Bsc algebra3 tanár gyakorlat

Önmagukra merőleges vektorok

Az alábbiak kiegészítések Freud Róbert 63. feladatához. A zárójeles állítás úgy szól, hogy $\mathbb{Z}_p^t$-ben, **ha** $t > 2$**, akkor** az önmagukra merőleges vektorok száma p-vel osztható. A bizonyítás Chevalley tételéhez kapcsolódik (Freud-Gyarmati: *Számelmélet*, 3.6.7b feladat).

Nyilván ha u önmagára merőleges, akkor λu is az. A $\mathbb{Z}_p^t$ nem nulla vektorait párhuzamosság szerint csoportosíthatjuk, így $p-1$ elemű osztályokat kapunk (hiszen $\mathbb{Z}_p$-ben $p-1$ darab nem nulla skalár van). Ezért az önmagukra merőleges vektorok száma (a nullvektorral együtt) $p-1$-gyel osztva 1 maradékot ad.

Az olyan $(a_1, a_2, \dots, a_n)$ önmagukra merőleges vektorok száma, amelyekre $a_1 \neq 0$, éppen $p-1$-szer annyi, mint az önmagukra merőleges, $(1, b_2, \dots, b_n)$ alakú vektorok száma, hiszen $(a_1, a_2, \dots, a_n)$ és $(1, (a_2/a_1), \dots, (a_n/a_1))$ párhuzamosak, de $(a_1, a_2, \dots, a_n)$ párhuzamossági osztályában csak 1 olyan vektor van, melynek az első komponense 1. Így kézzel kiszámolható, hogy $p = 7$ és $n = 3$ esetén a megoldásszám $6 \cdot 8 + 1 = 49$, mert az $a^2 + b^2 = -1$ megoldásszáma 8. (Ugyanis a kvadratikus maradékok $0, 1, 2, 4$, és ezekből a 6 csak egyféleképpen kapható meg összegként, amiből a két négyzetszám tételhez hasonlóan 8 megoldás lesz a és b előjelezésével és cseréjével). Ezt az állítást általánosítjuk majd.

Tanultuk tavaly számelméletből (és felhasználtuk a Gauss-prímek vizsgálatánál), hogy ha a $p > 0$ prím $4k+1$ alakú, akkor van olyan $u \in \mathbb{Z}_p$, hogy $u^2 = -1$, ha viszont a p prím $4k+3$ alakú, akkor nincs. Ez utóbbi esetben az $a^2 + b^2 = 0$ egyenletnek csak a triviális $a = b = 0$ megoldása van $\mathbb{Z}_p$-ben, mert ha $a \neq 0$, akkor $(b/a)^2 = -1$. Ezért ilyenkor $\mathbb{Z}_p^2$ önmagára merőleges vektorainak a száma 1.

Ha viszont a p prím $4k+1$ alakú, akkor $\mathbb{Z}_p^2$-ben $2p-1$ darab önmagára merőleges vektor van. Valóban, ha (a, b) ilyen, azaz $a^2 + b^2 = 0$, akkor $a = 0$ esetén $b = 0$, ez 1 megoldás. Ha $a \neq 0$, akkor a fentiek szerint a megoldások száma az $1 + x^2 = 0$ megoldásszámának $p-1$-szerese. Láttuk, hogy ennek van egy u megoldása, a másik megoldás $-u$, ami nem egyenlő u-val, mert $p \neq 2$ és $u \neq 0$. Ennek a másodfokú polinomnak tehát két gyöke van $\mathbb{Z}_p$-ben, és így az önmagukra merőleges vektorok száma $2(p-1)+1$.

Végül belátjuk, hogy minden p prímre $\mathbb{Z}_p^3$-ben p^2 darab önmagára merőleges vektor van. Ez $p = 2$-re nyilvánvaló, tegyük föl, hogy p páratlan. Elsőként megmutatjuk, hogy van olyan $a, b \in \mathbb{Z}_p$, hogy $a^2 + b^2 = -1$. Valóban, a négyzetelemek (kvadratikus maradékok és a nulla) száma $\mathbb{Z}_p$-ben $(p+1)/2$, hiszen $p-1$ nem nulla elemet emelhetünk négyzetre, de amit megkapunk, azt kétszer kapjuk meg, mert $a^2 = (-a)^2$. Így az a^2 és a $-b^2 - 1$ alakú elemek száma is $(p+1)/2$, ez együtt p-nél több, tehát van összeesés, amikor $a^2 = -b^2 - 1$.

Rögzítsük a, b-t. Ha $(x, y, z) \in \mathbb{Z}_p^3$ tetszőleges, akkor legyen $u = y + xa$ és $v = z + xb$, így $x^2 + y^2 + z^2 = (u^2 + v^2) - 2x(au + bv)$. Vagyis (x, y, z) pontosan akkor megoldás, ha $u^2 + v^2 = 2x(au + bv)$. Elég megszámolni az ilyen tulajdonságú (x, u, v) hármasokat, hiszen az (x, y, z) hármasok bijekcióban állnak az $(x, y + xa, z + xb) = (x, u, v)$ hármasokkal.

Mivel a és b nem mindkettő nulla, az $au + bv = 0$ egyenletet p darab (u, v) pár elégíti ki. Ezek akkor adnak megoldást, ha $u^2 + v^2 = 0$, ahonnan $0 = a^2u^2 + a^2v^2 = (a^2 + b^2)u^2 = -u^2$, azaz $u = 0$, és így $v = 0$. Ez csak egyetlen (u, v) pár, de x tetszőleges lehet, így összesen p megoldást kapunk. Ha $au + bv$ nem nulla, akkor $x = (u^2 + v^2)/(2au + 2bv)$ egyértelműen meghatározott. Ilyen (u, v) pár $p^2 - p$ darab van, mindegyik egy megoldást ad.