Eötvös Loránd Tudományegyetem
Természettudományi Kar

Kockarácsok

szakdolgozat

Témavezető:
Moussong Gábor
egyetemi adjunktus
ELTE Geometriai Tanszék

Írta:
Horváth Márton
matematikus szak

Budapest, 2009

Bevezetés

Ezen szakdolgozat a háromdimenziós $\mathbb{Z}^3$ rácsban található kockarácsokról szól. Azaz $\mathbb{Z}^3$ azon részrácsairól, melyek generálhatóak három egyenlő hosszú és páronként egymásra merőleges vektorral. Ezt a fogalmat már sokan vizsgálták, néhány elemi tulajdonság megtalálható a [3] és az [5] könyvekben, például, hogy egy kockarács élhossza egész. Sárközy András leszámlálta az adott élhosszúságú kockarácsokat a [6] cikkében.

Felmerülhet a kérdés, hogy bármely egész hosszúságú vektorhoz van-e olyan kockarács, melynek az a vektor az egyik élvektora. Ez a kérdés az [1] cikkben merült fel, és a pitagoraszi számnégyesek leírásának egyszerű következményeként igen a válasz. Feltehető ekkor az a kérdés is, hogy bármely vektorhoz van-e olyan kockarács, melyben benne van (nem feltétlenül élvektorként). Az [1] cikk erre is választ ad, megfogalmazza a következő tételt:

Tétel. *Tetszőleges* $\mathbf{v}$ *vektorhoz, melynek hossznégyzete* d^2m *alakban írható, létezik olyan* d *élhosszúságú kockarács, melyben* $\mathbf{v}$ *benne van. Ha a* $\mathbf{v}$ *vektor primitív, akkor ez a kockarács egyértelmű.*

Az [1] cikk ezt a tételt a Hurwitz-kvaterniók számelméletét használva bizonyítja be. Célunk erre a tételre egy olyan bizonyítást adni, mely csak a háromdimenziós vektor- és rácsgeometriát használja.

Az első fejezetben összefoglaljuk a szükséges rácsgeometriai ismereteket, melyek közül csak a speciálisabbakat bizonyítjuk. A második fejezetben bebizonyítjuk a fent említett főtételt. A bizonyításból az is kiderül, hogy pontosan mely vektorok tartoznak a kockarácsba. Ezen jellemzéssel, és a tétel segítségével tudjuk bizonyítani a harmadik fejezet tételeit. Először megmutatjuk, hogy minden kockarács a bizonyítás során alkotott kockarács

alkalmas nagyításával keletkezik. Ezután egy általánosabb problémával foglalkozunk, nevezetesen, hogy mely vektoroknak van úgynevezett ikre, azaz rá merőleges, vele azonos hosszúságú vektor. Erre nem ismert pontos válasz, bizonyos eredmények szerepelnek az [1] cikkben, ezeket fogjuk a főtétel segítségével elemien bizonyítani. Végül a kockarácsokat, mint részben rendezett halmazt vizsgáljuk, ahol a tartalmazás adja a rendezést. Látni fogjuk, hogy bármely két elemnek van közös alsó és felső korlátja, de ezek között nincsen mindig legnagyobb, illetve legkisebb (azaz nem alkotnak hálót).

Hasonló kérdések feltehetők kettő dimenzióban is. Ott minden vektornak van ikre, nevezetesen a 90°-os elforgatottja. Ezzel együtt egy olyan négyzetrácsot generál, melynek ő az élvektora. A négyzetrácsokat jellemzi az, hogy invariánsak a 90°-os elforgatásra, és ebből könnyen látható, hogy a négyzetrácsok hálót alkotnak. A háromdimenziós eset eme kanonikus forgatás hiánya miatt sokkal nehezebb.

Hálásan köszönöm témavezetőmnek, Moussong Gábornak az érdekes témát, és a sok hasznos észrevételt, amit munkám kapcsán tett.

1. fejezet

Rácsgeometriai ismeretek

Ebben a fejezetben kimondunk néhány ismert rácsgeometria definíciót és állítást. A rács definíciójával kezdjük.

1.1. definíció. *Egy n-dimenziós valós vektortérben egy $\mathbb{Z}^n$-nel izomorf additív diszkrét részcsoportot (n-dimenziós) rácsnak nevezzünk.*

Nyilván n független vektor egy n-dimenziós valós vektortérben egy rácsot generál. Ez az észrevétel vezet a következő definícióhoz.

1.2. definíció. *Egy n-dimenziós rácsban n független vektort, melyek generálják a rácsot, a rács bázisának nevezzük.*

Bevezetjük a részrács fogalmát, mely nem egyszerűen egy részcsoport.

1.3. definíció. *Egy n-dimenziós rácsnak egy K részcsoportját részrácsnak nevezzük, ha K is egy n-dimenziós rács.*

Könnyen következik a definíciókból az alábbi állítás.

1.4. állítás. *Egy L részcsoport pontosan akkor részrács egy K rácsban, ha az L indexe véges K-ban.*

A következő három állítás alapvető rácsgeometriai állítás, ezért nem fogjuk bizonyítani, a bizonyítás megtalálható a [4] könyvben.

Ha egy n-dimenziós rácsban kiválasztunk k független vektort, akkor azok a vektortérben egy k-dimenziós lineáris alteret feszítenek ki, és ebben k független vektorként egy k-dimenziós rácsot generálnak. Ez nem feltétlenül

egyezik meg az eredeti rácsnak a lineáris altérrel vett metszetével (a k független vektor nem feltétlenül generálja ezt), ha megegyezik, arról az esetről szól a következő állítás.

1.5. állítás. *Ha egy n-dimenziós valós vektortérben adott rácsban kiválasztunk k független vektort, melyek az általuk kifeszített k dimenziós lineáris altér ráccsal vett metszetében bázist alkotnak, akkor ehhez a k vektorhoz választható még $n-k$ vektor, hogy azok együtt az n-dimenziós rács bázisa.*

Ha egy rácsban rögzítünk egy bázist, akkor ahhoz definiálhatjuk az alapparalelepipedon fogalmát.

1.6. definíció. *Egy n-dimenziós rácsban a bázisvektorok által kifeszített paralelepipedont a rács alapparalelepipedonjának nevezzük.*

Bár az alapparalelepipedon függ a bázis választásától, ha rögzítünk egy térfogati formát a vektortéren, akkor a térfogata független a választástól a következő állítás szerint.

1.7. állítás. *Egy rácsban mindegyik alapparalelepipedonnak ugyanakkora a térfogata.*

Így az alapparalelepipedon térfogata a rácsra jellemző szám, és a részrácsok indexét is megadja a következő állítás szerint.

1.8. állítás. *Tetszőleges $K \subseteq L$ részrács esetén a K indexe az L-ben egyenlő az alapparalelepipedonok térfogatának arányával.*

A következő definíciók a rácsok vektoraival kapcsolatosak.

1.9. definíció. *Egy $\mathbf{v} \in L$ vektor osztható egy d pozitív egésszel, ha van olyan $\mathbf{u} \in L$ vektor, melyre $\mathbf{v} = d\mathbf{u}$.*

1.10. definíció. *Egy $\mathbf{v} \in L$ vektor primitív, ha nem osztható semmilyen 1-től különböző pozitív egésszel.*

1.11. állítás. *Minden $\mathbf{v} \in L$ vektor egyértelműen áll elő $\mathbf{v} = d\mathbf{u}$ alakban, ahol $\mathbf{u}$ primitív, és d pozitív egész.*

Bizonyítás. Legyen K a $\mathbf{v}$ irányú vektorok által generált részcsoport az L rácsban. Ez egy egydimenziós rács, így van benne egy generáló $\mathbf{u}$ vektor, mely nyilván primitív lesz az L-ben. Így $\mathbf{v} = d\mathbf{u}$, ahol d egész. Ha d negatív lenne, akkor az $\mathbf{u}$ helyett az ellentettjét választva pozitív d-t kapunk. □

Ezen állítás alapján értelmezni tudjuk egy $\mathbf{v} \in L$ vektor legnagyobb osztóját, mint az 1.11. állításban szereplő d pozitív egész számot.

1.12. definíció. *Egy $K \subseteq L$ részrács primitív, ha a K-ban szereplő vektorok legnagyobb közös osztója 1.*

A fenti definíciókból egyszerűen következik, hogy egy egydimenziós L rácsban a $\mathbf{v}$ vektor pontosan akkor primitív, ha a $\mathbf{v}$ által generált részrács primitív L-ben. Nyilvánvaló, hogy ha valamely $K \subseteq L$ részrácsban van olyan vektor, amely L-ben primitív, akkor K primitív részrács. A 3.1. szakaszban be fogjuk látni ennek a megfordítását: bármely primitív részrács tartalmaz primitív vektort.

A dolgozatban sok helyen használni fogjuk a következő definíciót.

1.13. definíció. *Egy L rács d arányú nagyításán, vagy egyszerűen a d-szeresén azt a részrácsát értjük, mely a benne levő d-vel osztható vektorokból áll (vagyis minden vektorát megszorozzuk d-vel). Jelölése: dL.*

1.14. állítás. *Egy n-dimenziós L rácsban a dL részrácsnak az indexe d^n.*

Bizonyítás. Az L rács bázisvektorainak a d-szeresei a dL részrácsnak egy bázisát alkotják. Emiatt az alapparalelepipedonok térfogatának aránya d^n, ami az 1.8. állítás szerint éppen a részrács indexe. □

Ha egy n-dimenziós rácsban rögzítünk egy bázist, akkor a rács vektorait felírhatjuk ezen vektorok egész együtthatós lineáris kombinációjaként, így a rácsot azonosíthatjuk $\mathbb{Z}^n$-nel, a befoglaló vektorteret pedig $\mathbb{R}^n$-nel. Ekkor egy vektor pontosan akkor osztható d-vel, ha az összes koordinátája osztható, és ponotsan akkor primitív, ha a koordinátái relatív prímek.

Innentől kezdve az $n = 3$ esetet tekintjük. A rácsban a $\mathbb{Z}^3$-bel való azonosítás meghatároz egy skaláris szorzást, továbbiakban ezt a skaláris szorzást tekintjük a rácsban. (Ha eredetileg egy háromdimenziós euklideszi

térből indultunk ki, ahol a rács bázisa ortonormált volt, akkor visszakapjuk az eredeti skaláris szorzást.) Ezzel értelmezni tudjuk egy $\mathbf{v} \in \mathbb{Z}^3$ vektor hossznégyzetét, mint önmagával vett skaláris szorzatot. Ennek négyzetgyöke a vektor hossza, melynek jelölése: $\|\mathbf{v}\|$. A skaláris szorzat a vektoriális szorzatot is meghatározza, ami nem fog kivezetni a rácsból. A szükséges vektorgeometriai ismeretek megtalálhatóak a [2] könyvben.

A következő állításokban $\mathbf{v} \in \mathbb{Z}^3$ egy tetszőleges primitív vektor, és legyen $L = \{\, \mathbf{x} \in \mathbb{Z}^3 \mid \mathbf{x} \perp \mathbf{v} \,\}$, a rá merőleges síknak a ráccsal vett metszete.

1.15. állítás. *L egy kétdimenziós rács.*

Bizonyítás. Nyilván L-beli vektorok összege is L-beli, így egy diszkrét additív részcsoportot alkotnak (diszkrét csoport részcsoportja). Így az általuk kifeszített lineáris altérben L egy rács. Ez a lineáris altér legfeljebb kétdimenziós, mivel a $\mathbf{v}^\perp$ sík része. A továbbiakban azt szeretnénk megmutatni, hogy pontosan kétdimenziós, amihez elegendő találni két független vektort benne. Ehhez válasszunk ki egy olyan koordinátasíkot, melyben nem fekszik $\mathbf{v}$ (ilyen nyilván lesz, mert a metszetük a nullvektor). Jelöljük ezt a koordinátasíkot kifeszítő egységvektorokat $\mathbf{i}$-vel és $\mathbf{j}$-vel. Az $\mathbf{i} \times \mathbf{v}$ és a $\mathbf{j} \times \mathbf{v}$ vektorok L-ben vannak, elegendő tehát azt megmutatni, hogy függetlenek. Ha nem lennének függetlenek, akkor a vektoriális szorzat linearitásából azt kapnánk, hogy az $\mathbf{i}$ és $\mathbf{j}$ egy lineáris kombinációjának nulla a vektoriális szorzata $\mathbf{v}$-vel. Ekkor ez a lineáris kombináció párhuzamos lenne $\mathbf{v}$-vel, ami ellentmondana annak, hogy az $\mathbf{i}$ és $\mathbf{j}$ által feszített koordinátasíkban nincsen benne $\mathbf{v}$. □

1.16. állítás. *L-ben az alapparalelogramma területe egyenlő a $\mathbf{v}$ hosszával.*

Bizonyítás. Nevezzük egy rácshoz asszociált vektornak az alapparalelogrammát kifeszítő vektorok vektoriális szorzatát. Ez a vektor merőleges a rácsra, és hossza az alapparalelogramma területe, így ± 1 szorzótól eltekintve független a választásunktól. Mivel $\mathbf{v}$ primitív, így az L-hez asszociált vektor a $\mathbf{v}$ többszöröse lesz.

A következő vektorok merőlegesek a $\mathbf{v} = (a, b, c)$ vektorra, így L-beliek.

$$\mathbf{x} = (0, c, -b)$$
$$\mathbf{y} = (-c, 0, a)$$
$$\mathbf{z} = (b, -a, 0)$$

Ezek páronként egy-egy részrácsot generálnak L-ben, ahol ezek a vektorok alapparalellogrammákat feszítenek ki. Így a hozzájuk asszociált vektorok:
$\mathbf{y}$ és $\mathbf{z}$ vektorok részrácsa: $\mathbf{y} \times \mathbf{z} = (-c, 0, a) \times (b, -a, 0) = (a^2, ab, ac) = a\mathbf{v}$
$\mathbf{z}$ és $\mathbf{x}$ vektorok részrácsa: $\mathbf{z} \times \mathbf{x} = (b, -a, 0) \times (0, c, -b) = (ab, b^2, bc) = b\mathbf{v}$
$\mathbf{x}$ és $\mathbf{y}$ vektorok részrácsa: $\mathbf{x} \times \mathbf{y} = (0, c, -b) \times (-c, 0, a) = (ac, bc, c^2) = c\mathbf{v}$
Mivel ezek az L-nek részrácsai, a hozzájuk asszociált vektorok az L-hez asszociált vektornak a többszörösei. Mivel $\text{lnko}(a, b, c) = 1$, így az L-hez asszociált vektor csak $\pm\mathbf{v}$ lehet (mivel $\mathbf{v}$ primitív), amiből következik az állítás. □

1.17. állítás. *Vezessük be a következő ekvivalenciarelációt a $\mathbb{Z}^3$-ben: $\mathbf{x} \sim \mathbf{y}$ pontosan akkor, ha a különbségük $\mathbf{v}$-nek többszöröse, azaz van olyan k egész, hogy $\mathbf{x} - \mathbf{y} = k\mathbf{v}$. A $\mathbf{v}$-vel való vektoriális szorzás bijekciót létesít ezen ekvivalenciaosztályok és L elemei között.*

Merőlegesen vetítsük le a rácsot a $\mathbf{v}$-re merőleges lineáris altérre (a $\mathbf{v}$-vel párhuzamosan). Ekkor egy ekvivalenciaosztály egy pont őse lesz a vetítésnél. Az állítás szerint ezen vetített képet 90°-kal elforgatva és ℓ-lel nyújtva megkapjuk az L rácsot (ahol ℓ a $\mathbf{v}$ hossza).

Bizonyítás. Két vektornak pontosan akkor lesz ugyanaz a vektoriális szorzata $\mathbf{v}$-vel, ha a különbségük párhuzamos $\mathbf{v}$-vel, azaz ugyanabban az ekvivalenciaosztályban vannak, így a leképezés injektív. A szürjektivitás bizonyításához tegyük fel, hogy adott egy $\mathbf{u} \in L$ vektor. Keressük azt az $\mathbf{x} \in \mathbb{Z}^3$ vektort, melyre $\mathbf{x} \times \mathbf{v} = \mathbf{u}$. Az 1.15. állításhoz hasonlóan bizonyítható, hogy a $\mathbb{Z}^3$-nek az $\mathbf{u}^\perp$ síkkal vett metszete egy kétdimenziós rács (ehhez nem kell $\mathbf{u}$-nak primitívnek lennie). Ebben a rácsban a $\mathbf{v}$ egy primitív vektor, melyet az 1.5. állítás szerint ki lehet egészíteni bázissá. A kiegészítése lesz a keresett $\mathbf{x}$ vektor megfelelő előjellel véve, ugyanis a rácshoz asszociált vektor a normálvektor lesz: $\mathbf{x} \times \mathbf{v} = \mathbf{u}$. □

2. fejezet

A főtétel

Ebben a fejezetben a $\mathbb{Z}^3$-ben keresünk kockarácsokat, először egy adott élvektorhoz. Ezután már csak azt követeljük meg, hogy az adott vektor benne legyen a kockarácsban. Erről szól a főtétel, melyet be is bizonyítunk.

2.1. A tétel kimondása

Először definiáljuk a kockarács fogalmát, mely ennek a dolgozatnak a főtémája.

2.1. definíció. *Az $\mathbb{R}^3$ euklideszi térbeli $\mathbb{Z}^3$ standard rácsban egy részrácsot kockarácsnak nevezzünk, ha vannak hozzá olyan generáló vektorok, melyek páronként merőlegesek és egyenlő hosszúak. Ezen vektorok alkotják a kockarács kockabázisát, a közös hosszuk pedig a kockarács élhossza.*

A kockarácsban levő vektorok hosszát mérhetjük a kockarácshoz képest is, a kockabázis vektorait egységnek tekintve. Ezt a relatív hosszt a kockarács élhosszával megszorozva kapjuk a vektor eredeti hosszát.

A következő elemi geometriai észrevétel megtalálható a [3] és az [5] könyvekben:

2.2. állítás. *Egy kockarácsnak az élhossza szükségképpen egész.*

Bizonyítás. Legyen a kockarács élhossza d, mely egy rácsvektor hossza, így d^2 egész. A kockarács kockabázisa által kifeszített kocka térfogata (d^3) éppen a kifeszítő vektorok vegyes szorzata, azaz koordinátáinak a determinánsa,

ami nyilván egész. Így $d = d^3/d^2$ racionális, és mivel a négyzete egész, szükségképpen d is egész. □

Nyilvánvalóan minden d pozitív egészhez van d élhosszúságú kockarács, például a $d\mathbb{Z}^3$, a d-vel osztható vektorok részrácsa. Az előbbi állítás szerint nem minden vektort tudunk kiegészíteni kockaráccsá, szükséges, hogy a hossza egész legyen. Felvetődik a kérdés, hogy ez elégséges feltétel-e, azaz van-e bármely egész hosszúságú vektorhoz olyan kockarács, aminek ő az élvektora. Ezt a kérdést az [1] cikkben vizsgálták, ahol leírták, hogy az igenlő válasz a pitagoraszi számnégyesek eredetileg Eulertól származó paraméterezéséből könnyen kiolvasható.

Ennél többet is kérdezhetünk: egy adott vektor milyen kockarácsban lehet benne (nem feltétlenül élvektorként). Ez volt a motiváló kérdés az [1] cikkben. Egy d élhosszúságú kockarácsban a vektor relatív hossznégyzete d^2-ed része lesz az eredetinek, tehát szükséges feltétel, hogy a hossznégyzete osztható legyen d^2-tel. A következő tétel szerint ez elegendő feltétel. Ez a dolgozat főtétele.

2.3. tétel. *Ha adott egy $\mathbf{v} \in \mathbb{Z}^3$ vektor, melynek hossznégyzete $\|\mathbf{v}\|^2 = \ell^2 = d^2m$ alakban írható, akkor létezik olyan részkockarács $\mathbb{Z}^3$-ben, melyben $\mathbf{v}$ benne van, és melynek az élhosszúsága d. Ha a $\mathbf{v}$ primitív, akkor rögzített d mellett ez a kockarács egyértelmű.*

Az $\ell^2 = d^2m$ felbontás általában nem egyértelmű, tetszőleges felbontást vehetünk. Ennek a tételnek a bizonyítása megtalálható az [1] cikkben négyzetmentes m esetére Hurwitz-kvaterniók számelméletének segítségével. A következőkben erre a tételre adunk egy olyan bizonyítást, mely csak a háromdimenziós vektor- és rácsgeometriát használja.

Ha a $\mathbf{v}$ nem primitív, akkor nem állíthatunk egyértelműséget, legyen ugyanis $\mathbf{v} = (5, 0, 0)$ vektor, melyre $\|\mathbf{v}\|^2 = 5^2 \cdot 1$. Ekkor ez a vektor benne van az $(5, 0, 0), (0, 5, 0), (0, 0, 5)$ illetve az $(5, 0, 0), (0, 3, 4), (0, 4, -3)$ vektorok által generált kockarácsokban is.

Megmutatjuk, hogy a tételt elég bizonyítani primitív vektor esetén. Ha $\mathbf{v}$ nem primitív, akkor az 1.11. állítás szerint létezik olyan f pozitív egész, és $\mathbf{u}$ primitív vektor, hogy $\mathbf{v} = f\mathbf{u}$. A $\|\mathbf{v}\|^2 = d^2m$ felbontásban a d-t és az

m-et tovább bonthatjuk ennek megfelelően. Legyen $d = d_1 d_2$ és $m = m_1^2 m_2$, melyre teljesül, hogy $d_1 m_1 = f$ és $\|\mathbf{u}\|^2 = d_2^2 m_2$. A tételt $\mathbf{u}$-ra (és az előbbi felbontására) alkalmazva kapunk egy d_2 élhosszúságú kockarácsot, amit d_1 arányban nagyítva $d = d_1 d_2$ élhosszúságú kockarácsot kapunk. Ebben benne van a $d_1\mathbf{u}$ vektor, aminek az m_1-szerese az $m_1 d_1 \mathbf{u} = f\mathbf{u} = \mathbf{v}$ vektor, ami így a konstruált d élhosszúságú kockarácsban benne lesz.

Először az egyértelműséget bizonyítjuk. Meghatározzuk, hogy mely vektorok tartozhatnak a keresett részrácsba, így meghatározunk egy részrácsot. Végül bebizonyítjuk, hogy ez valóban kockarács.

2.2. Az egyértelműség bizonyítása

Tegyük fel, hogy már találtunk egy ilyen K kockarácsot. A következő lemma segítségével megállapíthatjuk, hogy mely vektorok tartozhatnak a K-ba.

2.4. lemma. *Két $\mathbf{a}, \mathbf{b} \in K$ vektor vektoriális szorzata osztható d-vel, és a szorzat d-edrésze is K-ban van.*

Bizonyítás. Végezzük el a vektoriális szorzást K-ban. Ha a K-ban számolunk (mivel ott az egység d), akkor a kifeszített paralelogramma területe d^2-edrésze lesz a $\mathbb{Z}^3$-ben számolt értéknek. Emiatt a vektoriális szorzat hossza is d^2-ed akkora lesz, melynek hossza a $\mathbb{Z}^3$-ben d-szeres, azaz a $\mathbb{Z}^3$-ben számolt érték d-edrésze. □

Először csak a $\mathbf{v}$ vektorra merőleges $L = \{\, \mathbf{x} \in \mathbb{Z}^3 \mid \mathbf{x} \perp \mathbf{v} \,\}$ kétdimenziós rácsot tekintsük. A 2.4. lemma szerint L-ből csak azok az $\mathbf{a}$ vektorok tartozhatnak K-ba, melyeket $\mathbf{v}$-vel vektoriálisan szorozva d-vel osztható vektort kapunk. Legyen ezen vektorok halmaza M, azaz

$$M = \{\, \mathbf{a} \in L \mid \mathbf{a} \times \mathbf{v} \text{ osztható } d\text{-vel} \,\}.$$

A $\mathbf{v}$-vel való vektoriális szorzás L-ben egy $-90°$-os forgatás ($\mathbf{v}$ körül) és egy ℓ-lel való nyújtás kompozíciója. Emiatt egy $\mathbf{u} \in L$ vektor pontosan akkor lesz M-ben, ha $-90°$-kal elforgatva és $\ell/d = \sqrt{m}$-mel nyújtva L-beli vektort kapunk. Az így kapott vektor szintén M-ben lesz, mert ezt $-90°$-kal forgatva és $\sqrt{m}$-mel nyújtva, a $-m\mathbf{u}$ vektort kapjuk, ami nyilván L-beli.

Könnyen meggondolható, hogy M részcsoport, azaz összeadásra, és egésszel való szorzásra zárt. A következő állítás az 1.4. állítás szerint mutatja, hogy részrács is.

2.5. állítás. *Az M indexe L-ben d.*

Bizonyítás. A bizonyítás két részből áll, először bebizonyítjuk, hogy M indexe L-ben osztható d-vel, majd fordítva. Legyen $\mathbf{v} = (a, b, c)$.

Mivel $\mathbf{v}$ primitív, $\text{lnko}(a, b, c) = 1$, így léteznek olyan x, y, z egész számok, melyekre $ax + by + cz = 1$. Legyen $\mathbf{t} = (x, y, z)$, és ekkor $\mathbf{tv} = 1$. Legyen $\mathbf{u} = \mathbf{t} \times \mathbf{v}$, ami mivel $\mathbf{v}$-re merőleges vektor, L-ben van. A kifejtési tételt felhasználva

$$\begin{aligned}\mathbf{u} \times \mathbf{v} &= (\mathbf{t} \times \mathbf{v}) \times \mathbf{v} \\ &= (\mathbf{tv})\mathbf{v} - (\mathbf{vv})\mathbf{t} \\ &= \mathbf{v} - \ell^2\mathbf{t} \\ &= (a - \ell^2 x, b - \ell^2 y, c - \ell^2).\end{aligned}$$

Ez a vektor nem osztható d egyetlen p valódi osztójával sem. Ha ugyanis osztható lenne, akkor mivel p osztja $\ell^2 = d^2 m$-et, osztaná a, b, c-t is, ami nem lehet, mert $\mathbf{v}$ primitív vektor. Emiatt a $k\mathbf{u}\times\mathbf{v}$ vektorok $1 \leq k \leq d-1$-re nem lehetnek oszthatóak d-vel. Így az $\mathbf{u}, 2\mathbf{u}, \ldots, (d-1)\mathbf{u}$ vektorok nem lehetnek M-ben, mert az pontosan azt jelentené, hogy valamely k-ra a $k\mathbf{u} \times \mathbf{v}$ vektor osztható lenne d-vel. A $d\mathbf{u}$ vektor nyilván M-ben van, mert $d\mathbf{u} \times \mathbf{v}$ osztható d-vel. Legyen az $\mathbf{u}$ által generált részcsoport L-ben U. Az U-nak csak egy d indexű részcsoportja van M-ben, így M indexe L-ben d-nek többszöröse.

A másik irányt az [1] cikkben szereplő 7.4. tétel bizonyításához hasonlóan bizonyítom:

Tekintsük a következő vektorokat

$$\begin{aligned}\mathbf{r} &= (0, cd, -bd) \\ \mathbf{s} &= (\mathbf{r} \times \mathbf{v})/d = (b^2 + c^2, -ab, -ac).\end{aligned}$$

Látható, hogy ezen vektorok az M-ben vannak. Az általuk kifeszített alapparalelogramma (téglalap) területe $d\ell(b^2 + c^2)$. Jelöljük az általuk generált részrácsot M_1-gyel (ami tehát M részrácsa). Hasonlóan definiálhatjuk M_2-t és M_3-at is, melyeknél az alapparalelogramma területe $d\ell(a^2 + c^2)$, illetve

$d\ell(a^2+b^2)$. Az L-ben az alapparalelogramma területe ℓ, így az M_1, M_2, M_3 indexe L-ben rendre $d(b^2+c^2)$, $d(a^2+c^2)$ és $d(a^2+b^2)$. Emiatt az M indexe L-ben osztja az

$$\text{lnko}(d(b^2+c^2), d(a^2+c^2), d(a^2+b^2)) = d \cdot \text{lnko}(b^2+c^2, a^2+c^2, a^2+b^2)$$

számot. Számoljuk ki ezt a legnagyobb közös osztót.

$$\begin{aligned}\text{lnko}(b^2+c^2, a^2+c^2, a^2+b^2) = \\ = \text{lnko}(b^2+c^2, a^2+c^2, a^2+b^2, b^2-c^2, a^2-c^2, a^2-b^2) = \\ = \text{lnko}(2a^2, 2b^2, 2c^2, b^2+c^2, a^2+c^2, a^2+b^2)\end{aligned}$$

Tudjuk, hogy $\text{lnko}(a,b,c) = 1$, így ha az a, b, c számok nem mindegyike páratlan (és így van páratlan négyzetösszeg), akkor

$$\text{lnko}(b^2+c^2, a^2+c^2, a^2+b^2) = 1,$$

míg ha mindegyike páratlan, akkor

$$\text{lnko}(b^2+c^2, a^2+c^2, a^2+b^2) = 2.$$

Ha tehát az a, b, c nem mindegyike páratlan, akkor bebizonyítottuk, hogy M indexe L-ben osztja d-t. Ha az a, b, c számok mindegyike páratlan, akkor csak azt tudjuk, hogy az index osztja a $2d$-t. Ebben az esetben $\ell^2 = a^2+b^2+c^2$ páratlan, és így d is páratlan. Tekintsük a dL részrácsot L-ben, melynek indexe az 1.14. állítás szerint d^2. A dL rács részrácsa az M-nek, ugyanis egy $\mathbf{u} \in dL$ vektort (mely egy $\mathbf{x} \in L$ vektor d-szerese), $\mathbf{v}$-vel vektoriálisan szorozva nyilván d-vel osztható vektort kapunk, az $\mathbf{x} \times \mathbf{v}$ vektor d-szeresét. Tehát M indexe L-ben osztja d^2-et is (ami páratlan), és így mivel tudjuk, hogy osztja a $2d$-t, így osztja a d-t is. □

A K kockarácsba a 2.4. lemma szerint csak olyan $\mathbf{x}$ vektor tartozhat, melynek a $\mathbf{v}$-vel vett vektoriális szorzata osztható d-vel, és annak a d-edrésze is a K-ban van. Mivel a vektoriális szorzat merőleges $\mathbf{v}$-re, azaz L-ben lesz, és tudjuk, hogy ott csak az M részrács vektorai tartozhatnak a K-ba, szükséges, hogy az $(\mathbf{x} \times \mathbf{v})/d$ vektor az M-ben legyen. Ennek alapján a K kockarács a

$$K' = \{\, \mathbf{x} \in \mathbb{Z}^3 \mid (\mathbf{x} \times \mathbf{v})/d \in M \,\}$$

halmaznak része. Nyilvánvalóan $\mathbf{v} \in K'$. A vektoriális szorzat linearitásából következik, hogy K' részcsoport, és a következő állítás mutatja, hogy részrács is.

2.6. állítás. *A K' indexe $\mathbb{Z}^3$-ben d^3.*

Bizonyítás. Tekintsük a dM részrácsot, az M rács d-szeresét. Ez egy d^3 indexű részrács L-ben (mivel a dM részrács d^2 indexű M-ben, ami d indexű L-ben). A K'-be azon vektorok tartoznak a $\mathbb{Z}^3$-ből, melyeknek a $\mathbf{v}$-vel vett vektoriális szorzata dM-be esik (ez jelenti azt, hogy a d-edrésze M-ben van). Mivel az 1.17. állítás szerint a $\mathbf{v}$-vel vett vektoriális szorzás bijekció az ekvivalenciaosztályok és L között, és a dM egy d^3 indexű részcsoport L-ben, így a K' is egy d^3 indexű részcsoport. □

Tudjuk, hogy $K \subseteq K'$, és mindkettő d^3 indexű a $\mathbb{Z}^3$-ben, tehát egyenlőek. Azaz ha létezik a tételben szereplő kockarács, akkor az csak az imént megkonstruált K' lehet. Ezzel az egyértelműség bizonyítását befejeztük.

A későbbi hivatkozások végett írjuk fel a K' részrács definícióját.

2.7. definíció. *Egy adott d pozitív egészhez, és egy $\mathbf{v}$ primitív vektorhoz, melynek hossznégyzete osztható d^2-tel definiáljuk a $K(\mathbf{v}, d)$ részrácsot. Ez azon vektorokból áll, melyeket $\mathbf{v}$-vel vektoriálisan szorozva d-vel osztható vektort kapunk, továbbá a szorzat d-edrésze (az előzőekben definiált) M-ben van, azaz $\mathbf{v}$-vel újból vektoriálisan szorozva d-vel osztható vektort kapunk. Azaz formulával:*

$$K(\mathbf{v}, d) = \{\, \mathbf{x} \in \mathbb{Z}^3 \mid \mathbf{x} \times \mathbf{v} \text{ osztható } d\text{-vel és } (\mathbf{x} \times \mathbf{v}) \times \mathbf{v} \text{ osztható } d^2\text{-tel} \,\}.$$

A következő szakaszban látni fogjuk, hogy ez minden esetben egy d élhosszúságú kockarács.

2.3. A létezés bizonyítása

Ebben a szakaszban bebizonyítjuk, hogy a $K' = K(\mathbf{v}, d)$ részrács valóban kockarács. Ehhez először bizonyítunk néhány állítást.

2.8. állítás. *Tetszőleges $\mathbf{a} \in K'$ vektorra az $\mathbf{av}$ skaláris szorzat osztható d^2-tel.*

Bizonyítás. Írjuk fel a kifejtési tételt a következő szorzatra

$$(\mathbf{a} \times \mathbf{v}) \times \mathbf{v} = (\mathbf{av})\mathbf{v} - (\mathbf{vv})\mathbf{a}.$$

Mivel az $\mathbf{a}$ vektor a K'-ben van, így a fenti vektor osztható d^2-tel. A d^2-ed része a következő vektor (amiről így tudjuk, hogy a $\mathbb{Z}^3$-ben van):

$$\frac{(\mathbf{a} \times \mathbf{v}) \times \mathbf{v}}{d^2} = \frac{\mathbf{av}}{d^2}\mathbf{v} - \frac{\mathbf{vv}}{d^2}\mathbf{a}.$$

Tudjuk, hogy $\mathbf{vv}$ osztható d^2-tel, azaz $\frac{\mathbf{vv}}{d^2}\mathbf{a} \in \mathbb{Z}^3$, és így $\frac{\mathbf{av}}{d^2}\mathbf{v} \in \mathbb{Z}^3$ is fennáll. Mivel $\mathbf{v}$ primitív, az együtthatója egész, azaz $\mathbf{av}$ osztható d^2-tel. □

2.9. állítás. *Tetszőleges* $\mathbf{a}, \mathbf{b} \in K'$ *vektorokra* $\frac{\mathbf{a}\times\mathbf{b}}{d} \in K'$.

Bizonyítás. A kifejtési tétel szerint

$$(\mathbf{a} \times \mathbf{b}) \times \mathbf{v} = (\mathbf{av})\mathbf{b} - (\mathbf{bv})\mathbf{a}.$$

Definíció szerint $\frac{\mathbf{a}\times\mathbf{b}}{d}$ akkor van K'-ben, ha a $\mathbf{v}$-vel vett vektoriális szorzatának d-edrésze az M-ben van, ami az előző sor alapján

$$\frac{\frac{\mathbf{a}\times\mathbf{b}}{d} \times \mathbf{v}}{d} = \frac{\mathbf{av}}{d^2}\mathbf{b} - \frac{\mathbf{bv}}{d^2}\mathbf{a}.$$

Ez a vektor pontosan akkor van M-ben, ha a $\mathbf{v}$-vel vett vektoriális szorzatának d-ed része L-ben van, ami a jobb oldalból számolva

$$\frac{\mathbf{av}}{d^2} \cdot \frac{\mathbf{b} \times \mathbf{v}}{d} - \frac{\mathbf{bv}}{d^2} \cdot \frac{\mathbf{a} \times \mathbf{v}}{d}.$$

A 2.8. állítás szerint $\frac{\mathbf{av}}{d^2}$ és $\frac{\mathbf{bv}}{d^2}$ egész. Továbbá mivel $\mathbf{a}, \mathbf{b} \in K'$, a $\frac{\mathbf{b}\times\mathbf{v}}{d}$ és a $\frac{\mathbf{a}\times\mathbf{v}}{d}$ vektorok L-beliek, így a fenti kifejezés is L-beli, és így $\frac{\mathbf{a}\times\mathbf{b}}{d} \in K'$. □

2.10. állítás. *Tetszőleges* $\mathbf{a}, \mathbf{b} \in K'$ *vektorokra az* $\mathbf{ab}$ *skaláris szorzat osztható* d^2*-tel.*

Bizonyítás. A kifejtési tétel szerint

$$(\mathbf{a} \times \mathbf{v}) \times \mathbf{b} = (\mathbf{ab})\mathbf{v} - (\mathbf{vb})\mathbf{a}.$$

Mivel $\mathbf{a} \in K'$, $\mathbf{a} \times \mathbf{v}$ osztható d-vel, és a d-edrésze is K'-ben van. A 2.9. állítást alkalmazva erre és a $\mathbf{b}$ vektorra, azt kapjuk, hogy a $(\mathbf{a}\times\mathbf{v})\times\mathbf{b}$ vektor osztható d^2-tel. A jobb oldalon a 2.8. állítás szerint $\mathbf{vb}$ osztható d^2-tel, azaz $\frac{\mathbf{vb}}{d^2}\mathbf{a} \in \mathbb{Z}^3$, és így $\frac{\mathbf{ab}}{d^2}\mathbf{v} \in \mathbb{Z}^3$, amiből következik, hogy $\mathbf{ab}$ osztható d^2-tel (mivel $\mathbf{v}$ primitív). □

A következőkben ezekből a tulajdonságokból megmutatjuk, hogy a K' rács valóban egy d élhosszúságú kockarács.

A 2.6. állítás szerint a K' egy d^3 indexű részrács $\mathbb{Z}^3$-ben, ami azt jelenti, hogy az alapparalelepipedon térfogata d^3. Ennek segítségével bizonyítjuk a következő állítást.

2.11. állítás. *Van olyan* $\mathbf{a} \in K'$ *vektor, melynek a hossza* d*.*

Bizonyítás. Tegyük fel indirekten, hogy nincsen ilyen vektor. A 2.10. állítás szerint a vektorok hosszának négyzete osztható d^2-tel, és így egy nem nulla vektornak legalább $2d^2$ a hossznégyzete, azaz legalább $\sqrt{2}d$ hosszú. Ekkor a K' elemei köré rajzolt $\sqrt{2}d/2$ sugarú gömbök diszjunktak lesznek. Tekintsük ezen gömböket egy alapparalelepipedonon belül. Ezek összesen pontosan egy egész gömböt adnak ki, melynek térfogata:

$$\frac{4\pi}{3}\left(\frac{\sqrt{2}d}{2}\right)^3 > \frac{4\cdot 3}{3}\cdot\frac{2\sqrt{2}}{8}d^3 = \sqrt{2}d^3 > d^3.$$

Nagyobb a paralelepipedon térfogatánál, ami nem lehet, mert ez ellentmond annak, hogy diszjunktak a gömbök. Tehát van d hosszú vektor K'-ben. □

A továbbiakhoz rögzítsünk egy ilyen $\mathbf{a}$ vektort. Bármely $\mathbf{b} \in K'$ vektornak az $\mathbf{a}$-val vett skaláris szorzata a 2.10. állítás szerint osztható d^2-tel, így az $\mathbf{a}$ vektor egyenesére való vetületének a hossza d-nek többszöröse. Emiatt a K' rács elemei csak az $\mathbf{a}$-ra merőleges síkban, és ennek az $\mathbf{a}$ vektorral való eltoltjaiban lehetnek. Tekintsük a K' metszetét az $\mathbf{a}$-ra merőleges síkkal:

$$G = \{\, \mathbf{b} \in K' \mid \mathbf{b} \perp \mathbf{a} \,\}.$$

Az 1.15. állítás szerint ez egy kétdimenziós rács. Ebben a rácsban az alapparalelogramma területe d^2, mivel az $\mathbf{a}$ vektorral kiegészítve kapott alapparalelepipedon térfogata d^3. A 2.11. állításhoz hasonlót bizonyíthatunk G-ben:

2.12. állítás. *Van olyan* $\mathbf{b} \in G$ *vektor, melynek a hossza* d*.*

Bizonyítás. Tegyük fel indirekten, hogy nincsen ilyen vektor. A 2.10. állítás szerint a vektorok hosszának négyzete osztható d^2-tel, és így egy nem

nulla vektornak legalább $2d^2$ a hossznégyzete, azaz legalább $\sqrt{2}d$ hosszú. Ekkor az $\mathbf{a}$-ra merőleges síkban G elemei köré rajzolt $\sqrt{2}d/2$ sugarú körök diszjunktak lesznek. Tekintsük ezen köröket egy alapparalelogrammán belül. Ezek összesen pontosan egy egész kört adnak ki, melynek területe

$$\left(\frac{\sqrt{2}d}{2}\right)^2 \pi = \frac{\pi}{2}d^2 > d^2.$$

Nagyobb a paralelogramma területénél, ami nem lehet, mert ez ellentmond annak, hogy diszjunktak a körök. Tehát van d hosszú vektor G-ben. □

Rögzítsünk egy ilyen $\mathbf{b}$ vektort.

2.13. állítás. *A* $\mathbf{c} = \frac{\mathbf{a}\times\mathbf{b}}{d}$ *vektor* K'*-ben van, merőleges az* $\mathbf{a}$ *és* $\mathbf{b}$ *vektorokra, és a hossza* d*.*

Bizonyítás. A 2.9. állításból következik, hogy a $\mathbf{c}$ vektor K'-beli. A merőlegesség a vektoriális szorzat tulajdonsága. Mivel $\mathbf{a}$ és $\mathbf{b}$ hossza d, és merőlegesek, a vektoriális szorzatuk hossza d^2, aminek a d-edrésze a $\mathbf{c}$, ami így d hosszú. □

Az $\mathbf{a}, \mathbf{b}, \mathbf{c} \in K'$ vektorok tehát páronként merőlegesek, és hosszuk d, így a kifeszített paralelepipedonjuk térfogata d^3. Ez éppen annyi, amennyi a K' indexe $\mathbb{Z}^3$-ben, így ezek generálják a K' részrácsot. Azaz K' valóban egy d élhosszúságú kockarács, amit bizonyítani akartunk.

3. fejezet

Alkalmazások

Miután kimondtuk és bebizonyítottuk a főtételt, néhány alkalmazását mutatjuk be. Megnézzük, hogy a $\mathbb{Z}^3$ egy tetszőleges kockarácsa hogyan keletkezik. Ezután egy egyszerűbbnek látszó kérdéssel foglalkozunk, nevezetesen, hogy mikor van egy vektornak ikre, azaz rá merőleges, vele azonos hosszúságú vektor. Ki fog derülni, hogy ez jóval nehezebb probléma, és nincs is teljesen megválaszolva. Végül a kockarácsok egymáshoz való viszonyát is tanulmányozzuk.

3.1. A kockarácsok jellemzése

Az előző fejezetben leírt konstrukcióval kapott kockarács nagyítással keletkezik egy olyan kockarácsból, melyben van primitív vektor. Ezért kézenfekvő egy tetszőleges kockarácsban olyan vektort keresni, melynek legnagyobb osztója a kockarácsban fekvő vektorok legnagyobb közös osztója. Látni fogjuk, hogy ilyen vektor tetszőleges részrácsban van. Ezt először csak kétdimenziós rácsra bizonyítjuk be, ebből fog következni az állítás három dimenzió esetén.

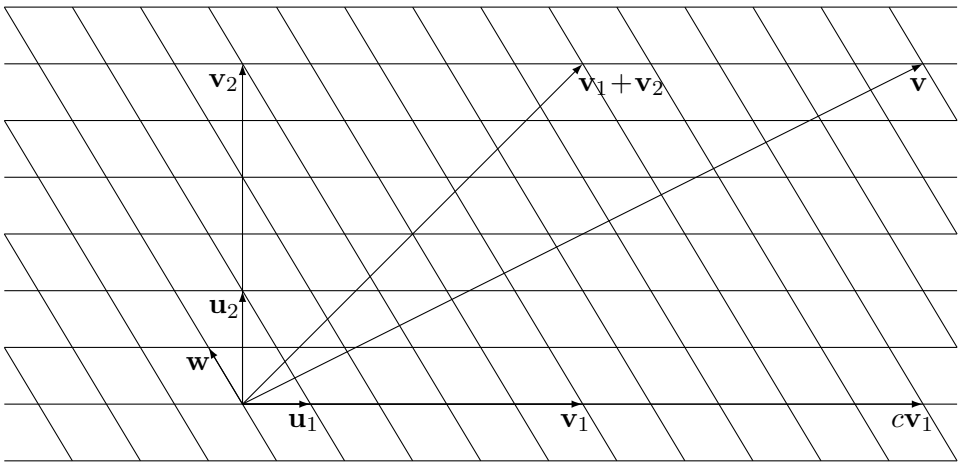
3.1. állítás. *Tekintsük egy L kétdimenziós rács K részrácsát, melyben szereplő vektorok legnagyobb közös osztója d. Ekkor van olyan vektor a K-ban, melynek a legnagyobb osztója d.*

Bizonyítás. Feltehető, hogy $d = 1$, ugyanis vehetjük L helyett a d-szeresét. Legyen a két K-t generáló vektor $\mathbf{v}_1 = d_1\mathbf{u}_1$ és $\mathbf{v}_2 = d_2\mathbf{u}_2$, ahol az $\mathbf{u}_1$ és

$\mathbf{u}_2$ vektorok primitívek, és a d_1 és d_2 számok pozitív egészek. Mivel a K-ban szereplő vektorok legnagyobb közös osztója 1, és a $\mathbf{v}_1$ és $\mathbf{v}_2$ vektorok generálják K-t, a d_1 és d_2 számok relatív prímek. Először tekintsük a $\mathbf{v}_1+\mathbf{v}_2$ vektort. Ez a vektor nem lehet osztható d_1 és d_2 semmilyen p prímosztójával sem. Ha ugyanis $\mathbf{v}_1+\mathbf{v}_2$ osztható lenne a d_1 szám p prímosztójával, akkor a

$$\frac{\mathbf{v}_1+\mathbf{v}_2}{p}=\frac{d_1}{p}\mathbf{u}_1+\frac{d_2}{p}\mathbf{u}_2$$

egyenlőségből azt kapnánk, hogy $\frac{d_2}{p}\mathbf{u}_2$ is rácsvektor. Így p osztaná d_2-t is (mivel $\mathbf{v}_2$ primitív), ellentmondásban azzal, hogy a d_1 és d_2 számok relatív prímek. A $\mathbf{v}_1+\mathbf{v}_2$ vektor azonban osztható lehet egy d_1d_2-höz relatív prím számmal. Ez nem lehet akármilyen szám, ahogyan hamarosan látni fogjuk. Az $\mathbf{u}_1$ vektor primitív, így van hozzá egy $\mathbf{w}$ vektor, mellyel együtt az L-et generálja. Ekkor az $\mathbf{u}_2$ vektort felírhatjuk ezen bázis segítségével: $\mathbf{u}_2=a\mathbf{u}_1+b\mathbf{w}$. Könnyen meggondolható, hogy a $\mathbf{v}_1+\mathbf{v}_2$ vektor csak a b osztóival lehet osztható.



Legyen c azon prímek szorzata, melyek osztják b-t, de nem osztják d_1d_2-t (ha nincs ilyen prímszám, akkor legyen $c=1$). Tekintsük a $\mathbf{v}_1+\mathbf{v}_2$ vektor helyett a

$$\mathbf{v}=c\mathbf{v}_1+\mathbf{v}_2\in K$$

vektort. Erről a vektorról mutatjuk meg, hogy primitív. Tegyük fel indirekten, hogy nem, osztható egy p prímszámmal. A $\mathbf{v}$ vektort (egyértelműen)

felírhatjuk az $\mathbf{u}_1$ és $\mathbf{w}$ vektorok segítségével:

$$\begin{aligned}\mathbf{v} &= c\mathbf{v}_1 + \mathbf{v}_2 \\ &= cd_1\mathbf{u}_1 + d_2\mathbf{u}_2 \\ &= cd_1\mathbf{u}_1 + d_2(a\mathbf{u}_1 + b\mathbf{w}) \\ &= (cd_1 + ad_2)\mathbf{u}_1 + bd_2\mathbf{w}.\end{aligned}$$

Ha ez a vektor osztható a p prímszámmal, akkor a p-edrészét is egyértelműen felírhatjuk az $\mathbf{u}_1$ és $\mathbf{w}$ vektorok segítségével. Így a felírt lineáris kombinációban az együtthatók oszthatóak p-vel, azaz p osztja bd_2-t, és mivel prím, osztja b-t vagy d_2-t. Ha a p prímszám d_2-t osztja, akkor d_2/p egész, és így

$$\frac{\mathbf{v}}{p} = \frac{cd_1\mathbf{u}_1 + d_2\mathbf{u}_2}{p} = \frac{cd_1}{p}\mathbf{u}_1 + \frac{d_2}{p}\mathbf{u}_2$$

alapján $\frac{cd_1}{p}\mathbf{u}_1$ is rácsvektor, azaz $\frac{cd_1}{p}$ egész (mivel $\mathbf{u}_1$ primitív). De ez nem lehet, mert d_1 és d_2 relatív prímsége miatt p nem oszthatja d_2-t (hiszen d_1-et osztja). Továbbá c-t sem oszthatja, mert c definíció szerint olyan prímek szorzata, melyek nincsenek d_2 prímosztói között. Ha a p prímszám b-t osztja, és d_2-t nem, akkor p osztja cd_1-et c definíciója szerint. Tehát $\frac{\mathbf{v}}{p}$ előbbi felírásában $\frac{cd_1}{p}$ egész, és így $\frac{d_2}{p}\mathbf{u}_2$ is rácsvektor. Mivel $\mathbf{u}_2$ primitív, a $\frac{d_2}{p}$ együttható egész, ellentmondásban azzal, hogy p nem osztja d_2-t. Ezzel bebizonyítottuk, hogy a $\mathbf{v}$ vektor primitív. □

Ezután bebizonyítjuk a háromdimenziós esetet.

3.2. lemma. *Tekintsünk egy tetszőleges L részrácsot $\mathbb{Z}^3$-ben, és legyen a benne szereplő vektorok legnagyobb közös osztója d. Ekkor van olyan vektor az L részrácsban, melynek a legnagyobb osztója d.*

Bizonyítás. Legyen az L-et generáló három vektor $\mathbf{v}_1$, $\mathbf{v}_2$ és $\mathbf{v}_3$, és a legnagyobb osztójuk rendre d_1, d_2, illetve d_3. Ezen vektorok legnagyobb közös osztója lesz az L minden vektorának a legnagyobb közös osztója, azaz $d = \text{lnko}(d_1, d_2, d_3)$. A $\mathbb{Z}^3$-nek a $\mathbf{v}_1$ és $\mathbf{v}_2$ vektorok által kifeszített síkjába eső vektorok alkossák az M kétdimenziós rácsot, melyben a $\mathbf{v}_1$ és $\mathbf{v}_2$ által generált részrács legyen K. Erre alkalmazva a 3.1. állítást, azt kapjuk, hogy van olyan $\mathbf{v}$ vektor K-ban, melynek a legnagyobb osztója $\text{lnko}(d_1, d_2)$. A 3.1.

állítást hasonlóan alkalmazva a $\mathbf{v}$ és $\mathbf{v}_3$ vektorokra olyan $\mathbf{v}'$ vektort kapunk, melynek a legnagyobb osztója $\text{lnko}(\text{lnko}(d_1, d_2), d_3) = \text{lnko}(d_1, d_2, d_3) = d$. Tehát a $\mathbf{v}'$ egy megfelelő vektor. □

Ezt az állítást mi csak a háromdimenziós rácsra fogjuk alkalmazni, de hasonlóan meggondolható, hogy igaz tetszőleges dimenziós rácsra is. A $d = 1$ esetben az az állítás, hogy bármely primitív részrácsban van primitív vektor.

Ezen állítás segítségével bizonyíthatjuk, hogy a $\mathbb{Z}^3$ minden kockarácsa az előző fejezetben leírt konstrukció szerinti kockarácsból keletkezik egy alkalmas nagyítással.

3.3. tétel. *A $\mathbb{Z}^3$-ben minden K kockarácshoz egyértelműen vannak olyan d_1, d_2 pozitív egészek, és $\mathbf{v} \in \mathbb{Z}^3$ primitív vektor (melynek hossznégyzete osztható d_2^2-tel), hogy a 2.7. definició szerinti $K(\mathbf{v}, d_2)$ kockarácsot d_1-szeresére nagyítva éppen a K kockarácsot kapjuk.*

Bizonyítás. Mivel a $K(\mathbf{v}, d_2)$ kockarácsban $\mathbf{v}$ primitív vektor, így a d_1-szeres nagyítás után a vektorok legnagyobb közös osztója d_1 lesz. Így a d_1 a K-ban szereplő vektorok legnagyobb közös osztója. Osszuk el a kockarács minden vektorát d_1-gyel, ekkor kapjuk K'-t, ami szintén kockarács, melynek élhossza legyen a d_2. A 3.2. lemma szerint K-ban van olyan vektor, melynek legnagyobb osztója d_1, így K'-ben lesz primitív vektor. Ez a vektor legyen a $\mathbf{v}$, melynek hossznégyzete osztható d_2^2-tel, mert egy d_2 élhosszúságú kockarácsban van benne. A kockarácsok egyértelműsége miatt $K' = K(\mathbf{v}, d_2)$. Ennek a d_1-szerese a K kockarács. □

3.4. lemma. *Tetszőleges d élhosszúságú K kockarácsban benne van $\mathbb{Z}^3$ minden vektorának a d^2-szerese, azaz $d^2\mathbb{Z}^3 \subseteq K$.*

Bizonyítás. Tegyük fel, hogy a kockarács a 2.7. definició szerinti $K(\mathbf{v}, d)$ kockarács. Legyen $\mathbf{x} \in \mathbb{Z}^3$ tetszőleges vektor. Ekkor a 2.7. definició szerint $d^2\mathbf{x}$ pontosan akkor lesz benne a kockarácsban, ha $d^2\mathbf{x} \times \mathbf{v}$ osztható d-vel, és $(d^2\mathbf{x} \times \mathbf{v}) \times \mathbf{v}$ osztható d^2-tel, melyek nyilván teljesülnek.

Ha nem a 2.7. definicióval kapjuk a kockarácsot, akkor a 3.3. tétel szerint van egy olyan $\mathbf{v}$ primitív vektor és d_1, d_2 pozitív egészek, hogy $K = d_1K(\mathbf{v}, d_2)$. A K kockarácsnak az élhossza $d = d_1d_2$. Az előző eset szerint

tetszőleges vektor d_2^2-szerese benne van $K(\mathbf{v}, d_2)$-ben, és így a $d_1 d_2^2$-szerese a K-ban. Így ennek a d_1-szerese, azaz a vektor d^2-szerese is benne van a K kockarácsban. □

Vizsgáljuk meg, hogy milyen élhosszúságú kockarácsot kaphatunk a 2.7. definícióból. Ehhez egy olyan primitív vektor szükséges, melynek hossznégyzete osztható egy adott d szám négyzetével. Szorítkozzunk először csak prímszám élhosszakra.

3.5. lemma. *Ha p páratlan prímszám, akkor van olyan $\mathbf{v} \in \mathbb{Z}^3$ primitív vektor, melynek hossznégyzete osztható p^2-tel.*

Bizonyítás. A $\mathbf{v}$ vektort az alábbi alakban keressük:

$$\mathbf{v} = (x, y, z) = (x_1 p + x_2, y_1 p + y_2, z_1 p + z_2).$$

A primitívség helyett egyelőre csak azt követeljük meg, hogy ne legyen osztható p-vel, azaz az x_2, y_2, z_2 számok közül nem mind osztható p-vel. A $\mathbf{v}$ vektor hossznégyzete:

$$\begin{aligned}\|\mathbf{v}\|^2 &= x^2 + y^2 + z^2 \\ &= (x_1 p + x_2)^2 + (y_1 p + y_2)^2 + (z_1 p + z_2)^2 \\ &= (x_1^2 + y_1^2 + z_1^2)p^2 + 2(x_1 x_2 + y_1 y_2 + z_1 z_2)p + x_2^2 + y_2^2 + z_2^2\end{aligned}$$

Erről szeretnénk, hogy osztható legyen p^2-tel. Ehhez először a 2-es indexű tagokat határozzuk meg, majd azután az 1-es indexűeket. A 2-es indexű tagokat úgy kell meghatározni, hogy $x_2^2 + y_2^2 + z_2^2$ osztható legyen p-vel (és ne legyen mindegyik osztható p-vel). Ehhez $\mathbb{Z}_p$-ben keresünk megfelelő elemeket, és abban is számolunk. Ezt két különböző módon tesszük attól függően, hogy a p páratlan prímszám $4k+1$ vagy $4k+3$ alakú.

Ha a p prímszám $4k+1$ alakú, akkor a -1 kvadratikus maradék, tehát van olyan x_2, melyre $x_2^2 = -1$, és így $y_2 = 1$ és $z_2 = 0$ választás megfelelő: $x_2^2 + y_2^2 + z_2^2 = (-1) + 1 + 0 = 0$.

Ha a p prímszám $4k+3$ alakú, akkor legyen B a kvadratikus maradékok halmaza. Tudjuk, hogy $|B| = (p-1)/2$, és hogy nincsen két B-beli, melynek az összege 0 (mert a -1 nem kavadratikus maradék ebben az esetben). Így két nemnulla elem közül, melyeknek az összege 0, pontosan az egyik van

B-ben. Tekintsük az összes kéttagú összeget B elemeiből. Ha így x_3 és y_3 összegeként előáll egy nem B-beli z_3 is (ami az előbbi megállapításunk szerint nem lehet 0), akkor $-z_3$ B-ben van. Ezekhez a számokhoz B definíciója szerint vannak olyan x_2, y_2 és z_2 számok, hogy $x_2^2 = x_3$, $y_2^2 = y_3$ és $z_2^2 = -z_3$, azaz $x_2^2 + y_2^2 + z_2^2 = x_3 + y_3 - z_3 = 0$, tehát ez egy megfelelő választás. Ha a B-ből képzett kéttagú összegek mindig B-beliek lennének, akkor egy $b \in B$ elemet kiválasztva $b + b = 2b$, $2b + b = 3b$, $\ldots$, $(p-1)b + b = 0$ is B-beli lenne, amiről tudjuk, hogy nincsen B-ben.

Így meghatároztunk $x_2, y_2, z_2 \in \mathbb{Z}_p$ elemeket, ezután legyenek x_2, y_2, z_2 az ezeknek megfelelő egész számok. Legyen $x_2^2 + y_2^2 + z_2^2 = kp$. Ezután úgy határozzuk meg az x_1, y_1, z_1 számokat, hogy a $\|v\|^2$ osztható legyen p^2-tel. Ehhez az kellene, hogy $2(x_1x_2 + y_1y_2 + z_1z_2)p + x_2^2 + y_2^2 + z_2^2$ osztható legyen p^2-tel, azaz $2(x_1x_2 + y_1y_2 + z_1z_2) + k$ osztható legyen p-vel. Tudjuk, hogy az x_2, y_2, z_2 számok nem mind oszthatóak p-vel, feltehető, hogy például x_2 nem osztható. Legyen $y_1 = z_1 = 0$, és $\mathbb{Z}_p$-ben számolva $x_1 = \frac{-k}{2x_2}$, illetve egy ennek megfelelő egész szám. Így a $\|\mathbf{v}\|^2$ osztható p^2-tel, ilyen $\mathbf{v}$-t kerestünk.

Erről a $\mathbf{v}$ vektorról csak azt tudjuk, hogy nem osztható p-vel. Ahhoz, hogy primitív legyen, osszuk le a legnagyobb osztójával (ami relatív prím p-hez), ekkor a hossznégyzete osztható marad p^2-tel. □

A lemmában szükséges volt kikötni, hogy p páratlan, mert az állítás $p = 2$ esetén nem igaz a következő állítás szerint.

3.6. állítás. *Bármely 4-gyel osztható hossznégyzetű $\mathbf{v} \in \mathbb{Z}^3$ vektor osztható 2-vel.*

Bizonyítás. Tegyük fel, hogy a $\mathbf{v} = (x, y, z)$ vektor hossznégyzete: $\|\mathbf{v}\|^2 = x^2 + y^2 + z^2$ osztható 4-gyel. Ismert, hogy négyzetszámok 4-gyel osztva 0 vagy 1 maradékot adnak, ebben az esetben csak az lehet, hogy x^2, y^2, z^2 mindegyike 0-t ad maradékul. Azaz x, y, z mindegyike páros, és így a $\mathbf{v}$ vektor osztható 2-vel. □

Az imént kimondott lemmákkal bizonyíthatjuk az alábbi tételt, melyet a következő szakaszban fogunk felhasználni.

3.7. tétel. *Tetszőleges* $\mathbf{v} = (a, b, c) \in \mathbb{Z}^3$ *primitív vektorhoz, és páratlan* d *egész számhoz van olyan* $\mathbf{u} \in \mathbb{Z}^3$ *primitív vektor, melynek a hossza* d*-szerese a* $\mathbf{v}$ *hosszának, és a 2.7. definició szerinti* $K(\mathbf{u}, d)$ *kockarácsban felvehető olyan rendezett kockabázis, melyben az* $\mathbf{u}$ *koordinátái éppen* (a, b, c) *lesznek.*

Bizonyítás. Indukcióval elég bizonyítani $d = p$ prímre az állítást. Ugyanis, ha a tétel alkalmazzuk d_1-re, majd a kapott kockarácsban d_2-re, akkor az így kapott kockarács az, ami $d = d_1 d_2$-höz kell.

Először keresünk egy olyan $\mathbf{w}$ primitív vektort, melynek hossznégyzete osztható p^2-tel, és a $\mathbf{v}$-vel vett skaláris szorzata nem osztható p-vel (később látni fogjuk, hogy ez miért jó). Indirekten tegyük fel, hogy nincsen ilyen vektor. A 3.5. lemma szerint van olyan $\mathbf{w} = (x, y, z)$ primitív vektor, melynek hossznégyzete osztható p^2-tel. A feltevés szerint a $\mathbf{vw} = ax+by+cz$ skaláris szorzat osztható p-vel. Tekintsük $\mathbf{w}$ helyett a $(-x, y, z)$ vektort, ami nyilván szintén primitív, és osztható a hossznégyzete p^2-tel. A $-ax+by+cz$ skaláris szorzat szintén osztható p-vel, így osztható a két skaláris szorzat különbsége is, azaz $2ax$, és mivel p páratlan, ax is. Hasonlóan az $(x, -y, z)$, illetve az $(x, y, -z)$ vektorokkal azt kapjuk, hogy by és cz osztható p-vel. Ha az egész gondolatmenetet (x, y, z) helyett a szintén megfelelő (y, z, x) vektorral csináljuk, akkor azt kapjuk, hogy az ay, bz, cx mindegyike osztható p-vel. A (z, x, y) vektorral pedig azt kapjuk, hogy az az, bx, cy mindegyike osztható p-vel. A $\mathbf{v} = (a, b, c)$ vektor primitív, így az a, b és c számok közül legalább az egyik nem osztható p-vel, feltehető, hogy például az a nem. Levezettük, hogy az ax, ay, és az mindegyike osztható p-vel. Mivel p prím, és a nem osztható p-vel, az x, y és z számok mindegyike osztható p-vel. Ez ellentmond annak, hogy az $\mathbf{w}$ vektor primitív. Tehát indirekt feltevésünk hamis, azaz van olyan $\mathbf{w}$ primitív vektor, melynek hossznégyzete osztható p^2-tel, és a $\mathbf{v}$-vel vett skaláris szorzata nem osztható p-vel.

Legyen K az a p élhosszúságú kockarács, melyben benne van az így megkapott $\mathbf{w}$ vektor. Mivel bármely két K-beli vektor skaláris szorzata ($\mathbb{Z}^3$-ben számolva) osztható p^2-tel, így a $\mathbf{v}, 2\mathbf{v}, \ldots, (p^2-1)\mathbf{v}$ vektorok nem tartozhatnak a K-ba (mivel $\mathbf{vw}$ nem osztható p-vel). A $p^2\mathbf{v}$ vektor viszont a 3.4. lemma szerint benne van K-ban, és az előbbiek szerint K-ban primitív vektor lesz. A K részrácsnak a $p^2\mathbb{Z}^3$ a 3.4. lemma szerint kockarácsa p

relatív élhosszúsággal. Így K-ban az $\mathbf{u} = p^2\mathbf{v}$ primitív vektorra elkészítve a p élhosszúságú kockarácsot az egyértelműség miatt éppen a $p^2\mathbb{Z}^3$ rácsot kapjuk. Ebben a $\mathbb{Z}^3$ rendezett bázisának a p^2-szeresét választva rendezett kockabázisnak, az $\mathbf{u}$ vektor koordinátái éppen (a, b, c) lesznek. □

3.2. Ikervektorok

Már megismerkedtünk a $\mathbb{Z}^3$-ben fekvő kockarácsokkal, melyeket három páronként merőleges, és egyenlő hosszú rácsvektor generál. Kézenfekvő ezt két lépésben megkonstruálni, tehát egy vektorhoz először csak egy ikervektort, azaz egy rá merőleges, és egyenlő hosszú vektort keresni. Nem ismert, hogy pontosan mely vektoroknak van ikre. Az [1] cikkben szerepel néhány ikervektorokra vonatkozó eredmény, ezeket fogjuk az eddigiek segítségével elemien bizonyítani.

3.8. definíció. *Két $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^3$ vektor iker, ha azonos hosszúak, és merőlegesek.*

A következő lemma és a bizonyítása megtalálható az [1] cikkben.

3.9. lemma. *Legyenek $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^3$ ikervektorok, melyeknek közös hossznégyzete n^2m, ahol m négyzetmentes. Ekkor az $\mathbf{x} \times \mathbf{y}$ vektor osztható nm-mel.*

Bizonyítás. Legyen

$$\mathbf{x} = (x_1, x_2, x_3)$$
$$\mathbf{y} = (y_1, y_2, y_3)$$

a két vektor koordinátái, a hossznégyzetük:

$$\|\mathbf{x}\|^2 = x_1^2 + x_2^2 + x_3^2 = nm^2$$
$$\|\mathbf{y}\|^2 = y_1^2 + y_2^2 + y_3^2 = nm^2.$$

Tudjuk, hogy merőlegesek, azaz

$$x_1y_1 + x_2y_2 + x_3y_3 = 0,$$

amiből

$$x_3^2y_3^2 = x_1^2y_1^2 + x_2^2y_2^2 + 2x_1x_2y_1y_2.$$

Tekintsük az $\mathbf{x} \times \mathbf{y}$ vektor harmadik koordinátáját, $x_1y_2 - x_2y_1$-t, melynek négyzete (felhasználva az eddigi egyenleteket):

$$\begin{aligned}(x_1y_2 - x_2y_1)^2 &= x_1^2y_2^2 + x_2^2y_1^2 - 2x_1x_2y_1y_2 \\ &= x_1^2y_2^2 + x_2^2y_1^2 + x_1^2y_1^2 + x_2^2y_2^2 - x_3^2y_3^2 \\ &= (x_1^2 + x_2^2)(y_1^2 + y_2^2) - x_3^2y_3^2 \\ &= (n^2m - x_3^2)(n^2m - y_3^2) - x_3^2y_3^2 \\ &= n^2m(n^2m - x_3^2 - y_3^2).\end{aligned}$$

Mivel m négyzetmentes, $(x_1y_2 - x_2y_1)^2$ osztható n^2m^2-tel, így az $\mathbf{x} \times \mathbf{y}$ vektor harmadik koordinátája osztható nm-mel. Hasonló gondolatmenettel belátható, hogy a másik két koordináta is osztható nm-mel, és így az $\mathbf{x} \times \mathbf{y}$ vektor osztható nm-mel. □

Ebből a lemmából következik, hogy ha két ikervektor ℓ hosszúsága egész, akkor a vektoriális szorzatuk (melynek hossza ℓ^2) osztható lesz ℓ-lel, és így azt ℓ-lel leosztva, ℓ hosszú vektort kapunk. E három vektor egy ℓ élhosszúságú kockarácsot generál.

Nem ismert pontos feltétel arra, hogy egy vektornak mikor van ikre. Ha egész hosszúságú, akkor nyilván van, mert tudjuk, hogy bármely egész hosszúságú vektorhoz van olyan élvektorú kockarács is, és a kockabázis bármelyik másik eleme ikre lesz. Azonban a kockarácsokkal ellentétben, itt a hossznégyzet nem határozza meg, hogy van-e ikre egy vektornak. Például a $(2, 2, 3)$ és a $(0, 1, 4)$ vektorok hossznégyzete ugyanúgy 17, de könnyen meggondolható, hogy az elsőnek nincsen ikre, míg a másodiknak a $(0, -4, 1)$ vektor ikre lesz. Ezért az [1] cikkben bevezették az ikerteljesség fogalmát:

3.10. definíció. *Egy n pozitív egész szám ikerteljes, ha $\mathbb{Z}^3$-ben minden n hossznégyzetű vektornak van ikre, és létezik is ilyen hossznégyzetű vektor.*

Az utóbbi feltétel, hogy legyen n hosszúságú vektor, azt jelenti, hogy az n szám előálljon három négyzetszám összegeként. Ez Gauss tétele szerint azzal ekvivalens, hogy az n szám nem $4^k(8l + 7)$ alakú.

Nem ismert, hogy pontosan mely számok ikerteljesek, bár van sejtés, melyet a 3.14. állításban fogalmazunk meg. A következő tétel szerint a kérdés visszavezethető a négyzetmentes számok ikerteljességének vizsgálatára:

3.11. tétel. *Egy n pozitív egész akkor és csak akkor ikerteljes, ha a négyzetmentes része az.*

Ez a tétel és a bizonyítása megtalálható az [1] cikkben szintén Hurwitz-kvaterniók segítségével. Az alábbiakban az idáig kimondott tételek segítségével bizonyítjuk elemi úton.

Bizonyítás. Először azt bizonyítjuk, hogy ha egy négyzetmentes szám ikerteljes, akkor az összes négyzetszámszorosa is. Legyen egy $\mathbf{v} \in \mathbb{Z}^3$ vektor hossznégyzete d^2m, ahol m négyzetmentes és ikerteljes. Ennek a $\mathbf{v}$ vektornak szeretnénk egy ikret találni. A 2.3. tételt alkalmazva a $\mathbf{v}$ vektorra, és hossznégyzetének d^2m felírására, kapunk egy d élhosszúságú kockarácsot, melyben a $\mathbf{v}$ vektor benne van, és melyben a hossznégyzete m. Mivel m ikerteljes, így ebben a kockarácsban lesz ikre, ami természetesen a $\mathbb{Z}^3$-ben is ikre (ugyanúgy merőleges, és ugyanolyan hosszú).

A másik irányhoz tegyük fel, hogy a d^2m szám ikerteljes. Legyen adott egy $\mathbf{v} = (a, b, c)$ vektor, melynek a hossznégyzete m négyzetmentes, és emiatt primitív. Először tegyük fel, hogy d páratlan. Vegyük a $\mathbf{v}$ vektorhoz a 3.7. tétel szerinti K kockarácsot, és abban egy d^2m hossznégyzetű $\mathbf{u}$ primitív vektort. A tétel szerint a K-ban tekintve a 2.7. definíció szerinti $K(\mathbf{u}, d)$ kockarácsot, az éppen a $\mathbb{Z}^3$, továbbá az $\mathbf{u} \in K$ vektornak a $\mathbf{v} \in \mathbb{Z}^3$ vektor felel meg. Mivel az $\mathbf{u}$ vektor hossza d^2m a K-ban, így a feltevés szerint van ikre, legyen ez a $\mathbf{w}$ vektor. Azt kellene belátni, hogy ez a $\mathbf{w}$ vektor is benne van a $K(\mathbf{u}, d) = \mathbb{Z}^3$ kockarácsban. Ehhez definíció szerint az kell, hogy egyrészt a K-ban a $\mathbf{w} \times \mathbf{u}$ vektoriális szorzat osztható legyen d-vel, ami a 3.9. lemma szerint teljesülni fog. Másrészt a

$$(\mathbf{w} \times \mathbf{u}) \times \mathbf{u} = (\mathbf{wu})\mathbf{u} - (\mathbf{uu})\mathbf{w} = -d^2m\mathbf{w},$$

vektoriális szorzat osztható legyen d^2-tel, ami nyilván teljesül.

Ahhoz, hogy minden d-re igaz legyen az állítás, elég azt belátni, hogy ha $4n$ ikerteljes, akkor n is. Ehhez tekintsünk egy n hossznégyzetű $\mathbf{v}$ vektort. Ekkor a $2\mathbf{v}$ vektornak (melynek a hossznégyzete $4n$) a feltevés szerint van $\mathbf{w}$ ikre. A $\mathbf{w}$ vektor a 3.6. állítás szerint osztható 2-vel (mivel a hossznégyzete $4n$), és így $\mathbf{w}/2$ vektor ikre lesz $\mathbf{v}$-nek. □

Annak eldöntését, hogy egy négyzetmentes szám ikerteljes-e, a következő állítás segítségével visszavezethetjük számelméleti kérdésre:

3.12. állítás. *Egy négyzetmentes m szám pontosan akkor ikerteljes, ha előáll mint két négyzetszám összege, de nem áll elő három pozitív négyzetszám összegeként.*

Bizonyítás. Ha az m szám két négyzetszám összege, de nem áll elő három pozitív négyzetszám összegeként, akkor egy m hosszúnégyzetű vektor az egyik koordinátasíkban fekszik. Abban a síkban a 90°-os elforgatottja egy ikre, azaz m ikerteljes szám.

A fordított irányhoz legyen m egy ikerteljes, négyzetmentes szám. Tekintsünk egy tetszőleges m hosszúnégyzetű $\mathbf{v}$ vektort, melynek m ikerteljessége miatt van egy $\mathbf{u}$ ikre. Legyen $\mathbf{w} = \mathbf{v} \times \mathbf{u}$ a vektoriális szorzatuk. Mivel a két ikervektor hossza $\sqrt{m}$ és merőlegesek, így a $\mathbf{w}$ hossza m. A 3.9. lemma szerint $\mathbf{w}$ osztható m-mel. Így a $\mathbf{w}/m$ rácsvektor hossza 1, azaz az egyik egységvektor (vagy az ellentettje). Mivel $\mathbf{v}$ és $\mathbf{u}$ vektorok merőlegesek $\mathbf{w}$-re, így egy koordinátasíkban fekszenek, és így a $\mathbf{v}$ vektornak az egyik koordinátája 0. Ebből következik, hogy a hosszúnégyzete, m előáll két négyzetszám összegeként. Ha m előállna három pozitív négyzetszám összegeként, akkor az annak megfelelő vektort választva $\mathbf{v}$ vektornak, ellentmondásra jutnánk. □

Az előbbi számelméleti jellemzéshez kapcsolódik az alábbi híres, régi számelméleti sejtés:

3.13. sejtés. *Azon négyzetmentes számok halmaza, melyek előállnak két négyzetszám összegeként, de nem állnak elő három pozitív négyzetszám összegeként, a következő:*

$$\{1, 2, 5, 10, 13, 37, 58, 85, 130\}$$

Az eddigieknek következménye az alábbi állítás az ikerteljes számokról:

3.14. állítás. *Ikerteljesek a következő számok:*

$$n^2, 2n^2, 5n^2, 10n^2, 13n^2, 37n^2, 58n^2, 85n^2, 130n^2$$

minden pozitív egész n számra. Ha igaz a 3.13. sejtes, akkor nincs több ikerteljes szám.

3.3. Kockarácsok, mint részben rendezett halmazok

Miután az eddigiek során jellemeztük a kockarácsokat, kézenfekvő az egymáshoz való viszonyukat is vizsgálni. Ehhez természetes módon adódik a tartalmazás, mint reláció, és így a kockarácsok egy R részben rendezett halmazt alkotnak.

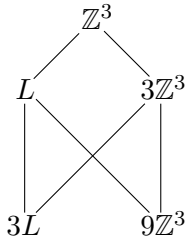
Hasonlóan tekinthetjük a $\mathbb{Z}^2$ rács négyzetrácsait, ezeket a 90°-os forgatásra való invariancia jellemzi. Emiatt ott bármely két négyzetrácsnak a metszete, illetve az uniója által generált részrács is négyzetes. Ezek a két négyzetrács legnagyobb alsó és legkisebb felső korlátja. Tehát a négyzetrácsok hálót alkotnak. A $\mathbb{Z}^3$ esete nem ilyen egyszerű, mivel ott nem tudjuk jellemezni a kockarácsokat ilyen egyszerűen.

Az R részben rendezett halmazban van legnagyobb elem, nyilvánvalóan a $\mathbb{Z}^3$. Továbbá, ha tekintünk egy tetszőleges elemet, egy K kockarácsot, akkor az annál kisebb elemek, azaz a K-ban fekvő kockarácsok részben rendezett halmaza izomorf lesz az R halmazzal. Ugyanis a K izomorf a $\mathbb{Z}^3$-bel, így benne ugyanolyan struktúrát alkotnak a kockarácsok.

A $\mathbb{Z}^2$-tel szemben nem alkotnak hálót a kockarácsok:

3.15. állítás. *Az R részben rendezett halmazban bármely két elemnek van alsó és felső korlátja, de ezek között nincs mindig legnagyobb, illetve legkisebb, azaz R nem háló.*

Bizonyítás. A 3.4. lemma szerint minden d élhosszúságú kockarácsnak alsó korlátja a $d^2\mathbb{Z}^3$ részrács. Egy d_1 és egy d_2 élhosszúságú kockarácsnak is lesz alsó korlátja, például a $d_1^2 d_2^2 \mathbb{Z}^3$ részrács. Természetesen mindennek a $\mathbb{Z}^3$ felső korlátja. Ennek ellenére ez nem lesz háló: nincs mindig legnagyobb alsó, és legkisebb felső korlát. Legyen ugyanis L egy primitív vektorból, például a $\mathbf{v} = (2, 2, 1)$ vektorból kapott 3 élhosszúságú kockarács ($\|\mathbf{v}\|^2 = 2^2 + 2^2 + 1 = 9 = 3^2$). Tekintsük ennek és a $\mathbb{Z}^3$-nek a 3-szorosát, illetve utóbbinak a 9-szeresét is.



Nyilvánvalóan fennáll a $9\mathbb{Z}^3 \leq 3\mathbb{Z}^3 \leq \mathbb{Z}^3$ és a $3L \leq L \leq \mathbb{Z}^3$ tartalmazás, ez utóbbiból a $3L \leq 3\mathbb{Z}^3$ tartalmazás is. A 3.4. lemma szerint $9\mathbb{Z}^3 \leq L$. Minden előbb felírt tartalmazás olyan, hogy nincs közöttük semmilyen kockarács, mert annak az élhossza 3-nak valódi osztója lenne, ami nincs. Így $3\mathbb{Z}^3$-nek és L-nek alsó korlátja a $9\mathbb{Z}^3$ és a $3L$, de nincsen legnagyobb alsó korlátjuk. Hasonlóan $9\mathbb{Z}^3$-nek és $3L$-nek felső korlátja a $3\mathbb{Z}^3$ és a L, de nincsen legkisebb felső korlát. □

Ennek ellenére a kockarácsok halmazában vannak olyan részhalmazok, melyek hálót alkotnak, ahogyan mutatja ezt a következő állítás.

3.16. állítás. *Egy adott $\mathbf{v} \in \mathbb{Z}^3$ primitív vektort tartalmazó kockarácsok hálót alkotnak. Ha $\|\mathbf{v}\|^2 = n^2m$, ahol m négyzetmentes, akkor ez a háló izomorf az n szám osztóhálójával.*

Bizonyítás. Az n szám minden d osztója meghatároz egy d élhosszúságú kockarácsot (melyben $\mathbf{v}$ benne van). Ha tekintünk egy d_1 osztóját n-nek, akkor az meghatároz egy d_1 élhosszú kockarácsot, melyben $\mathbf{v}$ relatív hossznégyzete $(n/d_1)^2m$. Ebben pontosan olyan kockarácsok vannak, melyeknek a relatív élhossza osztója n/d_1-nek. Ezért a $\mathbb{Z}^3$-beli élhossz olyan osztója n-nek, melynek d_1 osztója. Az egyértelműség miatt ezek ugyanazok, mint amiket közvetlenül kapunk. Így a $\mathbf{v}$-t tartalmazó kockarácsok részben rendezett halmaza éppen n osztóhálója. □

Irodalomjegyzék

[1] Lee M. Goswick, Emil W. Kiss, Gábor Moussong, Nándor Simányi: *Sums of squares and orthogonal integral vectors* (preprint, 2008., arXiv: 0806.3943)

[2] Hajós György: *Bevezetés a geometriába*, Tankönyvkiadó, Budapest, 1964.

[3] Kárteszi Ferenc: *Szemléletes geometria*, Gondolat, Budapest, 1966.

[4] C. G. Lekkerkerker: *Geometry of numbers*, North Holland, 1969.

[5] Reiman István: *A geometria és határterületei*, Gondolat, Budapest, 1986.

[6] Sárközy András: *A térbeli pontrács rácskockáiról*, Matematikai Lapok XII (1961) 232-245.

Tartalomjegyzék