HALMAZRENDSZEREK

Matematika MSc hallgatók számára

13. Előadás

Előadó: Hajnal Péter
Jegyzetelő: Hajnal Péter

2010. május 11.

A véges projektív sík fogalma

A projektív síkgeometriában vannak pontok, egyenesek és köztük egy illeszkedési reláció. A projektív síkgeometria illeszkedési axiómai a következőek:

(Gi) Tetszőleges két különböző ponthoz, pontosan egy egyenes tartozik, amire illeszkedik mindkét pont.

(Gii) Tetszőleges két különböző egyeneshezhoz, pontosan egy pont tartozik, ami illeszkedik mindkét egyenesre.

(Giii) Minden egyenesre legalább három pont illeszkedik.

(Giv) Van három olyan pont, ami nem illeszkedik egy egyenesre.

Axiómáink (matematikai szemüveggel nézve) egy kicsit szószátyárak. Az (Gi) axiómából következik, hogy két egyenesre illeszkedő közös pontok száma 0 vagy 1 Tehát (Gii)-ben a pontosan egy pont létezését megkövetelni felesleges, elegendő egy megfelelő pont létezését garantálni. Ezt a szóhasználatot azért választottuk, hogy az első két axióma közötti hasonóságot hangsúlyozzuk: a pont-egyenes szerepkörének felcserelésével egyik a másik állítását adja. Első két projektív síkgeometria tételünk lehet a (Giii) és (Giv) axióma pont-egyenes szerepcserével történő átírásának (dualizálásának) igazolása: Az axiómákból következik, hogy minden pontra legalább három egyenes illeszkedik, továbbá található három egyenes, amire nem illeszkedik közös pont. Ezen állítás logikai úton az axiómákból levezethető.

Ennek érdekes következményei vannak. A projektív geometria tételeinek duálisai automatikusan igazak. Egy tételhez vegyük levezetését. A levezetés mélyén axiómákra hivatkozunk. Ezen axiómák dualizáltjaira is építkezhetünk, hiszen ezek vagy axiómák maguk, vagy levezethetők. A dualizált alapokra ugyanazt a bizonyítási struktúrát rakva rendre a dualizált állításokat kapjuk, végül az eredeti tétel dualizáltja adódik.

Megjegyzés. (Gi) egy jólismert axióma az Euklideszi geometriából. (Gii) viszont az Euklideszi geometriától való különbséget pontosítja. Ott két különböző egyenes metsző (egy közös illeszkedő pont) vagy párhuzamos (nincs közös illeszkedő pont). A projektív síkon bármely két különböző egyenes metsző. (Giii) csupán következő lehetőséget zárja ki: Egy E egyenesünkre egy pont kivételével mindegyik illeszkedik. p az egyetlen E-re nem illezkedő pont. Az összes többi egyenesünkre két pont illeszkedik: p és E egy pontja (és minden E-re illeszkedő ponthoz van is ilyen egyenes). Eddigi axiómáink megengedik, hogy a sík helyett egyetlen egyenes pontjai alkossák

geometriánkat (kétdimenzió helyett egydimenzió legyen). (Giv) ezt a lehetőséget zárja ki.

A fenti logikai szemléletmód egy ponton fárasztóvá válhat. A geométerek is áttérnek egy halmazelméleti nyelvre (ahogy rajzolnak ezt teszik): Legyen $\mathcal{P}$ a pontok halmaza és $\mathcal{E}$ az egyenesek halmaza. Ha p illeszkedik E-re, akkor azt mondjuk E áthalad p-n, p az E egyenes egy pontja. E azonosítható a rá illeszkedő pontok halmazával, $\mathcal{P}$ egy részhalmazával. $p \in E$ az illeszkedés halmazelméleti szemléletmódban való kifejezése. Persze az axiómarendszer mögött több ponthalmaz és efeletti halmazrendszer (egyenesek ponthalmazai) állhatnak. Ezeket nevezzük az illeszkedési axiómák modelljeinek.

A logikailag levezetett állítások persze minden modellre érvényesek lesznek. Ennek ellenére fontos konkrét modelleket is vizsgálni. (Igazából a klasszikus projektív síkgeometria egyetlen modellt, az úgy nevezett valós projektív síkot vizsgálja.) Esetünkben véges ponthalmazzal rendelkező modellek is vannak. Ezek a véges projektív síkok. Mi ezeket vizsgáljuk.

Definíció. Egy V halmazfeletti $\mathcal{H}$ halmazrendszer akkor és csak akkor véges projektív sík, ha V elemeit pontoknak, éleit egyeneseknek nevezve, az illeszkedést pedig az „eleme” relációnak gondolva az (Gi)-(Giv) axiómákat teljesítő struktúrát kapunk.

Persze azt is mondhattuk volna, hogy $\mathcal{H}$ megkapható egy axiómatikusan leírt véges projektív geometriából a halmazelméleti nyelv bevezetésével.

1. Tétel. *Egy $\mathcal{H}$ halmazrendszer akkor és csak akkor projektív geometria, ha*

(Hi) A pontok száma $k^2 + k + 1$, alkalmas $k \geq 2$ egészre,

(Hii) $k + 1$-uniform,

(Hiii) Bármely két különböző pontot pontosan egy él tartalmaz,

Bizonyítás. A bizonyításnak két iránya van: Egy geometriából konstruált halmazrendszer eleget tesz a tételbeli feltételeknek. Továbbá, a fenti axiómáknak elegettevő halmazrendszerből képzett geometria eleget tesz (Gi)-(Giv)-nek. Mi csak az elsőt nézzük meg vázlatosan.

Először igazoljuk, hogy halmazrendszerünk uniform. Azaz a geoemtriánk bármely két egyenesére ugyanannyi pont illeszkedik. Legyen E és F két különböző egyenes. Ekkor (iii) és (iv) alapján konstruálható egy p pont, ami egyik egyenesre se illeszkedik. p-ből az E egyenes „vetíthető” F-re (egy E-re illeszkedő q ponthoz a vetítés a „$q \mapsto pq$ egyenes és F metszéspontja” pontot rendeli). Ez a vetítés egy bijekciót létesít E és F ponthalmaza között. A közös élméretet jelöljük $k + 1$-gyel. (Giii) miatt $k \geq 2$.

Ezek után k függvényében kifejezhető az összes pont száma: Legyen p egy pont és E egy rajtá át nem menő egyenes. Könnyű látni, hogy az p-n átmenő egyenesekre illeszkedő, p-től különböző pontok diszjunkt halmazokat adnak, amelyek lefedik az összes p-től különböző pontot. A p-n átmenő egyenesek halmaza mind px egyenes alakú, ahol x egy E-re illeszkedő pont. Sőt különböző x-ekre különböző px egyeneseket kapunk. Azaz p-n ugyananyi egyenes halad át, mint ahány pont illeszkedik E-re, $k + 1$. Ezen egyeneseknek k pontja különbözik p-től. Tehát a p pont és az őt nem tartalmazó $k + 1$ darab k elemű diszjunkt halmaz együtt kiadja az összes pontot, amiből ezek szerint $1 + (k + 1)k = k^2 + k + 1$ darab van.

(Hiii) a (Gii) axióma „szó szerinti” fordítása. □

Bizonyításunk vázlatos volt. A pq egyenesre való hivatkozás persze a (Gi) axióma alapján megalapozott. Két egyenes metszéspontjáról beszélni a (Gii) axióma miatt korrekt. A vetítés jól definiáltsága is többször kívánja az axiómákra való hivatkozást.

Definíció. A tételben szereplő k szám a véges projektív sík paramétere.

Alapkérdés, hogy milyen paraméterű projektív síkok léteznek.

A véges projektív síkok konstrukciói

Példa. Fano-sík.

Először nézzük a standard koordináta-geometriai konstrukciót.

Definíció. Legyen $\mathbb{F}$ egy tetszőleges test. $\mathbb{F}^3-\{(0,0,0)\}$-n definiáljuk azt a relációt, hogy „nem-nulla skalárral való szorzással megkaphatók egymásból". Ez egy ekvivalenciareláció. (a,b,c) osztályát $(a:b:c)$-vel jelöljük. Ezen ekvivalenciaosztályok alkotják a pontok halmazát.

Ugyanezen ekvivalenciareláció osztályai alkotják az egyenesek halmazát is. Ha (a,b,c) osztályát egyenesként szeretnénk értelmezni, akkor $(a:b:c)^*$-ként jelöljük.

$(a:b:c)$ és $(A:B:C)^*$ akkor és csak akkor illeszkedik, ha $aA+bB+cC=0$.

Az így kapott geometriát $PG(2,\mathbb{F})$-fel jelöljük.

Megjegyzés. Ha $\mathbb{F}=\mathbb{R}$, akkor a fenti konstrukció a szokásos leírása a valós projektív síknak. $\mathbb{R}^3$ a tér koordináta-geometriai leírása. A pontokat leíró ekvivalenciaosztályaink megfelelnek az origón átmenő egyeneseknek. Ezek az ekvivalenciaosztályok azonosítható a gömbfelület átellenes pontpárjaival. Az egyeneseket leíró ekvivalenciaosztályaink megfelelnek az origón átmenő síkoknak ($(A:B:C)^*$ egyenes). Ezek az ekvivalenciaosztályok azonosíthatók a gömbfelület főköreivel. Az illeszkedés a szokásos gömbfelületi illeszkedés.

Könnyű ellenőrizni (kellő aritmetikai jártassággal), hogy $PG(2,\mathbb{F})$ egy projektív sík. Ha $\mathbb{F}$ véges test, akkor $PG(2,\mathbb{F})$ egy véges projektív sík. $\mathbb{F}^3-\{(0,0,0)\}$ egy $|\mathbb{F}|^3-1$ elemű halmaz. A definiált ekvivalenciareláció minden ekvivalenciaosztálya $|\mathbb{F}|-1$ elemű. Azaz $\frac{|\mathbb{F}|^3-1}{|\mathbb{F}|-1}=|\mathbb{F}|^2+|\mathbb{F}|+1$ elemű lesz a ponthalmaz, $PG(2,\mathbb{F})$ paramétere $|\mathbb{F}|$.

Példa. $PG(2,\mathbb{F}_2)$ a Fano-sík(kal izomorf).

Algebrai tanulmányaink egyből adják a következő tételt.

2. Tétel. *Minden q prímhatványra van q paraméterű projektív sík.*

Nemcsak a fenti síkok ismertek. Van ezektől lényegesen kiülönböző projektív sík is. Viszont az összes ismert konstrukcióra teljesül, hogy paramétere egy prímhatvány. Tehát ebben a pillanatban lehetséges, hogy a paraméter prímhatványsága szükséges feltétel is. Ezt eddig senki sem tudta bizonyítani.

Sejtés. k akkor és csak akkor egy véges projektív sík paramétere, ha egy prímszám hatványa.

$PG(2,\mathbb{F})$-ben Desargues tétele igaz (akik nem tanulták ezt geometriából ugorják át ezt a megjegyzést). Igazából akik a valós projektív síkon látták a tételt és szerepelt koordináta-geometriai indoklás, azok nem lepődnek meg. A bizonyítás számolása csak olyan lineáris algebrát tartalmaz, ami tetszőleges test feletti vektortérben igaz. Vannak olyan véges (és végtelen) projektív síkok is, ahol Desargues-tétel nem igaz. Tehát nemcsak a fenti véges projektív síkok léteznek. Ez a sejtés igazolásának nehézségeire is rámutat.

Megjegyezzük, hogy fenti állításunk megfordítható: a Desargues-tétel akkor és csak akkor teljesül egy véges projektív síkon, ha az a $PG(2,\mathbb{F})$ példák egyike (illetve izomorf valamelyikkel).

A véges projektív síkok és latinnégyzetek

Emlékeztető. Egy $L_{n\times n}$ táblázat, amely elemei $A=\{1,2,\dots,n\}$-beliek akkor és csak akkor latinnégyzet, ha minden sorban és minden oszlopban A összes eleme szerepel (persze ekkor minden A-beli elem pontosan egyszer szerepel, aminek egy alternatív előírása lehetett volna, hogy a sorokban és oszlopokban ne legyen ismétlődő elem)

Definíció. L és L' két latinnégyzet ortogonális, ha az $(L_{i,j}, L'_{i,j})$ rendezettpárok kiadják A^2-t (vagy különbözőek, vagy A^2 minden elemét pontosan egyszer adják ki).

Példa. Egy 5×5-ös példa:

$$\begin{pmatrix} 1&2&3&4&5\\ 2&3&4&5&1\\ 3&4&5&1&2\\ 4&5&1&2&3\\ 5&1&2&3&4 \end{pmatrix}, \qquad \begin{pmatrix} 1&2&3&4&5\\ 3&4&5&1&2\\ 5&1&2&3&4\\ 2&3&4&5&1\\ 4&5&1&2&3 \end{pmatrix}.$$

A példában mindkét latinnégyzet első sora az elemek nagyságszerinti felsorolása. Könnyű látni, hogy az „átnevezés" operáció megtartja a latinnégyzetséget. Sőt, ha L és L' ortogonális latinnégyzetek akkor független átnevezéseikkel kapott $\widetilde{L}$ és $\widetilde{L}'$ is ortogonális lesz.

Páronként ortogonális latinnégyzetek nagyobb halmaza is megadható:

Példa. Az előző 5×5-ös példa megtoldható az alábbi két négyzettel. Az így kapott táblázatnégyesből bármelyik kettő ortogonális.

$$\begin{pmatrix} 1&2&3&4&5\\ 4&5&1&2&3\\ 2&3&4&5&1\\ 5&1&2&3&4\\ 3&4&5&1&2 \end{pmatrix}, \qquad \begin{pmatrix} 1&2&3&4&5\\ 5&1&2&3&4\\ 4&5&1&2&3\\ 3&4&5&1&2\\ 2&3&4&5&1 \end{pmatrix}.$$

Azonban van egy határ.

3. Lemma. *$n\times n$ méretű latinnégyzetekből legfeljebb $n-1$ lehet páronként ortogonális.*

Bizonyítás. Egy korábbi megjegyzésünk alapján négyzeteink átnevezhetők úgy, hogy mindegyik első sora a standard $1, 2, \ldots, n$ sor legyen. Ezek után nézzük meg, hogy mi áll a második sor legelső pozíciójában. A latinnégyzet tulajdonság (első oszlop) miatt az ott álló számok a $\{2, 3, \ldots, n\}$ halmazból kerülnek ki, Továbbá KÜLÖNBÖZŐEK: Valóban, ha az a elem állna ott L-ben és L'-ben is, akkor az $(L_{i,j}, L'_{i,j})$ párok között az (a, a) pár ismétlődne. □

A következő tétel kapcsolatot létesít a véges projektív síkokkal.

4. Tétel. *Akkor és csak akkor létezik k paraméterű véges projektív sík, ha létezik $k-1$ páronként ortogonális $k \times k$ méretű latinnégyzet.*

Bizonyítás. Az állítás két iránya közül csak az egyiket látjuk be. (A hiányzó rész abból következik, hogy az ismertetett gondolatmenet megfordítható. A megfordítást az érdeklődő hallgató elvégezheti.)

Tegyük fel, hogy van egy k paraméterű véges projektív síkunk. Konstruálunk $k-1$ páronként ortogonális latinnégyzetet.

Vegyünk egy p pontot és egy rajta átmenő S, O egyenest. S és O p-től különböző pontjait nevezzük el a $\{1, 2, \ldots, k\}$ halmaz elemeivel (ezek mátrixunk sor/oszlop-pozíciói). Legyen E egy szintén p-n átmenő egyenes, ami különbözik S és O-tól. E p-től különböző pontjait nevezzük el A elemeivel (mátrixunk elemeinek névhalmaza). Az E egyeneshez hozzárendelünk egy L_E latinnégyzetet: L_E i-edik sorában és j-edik oszlopában álljon az a karakter, amit úgy kapunk, hogy S i-nevű pontját összekötjük O j-nevű pontjával és megnézzük, hogy az összekötő egyenes hol metszette el E-t.

L_E valóban latinnégyzet. i-edik sorában az elemeket az S i nevű pontján átmenő (p-t elkerülő) egyenesek metszik ki E-ből. Ezek nyilván különböző pontok/elemek lesznek. Az oszlopokra hasonlóan látható a szükséges tulajdonság.

Az ortogonalitáshoz nézzük meg, hogy $((L_E)_{i,j}, (L_F)_{i,j})$ párok között hányszor szerepel (a, b). Ehhez E-n keressük meg az a, F-en a b nevű pontot. Ezek összekötő egyenese S-ből és O-ból kimetsz egy i, illetve j nevű pontot. Azaz a tetszőlegesen kiválasztott (a, b) szerepel a párjaink listáján (igazából az is látszik, hogy pontosan egyszer). □

A latinnégyzetek ortogonalitása a véges projektív síkok vizsgálata előtt az érdeklődés központjába került egy szórakoztató feladat révén. A feladat azt kérte, hogy masiniroztassunk 36 katonát egy 6×6-os elrendezésben, ha a 36 katona hat hadosztályból hat különféle ranggal jön (mindegyik hadosztályon belül mindegyik rang előfordul) és azt szeretnénk, hogy mindegyik sorban/mindegyik oszlopban mindegyik rang, illetve hadosztály reprezentálva legyen. Pontosabban fogalmazva adjunk egy feltételeknek megfelelő elrendezést vagy bizonyítsuk be, hogy ilyen nem lehetséges.

Euler érdeklődött a probléma iránt, de nem tudta megoldani. Hozzájárulása azonban az alapfogalom elnevezéséhez vezetett: a rendfokozatokat, illetve a rangokat latin, illetve görög betűkkel jelölte. Ő használta a latin- és görögnégyzet fogalmát. A két karakterhalmaz megkülönböztetése felesleges. A latinnégyzetek lettek a túlélők, habár ez ma már csak elnevezés. Mi is már a standardabb $\{1, 2, , \ldots, n\}$ jelkészletet használtuk.

A fentiek talán már sugalják, hogy a válasz az, hogy nem lehet megfelelő elrendezést találni. Az első teljes bizonyítás 1901-ben született. Gaston Tarry bizonyította be (amit Euler nem tudott), aki középiskolában részesült formális matematika oktatásban, később Algériában francia köztisztviselő lett. Bizonyítása lényegében az

összes lehetőség áttekintése (szimmetria meggondolásokkal kezelhetővé téve ezt a számítógépek korszaka előtti eset analízist).

5. Tétel (Tarry-tétel). *Nem létezik két* 6×6 *méretű ortogonális latinnégyzet.*

A tétel egy egyszerű következménye, hogy nincs 6 paraméterű projektív sík (amihez öt darab páronként ortogonális, 6×6 méretű latinnégyzet lenne szükséges). Ezt később Tarry tételétől függetlenül látni fogjuk.

Nem lehetséges paraméter értékek

Tudjuk, hogy $k = 2, 3, 4, 5, 7, 8, 9, 11$ értékre van ilyen paraméterű véges projektív sík. Kicsi nem prímhatványokra tudjuk-e, hogy nem létezik ilyen paraméter értékű projektív sík? A $k = 6$ eset viszonylag klasszikus állítás. A $k = 10$ eset is bizonyítva van, de mély matematikai elméletek bevetésével, igen intenzív számítógépes segédlettel.

6. Tétel. *(i) Nem létezik* 6 *paraméterű véges projektív sík,*

(ii) Nem létezik 10 *paraméterű véges projektív sík.*

A tétel első része következik Tarry tételéből és az alábbi általánosabb tételből is. Ez utóbbit be is bizonyítjuk.

7. Tétel (Bruck—Ryser-tétel). *Tegyük fel, hogy* $k \equiv 1, 2 \pmod 4$ *és létezik* k *paraméterű véges projektív sík. Ekkor* k *két négyzetszám összege.*

Bizonyítás. Legyen n a feltételezett k paraméterű véges projektív sík pontszáma ($n = k^2 + k + 1$). A feltétel alapján $n \equiv 3 \pmod 4$. (Természetesen n egyben a síkunk egyenesszáma is.)

Legyen A a síkunk pont-egyenes illeszkedési mátrixa. Azaz A egy $n \times n$ méretű mátrix és egy pontnak megfelelő sor és egy egyenesnek megfelelő oszlop találkozásában 1 áll illeszkedésük esetén, 0 különben. Legyen I az egységmátrix, J a csupa 1 elemet tartalmazó mátrix (minden mátrixunk $n \times n$ méretű lesz). Könnyű ellenőrizni, hogy

$$A \cdot A^t = J + k \cdot I.$$

Vizsgáljuk az

$$x \cdot A \cdot A^t \cdot x = x(J + k \cdot I)x^t = x \cdot J \cdot x^t + k \cdot x \cdot I \cdot x^t.$$

kvadratikus alakot (ami nyilván pozitív definit), ahol $x = (x_1, x_2, \ldots, x_n)$. Legyen $y = x \cdot A$ és $s = x_1 + x_2 + \ldots + x_n$. Ekkor a fenti egyenlőségünk $y \cdot y^t = s^2 + k \cdot x \cdot x^t$ alakot ölti. Persze $x \cdot x^t = x_1^2 + x_2^2 + \ldots + x_n^2$ és $y \cdot y^t = y_1^2 + y_2^2 + \ldots + y_n^2$. Az egyenlőség két oldalához kx_{n+1}^2-et adva kapjuk, hogy

$$y_1^2 + y_2^2 + \ldots + y_N^2 + kx_{n+1}^2 = k(x_1^2 + x_2^2 + \ldots + x_n^2 + x_{n+1}^2) + s^2.$$

Vezessük be az $\widetilde{x} = (x_1, x_2, \ldots, x_n, x_{n+1})$ jelölést. k (mint minden természetes szám felírható négy négyzetszám öszegeként. A zárójelben lévő négyzetösszeg tagjainak

száma néggyel osztható, azaz a tagok csooprtosíthatók $(n+1)/4$ csoportba, amelyek mindegyike négy x_i-négyzet összege. n és egy-egy csoport szorzata átírható az

$$(\alpha^2+\beta^2+\gamma^2+\delta^2)(a^2+b^2+c^2+d^2) = (\alpha a-\beta b-\gamma b-\delta d)^2+(\beta a+\alpha b-\delta c-\gamma d)^2+ \\ (\gamma a+\alpha c-\beta d-\delta b)^2+(\delta a+\alpha d+\gamma b-\beta c)^2$$

azonosság alapján. (Az azonosság első pillantásra sokkoló (hogyan lehet erre rájönni?). Ha azonban valaki ismeri a kvaterniók aritmetikáját, akkor a csoda természetessé válik.) Így áttérhetünk $z=(z_1,z_2,\ldots,z_{n+1})$ változókra, amelyekre $k(x_1^2+x_2^2+\ldots+x_n^2+x_{n+1}^2)=z_1^2+z_2^2+\ldots+z_n^2+z_{n+1}^2$. Továbbá z az x vektorból lineáris helyettesítéssel kaphatók. (Itt használtuk a fenti összefüggést. Egy csoport k-szorosa egész koordinátájú x esetén mindig egész, így szükségszerűen felírható négy négyzetszám összegeként. A képlet „csak" a függőség linearitását mutatja.) Összefoglalva

$$y_1^2+y_2^2+\ldots+y_n^2+kx_{n+1}^2=z_1^2+z_2^2+\ldots+z_n^2+z_{n+1}^2+s^2,$$

ahol $y=x\cdot A$ és $z=\widetilde{x}\cdot B$ alkalmas A és B egész mátrixokra.

A bizonyítás végén rögzítünk $\widetilde{x}$ koordinátái közt homogén lineáris összefüggéseket úgy, hogy $y_i=\pm z_{\pi(i)}$ teljesüljön $i=1,2,\ldots,n$ esetén, az $\{1,2,\ldots,n\}$ egy alkalmas permutációjára.

A bal és jobb oldali kifejezéseket felírva az $x_1,x_2,x_3,\ldots$ változók mindegyike szerepel (mindkét oldal pozitív definit függvénye az $x_1,x_2,x_3,\ldots$ változóknak). Válasszunk olyan y_i és z_j változókat, amelyeket az x_i-k lineáris kombinációjaként felírva szerepel az x_1 változó. Az egyszerűség kedvéért tegyük fel, hogy y_1 és z_1 felírása is használja x_1-et. Ekkor $y_1=z_1$ vagy $y_1=-z_1$ feltétel teljesül, ha x_1 alkalmas lineáris kombinációja a többi x_i változónak. Ezt tegyük fel és ennek megfelelően alakítsuk át az egyenletünket:

$$y_2^2+\ldots+y_n^2+kx_{n+1}^2=z_2^2+\ldots+z_n^2+z_{n+1}^2+s^2,$$

ahol az y_i és z_j változók már csak $x_2,x_3,\ldots$ változóktól függnek. A kapott egyenlőség két oldala az $x_2,x_3,\ldots$ változók pozitív definit függvénye! Így mindkét oldalon szerepel x_2. Ennek alkalmas (racionális együtthatós, homogén lineáris) függőséget lerögzítve

$$y_3^2+\ldots+y_n^2+kx_{n+1}^2=z_3^2+\ldots+z_n^2+z_{n+1}^2+s^2$$

összefüggéshez jutunk. Eljárásunkat folytathatjuk, amíg az

$$kx_{n+1}^2=z_{n+1}^2+s^2$$

egyenletet nem kapjuk. x_{n+1} alkalmas rögzítésével egy nem-triviális racionális megoldást kapunk, ami ad egy nem-triviális egész megoldást is.

Számelméleti meggondolásokból adódik, hogy ez csak úgy lehet, ha k két négyzetszám összege. Ez a tételt bizonyítja. □

A fenti tétel végtelen sok paraméter értéket kizár mint lehetőség. Ennek ellenére a 12 paraméterérték esete mind a mai napig nyitott.