleti alkalmazására derítettek fényt.

Szakdolgozatom 3. fejezetének első felében főként Cassels [1] könyvének a segítségével ezen tételt és általánosításait járom körül, valamint néhány érdekes számelméleti alkalmazására is mutatok példát. Ide sorolható például a diofantikus approximáció és a híres négy négyzetszám tétel bizonyítása is. A fejezet másik részében bevezetem a szukcesszív minimumok fogalmát, és velük, valamint origóra szimmetrikus konvex testek rácspontjainak a számával kapcsolatos tételeket mutatok be. Ezek közé tartozik Minkowski második tétele is, amelyből könnyedén bebizonyítható az eredeti. A 4. fejezetben olyan halmazokkal kapcsolatos erdményekről írok, amelyek egy adott rács origóján kívül nem tartalmaznak más rácspontokat. Ide tartozik például egy meglehetősen összetett tétel is, amellyel Minkowski a pályafutása végén rengeteget foglalkozott, de csak 1944-ben sikerült Edmund Hlawkának bebizonyítania. Végül utolsó témakörként a rácsok geometriájának egy az eddigiektől eltérő szép szegmenséről, a rácspolitópokról is tárgyalok néhány érdekességet, amelyekhez Gruber [3] művét használtam fel.

2. Előkészületek

2.1. Definíció. Legyenek $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ lineárisan független vektorok az n-dimenziós euklideszi térben. A

$$\Lambda = \{u_1\boldsymbol{v}_1 + \cdots + u_n\boldsymbol{v}_n : u_1, \ldots, u_n \in \mathbb{Z}\}$$

ponthalmazt rácsnak nevezzük, amelynek a bázisa $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$.

A csupa egész koordinátájú vektorokból álló rácsot $\mathbb{R}^n$-ben Λ_0-val fogjuk jelölni. Jelölje $A = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ azt az $n \times n$-es mátrixot, amelynek i-edik oszlopa $\boldsymbol{v}_i$.
Ha a Λ rács bázisa $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$, akkor Λ pontjai éppen az $A\boldsymbol{p}$, $\boldsymbol{p} \in \Lambda_0$, pontok, azaz $\Lambda = A\Lambda_0$. Vagyis tetszőleges Λ rácshoz létezik olyan $A \in \mathbb{R}^{n\times n}$-es nemszinguláris mátrix, amivel $\Lambda = A\Lambda_0$.

2.2. Lemma. Legyen a Λ egy bázisa $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$, $A = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$. Ekkor a $\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_n \in \Lambda$ vektorok pontosan akkor alkotják a Λ bázisát, ha a $B = (\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_n)$ mátrixhoz létezik olyan $U \in \mathbb{Z}^{n\times n}$ unimoduláris (azaz ±1-determinánsú) mátrix, amivel $B = AU$.

Bizonyítás. Ha létezik olyan $U \in \mathbb{Z}^{n\times n}$ unimoduláris mátrix, amivel $B = AU$, akkor U és U^{-1} egész mátrixok, így $\Lambda_0 = U\Lambda_0$. Ekkor $B\Lambda_0 = AU\Lambda_0 = A\Lambda_0 = \Lambda$, így B is a Λ bázisa.
Megfordítva, ha B is a Λ bázisa, akkor $A\Lambda_0 = \Lambda = B\Lambda_0$, vagyis $A^{-1}B = U_0$ esetén $U_0\Lambda_0 = \Lambda_0 = U_0^{-1}\Lambda_0$, azaz $U_0, U_0^{-1} \in \mathbb{Z}^{n\times n}$. Ekkor a determinánsok szorzástétele szerint U_0 unimoduláris. □

2.2.1. Következmény. Ha a Λ rács két bázisa $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ és $\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_n$, akkor

$$\det(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = \pm\det(\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_n).$$

Ezért $d(\Lambda) = |\det(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)|$ nem függ attól, hogy Λ melyik bázisát választjuk. Mivel a bázis lineárisan független vektorokból áll, így $d(\Lambda) > 0$.

2.3. Definíció. Ezt a $d(\Lambda)$ számot a Λ rács determinánsának nevezzük.

2.4. Lemma. Minden rács az $\mathbb{R}^n$ tér diszkrét additív részcsoportja.

Bizonyítás. Legyen Λ egy $B = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ bázisú rács. Ekkor tetszőleges $\boldsymbol{a}, \boldsymbol{b} \in \Lambda$ pontok $u_1\boldsymbol{v}_1 + \cdots + u_n\boldsymbol{v}_n$ $(u_1, \ldots, u_n \in \mathbb{Z})$ alakban írhatók,

és $\boldsymbol{a}-\boldsymbol{b}$ is ilyen alakú. Ezért Λ az $\mathbb{R}^n$ additív részcsoportja. Tetszőleges $\boldsymbol{c} \in \Lambda$ pontra és a $K = \{\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n : |x_j| \leq 1; j = 1, \ldots, n\}$ kockára Λ-nak nincsen $\boldsymbol{c}$-en kívül más $\boldsymbol{c} + BK$ alakú pontja. Mivel BK tartalmaz egy megfelelő $r > 0$-nál nem nagyobb sugarú gömböt, így bármely két különböző Λ-beli pont távolsága minimum r. Vagyis Λ diszkrét. □

2.5. Lemma. Ha Λ az $\mathbb{R}^n$ térnek egy olyan diszkrét additív részcsoportja, amely nincs benne egy $(n-1)$-dimenziós lineáris altérben, akkor Λ egy rács.

Bizonyítás. Egy eljárást adunk n különböző $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ pont választására, és megmutatjuk, hogy Λ egy olyan rács, amelynek $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ a bázisa.
Mivel Λ diszkrét, így tudunk választani egy olyan $\boldsymbol{v}_1 \in \Lambda$ origótól különböző pontot, hogy az origót és $\boldsymbol{v}_1$-et összekötő szakaszon ne legyen más Λ-beli pont. Tegyük fel, hogy a $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1}$ pontokat már induktívan megválasztottuk, és legyen $L_{j-1} = span\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1}\}$. Vegyünk egy tetszőleges $\boldsymbol{a} \in \Lambda$ pontot, ami nincs benne L_{j-1}-ben, és jelölje az $\boldsymbol{a}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1}$ pontok által kifeszített j-dimenziós paralelopipedont P_j. Ekkor $\boldsymbol{a} \in P_j \cap \Lambda$ miatt $P_j \cap \Lambda \neq \emptyset$, és mivel Λ diszkrét, így P_j-ben csak véges sok Λ-beli pont lehet. Ezek közül válasszunk egy olyat $\boldsymbol{v}_j$-nek, amelynek L_{j-1}-től való távolsága az L_{j-1}-től való pozitív távolságok közül minimális. Ha a $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ pontokat az eljárásnak megfelelően választottuk meg, akkor

$$\boldsymbol{v}_1 \neq \boldsymbol{0} \text{ és } \boldsymbol{v}_j \notin L_{j-1} \ (j = 2, \ldots, n)$$

miatt $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ lineárisan független Λ-beli pontok. Mivel Λ additív csoport, így minden $u_1\boldsymbol{v}_1 + \cdots + u_n\boldsymbol{v}_n$ $(u_1, \ldots, u_n \in \mathbb{Z})$ alakú pont Λ-beli. Már csak azt kell megmutatni, hogy Λ-nak nincsen más pontja. Legyen $\boldsymbol{b} \in \Lambda$ tetszőleges pont. Mivel Λ az $\mathbb{R}^n$ részcsoportja, így $\boldsymbol{b} = r_1\boldsymbol{v}_1 + \cdots + r_n\boldsymbol{v}_n$ alakban írható megfelelő $r_1, \ldots, r_n \in \mathbb{R}$ számokkal. Mivel Λ csoport, így

$$\boldsymbol{b}' = (r_1 - \lfloor r_1 \rfloor)\boldsymbol{v}_1 + \cdots + (r_n - \lfloor r_n \rfloor)\boldsymbol{v}_n \in \Lambda.$$

A $\boldsymbol{v}_n$ pontot úgy választottuk a $P_j \cap \Lambda$-beli pontok közül, hogy távolsága L_j-től az L_j-től való pozitív távolságok közül minimális legyen, így csakis $r_n - \lfloor r_n \rfloor = 0$ lehet. Ugyanígy adódik, hogy $r_{n-1} - \lfloor r_{n-1} \rfloor = 0, \ldots, r_1 - \lfloor r_1 \rfloor = 0$, vagyis $r_1, \ldots, r_n \in \mathbb{Z}$. Ez bizonyítja, hogy Λ egy $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ bázisú rács. □

Megjegyzés. Legyenek $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ a Λ rács lineárisan független pontjai. Ekkor az előző lemma bizonyításában $j = 1, \ldots, n$-re a j-edik lépésben $\boldsymbol{a}$-t $\boldsymbol{a}_j$-nek választva $\boldsymbol{v}_j \in span\{\boldsymbol{a}_j, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1}\}$, ami $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ lineáris függetlensége miatt ekvivalens azzal, hogy $\boldsymbol{a}_j \in span\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_j\}$.
Tehát azt kaptuk, hogy tetszőleges $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \in \Lambda$ lineárisan független pontokra létezik Λ-nak egy olyan $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ bázisa, hogy $j = 1, \ldots, n$-re

$$\boldsymbol{a}_j \in span\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_j\}.$$

Sőt, a következő lemma szerint ennél erősebb állítás is igaz.

2.6. Lemma. Tetszőleges $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n \in \Lambda$ lineárisan független pontokra és Λ rácsra létezik Λ-nak egy olyan $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ bázisa, hogy $j = 1, \ldots, n$-re megfelelő $u_{ij} \in \mathbb{Z}$ számokkal

$$\boldsymbol{a}_j = u_{1j}\boldsymbol{v}_1 + \cdots + u_{jj}\boldsymbol{v}_j, \text{ ahol}$$

$$u_{jj} > 0 \text{ és } u_{jj} > u_{ij} \geq 0 \ (j = 1, \ldots, n; i < j).$$

Bizonyítás. A megjegyzés szerint létezik Λ-nak olyan $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ bázisa és $j = 1, \ldots, n$; $i = 1, \ldots, j$-re léteznek olyan $u_{i,j} \in \mathbb{Z}$ számok, amikre $\boldsymbol{a}_j = u_{1,j}\boldsymbol{v}_1 + \cdots + u_{j,j}\boldsymbol{v}_j$. Rögzített j-re legyen

$$\boldsymbol{v}'_j = \pm(\boldsymbol{v}_j - s_{1,j}\boldsymbol{v}_1 - \cdots - s_{j-1,j}\boldsymbol{v}_{j-1}),$$

ahol az $s_{1,j}, \ldots, s_{j-1,j} \in \mathbb{Z}$ számokat és az előjelet később választjuk meg. Ekkor $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1}, \boldsymbol{v}'_j, \boldsymbol{v}_{j+1}, \ldots, \boldsymbol{v}_n$ is bázisa Λ-nak, és

$$\boldsymbol{a}_j = (u_{1,j} + s_{1,j}u_{j,j})\boldsymbol{v}_1 + \cdots + (u_{j-1,j} + s_{j-1,j}u_{j,j})\boldsymbol{v}_{j-1} \pm u_{jj}\boldsymbol{v}'_j.$$

Az $s_{1,j}, \ldots, s_{j-1,j} \in \mathbb{Z}$ számokat és az előjelet úgy választjuk meg, hogy $i = 1, \ldots, j-1$-re

$$\pm u_{j,j} > 0 \text{ és } 0 \leq u_{i,j} + s_{i,j}u_{j,j} < |u_{j,j}|$$

teljesüljenek. Ekkor $j = 1, \ldots, n$-re a $\boldsymbol{v}_j$ báziselemet $\boldsymbol{v}'_j$-re cserélve egy a lemma állításának megfelelő bázist kapunk. □

Sőt, ha $j = 1, \ldots, n$-re $u_{j,j} = 1$, akkor minden Λ-beli rácspont felírható $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ lineáris kombinációjaként, így $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ bázisa Λ-nak. Ennek az eredménynek a felhasználásával adódik egy egyszerű kritérium annak az eldöntésére, hogy egy síkbeli rács két lineárisan független pontja bázist alkot-e. Az alábbi következménynek a 3. fejezeteben egy szép alkalmazását is meg fogjuk mutatni.

2.6.1. Következmény. Legyen $\boldsymbol{a}_1$ és $\boldsymbol{a}_2$ a $\Lambda \subset \mathbb{R}^2$ rács két lineárisan független rácspontja. Ha $conv\{\mathbf{0}, \boldsymbol{a}_1, \boldsymbol{a}_2\}$-ben nincs más Λ-beli pont, akkor $\boldsymbol{a}_1, \boldsymbol{a}_2$ a Λ rács bázisa.

Bizonyítás. $\boldsymbol{v}_1, \boldsymbol{v}_2$ legyen a Λ bázisa úgy, hogy az $u_{1,1} > 0$ és $0 \leq u_{2,1} < u_{2,2}$ egészekkel $\boldsymbol{a}_1 = u_{1,1}\boldsymbol{v}_1$ valamint $\boldsymbol{a}_2 = u_{2,1}\boldsymbol{v}_1 + u_{2,2}\boldsymbol{v}_2$ teljesüljön. Mivel $\boldsymbol{a}_1$-et és az origót összekötő szakasz belsejében nincs Λ-beli pont, így $u_{1,1} = 1$. Vagyis ha $u_{2,2} = 1$ is teljesül, akkor $\boldsymbol{a}_1, \boldsymbol{a}_2$ valóban a Λ bázisa. Tegyük fel indirekt módon, hogy $u_{2,2} \geq 2$. Ekkor a $conv\{\mathbf{0}, \boldsymbol{a}_1, \boldsymbol{a}_2\}$ háromszöglemez $u_{2,1} = 0$ esetén tartalmazza a $\boldsymbol{v}_2$ rácspontot, $u_{2,1} \geq 1$ esetén pedig a $\boldsymbol{v}_1 + \boldsymbol{v}_2$ rácspontot. Ez ellentmondás, tehát $u_{2,2} = 1$. □

2.7. Definíció. Legyenek adottak a $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ bázisú Λ rácsban az $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ vektorok. (Ekkor $\boldsymbol{a}_i = \sum_{j=1}^{n} u_{ij}\boldsymbol{v}_j$ alakban írhatók, ahol u_{ij}-ek egész számok.) A $|\det(u_{ij})| = \frac{|\det(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_n)|}{|\det(\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n)|}$ szám az $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ vektorok indexe Λ-ban.

2.8. Definíció. Ha a Λ' rács minden pontja egyben a Λ rácsnak is pontja, akkor azt mondjuk, hogy Λ' részrácsa Λ-nak.

Legyenek $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ és $\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_n$ rendre a Λ és Λ' bázisai. Ekkor léteznek olyan u_{ij} számok, amikre $\boldsymbol{v}'_i = \sum_{j=1}^{n} u_{ij}\boldsymbol{v}_j$, mert $\boldsymbol{v}'_j \in \Lambda$.

2.9. Definíció. A $|\det(u_{ij})| = \frac{|\det(\boldsymbol{v}'_1,\ldots,\boldsymbol{v}'_n)|}{|\det(\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n)|} = \frac{d(\Lambda')}{d(\Lambda)}$ számot a Λ' rács indexének nevezzük Λ-ban.

A 2.4-es lemma miatt ez megegyezik a Λ' (algebrai értelemben vett) indexével Λ-ban, azaz Λ-nak a Λ'-szerinti jobb-, illetve baloldali mellékosztályainak a számával.

Most pedig vezessük be a keresztpolitópok fogalmát, amely nem kifejezetten rácsgeometriai, azonban a szakdolgozatomban több tétel bizonyításában is hivatkozni fogok rájuk.

2.10. Definíció. A $K_n = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : |x_1| + \cdots + |x_n| \leq 1\}$ ponthalmazt keresztpolitópnak nevezzük.

2.11. Lemma. Egy $K_n \subset \mathbb{R}^n$ keresztpolitóp (n-dimenziós) térfogata

$$V_n(K_n) = \frac{2^n}{n!}$$

.

Bizonyítás. n szerinti teljes indukcióval bizonyítunk. $n = 1$-re az állítás teljesül, mert a $[-1, 1]$ intervallum hossza 2. Tegyük fel, hogy n-ig teljesül az állítás. Az $\mathbb{R}^{n+1}$ térben vegyük fel a K_n keresztpolitópot. Ekkor K_{n+1}-et úgy kapjuk, hogy az $n + 1$-edik dimenzió szerint $\forall t \in [-1, 1]$-re K_n-nek az $1-|t|$-szeresre nagyított változatát t-vel eltoljuk az $n+1$-edik koordinátatengely mentén, és ezeket a hipertesteket egymásra pakoljuk. Szimmetriai okokból az $n - 1$-edik dimenzió szerinti alsó, illetve felső féltérre eső része egybevágó K_{n+1}-nek, így

$$V_{n+1}(K_{n+1}) = 2 \int_0^1 \frac{2^n}{n!}(1-t)^n \, dt = \frac{2^{n+1}}{n!} \left[-\frac{(1-t)^{n+1}}{n+1} \right]_{t=0}^{1} = \frac{2^{n+1}}{(n+1)!}.$$

□

3. Minkowski-tételkör

3.1. Minkowski tétele és általánosításai

Érdekes számtani probléma volt a 19. században egy adott $f\colon \mathbb{R}^n \to \mathbb{R}$ függvényhez olyan nem csupa 0 egész koordinátákból álló $(u_1, \ldots, u_n)$ vektort találni, amelyre $f(u_1, \ldots, u_n) \leq 1$. Ez ekvivalens azzal, hogy a $\mathbb{Z}^n$ rács egy olyan origótól különböző rácspontját keressük, amely benne van az $\{\boldsymbol{x} : f(\boldsymbol{x}) \leq 1\}$ halmazban. Ennek hatására kezdett Minkowski azzal foglalkozni, hogy milyen feltételek mellett tartalmaz egy adott halmaz biztosan egy az origótól különböző rácspontot.

3.1. Tétel (Minkowski-féle konvex test tétel)**.** *Minden $\mathbb{R}^n$-beli, origóra szimmetrikus, $V(H) > 2^n$ térfogatú konvex H test tartalmaz minimum egy origótól különböző, egész koordinátákkal rendelkező pontot.*

Minkowski eredetileg ezt a tételt bizonyította be, amelynek segítségével később számos szép eredményre jutottak a matematikusok a rácsgeometria területén. Mi azonban a tételnek egy erősebb változatát fogjuk Blichfeldt tételének a segítségével bebizonyítani.

Megjegyzés. Ez az eredmény éles, hiszen például a 2^n térfogatú $H = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : |x_1| < 1, \ldots, |x_n| < 1\}$ kocka nem tartalmaz a Λ_0 rácsból origótól különböző pontot.

3.2. Tétel (Blichfeldt tétele)**.** *Legyen adott egy k pozitív egész szám, egy $d(\Lambda)$ determinánsú Λ rács és egy $V(H)$ térfogatú $H \subset \mathbb{R}^n$ halmaz. Tegyük fel, hogy az alábbi két lehetőség közül az egyik teljesül:*

- $V(H) > kd(\Lambda)$
- $V(H) = kd(\Lambda)$ *és H kompakt.*

Ekkor létezik H-nak $k+1$ különböző $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_{k+1}$ pontja úgy, hogy a $\boldsymbol{p}_i - \boldsymbol{p}_j$ különbségek mindegyike Λ-beli.

Bizonyítás. Legyen $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n$ a Λ rács bázisa, és $M := \{a_1\boldsymbol{g}_1 + \cdots + a_n\boldsymbol{g}_n : 0 \leq a_i < 1;\ i = 1, \ldots n\}$. Ekkor $d(\Lambda) = |\det(\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n)| = V(M)$.
Legyen $P(\boldsymbol{q}) := \{\boldsymbol{r} \in M : \boldsymbol{q} + \boldsymbol{r} \in H\}$ minden $\boldsymbol{q} \in \Lambda$ rácspontra. Λ pontjai $a_1\boldsymbol{g}_1 + \cdots + a_n\boldsymbol{g}_n$ alakúak, ahol $a_1, \ldots, a_n \in \mathbb{Z}$, ezért a tér

minden $\boldsymbol{p}$ pontja egyértelműen írható fel $\boldsymbol{p} = \boldsymbol{q} + \boldsymbol{r}$ alakban, ahol $\boldsymbol{q} \in \Lambda$ és $\boldsymbol{r} \in M$. Ebből az következik, hogy

$$\sum_{\boldsymbol{q} \in \Lambda} V(P(\boldsymbol{q})) = V(H).$$

Először nézzük a $V(H) > kd(\Lambda)$ esetet.
Mivel minden $\boldsymbol{q} \in \Lambda$-ra $P(\boldsymbol{q}) \in M$, így a skatulya-elv szerint létezik olyan $\boldsymbol{r}_0 \in M$, amire teljesül $i = 1, \ldots, k+1$-re, hogy $\boldsymbol{r}_0 \in P(\boldsymbol{q}_i)$. Tehát a $\boldsymbol{p}_i = \boldsymbol{r}_0 + \boldsymbol{q}_i$ és $\boldsymbol{p}_j = \boldsymbol{r}_0 + \boldsymbol{q}_j$ különböző H-beli pontokra $\boldsymbol{p}_i - \boldsymbol{p}_j = \boldsymbol{q}_i - \boldsymbol{q}_j \in \Lambda$.
Ha $V(H) = kd(\Lambda)$ és H kompakt, akkor (ε_m) legyen egy 0-hoz tartó pozitív számsorozat. Ekkor minden m-re

$$V((1+\varepsilon_m)H) = (1+\varepsilon_m)^n V(H) = kd(\Lambda),$$

így az előző eset szerint léteznek olyan $\boldsymbol{p}_{mj} \in (1+\varepsilon_m)H$ pontok ($j = 1, \ldots, k+1$), hogy minden $i \neq j$-re $\boldsymbol{p}_{mj} - \boldsymbol{p}_{mi} \in \Lambda$ és $\boldsymbol{p}_{mj} - \boldsymbol{p}_{mi} \neq \boldsymbol{0}$.
Mivel H kompakt, így $\boldsymbol{p}_{mj}$-eknek létezik $\boldsymbol{p}_{m_l j}$ konvergens részsorozatuk, $\lim\limits_{l\to\infty} \boldsymbol{p}_{m_l j} := \boldsymbol{p}'_j$. Mivel H kompakt, így nem lehet belőle kikonvergálni, azaz $\boldsymbol{p}'_j \in H$.
Így $i, j = 1, \ldots, k+1$, $i \neq j$-re $\boldsymbol{p}'_j - \boldsymbol{p}'_i = \lim\limits_{l\to\infty}(\boldsymbol{p}_{m_l j} - \boldsymbol{p}_{m_l i}) \in \Lambda$ és $\boldsymbol{p}'_j - \boldsymbol{p}'_i \neq \boldsymbol{0}$. □

3.3. Tétel (Minkowski tétele)**.** *Legyen adott egy k pozitív egész szám, egy $d(\Lambda)$ determinánsú Λ rács és egy $V(H)$ térfogatú, origóra szimmetrikus, konvex H halmaz. Tegyük fel, hogy az alábbi két lehetőség közül az egyik teljesül:*

- $V(H) > k2^n d(\Lambda)$
- $V(H) = k2^n d(\Lambda)$ *és H kompakt.*

Ekkor létezik H-nak minimum $2k$ egymástól és az origótól különböző $\pm\boldsymbol{p}_i$ rácspontja ($1 \leq i \leq k$).

Bizonyítás. Blichfeldt tételét az $\frac{1}{2^n}V(H)$ térfogatú $\frac{1}{2}H$ halmazra alkalmazva azt kapjuk, hogy létezik $k+1$ különböző $\frac{1}{2}\boldsymbol{q}_i$ pontja H-nak ($i = 1, \ldots, k+1$) úgy, hogy az $\frac{1}{2}\boldsymbol{q}_i - \frac{1}{2}\boldsymbol{q}_j$ pontok a Λ rács origótól különböző pontjai.
Az n-dimenziós vektorok halmazán definiáljunk egy olyan rendezést,

amelyre $\boldsymbol{p}_i \succ \boldsymbol{p}_j$ akkor teljesüljön, ha a $\boldsymbol{p}_j - \boldsymbol{p}_i$ vektor első nem nulla koordinátája negatív.
Feltehető, hogy $\frac{1}{2}\boldsymbol{q}_1 \succ \frac{1}{2}\boldsymbol{q}_2 \succ \cdots \succ \frac{1}{2}\boldsymbol{q}_{m+1}$.
$\boldsymbol{p}_i := \frac{1}{2}\boldsymbol{q}_i - \frac{1}{2}\boldsymbol{q}_{m+1}$-re $\pm\boldsymbol{p}_i$-ek egymástól és az origótól különbözőek. $-\boldsymbol{q}_{m+1} \in H$, mert $\boldsymbol{q}_{m+1} \in H$ és H szimmetrikus az origóra. Mivel H konvex, így azt kapjuk, hogy $\boldsymbol{p}_i = \frac{1}{2}\boldsymbol{q}_i + \frac{1}{2}(-\boldsymbol{q}_{m+1}) \in H$. □

A következőkben mutatunk egy-egy érdekes példát arra, hogy miként lehet Blichfeldt és Minkowski tételeit nemnegatív függvényekre általánosítani.

3.4. Tétel (Blicheldt tételének általánosítása)**.** *Legyen Λ egy $d(\Lambda)$ determinánsú rács, és f egy integrálható függvény. Ekkor létezik olyan $\boldsymbol{p}_0$ pont, amelyre a*

$$d(\Lambda)\sum_{\boldsymbol{q}\in\Lambda} f(\boldsymbol{q}+\boldsymbol{p}_0) \geq \int_{\mathbb{R}^n} f(\boldsymbol{x})\,d\boldsymbol{x}$$

egyenlőtlenség teljesül, ahol $d\boldsymbol{x} = dx_1 \dots dx_n$.

Bizonyítás. Blichfeldt tételének bizonyításához hasonlóan $\boldsymbol{g}_1, \dots, \boldsymbol{g}_n$ legyen a Λ rács egy bázisa, és
$M := \{a_1\boldsymbol{g}_1 + \cdots + a_n\boldsymbol{g}_n : 0 \leq a_i < 1;\, i = 1, \dots, n\}$. Ekkor a tér minden $\boldsymbol{x}$ pontja egyértelműen írható fel $\boldsymbol{x} = \boldsymbol{p} + \boldsymbol{q}$, $\boldsymbol{p} \in M$, $\boldsymbol{q} \in \Lambda$ alakban.

$$\int_{\mathbb{R}^n} f(\boldsymbol{x})\,d\boldsymbol{x} = \sum_{\boldsymbol{q}\in\Lambda}\int_{\boldsymbol{p}\in M} f(\boldsymbol{q}+\boldsymbol{p})\,d\boldsymbol{p} = \int_{\boldsymbol{p}\in M}\sum_{\boldsymbol{q}\in\Lambda} f(\boldsymbol{q}+\boldsymbol{p})\,d\boldsymbol{p},$$

így $d(\Lambda) = V(M)$-ből következik, hogy $\exists \boldsymbol{p}_0 \in M$, amire a bizonyítandó egyenlőtlenség teljesül. □

Megjegyzés. Ha f-et a Blichfeldt tételében kapott H halmaz karakterisztikus függvényének választjuk, akkor $V(H) = \int_{\mathbb{R}^n} f(\boldsymbol{x})\,d\boldsymbol{x}$. Ha egy adott k pozitív egész számra $V(H) > kd(\Lambda)$, akkor az általánosított tétel szerint létezik olyan $\boldsymbol{p}_0$ pont, amire $\sum_{\boldsymbol{q}\in\Lambda} f(\boldsymbol{q}+\boldsymbol{p}_0) > k$, azaz $\sum_{\boldsymbol{q}\in\Lambda} f(\boldsymbol{q}+\boldsymbol{p}_0) \geq k+1$ teljesül. Vagyis létezik $k+1$ különböző $\boldsymbol{q}_i \in \Lambda$ pont, amikre $\boldsymbol{p}_0 + \boldsymbol{q}_i \in H$. Ezek páronkénti különbségei mind Λ-ban vannak, tehát ez a tétel valóban általánosítja Blichfeldt tételét.

Minkowski tételének általánosításához két lemmára lesz szükségünk.

3.5. Lemma. Legyen adott vektorok egy $\boldsymbol{s}_0, \boldsymbol{s}_1, \ldots$ sorozata. Ekkor létezik egy olyan $\boldsymbol{t}_0, \boldsymbol{t}_1, \ldots$ vektorsorozat, amelyre $\boldsymbol{t}_0 = \boldsymbol{0}$, $i \neq j$-re $\pm\boldsymbol{t}_i \neq \boldsymbol{t}_j$, és $\forall r > 0$-ra $\exists k_r \leq r, l_r \leq r$, amelyekre $\boldsymbol{t}_r = \boldsymbol{s}_{k_r} - \boldsymbol{s}_{l_r}$.

Bizonyítás. Vezessük be az n-dimenziós valós vektorok $\succ$ lexikografikus rendezését, ahol $\boldsymbol{w}_1 \succ \boldsymbol{w}_2$ pontosan akkor, ha $\boldsymbol{w}_1 - \boldsymbol{w}_2$ első nemnulla koordinátája pozitív.
A $\boldsymbol{t}_1, \boldsymbol{t}_2, \ldots$ vektorokat úgy választjuk, hogy $\forall r > 0$-ra $\boldsymbol{t}_r \succ \boldsymbol{0}$ legyen. $\boldsymbol{t}_0$ adott, és tegyük fel, hogy rögzített $r \geq 1$-re $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_{r-1}$-eket már megkonstruáltuk. Még meg kell adnunk egy megfelelő $\boldsymbol{t}_r$-et. Az $\boldsymbol{s}_0, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_r$ vektorok rendezése legyen $\boldsymbol{s}_{m_r} \succ \cdots \succ \boldsymbol{s}_{m_1} \succ \boldsymbol{s}_{m_0}$.
Ekkor $i = 1, \ldots, r$-re az $\boldsymbol{s}_{m_i} - \boldsymbol{s}_{m_0}$ vektorok rendre különböznek egymástól és az origótól. Mivel ez r darab vektor, így kiválasztható közülük egy olyan $\boldsymbol{t}_r$-nek, ami különbözik $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_{r-1}$ mindegyikétől. Mivel $i = 1, \ldots, r$-re $\boldsymbol{t}_i \succ \boldsymbol{0}$-át választottunk, így $\boldsymbol{t}_r = -\boldsymbol{t}_i$ sem fordulhat elő. □

Mostantól $\mathcal{A}$ jelöljön egy lineáris leképezést az n-dimenziós vektortérről önmagába úgy, hogy $\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{x}' = (x'_1, \ldots, x'_n)$ és $\mathcal{A}\boldsymbol{x} = \boldsymbol{x}'$ esetén $\boldsymbol{x}'_i = \sum_{j=1}^{n} \mathcal{A}_{ij} x_j$ legyen, és a $\det(\mathcal{A}) = \det(\mathcal{A}_{ij})$ jelölést vezessük be.

3.6. Lemma. Λ egy tetszőleges rács. Legyen adott egy $\varphi\colon \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ függvény, ami olyan, hogy $\forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$-re

$$\varphi(\mathcal{A}\boldsymbol{x} - \mathcal{A}\boldsymbol{y}) \geq \min\{\varphi(\boldsymbol{x}), \varphi(\boldsymbol{y})\},$$

és legyen $\det(\mathcal{A}) \neq 0$ (vagyis $\exists \mathcal{A}^{-1}$). Ekkor $\forall \boldsymbol{v} \in \mathbb{R}^n$-re

$$\sum_{\boldsymbol{u} \in \Lambda} \varphi(\mathcal{A}^{-1}\boldsymbol{u} + \mathcal{A}^{-1}\boldsymbol{v}) \leq \varphi(\boldsymbol{0}) + \frac{1}{2} \sum_{\substack{\boldsymbol{u} \in \Lambda \\ \boldsymbol{u} \neq \boldsymbol{0}}} \varphi(\boldsymbol{u}).$$

Bizonyítás. Rögzített $\boldsymbol{v} \in \mathbb{R}^n$-re $(\boldsymbol{s}_r)$ legyen $\boldsymbol{s} \in \Lambda$ vektorok olyan sorozata, hogy $r' \geq r$ esetén

$$\varphi(\mathcal{A}^{-1}\boldsymbol{v} + \mathcal{A}^{-1}\boldsymbol{s}_{r'}) \leq \varphi(\mathcal{A}^{-1}\boldsymbol{v} + \mathcal{A}^{-1}\boldsymbol{s}_r)$$

teljesüljön. Így a 3.5-ös lemmában kapott $k_r \leq r$ és $l_r \leq r$-ekre

$$\min\{\varphi(\mathcal{A}^{-1}\boldsymbol{v} + \mathcal{A}^{-1}\boldsymbol{s}_{l_r}), \varphi(\mathcal{A}^{-1}\boldsymbol{v} + \mathcal{A}^{-1}\boldsymbol{s}_{k_r})\} \geq \varphi(\mathcal{A}^{-1}\boldsymbol{v} + \mathcal{A}^{-1}\boldsymbol{s}_r).$$

A 3.5-ös lemma jelöléseivel élve és azt az $\boldsymbol{s}_r$ vektorokra alkalmazva

$$\boldsymbol{t}_r = \mathcal{A}((\mathcal{A}^{-1}\boldsymbol{v} + \mathcal{A}^{-1}\boldsymbol{s}_{k_r}) - (\mathcal{A}^{-1}\boldsymbol{v} + \mathcal{A}^{-1}\boldsymbol{s}_{l_r})).$$

Így az előző egyenlőtlenség és a lemma feltételei szerint

$$\varphi(\boldsymbol{t}_r) \geq \varphi(\mathcal{A}^{-1}\boldsymbol{v} + \mathcal{A}^{-1}\boldsymbol{s}_r).$$

$\mathcal{A}^{-1}\boldsymbol{v} + \mathcal{A}^{-1}\boldsymbol{s}_{k_r}$ és $\mathcal{A}^{-1}\boldsymbol{v} + \mathcal{A}^{-1}\boldsymbol{s}_{k_l}$ szerepcseréjével adódik, hogy a

$$\varphi(-\boldsymbol{t}_r) \geq \varphi(\mathcal{A}^{-1}\boldsymbol{v} + \mathcal{A}^{-1}\boldsymbol{s}_r)$$

egyenlőtlenség is teljesül. A $\boldsymbol{t}_r$ vektorok mind Λ-beliek és φ nemnegatív függvény, így

$$\sum_{\boldsymbol{u}\in\Lambda} \varphi(\boldsymbol{u}) \geq \varphi(\boldsymbol{t}_0) + \sum_{r>0}(\varphi(\boldsymbol{t}_r) + \varphi(-\boldsymbol{t}_r)) \geq \varphi(\mathcal{A}^{-1}\boldsymbol{t}_0 + \mathcal{A}^{-1}\boldsymbol{v})) +$$
$$2\sum_{r>0} \varphi(\mathcal{A}^{-1}\boldsymbol{t}_r + \mathcal{A}^{-1}\boldsymbol{v}) = -\varphi(\mathcal{A}^{-1}\boldsymbol{t}_0 + \mathcal{A}^{-1}\boldsymbol{v})) + 2\sum_{\boldsymbol{u}\in\Lambda} \varphi(\mathcal{A}^{-1}\boldsymbol{u} + \mathcal{A}^{-1}\boldsymbol{v}).$$

Mivel $\forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$-re

$$\varphi(\mathcal{A}\boldsymbol{x} - \mathcal{A}\boldsymbol{y}) \geq \min\{\varphi(\boldsymbol{x}), \varphi(\boldsymbol{y})\},$$

így $\boldsymbol{x} = \boldsymbol{y}$ helyettesítéssel adódik, hogy $\forall \boldsymbol{x} \in \mathbb{R}^n$-re $\varphi(\boldsymbol{0}) \geq \varphi(\boldsymbol{x})$, azaz

$$\varphi(\boldsymbol{0}) \geq \varphi(\mathcal{A}^{-1}\boldsymbol{t}_0 + \mathcal{A}^{-1}\boldsymbol{v}).$$

Ezt összevetve az előző egyenlőtlenséggel éppen a bizonyítandó állítás adódik. □

3.7. Tétel (Minkowski tételének általánosítása)**.** *Legyen adott egy tetszőleges Λ rács és egy korlátos halmazon kívül eltűnő $\varphi\colon \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ függvény, ami olyan, hogy $\forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$-re*

$$\varphi(\mathcal{A}\boldsymbol{x} - \mathcal{A}\boldsymbol{y}) \geq \min\{\varphi(\boldsymbol{x}), \varphi(\boldsymbol{y})\}.$$

Ekkor az alábbi egyenlőtlenség teljesül:

$$\frac{|\det(\mathcal{A})|}{d(\Lambda)} V(\varphi) \leq \varphi(\boldsymbol{0}) + \frac{1}{2}\sum_{\substack{\boldsymbol{u}\in\Lambda \\ \boldsymbol{u}\neq\boldsymbol{0}}} \varphi(\boldsymbol{u}),$$

ahol $V(\varphi) = \int\limits_{\mathbb{R}^n} \varphi(\boldsymbol{x})\, d\boldsymbol{x}$ *és* $d\boldsymbol{x} = dx_1 \dots dx_n$.

Bizonyítás. Legyen $M := \{a_1\boldsymbol{g}_1 + \cdots + a_n\boldsymbol{g}_n : 0 \le a_i < 1; i = 1, \ldots, n\}$. Ekkor

$$\int\limits_{\boldsymbol{v}\in M} \sum_{\boldsymbol{u}\in\Lambda} \varphi(\mathcal{A}^{-1}\boldsymbol{u} + \mathcal{A}^{-1}\boldsymbol{v})\, d\boldsymbol{v} = \int\limits_{\mathbb{R}^n} \varphi(\mathcal{A}^{-1}\boldsymbol{v})\, d\boldsymbol{v} =$$

$$= |\det(\mathcal{A})| \int\limits_{\mathbb{R}^n} \varphi(\boldsymbol{v})\, d\boldsymbol{v} = |\det(\mathcal{A})| V(\varphi)$$

felhasználva a lineáris transzformált integrálására jól ismert formulát. Másrészt

$$\int\limits_{\boldsymbol{v}\in M} (\varphi(\boldsymbol{0}) + \frac{1}{2}\sum_{\substack{\boldsymbol{u}\in\Lambda\\ \boldsymbol{u}\neq\boldsymbol{0}}} \varphi(\boldsymbol{u}))\, d\boldsymbol{v} = V(M)(\varphi(\boldsymbol{0}) + \frac{1}{2}\sum_{\substack{\boldsymbol{u}\in\Lambda\\ \boldsymbol{u}\neq\boldsymbol{0}}} \varphi(\boldsymbol{u})) =$$

$$= d(\Lambda)(\varphi(\boldsymbol{0}) + \frac{1}{2}\sum_{\substack{\boldsymbol{u}\in\Lambda\\ \boldsymbol{u}\neq\boldsymbol{0}}} \varphi(\boldsymbol{u})).$$

Ekkor a 3.6-os lemmát alkalmazva éppen a bizonyítandó egyenlőtlenség adódik. □

Megjegyzés. Ez a tétel valóban implikálja Minkowski tételének az első alternatíváját abban az esetben, ha φ a Minkowski tételbeli H halmaz karakterisztikus függvénye (vagyis $V(\varphi) = V(H)$), és $\mathcal{A}(\boldsymbol{x}) = \frac{1}{2}\boldsymbol{x}$. Ekkor $\min\{\varphi(\boldsymbol{x}), \varphi(\boldsymbol{y})\} = 0$ kivéve, ha $\boldsymbol{x}, \boldsymbol{y} \in H$. Ilyenkor ugyanis $\min\{\varphi(\boldsymbol{x}), \varphi(\boldsymbol{y})\} = 1$, de H konvexsége miatt $\mathcal{A}(\boldsymbol{x} - \boldsymbol{y}) = \frac{1}{2}\boldsymbol{x} + \frac{1}{2}(-\boldsymbol{y}) \in H$, így $\varphi(\mathcal{A}\boldsymbol{x} - \mathcal{A}\boldsymbol{y}) = 1$ is teljesül. Vagyis $\forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$-re $\varphi(\mathcal{A}\boldsymbol{x} - \mathcal{A}\boldsymbol{y}) \ge \min\{\varphi(\boldsymbol{x}), \varphi(\boldsymbol{y})\}$. Ezen kívül a $\det(\mathcal{A}) = (\frac{1}{2})^n$ egyenlőség is fennáll. Ha l-el jelöljük az olyan origótól különböző $\pm\boldsymbol{u} \in \Lambda$ pontpárok számát, amik H-ban vannak, akkor a tételben szereplő egyenlőtlenség jobb oldala éppen $l+1$. Így azt kapjuk, hogy a tételben szereplő egyenlőtlenség bal oldala legfeljebb $l+1$, a Minkowski-tétel első alternatívájában szereplő $V(H) > k2^n d(\Lambda)$ feltétel pedig azt eredményezi, hogy K-nál nagyobb. Tehát $k < l + 1$, azaz $k \le l$.

3.2. Minkowski tételének számelméleti alkalmazásai

3.2.1. Tételek négyzetszámok összegére

3.8. Tétel. *Minden p prímszám, amire -1 kvadratikus maradék felírható $p = a^2 + b^2$ alakban, ahol $a, b \in \mathbb{Z}$.*

Bizonyítás. Legyen $c^2 \equiv -1 \pmod{p}$, és $\Lambda \subset \mathbb{R}^2$ legyen az a rács, aminek bázisa $\{(0,p),(1,c)\}$. Ekkor $d(\Lambda) = p$. Vegyük az origó középpontú $r = \sqrt{\frac{3}{2}p}$ sugarú körlemezt. Ennek a területe $\pi r^2 > 2^2 p$, így a Minkowski-féle konvex test tétel szerint létezik az origótól különböző rácspontja. Ez legyen $n(0,p) + m(1,c)$, ahol $m, n \in \mathbb{Z}$. Ekkor $a = m$, $b = np + mc$, $a^2 + b^2 \equiv m^2 + m^2c^2 \equiv m^2(1+c^2) \equiv 0 \pmod{p}$, és $0 < a^2 + b^2 < \frac{3}{2}p$, így $p = a^2 + b^2$. □

3.9. Lemma. Bármely p prímszámhoz léteznek olyan $x, y \in \mathbb{Z}$ számok, amelyekre $x^2 + y^2 + 1 \equiv 0 \pmod{p}$.

Bizonyítás. Ha $p = 2$, akkor $2 = 0^2 + 1^2 + 1$. Mostantól tegyük fel, hogy $p > 2$.
Mivel 0^2, 1^2, 2^2,…,$(\frac{p-1}{2})^2$ páronként mind inkongurensek $\pmod{p}$, és $(p-u)^2 \equiv (-u)^2 \equiv u^2 \pmod{p}$ minden $u \in \mathbb{Z}$-re, így $\frac{p+1}{2}$ darab különböző értéket vesz fel x^2, amint az x változó $\pmod{p}$ egy teljes maradékrendszer elemein fut végig. Ugyanígy $\frac{p+1}{2}$ különböző értéket vesz fel $-y^2-1$, amint az y változó $\pmod{p}$ egy teljes maradékrendszer elemein fut végig, így $-y^2 - 1$ és x^2 összesen $p+1$ értéket vesznek fel $\pmod{p}$. Vagyis a skatulyaelv miatt létezik olyan (x_0, y_0) számpár, amire $x_0^2 \equiv -y_0^2 - 1 \pmod{p}$, azaz $x_0^2 + y_0^2 + 1 \equiv 0 \pmod{p}$. □

3.10. Tétel (Négy négyzetszám tétel)**.** *Minden pozitív egész szám felírható* 4 *négyzetszám összegeként.*

Bizonyítás. Ha az $m, n \in \mathbb{Z}_{>0}$ számok felírhatók 4 négyzetszám összegeként $n = a^2 + b^2 + b^2 + d^2$ és $m = x^2 + y^2 + z^2 + w^2$ módon, akkor a szorzatuk is felírható $nm = h_1^2 + h_2^2 + h_3^2 + h_4^2$ alakban, ahol $h_1 = ax+by+cz+dw$, $h_2 = -ay+bx-cw+dz$, $h_3 = az-bw-cx-dy$, $h_4 = aw + bz - cy - dx$. Így a tételt elég p prímszámokra belátni. A 3.9-es lemma szerint léteznek olyan $t, s \in \mathbb{Z}$ számok, amikre $t^2 + s^2 + 1 \equiv 0 \pmod{p}$. Legyen $\Lambda \subset \mathbb{R}^4$ az a rács, aminek egy bázisa $\{(0,0,0,p),(0,0,p,0),(0,1,t,-s),(1,0,s,t)\}$. Ekkor $d(\Lambda) = p$, és egy tetszőleges $(i,j,k,l) \in \Lambda$ rácspontra $is + jt \equiv k \pmod{p}$ illetve $it - js \equiv l \pmod{p}$. Vegyünk egy origó középpontú, $r = \sqrt{\frac{19}{10}p}$ sugarú $\mathbb{R}^4$-beli gömböt. Ennek a térfogata $\frac{\pi^2}{2}r^4$. Itt felhasználtuk azt az egyszerű analízisbeli állítást, hogy egy $B_{2n} \subset \mathbb{R}^{2n}$ gömb $2n$-dimenziós térfogata $V(B_{2n}) = \frac{\pi^n}{n!}r^{2n}$. Mivel $\frac{\pi^2}{2}r^4 > 2^4p^2$, így a Minkowski-féle konvex test tétel szerint létezik olyan $(i,j,k,l) \in \Lambda$ rácspont, amire $i^2 + j^2 + k^2 + w^2 \leq \frac{19}{10}p$. Mivel $(i,j,k,l) \neq \mathbf{0}$, és

$$i^2+j^2+k^2+w^2 \equiv i^2+j^2+i^2s^2+j^2t^2+2ijst+i^2t^2+j^2s^2-2ijst \equiv$$
$$i^2(t^2+s^2+1)+j^2(t^2+s^2+1) \equiv 0 \pmod{p},$$

így $i^2+j^2+k^2+w^2=p$. □

3.2.2. Diofantikus approximáció

A Minkowski-féle konvex test tétel síkbeli változatát irracionális számok racionális számokkal való közelítésére is lehet alkalmazni.

3.11. Tétel (Diofantikus approximáció)**.** *Bármely α irracionális számhoz végtelen sok olyan különböző $\frac{p}{q}$ szám létezik ($p,q \in \mathbb{Z}$), amelyre*

$$|\alpha - \frac{p}{q}| < \frac{1}{2}\frac{1}{q^2}.$$

Bizonyítás. Az állítással ekvivalens, hogy tetszőleges α irracionális számhoz végtelen sok olyan különböző $\frac{p}{q}$ szám létezik ($p,q \in \mathbb{Z}$), amire $|(p-\alpha q)q| < \frac{1}{2}$. Legyen $x = p-\alpha q$ és $y=q$. Az (x,y) síkbeli pontok egy Λ paralelogrammarácsot határoznak meg, amint p és q befutják az egész számokat. Tehát azt kell bizonyítanunk, hogy az $|xy| < \frac{1}{2}$ egyenletű hiperbola $xy=\frac{1}{2}$ és $xy=-\frac{1}{2}$ ágai közé végtelen sok rácspont esik. A $\boldsymbol{v}(1-\alpha,1)$ és $\boldsymbol{u}(-\alpha,1)$ vektorok a rács egy bázisát alkotják, így $d(\Lambda) = |\det(\boldsymbol{v},\boldsymbol{u})| = 1$. Vegyük fel a $(0,\sqrt{2})$, $(\sqrt{2},0)$, $(0,-\sqrt{2})$, $(-\sqrt{2},0)$ csúcsokkal rendelkező négyzetet a síkon. Ez a $(\pm\frac{1}{\sqrt{2}},\pm\frac{1}{\sqrt{2}})$ pontokban érinti az $|xy|=\frac{1}{2}$ egyenletű hiperbolát, és belseje az $|xy|<\frac{1}{2}$ tartományba esik. Tehát kaptunk egy origóra szimmetrikus, konvex, zárt tartományt, aminek 4 a területe. Így a Minkowski-féle konvex test tétel szerint van benne egy origótól különböző rácspont. Ha $q \neq 0$ is elérhető, akkor erre $|\alpha - \frac{p}{q}| < \frac{1}{2}\frac{1}{q^2}$ teljesül. Egyszerű geometriai állítás, hogy egy adott hiperbolaág bármely pontbeli érintője és a koordinátatengelyek által meghatározott háromszög területe állandó. Így az $|xy|=\frac{1}{2}$ hiperbolapár 4 ágához a $(\pm a,\pm b)$ pontokban $(a,b>0)$ húzott érintők által meghatározott paralelogramma egy origóra szimmetrikus, 4 területű, zárt tartomány. Úgy válasszuk meg az érintőket, hogy a paralelogrammába eső rácspontok ne tartalmazzák az imént felvett négyzetbe eső rácspontokat. Így Minkowski tétele szerint új rácspontokat kaptunk az $|xy|<\frac{1}{2}$ tartományban. Ezt iterálva végtelen sok rácspont adódik. Arra ügyelni kell, hogy $q \neq 0$ mindig teljesüljön, de ez elérhető úgy, hogy a-t egyre kisebbnek választjuk.

A kapott (x, y) rácspontoknak megfelelő $\frac{p}{q}$ számok között végtelen sok különböző van, mert ellenkező esetben a (p, q) pontpárok véges sok egyenesen helyezkednének el. Ekkor azonban lenne olyan egyenes, amin végtelen sok (p, q) pontpár van. A két tengely nem lehet ilyen, mert $q \neq 0$ és α irracionális. Ezeken kívül minden egyenesnek csak egy véges szakasza esik a hiperbolaágak által meghatározott tartományba, így ilyen egyeneseken nem lehet végtelen sok rácspont. Vagyis ellentmondásra jutottunk. □

Megjegyzés. A diofantikus approximációra vonatkozó legerősebb tétel Hurwitz nevéhez fűződik, amely azt mondja, hogy tetszőleges α irracionális számhoz végtelen sok olyan különböző $\frac{p}{q}$ szám létezik $(p, q \in \mathbb{Z})$, amire $|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}} \frac{1}{q^2}$.
Ez a tétel is bizonyítható rácsgeometriai eszközökkel, azonban ennek előkészítése lényegesen hosszadalmasabb lenne.

3.12. Lemma. Legyenek $l_1, \ldots, l_n$ n-változós valós lineáris formák, amiknek d determinánsa nem nulla. Ekkor tetszőleges $a_1, \ldots, a_n$ pozitív számokra, amikre $a_1 \ldots a_n \geq |d|$ létezik az

$$|l_1(x_1, \ldots, x_n)| \leq a_1, \ldots, |l_n(x_1, \ldots, x_n)| \leq a_n$$

rendszernek $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$ egész megoldása.

Bizonyítás. $H = \{(x_1, \ldots, x_n) : |l_1(x_1, \ldots, x_n)| \leq a_1, \ldots, |l_n(x_1, \ldots, x_n)| \leq a_n\}$ esetén

$$V(H) = \frac{2^n a_1 \ldots a_n}{d} \geq 2^n,$$

így a Minkowski-féle konvex test tételt H-ra és a Λ_0 rácsra alkalmazva az állítás adódik. □

3.13. Tétel (Szimultán diofantikus approximáció)**.** *Tetszőleges* $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ *számokhoz az*

$$|\alpha_1 - \frac{p_1}{q}| \leq q^{-\frac{n+1}{n}}, \ldots, |\alpha_n - \frac{p_n}{q}| \leq q^{-\frac{n+1}{n}}$$

rendszernek végtelen sok $(p_1, \ldots, p_n, q) \in \mathbb{Z}^n$ *megoldása létezik* $(q \neq 0)$.

Bizonyítás. Ha $\alpha_1, \ldots, \alpha_n$ mind racionálisak, akkor $p_1, \ldots, p_n, q \neq 0$ legyenek olyanok, amikre $\alpha_1 = \frac{p_1}{q}, \ldots, \alpha_n = \frac{p_n}{q}$. Ekkor minden $k \in \mathbb{Z}$-re $(kp_1, \ldots, kp_n, kq)$ megoldás. Ha $\alpha_1, \ldots, \alpha_n$ nem mind racionális, akkor

feltehető, hogy α_1 irracionális.
Az $n+1$-változós $q\alpha_1 - p_1, \ldots, q\alpha_n - p_n$ és q lineáris formák determinánsának abszolút értéke 1, így tetszőleges $0 < \varepsilon_1 < 1$-re az 3.12-es lemmát alkalmazva az

$$|q\alpha_1 - p_1| \leq \varepsilon_1, \ldots, |q\alpha_n - p_n| \leq \varepsilon_1, |q| \leq \frac{1}{\varepsilon_1^n}$$

rendszernek létezik nemtriviális egész $(p_1^1, \ldots, p_n^1, q^1)$ megoldása, ahol $q^1 \neq 0$, máskülönben $0 < \varepsilon_1 < 1$ miatt $p_1^1 = \cdots = p_n^1 = 0$ lenne. p_1^1 irracionális, így $0 < |q^1\alpha_1 - p_1^1|$. Legyen $0 < \varepsilon_2 < \varepsilon_1$ olyan, hogy $\varepsilon_2 < |q^1\alpha_1 - p_1^1|$. Ekkor az

$$|q\alpha_1 - p_1| \leq \varepsilon_2, \ldots, |q\alpha_n - p_n| \leq \varepsilon_2, |q| \leq \frac{1}{\varepsilon_2^n}$$

rendszernek létezik $(p_1^1, \ldots, p_n^1, q^1)$-től különböző $(p_1^2, \ldots, p_n^2, q^2)$, megoldása, ahol $q^2 \neq 0$. Ezt ismételgetve végtelen sok különböző megoldás adódik. □

3.2.3. Alsó becslés irreducibilis polinomok diszkriminánsára

3.14. Tétel. *Ha $p(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0$ egy egész együtthatós irreducibilis polinom, aminek mind az n komplex gyöke valós, akkor p-nek a D diszkiriminánsára teljesül, hogy*

$$D \geq (\frac{n^n}{n!})^2.$$

Bizonyítás. Legyenek p gyökei $x_1, \ldots, x_n$, és nézzük az alábbi lineáris formákat:

$$\begin{aligned} l_1(\boldsymbol{u}) &= x_1^{n-1}u_n + x_1^{n-2}u_{n-1} + \cdots + x_1u_2 + u_1 \\ l_2(\boldsymbol{u}) &= x_2^{n-1}u_n + x_2^{n-2}u_{n-1} + \cdots + x_2u_2 + u_1 \\ &\cdots \\ l_n(\boldsymbol{u}) &= x_n^{n-1}u_n + x_n^{n-2}u_{n-1} + \cdots + x_nu_2 + u_1, \end{aligned}$$

ahol $\boldsymbol{u} = (u_1, \ldots, u_n)$.
$\boldsymbol{u} \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}$ esetén minden $i = 1, \ldots, n$-re $l_i(\boldsymbol{u}) \neq 0$, mert különben $l_i(\boldsymbol{u})$ egy x_i-ben legfeljebb $n-1$-edfokú (vagyis p-nél alacsonyabb fokú) egész együtthatós polinom lenne, aminek x_i gyöke. Ez azonban nem lehetséges, hiszen p irreducibilis. Így $l_1 \ldots l_n \neq 0$. $l_1 \ldots l_n$ egy szimmetrikus polinom az $x_1, \ldots, x_n$ változókban egész együtthatókkal, így

a szimmetrikus polinomok alaptétele szerint felírható $l(v_1, \dots, v_n)$ alakban, ahol l egész együtthatós, és $v_1, \dots, v_n \in \mathbb{Z}$. Ezért $l_1 \dots l_n$ egész, azaz $|l_1(\boldsymbol{u}) \dots l_n(\boldsymbol{u})| \geq 1$ minden $\boldsymbol{u} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$-ra.
Így a $\Lambda = \{(l_1(\boldsymbol{u}), \dots, l_n(\boldsymbol{u})) : \boldsymbol{u} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}\}$ rács nem tartalmaz az $\{(y_1, \dots, y_n) : |y_1 \dots y_n| \leq 1\}$ halmazból origótól különböző pontot.
A számtani és mértani közepek közti egyenlőtlenség szerint ez a halmaz tartalmazza a $H = \{(y_1, \dots, y_n) : \frac{1}{n}(|y_1| + \dots + |y_n|) \leq 1\}$ origóra szimmetrikus, konvex halmazt, így Λ nem tartalmaz az origótól különböző H-beli pontot sem. H egy keresztpolitóp, így térfogata a 2.11-es lemma szerint $V(H) = \frac{2^n n^n}{n!}$.
Így a Minkowski-féle konvex test tételt felhasználva $d(\Lambda) \geq \frac{n^n}{n!}$ adódik. Vandermonde tételét az

$$A = \begin{pmatrix} 1 & x_1 & \dots & x_1^{n-1} \\ 1 & x_2 & \dots & x_2^{n-1} \\ \dots & & & \\ 1 & x_n & \dots & x_n^{n-1} \end{pmatrix}$$

mátrixra alkalmazva $D = (\det(A))^2$ adódik. Vagyis $D = (d(\Lambda))^2$, amiből a tétel állítása következik.

□

3.2.4. Rédei és Hlawka tétele

3.15. Tétel (Rédei)**.** *Tetszőleges m pozitív egész számra legyenek $k_1, \dots, k_m$ pozitív egészek, és K legyen egy origóra szimmetrikus $V(K) > 2^n k_1 \dots k_m$ térfogatú konvex test $\mathbb{R}^n$-ben. Az $f_1, \dots, f_m$ függvények legyenek olyanok, hogy*

- *minden $\boldsymbol{u} \in \Lambda_0$-ra $f_i(\boldsymbol{u})$ értelmes és egész $(i = 1, \dots, m)$*
- *ha $i = 1, \dots, m$-re $f_i(\boldsymbol{u}_1) \equiv f_i(\boldsymbol{u}_2) \pmod{k_i}$, akkor $f_i(\boldsymbol{u}_1 - \boldsymbol{u}_2) \equiv 0 \pmod{k_i}$.*

Ekkor létezik K-nak olyan az origótól különböző $\boldsymbol{u}_0 \in \Lambda_0$ rácspontja, amire $i = 1, \dots, m$-re $f_i(\boldsymbol{u}_0) \equiv 0 \pmod{k_i}$.

Ehelyett Hlawkának egy erősebb eredményére mutatunk bizonyítást, amely azonnal implikálja Rédei tételét.

3.16. Tétel (Hlawka)**.** *Legyen $G = \{g_0, \dots, g_{l-1}\} \subset \mathbb{R}^n$ egy véges halmaz, és $\psi : \Lambda_0 \to G$ olyan leképezés, amire $\psi(\boldsymbol{p}_1) = \psi(\boldsymbol{p}_2)$ esetén $\psi(\boldsymbol{p}_1 - \boldsymbol{p}_2) = g_0$ teljesül.*

Ekkor egy tetszőleges $V(K) > 2^n l$ térfogatú, origóra szimmetrikus konvex K test tartalmaz olyan origótól különböző $\boldsymbol{p}$ pontot, amelyre $\psi(\boldsymbol{p}) = g_0$.

Bizonyítás. Jelölje $i = 0, \dots, l$-re H_i azoknak a $\boldsymbol{p} \in \Lambda_0$ pontoknak a halmazát, amelyekre $\psi(\boldsymbol{p}) = g_0$. Ekkor $\boldsymbol{p}_1^i, \boldsymbol{p}_2^i \in H_i$ esetén $\boldsymbol{p}_1^i - \boldsymbol{p}_2^i \in H_0$, így H_0 a Λ_0 rács additív részcsoportja. Sőt $\boldsymbol{p}^i \in H_i$ esetén $H_i - \boldsymbol{p}^i \subset H_0$, azaz $i = 1, \dots, l$-re H_i része egy H_0 szerinti mellékosztálynak. Kihasználva, hogy $\Lambda_0 = \bigcup_{i=0}^{l} H_i$ azt kapjuk, hogy H_0 a Λ_0 rácsnak egy l-nél nem nagyobb indexű részrácsa. Ezért $\exists A \in \mathbb{R}^{n\times n}$ nemszinguláris mátrix, amellyel $H_0 = A\Lambda_0$ és $|\det A| \le l$, azaz $|\det A^{-1}| \ge \frac{1}{l}$. Ekkor $d(A^{-1}H_0) = 1$, és így $V(A^{-1}K) = |\det A^{-1}|V(K) > \frac{1}{l}2^n l = 2^n d(A^{-1}H_0)$, vagyis alkalmazható Minkowski tétele $A^{-1}K$-ra, amely szerint $A^{-1}K$ tartalmaz az origótól különböző pontot az $A^{-1}H_0$ rácsból. Tehát K tartalmaz az origótól különböző pontot az H_0 rácsból. Épp ezt kellett bizonyítani. □

Megjegyzés. Rédei és Hlawka tételeinek a jelöléseivel $i = 1, \dots, m$-re c_i-et lefixálva, ha G elemeinek a $g_i \equiv c_1 \pmod{k_i}$ kongurenciák által meghatározott redukált maradékrendszereket választjuk, akkor nyilvánvalóan teljesülnek Rédei tételének a feltételei, így Hlawka tételéből valóban következik Rédei tétele.
Rédei tételének sok érdekes számelméleti következménye van, amelyeket más eszközökkel nehéz bebizonyítani, de a tételt alkalmazva azonnal adódnak. Erre mutatok két példát.

3.16.1. Következmény. Tegyük fel, hogy p egy prímszám és K egy $4p$ területű, origóra szimmetrikus, konvex síkidom, ami nem tartalmaz a $\mathbb{Z}^2$ rácsból olyan origótól különböző $\boldsymbol{v} = (v_1, v_2)$ rácspontot, amelynek mindkét koordinátája osztható p-vel. Ekkor bármely $k \in \mathbb{Z}$ p-vel nem osztható számhoz létezik $v_1, v_2 \in \mathbb{Z}$, amelyek nem oszthatók p-vel, $v_1 \equiv kv_2 \pmod{p}$ és $(v_1, v_2) \in K$.

Bizonyítás. Ez Rédei tételének alkalmazása az $m = 1$, $k_1 = p$, $f_1(\boldsymbol{v}) = kv_2 - v_1$ esetre. □

3.16.2. Következmény. Legyenek $n, k, m, k_1, \dots, k_m$ pozitív egész számok, ahol $m < n$ és $k_1 \dots k_m < k^m$. Ekkor tetszőleges h_{ij} $(i = 1, \dots, m;$ $j = 1, \dots, n)$ egészekből álló számhalmazra léteznek $u_1, \dots, u_n$ nem mind nulla egész számok, amelyekre

$j = 1, \dots, n$-re $|u_j| \le (k^m)^{\frac{1}{n}}$ és $i = 1, \dots, m$-re $\sum_{j=1}^{n} h_{ij}u_j \equiv 0 \pmod{k_i}$.

Bizonyítás. Alkalmazzuk Rédei tételét a
$K = \left\{(x_1, \dots, x_n) \in \mathbb{R}^n : |x_1| \le (k^m)^{\frac{1}{n}}, \dots, |x_n| \le (k^m)^{\frac{1}{n}}\right\}$ kockára. □

3.3. Konvex testek szukcesszív minimumai

3.17. Definíció. Legyen Λ egy n-dimenziós rács, és $H \subset \mathbb{R}^n$ egy origóra szimmetrikus konvex test. Ekkor $i = 1, \dots, n$-re $\lambda_i(H, \Lambda) = \min\{\lambda \in \mathbb{R}_{\ge 0} : \lambda H$ tartalmaz i lineárisan független Λ-beli rácspontot$\}$ számot a H Λ-ra vonatkozó i-edik szukcesszív minimumának nevezzük.

A definícióból adódik, hogy

$$\lambda_1(H, \Lambda) \le \lambda_2(H, \Lambda) \le \cdots \le \lambda_n(H, \Lambda).$$

A következőkben egy érdekes becslést mutatok be a szukcesszív minimumok szorzatára, amelyet Minkowski második tételeként is szoktak említeni.
Előbb azonban tegyünk két egyszerű észrevételt:
Tetszőleges $\Lambda \subset \mathbb{R}^n$ rácshoz létezik olyan A $n \times n$-es nemszinguláris mátrix, amivel $\Lambda = A\Lambda_0$, és $\lambda_i(H, \Lambda) = \lambda_i(A^{-1}H, \Lambda_0)$.
A másik észrevétel, amit fel fogok használni az, hogy tetszőleges $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n \in \Lambda$ lineárisan független vektorokra létezik olyan $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) \in \Lambda$ bázis, amelyre $span\{\boldsymbol{u}_1, \dots, \boldsymbol{u}_n\} = span\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$. Speciálisan ha $\boldsymbol{z}_1, \dots, \boldsymbol{z}_n \in \Lambda_0$ olyan lineárisan független rácsvektorok, amelyekre $i = 1, \dots, n$-re $\boldsymbol{z}_i \in \lambda_i(H, \Lambda_0)H$, akkor a 2.2-es lemma szerint létezik olyan U $n \times n$-es unimoduláris mátrix, amellyel $i = 1, \dots, n$-re

$$U\boldsymbol{z}_i \in \lambda_i(UH, \Lambda_0)UH \cap span\{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}.$$

Itt $\boldsymbol{e}_i$ az i-edik egységvektort jelöli.

3.18. Tétel (Minkowski tétele konvex testek szukcesszív minimumaira)**.** *Legyen Λ egy n-dimenziós rács, $H \subset \mathbb{R}^n$ egy origóra szimmetrikus konvex test, és $\lambda_i = \lambda_i(H, \Lambda)$. Ekkor*

$$\frac{2^n}{n!}d(\Lambda) \le \lambda_1 \cdots \lambda_n V(H) \le 2^n d(\Lambda).$$

Bizonyítás. Az első észrevétel szerint elegendő, ha a tételt $\Lambda = \Lambda_0$ esetén bizonyítjuk be. A második észrevétel szerint pedig feltehetjük, hogy a $\boldsymbol{v}^1, \ldots, \boldsymbol{v}^n$ lineárisan független pontokra, amelyekre $j = 1, \ldots, n$-re $\boldsymbol{v}^j \in \lambda_j H \cap \Lambda_0$ teljesül, hogy $span\{\boldsymbol{v}^1, \ldots, \boldsymbol{v}^j\} = span\{\boldsymbol{e}^1, \ldots, \boldsymbol{e}^j\} := L_j$. Itt $\boldsymbol{e}^1, \ldots, \boldsymbol{e}^j$ az $\mathbb{R}^j$ tér standard bázisát jelöli. Legyen $H_j = \frac{\lambda_j}{2} H$. Tetszőleges $k \in \mathbb{N}$-re $K_k^n := \{\boldsymbol{v} \in \Lambda_0 : |v_j| \leq k; j = 1, \ldots, n\}$, és $j = 1, \ldots, n-1$-re legyen $K_k^j = K_k^n \cap L_j$. Mivel H korlátos, így létezik olyan c konstans, amelyre

$$V(K_k^n + H_n) \leq (2k + c)^n.$$

Tetszőleges $\boldsymbol{v}, \boldsymbol{v}' \in \Lambda_0$ rácspontokra

$$(\boldsymbol{v} + int(H_1)) \cap (\boldsymbol{v}' + int(H_1)) = \emptyset,$$

máskülönben a
$\boldsymbol{v} - \boldsymbol{v}' \in (int(H_1) - int(H_1)) \cap \Lambda_0 = int(H_1 - H_1) \cap \Lambda_0 = int(\lambda_1 H) \cap \Lambda_0$
$= \{\boldsymbol{0}\}$ ellentmondásra jutnánk. Ezért

$$V(K_k^n + H_1) = (2k+1)^n V(H_1) = \frac{(2k+1)^n \lambda_1^n}{2^n} V(H).$$

$j = 1, \ldots, n-1$-re azt szeretnénk megmutatni, hogy

$$V(K_k^n + H_{j+1}) \geq \left(\frac{\lambda_{j+1}}{\lambda_j}\right)^{n-j} V(K_k^n + H_j).$$

Ebből következne, hogy

$$\begin{aligned}(2k+c)^n \geq V(K_k^n + H_n) \geq \left(\frac{\lambda_n}{\lambda_{n-1}}\right) V(K_k^n + H_{n-1}) \geq \\ \left(\frac{\lambda_n}{\lambda_{n-1}}\right)\left(\frac{\lambda_{n-1}}{\lambda_{n-2}}\right)^2 V(K_k^n + H_{n-2}) \geq \cdots \geq \\ \left(\frac{\lambda_n}{\lambda_{n-1}}\right)\left(\frac{\lambda_{n-1}}{\lambda_{n-2}}\right)^2 \cdots \left(\frac{\lambda_2}{\lambda_1}\right)^{n-1} V(K_k^n + H_1) = \\ = \lambda_1 \cdots \lambda_n \left(\frac{2k+1}{2}\right)^n V(H),\end{aligned}$$

vagyis $\lambda_1 \ldots \lambda_n V(H) \leq 2^n \left(\frac{2k+c}{2k+1}\right)^n$. Ez minden $k \in \mathbb{N}$-re igaz, amiből $\lambda_1 \ldots \lambda_n V(H) \leq 2^n$ következik. Ez $d(\Lambda_0) = 1$ miatt éppen a jobboldali bizonyítandó egyenlőtlenség. Már csak azt kéne megmutatnunk, hogy

$j = 1, \ldots, n-1$-re $V(K_k^n + H_{j+1}) \geq \left(\frac{\lambda_{j+1}}{\lambda_j}\right)^{n-j} V(K_k^n + H_j)$.
$\lambda_{j+1} = \lambda_j$ esetén az egyenlőtlenség egyértelműen teljesül, ezért tegyük fel, hogy $\lambda_{j+1} > \lambda_j$. Legyenek $\boldsymbol{v}, \boldsymbol{v}' \in \Lambda_0$ olyan rácspontok, amelyekre $(v_{j+1}, \ldots, v_n) \neq (v'_{j+1}, \ldots, v'_n)$. Ekkor

$$(\boldsymbol{v} + int(H_{j+1})) \cap (\boldsymbol{v}' + int(H_{j+1})) = \emptyset,$$

máskülönben lenne $j+1$ darab $\boldsymbol{v}^1, \ldots, \boldsymbol{v}^j, \boldsymbol{v} - \boldsymbol{v}' \in int(\lambda_{j+1} H)$ lineárisan független rácspont, ami ellentmond λ_{j+1} definíciójának. Ebből az következik, hogy

$$V(K_k^n + H_{j+1}) = (2k+1)^{n-j} V(K_k^j + H_{j+1}).$$

Hasonlóan adódik, hogy

$$V(K_k^n + H_j) = (2k+1)^{n-j} V(K_k^j + H_j),$$

így elég belátni, hogy

$$V(K_k^j + H_{j+1}) \geq \left(\frac{\lambda_{j+1}}{\lambda_j}\right)^{n-j} V(K_k^j + H_j).$$

Ehhez vezessük be a következő $f, g \colon \mathbb{R}^n \to \mathbb{R}^n$ lineáris leképezéseket:

$$f(\boldsymbol{x}) = \left(\frac{\lambda_{j+1}}{\lambda_j} x_1, \ldots, \frac{\lambda_{j+1}}{\lambda_j} x_j, x_{j+1}, \ldots, x_n\right),$$
$$g(\boldsymbol{x}) = \left(x_1, \ldots, x_j, \frac{\lambda_{j+1}}{\lambda_j} x_{j+1}, \ldots, \frac{\lambda_{j+1}}{\lambda_j} x_n\right).$$

Mivel $V(K_k^j + H_{j+1}) = g(K_k^j + f(H_j))$, így

$$V(K_k^j + H_{j+1}) = \left(\frac{\lambda_{j+1}}{\lambda_j}\right)^{n-j} V(K_k^j + f(H_j)),$$

vagyis elegendő az

$$V(K_k^j + H_j) \leq V(K_k^j + f(H_j))$$

egyenlőtlenséget igazolni. Egyszerű geometriai észrevétel, hogy $\forall \boldsymbol{x} \in L_j^{\perp}$-ra $\exists \boldsymbol{y} \in L_j$, amelyre

$$H_j \cap (\boldsymbol{x} + L_j) \subset \boldsymbol{y} + (f(H_j) \cap (\boldsymbol{x} + L_j)), \text{ azaz}$$

$$(K_k^j + H_j) \cap (\boldsymbol{x} + L_j) \subset \boldsymbol{y} + [(K_k^j + f(H_j)) \cap (\boldsymbol{x} + L_j)].$$

Ekkor a j-dimenziós térfogatot V_j-vel jelölve és a Fubini-tételt alkalmazva a bizonyítandó

$$V(K_k^j + f(H_j)) = \int_{\boldsymbol{x} \in L_j^\perp} V_j((K_k^j + f(H_j)) \cap (\boldsymbol{x} + L_j))\, d\boldsymbol{x} \geq$$

$$\int_{\boldsymbol{x} \in L_j^\perp} V_j((K_k^j + H_j) \cap (\boldsymbol{x} + L_j))\, d\boldsymbol{x} = V(K_k^j + H_j)$$

egyenlőtlenséget kapjuk.
A tételben szereplő baloldali egyenlőtlenség bizonyításához vegyünk olyan lineárisan független $\boldsymbol{v}^1, \ldots, \boldsymbol{v}^n \in \Lambda_0$ rácspontokat, amelyekre $j = 1, \ldots, n$ esetén $\boldsymbol{v}^j \in \lambda_j H$. Mivel H az origóra szimmetrikus konvex test, így ekkor tartalmazza az $M = conv\left\{\pm\frac{\boldsymbol{v}^1}{\lambda_1}, \ldots, \pm\frac{\boldsymbol{v}^n}{\lambda_n}\right\}$ keresztpolitópot. Vagyis a 2.11-es lemma szerint

$$V(H) \geq V(M) = \frac{2^n}{n!}\left|\det\left(\frac{\boldsymbol{v}^1}{\lambda_1}, \ldots, \frac{\boldsymbol{v}^n}{\lambda_n}\right)\right| = \frac{2^n|\det(\boldsymbol{v}^1, \ldots, \boldsymbol{v}^n)|}{n!\lambda_1 \cdots \lambda_n} \geq$$
$$\geq \frac{2^n}{n!\lambda_1 \cdots \lambda_n}.$$

Mivel $d(\Lambda_0) = 1$, így éppen ezt kellett bizonyítani. □

Megjegyzés. Ebből a tételből következik a Minkowski-féle konvex test tétel, ugyanis

$$\lambda_1^n V(H) \leq \lambda_1 \cdots \lambda_n V(H) \leq 2^n d(\Lambda),$$

így ha $2^n d(\Lambda) \leq V(H)$, akkor $\lambda_1 \leq 1$, ami ekvivalens a konvex test tétellel.

Ugyan Minkowski második tételének nincs olyan sokféle ismert felhasználása, mint az eredetinek, de például érdekes becslések adhatók egy konvex test rácspontjainak a számára a szukcesszív minimumok segítségével.
Mostantól jelölje $\#(H \cap \Lambda)$ a H test Λ-beli rácspontjainak a számát.

3.19. Lemma. Legyen Λ egy n-dimenziós rács, Λ' a Λ részrácsa, és $H \subset \mathbb{R}^n$ egy origóra szimmetrikus konvex test. Ekkor

$$\#(H \cap \Lambda) \leq \frac{d(\Lambda')}{d(\Lambda)} \#(2H \cap \Lambda').$$

Bizonyítás. Legyen $k = \#(H \cap \Lambda)$, és tegyük fel, hogy létezik minimum $k+1$ különböző $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{k+1} \in \Lambda \cap H$ pont, amikre $i = 1, \ldots, k+1$-re $\boldsymbol{u}_1 - \boldsymbol{u}_i \in \Lambda'$. Mivel H az origóra szimmetrikus és konvex, így $H - H = 2H$. Tehát $i = 1, \ldots, k+1$-re

$$\boldsymbol{u}_1 - \boldsymbol{u}_i \in (H - H) \cap \Lambda' = 2H \cap \Lambda',$$

ami ellentmondás, mert $\#(H \cap \Lambda) = k$. Vagyis Λ-nak minden Λ'-szerinti mellékosztálya legfeljebb k darab $\Lambda \cap H$-beli pontot tartalmaz. Az algebrából ismert Lagrange-tétel szerint Λ-nak $\frac{d(\Lambda)}{d(\Lambda')}$ darab Λ'-szerinti mellékosztálya van. Ez bizonyítja a lemma állítását. □

3.20. Tétel. *Legyen $n \geq 2$, Λ egy n-dimenziós rács, és $H \subset \mathbb{R}^n$ egy origóra szimmetrikus konvex test. Ekkor*

$$\#(H \cap \Lambda) < 2^{n-1} \prod_{i=1}^{n} \left\lfloor \frac{2}{\lambda_i(H, \Lambda)} + 1 \right\rfloor.$$

Bizonyítás. Ha az $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in \Lambda$ lineárisan független pontok olyanok, hogy $i = 1, \ldots, n$-re $\boldsymbol{u}_i \in \lambda_i(H, \Lambda)H$, akkor a szukcesszív minimumok definíciója szerint

$$int(\lambda_i(H, \Lambda)H) \cap \Lambda \subset span\{\boldsymbol{0}, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}\} \cap \Lambda.$$

Ezt összevetve a Minkowski második tételét megelőző észrevételekkel és azzal, hogy tetszőleges A nemszinguláris mátrixra $\#(H \cap \Lambda) = \#(AH \cap A\Lambda)$ feltehetjük, hogy $\Lambda = \Lambda_0$, és $i = 1, \ldots, n$-re

$$int(\lambda_i(H, \Lambda_0)H) \cap \Lambda_0 \subset span\{\boldsymbol{0}, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_{i-1}\} \cap \Lambda_0.$$

Legyen $i = 1, \ldots, n$ esetén $c_i = \prod_{i=1}^{n} \left\lfloor \frac{2}{\lambda_i(H, \Lambda)} + 1 \right\rfloor$. Megmutatjuk, hogy konstruálhatók olyan d_i természetes számok, amelyekre teljesül, hogy $d_n = c_n$, és $i = 1, \ldots, n-1$-re $c_i \leq d_i < 2c_i$, valamint d_i-nek osztója d_{i+1}. Meg kell mutatni, hogy megadható ilyen d_k, feltéve, hogy $d_n, \ldots, d_{k+1}$-et már megkonstruáltuk. Ha $d_{k+1} \geq c_k$, akkor legyen $d_k = d_{k+1}$. Ekkor az oszthatóság nyilván teljesül, és $c_k \leq d_{k+1} = d_k < 2c_{k+1} \leq 2c_k$.
Ha $d_{k+1} < c_k$, akkor maradékosan osztjuk c_k-at d_{k+1}-gyel, azaz $c_k = qd_{k+1} + r$, ahol $q > 0$ és $0 \leq r < d_{k+1}$ egész számok. Ez esetben legyen $d_k = d_{k+1} + c_k - r$. Ekkor d_{k+1} osztója d_k-nak, és $c_k \leq d_k < 2c_k$.
Λ' legyen a Λ_0-nak az a részrácsa, amit a $d_1\boldsymbol{e}_1, \ldots, d_n\boldsymbol{e}_n$ vektorok generálnak. Vagyis $\frac{d(\Lambda')}{d(\Lambda_0)} = d_1 \ldots d_n$, így a 3.19-es lemmát alkalmazva

$$\#(H\cap\Lambda_0) \le d_1 \dots d_n \#(2H\cap\Lambda') < 2^{n-1}\prod_{i=1}^{n}\left\lfloor \frac{2}{\lambda_i(H,\Lambda)}+1\right\rfloor \#(2H\cap\Lambda')$$

adódik. Tehát a bizonyítás befejezéséhez elég megmutatnunk, hogy

$$\#(2H\cap\Lambda') = 1.$$

$2H$ az origóra szimmetrikus és konvex, így $\mathbf{0}\in 2H\cap\Lambda'$. Tegyük fel, hogy $\mathbf{0}\neq \boldsymbol{p}\in 2H\cap\Lambda'$, és p_m legyen $\boldsymbol{p}$-nek a legnagyobb indexű nem nulla koordinátája. Ekkor megfelelő $b_1,\dots,b_m\in\mathbb{Z}$ számokkal $\boldsymbol{p}$ a következő alakban írható fel:

$$\boldsymbol{p} = b_1 d_1 \boldsymbol{e}_1 + \dots + b_m d_m \boldsymbol{e}_m \in 2H.$$

Mivel d_m osztja a $d_1,\dots,d_m$ számokat, így $\frac{1}{d_m}\boldsymbol{p}\in\frac{2H}{d_m}\cap\Lambda_0$. Másrészt $d_1,\dots,d_n$ konstrukciója miatt $\frac{2}{d_m}\le\lambda_m(H,\Lambda_0)$, ezért $\frac{2H}{d_m}\cap\Lambda_0\subset int(\lambda_m(H,\Lambda_0)H)\cap\Lambda_0$, azaz

$$\frac{1}{d_m}\boldsymbol{p}\in int(\lambda_m(H,\Lambda_0)H)\cap\Lambda_0.$$

De feltevésünk szerint

$$int(\lambda_m(H,\Lambda_0)H)\cap\Lambda_0\subset span\{\mathbf{0},\boldsymbol{e}_1,\dots,\boldsymbol{e}_{m-1}\}\cap\Lambda_0,$$

ami viszont ellentmondás, mivel $p_m\neq 0$. Vagyis $2H\cap\Lambda'=\{\mathbf{0}\}$. □

3.21. Tétel. *Tetszőleges n-dimenziós Λ rácsra és $H\subset\mathbb{R}^n$ origóra szimmetrikus konvex testre*

$$\#(H\cap\Lambda)\le\left(\left\lfloor\frac{2}{\lambda_1(H,\Lambda)}+1\right\rfloor\right)^n.$$

Sőt, ha H szigorúan konvex, akkor

$$\#(H\cap\Lambda)\le 2\left(\left\lceil\frac{2}{\lambda_1(H,\Lambda)}\right\rceil\right)^n-1.$$

Mindkét becslés éles.

Bizonyítás. Most is elegendő a $\Lambda=\Lambda_0$ rácsra bizonyítani. Legyen $d=\left\lfloor\frac{2}{\lambda_1(H,\Lambda)}+1\right\rfloor$, és tegyük fel, hogy létezik H-ban két különböző

$\boldsymbol{u} = (u_1, \ldots, u_n)$ és $\boldsymbol{v} = (v_1, \ldots, v_n)$ rácspont úgy, hogy $i = 1, \ldots, n$-re $u_i \equiv v_i \pmod{d}$. Mivel $\frac{2}{d} < \lambda_1(H, \Lambda)$ és H konvex, így

$$\frac{\boldsymbol{u} - \boldsymbol{v}}{d} = \frac{1}{2}\left(\frac{2}{d}\boldsymbol{u}\right) + \frac{1}{2}\left(-\frac{2}{d}\boldsymbol{v}\right) \in int(\lambda_1(H, \Lambda 0)H) \cap (\Lambda_0 \setminus \{\boldsymbol{0}\}),$$

ami ellentmond λ_1 definíciójának. Tehát nincs két olyan H-beli rácspont, amelyeknek mind az n darab koordinátájuk azonos d-szerinti maradékosztályba tartozna. Ebből $d = \left\lfloor \frac{2}{\lambda_1(H,\Lambda)} + 1 \right\rfloor$ miatt következik a tétel első fele.
Tetszőleges $l \in \mathbb{N}$ számra a $K = \{\boldsymbol{x} \in \mathbb{R}^n : |x_i| \leq l; i = 1, \ldots, n\}$ n-dimenziós kockára

$$\#(K, \Lambda_0) = (2l+1)^n = \left(\left\lfloor \frac{2}{\lambda_1(K, \Lambda_0)} + 1 \right\rfloor\right)^n,$$

így a becslés valóban éles. Ha H szigorúan konvex, akkor legyen $d = \left\lceil \frac{2}{\lambda_1(H,\Lambda)} \right\rceil$, és $\boldsymbol{u}, \boldsymbol{v} \in H \cap \Lambda_0$ olyan pontok, amelyek megfelelő koordinátái kongurensek $\pmod{d}$. Ekkor $\frac{2}{d} \leq \lambda_1(H, \Lambda)$ miatt $\frac{1}{2}\left(\frac{2}{d}\boldsymbol{u}\right) + \frac{1}{2}\left(-\frac{2}{d}\boldsymbol{v}\right)$ pont a $\lambda_1(H, \Lambda_0)$ határán van, ami H szigorú konvexitása miatt csakis úgy lehet, hogy $\boldsymbol{u} = -\boldsymbol{v}$. Vagyis minden koordináta d-szerinti maradékosztályához legfeljebb egy $\boldsymbol{u}, -\boldsymbol{u}$ pontpár tartozhat, ahol $\boldsymbol{u} \in H \cap (\Lambda_0 \setminus \{\boldsymbol{0}\}$. Ez bizonyítja a tétel második részét. □

Máig is bizonyítatlan sejtés, hogy az előző tétel a következő módon erősíthető:
Tetszőleges n-dimenziós Λ rácsra és $H \in \mathbb{R}^n$ origóra szimmetrikus konvex testre

$$\#(H \cap \Lambda) \leq \prod_{i=1}^{n} \left\lfloor \frac{2}{\lambda_i(H, \Lambda)} + 1 \right\rfloor.$$

Sőt, ha H szigorúan konvex, akkor

$$\#(H \cap \Lambda) \leq 2\left(\prod_{i=1}^{n} \left\lceil \frac{2}{\lambda_i(H, \Lambda)} \right\rceil\right) - 1.$$

Azonban $n = 2$ esetre a sejtés bizonyíthatóan igaz.

3.22. Tétel. *Egy 2-dimenziós Λ rácsra és $H \subset \mathbb{R}^2$ origóra szimmetrikus konvex síkidomra az*

$$\#(H \cap \Lambda) \leq \left\lfloor \frac{2}{\lambda_1(H, \Lambda)} + 1 \right\rfloor \left\lfloor \frac{2}{\lambda_2(H, \Lambda)} + 1 \right\rfloor$$

egyenlőtlenség is teljesül. Sőt, ha H szigorúan konvex, akkor

$$\#(H \cap \Lambda) < 2 \left\lceil \frac{2}{\lambda_1(H,\Lambda)} \right\rceil \left\lceil \frac{2}{\lambda_2(H,\Lambda)} \right\rceil - 1.$$

Bizonyítás. Megint elég a tételt a $\Lambda = \Lambda_0 = \mathbb{Z}^2$ rácsra bizonyítani. Legyen $\boldsymbol{v}_1$ és $\boldsymbol{v}_2$ két lineárisan független rácspont, amelyekre $\boldsymbol{v}_1 \in \lambda_1(H,\Lambda_0)$ és $\boldsymbol{v}_2 \in \lambda_2(H,\Lambda_0)$, és az őket összekötő szakaszon nincs más rácspont. Ekkor $conv\{\mathbf{0}, \boldsymbol{v}_1, \boldsymbol{v}_2\} \cap \Lambda_0 = \{\mathbf{0}, \boldsymbol{v}_1, \boldsymbol{v}_2\}$, így alkalmazhatjuk a 2.6.1-es következményt, amely szerint $\boldsymbol{v}_1, \boldsymbol{v}_2$ a rács bázisa. A 2.2-es lemma szerint feltehető, hogy $\boldsymbol{v}_1 = (1,0)$ és $\boldsymbol{v}_2 = (0,1)$. Legyen $j = 1,2$-re $d_j = \left\lfloor \frac{2}{\lambda_j(H,\Lambda_0)} + 1 \right\rfloor$, és tekintsük az alábbi $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ lineáris leképezést:

$$f((x_1,x_2)) = \left(\frac{2}{d_1} x_1, \frac{2}{d_2} x_2 \right).$$

Mivel $\frac{2}{d_2} < \lambda_2(H,\Lambda_0)$, így a második szukcesszív minimum definíciója szerint $f(H)$ legfeljebb egy lineárisan független rácspontot tartalmazhat, azaz $\boldsymbol{v}_1$-et. De $\frac{2}{d_1} < \lambda_1(H,\Lambda_0)$, így $f(H)$ nem tartalmazhatja $\boldsymbol{v}_1$-et sem, vagyis $f(H) \cap \Lambda_0 = \{\mathbf{0}\}$.
Legyenek $\boldsymbol{a}, \boldsymbol{b} \in H$ olyan rácspontok, amelyekre

$$a_1 \equiv b_1 \pmod{d_1} \text{ és } a_2 \equiv b_2 \pmod{d_2}.$$

H konvex és f lineáris leképezés, ezért $f(H)$ is konvex, így

$$\frac{1}{2} f(\boldsymbol{a}) + \frac{1}{2} f(-\boldsymbol{b}) = \left(\frac{a_1 - b_1}{d_1}, \frac{a_2 - b_2}{d_2} \right) \in f(H) \cap (\Lambda_0 \setminus \{\mathbf{0}\}).$$

Ez azonban ellentmondás, tehát nincs két olyan rácspont H-ban, amelyeknek megfelelő koordinátáik rendre azonos maradékosztályba tartoznának d_1-gyel illetve d_2-vel osztva is. Vagyis H-ban legfeljebb $d_1 d_2$ darab rácspont lehet.
Ha H szigorúan konvex, akkor legyen $j = 1,2$-re $d_j = \left\lceil \frac{2}{\lambda_j(H,\Lambda_0)} \right\rceil$, és az $\boldsymbol{a}, \boldsymbol{b}$ pontokat, valamint az f függvényt definiáljuk úgy, mint az előző esetben. Most $j = 1,2$-re $\frac{2}{d_j} \leq \lambda_j(H,\Lambda_0)$, ezért az előző esettel analóg módon azt kapjuk, hogy $int(f(H)) \cap \Lambda_0 = \{\mathbf{0}\}$. Így $\frac{1}{2} f(\boldsymbol{a}) + \frac{1}{2} f(-\boldsymbol{b})$ a szigorúan konvex H határán van, ami csakis úgy lehet, hogy $\boldsymbol{a} = -\boldsymbol{b}$. Vagyis $j = 1,2$-re a j-edik koordináta d_j-szerinti maradékosztályához legfeljebb egy $a_j, -a_j$ koordinátapár tartozhat, ahol $\boldsymbol{a} = (a_1, a_2) \in H \cap (\Lambda_0 \setminus \{\mathbf{0}\})$. Ebből adódik a tétel második része. □

3.23. Tétel. *Legyen Λ egy n-dimenziós rács, $H \subset \mathbb{R}^n$ egy origóra szimmetrikus konvex test, és $\lambda_1(H,\Lambda) \leq 1$. Ekkor*

$$\#(H \cap \Lambda) \geq \frac{2^n}{n!}\left(1 - \frac{\lambda_1(H,\Lambda)}{2}\right)^n \prod_{i=1}^{n} \frac{1}{\lambda_i(H,\Lambda)}.$$

Bizonyítás. Most is elég a $\Lambda = \Lambda_0$ rácsra bizonyítani. Legyenek $i = 1,\ldots,n$-re $\boldsymbol{u}_i \in \lambda_1(H,\Lambda_0)H$ lineárisan független Λ_0-beli rácspontok, vagyis $\frac{\boldsymbol{u}_i}{\lambda_1(H,\Lambda_0)} \in H$. Legyen P az a keresztpolitóp, amelynek csúcsai $\pm\frac{\boldsymbol{u}_i}{\lambda_1(H,\Lambda_0)}$-ek, és Q az a keresztpolitóp, amelynek csúcsai $\pm\frac{\boldsymbol{e}_i}{\lambda_1(H,\Lambda_0)}$-ek. Ekkor nyilván $Q \subset P \subset H$, így

$$\#(H \cap \Lambda_0) \geq \#(P \cap \Lambda_0) \geq \#(Q \cap \Lambda_0).$$

A keresztpolitópok térfogatára megmutatott 2.11-es lemmabeli képlet szerint

$$V(Q) = \frac{2^n}{n!}\prod_{i=1}^{n} \frac{1}{\lambda_i(H,\Lambda)},$$

így elég megmutatni, hogy

$$\left(1 - \frac{\lambda_1(H,\Lambda)}{2}\right)^n V(Q) \leq \#(Q \cap \Lambda_0).$$

Legyen $d = 1 - \frac{\lambda_1(H,\Lambda_0)}{2}$ és $i = 1,\ldots,n$-re $L_i = span\{\boldsymbol{e}_1,\ldots,\boldsymbol{e}_n\}$. Teljes indukcióval megmutatjuk, hogy minden $\boldsymbol{u}_i \in L_i^{\perp} \cap \Lambda_0 \cap dQ$-ra

$$V_i((\boldsymbol{u}_i + L_i) \cap dQ) \leq \#((\boldsymbol{u}_i + L_i) \cap Q \cap \Lambda_0)$$

teljesül ,ahol V_i az i-dimenziós térfogatot jelöli. Ebből következik az állítás, hiszen $n = i$-re az alábbi két egyenlőség teljesül:

$$\#((\boldsymbol{u}_n + L_n) \cap Q \cap \Lambda_0) = \#(H \cap \Lambda_0),$$

$$V_n((\boldsymbol{u}_n + L_n) \cap dQ) = \left(1 - \frac{\lambda_1(H,\Lambda)}{2}\right)^n V(Q).$$

$i = 1$-re az $(\boldsymbol{u}_i + L_i) \cap Q$ szakasz hossza $\frac{2}{\lambda_1(H,\Lambda_0)}$, az $(\boldsymbol{u}_i + L_i) \cap dQ$ szakaszé pedig $\frac{2d}{\lambda_1(H,\Lambda_0)} = \frac{2}{\lambda_1(H,\Lambda_0)} - 1$ kihasználva, hogy Q-nak $\pm\frac{\boldsymbol{e}_i}{\lambda_1(H,\Lambda_0)}$-ek csúcsai és $\boldsymbol{e}_1$ egységnyi hosszú. E mellett tetszőleges S szakaszra $\#(S,\Lambda_0) \geq V_1(S) - 1$, így $i = 1$-re állításunk helyes. Tegyük fel, hogy $i = j$-ig igaz. Legyen $\boldsymbol{u}_{j+1} \in L_{j+1}^{\perp} \cap \Lambda_0 \cap dQ$ és $c := \max\{c \in \mathbb{R} : c\boldsymbol{e}_{j+1} + \boldsymbol{u}_{j+1} \in dQ\}$. Ekkor

$$\#((\boldsymbol{u}_{j+1}+L_{j+1})\cap Q\cap\Lambda_0)=\sum_{k=-\infty}^{\infty}\#((\boldsymbol{u}_{j+1}+k\boldsymbol{e}_{j+1}+L_j)\cap Q\cap\Lambda_0)\geq$$

$$\sum_{k=-\lfloor c\rfloor}^{\lfloor c\rfloor}\#((\boldsymbol{u}_{j+1}+k\boldsymbol{e}_{j+1}+L_j)\cap Q\cap\Lambda_0)\geq\sum_{k=-\lfloor c\rfloor}^{\lfloor c\rfloor}V_j((\boldsymbol{u}_{j+1}+k\boldsymbol{e}_{j+1}+$$

$$L_j)\cap dQ)=V_j((\boldsymbol{u}_{j+1}+L_j)\cap dQ)\sum_{k=-\lfloor c\rfloor}^{\lfloor c\rfloor}\left(1-\frac{|k|}{c}\right)^j,$$

ahol a második egyenlőtlenségnél az $\boldsymbol{u}_{j+1}+k\boldsymbol{e}_{j+1}\in L_i^{\perp}\cap\Lambda_0\cap dQ$ miatt fennálló indukciós lépést alkalmaztuk. Vezessük be a

$$g(x)=\left(1-\frac{x}{c}\right)^j\varkappa(x\in(-\infty,c])$$

folytonos valós függvényt, ahol $\varkappa$ a karakterisztikus függvényt jelöli. Erre

$$\sum_{k=-\lfloor c\rfloor}^{\lfloor c\rfloor}\left(1-\frac{|k|}{c}\right)^j=2\sum_{k=0}^{\lfloor c\rfloor}\left(\frac{g(k)+g(+1)}{2}\right)^j\geq$$

$$2\sum_{k=0}^{\lfloor c\rfloor}\left(g\left(\frac{2k+1}{2}\right)\right)^j\geq 2\int_0^c g(x)\,dx=\frac{2c}{j+1},$$

kihasználva g konvexségét és az integrál-összeg közelítő formulára vonatkozó egyenlőtlenséget. Vagyis

$$V_{j+1}((\boldsymbol{u}_{j+1}+L_{j+1})\cap dQ)=\frac{2c}{j+1}V_j((\boldsymbol{u}_{j+1}+L_j)\cap dQ)\leq$$

$$\leq\#((\boldsymbol{u}_{j+1}+L_{j+1})\cap Q\cap\Lambda_0)$$

felhasználva a keresztpolitópok 2.11-es lemmában felírt térfogatképletét. □

Ezen kívül Minkowski második tételét egy test és polár testének térfogatszorzatának a becslésére is lehet alkalmazni.

3.24. Definíció. Egy olyan $K\subset\mathbb{R}^n$ test polár teste, amelyre $\mathbf{0}\in int(K)$ a következő:

$$K^*=\{\boldsymbol{y}\in\mathbb{R}^n:\langle\boldsymbol{x};\boldsymbol{y}\rangle=1\ \forall\boldsymbol{x}\in K\}.$$

Itt $\langle\cdot;\cdot\rangle$ a skaláris szorzást jelöli.

3.25. Definíció. Egy $\Lambda \subset \mathbb{R}^n$ rács polár rácsa a következő:

$$\Lambda^* = \{\boldsymbol{v} \in \mathbb{R}^n : \langle \boldsymbol{u}; \boldsymbol{v} \rangle \in \mathbb{Z} \ \forall \boldsymbol{u} \in \Lambda\}.$$

3.26. Lemma. Tetszőleges $H \subset \mathbb{R}^n$ origóra szimmetrikus konvex testre

$$\frac{4^n}{(n!)^2} \leq V(H)V(H^*).$$

Bizonyítás. Mivel tetszőleges nemszinguláris $\mathcal{A}\colon \mathbb{R}^n \to \mathbb{R}^n$ lineáris transzformációra $V(H)V(H^*) = V(\mathcal{A}H)V(\mathcal{A}H^*)$, így feltehetjük, hogy a $P = \{\boldsymbol{x} \in \mathbb{R}^n : |x_1| + \cdots + |x_n| \leq 1\}$ keresztpolitóp a H-ba írható keresztpolitópok közül a maximális térfogatú. Ekkor $H \subseteq K$, ahol $K = \{\boldsymbol{x} \in \mathbb{R}^n : |x_i| \leq 1; i = 1, \ldots, n\}$. Mivel $P \subseteq H \subseteq K$, így $K^* \subseteq H^* \subseteq P^*$. Egyszerűen látható, hogy $P = K^*$, mert

$$K^* = \{\boldsymbol{x} \in \mathbb{R}^n : |x_i| \leq 1; i = 1, \ldots, n\}^* = \{\boldsymbol{y} \in \mathbb{R}^n : \langle \boldsymbol{x}; \boldsymbol{y} \rangle \leq 1$$

$$\forall \boldsymbol{x} \in K\} = \{\boldsymbol{y} \in \mathbb{R}^n : |y_1| + \cdots + |y_n| \leq 1\},$$

így a keresztpolitópok térfogatképlete (2.11-es lemma) alapján

$$V(H)V(H^*) \geq V(P)V(K^*) = (V(P))^2 = \left(\frac{2^n}{n!}\right)^2. \qquad \square$$

3.27. Tétel. *Adott egy n-dimenziós Λ rács és $H \subset \mathbb{R}^n$ origóra szimmetrikus konvex test, ahol $\lambda_i = \lambda_i(H, \Lambda)$ és $\lambda_i^* = \lambda_i^*(H, \Lambda)$. Ekkor $i = 1, \ldots, n$-re*

$$1 \leq \lambda_i \lambda_{n-i+1}^* \leq \frac{4^n}{V(H)V(H^*)} \leq (n!)^2.$$

Bizonyítás. Legyenek $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in \Lambda$ és $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in \Lambda^*$ olyan lineárisan független pontok, amelyekre $\forall k, l = 1, \ldots, n$-re $\boldsymbol{u}_k \in \lambda_k H$ és $\boldsymbol{v}_l \in \lambda_l^* H^*$, vagyis $\pm\frac{1}{\lambda_k}\boldsymbol{u}_k \in H$ és $\pm\frac{1}{\lambda_l^*}\boldsymbol{v}_l \in H^*$. A polár test definíciója miatt $\pm\left\langle \frac{\boldsymbol{u}_k}{\lambda_k}; \frac{\boldsymbol{v}_l}{\lambda_l^*} \right\rangle \leq 1$, azaz $\pm\langle \boldsymbol{u}_k; \boldsymbol{v}_l \rangle \leq \lambda_k \lambda_l^*$. Így a polár rács definíciója szerint $\forall k, l = 1, \ldots, n$-re

$$1 \leq \lambda_k \lambda_l^* \text{ vagy } \pm\langle \boldsymbol{u}_k; \boldsymbol{v}_l \rangle = \boldsymbol{0}.$$

Az $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i$ által kifeszített altér i-dimenziós, mert a pontok lineárisan függetlenek. Így ennek az altérnek az ortokomplementere $n - i$-dimenziós, ezért a lineárisan független $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{n-i+1}$ pontok között van olyan $\boldsymbol{v}_l$, ami nincs benne az ortokomplementerben. Tehát megfelelő

$1 \leq k \leq i$ és $1 \leq l \leq n-i+1$-re $\langle \boldsymbol{u}_k; \boldsymbol{v}_l \rangle \neq \mathbf{0}$, ezért $1 \leq \lambda_k \lambda_l^*$. Mivel $k \leq i$ és $l \leq n-i+1$, így $\lambda_k \leq \lambda_i$ és $\lambda_l^* \leq \lambda_{n-i+1}^*$, azaz

$$1 \leq \lambda_k \lambda_l^* \leq \lambda_i \lambda_{n-i+1}^*.$$

Minkowski második tétele szerint

$$\lambda_1 \cdots \lambda_n V(H) \leq 2^n d(\Lambda) \text{ és } \lambda_1^* \cdots \lambda_n^* V(H^*) \leq 2^n d(\Lambda^*),$$

vagyis ezen két egyenlőtlenség megfelelő oldalait összeszorozva

$$V(H)V(H^*) \prod_{i=1}^{n} \lambda_i \lambda_{n-i+1}^* \leq 4^n d(\Lambda) d(\Lambda^*) = 4^n$$

adódik, mert a polár rács definíciója és a determinánsok szorzástétele szerint tetszőleges Λ rácsra $d(\Lambda)d(\Lambda^*) = 1$. Felhasználva a 3.26-es lemmát és azt, hogy minden $i = 1, \ldots, n$-re $\lambda_i \lambda_{n-i+1}^* \geq 1$ a tétel maradék két egyenlőtlenségét is megkapjuk. □

Ezt a tételt kombinálva Minkowski második tételével kaphatunk egy újabb érdekes eredményt a diofantikus approximációhoz kapcsolódóan. Meg fogjuk mutatni, hogy tetszőleges $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$ számokat pontosan akkor nem tudunk szimultán azonos nevezőjű racionális számokkal jól approximálni, ha az $u_1\alpha_1 + \cdots + u_k\alpha_k$ lineáris formát (ahol $u_1, \ldots, u_n$ nem mind 0 egészek) nem tudjuk egészekkel jól approximálni. Ehhez először egy lemmára lesz szükségünk.

3.28. Lemma. Legyenek $H = \{\boldsymbol{x} \in \mathbb{R}^n : |A\boldsymbol{x}| \leq \mathbf{1}\}$ és $K = \{\boldsymbol{x} \in \mathbb{R}^n : |B\boldsymbol{x}| \leq \mathbf{1}\}$, ahol $A, B \in \mathbb{R}^{n \times n}$-es mátrixok, $\mathbf{1} \in \mathbb{R}^n$ csupa 1-es koordinátából álló vektor, és $A^{-T} = B$.
Ekkor az alábbi két egyenlőtlenség teljesül:

$$\lambda_1(H, \Lambda_0) \leq (n\lambda_1(K, \Lambda_0)|\det A|)^{\frac{1}{n-1}} \tag{1}$$

$$\lambda_1(K, \Lambda_0) \leq (n\lambda_1(H, \Lambda_0)|\det B|)^{\frac{1}{n-1}} \tag{2}$$

(Az A^{-T} mátrix $(A^{-1})^T$-at jelöli.)

Bizonyítás. Tetszőleges origóra szimmetrikus L konvex testre

$$(A^{-1}L)^* = \{\boldsymbol{y} \in \mathbb{R}^n : \langle \boldsymbol{y}; A^{-1}\boldsymbol{x} \rangle \leq 1 \forall \boldsymbol{x} \in L\} =$$
$$\{A^T A^{-T}\boldsymbol{y} \in \mathbb{R}^n : \boldsymbol{y}^T A^{-1}\boldsymbol{x} = (A^{-T}\boldsymbol{y})^T\boldsymbol{x} = \langle A^{-T}\boldsymbol{y}; \boldsymbol{x} \rangle \leq 1 \forall \boldsymbol{x} \in L\}$$
$$= \{A^T\boldsymbol{z} \in \mathbb{R}^n : \langle \boldsymbol{z}; \boldsymbol{x} \rangle \leq 1 \forall \boldsymbol{x} \in L\} = A^T L^*, \text{ így}$$
$$H^* = \{\boldsymbol{x} \in \mathbb{R}^n : |A\boldsymbol{x}| \leq \mathbf{1}\}^* = \{A^{-1}\boldsymbol{x} \in \mathbb{R}^n : |\boldsymbol{x}| \leq \mathbf{1}\}^* =$$
$$A^T\{\boldsymbol{x} \in \mathbb{R}^n : |\boldsymbol{x}| \leq \mathbf{1}\}^* = B^{-1}\{\boldsymbol{y} \in \mathbb{R}^n : |y_1| + \cdots + |y_n| \leq 1\} =$$
$$\{\boldsymbol{z} \in \mathbb{R}^n : |b_{11}z_1 + \cdots + b_{1n}z_n| + \cdots + |b_{n1}z_1 + \cdots + b_{nn}z_n| \leq 1\}.$$

Ebből az következik, hogy $\frac{1}{n}K \subset H^* \subset K$, azaz

$$\lambda_1(K, \Lambda_0) \leq \lambda_1(H^*, \Lambda_0) \leq n\lambda_1(K, \Lambda_0).$$

Minkowski második tétele szerint

$$(\lambda_1(H, \Lambda_0))^{n-1} \leq \lambda_1(H, \Lambda_0) \dots \lambda_{n-1}(H, \Lambda_0) \leq$$
$$\leq \frac{2^n}{\lambda_n(H, \Lambda_0)V(H)} = \frac{|\det A|}{\lambda_n(H, \Lambda_0)}.$$

Az 3.27-es tétel szerint $1 \leq \lambda_n(H, \Lambda_0)\lambda_1(H^*, \Lambda_0)$, így

$$(\lambda_1(H, \Lambda_0))^{n-1} \leq \frac{2^n}{\lambda_n(H, \Lambda_0)V(H)} = \frac{\det A}{\lambda_n(H, \Lambda_0)} \leq \lambda_1(H^*, \Lambda_0)|\det A|.$$

Mivel $\lambda_1(H^*, \Lambda_0) \leq n\lambda_1(K, \Lambda_0)$, így

$$(\lambda_1(H, \Lambda_0))^{n-1} \leq \lambda_1(H^*, \Lambda_0)|\det A| \leq n\lambda_1(K, \Lambda_0)|\det A|,$$

vagyis az első bizonyítandó egyenlőtlenséget beláttuk. (2) szimmetriai okokból ugyanígy következik. □

3.29. Tétel. *Tetszőleges $\alpha_1, \dots, \alpha_k \in \mathbb{R}$ számokra a következők ekvivalensek:*

- *Létezik $b > 0$ konstans úgy, hogy a következő egyenlőtlenségrendszernek nincs $(u_0, u_1, \dots, u_k)$ egész megoldása, ahol $u_0 \neq 0$:*

$$\left|\alpha_1 - \frac{u_1}{u_0}\right| \leq \frac{b}{u_0^{1+\frac{1}{k}}}, \dots, \left|\alpha_k - \frac{u_k}{u_0}\right| \leq \frac{b}{u_0^{1+\frac{1}{k}}}.$$

- *Létezik $c > 0$ konstans úgy, hogy a következő egyenlőtlenségnek nincs a csupa 0-ból álló megoldáson kívül egész $(u_0, u_1, \dots, u_k)$ megoldása:*

$$|u_1\alpha_1 + \dots + u_k\alpha_k - u_0| \leq \frac{c}{(\max\{|u_1|, \dots, |u_k|\})^k}.$$

Bizonyítás. Csak azt mutatjuk meg, hogy az első állításból következik a második. A másik irány teljesen hasonlóan működik.
Ha az első állítás teljesül, akkor $f > b^k$ esetén az

$$|u_0| \leq f, |u_0\alpha_1 - u_1| \leq \frac{b}{f^{\frac{1}{k}}}, \dots, |u_0\alpha_k - u_k| \leq \frac{b}{f^{\frac{1}{k}}}$$

egyenlőtlenség-rendszernek csak a triviális egész megoldása létezik, ezért

$$H = \left\{ \boldsymbol{x} \in \mathbb{R}^{k+1} : \left|\tfrac{1}{f} x_0\right| \le 1, \left|\tfrac{f^{\frac{1}{k}}}{b}(x_1 - \alpha_1 x_0)\right| \le 1, \dots, \left|\tfrac{f^{\frac{1}{k}}}{b}(x_k - \alpha_k x_0)\right| \le 1 \right\}$$

a $\mathbb{Z}^{k+1}$ rácsból nem tartalmaz az origón kívül más rácspontot. Azaz $\lambda_1(H, \mathbb{Z}^{k+1}) > 1$. A H-t meghatározó lineáris formák együtthatómátrixa legyen A, azaz

$$A = \begin{pmatrix} \frac{1}{f} & 0 & 0 & \dots & 0 \\ -\frac{f^{\frac{1}{k}}\alpha_1}{b} & \frac{f^{\frac{1}{k}}}{b} & 0 & \dots & 0 \\ \dots & & & & \\ -\frac{f^{\frac{1}{k}}\alpha_k}{b} & 0 & \dots & 0 & \frac{f^{\frac{1}{k}}}{b} \end{pmatrix}$$

Ez egy alsó-háromszög mátrix, így izverzének a transzponáltja egyszerűen meghatározható:

$$A^{-T} = \begin{pmatrix} f & f\alpha_1 & f\alpha_2 & \dots & f\alpha_k \\ 0 & \frac{b}{f^{\frac{1}{k}}} & 0 & \dots & 0 \\ \dots & & & & \\ 0 & 0 & \dots & 0 & \frac{b}{f^{\frac{1}{k}}} \end{pmatrix}$$

$$K := \left\{ \boldsymbol{x} \in \mathbb{R}^{k+1} : f\,|\alpha_1 x_1 + \dots + \alpha_k x_k + x_0| \le 1,\ \max_{1 \le i \le k} \left|\frac{b}{f^{\frac{1}{k}}} x_i\right| \le 1 \right\}$$

esetén A^{-T} éppen a K-t meghatározó lineáris forma együtthatómátrixa, így $\lambda_1(H, \mathbb{Z}^{k+1}) > 1$, és a 3.28-es lemma miatt

$$((k+1)\lambda_1(K, \mathbb{Z}^{k+1})|\det A|)^{\frac{1}{k}} \ge \lambda_1(H, \mathbb{Z}^{k+1}) > 1,$$

vagyis

$$\frac{b^k}{k+1} < \frac{(\lambda_1(H, \mathbb{Z}^{k+1}))^k}{(k+1)|\det A|} \le \lambda_1(K, \mathbb{Z}^{k+1})$$

kihasználva, hogy $\det A = \frac{1}{b^k}$. Ebből következik, hogy $\frac{b^k}{k+1} K \cap \mathbb{Z}^{k+1} = \{\mathbf{0}\}$. Mivel

$$K = \left\{ \boldsymbol{x} \in \mathbb{R}^{k+1} : |\alpha_1 x_1 + \dots + \alpha_k x_k + x_0| \le \tfrac{1}{f}, |x_1| \le \tfrac{f^{\frac{1}{k}}}{b}, \dots, |x_k| \le \tfrac{f^{\frac{1}{k}}}{b} \right\},$$

így ebből adódik, hogy az

$$|\alpha_1 x_1 + \cdots + \alpha_k x_k + x_0| \leq \frac{b^k}{(k+1)f}, |x_1| \leq \frac{b^{k-1} f^{\frac{1}{k}}}{k+1}, \ldots, |x_k| \leq \frac{b^{k-1} f^{\frac{1}{k}}}{k+1}$$

egyenlőtlenség-rendszernek nincsen nemtriviális egész megoldása, vagyis nincs olyan $(u_0, u_1, \ldots, u_n)$ egész megoldása, amelyre $(u_1, \ldots, u_n) \neq (0, \ldots, 0)$. Az $m = \frac{b^{k-1} f^{\frac{1}{k}}}{k+1}$ és $c = \frac{b^{k^2}}{(k+1)^{k+1}}$ helyettesítésből adódik, hogy az

$$|\alpha_1 x_1 + \cdots + \alpha_k x_k + x_0| \leq \frac{c}{m^k}, |x_1| \leq m, \ldots, |x_k| \leq m$$

egyenlőtlenség-rendszernek nincs olyan $(u_0, u_1, \ldots, u_n)$ egész megoldása, ahol $(u_1, \ldots, u_n) \neq (0, \ldots, 0)$, ami az x_0 helyett $-x_0$-át behelyettesítve ekvivalens azzal, hogy az

$$|\alpha_1 x_1 + \cdots + \alpha_k x_k - x_0| \leq \frac{c}{m^k}, |x_1| \leq m, \ldots, |x_k| \leq m$$

rendszernek sincsen ilyen megoldása. □

4. Elfogadható rácsok

4.1. Definíció. Adott egy H ponthalmaz és egy Λ rács. Ha Λ-nak legfeljebb az origó az egyetlen olyan pontja, amelyet H tartalmaz, akkor Λ-t H-elfogadhatónak hívjuk.

4.1. Becslések a rácskonstansra

4.2. Definíció. A $\Delta(H) = \inf_{\mathcal{A}(H)} d(\Lambda)$ kifejezés értékét a H halmaz rácskonstansának hívjuk, ahol $\mathcal{A}(H) = \{\Lambda : \Lambda H\text{-elfogadható}\}$. Ha $\mathcal{A}(H) = \emptyset$, akkor $\Delta(H) = \infty$.

4.3. Definíció. Ha egy H-elfogadható Λ rácsra $\Delta(H) = d(\Lambda)$ teljesül, akkor azt mondjuk, hogy Λ a H halmaz kritikus rácsa.

Ha H az origóra szimmetrikus, konvex halmaz, akkor a Minkowski-féle konvex test tételből kapjuk az alábbi alsó becslést:

$$\Delta(H) \geq \frac{1}{2^n} V(H).$$

Ha H nem ilyen tulajdonságú, de írható a belsejébe egy origóra szimmetrikus, konvex H' halmaz, akkor mivel minden H-elfogadható rács egyben H'-elfogadható is, így az előző becslés szerint $\Delta(H) \geq \Delta(H') \geq \frac{1}{2^n} V(H')$.
Halmazok rácskonstansának felső becslésére a Minkowski-Hlawka tétel segítségével kaphatunk eredményeket. Ehhez szükségünk lesz néhány előkészítő lemmára.

4.4. Lemma. Adott egy p prímszám és egy n-dimenziós Λ rács. $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ legyenek olyan Λ-beli pontok amelyek nem $p\boldsymbol{a}$, $\boldsymbol{a} \in \Lambda$ alakúak, $m_1, \ldots, m_k$ pedig legyenek tetszőleges valós számok. Ekkor létezik olyan Γ rács, amelynek az indexe Λ-ban p, és

$$\sum_{\boldsymbol{a}_{k'} \in \Gamma} m_{k'} \leq \frac{p^{n-1} - 1}{p^n - 1} \sum_{1 \leq k' \leq k} m_{k'}.$$

Bizonyítás. $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ legyen a Λ rács egy bázisa, és vegyünk olyan p-nél kisebb $l_1, \ldots, l_n$ nemnegatív egész számokat, amelyek közül nem mindegyik 0. A Γ rács álljon a $h_1\boldsymbol{v}_1 + \cdots + h_n\boldsymbol{v}_n$ alakú rácspontokból, ahol $h_1, \ldots, h_n \in \mathbb{Z}$ és

$$h_1 l_1 + \cdots + h_n l_n \equiv 0 \pmod{p}.$$

Mivel Λ a $h_1\boldsymbol{v}_1+\cdots+h_n\boldsymbol{v}_n$ alakú rácspontokból áll, ahol $h_1,\ldots,h_n\in\mathbb{Z}$, Γ pedig azon $h_1\boldsymbol{v}_1+\cdots+h_n\boldsymbol{v}_n$ alakúakból, ahol $h_1,\ldots,h_n\in\mathbb{Z}$, de közülük $n-1$ darab egyértelműen meghatározza az n-ediket (mod p), így Γ indexe Λ-ban p. A lehetséges Γ rácsok száma p^n-1, mert ennyiféle lehetséges $(l_1,\ldots,l_n)$ létezik.
Minden $\boldsymbol{a}_{k'}\in\Lambda$, ami nem $p\boldsymbol{a}$, $\boldsymbol{a}\in\Lambda$ alakú felírható

$$\boldsymbol{a}_{k'}=h_{k'1}\boldsymbol{v}_1+\cdots+h_{k'n}\boldsymbol{v}_n$$

alakban, ahol a $h_{k'1},\ldots,h_{k'n}$ egész számok nem mind oszthatók p-vel. Ha $h_{k'i}$ a p-vel nem osztható (az egyik, ha több is van), akkor a

$$h_{k'1}l_1+\cdots+h_{k'n}l_n\equiv 0 \pmod{p}$$

kongurencia egyértelműen meghatározza l_i-t Ha $l_1=\cdots=l_{i-1}=l_{i+1}=\cdots=l_n=0$, akkor $l_i=0$, ami nem lehetséges, így $(l_1,\ldots,l_{i-1}=l_{i+1},\ldots,l_n)$ pontosan $p^{n-1}-1$-féle lehet. Vagyis minden ilyen tulajdonságú $\boldsymbol{a}_{k'}$ éppen $p^{n-1}-1$ lehetséges Γ rácsnak pontja ($k'=1,\ldots,k$). Ebből következik, hogy $\sum_{\boldsymbol{a}_{k'}\in\Gamma} m_{k'}$-et átlagolva az összes lehetséges Γ rácsra éppen $\frac{p^{n-1}-1}{p^n-1}\sum_{1\le k'\le k} m_{k'}$ adódik, azaz létezik olyan Γ rács, amire

$$\sum_{\boldsymbol{a}_{k'}\in\Gamma} m_{k'}\le\frac{p^{n-1}-1}{p^n-1}\sum_{1\le k'\le k} m_{k'}.$$

□

4.4.1. Következmény. Adott egy p prímszám és egy n-dimenziós Λ rács. $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_p$ legyenek olyan Λ-beli pontok amelyek nem $p\boldsymbol{a}$, $\boldsymbol{a}\in\Lambda$ alakúak. Ekkor létezik olyan Γ rács, amely nem tartalmazza az $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_p$ pontokat, és az indexe Λ-ban p.

Bizonyítás. Alkalmazzuk a 4.4-es lemmát úgy, hogy $k'=1,\ldots,p$-re $m_{k'}=1$ legyen. Ekkor

$$\sum_{\boldsymbol{a}_{k'}\in\Gamma} 1\le\frac{p^{n-1}-1}{p^n-1}p<1,$$

amiből az állítás következik. □

4.5. Lemma. $f\colon \mathbb{R}^n \to \mathbb{R}$ legyen egy Riemann-integrálható függvény, ami egy korlátos halmazon kívül azonosan 0. Ekkor adott $\varepsilon > 0$ és $d_1 > 0$ számokhoz létezik olyan Γ rács, aminek determinánsa d_1 és

$$d_1 \sum_{\substack{\boldsymbol{a}\in\Gamma\\ \boldsymbol{a}\neq\boldsymbol{0}}} f(\boldsymbol{a}) < \varepsilon + \int f(\boldsymbol{x})\, d\boldsymbol{x}.$$

(Jelölésünk szerint $\boldsymbol{x} = (x_1, \dots, x_n)$ és $d\boldsymbol{x} = dx_1 \dots dx_n$).

Bizonyítás. Legyen $\alpha = \left(\frac{d_1}{p}\right)^{\frac{1}{n}}$. Mivel minden $\mathbb{R}^n$-beli korlátos halmaz befoglalható egy origó középpontú n-dimenziós kockába, így feltehető, hogy $\forall \boldsymbol{x} \notin K$-ra $f(\boldsymbol{x}) = 0$, ahol K az origó középpontú $2c$-élű kocka (c valós konstans).
Definiáljuk a

$$\Lambda := \{(\alpha k_1, \dots, \alpha k_n) : k_1, \dots, k_n \in \mathbb{Z}\}$$

rácsot. Ennek egy bázisa $(\alpha, \dots, \alpha)$, így $d(\Lambda) = \alpha^n$.
Mivel f Riemann-integrálható, így kellően kicsi α-ra az integrálja a megfelelő integrálközelítő-összeggel alulról becsülhető:

$$\alpha^n \sum_{\substack{\boldsymbol{a}\in\Lambda\\ \boldsymbol{a}\neq\boldsymbol{0}}} f(\boldsymbol{a}) < \varepsilon + \int f(\boldsymbol{x})\, d\boldsymbol{x}.$$

$\alpha = \left(\frac{d_1}{p}\right)^{\frac{1}{n}}$ miatt α akkor lesz kellően kicsi, ha p elég nagy. p-t válasszuk olyan nagynak, hogy $p > \frac{c}{\alpha}$ teljesüljön. Mivel azok az origótól különböző $\boldsymbol{a} \in \Lambda$ pontok, amikre $f(\boldsymbol{a}) \neq 0$ a K-n kívül vannak, így nem lehetnek $p\boldsymbol{a}'$, $\boldsymbol{a}' \in \Lambda$ alakúak. Ezért a 4.4-es lemma jelöléseivel $\boldsymbol{a}_1, \dots, \boldsymbol{a}_k$ legyenek azok az $\boldsymbol{a} \in \Lambda$ origótól különböző pontok, amikre $f(\boldsymbol{a}) \neq 0$, és $m_i := f(\boldsymbol{a}_i)$ minden $i = 1, \dots, k$-re. Ekkor létezik olyan Γ rács, amire

$$\sum_{\substack{\boldsymbol{a}\in\Gamma\\ \boldsymbol{a}\neq\boldsymbol{0}}} f(\boldsymbol{a}) \leq \frac{p^{n-1}-1}{p^n-1} \sum_{\substack{\boldsymbol{a}\in\Lambda\\ \boldsymbol{a}\neq\boldsymbol{0}}} f(\boldsymbol{a}). \text{ Így } d_1 \sum_{\substack{\boldsymbol{a}\in\Gamma\\ \boldsymbol{a}\neq\boldsymbol{0}}} f(\boldsymbol{a}) = p\alpha^n \sum_{\substack{\boldsymbol{a}\in\Gamma\\ \boldsymbol{a}\neq\boldsymbol{0}}} f(\boldsymbol{a}) \leq$$
$$\alpha^n \frac{p^n-p}{p^n-1} \sum_{\substack{\boldsymbol{a}\in\Lambda\\ \boldsymbol{a}\neq\boldsymbol{0}}} f(\boldsymbol{a}) < \frac{p^n-p}{p^n-1} \left(\varepsilon + \int f(\boldsymbol{x})\, d\boldsymbol{x}\right) < \varepsilon + \int f(\boldsymbol{x})\, d\boldsymbol{x}.$$

És szintén a 4.4-es lemma szerint $d(\Gamma) = pd(\Lambda) = d_1$. □

4.5.1. Következmény. Ha H egy $V(H) < d_1$ térfogatú halmaz, akkor létezik olyan H-elfogadható Γ rács, amire $d(\Gamma) = d_1$.

Bizonyítás. Legyen a 4.5-ös lemmabeli f a H karakterisztikus függvénye. Ekkor a H halmazban az origótól különböző rácspontok száma $\sum_{\substack{\boldsymbol{a}\in\Gamma\\ \boldsymbol{a}\neq\boldsymbol{0}}} f(\boldsymbol{a})$, ami nemnegatív egész szám. ε-t válaszuk olyan kicsinek, hogy $V(H)+\varepsilon < d_1$ teljesüljön. Ekkor a 4.5-es lemma szerint

$$\sum_{\substack{\boldsymbol{a}\in\Gamma\\ \boldsymbol{a}\neq\boldsymbol{0}}} f(\boldsymbol{a}) < \frac{1}{d_1}\left(\varepsilon + \int f(\boldsymbol{x})\,d\boldsymbol{x}\right) = \frac{1}{d_1}(V(H)+\varepsilon) < 1.$$

Így csakis $\sum_{\substack{\boldsymbol{a}\in\Gamma\\ \boldsymbol{a}\neq\boldsymbol{0}}} f(\boldsymbol{a}) = 0$ lehet, azaz Γ H-elfogadható. □

4.6. Definíció. Az $\boldsymbol{x}$ pont a Λ rácsnak primitív pontja, ha $\boldsymbol{x} \in \Lambda$, de $\nexists k > 1$ egész szám és $\boldsymbol{y} \in \Lambda$, hogy $\boldsymbol{x} = k\boldsymbol{y}$.

4.7. Definíció. $n > 1$ egész számra a Riemann-féle ζ függvény így definiált:

$$\zeta(n) = \sum_{k=1}^{\infty} \frac{1}{k^n}.$$

4.8. Lemma. $f\colon \mathbb{R}^n \to \mathbb{R}$ legyen $n > 1$-re egy Riemann-integrálható függvény, ami egy korlátos halmazon kívül azonosan 0. Ekkor adott $\varepsilon > 0$ és $d_1 > 0$ számokhoz létezik olyan Γ rács, aminek determinánsa d_1 és

$$d_1\zeta(n)\sum_{\boldsymbol{a}\in\Gamma}{}'' f(\boldsymbol{a}) < \varepsilon + \int f(\boldsymbol{x})\,d\boldsymbol{x},$$

ahol $''$ azt jelöli, hogy csak az adott rács primitív pontjai szerint összegzünk.

Bizonyítás. Megmutatjuk, hogy a 4.5-ös lemmában kapott Γ rács jó lesz.

A Λ rácsot, α-t és a K kockát definiáljuk úgy, mint a 4.5-es lemmában. Megint tegyük fel, hogy f a K-n kívül azonosan 0. Egy tetszőleges rács primitív pontjainak összes pozitív egész számszorosai éppen az összes rácspontot adják ki, így

$$\sum_{\substack{\boldsymbol{a}\in\Lambda\\ \boldsymbol{a}\neq\boldsymbol{0}}} f(\boldsymbol{a}) = \sum_{k=1}^{\infty}\sum_{\boldsymbol{a}\in\Lambda}{}'' f(k\boldsymbol{a}).$$

A Möbius-féle inverziós formulát alkalmazva adódik, hogy

$$\sum_{\boldsymbol{a}\in\Lambda}{}'' f(\boldsymbol{a}) = \sum_{k=1}^{\infty} \mu(k) \sum_{\substack{\boldsymbol{a}\in\Lambda \\ \boldsymbol{a}\neq\boldsymbol{0}}} f(k\boldsymbol{a}).$$

Mivel $\Lambda = \{(\alpha l_1, \ldots, \alpha l_n) : l_1, \ldots, l_n \in \mathbb{Z}\}$, így

$$\alpha^n \sum_{\boldsymbol{a}\in\Lambda}{}'' f(\boldsymbol{a}) = \sum_{k=1}^{\infty} \frac{\mu(k)}{k^n} ((k\alpha^n) \sum_{\substack{\boldsymbol{l}\in\Lambda_0 \\ \boldsymbol{l}\neq\boldsymbol{0}}} f(k\alpha\boldsymbol{l})).$$

A pozitív $k\alpha$-val 0-hoz, azaz p-vel ∞-hez tartva a Riemann-integrálhatóság definíciójából kapjuk, hogy

$$\lim_{k\alpha\to 0} (k\alpha^n) \sum_{\substack{\boldsymbol{l}\in\Lambda_0 \\ \boldsymbol{l}\neq\boldsymbol{0}}} f(k\alpha\boldsymbol{l}) = \int f(\boldsymbol{x})\, d\boldsymbol{x}.$$

Felhasználva a ζ-függvényre ismert $\frac{1}{\zeta(n)} = \sum_{k=1}^{\infty} \frac{\mu(k)}{k^n}$ formulát azt kapjuk, hogy

$$\lim_{\alpha\to 0} \alpha^n \sum_{\boldsymbol{a}\in\Lambda}{}'' f(\boldsymbol{a}) = \frac{1}{\zeta(n)} \int f(\boldsymbol{x})\, d\boldsymbol{x}.$$

Ez ekvivalens a bizonyítandó állítással, mert $d(\Lambda) = \alpha^n$ és a K kockán belül egy pont pontosan akkor primitív pontja Γ-nak, ha Λ-nak is primitív pontja. □

4.8.1. Következmény (Minkowski-Hlawka tétel)**.** Ha adott $d_1 \in \mathbb{R}_{>0}$, és H egy $V(H) < 2d_1\zeta(n)$ térfogatú origóra szimmetrikus, korlátos csillagszerű test $\mathbb{R}^n$-ben, akkor létezik olyan H-elfogadható Γ rács, amire $d(\Gamma) = d_1$.

Ehelyett egy olyan állítást látunk be, ami $n = 2$ esetén a Minkowski-Hlawka tétellel ekvivalens, de $n > 2$ esetén erősebb nála:

4.8.2. Következmény. Ha adott $d_1 \in \mathbb{R}_{>0}$, és H egy Jordan-mérhető, $V(H)$ térfogatú, origóra szimmetrikus csillagszerű test $\mathbb{R}^n$-ben, amire

$$V(H) < \frac{3}{1 + 2^{1-n}} d_1\zeta(n),$$

akkor létezik olyan H-elfogadható Γ rács, amire $d(\Gamma) = d_1$.

Bizonyítás. Legyen $\varkappa$ a H halmaz karakterisztikus függvénye, és

$$f(\boldsymbol{x}) := \varkappa(\boldsymbol{x}) + 2\varkappa(2\boldsymbol{x}).$$

Vagyis $f(\boldsymbol{x}) = \begin{cases} 3 & \text{ha } x \in \frac{1}{2}H, \\ 1 & \text{ha } x \in H \setminus \frac{1}{2}H, \\ 0 & \text{ha } x \notin H. \end{cases}$

$\varepsilon > 0$ legyen olyan kicsi, hogy

$$V(H) + \varepsilon < \frac{3}{1 + 2^{1-n}} d_1 \zeta(n)$$

teljesüljön. Mivel

$$\int f(\boldsymbol{x})\, d\boldsymbol{x} = (1 + 2^{1-n}) V(H),$$

így a 4.8-es lemmát $\varepsilon(1 + 2^{1-n})$-ra és $\frac{1}{2}d_1$-re alkalmazva létezik olyan Λ rács, aminek determinánsa $\frac{1}{2}d_1$, és

$$\begin{aligned} \frac{1}{2} d_1 \zeta(n) \sum_{\boldsymbol{a} \in \Lambda}{}'' f(\boldsymbol{a}) &< \varepsilon(1 + 2^{1-n}) + \int f(\boldsymbol{x})\, d\boldsymbol{x} = \\ &= \varepsilon(1 + 2^{1-n}) + (1 + 2^{1-n}) V(H) < 3 d_1 \zeta(n), \end{aligned}$$

így $\sum_{\boldsymbol{a} \in \Lambda}{}'' f(\boldsymbol{a}) < 6$.

Mivel H szimmetrikus az origóra, így $f(\boldsymbol{x}) = f(-\boldsymbol{x})$, amiből az következik, hogy nincs olyan $\boldsymbol{a} \in \Lambda$ primitív pont, amire $f(\boldsymbol{a}) = 3$, vagyis $\frac{1}{2}H$-ban nincs az origón kívül más Λ-beli pont.

E mellett a $\sum_{\boldsymbol{a} \in \Lambda}{}'' f(\boldsymbol{a}) < 6$ egyenlőtlenségből az is következik, hogy legfeljebb két $\pm\boldsymbol{a}_1, \pm\boldsymbol{a}_2 \in \Lambda$ primitív pontpár lehet H-ban.

A 4.4.1-es következmény szerint létezik olyan Γ rács, aminek az indexe Λ-ban 2, azaz $d(\Gamma) = 2d(\Lambda) = d_1$, és nem tartalmazza $\boldsymbol{a}_1$-et valamint $\boldsymbol{a}_2$-et sem. Mivel Γ indexe Λ-ban 2, így $2\boldsymbol{a}_1, 2\boldsymbol{a}_2 \in \Gamma$, de $\boldsymbol{a}_1, \boldsymbol{a}_2 \notin \frac{1}{2}H$ miatt $2\boldsymbol{a}_1, 2\boldsymbol{a}_2 \notin H$. Vagyis Γ H-elfogadható. □

Wolfgang Schmidt egy ehhez hasonló, de jóval több számolást igénylő bizonyítással adott felső becslést Jordan mérhető, korlátos halmazok rácskonstansára.

4.9. Lemma (Schmidt lemmája)**.** Ha adott $d_1 \in \mathbb{R}_{>0}$, és H egy Jordan-mérhető, $V(H)$ térfogatú, korlátos halmaz $\mathbb{R}^n$-ben, amire

$$V(H) < \frac{2d_1}{(1+2^{1-n})(1+3^{1-n})}$$

telsjesül, akkor létezik olyan H-elfogadható Γ rács, melyre $d(\Gamma) = d_1$.

4.2. Tételek konvex testekre

Most pedig az elfogadható rácsok és a konvex testek egy érdekes kapcsolatára mutatunk rá.

4.10. Tétel (Swinnerton-Dyer)**.** *Legyen $H \subset \mathbb{R}^n$ egy origóra szimmetrikus, korlátos, konvex nyílt halmaz, és Λ a H kritikus rácsa. Ekkor H határán minimum $\frac{1}{2}n(n+1)$ darab Λ-beli $(+\boldsymbol{p}, -\boldsymbol{p})$ pontpár van.*

Bizonyítás. Legyen Λ bázisa $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$, és $\pm\boldsymbol{x}_1, \ldots, \pm\boldsymbol{x}_k$ legyenek Λ-nak pontosan azok a pontpárjai, amik H határán vannak. Egyszerű geometriai állítás, hogy egy korlátos konvex halmaznak minden pontjában létezik érintő hipersíkja. Az $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ pontokban rendre vegyük fel H-nak egy-egy érintő hipersíkját, $\Sigma_1, \ldots, \Sigma_k$-at. Definiáljunk egy Λ' rácsot a Λ egy kis $|\delta|$-sugarú környezetében, amelynek bázisa $\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_n$ úgy, hogy $i = 1, \ldots, n$-re $\boldsymbol{v}'_i = \boldsymbol{v}_i + \delta \sum_{j=1}^{n} a_{ij}\boldsymbol{v}_j$ legyen, ahol minden $i, j = 1, \ldots, n$-re $|a_{ij}| \leq 1$ és $i \neq j$ esetén $a_{ij} = a_{ji}$ teljesüljön. Ez a H halmaz origóra való szimmetriája miatt megtehető. E mellett kössük ki, hogy $l = 1, \ldots, k$-ra a Λ' rács $\boldsymbol{x}'_l$ pontja Σ_l-ben legyen. Ezt összevetve azzal, hogy minden $i = 1, \ldots, k$-ra $\boldsymbol{x}_i \in \Sigma_i$ adódik az a_{ij}-ek lineáris kombinációjára, hogy

$$\sum_{j=1}^{n}\sum_{i=1}^{n} \gamma_{ij}^{l} a_{ij} = 0$$

minden $l = 1, \ldots, k$-ra. (γ_{ij}^{l} csak $\boldsymbol{x}_l$-től és Σ_l-től függ). Mivel $\boldsymbol{x}_i$-ek a H nyílt halmaz érintő hipersikjaiban vannak, így nincsenek H-ban,ezért kellően kicsi $|\delta|$-ra Λ'-nek az origón kívül nincs más pontja H belsejében. Tehát Λ' H-elfogadható. Legyen

$$A = \begin{pmatrix} 1+a_{11}\delta & a_{12}\delta & \ldots & a_{1n}\delta \\ a_{21}\delta & 1+a_{22}\delta & \ldots & a_{2n}\delta \\ \ldots & & & \\ a_{n1}\delta & a_{n2}\delta & \ldots & 1+a_{nn}\delta \end{pmatrix}$$

Ekkor $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = A(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$, így felhasználva a determinánsok szorzástételét és azt, hogy Λ kritikus rácsa H-nak:

$$d(\Lambda') = |\det(A)||\det(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)| \geq |\det(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)| = d(\Lambda) = \Delta(H).$$

Így $1 \leq \det(A) = 1 + B_1\delta + B_2\delta^2 + \cdots + B_n\delta^n$. Ez minden kellően kicsi $|\delta|$-ra igaz, ezért $B_1 = 0$ és $B_2 \geq 0$, vagyis

$$2B_2 - B_1^2 \geq 0.$$

Indirekt módon tegyük fel, hogy $k < \frac{1}{2}n(n+1)$. Mivel az n^2 darab a_{ij} között $\frac{1}{2}n(n-1)$ pár rendre megegyezik, így $\frac{1}{2}n(n+1)$ darab változóra adott kevesebb, mint $\frac{1}{2}n(n+1)$ egyenlet, tehát létezik olyan megoldás, ahol az n^2 darab a_{ij} változó közül nem mindegyik 0. Ekkor azonban

$$2B_2 - B_1^2 = 2\left(\sum_{j>i} a_{ii}a_{jj} - \sum_{j>i} a_{ji}a_{ij}\right) - \left(\sum_i a_{ii}\right)^2 = -\sum_{\substack{1\leq j\leq n\\ 1\leq i\leq n}} a_{ij}^2 < 0,$$

ami ellentmondás. □

4.11. Definíció. A H halmazt szigorúan konvexnek nevezzük, ha minden $0 < t < 1$-re és H bármely két különböző $\boldsymbol{x}$ és $\boldsymbol{y}$ határpontjára $t\boldsymbol{x} + (1-t)\boldsymbol{y}$ a H-nak belső pontja.

4.12. Tétel. *Legyen H egy az origóra szimmetrikus, szigorúan konvex nyílt halmaz, és Λ egy H-elfogadható rács. Ekkor legfeljebb $2^n - 1$ Λ-beli $(+\boldsymbol{p}, -\boldsymbol{p})$ pontpár eshet H határára.*

Bizonyítás. $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ legyen a Λ egy bázisa, és tegyük fel, hogy $\boldsymbol{p} = a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n$ a H egy határpontja. Ekkor $a_1, \ldots, a_n$ mindegyike nem lehet páros, mert ilyenkor H szigorú konvexitása miatt az $\frac{1}{2}\boldsymbol{p}$ rácspont a H-nak egy az origótól különböző belső pontja lenne. Ez nem lehetséges, mivel Λ H-elfogadható.
Tegyük fel, hogy $\boldsymbol{p}' = a_1'\boldsymbol{v}_1 + \cdots + a_n'\boldsymbol{v}_n$ is a H egy határpontja úgy, hogy minden $i = 1, \ldots, n$-re a_i és a_i' azonos paritásúak. Ekkor $\frac{1}{2}(\boldsymbol{p}+\boldsymbol{p}')$ szintén rácspont, és H szigorú konvexitása miatt a H-nak belső pontja. Mivel Λ H-elfogadható, így ez a pont csakis az origó lehet, vagyis $\boldsymbol{p} = -\boldsymbol{p}'$. Ebből következik, hogy a határpontpárok maximális száma megegyezik az n-es számsorozatokra képzett (mod 2) maradékosztályok számával a $(0, \ldots, 0)$ maradékosztályt leszámítva. □

5. Rácspolitópok

A rácspolitópok a rácsok geometriájának szintén egy különösen bő fejezte. Mi ezen belül most a rácspolitópok rácspontjainak számára vonatkozó érdekességekre fókuszálunk. Ebben a fejezetben kizárólag a Λ_0 ráccsal fogunk foglalkozni.
Először Pick tételét fogjuk ismertetni, amelynek bizonyításához két lemmára lesz szükségünk.

5.1. Definíció. Egy síkbeli konvex rácssokszöget nevezzünk egyszerűnek, ha csúcsai egész koordinátájú pontok, de rajtuk kívül nem tartalmaz további rácspontokat.

5.2. Lemma. Minden síkbeli egyszerű $H = conv\{\boldsymbol{v}_0, \boldsymbol{v}_1, \boldsymbol{v}_2\}$ rácsháromszög területe $\frac{1}{2}$.

Bizonyítás. Jelölje $\mathcal{A}$ a $\boldsymbol{v}_1$ és $\boldsymbol{v}_2$ pontokat összekötő szakasz felezőpontjára való középpontos tükrözést. A $\boldsymbol{v}_0$,$\boldsymbol{v}_1$,$\boldsymbol{v}_2$,$\boldsymbol{v}_1+\boldsymbol{v}_2-\boldsymbol{v}_0$ csúcsú P paralelogramma és a $\Lambda_0 = \mathbb{Z}^2$ rács is szimmetrikus $\mathcal{A}$-ra, így a $P = H \cup \mathcal{A}(H)$ paralelogramma is egyszerű, és egész koordinátájú eltoltjaival kiparkettázható a sík. Vagyis $\boldsymbol{v}_1 - \boldsymbol{v}_0$,$\boldsymbol{v}_2 - \boldsymbol{v}_0$ a $\mathbb{Z}^2$ rács bázisa, aminek determinánsa 1, így P területe 1, azaz H területe $\frac{1}{2}$. □

5.3. Definíció. Egy síkbeli P rácssokszög felbontását olyan rácsháromszögekre, amelyek csúcsai P belső és határra eső rácspontjai közül valók a P háromszögelésének nevezzük.

5.4. Lemma. Minden síkbeli rácssokszögnek létezik háromszögelése.

Bizonyítás. A rácssokszög csúcsinak a száma legyen n. A lemmát n-szerinti indukcióval bizonyítjuk. $n = 3$-ra triviálisan teljesül. $n \geq 4$ esetén tegyük fel, hogy az indukciós feltevés $n-1$-re teljesül. Ahhoz, hogy a lemma egy tetszőleges n-csúcsú rácssokszögre is teljesüljön elég találni egy olyan átlót, amely két olyan kevesebb csúcsú rácssokszögre vágja az eredetit, amik összeilleszthetők úgy a megfelelő oldalak mentén, hogy visszakapjuk az eredetit.
Nevezzünk egy $\boldsymbol{p}$ csúcsot konvexnek, ha a rácssokszög $\boldsymbol{p}$-nél lévő belső szöge 180°-nál kisebb. A rácssokszög belső szögeinek az összege $(n-2)180°$, így a skatulyaelv szerint létezik legalább 3 konvex csúcsa. Legyen egy ilyen csúcs $\boldsymbol{p}$, és $\boldsymbol{p}$ két szomszédos csúcsa legyen $\boldsymbol{q}$ és $\boldsymbol{r}$. Amennyiben a $\boldsymbol{qr}$ szakasz teljes egészében a rácssokszögben fekszik,

akkor ő jó lesz átlónak. Ha nem, akkor a $\boldsymbol{pqr}$ háromszög további csúcsokat is tartalmaz, így a $\boldsymbol{qr}$ szakasz egyenesét toljuk el $\boldsymbol{p}$ felé addig, ameddig rá nem esik az utolsó $\boldsymbol{pqr}$-ben lévő $\boldsymbol{s}$ csúcs. Ekkor $\boldsymbol{sp}$ teljes egészében a rácssokszögben van, és ő megfelelő átló lesz. □

5.5. Tétel (Pick). *Bármely P síkbeli rácssokszög területére teljesül*

$$t(P) = n_b + \frac{1}{2}n_h - 1$$

egyenlőség, ahol n_h és n_b rendre a sokszög határán, illetve belsejében lévő rácspontok számát jelölik.

Bizonyítás. Az előkészítő lemmáink szerint létezik P-nek háromszögelése $\frac{1}{2}$ területű rácsháromszögekre. Ezt a háromszögfelbontást értelmezzük egy síkbeli gráfként, ami a síkot $k-1$ darab $\frac{1}{2}$ területű rácsháromszögre és egy nem korlátos tartományra bontja. Tehát $t(P) = (k-1)\frac{1}{2}$. P csúcsainak és éleinek a számát jelölje rendre n és e, a gráfnak P oldalaival megegyező éleinek a számát e_h, a többi élének a számát pedig e_b. Minden kis rácsháromszögnek 3 oldala van, és minden e_h-hoz számolt él egy, míg minden e_b-hez számolt él két kis háromszögenek oldaléle, így $3(k-1) = e_h + 2e_b$, vagyis $k = 2(e-k) - e_h + 3$. Nyilván $n_h = e_h$. A síkgráfokra jól ismert Euler-formulát felhasználva adódik, hogy

$$k = 2(e-k) - e_h + 3 = 2(n-2) - n_h + 3 = n_h + 2n_b - 1,$$

azaz

$$t(P) = n_b + \frac{1}{2}n_h - 1.$$ □

I.G. MacDonald és J.E. Reeve egy nagyon szép kiterjesztését mutatták meg Pick tételének magasabb dimenziós euklideszi terekre. Tételük bizonyításához fel fogjuk használni Ehrhart polinomialitási és reciprocitási tételét. Ezeknek a bizonyítása [3]-ban megtalálható, azonban rendkívül hosszadalmasak, így én most csupán kimondom és nem bizonyítom őket.
Mostantól az egyszerűség kedvéért egy $P \subset \mathbb{R}^n$ politópban lévő $\Lambda_0 = \mathbb{Z}^n$-beli rácspontok számát $l(P) := \#(P \cap \Lambda_0)$-vel jelöljük, és legyen továbbá $l^b(P) := (-1)^{n-dim(P)}\#(relint(P) \cap \Lambda_0)$.

5.6. Tétel (Ehrhart). *Legyen P egy tetszőleges $\mathbb{R}^n$-beli konvex politóp, amelynek a relatív belseje nem üres. Ekkor:*

- $l(kP) = p_P(k)\ \forall k \in \mathbb{N}$, *ahol* p_P *egy olyan* n*-edfokú polinom, amelynek főegyütthatója* $V(P)$ *és konstans tagja* 1.
- $l^b(kP) = (-1)^n p_P(-k)\ \forall k \in \mathbb{N}$.

Megjegyzés. Érdekesség, hogy M. Henk, A. Schürmann és J.M. Wills egy meglepő összefüggést találtak az Ehrhart-polinomok gyökei, és a rácspolitópok szukcesszív minimumai között. Megmutatták, hogy amennyiben P egy $\mathbb{R}^n$-beli konvex rácspolitóp, amelynek a relatív belseje nem üres, és $i = 1, \ldots, n$-re szukcesszív minimumai a $\mathbb{Z}^n$ rácsra vonatkozóan $\lambda_i(P, \mathbb{Z}^n) = \lambda_i$-ek, a p_P Ehrhart-polinomnak a gyökei pedig α_i-ek, akkor

$$-(\alpha_1 + \cdots + \alpha_n) \leq \tfrac{1}{2}(\lambda_1 + \cdots + \lambda_n).$$

És egyenlőség csakis a $P = \{\boldsymbol{x} \in \mathbb{R}^n : -1 \leq x_i \leq 1\}$ kockára áll fenn.

Most azonban térjünk rá MacDonald és Reeve tételére.

5.7. Tétel (MacDonald és Reeve)**.** *Legyen* $P \subset \mathbb{R}^n$ *egy konvex* $\mathbb{Z}^n$*-beli rácspolitóp, amelynek relatív belseje nem üres. Ekkor:*

- $n!V(P) = \displaystyle\sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} l(jP).$
- $\frac{(n-1)n!}{2} V(P) = \frac{1}{2} + \frac{(-1)^n}{2} + \displaystyle\sum_{i=0}^{n-2} (-1)^j \binom{n-1}{j} L((n-1-j)P)$, *ahol* $L(P) = \frac{1}{2}\left(l(P) + l^b(P)\right)$.

Bizonyítás. Ehrhart tételének első része szerint létezik olyan n-edfokú $V(P)$ főegyütthatójú és 1 konstans tagú p_P polinom, hogy $\forall k \in \mathbb{N}$-re $l(kP) = p_P(k)$. Mivel $i = 0, \ldots, n$-re $p_P(i) = l(iP) \neq 0$, így alkalmazhatjuk Lagrange parciális törtekre vonatkozó tételét, amely szerint megfelelő c_j együtthatókkal

$$\frac{p_P(x)}{\displaystyle\prod_{i=0}^{n}(x-i)} = \sum_{j=0}^{n} \frac{c_j}{x-j},$$

vagyis

$$p_P(x) = \left(\prod_{i=0}^{n}(x-i)\right) \sum_{j=0}^{n} \frac{c_j}{x-j} = \left(\sum_{j=0}^{n} c_j\right) \prod_{\substack{i=0 \\ i \neq j}}^{n} (x-i) \qquad (1)$$

$j = 0, 1, \ldots, n$-re végezzük el az $x = j$ helyettesítést. Így

$$l(jP) = p_P(j) = c_j \prod_{\substack{i=0 \\ i \neq j}}^{n} (j - i) =$$

$c_j(j-0)(j-1)\ldots(j-(j-1))(j-(j+1))\ldots(j-n)$, azaz

$$c_j = \frac{(-1)^{n-j} l(jP)}{j!(n-j)!} \tag{2}$$

Mivel az (1) egyenlőség bal illetve jobb szélén álló kifejezésben az x^n együtthatója rendre $V(P)$ és $\sum_{j=0}^{n} c_j$, így ezeknek meg kell egyezniük. A (2) egyenlőség alapján $n! \sum_{j=0}^{n} c_j = \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} l(jP)$, így épp az első bizonyítandó egyenlőség adódik.
A tétel második részének bizonyításához fontos észrevétel, hogy Ehrhart tételéből $k \in \mathbb{N}$-re

$$L(kP) = \frac{1}{2}\left(l(kP) + l^b(kP)\right) = \frac{1}{2}\left(p_P(k) + (-1)^n p_P(-k)\right)) = q_P(k)$$

következik, ahol q_P egy n-edfokú, $V(P)$ főegyütthatójú polinom, amelyben az $n-1$-edfokú tag együtthatója 0, a konstans tag pedig $\frac{1}{2} + \frac{(-1)^n}{2}$. Mivel $i = 0, \ldots, n$-re $q_P(i) \neq 0$, így megint alkalmazhatjuk Lagrange tételét, de most olyan formában, amelyben kihasználjuk, hogy q_P főegyütthatója $V(P)$. Tehát megfelelő d_j együtthatókkal

$$\frac{q_P(x)}{\prod_{i=0}^{n-1}(x-i)} = V(P) + \sum_{j=0}^{n-1} \frac{d_j}{x-j},$$

vagyis

$$q_P(x) = V(P)\left(\prod_{i=0}^{n-1}(x-i)\right) + \left(\prod_{\substack{i=0 \\ i \neq j}}^{n-1}(x-i)\right) \sum_{j=0}^{n-1} d_j. \tag{3}$$

Megint végezzük el $j = 0, 1 \ldots, n$-re az $x = j$ helyettesítést. Így

$$L(jP) = q_P(j) = d_j \prod_{\substack{i=0 \\ i \neq j}}^{n-1} (j-i), \text{ azaz}$$

$$d_j = \frac{(-1)^{n-j-1} L(jP)}{j!(n-j-1)!}. \tag{4}$$

Itt $L(0P)$ jelöli $\frac{1}{2} + \frac{(-1)^n}{2}$-et. Mivel a (3) egyenlőség két oldalán álló kifejezésben x^{n-1} együtthatójának meg kell egyeznie, és $q_p(x)$-ben ez az együttható 0, így (4) alapján

$$0 = (n-1)!V(P) \left(\sum_{j=0}^{n-1} (-j) \right) + \left(\sum_{j=0}^{n-1} (-1)^{n-j-1} \binom{n-1}{j} L(jP) \right).$$

Ebből az egyenlőségből azonnal következik a tétel második része kihasználva, hogy $\sum_{j=0}^{n-1} (-j) = -\frac{n(n-1)}{2}$. □

Hivatkozások

[1] J. W. S. Cassels: An introduction to the geometry of numbers. Springer, Berlin, 1959.

[2] C. G. Lekkerkerker: Geometry of numbers. Wolters-Noordhoff, Groningen, and North-Holland, Amsterdam, 1969.

[3] Peter M. Gruber: Convex and Discrete Geometry. Springer-Verlag Berlin Heidelberg, 2007.

[4] Martin Henk: Successive minima and lattice points. Wien, 2002.

[5] M. Henk, U. Betke, J. M. Wills: Successive-Minima-Type Inequalities. Springer-Verlag New York, Siegen, 1993.

[6] Martin Aigner, Günter M. Ziegler: Proof from THE BOOK. Springer-Verlag Berlin Heidelberg, 1998.

[7] Jesse Ira Deutsch: Geometry of Numbers Proof of Götzky's Four-Squares Theorem. University of Botswana, 2002.

[8] H.P.F. Swinnerton-Dyer: Extremal lattices of convex bodies. Cambridge, 1952.

[9] Gyarmati Edit: Számelmélet. Budapest, 1993.