Kombinatorikusan definiált ponthalmazok véges síkokon

Diplomamunka

Írta: Csajbók Bence

Matematikus szak,
Matematika tanár szak

Témavezető:

Kiss György, egyetemi docens
Geometriai tanszék

Eötvös Loránd Tudományegyetem
Természettudományi Kar
2010

Tartalomjegyzék

Bevezetés **3**

1. Szemiívekről általában **5**
1.1. Tételek, definíciók, jelölések 5
1.2. Szemiívek létezése 6
1.3. Felső becslés szemiívek elemszámára 8
1.4. Szemiívek hosszú szelővel 9
1.5. Szemiívek 2 db hosszú szelővel 11

2. Szemiívek három egyenesen **15**
2.1. Szemiívek két egyenesen 15
2.2. Szemiívek három, egy ponton átmenő egyenesen 15
2.3. Szemiívek projektív háromszögben 19

3. Szemioválisok három, egy ponton átmenő egyenesen **23**
3.1. Pollard és Grynkiewicz tétele 23
3.2. Elemszám becslések 24
3.3. Tételek erős szemioválisokról 28
3.4. Erős szemioválisok karakterizációja 28

4. További konstrukciók **31**
4.1. 2- és 3-szemiívek 31
4.2. Példák görbék segítségével 34

5. Véges geometriák és additív kombinatorika középiskolában **36**
5.1. Bevezetés 36
5.2. Egy kártyatrükk, és ami mögötte van 38
5.3. Additív kombinatorikai feladatok 45
5.4. Összefoglalás 49

Irodalomjegyzék **50**

Bevezetés

A q-adrendű Π_q projektív sík S_k nemüres ponthalmazát k-szemiívnek nevezzük, ha minden $P \in S_k$ pont esetén pontosan k db $l_1, l_2, \ldots, l_k$ egyenes van, melyre $S_k \cap l_i = \{P\}$ teljesül $(i = 1, 2, \ldots, k)$. Ezeket az egyeneseket S_k P-beli érintőinek nevezzük. A szemiív elnevezés onnan származik, hogy a projektív sík k-ívei egyben $(q + 2 - k)$-szemiívek. Az 1-szemiívek a szemioválisok, melyeket az elmúlt 10 évben sokan vizsgáltak, de még ezekkel kapcsolatban is nagyon sok megoldatlan probléma van.

A szemiívek teljes leírása reménytelen feladat, ezért érdemes plusz feltételek mellett vizsgálni őket. Ilyen feltétel például, ha a szemiív tartalmaz sok pontból álló kollineáris ponthalmazt (hosszú szelőt). Néhány ezzel kapcsolatos, szemioválisokra vonatkozó, Dover [6] által bizonyított eredményt sikerült szemiívekre általánosítani, ezek az 1.4-es szakaszban szerepelnek. Ezt követően azokat a szemiíveket vizsgáljuk, melyeknek legalább két, viszonylag hosszú szelője van.

Egy másik vizsgált kérdés, azon szemioválisok karakterizálása, melyeket tartalmaz három egyenes [3], [13]. Ennek okán a 2. fejezetben megpróbáljuk hasonló módon karakterizálni a szemiíveket. A $PG(2, q)$-síkokon bizonyos esetben ez teljesen sikerült.

A három egy ponton átmenő egyenes által tartalmazott szemioválisok elemszámára additív kombinatorikai tételek segítségével új alsó becsléseket adunk a 3. fejezetben. A tételek általánosíthatóak voltak 2-szemiívekre, melyekre további példákat is megadunk. Ez a 4. fejezetben szerepel, néhány további konstrukcióval együtt. A felhasznált additív kombinatorikai tételek Grynkiewicz [8] és Pollard [15] eredményei.

A három egy ponton átmenő egyenes által tartalmazott szemioválisok közül az egy bizonyos extra tulajdonsággal rendelkezőket erős szemioválisnak nevezik [3]. A 3. fejezetben az eddigi eredményeket megjavítva megmutatjuk, hogy a $PG(2, p^{2n})$ síkokon ezek elemszáma csak $3(p^{2n} - p^n)$ lehet, míg $p > 7$ esetén $PG(2, p^{2n+1})$ síkokon nem léteznek ilyen struktúrák.

Az 5. fejezet a diplomamunkám tanári része, melyhez a fejezet elején külön bevezető található.

A szakirodalomban megtalálható tételek bizonyításához csak hivatkozásokat közlünk. Ez alól egyedül a szerző Középiskolai Matematikai Lapokban megjelent [4], és a Kiss Györggyel közös, közlésre benyújtott cikke [5], valamint az 5. fejezet egyes állításai jelentenek kivételt.

Köszönetnyilvánítás

Köszönettel tartozom témavezetőmnek, Kiss Györgynek, a kiváló témajavaslatért, a sok szakirodalomért, valamint hogy mindig szakított időt a jegyzeteim átnézésére és az ezekkel kapcsolatos hasznos észrevételeire.

1. fejezet

Szemiívekről általában

1.1. Tételek, definíciók, jelölések

A véges projektív sík axiómáit és alapvető kombinatorikus tulajdonságait dolgozatom utolsó fejezetében egy középiskolásoknak szánt kártyatrükk bemutatása során ismertetem, így ezekre itt most nem térek ki. Amennyiben az olvasó az ott leírtaknál tömörebb bevezetőt szeretne, akkor Kiss György és Szőnyi Tamás: *Véges Geometriák* [14] című könyvét tudom ajánlani. Az alábbiakban néhány alapvető állítás, definíció és jelölés következik, melyeket a dolgozatban használni fogunk. Π_q-val mindig q-adrendű véges projektív síkot fogunk jelölni.

1.1.1 Állítás: A K test feletti háromdimenziós vektortér egydimenziós altereinek halmazát jelöljük $\mathcal{P}$-vel, kétdimenziós altereinek halmazát pedig $\mathcal{E}$-vel. Ekkor a $(\mathcal{P}, \mathcal{E})$ pár projektív síkot alkot (az illeszkedési reláció a tartalmazás).

A bizonyításhoz lásd [14, p. 3].

1.1.2 Definíció: Amennyiben K a q-elemű véges test, akkor a fenti módon definiált véges projektív síkot $PG(2, q)$-val jelöljük. Véges projektív síkokon a Desargues-tétel pontosan a $PG(2, q)$ síkokon teljesül [14, p. 49], ezért néha Desargues sík elnevezést fogjuk használni.

A későbbiekben sokszor fogjuk használni az alábbi jól ismert trükköt [3], [13]:

1.1.3 Állítás: Amennyiben l_1, l_2, l_3 a $PG(2, q)$ páratlan rendű sík három, egy ponton átmenő egyenese, akkor a koordinátarendszert megválaszthatjuk úgy, hogy az egyenesek egyenletei: $X_1 = -X_3$, $X_1 = 0$ és $X_1 = X_3$ legyenek. Ilyenkor a metszéspont koordinátái: $(0, 1, 0)$ és az egyenesek $(-1, a, 1)$, $(0, b, 2)$, $(1, c, 1)$ pontjai pontosan akkor kollineárisak, ha az alábbi determináns értéke 0:

$$\begin{vmatrix} -1 & a & 1 \\ 0 & b & 2 \\ 1 & c & 1 \end{vmatrix}.$$

Ez pedig akkor teljesül, ha $a + c = b$.

1.1.4 Állítás: Amennyiben l_1, l_2, l_3 a $PG(2, q)$ sík három, nem egy ponton átmenő egyenese, akkor a koordinátarendszert megválaszthatjuk úgy, hogy a három egyenes

metszéspontjai az $(1,0,0)$, $(0,1,0)$ és $(0,0,1)$ pontok legyenek [13]. Ekkor az egyenesek $(0,a,1)$, $(b,0,1)$ és $(-c,1,0)$ pontjai pontosan akkor kollineárisak, ha az alábbi determináns 0:

$$\begin{vmatrix} 0 & a & 1 \\ b & 0 & 1 \\ -c & 1 & 0 \end{vmatrix}.$$

Ez pedig akkor teljesül, ha $b = ac$.

1.1.5 Definíció: Amennyiben A és B egy additív csoport részhalmazai, használni fogjuk az alábbi jelöléseket:

$$A + B = \{a + b \mid a \in A, b \in B\},$$

$$A - B = \{a - b \mid a \in A, b \in B\}.$$

1.1.6 Definíció: A Π_q sík olyan ponthalmazát, mely nem tartalmaz három egy egyenesen lévő pontot, ívnek nevezzük. A k pontból álló íveket k-ívnek hívjuk. Páratlan rendű sík $(q+1)$-íveit oválisnak, páros rendű sík $(q+2)$-íveit hiperoválisnak nevezzük.

1.1.7 Állítás: $PG(2,q)$-ban léteznek oválisok, ha q páros, akkor hiperoválisok is.

A bizonyítása [14, p. 90]-ben megtalálható.

1.1.8 Definíció: A Π_q q-adrendű projektív sík $\sqrt{q}$-adrendű részsíkját Baer-részsíknak nevezzük.

1.1.9 Definíció: A Π_q q-adrendű sík olyan ponthalmazát mely nem tartalmaz teljes egyenest, de minden egyenest metsz, blokkoló halmaznak nevezzük.

1.1.10 Tétel: Minden Baer-részsík blokkolóhalmaz.

A bizonyítása szintén [14, p. 99]-ben olvasható.

1.1.11 Definíció: Az l egyenest az $S \subset \Pi_q$ ponthalmaz k-szelőjének hívjuk, ha $|l \cap S| = k$.

1.1.12 Definíció: Az l egyenest az $S \subset \Pi_q$ ponthalmaz érintőjének P-beli érintőjének hívjuk, ha $l \cap S = \{P\}$.

1.2. Szemiívek létezése

Ebben a fejezetben definiáljuk a szemiíveket, és megadunk néhány egyszerű példát, mely bizonyítja, hogy minden pozitív egész k-érték esetén léteznek k-szemiívek.

1.2.1 Definíció: Egy $S_k \subset \Pi_q$ nemüres ponthalmazt $1 \leq k \leq q$ esetén k-szemiívnek nevezünk, ha minden $P \in S_k$ pont esetén P-nek pontosan k db érintője van.
Az 1-szemiíveket szemioválisnak nevezik.

1.2.2 Állítás: Legyen $S_k \subset \Pi_q$ egy k-szemiív, ekkor teljesül az alábbi négy állítás:

1. $k = q + 1$ pontosan akkor, ha S_k egyetlen pontból áll,

2. $k = q$ pontosan akkor, ha S_k egy egyenes egynél több pontból álló részhalmaza,

3. $k = q - 1$ pontosan akkor, ha S_k három nem kollineáris pontból áll,

4. $k = q - 2$ pontosan akkor, ha S_k az alábbiak egyike:

   - S_k négy általános helyzetű pont
   - S_k egy teljes négyszög 6 csúcsa
   - S_k egy Fano-részsík.

Bizonyítás: Csak a 4. pontot bizonyítjuk, az első három magától értetődő. Tegyük fel, hogy $k = q - 2$ és legyen $P \in S_k$. Ekkor P-n át kell, hogy menjen pontosan 3 olyan egyenes: l_1, l_2, l_3, amely tartalmaz P-n kívül is S_k-beli pontot.

Az l_i ($i \in \{1, 2, 3\}$) egyenesek egyike sem tarlamzahat 3-nál több pontot, mert ha lenne köztük ilyen, akkor a másik két egyenes P-n kívüli pontjainak legfeljebb $q - 3$ db érintője lenne. Ez alapján 3-esetet különböztethetünk meg:

1. Ha mindhárom egyenes 2-2 pontot tartalmaz, akkor ez egy 4 elemű ponthalmaz, mely könnyen láthatóan nem tartalmazhat három kollineáris pontot.

2. Ha a három egyenes egyike 3 pontot tartalmaz, a másik kettő pedig 2 pontot, akkor a 2 db 2 pontot tartalmazó egyenes P-től különböző A illetve B pontjai egy egyenesre kell, hogy essenek a 3 pontot tartalmazó egyenes valamely P-től különböző Q pontjával, másküllönben A-nak és B-nek legfeljebb $q - 3$ érintője lenne. Ekkor azonban a ponthalmazunk lefedhető az AB és PQ egyenesekkel és így a $Q \in S_k$ pontnak $q - 1$ érintője van, ami ellentmondás.

3. Ha a három egyenes egyike 2 pontot tartalmaz (P és Q), a másik kettő pedig 3 pontot (P, A_1, B_1 és P, A_2, B_2), akkor könnyen látható, hogy $Q = A_1A_2 \cap B_1B_2$ vagy $Q = A_1B_2 \cap A_2B_1$. Mindkét eset egy teljes négyoldal 6 csúcsát adja.

4. Ha mindhárom egyenes 3 pontot tartalmaz, az l_i egyenes pontjait jelöljük P, A_i, B_i-vel. Könnyen látható, hogy ekkor az $\{A_iA_j \cap B_iB_j, A_iB_j \cap A_jB_i\} = \{A_h, B, h\}$, $\{i, j, h\} = \{1, 2, 3\}$ esetén. Ilyen konfiguráció pedig egyedül a Fano-sík van.

Hogy a megadott példák valóban $(q - 2)$-szemiívek, azt könnyű ellenőrizni. □

A dolgozat további részében feltesszük, hogy $k < q - 2$. Az alábbi példát Kiss Györgytől hallottam, és ez volt az első példa amit megismertem:

1.2.3 Példa: Ha a Π_q síkon létezik Derargues-konfiguráció (2 db pontra nézve perspektív háromszög, és megfelelő oldalpárjaik metszéspontja, valamint a perspektivitási pont), akkor ez a 10 pont $(q - 5)$-szemiívet alkot.

1.2.4 Állítás: Legyen S_k egy k-szemiív a Π_q síkon. Ekkor $|S_k| \geq q - k + 2$.

1.2.4 élességét az alábbi példa igazolja.

1.2.5 Példa: A Π_q sík minden $(q-k+2)$-íve k-szemiív, ezért 1.1.7 miatt következik, hogy $PG(2, q)$-ban léteznek $q - k + 2$ pontból álló k-szemiívek.

1.2.6 Példa: Legyen l_1 és l_2 két egyenes a Π_q síkon. Töröljük a két egyenes metszéspontját és még k-k db pontotot mindkét egyenesről. A megmaradó $2q - 2k$ db pont k-szemiívet alkot.

1.2.7 Példa: Legyen $q = s^2 \geq 16$ és Π_s a Π_q sík Baer-részsíkja. Legyen l egy olyan egyenes, mely $s+1$ pontban metszi a Π_s részsíkot. Legyen $L \subseteq \{l\} \setminus \Pi_s$ tetszőleges k elemű ponthalmaz, $K \subseteq \Pi_s \setminus \{l\}$ pedig egy olyan k-elemű ponthalmaz, mely legfeljebb $s-2$ db kollineáris pontot tartalmaz. Ekkor $S_k := (\Pi_s \setminus (K \cup l)) \cup (l \setminus (L \cup \Pi_s))$ egy $2q - \sqrt{q} - 2k$ pontú k-szemiív. Ennek igazolása két részből áll:

Legyen $P \in l \cap S_k$, ekkor 1.1.10 miatt Π_s minden P-n átmenő egyenest metsz. l-en kívül semelyik másik egyenest sem metszheti egynél több pontban, ha ugyanis lenne egy ilyen $r \neq l$ egyenes, akkor erre $r \in \Pi_s$ és így $r \cap l = \{P\} \in \Pi_s$, ami ellentmond P választásának. Ebből már következik, hogy P érintői éppen a P-t a K-beli pontokkal összekötő k db egyenes.

Legyen $Q \in \Pi_s \cap S_k$, a Q-t a $\Pi_s \cap l$-beli pontokkal összekötő egyenesek $s+1$ db Π_s-beli pontot tartalmaznak. A K-ra tett feltételünk miatt minden ilyen egyenes tartalmaz legalább két db S_k-beli pontot, így ezek az egyenesek nem lehetnek Q-érintői. Tehát Q érintői a Q-t az L-beli pontokkal összekötő k db egyenes.

1.3. Felső becslés szemiívek elemszámára

1.3.1 Tétel: Legyen S_k egy k-szemiív a Π_q síkon, ekkor

$$|S_k| \leq 1 + \left\lfloor \frac{q\left(k - 1 + \sqrt{4kq - 3k^2 + 2k + 1}\right)}{2k} \right\rfloor.$$

Bizonyítás: Legyen $|S_k| = s$ és $\Pi_q \setminus S_k = \{P_1, P_2, \ldots, P_{q^2+q+1-s}\}$. Legyen továbbá t_i a P_i-n átmenő érintők száma. Számoljuk meg kétféleképpen azon (P_i, l_j) rendezett párokat, ahol l_j az S_t P_i-beli érintője, így az alábbi egyenlőséget kapjuk:

$$\sum t_i = ksq.$$

Azon (P_i, l_j, l_k) rendezett párok leszámlálásával, ahol l_j és l_k is az S_k P_i-beli érintője, kapjuk másik egyenlőségünket:

$$\sum t_i(t_i - 1) = k^2 s(s-1), \text{ tehát } \sum t_i^2 = ks(q + ks - k).$$

A számtani és négyzetes közepek közötti egyenlőtlenség szerint:

$$\left(\frac{\sum t_i}{q^2 + q + 1 - s}\right)^2 \leq \frac{\sum t_i^2}{q^2 + q + 1 - s}.$$

Ahová a kapott kifejezéseket beírva és átrendezve kapjuk, hogy

$$ks^2 + s(q - kq - 2k) - (q^2 + q + 1)(q - k) \leq 0.$$

Innen a másodfokú egyenlet megoldóképletéből kapjuk a bizonyítandó egyenlőtlenséget. □

A fenti tétel szemioválisok esetén Thas [19] és Hubaut [9] egymástól független eredménye, a felhasznált ötletet Kiss György mutatta meg nekem.

1.3.2 Példa: A q-adrendű Π_q sík m-edrendű Π_m részsíkja $q-m$-szemiív. Legyen ugyanis $P \in \Pi_m$, ekkor P-n át megy $m+1$ db szelő és $(q+1)-(m+1)$ db érintő, amivel állításunkat igazoltuk.

Előző tételünk élességét a Baer-részsíkok bizonyítják (lásd 1.1.8), melyek $(q-\sqrt{q})$ -szemiívet alkotnak és elemszámuk $q+\sqrt{q}+1$.

1.4. Szemiívek hosszú szelővel

A következő tétel Dover [6] szemioválisokra vonatkozó eredményének az általánosítása k-szemiívekre.

1.4.1 Tétel: Legyen S_k egy k-szemiív a Π_q síkon. Amennyiben $k < \lfloor \sqrt[3]{q} \rfloor$, akkor S_k-nak nincsenek $(q+1-k)$-szelői.

Bizonyítás: Tegyük fel, hogy l egy olyan egyenes, melyre $|S_k \cap l| = q+1-k$. Megmutatjuk, hogy ekkor $q < (k+1)^3$, és így $\sqrt[3]{q}-1 < k$, ami k egész volta miatt $k < \lfloor \sqrt[3]{q} \rfloor$ esetén ellentmondáshoz vezet.

Legyen $O = S_k \setminus l$, először megmutatjuk, hogy $q-k \leq |O| \leq q$. Mivel minden $P \in S_k \cap l$ ponton át kell mennie pontosan $q-k$ db olyan egyenesnek, mely tartalmaz O-beli pontot, ezért az alsó becslés nyilvánvaló. A felső becsléshez gondoljuk meg, hogy minden O-beli ponthoz tartozik S_k-nak k db érintője, ez összesen $|O| \cdot k$ db érintő. Ezek az érintők l-et csak $l \setminus S$-ben metszhetik, így számuk legfeljebb $k \cdot q$, amiből a felső becslés következik.

Jelöljük $\mathcal{M}$-mel a sík azon egyeneseinek halmazát, melyek legalább két O-beli pontot tartalmaznak. Legyem $m \in \mathcal{M}$, ekkor $m \cap l \in S_k$, ellenkező esetben $m \cap O$ pontjainak legfeljebb $k-1$ érintője lenne.

1. eset: $|O| = q-k$. $k < q-2$ miatt létezik $P, Q \in O$, legyen az általuk meghatározott egyenes m. Ekkor az előző észrevételünk miatt $m \cap l \in S_k$, ugyanakkor ennek a metszéspontnak legalább $k+1$ érintője van, ami ellentmondás.

2. eset: $|O| = q-k+t$, ahol $t \in \{1, 2, \ldots, k\}$. Ekkor az alábbi észrevételeket tehetjük:

Minden $P \in l \cap S_k$-beli pontból csak $1, 2, \ldots, t+1$-szelők mehetnek O-hoz, ellenkező esetben P-nek k-nál kevesebb érintője lenne.

Legyen c_R az $R \in O$ pontból induló $\mathcal{M}$-beli egyenesek száma.
Ekkor $|O| = q-k+t \leq c_R \cdot t + 1$, amiből következik, hogy

$$\frac{q-k+t-1}{t} \leq c_R.$$

Előző két észrevételünk miatt:

$$\frac{(q-k+t-1)(q-k+t)}{t(t+1)} \leq \sum_{R \in O} c_R.$$

Mivel az $\mathcal{M}$-beli egyenesek S_k-ban metszik l-t, ezért a skatulya-elv miatt lesz egy olyan $D \in S_k \cap l$ pont, melyre:

$$\frac{(q-k+t-1)(q-k+t)}{t(t+1)(q-k+1)} \leq c_D.$$

Jelöjük t_D-vel a D-ből O-hoz húzható érintők számát. Ekkor $2c_D + t_D \leq |O| = q - k + t$ és $c_D + t_D = q - k$, hiszen S_k D-beli érintőinek a száma k. Ebből $c_D \leq t$ következik, amiből előző egyenlőtlenségünket felhasználva ezt kapjuk:

$$\frac{(q-k+t-1)(q-k+t)}{t(t+1)(q-k+1)} \leq t$$

Az egyenlőtlenséget átrendezve kapjuk, hogy:

$$\left(\frac{q-k-1}{t}+1\right)\left(\frac{q-k-1}{t+1}+1\right) \leq t\,(q+1-k)\,.$$

$t < q-1$ miatt t-t növelve a bal oldal csökken, míg a jobb oldal nő. Így az egyenlőtlenség a $t = k$ esetben is teljesül, és ekkor az alábbihoz vezet:

$$q^2 - q(k^3+k^2+1) + k^4 - k^2 \leq 0,$$

amiből

$$q \leq \frac{1}{2} \cdot (k^3+k^2+1+\sqrt{k^6+2k^5-3k^4+2k^3+6k^2+1}) < k^3+k^2+1 < (k+1)^3.$$

□

A továbbiakban azokat a k-szemiíveket vizsgáljuk, melyeknek van $(q-k)$-szelője. Szemioválisok esetén szintén Dover [6] vizsgálta a kérdést.

1.4.2 Állítás: Ha a Π_q sík egy S_k k-szemiívének van $(q-k)$-szelője, akkor

$$2q - 2k \leq |S_k| \leq 2q - k + \frac{q}{k}.$$

Bizonyítás: Legyen l olyan egyenes, amire $|l \cap S_k| = q-k$ és legyen $L = l \setminus S_k$, $O = S_k \setminus l$. Először a felső becslést igazoljuk:

$|L| = k+1$ és L minden pontjából legfeljebb q db, így L pontjaibók összesen legfeljebb $(k+1)q$ db érintő húzható az O-beli pontokhoz. Az O-beli pontok mindegyikén át k db érintő megy, melyek midnegyike L-ben metszi l-t, így az alábbi becslés adódik: $|O|k \leq (k+1)q$.

Másrészről $q-k \leq |O|$, ellenkező esetben az $S_k \cap l$-beli pontoknak legalább $k+1$ érintőjük lenne. Így $|O|$-ra az alábbi becsléseket nyertük:

$$q - k \leq |O| \leq \frac{(k+1)q}{k}.$$

Az egyenlőtlenséghez $|S_k \cap l| = q-k$-t hozzáadva a bizonyítandó állítást kapjuk. □

Az alsó becslés élessége esetén az alábbi karakterizációt tehetjük:

1.4.3 Állítás: Ha a Π_q sík egy S_k k-szemiívének van $(q-k)$-szelője és $|S_k| = 2q-2k$, akkor S_k az 1.2.6 példában bemutatott konstrukció.

Bizonyítás: Az előző bizonyításból vegyük át az l, L és O jelöléseket, $k < q-2$ miatt létezik O-nak három tetszőleges pontja, legyenek ezek A, B, C. Az AB, AC, BC egyenesek csak L-ben metszhetik l-t, hiszen a metszéspontból $|O| = q-k$ miatt legalább $k+1$ érintője lenne S_k-nak. Ha ez a 3 egyenes 3 különböző pontban metszené L-t, akkor az A, B, C pontok mindegyikének legfeljebb $k-1$ érintője lenne. Tehát kell, hogy legyen közöttük két egyenes, mely ugyanabban az L-beli pontban metszi egymást, ám ekkor A, B és C egy egyenesre esik. Mivel ez 3 tetszőlegesen választott pont volt, így minden O-beli pont egy egyenesre esik, mely egy S-en kívüli pontban metszi l-t.

□

1.5. Szemiívek 2 db hosszú szelővel

A továbbiakban azokat a k-szemiíveket vizsgáljuk, melyeknek létezik 2 db hosszú szelője. Az alábbi lemma bizonyítását témavezetőm ötlete tette ilyen egyszerűvé, előtte az 1.5.4 lemma bizonyításához hasonlóan, bonyolultabban bizonyítottam kicsivel gyengébb állítást.

1.5.1 Lemma: Ha a Π_q sík egy S_k k-szemiívének van egy $(q-n)$-szelője és egy $(q-m)$-szelője, valamint

$$q > k + 1 + \frac{(n+1)(m+1)}{k},$$

akkor ez a két szelő S_k-n kívül metszi egymást.

Bizonyítás: Legyen $|l_1 \cap S_k| = q - n$ és $|l_2 \cap S_k| = q - m$ és indirekt tegyük fel, hogy $l_1 \cap l_2 = P \in S_k$. Legyen $O = S_k \setminus (l_1 \cup l_2)$, ekkor $P \in S_k$ miatt $q - k - 1 \leq |O|$. Az O-beli pontokon át összesen $|O|k$ db érintője megy S_k-nak. Mivel ezek mindegyike S_k-n kívül metszi a két hosszú szelőt, ezért számuk $(n+1)(m+1)$-gyel felülről becsülhető. Így az alábbi egyenlőtlenséget kapjuk:

$$q - k - 1 \leq |O| \leq \frac{(m+1)(n+1)}{k},$$

amiből

$$q \leq k + 1 + \frac{(m+1)(n+1)}{k}.$$

Ez pedig ellentmond a q-ra vonatkozó feltételünknek. □

1.5.2 Állítás: Ha a Π_q sík egy S_k k-szemiívének két db $(q-k)$-szelője van, és $q > 2k + 3 + \frac{1}{k}$, akkor ezek a hosszú szelők S_k-n kívül metszik egymást.

A következő tétel karakterizálja a 2 db $(q-2)$-szelővel rendelkező 2-szemiíveket 8-nál nagyobb rendű síkokon.

1.5.3 Tétel: Ha a Π_q sík egy S_2 2-szemiívének van 2 db $(q-2)$-szelője és $q \geq 8$, akkor a hosszú szelők S_2-n kívül metszik egymást és az alábbiak egyike teljesül:

1. S_2 az 1.2.6 példában szereplő konstrukció,
2. $|S_2| = 2q-2$, a hosszú szelőkön kívül eső 2 db S_2-beli pont, és a szelőegyenesek S_2-ből kimaradó 5 pontja egy Fano-részsíkot alkot.

Bizonyítás: Legyen a két hosszú szelő l_1 és l_2, valamint $P = l_1 \cap l_2$, ekkor az előző állítás miatt $P \notin S_2$. Legyen továbbá $\{l_1\} \setminus S_2 = \{P, Q_1, R_1\}$ és $\{l_2\} \setminus S_2 = \{P, Q_2, R_2\}$, valamint $O = S_2 \setminus (l_1 \cup l_2)$. Amennyiben $|O| = 0$, akkor az első eset teljesül.

Tegyük fel, hogy $|O| > 0$ és legyen $M_1 = Q_1Q_1 \cap R_1R_2$, $M_2 = Q_1R_2 \cap Q_2R_1$, valamint $M \in O$ egy tetszőleges pont. Ekkor $M \in \{M_1, M_2\}$, máskülönben az MR_1, MR_2, MQ_1, MQ_2 egyenesek közül lenne olyan, mely l_1 és l_2 közül legalább egyet S_2-ben metsz, de akkor ennek a metszéspontnak legfeljebb egy érintője lenne. Ezzel azt is beláttuk, hogy $|O| \leq 2$.

Ha $O = \{M\}$, akkor M-nek PM is érintője, tehát 3 db érintője lenne, ami nem lehetséges. Azt kaptuk, hogy $O = \{M_1, M_2\}$, ekkor M_1, M_2 és P egy egyenesre kell, hogy essen, máskülönben mindkét O-beli pontnak 3 db érintője lenne.

Ekkor $|S| = 2q - 2$ és $P, Q_1, R_1, Q_2, R_2, M_1, M_2$ egy Fano-síkot alkot. □

1.5.4 Lemma: Legyen S_k egy k-szemiív, a Π_q síkon és legyen $k \geq 3$, l_1 és l_2 pedig két egyenes, melyekre

$$|S_k \cap l_1| = q - n,$$

$$|S_k \cap l_2| = q - m,$$

valamint $l_1 \cap l_2 \notin S_k$. Tegyük fel továbbá, hogy $m \geq n \geq k$ és $m \geq k + 1 + \frac{2}{k-2}$. Megmutatjuk, hogy ez csak akkor lehetséges, ha $q \leq mn$.

Bizonyítás: Legyen $l_1 \cap l_2 = M$, $l_1 \setminus S_k$ pontjai: $M, P_1, P_2, \ldots P_n$ és $l_2 \setminus S_k$ pontjai: $M, Q_1, Q_2, \ldots Q_m$. A $\{P_1, P_2, \ldots, P_n\}$ pontokat $\binom{m}{k}$ db diszjunkt halmazba osztjuk a következő módon:

Legyen $I \subset \{1, 2 \ldots, m\}$ és $|I| = k$. $P \in H_I$ pontosan akkor, ha P érintői a $\{Q_i \mid i \in I\}$ pontokban metszik l_2-t.

Minden $l \in \{1, 2, \ldots, m\}$ esetén legyen $T_l = \cup_{l \notin I} H_I$. Ekkor minden $P_i \in T_l$ pont esetén a P_iQ_l egyenes tartalmaz P_i-n kívül legalább még egy S_k-beli pontot, hiszen, T_l definíciója miatt, nem érintője a P_i-nek. Minden $P_i \in T_l$ esetén válasszunk hát egy ilyen pontot, és nevezzük el O_{il}-nek. Ezek az O_{il} pontok különböző $P_i \in T_l$ pontok esetén különbözők, hiszen különböző Q_l-en átmenő egyenesen vannak. Vezessük be az $O_l = \{O_{il} \mid P_i \in T_l\}$ jelölést, ekkor $|T_l| = |O_l|$ és a H_I halmazok diszjunk volta miatt:

$$\sum_{l \notin I} |H_I| = |T_l| = |O_l|. \tag{1.1}$$

Minden O_l-beli pontnak lehet egy érintője, mely az M-en megy át, és van legalább $k - 1$ db érintője, mely P_aQ_b alakú, ahol $a \in \{1, 2, \ldots n\}$ és $b \in \{1, 2, \ldots, m\} \setminus \{l\}$. Az ilyen érintők száma legfeljebb $(m - 1)n$, így az alábbi becslést kapjuk:

$$|O_l|(k - 1) \leq (m - 1)n \tag{1.2}$$

1.1 és 1.2 miatt kapjuk, hogy:

$$(k - 1) \sum_{l \notin I} |H_I| \leq (m - 1)n$$

Végezzük el a fenti becslést minden $l \in \{1, 2, \ldots m\}$ esetén, így ezt kapjuk:

$$(k - 1) \sum_{l=1}^{m} \sum_{l \notin I} |H_I| \leq m(m - 1)n.$$

Most a bal oldalon minden $|H_I|$-t $m-k$-szor számoltunk (valahányszor $l \notin I$). Tehát egyenlőtlenségünk így is írható:

$$(m - k)(k - 1) \sum_{I} |H_I| \leq m(m - 1)n.$$

Ugyanakkor minden $S_k \cap l_1$-beli pont beletartozik a diszjunk H_I halmazok valamelyikébe, tehát $\sum_I |H_I| = |(S_k \cap l_1)| = q - n$. Ez alapján egyenlőtlenségünket így írhatjuk át:

$$(m-k)(k-1)(q-n) \leq m(m-1)n,$$

ahonnan

$$q \leq n + \frac{m(m-1)n}{(m-k)(k-1)}. \tag{1.3}$$

Már csak azt kell belátnunk, hogy:

$$n + \frac{m(m-1)n}{(m-k)(k-1)} \leq mn.$$

Mindkét oldalból n-et kivonva, majd $n(m-1)$-gyel egyszerűsítve ezt kapjuk:

$$\frac{m}{(m-k)(k-1)} \leq 1.$$

Ebből rendezés után:

$$0 \leq m(k-2) - k^2 + k,$$
$$\frac{k^2-k}{k-2} \leq m,$$

ahol a bal oldal $k + 1 + \frac{2}{k-2}$-vel egyenlő, így a feltételünk miatt készen vagyunk. □

1.5.5 Definíció: Az alábbi, 1.3 egyenlőtlenségben szereplő kifejezésre vezessünk be egy jelölést:

$$F_k(m,n) := n + \frac{m(m-1)n}{(m-k)(k-1)}$$

Ekkor egyszerű függvényvisgálattal nem nehéz belátni, hogy $3 \leq k$ esetén:

$$F_k(k+1, k+1) \leq \frac{(k+6)^2}{2} \tag{1.4}$$

$$F_k(k+2, k+2) \leq \frac{(k+6)^2}{2} \tag{1.5}$$

1.5.6 Tétel: A Π_q síkon $3 \leq k < \sqrt{2q} - 6$ esetén nincsenek olyan k-szemiívek, melyeknek két db $q - t$ szelőjük van, valahányszor $k < t < \sqrt{q}$.

Bizonyítás: Tegyük fel, hogy létezik a megadott tulajdonságokkal szemiív. Először 1.5.1 lemmát szeretnénk használni annak belátására, hogy a szelők S_k-n kívül metszik egymást. Ehhez az kell, hogy:

$$k + 1 + \frac{(t+1)^2}{k} < q.$$

A k-ra és t-re tett feltételeinkből ez következik, hiszen:

$$k + 1 + \frac{(t+1)^2}{k} < \sqrt{2q} - 5 + \frac{(\sqrt{q}+1)^2}{3} < q,$$

könnyen ellenőrizhető. Ezek szerint az 1.5.4 lemma használható minden $t \geq k+1+\frac{2}{k-2}$ esetben, és ebből $q \leq t^2 < q$ következik, ami ellentmondás.

Hogy ha $t < k+1+\frac{2}{k-2}$, akkor ez $k < t$ miatt csak úgy lehet, hogy $t = k+1$ vagy $t = k+2$. Az 1.3 egyenlőtlenséget ilyenkor is használhatjuk, hiszen a lemma bizonyításában csak ez után használtuk a nem teljesülő feltételünket. Így 1.3 tetszőleges $m \geq n$, $m > k > 1$ egészek esetén igaz. Ebből azt kapjuk, hogy $q \leq F_k(k+1, k+1)$ és $q \leq F_k(k+2, k+2)$.

Ennek viszont ellentmond 1.4 és 1.5 miatt a k-ra tett feltételünk, mert abból $(k+6)^2/2 < q$ következik. □

1.5.7 Megjegyzés: Előző tételünk érdekessége, hogy 2 db $(q-k)$-szelővel, vagy 2 db $(q-\sqrt{q})$-szelővel rendelkező szemiívekre bőségesen vannak példák, melyeket a következő fejezetben bemutatunk. A teljesség kedvéért a 2-szemiíveknél, tehát a $k = 2$ esetben is megadunk az 1.5.4 lemmához hasonló állítást.

1.5.8 Állítás: Legyen S_2 egy 2-szemiív a Π_q síkon és legyen l_1, l_2 két egyenes, melyekre $|S_2 \cap l_1| = q-n$ és $|S_2 \cap l_2| = q-m$, valamint $l_1 \cap l_2 \notin S$. Legyen $m \geq n \geq 2$ és $m \geq 3$. Megmutatjuk, hogy ez csak akkor lehetséges, ha $q \leq mn+m+n+6$.

Bizonyítás: A bizonyítást a $k \geq 3$ esetben látottakhoz hasonlóan végezve kapjuk, hogy:

$$q \leq n\frac{m^2-2}{m-2},$$

ahol a jobb oldal $F_2(m,n)$. Már csak azt kell belátnunk, hogy:

$$n\frac{m^2-2}{m-2} \leq mn+m+n+6,$$

átszorzás és rendezés után:

$$mn+12 \leq m^2+4m.$$

Ez pedig $m \geq n$ és $m \geq 3$ miatt teljesül. □

2. fejezet

Szemiívek három egyenesen

2.1. Szemiívek két egyenesen

Ebben a fejezetben osztályozzuk az k-szemiíveket aszerint, hogy legkevesebb hány egyenessel lehet őket lefedni.

2.1.1 Állítás: A Π_q-sík egy egyenessel lefedhető k-szemiívei 1.2.2 szerint kétfélék lehetnek:

1. S_k egyetlen pont, ekkor $k = q + 1$,
2. S_k egy egyenes egynél több pontja, ekkor $k = q$.

2.1.2 Állítás: A Π_q sík azon S_k k-szemiívei, melyek nem fedhetők le egy egyenessel, de lefedhetők két egyenessel, két csoportba oszthatók. Legyen a két fedő egyenes l_1 és l_2, metszéspontjuk pedig P:

1. S_k három db nem kollineáris pontból áll, ekkor $k = q - 1$,
2. S_k az 1.2.6 példában szereplő konstrukció.

Bizonyítás: Amennyiben $P \in S_k$, úgy P-nek pontosan $q - 1$ érintője van így $k = q - 1$, tehát 1.2.2 miatt készen vagyunk.

Amennyiben $P \notin S_k$, úgy feltehető, hogy mindkét egyenesen van legalább 2 db S_k-beli pont, ellenkező esetben meg tudunk adni két olyan S_k-t fedő egyenest, melyek metszéspontja S_k-ban van, ezt az esetet pedig az előbb vizsgáltuk. Mivel mindkét egyenes tartalmaz legalább 2 pontot, ezért az $l_i \cap S_k$-beli pontok érintőinek száma $i \in \{1, 2\}$ esetén: $k = |l_i \backslash S_k| - 1$. Ebből pedig következik, hogy S_k mindkét egyenesről $q - k$ pontot tartalmaz és így valóban az 1.2.6 példában szereplő konstrukció. $\square$

2.2. Szemiívek három, egy ponton átmenő egyenesen

Ebben a fejezetben már csak olyan szemiívekkel foglalkozunk, melyek három kongruens egyenessel lefedhetők, de kettővel nem.

2.2.1 Állítás: Amennyiben az S_k k-szemiívet fedő három egy ponton átmenő egyenes P metszéspontjára $P \in S_k$ teljesül, akkor S_k kétféle lehet: egy teljes négyoldal 6 csúcsa, illetve a Fano-sík. Mindkét esetben $k = q - 2$.

BIZONYÍTÁS: Mindhárom egyenes tartalmaz P-n kívül is pontot S_k-ból, különben már két fedőegyenes is elég lenne. Ekkor a P-beli érintők száma $q-2$, tehát $k = q-2$ és így 1.2.2 miatt csak 3 lehetőség jöhet szóba. Ezek közül a 4 általános helyzetű pont már 2 egyenessel is lefedhető, a másik két példa viszont megfelelő. □

Legyen $S_k \subset \{l_1 \cup l_2 \cup l_3\}$, $P = l_1 \cap l_2 \cap l_3$ és a $P \notin S_k$ eset vizsgálatához vezessük be az alábbi jelöléseket:

$$|S_k \cap l_1| = q - x,$$
$$|S_k \cap l_2| = q - y,$$
$$|S_k \cap l_3| = q - z.$$

Jegyezzük meg, hogy x, y, z egyike sem lehet q, hiszen ekkor S_k-t már 2 egyenes lefedné. Ugyanez a helyzet, ha x, y, z közül legalább kettőnek az értéke $q - 1$. A folytatáshoz szükségünk lesz az alábbi lemmákra.

2.2.2 Lemma: Amennyiben az előbb definiált x, y, z értékek egyike $q - 1$, a másik kettő pedig ennél kisebb (ezt az előző észrevétel miatt feltehetjük), úgy $|S_k| = 5$, S_k általános helyzetű és $k = q - 3$.

BIZONYÍTÁS: Az általánosság megszorítása nélkül feltehetjük, hogy $z = q-1$. Ekkor az S_k-t nem metsző, P-t elkerülő egyenesek számát kétféleképpen megszámolva az alábbi egyenlőséget kapjuk:

$$(q-1)x - (q-y)k = (q-1)y - (q-x)k.$$

Ezt átrendezve azt kapjuk, hogy $(q-1)(x-y) = k(x-y)$.

Amennyiben $x \neq y$, abből $q - 1 = k$ következne, ami nem lehetséges, hiszen $y \leq q-2$ miatt egy $l_1 \cap S_k$-beli pontnak legfeljebb $q-2$ érintője van. Beláttuk tehát, hogy $x = y$.

Legyen $S_k \cap l_3 = C$ és tegyük fel, hogy C-n át van olyan e egyenes mely l_1-et és l_2-t is S_k-ban metszi. Legyen ez a két metszéspont A és B. Ekkor mind A-nak, mind B-nek x db érintője van, tehát C-nek is x db érintője kell, hogy legyen. Mivel CP a C-nek érintője, ezért lesz pontosan egy olyan $A' \in l_1 \setminus (S_k \cup P)$, melyre $A'C$ nem érintő, vagyis $B' = A'C \cap l_2 \in S_k$. Ekkor azonban B'-nek legfeljebb $x-1$ érintője van, ami ellentmondás. Azt kaptuk tehát, hogy nincsen ilyen e egyenes, amiből $k = x-1$ következik, mert bármely $(l_1 \cup l_2) \cap S_k$-beli pontnak ennyi érintője van.

A C pont érintőinek a száma $x - (q-x) + 1$, hiszen C-t az $l_2 \cap S_k$-beli pontokkal összekötve l_1-et $l_1 \setminus (S_k \cup P)$-ben metsző pontokat kapunk, így CP-n kívül $|l_1 \setminus (S_k \cup P)| - |l_2 \cap S_k|$ db érintője lesz.

A $2x - q + 1 = x - 1$ egyenletből kapjuk, hogy $x = q - 2$, amiből $|S_k| = 5$ már következik. Az általános helyzetűség, és hogy $(q-3)$-szemiívet kaptunk, könnyen látható. □

2.2.3 Tétel: Ismét a korábbi jelöléseket használva megmutatjuk, hogy a fennmaradó $x, y, z \leq q - 2$ esetben az alábbi két állítás egyike teljesül:

1. $x = y = z$,
2. x, y, z közül kettő egyenlő k-val.

Amennyiben 2. teljesül úgy a harmadik (k-tól különböző) érték $q-k$ és $q-2$ közé esik.

BIZONYÍTÁS:

Ismét az S_k-t nem metsző, P-t elkerülő egyenesek számából kapjuk az alábbi egyenlőségeket:

$$xz-(q-y)k = yz-(q-x)k = xy-(q-z)k.$$

Ebből átrendezéssel nyerjük, hogy:

$$y(x-z) = k(x-z),$$
$$x(z-y) = k(z-y),$$
$$z(y-x) = k(y-x),$$

amiből a lemma első fele már következik.

A második rész igazolásához az általánosság megszorítása nélkül feltehetjük, hogy $x=y=k$. $z \leq q-2$ feltétel volt, az alsó korlát megmutatásához pedig válasszunk egy tetszőleges P-től különböző $Q \in l_1 \setminus S_k$ pontot. Ekkor minden $S_k \cap l_2$-beli, illetve minden $S_k \cap l_3$-beli pontból megy érintő Q-n át. A Q-n átmenő érintők száma tehát egyrészt $(q-k)+(q-z)$, másrészt legfeljebb q, ahonnan $q-k \leq z$ következik. □

2.2.4 Megjegyzés: Szemioválisok esetén a fenti bizonyítás [3]-ban is megtalálható. $q>3$ esetén csak 1. típusú szemioválisok léteznek.

2.2.5 Tétel: Ha a Π_q, p-karakterisztikájú síkban egy S_k halmaz lefedhető három kongruens egyenessel (melyek P metszéspontját nem tartalmazza S_k) és a korábbi definíciókat használva: $x=y=k$, $q-k \leq z \leq q-2$, akkor $p|k$.

BIZONYÍTÁS: Legyen $Y, Z \in l_3 \cap S_k$, $P_0 \in l_2 \setminus S_k$ és $Q_o \in l_1 \setminus S_k$ úgy, hogy $Q_0P_0 \cap l_3 = Z$. Nézzük most az alábbi vetítési eljárást, mely megtalálható Kárteszi Ferenc, Bevezetés a véges geometriákba című könyvében [10, p. 147]:

P_0-t Y-ból l_1-re vetítve kapjuk Q_1-et, Q_1-et Z-ből l_2-re vetítve P_1-et, P_1-et Y-ból l_1-re vetítve Q_2-t stb. Mivel $Y, Z \in S_k$ és $x=y=k$ így minden i-re $P_i, Q_i \notin S_k$. Mivel a sík karakterisztikája p, így az eljárás p-lépésben záródni fog. Ekkor új $Q_0, P_0 \notin S_k$ pontokat választva folytassuk az eljárást. Amikor az utolsó záródás után már nem tudjuk újrakezdeni a műveletet, akkor P-n kívül minden $l_1 \setminus S_k$ és $l_2 \setminus S_k$-beli pontot sorra vettünk, így ezek száma valóban p többszöröse. □

Az alábbi tétellel karakterizáljuk a páratlan rendű $GF(2,q)$-sík azon k-szemiíveit, melyek 2.2.3 2. esetébe tartoznak. Az 1.1.3 állításban leírtakat követve feltehető, hogy l_1, l_2, l_3 az $X_1=-X_3$, $X_1=0$ és $X_1=X_3$ egyenesek, melyek tehát a közös $(0,1,0)$ pontban metszik egymást. Az is feltehető, hogy $x=z=k$ és $q-k \leq y \leq q-2$. A feltételeknek eleget tevő S_k k-szemioválisokkal kapcsolatban legyen $L_i = S_k \cap l_i$ $(i=1,2,3)$, és vezessük be az alábbi jelöléseket:

$$A = \{a \in GF(q) : (-1,a,1) \notin L_1\}$$
$$B = \{b \in GF(q) : (0,b,2) \in L_2\}$$

$$C = \{c \in GF(q) : (1, c, 1) \notin L_3\}$$

Mint azt az 1.1.3 állításban megmutattuk, az $(-1, a, 1)$, $(0, b, 2)$ és $(1, c, 1)$ pontok pontosan akkor kollineárisak, ha $a + c = b$.

2.2.6 Tétel: (Exact inverse sumset theorem) Legyen A és B a Z Abel csoport véges, nemüres részhalmazai, ekkor az alábbiak ekvivalensek:

- $|A + B| = |A|$
- $|A - B| = |A|$
- B a $stab(A)$ egy mellékosztályának részhalmaza, A pedig $stab(A)$ mellékosztályainak uniója

A tétel bizonyítása megtalálható Tao és Vu könyvében [18, p. 71].

2.2.7 Tétel: Páratlan p esetén $PG(2, p^n)$ összes olyan k-szemiíve esetén, mely a 2.2.3 tétel 2. esetébe tartozik, teljesül hogy:

A szemiív által meghatározott A és C halmazok előállnak $GF(p^n)^+$ egy G részcsoportja mellékosztályainak uniójaként, B pedig a G egy mellékosztályának részhalmaza. Továbbá ha ϕ jelöli a természetes homomorfizmust $GF(p^n)^+$-ból a $GF(p^n)^+/G$ faktorcsoportba, ekkor $\phi(C) = \phi(B) - \phi(A)$, ahol $|\phi(B)| = 1$.

Ha az előző bekezdésben megfogalmazott állítások teljesülnek, akkor az A, B, C által meghatározott ponthalmaz egy $|G||\phi(C)|$-szemiív, melynek elemszáma $2p^n - 2|G||\phi(C)| + |B|$.

Bizonyítás: Mivel minden S_k-beli pontnak, így az L_2-beli pontoknak is k db érintője van és $|A| = |C| = k$, ezért $B - A \subseteq C$ és $B - C \subseteq A$, tehát $|B - A| \leq |C|$ és $|B - C| \leq |A|$. Felhasználva, hogy $|C| = |A| \leq |B - A|$ és $|A| = |C| \leq |B - C|$, kapjuk hogy az előbbi egyenlőtlenségekben egyenlősség áll, így $|B - A| = |A|$ és $|B - C| = |C|$. Előbbi a 2.2.6 tétel miatt ekvivalens azzal, hogy $|A + B| = |A|$ és $|C + B| = |C|$.

Szintén ebből a tételből kapjuk, hogy B a $stab(A)$ egy mellékosztályának részhalmaza, A pedig $stab(A)$ mellékosztályainak uniója. A tétel állításában szereplő G-t válasszuk $stab(A)$-nak, ezzel állításunk első felét beláttuk.

$|B - A| = |C|$ és $B - A \subseteq C$ miatt $B - A = C$, így ezért készen vagyunk $\phi(C) = \phi(B) - \phi(A)$ szükségessével is.

A feltételeinkből $B - A = C$ és $B - C = A$ is következik, amiből világos, hogy az L_2-beli pontoknak pontosan k db érintőjük van. Vegyünk most egy tetszőleges $Q \in L_1$ pontot, koordinátái legyenek: $(-1, q, 1)$, ahol tehát $q \notin A$. Azt kell megmutatnunk, hogy $(q + C) \cap B = \emptyset$. Indirekt, ha lenne olyan $b_1 \in B$, $c_1 \in C$, melyekre $q + c_1 = b_1$, akkor $q \in B - C$, ami ellentmondás, hiszen $q \notin A$. Hasonlóan belátható, hogy az L_3-beli pontoknak is pontosan k db érintője van. □

2.2.8 Példa: Előző tételünkből következik, hogy $PG(2, q)$-ban $q = p^n$, q páratlan esetben léteznek $2q - 2k + t$ elemszámú k-szemiívek, minden olyan k és t értékre, ahol $p|k$ és $2 \leq t \leq p^{\lfloor \log_p k \rfloor}$.

2.2.9 Példa: Amennyiben a Π_q (nem-feltétlenül Desargues) sík tartalmaz egy Π_k részsíkot, akkor válasszuk az l_1, l_2, l_3 egyeneseket úgy, hogy ezek mindegyike $k + 1$

pontban messe Π_k-t, egymást pedig egy $P \in \Pi_k$ pontban. Legyen $Z \subseteq (l_3 \cap \Pi_k) \setminus \{P\}$ tetszőleges részhalmaz az alábbi feltétellel: $2 \leq |Z| \leq k$.

$$S_k := (l_1 \setminus \Pi_k) \cup (l_2 \setminus \Pi_k) \cup Z$$

Megmutatjuk, hogy S_k k-szemiív: legyen $\{i, j\} = \{1, 2\}$, ekkor $Q \in l_i \setminus \Pi_k$-nak pontosan k db érintője van, melyek a $(\Pi_k \cap l_j) \setminus \{P\}$ pontokban metszik l_j-t ($j \neq i$). $R \in l_3 \cap S_k$-nak is pontosan ennyi érintője van, hiszen az érintői pont azok az l_3-on kívüli egyenesek lesznek, melyek l_1-et illetve l_2-t Π_k-ban metszik, ilyenből pedig pontosan k db van.

Az így kapott S_k halmazok elemszáma $2q-2k+2$ és $2q-k$ között minden értéket felvehet.

2.2.10 Példa: Mivel létezik olyan 9-rendű (nem Desargues) sík, melynek van 2-rendű részsíkja [10, p. 28], így ebben a síkban megadhatunk az előző példánknak megfelelő 16, 17, 18 elemszámú 2-szemiíveket. Ez az első példánk olyan szemiívre, mely csak nem Desargues síkon létezik.

Az 1. esetbe tartozó k-szemiívekre a "További konstrukciók" című fejezetben mutatunk példákat. A későbbi fejezetekben szükségünk lesz az alábbi lemmára:

2.2.11 Lemma: Amennyiben a Π_q sík S_k szemioválisát tartalmazza három egy ponton átmenő egyenes, melyek mindegyike t db S_k-beli pontot tartalmaz, akkor

$$t \geq \sqrt{qk + \frac{k^2}{4}} - \frac{k}{2}.$$

Bizonyítás: Legyen a három fedőegyenes l_1, l_2, l_3, és a közös metszéspontjuk M. Ekkor bármely $l_1 \cap S_k$-beli pontnak van k db érintője, mely az $l_2 \setminus M$ és $l_3 \setminus M$ egyenesek mindegyikét csak t db pontban metszheti. Így az alábbi becslést nyerjük:

$$(q - t)k \leq t^2,$$

ebből a lemma állítása következik. □

A becslés szemioválisok esetén [3]-ban megtalálható.

2.3. Szemiívek projektív háromszögben

A szemioválisok között több olyan példa is van, amit egy projektív háromszög oldalai tartalmaznak (lásd [13]). A következőkben ugyanezzel a tulajdonsággal bíró szemiíveket fogunk vizsgálni.

2.3.1 Állítás: A Π_q síkon $k < \frac{q-1}{2}$ esetben nincs olyan k-szemiív, melyet tartalmaz az l_1, l_2, l_3 nem egyponton átmenő egyenesek uniója és S_k tartalmazza ezek metszéspontjait.

Bizonyítás: Világos, hogy ekkor l_1, l_2, l_3 mindegyikén pontosan k pont hiányzik S_k-ból. Legyen $O = S_k \setminus l_3$, megmutatjuk, hogy $|O| \leq q$. Minden O-beli ponthoz tartozik S_k-nak k db érintője, ez összesen $|O| \cdot k$ db érintő. Ezek az érintők l-t csak

$l \setminus S_k$-ban metszhetik, így számuk legfeljebb $k \cdot q$, amiből $|O| \leq q$ következik. Így azt nyertük, hogy:

$$|O| = |(l_2 \cup l_3) \setminus l_1| = 2q - 2k - 1 \leq q,$$

amiből $q \leq 2k + 1$ és így az állítás következik. □

Előbbi korlátunk élességét 4.1.7 példában mutatjuk meg.

2.3.2 Állítás: Ha a Π_q sík S_k k-szemiívét tartalmazza az l_1, l_2, l_3 nem egy ponton átmenő egyenesek uniója, és S_k ezek metszéspontjai közül 2-t tartalmaz, akkor S_k a 1.2.6 példában szereplő konstrukció, és így már két egyenes tartalmazza.

Bizonyítás: Legyen a két tartalmazott csúcs $l_1 \cap l_3$ és $l_2 \cap l_3$, ekkor l_1 és l_2 mindegyike $(q-k)$-szelő. Legyen $x = q - 1 - |l_3 \cap S_k|$ és jelöljük M-mel a háromszög három csúcsának a halmazát. Az $(l_1 \cup l_3) \setminus M$-ponthalmazt S_k-n kívül metsző egyeneseket kétféleképpen leszámolva kapjuk az alábbi egyenlőséget:

$$kx = k^2 - (k-1)(q-1-x) + (q-1-k)k,$$

amit rendezve $x = q - 1$ adódik. Ez pedig azt jelenti, hogy l_3 csak két S_k-beli pontot tartalmaz. □

2.3.3 Tétel: Ha a Π_q sík S_k k-szemiívét tartalmazza az l_1, l_2, l_3 nem egy ponton átmenő egyenesek uniója, és S_k ezek metszéspontjai közül 1-et tartalmaz, akkor, a háromszög három oldala egy $(q-1-k)$-szelő és két $(q-t)$-szelő, ahol $t = k - \frac{1}{2} + \sqrt{q - k - \frac{3}{4}}$. Megmutatjuk, hogy rögzített $k \geq 2$ esetén csak véges sok k-szemiív van, mely ebbe a típusba tartozik, és ilyenek csak akkor létezhetnek, ha $4q - 4k - 3$ négyzetszám.

Bizonyítás: Feltehetjük, hogy $l_1 \cap l_2 \in S_k$, ekkor $|l_3 \cap S_k| = q - 1 - k$. Legyen $x = q - |S_k \cap l_1|$ és $y = q - |S_k \cap l_2|$.

Jelöljük M-mel a háromszög három csúcsának a halmazát. Az $(l_1 \cup l_3) \setminus M$-ponthalmazt S_k-n kívül metsző egyeneseket kétféleképpen leszámolva kapjuk az alábbi egyenlőséget:

$$kx = yk - (k-1)(q-1-x) + (q-1-y)(k-1),$$

ebből rendezés után kapjuk, hogy $k(x-y) = (k-1)(x-y)$, tehát $x = y$.

$x = y$ felhasználásával számoljuk meg kétféleképpen az $(l_1 \cup l_2) \setminus M$ ponthalmazt S_k-n kívül metsző egyeneseket:

$$x^2 = kx - (k-1)(q-1-x) + (q-1-k)k,$$

amiből rendezés után kapjuk, hogy:

$$x^2 + x(1-2k) + k^2 - q + 1 = 0.$$

Ebből kifejezhetjük x-et:

$$x_{1,2} = \frac{2k - 1 \pm \sqrt{4q - 4k - 3}}{2}.$$

Mivel x-egész, ez csak akkor lehetséges, ha $4q-4k-3$ négyzetszám. $x \geq k$, ellenkező esetben az $l_3 \cap S_k$-beli pontoknak nem lehetne k db érintője, így azt kapjuk, hogy $x = k - \frac{1}{2} + \sqrt{q-k-\frac{3}{4}}$.

$l_1 \cap S_k$ minden pontjának van $k-1$ db olyan érintője, mely l_2-t és l_3-at nem az $l_2 \cap l_3$ csúcsban metszi, így az alábbi becslést kapjuk:

$$(q-1-x)(k-1) \leq kx.$$

A folytatásban tegyük fel, hogy $2 \leq k$.
Írjuk be ide az x-re kapott kifejezést:

$$\left(q - \frac{1}{2} - k - \sqrt{q-k-\frac{3}{4}}\right)(k-1) \leq k\left(k - \frac{1}{2} + \sqrt{q-k-\frac{3}{4}}\right),$$

a bal oldalt alulról, a jobb oldalt felülről becsülve:

$$(q-1-k-\sqrt{q})\,(k-1) \leq k(k+\sqrt{q}).$$

Ez az alábbi egyenlőtlenségre vezet:

$$(k-1)q - \sqrt{q}(2k-1) - 2k^2 + 1 \leq 0,$$

és ebből $q \leq c \cdot k$ következik pl. $7 \leq k$ esetén $c = 4$ megfelelő lesz. Azt kaptuk tehát, hogy rögzített k esetén, csak véges sok ebbe a típusba sorolható k-szemiív létezik. □

Amikor $k = 1$, vagyis S_k egy szemioválís, akkor $PG(2,q)$ síkokon az előbbi eset teljes karakterizációja megtalálható Kiss György és Ruff János közös cikkében [13].

2.3.4 Tétel: Ha a Π_q sík S_k k-szemiívét tartalmazza az l_1, l_2, l_3 nem egy ponton átmenő egyenesek uniója, és S_k nem tartalmazza ezek metszéspontjait, akkor az alábbiak egyike teljesül:

1. S_k mindhárom egyenesről ugyanannyi pontot tartalmaz,
2. S_k két egyenesről $q-k$ pontot tartalmaz, a harmadikról pedig legalább 2-t és legfeljebb $k-1$-et.

Bizonyítás: Legyen $x = q-1-|S_k \cap l_1|$, $y = q-1-|S_k \cap l_2|$ és $z = q-1-|S_k \cap l_3|$. Jelöljük a háromszög három csúcsának a halmazát M-mel. Ekkor az $(l_1 \cup l_3) \setminus M$ ponthalmazt S_k-n kívül metsző egyeneseket kétféleképp megszámolva:

$$yz = xy - (k-1)(q-1-z) + (k-1)(q-1-x),$$

amiből:

$$y(z-x) = (k-1)(z-x).$$

Hasonlóan kapjuk, hogy:

$$x(y-z) = (k-1)(y-z),$$

$$z(x-y) = (k-1)(x-y).$$

Ebből $x = y = z$ vagy pedig az következik, hogy x, y, z közül kettő $k-1$-gyel egyenlő.

Tegyük fel, hogy $k-1=x=y$, ekkor az $l_3 \cap S_k$-beli pontok mindegyikéhez tartozik $k-1$ db érintő, mely elkerüli M-et. Ezek számára a következő egyenlőtlenséget kapjuk:

$$(q-1-z)(k-1) \leq (k-1)^2,$$

ebből kapjuk, hogy $q-k \leq z$, amiből $|l_3 \cap S_k| \leq k-1$ következik

Indirekt tegyük fel, hogy $|l_3 \cap S_k| = 1$, és legyen ez a metszéspont P. Ekkor S_k lefedhető az $l_1 \cap l_2 = \{Q\}$ metszésponton átmeő PQ, ill. l_1, l_2 egy ponton átmenő egyenesekkel, így 2.2.2 lemma miatt ez 5 általános helyzetű pont. □

2.3.5 Megjegyzés: Speciálisan, ha $k = 2$, akkor nincsenek a 2. típusba tartozó szemiívek, erről szólt 1.5.3 tétel is. Megmutatjuk, hgy $k > 2$ esetén már léteznek ilyen struktúrák.

2.3.6 Példa: Legyen $k > 2$ és Π_k a Π_q sík k-adrendű részsíkja. Legyen l_1, l_2, l_3 három egyenes, melyek Π_k-t $k+1$ pontban metszik. Legyen $L_1 = l_1 \setminus \Pi_k$, $L_2 = l_2 \setminus \Pi_k$, és $L_3 \subset l_3 \cap \Pi_k$ úgy, hogy $2 \leq |L_3|$ $k-1$. Ekkor:

$$S_k := L_1 \cup L_2 \cup L_3$$

egy k-szemiív. Valóban, egy L_i-beli pont érintői az $l_j \cap \Pi_k \setminus l_1 \cap l_2$ pontokban metszik l_j-t ({i,j}={1,2}). Míg egy L_3-beli pont érintői, a rajta átmenő Π_k-beli egyenesek l_3 kivételével.

Az 1. esetbe tartozó k-szemiívekre $k = 3$ esetén a "További konstrukciók" című fejezetben mutatunk példákat.

3. fejezet

Szemioválisok három, egy ponton átmenő egyenesen

3.1. Pollard és Grynkiewicz tétele

Ebben a szakaszban összefoglaljuk a fejezetben használt additív kombinatorikai tételeket és jelöléseket.

3.1.1 Definíció: Legyen G egy tetszőleges csoport, $A, B \subseteq G$ nemüres részhalmazok, $\odot$ pedig a csoportművelet. Jelöljük $N_t(A, B)$-vel azon $c \in A \odot B$ elemek halmazát, melyek legalább t-féleképpen állnak elő $c = a \odot b$ alakban ($a \in A, b \in B$). Amennyiben egyértelmű, $N_t(A, B)$ helyett N_t-t írunk. Speciálisan $N_1(A, B) = A \odot B = \{a \odot b \mid a \in A, b \in B\}$.

3.1.2 Definíció: Legyen A a $(G, \odot)$ Abel-csoport egy részhalmaza. Ekkor A stabilizátorán az alábbi halmazt értjük:

$$stab(A) = \{g \in G \mid A \odot g = A\}.$$

Ismert és könnyű belátni, hogy $stab(A)$ mindig a G egy részcsoportja.

Az alábbi tétel Pollard [15] eredménye 1974-ből, a kövezkető szakaszban prímrendű síkok szemioválisainak elemszámbecsléséhez fogjuk használni.

3.1.3 Tétel: (Pollard) Legyen G egy Abel-csoport, $|G| = p$ prím, $A, B \subseteq G$ nemüres részhalmaz. Ekkor $1 \leq t \leq \min\{|A|, |B|\}$ esetén:

$$|N_1| + |N_2| + \ldots + |N_t| \geq t \cdot \min\{p, |A| + |B| - t\}$$

Az alábbi tétel Grynkiewicz [8] 2010-es eredménye, mely a Pollard-tétel általánosítása. Ezt szintén elemszámbecslésekhez, illetve az erős szemioválisok karakterizálására fogjuk használni.

3.1.4 Tétel: (Grynkiewicz) Legyen G Abel-csoport, $A, B \subseteq G$ véges, nemüres részhalmaz, ekkor

$$\sum_{i=1}^{t} |N_i| \geq t(|A| + |B|) - 2t^2 + 1$$

Vagy létezik olyan $A' \subseteq A$ és $B' \subseteq B$ részhalmaz, hogy

$$l := |A \setminus A'| + |B \setminus B'| \leq t - 1$$
$$N_t(A', B') = N_1(A', B') = N_t(A, B)$$
$$\sum_{i=1}^{t} |N_t| \geq t(|A| + |B|) - (t - l)(|H| - \rho) - tl \geq t(|A| + |B| - |H|)$$

Ahol H az $N_t(A, B)$ nem triviális stabilizátora és $\rho = |A' \odot H| - |A'| + |B' \odot H| - |B'|$. Amennyiben $t = 2$ úgy az első egyenlőtlenség helyett $|N_1| + |N_2| \geq 2(|A| + |B|) - 4$-et is írhatunk.

3.2. Elemszám becslések

2.2.3 tételben megmutattuk, hogy egyetlen kivétellel, a három egy ponton átmenő egyenesre illeszkedő szemiívek kétfélék lehetnek, ezek közül a szemioválisok $q > 3$ esetén mind abba a csoportba tartoznak, ahol mindhárom fedőegyenes ugyanannyi pontban metszi a ponthalmazt. Ebben a fejezetben ilyen szemioválisokat fogunk vizsgálni a $PG(2, q)$ síkokon. 2.2.11 lemma alapján bármely szemiív, speciálisan szemioválisok elemszámára is könnyen tudunk felső becslést adni. Az alábbi tétel [3]-ban megtalálható:

3.2.1 Tétel: Legyen S a Π_q sík olyan szemioválisa, melyet tartalmaz három egy ponton átmenő egyenes. Ekkor $q > 3$ esetén $|S| \leq 3\left\lceil q - \sqrt{q}\right\rceil$.

S elemszámának alsó becslésére [13]-ben található az alábbi becslés.

3.2.2 Tétel: Legyen S a q-adrendű sík olyan szemioválisa, melyet tartalmaz három egy ponton átmenő egyenes, ekkor $q > 9$ esetén $|S| > 3(q - 2)/2$.

Az ebben a fejezetben vizsgált szemioválisokra példaként eddig egyetlen osztályt ismerünk, melyet szintén [13]-ban publikáltak szerzői, és élességgel teljesíti az elemszámra vonatkozó felső becslést. A példát a szakasz végén közöljük. Most bevezetünk néhány jelölést:

3.2.3 Definíció: Legyen a $PG(2, q)$ sík S szemioválisát tartalmazó három egy ponton átmenő egyenes l_1, l_2, l_3, közös metszéspontjuk pedig $l_1 \cap l_2 \cap l_3 = P$. 2.2.1 állítás miatt $q > 3$ esetén $P \notin S$ feltehető. Az egyenesek S ponthalmazzal vett metszetei legyenek:

$$L_1 = S \cap l_1,\ L_2 = S \cap l_2,\ L_3 = S \cap l_3,$$

melyekre $|L_1| = |L_2| = |L_3|$. Legyen $k = q - |L_i|$ "az egyenesekről kimaradó pontok" száma. Ekkor $|S| = 3q - 3k$, tehát 3.2.2 és 2.2.11 alapján k-ra a következő adódik:

$$\sqrt{q + \frac{1}{4}} - \frac{1}{2} \leq k \leq \frac{q + 1}{2}.$$

3.2.4 Definíció: A koordinátarendszert válasszuk meg 1.1.3 állításnak megfelelően úgy, hogy l_1, l_2, l_3 egyenletei $X_1 = -X_3$, $X_1 = 0$ és $X_1 = X_3$ legyenek, ekkor P koordinátái: $(0, 1, 0)$. Az egész fejezetre nézve definiáljuk az alábbi halmazokat:

$$A = \{a \in GF(q) : (-1, a, 1) \notin L_1\},$$
$$B = \{b \in GF(q) : (0, b, 2) \notin L_2\},$$
$$C = \{c \in GF(q) : (1, c, 1) \notin L_3\}.$$

Ekkor A, B és C a $GF(q)$ additív csoportjának k elemű részhalmaza. A $(-1, a, 1)$, $(0, b, 2)$, $(1, c, 1)$ pontok pedig pontosan akkor kollineárisak, ha $a + c = b$.

A vizsgált szemioválisok elemszámáról az eddigi tételek alapján csak annyit tudtunk, hogy:

$$3(q-2)/2 < |S| \leq 3\lceil q - \sqrt{q}\rceil .$$

A következőkben az alsó korláton szeretnénk javítani, az előző szakaszban ismertetett tételek segítségével.

3.2.5 Tétel: Legyen S szemioválisa a $PG(2, p)$ síkon, ahol p páratlan prím. Legyen l_1, l_2, l_3 három egyenes, mely egy közös $P \notin S$ pontban metszi egymást és legyen $S \subset \{l_1 \cup l_2 \cup l_3\}$. Ekkor $|S| \geq 3p - 6\left\lceil\sqrt{p+1}\right\rceil + 6$.

Bizonyítás: Használjuk 3.2.3, 3.2.4 és 3.1.1 jelöléseit. Emlékeztetőül:
$k = q - |L_i| = |A| = |B| = |C|$.

Mivel S szemioválisa, nincsen olyan L_2-beli pont, melynek 1-nél több érintője van, tehát $N_t(A, C) \subseteq B$ minden $t \geq 2$ esetén, tehát ilyenkor $|N_t(A, C)| \leq k$, míg $|N_1(A, C)| \leq p$.

$t \geq 1$ és $k \leq \frac{1}{2}(p + 1)$ miatt:

$$\min\{p, |C| + |A| - t\} = |C| + |A| - t = 2k - t,$$

tehát a Pollard tétel szerint:

$$p + (t-1)k \geq |N_1| + |N_2| + \ldots |N_t| \geq 2tk - t^2$$

A kapott egyenlőtlenséget átrendezve:

$$\frac{p+1}{t+1} + t - 1 \geq k$$

Ez a kifejezés akkor minimális, ha $t = \sqrt{p+1} - 1$, válasszuk hát t-t $\left\lceil\sqrt{p+1}\right\rceil - 1$-nek, ekkor $k \leq 2\left\lceil\sqrt{p+1}\right\rceil - 2$ következik (ha a Pollard tételhez szükséges $t \leq k$ feltétel nem teljesülne, akkor a még erősebb $k \leq \left\lceil\sqrt{p+1}\right\rceil - 1$ is igaz).
$|S| = 3p - 3k$ miatt a tétel állítása következik. □

3.2.6 Tétel: Legyen S mint az előbb, csak most a $PG(2, q)$ síkon. Legyen $q = p^n$ és $n \geq 2$, p páratlan prím, ekkor $|S| \geq 3q - 3f_n(q)$, ahol:

$$f_n(q) = \begin{cases} 4\left\lceil\sqrt{\frac{q+1}{2}}\right\rceil - 4 & \text{ha } n = 2 \\ q^{\frac{n-1}{n}} + q^{\frac{1}{n}} - 1 & \text{ha } n \geq 3 \end{cases}$$

BIZONYÍTÁS: Használjuk az eddigi jelöléseket és Grynkiewicz tételét. Amennyiben

$$\sum_{i=1}^{T} |N_i| \geq T(|A| + |C|) - 2T^2 + 1,$$

teljesül valamely $T \leq k$-ra, akkor ez a következő egyenlőtlenségre vezet:

$$q + (T-1)k \geq 2Tk - 2T^2 + 1.$$

Ezt átrendezve:

$$\frac{q+1}{T+1} + 2T - 2 \geq k \tag{3.1}$$

Amennyiben $\frac{q+1}{T+1} + 2T - 2 < k$, akkor létezik a tétel állításában szereplő A' és C' részhalmaz. Ekkor alkalmazzuk a tételt $t = 1$ esetben erre a két részhalmazra:

$$|A' + C'| \geq |A'| + |C'| - |H|,$$

ahol H az $A' + C'$ stabilizátor részcsoportja. Szintén a tételből következik, hogy $\frac{q+1}{T+1} + 2T - 2 < k$ esetén:

$$T - 1 \geq |A \setminus A'| + |B \setminus B'|,$$

amiből kapjuk, hogy:

$$|A'| + |C'| \geq |A| + |C| - T + 1.$$

Az alábbi egyenlőségek szintén a tételből, míg a tartalmazás abból következik, hogy S szemioválisés így egyik pontjának sem lehet $1 < T$ db érintője (T választását még nem mondtuk meg, de 1-nél nagyobb lesz):

$$N_1(A', C') = N_T(A', C') = N_T(A, C) \subseteq B,$$

ebből pedig $|B| \geq |A' + C'|$ következik. Az eddigi egyenlőtlenségeket összerakva:

$$|B| \geq |A' + C'| \geq |A'| + |C'| - |H| \geq |A| + |C| - T + 1 - |H|$$

Így $k \geq 2k - T + 1 - |H|$ adódik, amit átrendezve:

$$|H| + T - 1 \geq k. \tag{3.2}$$

3.1 és 3.2 egyenlőtlenségekből következik, hogy $\forall\ 1 < t \leq k$ esetén:

$$\max\left\{\frac{q+1}{t+1} + 2t - 2\ ,\ |H| + t - 1\right\} \geq k.$$

$n \geq 3$ esetén legyen $t = p$, ekkor:

$$\frac{q+1}{t+1} + 2t - 2 = \frac{p^n + 1}{p+1} + 2p - 2 \leq p^{n-1} + p - 1,$$

ahol a jobb oldal $|H| + t - 1$ maximuma, így:

$$p^{n-1} + p - 1 \geq k.$$

$n = 2$ esetén $|H|$ csak $\sqrt{q}$ lehet és ekkor:

$$\frac{q+1}{t+1} + 2t - 2 \geq \sqrt{q} + t - 1,$$

ezért a bal oldalt kell minimalizálnunk. Ez a minimum $\sqrt{\frac{q+1}{2}} - 1$-nél, ezért legyen $t = \left\lceil \sqrt{\frac{q+1}{2}} \right\rceil - 1$, ebből:

$$4\left\lceil \sqrt{\frac{q+1}{2}} \right\rceil - 4 \geq \frac{q+1}{\left\lceil \sqrt{\frac{q+1}{2}} \right\rceil} + 2\left\lceil \sqrt{\frac{q+1}{2}} \right\rceil - 2 \geq k$$

Mindkét esetben igaz, hogy ha a Grynkiewicz tétel $t \leq k$ feltétele nem teljesül, akkor k-ra még kisebb felső korlátot, és így $|S|$-re még nagyobb alsó korlátot kapunk. □

A már említett [13]-ban szereplő példa az ottaninál a fenti jelölésrendszerhez jobban illeszkedő megfogalmazásban, és kicsivel általánosabban:

3.2.7 Példa: (Kiss, Ruff) $PG(2,q)$ síkokon $q = p^{2n}$, p páratlan prím esetben léteznek szemioválisok 3 kongruens egyenesen. Jelüljük $GF(p^{2n})$ additív csoportját G-vel. $G \cong Z_p^{2n}$, ahol Z_p a p-rendű ciklikus csoport. Legyen $G_1, G_2 \subset G$ olyan részcsoportok, hogy $G_1 \cong G_2 \cong Z_p^n$ és $G_1 \times G_2 = G$. Ekkor $G = \{(x,z) \mid x \in G_1, z \in G_2\}$, és legyen σ a G_1 egy tetszőleges permutációjának, egy $G_1 \to G_2$ izomorfizmussal vett kompozíciója. Definiáljuk A, B, C-t a következő módon:

$$A := \{(x,0) \mid x \in G_1\}$$
$$B := \{(y,\sigma(y)) \mid y \in G_1\}$$
$$C := \{(0,z) \mid z \in G_2\}$$

Legyen:

$$L_1 = \{(-1,a,1) \mid a \notin A\}$$
$$L_2 = \{(0,b,2) \mid b \notin B\}$$
$$L_3 = \{(1,c,1) \mid c \notin C\}$$

Ekkor $S := L_1 \cup L_2 \cup L_3$ egy $3q - 3\sqrt{q}$ elemszámú szemioválisa. Azt, hogy S minden pontjának pontosan egy érintője van, az L_1-beli pontokon fogjuk megmutatni, a másik két esetben hasonlóan belátható. Legyen $Q \in L_1$, ekkor Q koordinátái: $(-1,q,1)$, ahol $q \in G = \{(x,z) \mid x \in G_1, z \in G_2\}$, továbbá $q \notin A$ miatt $q = (x_q, y_q)$ második, G_2-szerinti koordinátája nem 0.

Azt kell megmutatnunk, hogy pontosan egy olyan $R(0,r,2) \notin L_2$, $T(1,t,1) \notin L_3$ pontpár van, melyre $q + t = r$. Valóban, $t \in C$ miatt t első, G_1-szerinti koordinátája 0 és így r első koordinátája x_q kell legyen. $r \in B$ miatt $r = (x_q, \sigma(x_q))$, ebből pedig $t = (0, \sigma(x_q) - y_q)$ következik.

Ezzel beláttuk, hogy a Q pont egyértelműen meghatározza R-t és T-t.

3.3. Tételek erős szemioválisokról

Az előző példának van egy speciális tulajdonsága:
Bármely $Q \in l_1 \cup l_2 \cup l_3 \setminus (S \cup \{P\})$ pont esetén Q-n át pontosan ugyanannyi, jelen esetben $(\sqrt{q}-1)^2$ db 2-szelője megy a szemioválisnak (P-vel most is a 3 egyenes metszéspontját jelöltük).

3.3.1 Definíció: A három, egy ponton átmenő l_1, l_2, l_3 egyenesek által tartalmazott S szemioválist erős szemioválisnak nevezzük, ha minden $l_1 \cup l_2 \cup l_3 \setminus (S \cup \{P\})$-beli pontján át S-hez ugyanannyi db 2-szelő húzható. Ezt a számot az erős szemiováis paraméterének nevezzük.

A definíciót Blokhuis és szerzőtársai vezették be [3]-ban. Szintén ebben a cikkben bizonyítják az alábbi állításokat:

3.3.2 Állítás: Ha a $PG(2,q)$ sík k-paraméterű erős szemioválisa $3a$ pontot tartalmaz, akkor:

$$k = a - \frac{a}{q-a}.$$

Ebből egyszerűen következik, hogy $(q-a)$ osztja a-t, és így $(q-a)+a=q$-t is. Tehát, ha $q=p^m$, akkor $a=p^m-p^l$, és így $|S|=3(p^m-p^l)$. Mivel S, az l_1, l_2, l_3 egyenesek mindegyikéről ugyanannyi pontot kell, hogy tartalmazzon, ezért ilyenkor:

$$|L_1| = |L_2| = |L_3| = p^l,$$

ahol a 3.2.1 tétel miatt $m/2 \leq m$. Ebből rögtön adódik, hogy $PG(2,p)$ prímrendű síkon nincsenek erős szemioválisok. Az említett cikk szerzői a $PG(2,p^2)$ esetben megadták az erős szemioválisok teljes leírását. Bizonyították továbbá, hogy:

3.3.3 Tétel: Ha a $PG(2,p^m)$, páratlan rendű sík egy erős szemioválisára:

1. $p \equiv -1 \pmod 4$ esetén $m \leq (p-1)^2$,
2. $p \equiv 1 \pmod 4$ esetén $m \leq 2(p-1)^2$,

akkor $|S| = 3(q-\sqrt{q})$.

A következő szakaszban ezt a tételt fogjuk általánosítani.

3.4. Erős szemioválisok karakterizációja

A bizonyításokban használt A, B és C jelölések a 3.2.4 definícióban lettek bevezetve.

3.4.1 Tétel: Legyen S egy erős szemioválís a $PG(2,q)$ síkon, ahol $q=p^{2l}$ és p egy páratlan prím. Ekkor:

$$|S| = 3(q-\sqrt{q}).$$

Bizonyítás: Legyen $|A|=|B|=|C|=p^r$, ahol az előző szakaszban említettek miatt $l \leq r < 2l$. Bebizonyítjuk, hogy $r=l$. A 3.2.6 tétel bizonyításából tudjuk, hogy minden $t \leq p^r$ esetén:

$$p^r \leq \frac{p^{2l}+1}{t+1} + 2t - 2, \tag{3.3}$$

vagy pedig létezik $N_t(A, C)$ nem triviális H stabilizátor részcsoportja, melyre:

$$p^r \leq |H| + t - 1. \tag{3.4}$$

Ezt a $t = p^l$ esetben fogjuk hasznláni. Hogy ha 3.3 esete áll fenn, akkor:

$$p^r \leq \frac{p^{2l}+1}{p^l+1} + 2p^l - 2 < 3p^l - 2 < p^{l+1},$$

és ezért $r = l$.

Amennyiben 3.4 teljesül, akkor $N_{p^l}(A, C)$ H mellékosztályainak az uniója és B-nek részhalmaza. Ezért $|H| \leq |B| = p^r$. Először megmutatjuk, hogy $|H| = |B|$, tehát B a H-nak egy mellékosztálya. Mostantól tegyük fel, hogy $r > l$ máskülönben készen vagyunk. $|H| < p^r$ ezt eredményezné:

$$p^r \leq |H| + p^l - 1 \leq p^{r-1} + p^l - 1 \leq 2p^{r-1} - 1 < p^r - 1,$$

ami ellentmondás. Legyen $A' = -A$, $B' = C$ és $C' = B$, pontosan ugyanezt a bizonyítást elmondhatjuk A', B', C' halmazokkal A, B, C helyett, tehát feltehetjük, hogy $B' = C$ is egy mellékosztály. Az $A'' = B$, $B'' = A$ és $C'' = -C$ jelölés mutatja, hogy ugyanez mondható az A halmazról is. Ekkor $A+C$ is egy részcsoport mellékosztálya és az elemszámára:

$$|A + C| > p^{2l} - p^r \geq p^{2l} - p^{2l-1} > p^{2l-1}.$$

Ez csak akkor történhet meg, ha $A + C$ a $GF(p^{2l})$ teljes additív csoportja. $A + C$ minden eleme előáll $\frac{|A||C|}{|A+C|}$ db különböző $a+c$ alakú összegként, ahol $a \in A$ és $c \in C$. $r > l$ miatt ez az érték nagyobb mint p^2, ami ellentmond annak, hogy S szemioválisis, hiszen minden L_2-beli pontnak p^2 érintője lenne. □

3.4.2 Tétel: Legyen $p > 7$ prím, ekkor nincsenek erős szemioválisok a $PG(2, p^{2l+1})$ síkon.

Bizonyítás: Tegyük fel, hogy S egy erős szemioválisis és $|A| = |B| = |C| = p^r$, ahol $l + 1 \leq r < 2l + 1$. Mint az előző bizonyításban, most is a 3.2.6-ben található egyenlőtlenségeket fogjuk használni, ezúttal a $t = \left\lfloor p^{l+\frac{1}{2}} \right\rfloor$ választással, mely a következőket mondja nekünk:

$$p^r \leq \frac{p^{2l}+1}{\left\lfloor p^{l+\frac{1}{2}} \right\rfloor + 1} + 2\left\lfloor p^{l+\frac{1}{2}} \right\rfloor - 2,$$

vagy létezik az $N_{\left\lfloor p^{l+\frac{1}{2}} \right\rfloor}(A, C)$ nemtriviális H stabilizátor részcsoportja, melyre:

$$p^r \leq |H| + \left\lfloor p^{l+\frac{1}{2}} \right\rfloor - 1.$$

Az első esetben ezt állíthatjuk:

$$p^r \leq \frac{p^{2l}+1}{\left\lfloor p^{l+\frac{1}{2}} \right\rfloor + 1} + 2\left\lfloor p^{l+\frac{1}{2}} \right\rfloor - 2 < 3\left\lfloor p^{l+\frac{1}{2}} \right\rfloor - 1 < p^{l+1},$$

Ami ellentmondás, mivel $r \geq l+1$.

A második esetben $N_{\lfloor p^{l+\frac{1}{2}} \rfloor}(A,C)$ előáll mint H mellékosztályainak az uniója, továbbá a B-nek részhalmaza. Ebből kapjuk, hogy $|H| \leq |B| = p^r$. Megmutatjuk, hogy $|H| = |B|$, és így B a H egy mellékosztálya. Ha $r = l+1$, akkor $|H| < p^r$ ezt eredményezné:

$$p^{l+1} \leq |H| + \left\lfloor p^{l+\frac{1}{2}} \right\rfloor - 1 < p^l + p^{l+\frac{1}{2}}$$

Míg abban az esetben, ha $r \geq l+2$:

$$p^r \leq |H| + \left\lfloor p^{l+\frac{1}{2}} \right\rfloor - 1 < 2p^{r-1}.$$

Mindkét eset ellentmondáshoz vezet. Mint az előző bizonyításban, most is feltehetjük, hogy A, C és így $A+C$ is mellékosztály, mitöbb $A+C$ a $GF(p^{2l+1})$ teljes additív csoportja. $A+C$ minden eleme előáll $\frac{|A||C|}{|A+C|}$ db külömböző összegként és ez az érték nagyobb mint p, ami ellentmondás, mivel minden L_2-beli pontnak p db érintője lenne. □

3.4.3 Tétel: Legyen S egy erős szemioválís a $PG(2, p^{2l+1})$ síkon, ahol $p = 3, 5$ vagy 7. Ekkor:

$$|S| = 3(p^{2l+1} - p^{l+1}).$$

Bizonyítás: Legyen $|A| = |B| = |C| = p^r$, ahol $l+1 \leq r < 2l+1$. Belátjuk, hogy ekkor $r = l+1$. A már jól ismert egyenlőtlenségeinket használjuk ezúttal a $t = p^l$ választással, így:

$$p^r \leq \frac{p^{2l+1}+1}{p^l+1} + 2p^l - 2,$$

vagy létezik az $N_{p^l}(A,C)$ nemtriviális H stabilizátor részcsoportja, melyre:

$$p^r \leq |H| + p^l - 1.$$

Az első esetben ezt állíthatjuk:

$$p^r \leq \frac{p^{2l+1}+1}{p^l+1} + 2p^l - 2 < p^{l+1} + 2p^l - 2 < 3p^{l+1}$$

Ami egyedül az $r = l+1$ esetben teljesülhet.

A második esetben $N_{p^l}(A,C)$ a H mellékosztályainak uniója, és a B-nek részhalmaza. Ebből kapjuk, hogy $|H| \leq |B| = p^r$. Megmutatjuk, hogy $|H| = |B|$, és így B a H egy mellékosztálya. Mostantól tegyük fel, hogy $r > l+1$ ellenkező esetben készen vagyunk. $|H| < p^r$ ezt eredményezné:

$$p^r \leq |H| + p^l - 1 < 2p^{r-1} - 1 < p^r,$$

ami nem lehetséges. Mint az előző bizonyításokban, most is feltehetjük, hogy A, C és így $A+C$ is mellékosztály, sőtt $A+C$ a $GF(p^{2l+1})$ teljes additív csoportja. $A+C$ minden eleme előáll $\frac{|A||C|}{|A+C|}$ db különböző összegként, és ez az érték nagyobb mint p, ami ellentmondás, mert ekkor minden L_2-beli pontnak p db érintője lenne.

□

4. fejezet

További konstrukciók

4.1. 2- és 3-szemiívek

Ebben a szakaszban először alsó korlátot adunk olyan 2-szemiívek elemszámára, melyeket tartalmaz három egy ponton átmenő egyenes és ezek mindegyike ugyanannyi pontot tartalmaz a szemiívről. A bizonyítás menete a szemioválisoknál látottakhoz hasonló lesz, ám a szemioválisokkal ellentétben itt sikerült olyan végtelen osztályt találni, mely nagyságrendileg megközelíti az alsó korlátot. A példát, egy 3-szemiívekre vonatkozó megjegyzés mellett, a tétel után mutatjuk be.

4.1.1 Tétel: Legyen S_2 egy 2-szemiív a $PG(2,p)$ síkon, ahol p páratlan prím. Legyen l_1, l_2, l_3 három egyenes, mely egy közös P pontban metszi egymást és legyen $S_2 \subset \{l_1 \cup l_2 \cup l_3\}$. Ekkor:

$$|S_2| \geq 3p - 6\left\lceil\sqrt{2p+4}\right\rceil + 12.$$

Bizonyítás: Legyen $|L_1| = |L_2| = |L_3| = p - k$ és a szemioválisokhoz hasonlóan most is haszáljuk Pollard tételét:

$$2p + (t-2)k \geq \sum_{i=1}^{t} |N_t| \geq 2tk - t^2$$

A kapott egyenlőtlenséget átrendezve:

$$\frac{2p+4}{t+2} + t - 2 \geq k$$

Ez a kifejezés akkor minimális, ha $t = \sqrt{2p+4} - 2$, legyen hát $t = \left\lceil\sqrt{2p+4}\right\rceil - 2$, ekkor $k \leq 2\left\lceil\sqrt{2p+4}\right\rceil - 4$ következik (ha a Pollard tételhez szükséges $t \leq k$ feltétel nem teljesülne, akkor a még erősebb $k \leq \left\lceil\sqrt{2p+4}\right\rceil - 2$ is igaz). Ezzel állításunkat beláttuk. □

4.1.2 Tétel: Vegyünk egy S_2 halmazt, mint az előbb, csak most a $PG(2,q)$ síkon, ahol $q = p^n$ és $n \geq 2$ (p páratlan prím), ekkor $|S_2| \geq 3q - 3f_n(q)$. Ahol:

$$f_n(q) = \begin{cases} 4\left\lceil \sqrt{q+\frac{7}{2}} \right\rceil - 8 & \text{ha } n = 2 \\ 14 & \text{ha } n = 3 \text{ és } p = 3 \\ 37 & \text{ha } n = 3 \text{ és } p = 5 \\ 66 & \text{ha } n = 3 \text{ és } p = 7 \\ p^2 + 2p + 2 & \text{ha } n = 3 \text{ és } p \geq 11 \\ p^{n-1} + 2p - 2 & \text{ha } n \geq 4 \end{cases}$$

Bizonyítás: A szemioválisokhoz hasonlóan most is Grynkiewicz tételét használjuk. Amennyiben

$$\sum_{i=1}^{T} |N_i| \geq T(|A| + |C|) - 2T^2 + 1$$

teljesül valamely $T \leq k$-ra, akkor ez a következő egyenlőtlenségre vezet:

$$2q + (T-2)k \geq 2Tk - 2T^2 + 1.$$

Ezt átrendezve:

$$\frac{2q+7}{T+2} + 2T - 4 \geq k$$

Ahonnan a már látott módon kapjuk, hogy $\forall t \leq k$ esetén:

$$\max\left\{\frac{2q+7}{t+2} + 2t - 4, |H| + t - 1\right\} \geq k$$

$n = 2$ esetén $\frac{2q+7}{t+2} + 2t - 4 \geq \sqrt{q} + t - 1$ miatt a bal oldalt kell minimalizálnunk, ez a minimum $T = \sqrt{q+\frac{7}{2}} - 2$-nél van, így ekkor t-t válasszuk $\left\lceil \sqrt{q+\frac{7}{2}} \right\rceil - 2$-nek, amiből $k \geq 4\left\lceil \sqrt{q+\frac{7}{2}} \right\rceil - 8$.

$n = 3$ és $p = 3$ esetén $\frac{2\cdot 27+7}{t+2} + 2t - 4 \geq 9 + t - 1$ miatt elég a bal oldalt minimalizálni, ezt az egészek körében $t = 4$-nél veszi fel és ebből k-ra a 14-es felső becslést kapjuk.

$n = 3$ és $p = 5$ esetén $\frac{2\cdot 125+7}{t+2} + 2t - 4 \geq 25 + t - 1$ miatt elég a bal oldalt minimalizálni, ezt az egészek körében $t = 9$-nél veszi fel és ebből k-ra a 37-es felső becslést kapjuk.

$n = 3$ és $p = 7$ esetén $\frac{2\cdot 343+7}{t+2} + 2t - 4$ minimuma $t = 17$-nél van és itt az értéke nagyobb mint $49 + t - 1$-nek a $t = 17$-nél felvett értéke. Tehát k-ra a bal oldal minimumából adódó 66-os felsőbecslés következik.

$n = 3$ és $p \geq 11$ esetén $t = 2p + 3$ választással $\frac{2p^3+7}{t+2} + 2t - 4 \leq p^2 + t - 1$. Így k-ra a $p^2 + 2p + 2$ felső becslés adódik.

$n \geq 4$ esetén $t = 2p - 1$ választással $\frac{2p^3+7}{t+2} + 2t - 4 \leq p^2 + t - 1$. Amiből k-ra a $p^{n-1} + 2p - 2$-es felső becslést kapjuk. □

4.1.3 Példa: Az előző tételben 2-szemioválisok elemszámára kapott alsó korlátokat, ha pontosan nem is, de nagyságrendileg el tudjuk érni. $q = p^n$, $n \geq 3$ esetén bontsuk fel $GF(q)$ additív csoportját $X + Y$ direktösszegre és legyen:

$$A = B = C := (X \cup Y),$$

továbbá:

$$L_1 := \{(-1, a, 1) \mid a \notin A\},$$
$$L_2 := \{(0, b, 2) \mid b \notin B\},$$
$$L_3 := \{(1, c, 1) \mid c \notin C\}.$$

Ekkor $S_2 := L_1 \cup L_2 \cup L_3$ 2-szemiív lesz. Valóban, ha választok pl. egy L_2-beli pontot, akkor az őt reprezentáló b csoportelem pontosan egyféleképpen áll elő $b = x + y$ alakban, ahol $x \in X$ és $y \in Y$. Emiatt b-nek pontosan 2 db érintője lesz, az egyik L_1-et metszi az x-nek megfelelő pontban és L_2-t az y-nak megfelelőben, a másik pedig fordítva. Azt is láthatjuk, hogy:

$$|S_2| = 3q - 3(|X| + |Y| - 1),$$

ha tehát $q = p^n$, $n \geq 3$, akkor ezzel a módszerrel $|X| = p^{n-1}$ és $|Y| = p$ választással elő tudunk állítani $3q - 3p^{n-1} - 3p + 3$ elemszámú S_2 halmazokat.

4.1.4 Példa: Tekintsük a $PG(2, q)$ síkot, ahol $q = p^{3k}$, p páratlan prím, X, Y, Z, pedig a $G = Z_p^{3k}$ additív csoportnak Z_p^{2k}-val izomorf részcsoportja úgy, hogy páronként vett metszeteik Z_p^k-val izomorfak és $(X \cap Z) \times (X \cap Y) \times (Y \cap Z) = G$. Ekkor $G = \{(a, b, c) \mid a \in X \cap Z,\ b \in X \cap Y,\ c \in Y \cap Z\}$. Definiáljuk az additív csoport alábbi részhalmazait:

$$A := \{(a_1, a_2, 0) \mid a_i \in X \cap Z)\}$$
$$B := \{(0, b_1, b_2) \mid b_i \in X \cap Y\}$$
$$C := \{(c_1, 0, c_2) \mid c_i \in Y \cap Z\}$$

Ezeket a részhalmazokat a szokásos módon feleltessük meg a fedőegyenesekről elhagyott pontokkal. Ekkor $\overline{A} = \{(x, y, z) \mid x, y \in Z_p^k, z \in Z_p^k \setminus \{0\}\}$ és benne egy tetszőleges (x_0, y_0, z_0) csoportelemnek megfelelő L_1-beli pont érintői az l_2 és l_3 egyeneseket a $(0, y_0, w) \in B$ és $(x_0, 0, w - z_0) \in C$ elemeknek megfelelő pontokban metszheti, ahol $w \in Z_p^k$ tetszőleges, tehát minden L_1-beli pontnak pontosan $|Z_p^k|$ érintője van. Hasonlóan belátható, hogy ugyanez igaz az L_2- és L_3-beli pontokra is, így A, B, C egy $3q - 3q^{\frac{2}{3}}$ elemszámú $\sqrt[3]{q}$-szemiívet határoz meg.

4.1.5 Megjegyzés: Pollard és Grynkiewicz tételét akkor is használhatjuk szemiívek elemszámának alsó becslésére, amikor S egy projektív háromszög részhalmaza, mely nem tartalmazza a háromszög csúcsait. Ez esetben $GF(q)$ multiplikatív csoportját kell vizsgálnunk 1.1.4 állítás segítségével, és amennyiben $q - 1$ prím ($q = 3$-at kivéve ez egyedül akkor fordulhat elő, ha $q - 1$ Mersenne-prím), akkor Pollard tételét, a többi esetben pedig Grynkiewicz-tételét érdemes alkalmazni.

4.1.6 Példa: Amennyiben Z_{q-1} előáll 2 valódi részcsoportjának direktszorzataként, úgy $PG(2, q)$-ban az előző példához hasonlóan készíthetünk olyan 3-szemiíveket, melyeket egy projektív háromszög tartalmaz. Legyen $GF(q)^\times = X \times Y$ és legyen $A = B = C := X \cup Y$, valamint:

$$L_1 := \{(0, a, 1) \mid a \notin A\},$$
$$L_2 := \{(b, 0, 1) \mid b \notin B\},$$

$$L_3 := \{(-c, 1, 0) \mid c \notin C\}.$$

Ekkor az előző példához hasonlóan itt is belátható, hogy $S := L_1 \cup L_2 \cup L_2$ 3-szemiív (az előzőhöz képest itt minden pontnak van még egy extra érintője, mely a pontot tartalmazó oldallal szemközti csúcson halad át).

4.1.7 Példa: Legyen l_1, l_2, l_3 a 1.1.4 állításban meghatározott egyenesek a $PG(2, q)$ síkon, ahol $q = 4k + 3$. Ekkor $GF(q)^\times = Z_2 \times Z_{2k+1}$. Megadunk egy $(2k + 1)$-szemiívet, mely tartalmazza az egyenesek metszéspontjait. Tekinthetjük úgy, hogy $GF(q)^\times = \{(a, b) \mid a \in \{0, 1\},\ b \in \{0, 1, \ldots, 2k\}\}$, ahol a művelet a koordinátánkénti összeadás, modulo 2, ill. modulo $(2k + 1)$. Hagyjuk el mindhárom egyenesről az $\{(1, x) \mid x \in \{0, 1, \ldots 2k\}\}$ elemeknek megfelelő pontokat. A megmaradó pontok $(2k + 1)$-szemiívet alkotnak. Ez a példa mutatja 2.3.1 állítás élességét.

4.2. Példák görbék segítségével

Ismét három, egy ponton átmenő egyenesen lévő szemiívekre fogunk példákat mutatni.

4.2.1 Példa: Tekintsük a $PG(2, q)$ síkot, ahol $q = 4k + 3$ $(k \in Z)$. Példát adunk $(k + 2)$-szemiívre.

$A = C$ álljon $GF(q)$ kvadratikus maradékaiból (a 0-t is beleértve), míg B a kvadratikus nem-maradékokból és a 0-ból. Ekkor $|A| = |B| = |C| = 2k + 2$. Legyen $(-1, a, 1) \in L_1$ tetszőleges (ekkor a kvadratikus nem-maradék). q választása miatt a kvadratikus nem-maradékok mindegyike egyértelműen előáll úgy, mint egy kvadratikus maradék ellentettje, így ennek a pontnak pontosan annyi érintője lesz, mint ahány (y^2, z^2) megoldáspár kielégíti az $a + z^2 = -y^2$ egyenletet. Hasonlóan látható, hogy egy tetszőleges $(0, b, 2) \in L_2$ pont érintőinek a száma, azon (x^2, z^2) megoldáspárok száma, melyek kielégítik az $x^2 + z^2 = b$ egyenletet (ahol b nem-nulla kvadratikus maradék). Illetve egy tetszőleges $(1, c, 1) \in L_3$ pont érintőinek a száma, azon (x^2, y^2) megoldáspárok száma, melyek kielégítik az $x^2 + c = -y^2$ egyenletet (ahol c kvadratikus nem-maradék). Az egyenleteket átrendezve és ismét felhasználva, hogy egy kvadratikus nem-maradék ellentettje nem-nulla kvadratikus maradék, mindhárom egyenlet az alábbi alakra hozható:

$$X^2 + Y^2 = C$$

ahol C nem-nulla kvadratikus maradék. Az érintők száma pedig az (X^2, Y^2) rendezett megoldáspárok száma. Projektív koordinátákra áttérve láthatjuk, hogy az így definiált másodrendű görbének nincsenek ideális pontjai, hiszen $X^2 = -Y^2$ a q választása miatt nem lehetséges. A görbének tehát $q + 1$ db $(X, Y, 1)$ alakú pontja van. A görbe pontjai között szerepel: $(0, u, 1), (u, 0, 1), (-u, 0, 1), (0, -u, 1)$, ahol $u^2 = C$ (és nincsen több pontja, melynek valamelyik koordinátája 0). Ezekhez a pontokhoz az (X^2, Y^2) párra 2 megoldás tartozik: $(C, 0)$ és $(0, C)$.

Amennyiben a 2 kvadratikus maradék $GF(q)$-ban, úgy a görbe pontjai között szerepel a következő 4 pont: $(v, v, 1), (-v, -v, 1), (v, -v, 1), (-v, v, 1)$, ahol $v^2 = C/2$ (ugyanakkor nincsen több görbepont, mely kielégítené az $X^2 = Y^2$ egyenletet). Ezekhez a pontokhoz az (X^2, Y^2) párra 1 megoldása tartozik: $(C/2, C/2)$.

Mivel az előbb említett 8 ponton kívül a görbe bármely $(x, y, 1)$ pontja esetén

$(-x, y, 1), (-x, -y, 1), (x, -y, 1)$ is páronként különböző görbepont melyekhez az (X^2, Y^2) párra ugyanaz a (x^2, y^2) megoldása tartozik, így az értintők száma ebben az esetben: $\frac{q+1-8}{4} + 3 = \frac{q+5}{4}$.

Amennyibe a 2 kvadratikus nem-maradék, úgy a görbének nem lesz az $X^2 = Y^2$ egyenletet is kielégítő pontja, ám az érintők száma ekkor is: $\frac{q+1-4}{4} + 2 = \frac{q+5}{4}$.

4.2.2 Példa: Tekintsük ismét a $PG(2, q)$ síkot, ahol $q = 4k+3$ ($k \in Z$). Megadunk a síkon egy $(k+1)$-szemiívet.

Álljon $A = B = C$ a kvadratikus maradékokból (a 0-t is beleértve). Ekkor $|A| = |B| = |C| = 2k + 2$. Legyen $(-1, a, 1) \in L_1$ tetszőleges (ekkor a kvadratikus nem-maradék). Ennek a pontnak pontosan annyi érintője lesz, mint ahány (y^2, z^2) megoldáspár kielégíti az $a + z^2 = y^2$ egyenletet. Egy tetszőleges $(0, b, 2) \in L_2$ pont érintőinek a száma, azon (x^2, z^2) megoldáspárok száma, melyek kielégítik az $x^2 + z^2 = b$ egyenletet (ahol b kvadratikus nem-maradék). Egy tetszőleges $(1, c, 1) \in L_3$ pont érintőinek a száma: azon (x^2, y^2) megoldáspárok száma, melyek kielégítik az $x^2 + c = y^2$ egyenletet (ahol c kvadratikus nem-maradék). Az első és az utolsó egyenlet ugyanolyan típusú, tehát egy L_1- illetve L_3-beli pont érintőinek a száma, az

$$Y^2 - X^2 = C$$

egyenlet rendezett (X^2, Y^2) megoldásainak a száma, ahol C kvadratikus nem-maradék. Projektív koordinátákra áttérve láthatjuk, hogy a fenti egyenlettel definiált másodrendű görbének két ideális pontja van, melyek: $(1, 1, 0)$ és $(1, -1, 0)$. Ehhez a két ponthoz nem tartozik megoldása az egyenletnek. A görbén van továbbá a következő két pont: $(u, 0, 1), (-u, 0, 1)$, ahol $u^2 = -C$. Ehhez a két ponthoz az egyenlet egy megoldása tartozik: $(-C, 0)$. Az ideális pontokat leszámítva a görbének nincsen az $X^2 = Y^2$ egyenletet is kielégítő megoldása, így az előző példához hasonlóan adódik, hogy összesen $\frac{q+1-2-2}{4} + 1 = \frac{q+1}{4}$ db megoldáspárt kapunk, vagyis egy L_1- illetve L_3-beli ponton át ennyi érintő halad. Az L_2-beli pontok esetén az

$$X^2 + Y^2 = C$$

egyenletet vizsgáljuk és a rendezett (X^2, Y^2) megoldáspárok száma adja meg az érintők számát, ahol C kvadratikus nem-maradék. Először jegyezzük meg, hogy az így definiált görbének nem lesz ideális pontja, és nem lesz olyan pontja sem, melynek valamely koordinátája 0.

Amennyiben a 2 kvadratikus maradék, úgy nem lesz az $X^2 = Y^2$-nek eleget tevő pontja sem, így a már korábban látott módon kapjuk, hogy az egyenletünknek $\frac{q+1}{4}$ db megoldáspár tesz eleget.

Amennyiben a 2 kvadratikus nem-maradék, úgy a görbe pontjai között szerepel: $(v, v, 1), (-v, -v, 1), (v, -v, 1), (-v, v, 1)$, ahol $v^2 = C/2$ (ugyanakkor nincsen több görbepont, mely kielégítené az $X^2 = Y^2$ egyenletet). Ezekhez a pontokhoz az egyenlet 1 megoldása tartozik: $(C/2, C/2)$. Innen a már ismert módon kapjuk, hogy az egyenletnek $\frac{q+1-4}{4} + 1 = \frac{q+1}{4}$ megoldáspár tesz eleget.

5. fejezet

Véges geometriák és additív kombinatorika középiskolában

5.1. Bevezetés

A szakdolgozat első részében többször additív kombinatorikai módszerekkel bizonyítottunk véges projektív síkokra vonatkozó állításokat. Mind az additív kombinatorikának, mind a véges síkok témakörének számtalan, a középiskolások számára is érthető és élvezhető része van.

A véges geometriákkal egyrészt azért érdemes középiskolás szakkörön foglalkozni, mert összekapcsolja a halmazelméletből, kombinatorikából és geometriából tanultakat, így elősegíti mindhárom terület jobb megértését. Másrészt mert egy olyan terület, ahová gimnazisták is könnyen betekintést nyerhetnek, és komolyabb matematikai apparátus nélkül megérthetik a témakör megoldatlan problémáit, kihívásait. Képet kaphatnak arról, milyen dolgokkal foglalkoznak a matematikusok, fejlődik az absztrakciós képességük és reményeim szerint mindeközben jól érzik magukat, hiszen izgalmas és sokszor meglepő feladatokat oldanak meg. Röviden tekintsük át ennek a fejezetnek a felépítését:

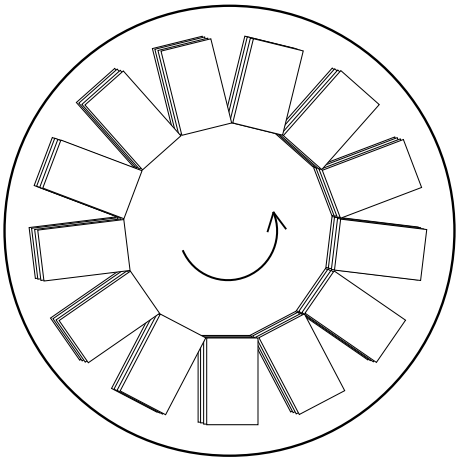
Először bemutatunk egy kártyatrükköt, mely a matematika iránt kevéssé nyitott diákok érdeklődését is felkeltheti. A trükk magyarázata közben eljutunk a *projektív sík* axiómáihoz, illetve a *ciklikus modell* leírásához. A trükk itt található leírása rövidített formában megjelent a Középiskolai Matematikai és Fizikai Lapok 2010. májusi számában [4]. Ez a leírás annyival bővebb, hogy a tanítási tapasztalataimat is tartalmazza. Sajnos a trükköt még nem tudtam középiskolásoknak előadni, de sok itt is előjövő feladatot már igen.

Ezután pár additív kombinatorikai feladatot fogok ismertetni, melyeket egy 8. osztályosoknak szóló szakkörön kipróbáltam az Apáczai Csere János Gimnáziumban. A véges geometriákhoz kapcsolódó feladatok a második órán kerültek elő és a kártyatrükk leírásánál szerepelnek. Ezzel a két témával csak ebben a két órában foglalkoztunk, de úgy vélem, hogy éppen addig jutottunk el, ameddig a csoport nagy része biztonsággal követni tudta az órát.

Az első szakköri óra leírása után két nehezebb feladat is szerepel, melyeket Hegyvári Norbert tanár úrtól hallottam az "Additív kombinatorika" című kurzuson. Noha az első óra feladatai ezekhez jó felvezetésül szolgálnak, a szakkörön mégsem beszéltük meg őket. Úgy éreztem, hogy a viszonylag hosszú bizonyításokat nem mindenki követné a csoportból, és a feladatokat inkább idősebbeknek érdemes feladni.

A Berzsenyi Dániel Gimnázium matematika táborában "Ismerkedés a véges geometriákkal" címmel tartottam foglalkozást 12. osztályosoknak. A trükk leírása közben az itt szerzett tapasztalataimat is ismertetni fogom.

5.2. Egy kártyatrükk, és ami mögötte van



5.1. ábra.

Egy bűvész 13 db, egyenként 4-4 kártyából álló kupacba osztotta az 52 lapos francia kártya lapjait, majd a kupacokat az ábrán látható módon hátlappal felfelé, egy olyan kör alakú asztalra helyezte, amely a középpontja körül bármerre elforgatható.

A mutatvány a következő: a bűvész kihív egy önként jelentkezőt a nézők közül és felkéri, hogy forgassa meg párszor az asztalt, majd válasszon ki két tetszőleges kupacot. Az így kiválasztott 8 lapot nézze meg és amenynyiben talál köztük azonos értékű kártyákat, úgy azokat hátlappal felfelé tegye félre, a többi lapot pedig helyezze vissza oda, ahonnan elvette (a kártyák ügyes elrendezése miatt minden esetben két kártyát kell félretennie).

Ezután a bűvész választ két kupacot. Ezeket megnézi, majd két lap kivételével visszateszi a kártyákat a helyükre. Végül megkéri az önként jelentkezőt, vegye kézbe ő is félretett lapjait és mutassák meg a közönségnek egyszerre, mi is az a 2-2 kártya, ami a kezükben van.

Meglepetésre, mind a négy kártyának ugyanaz az értéke.

A megfejtéshez először gondoljuk végig hogyan lehetséges, hogy a jelentkezőnek minden esetben pontosan két kártyát kell félretennie. Hogy ez így legyen, semelyik két kupacban nem szerepelhet ugyanaz az érték kettőnél többször, vagyis minden kupacban minden kártya legfeljebb egyszer szerepelhet. Ebből már adódik első tulajdonságunk:

1. bármely két különböző kupacot választva kell lennie pontosan egy olyan értéknek, amely mindkét kupacban szerepel.

Mivel egy kupacon belül csak különböző értékű lapok szerepelnek, ezért minden kupacon belül $\binom{4}{2}$ különböző értékekből álló értékpár van. Egyik ilyen pár sem szerepelhet két különböző kupacban, hiszen ha lenne két ilyen kupac, ezekre nem teljesülne az 1. tulajdonság. Tehát azon különböző értékekből álló értékpárok száma, ahol a pár mindkét tagja ugyanabban a kupacban szerepel: $13 \cdot \binom{4}{2} = \binom{13}{2}$. Ez megegyezik az összes különböző értékekből álló értékpárok számával, tehát az alábbi tulajdonságnak is teljesülnie kell:

2. bármely két különböző értéket választva kell lennie pontosan egy olyan kupacnak, melyben mindkét érték szerepel.

A trükk vizsgálatát egy kicsit félretéve, ismerkedjünk meg a projektív síkokkal. Legyen $\mathcal{P}$ egy tetszőleges halmaz, $\mathcal{E}$ pedig $\mathcal{P}$ bizonyos részhalmazainak halmaza. $\mathcal{P}$ elemeit pontoknak, $\mathcal{E}$ elemeit pedig egyeneseknek fogjuk hívni. Amennyiben egy

$P \in \mathcal{P}$ pont és $e \in \mathcal{E}$ egyenes esetén $P \in e$ teljesül, akkor azt mondjuk, hogy a P pont illeszkedik az e egyenesre. A $\Pi = (\mathcal{P}, \mathcal{E})$ párt *projektív síknak* nevezzük, ha az alábbi négy axiómának eleget tesz:

P1. bármely két különböző ponthoz pontosan egy olyan egyenes van, melyre mindkét pont illeszkedik,

P2. bármely két különböző egyeneshez pontosan egy olyan pont van, mely mindkét egyenesre illeszkedik,

P3. minden egyenesre illeszkedik legalább három különböző pont,

P4. minden pont legalább három különböző egyenesre illeszkedik.

A P1, P2 axiómák helyett a geometriai szóhasználattal élve azt is mondhatjuk, hogy két ponton át egyértelműen létezik az őket összekötő egyenes, illetve, hogy bármely két egyenesnek egyértelműen létezik metszéspontja. A P3, P4 axiómák az elfajuló esetek kizárására szolgálnak.

Szembetűnő a hasonlóság az első két axióma és a kártyakupacokra vonatkozó két tulajdonság között. Legyen $\mathcal{P}$ a 13 db kupacból álló halmaz. Definiáljuk továbbá a kupacok alábbi részhalmazait:

h_A: Azoknak a kupacoknak a halmaza, melyekben szerepel ász

h_2: Azoknak a kupacoknak a halmaza, melyekben szerepel 2-es

$\vdots$

h_K: Azoknak a kupacoknak a halmaza, melyekben szerepel király

Mivel a francia kártyában 13 különböző értékű lap van és mindegyik kupacban minden érték legfeljebb egyszer szerepelhet, ezért összesen 13 db 4-elemű részhalmazt definiáltunk a kupacokon. Legyen $\mathcal{E} = \{h_A, h_2, \cdots, h_K\}$, ekkor a $(\mathcal{P}, \mathcal{E})$-pár az 1. és 2. tulajdonság miatt kielégíti a P1, P2 axiómákat, és nyilvánvalóan kielégíti P3-at és P4-et is, tehát projektív síkot alkot. Az alábbi tétel fontos lesz a későbbiek során (a bizonyítás megtalálható pl. [14], [7]-ben vagy az interneten is elérhető [2]-ban):

5.2.1 Tétel: Ha a Π projektív síknak van olyan egyenese, melyre $n+1$ pont illeszkedik, akkor Π minden egyenesére $n+1$ pont illeszkedik, Π minden pontján át $n+1$ egyenes megy át, Π összesen n^2+n+1 pontot és ugyanennyi egyenest tartalmaz.

Az előző tétel alapján értelmes a következő definíció:

5.2.2 Definíció: A Π projektív sík rendje n, ha Π-nek létezik olyan egyenese, melyre $n+1$ pont illeszkedik. Ez esetben Π-t n-edrendű véges projektív síknak nevezzük.

A 12. osztályos tanulók foglalkozásán feladatként szerepelt a tétel, két segítő feladattal. Azon az órán a projektív sík P3 és P4 axiómái helyett az alábbi szerepelt:

P3'. Létezik négy általános helyzetű pont, vagyis négy olyan pont, melyek közül semelyik három nem esik egy egyenesre.

Nem nehéz belátni, hogy ezzel valóban helyettesíthetjük az elfajuló esetek kizárására szolgáló két axiómát (lásd [14]). A segítő feladatok, melyek megoldása [7]-ben megtalálható:

5.2.3 Feladat: Ha az x pont nem illeszkedik az e egyenesre, akkor x-re pontosan $|e|$ db egyenes illeszkedik.

5.2.4 Feladat: Ha x_1, x_2, x_3, x_4 általános helyzetű pontok, akkor van olyan n természetes szám, hogy a négy pont mindegyike $n+1$ egyenesre illeszkedik, és minden általuk meghatározott egyenes pontosan $n+1$ pontot tartalmaz.

A feladatok megoldása eléggé döcögősen ment, ennek fő oka szerintem az lehetett, hogy még az óra elején jártunk és csak ismerkedtek a fogalmakkal a gyerekek. Én a táblánál rajzokkal segítettem őket és ha valahol elakadtak, mutattam melyik axiómát próbálják meg használni. A tétel bizonyítása során a sík egyeneseinek, illetve pontjainak a számát már könnyen meghatározták.

Egy másik feladatban arra kerestük a választ, hogy vajon miért van szükség a P3 axiómára. Az elfajuló projektív síkokat könnyen megtalálták, és egyetértettek abban, hogy ezek még nem túlzottan érdekesek.

Hogy milyen n értékek esetén létezik n-edrendű projektív sík, illetve adott n esetén hány db egymástól lényegesen különböző (nem izomorf) sík létezik, máig megoldatlan probléma. Ha n prímhatvány, akkor véges testek segítségével tudunk n-edrendű síkot konstruálni (ez szintén megtalálható [14]-ben) és a sejtés az, hogy csak prímhatvány rendű síkok léteznek. A nemlétezésre vonatkozó legfontosabb eredmény a következő:

5.2.5 Tétel: (Bruck-Ryser) Ha $n \equiv 1, 2 \pmod 4$ és létezik n-edrendű projektív sík, akkor n előáll két négyzetszám összegeként.

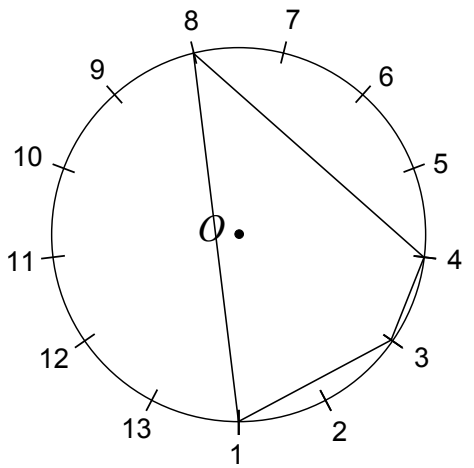
A tétel bizonyítása [14]-ben megtalálható.

Annyit azonban már mi is beláttunk, hogy ha hihetünk a bűvészünknek és tényleg kupacokba tudja osztani az 1. és 2. tulajdonságoknak megfelelően az 52-lapos francia kártyát, akkor létezik 3-rendű projektív sík, hiszen az előző oldalon definiált $(\mathcal{P}, \mathcal{E})$ pár kielégíti az axiómákat és $3^2 + 3 + 1 = 13$.

A továbbiakban ismertetünk egy módszert, mely [14]-ben is megtalálható és amelynek a segítségével véges projektív síkokat készíthetünk. Ismertetek néhány ezzel kapcsolatos tanítási tapasztalatot, majd megmutatjuk, hogyan kell a bűvésznek szétosztani a kártyákat, illetve honnan tudja, hogy melyik két kupacot kell kiválasztania.

A ciklikus modell

Legyen $\mathcal{S}$ az O középpontú körbe írt szabályos (n^2+n+1)-szög. Ha P és Q a sokszög két különböző csúcsa, akkor nevezzük a P és Q távolságának k-t, ha a rövidebb PQ ívhez tartozó középponti szög $k{\cdot}360°/(n^2+n+1)$. Legfeljebb hány csúcsát lehet kiválasztani S-nek, hogy bármely kettő távolsága különböző legyen? Mivel a sokszög csúcsai összesen $(n^2+n)/2 = \binom{n+1}{2}$ különböző távolságot határoznak meg, ezért legfeljebb $(n+1)$-et. Tegyük fel, hogy sikerült kiválasztanunk $(n+1)$ db csúcsot a megadott feltétellel és az általuk meghatározott részsokszöget jelöljük $\mathcal{R}$-rel (az ilyen részsokszögeket szokás *teljesen szabálytalan részsokszögnek* nevezni). A 2. ábrán az $n=3$ esetben berajzoltunk egy teljesen szabálytalan résznégyszöget.



5.2. ábra.

$\mathcal{R}$-nek O-körüli $k{\cdot}360°/(n^2+n+1)$ szögű elforgatottjait $(k=0,1,\ldots,n^2+n)$ jelöljük $\mathcal{R}_0,\mathcal{R}_1,\ldots,\mathcal{R}_{n^2+n}$-vel. Az $\mathcal{R}_i$ részsokszög csúcsainak a halmazát pedig r_i-vel.

A pontok, vagyis $\mathcal{P}$ legyen $\mathcal{S}$ csúcsainak a halmaza, az egyenesek pedig $\mathcal{E} = \{r_0, r_1, \cdots, r_{n^2+n}\}$. Tehát a $P \in \mathcal{P}$ pont pontosan akkor illeszkedik az $r_j \in \mathcal{E}$ egyenesre, ha P az $\mathcal{R}$ részsokszög $j{\cdot}360°/(n^2+n+1)$ szögű elforgatottjának az egyik csúcsa.

Megmutatjuk, hogy modellünk kielégíti a P1-P4 axiómákat. Legyen P, Q két különböző pont, melyek távolsága k. $\mathcal{R}$ csúcsai között minden távolság pontosan egyszer fordul elő, így pontosan egy olyan elforgatottja van, melynek P és Q is csúcsa. Ezzel beláttuk, hogy P1 teljesül.

Legyen $\mathcal{R}_m$ és $\mathcal{R}_l$ két különböző egyenes, ekkor $n^2+n+1 = n(n+1)+1$ páratlan volta miatt, az $\mathcal{R}_m$-et $\mathcal{R}_l$-be, illetve az $\mathcal{R}_l$-t $\mathcal{R}_m$-be vivő pozitív irányú forgatások közül az egyiknek a szöge kisebb mint 180°. Az indexeket választhatjuk úgy, hogy ez az $\mathcal{R}_m$-et $\mathcal{R}_l$-be vivő forgatás legyen és a szögét jelöljük $k{\cdot}360°/(n^2+n+1)$-val. Ekkor $k \in \{1,\ldots,(n^2+n)/2)\}$. Egy M pont pontosan akkor van rajta mindkét szóbanforgó egyenesen, ha $\mathcal{R}_m$-nek létezik egy olyan N csúcsa, melyre az NOM irányított szög $+k{\cdot}360°/(n^2+n+1)$. Ilyen M, N pontpár viszont pontosan egy van $\mathcal{R}_m$ csúcsai között, hiszen ott $\mathcal{R}$ csúcsaihoz hasonlóan minden távolság pontosan egyszer lép fel.

Ezzel P2 teljesülését is beláttuk, P3 és P4 teljesülése pedig $n \geq 2$ esetén nyilvánvaló.

Az így kapott véges projektív síkokat szokás *ciklikus síkoknak* nevezni. Mivel a 2. ábrán látható szabályos 13-szögben a berajzolt (1,3,4,8-csúcsok által meghatározott) résznégyszög teljesen szabálytalan, ezért létezik 3-rendű ciklikus sík. Megmutatható, hogy lényegében ez az egyetlen 3-rendű projektív sík, vagyis bármely más, a P1-P4 axiómákat teljesítő 13 pontból álló modell pontjai és egyenesei, illeszkedéstartó módon megfeleltethetők a mi példánk pontjainak és egyeneseinek. Ez azonban nincs mindig így, pl. 9-rendű projektív síkból négy különböző létezik, melyek közül csak az egyiket kapjuk meg a fent ismertetett eljárással.

Bizonyítható, hogy ha n prímhatvány, akkor a szabályos (n^2+n+1)-szög csúcsai közül mindig kiválasztható egy teljesen szabálytalan $(n+1)$-szög (lásd [14]), és az így kapott ciklikus sík lényegében ugyanaz, mint a korább említett (de nem részletezett) véges testek segítségével konstruálható sík.

A 8. osztályosoknak tartott második szakkörön az alábbi feladatot kapták a tanulók:

5.2.6 Feladat: Tud-e hét jóbarát a hét napjaira hét találkozót szervezni úgy, hogy bármely két baráthoz pontosan egy olyan találkozó legyen, melyen mindketten résztvesznek?

A feladatot senki sem oldotta meg, igaz nem is hagytam rá elég időt. Csak azt szerettem volna érzékeltetni, hogy a feladat egyáltalán nem magától értetődő. Ezután a táblára rajzoltam egy szabályos 7-szöget és megkérdeztem a gyerekeket:

5.2.7 Feladat: Legfeljebb hány csúcsát lehet úgy kiválasztani a 7-szögnek, hogy bármely két kiválasztott pont távolsága különböző legyen?

Talán mert a rendes tanórán éppen kombinatorikát tanultak, hamar rájöttek, hogy 4 csúcsot már nem lehet kiválasztani, hármat viszont igen. Berajzoltam az általuk javasolt három csúcs által meghatározott háromszöget, és feladtam nekik a következő feladatot:

5.2.8 Feladat: Bizonyítsd be, hogy a háromszöget a 7-szög középpontja körül $k{\cdot}360°/\ 7$ szöggel elforgatva $(k = 0, 1, \ldots, 6)$ kapott 7 db háromszög közül bármely kettőnek pontosan egy közös csúcsa van.

A feladatot szerencsére többen is megoldották. Volt aki a csúcsok elnevezése után felírta a 7 db háromszög csúcsait, és egyenként nézte meg, hány közös eleme lehet egy-egy csúcshármasnak. Voltak viszont olyan megoldások is, melyek a háromszög *teljesen szabálytalan* voltát használták ki, és nyugodtan lehetett volna őket általánosítani.

Ezután azt tanácsoltam a diákoknak, próbálják meg most a hét jóbarát feladatát. Szinte rögtön érkezett a válasz az egyik tanulótól: "De hiszen ez ugyanaz!". Az indoklása is helyes volt: a sokszög hét csúcsát a hét napjainak megfeleltetve, az egyes háromszögek pontosan azt mutatják meg, hogy melyik barát, melyik három nap menjen el az aznapi találkozóra.

A 12. osztályosoknál más felvezetéssel került elő a ciklikus modell. Miután a véges projektív síkok kombinatorikus tulajdonságait megbeszéltük, és elmondtam nekik a Bruck-Ryser tételt, még mindig adós voltam azzal, hogy egyáltalán létezik-e nem elfajuló véges projektív sík. A Fano-sík bemutatása után azt a kérdést vizsgáltuk, hogy vajon "görbe egyenes" nélkül is le lehet-e rajzolni egy projektív síkot. Az alábbi tétel felvetése Sylvestertől, és tőle függetlenül Erdőstől származik:

5.2.9 Tétel: A sík bármely nem egy egyenesre eső véges $\mathcal{P}$ ponthalmazából kiválasztható két pont úgy, hogy az általuk meghatározott egyenes nem tartalmaz több $\mathcal{P}$-beli pontot.

A tétel igazolásához, Gallai Tibor bizonyításából kiindulva, először ezt a segítséget kapták a tanulók:

Legyen $\mathcal{L}$ azoknak az egyeneseknek a halmaza, melyek legalább két $\mathcal{P}$-beli pontot tartalmaznak. Válasszuk ki azt a $p \in \mathcal{P}$, $l \in \mathcal{L}$ pont-egyenes párt, melyre $p \notin l$ és p-nek az l-től vett távolsága minimális. Bizonyítsuk be, hogy ez az e-egyenes csak két $\mathcal{P}$-beli pontot tartalmazhat. Ez után az ötlet után a bizonyítás már nem nehéz, indirekt módon kell folytatni [7]:

Tegyük fel, hogy létezik $x_1, x_2, x_3 \in e$ és ezek közül x_2 a középső. Ekkor az x_1x_2p és x_2x_3p háromszögek egyikében x_2-nél legalább 90°-os szög van. Ebben a háromszögben az x_2-höz tartozó magasság lesz a legkisebb magasság, vagyis kisebb mint p l-től vett távolsága, ami ellentmondás.

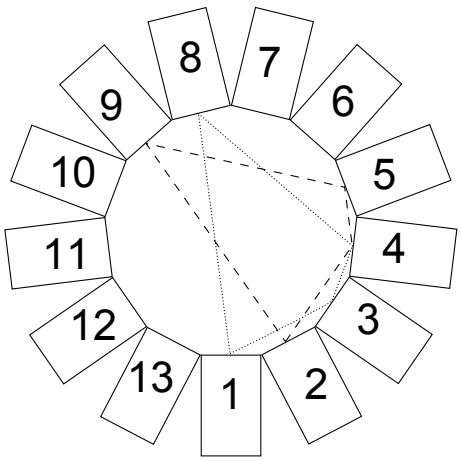
A bizonyításhoz annyi segítségre még szüksége volt a gyerekeknek, hogy elárultam: Próbáljanak az x_1x_2p és x_2x_3p háromszögek egyikében olyan (nem illeszkedő) csúcs-oldal párt találni, melyek egymástól vett távolsága kisebb mint p l-től vett távolsága.

Ez után már mindenki számára világos volt, hogy "görbe egyenesek" nélkül legfeljebb 1-rendű véges projektív síkot tudunk rajzolni, az viszont az elfajuló esetek közé tartozik. Hogy akkor mégis hogyan lehet nem elfajuló projektív síkokat konstruálni, ehhez adtam fel feladatnak, hogy a két oldallal korábban bemutatott módszerrel, szabályos 13-szög esetén, a 3-rendű projektív síkot kapjuk. Az axiómák teljesülését önállóan látták be a gyerekek. Ezek után megkérdeztem tőlük a következőt:

5.2.10 Feladat: Adott egy szabályos 43-szög a síkon. Igaz-e, hogy bárhogyan választjuk ki 7 csúcsát, a kiválasztott csúcsok által meghatározott 21 távolság között mindig lesz két egyforma?

Több percig senki sem szólt semmit a hallgatóság közül. Végül emlékeztettem őket a korábban említett Bruck-Ryser tételre, ami után egyszerre többen is mondták a helyes megoldást: ha nem lenne két egyforma távolság, akkor a 13-szögnél látott módszerrel 6-odrendű projektív síkot készíthetnénk, de a 6 nem áll elő két négyzetszám összegeként. Ezzel a projektív síkok létezésére vonatkozó komplikált feltételünk alkalmazást nyert. Itt jegyezzük meg, hogy visszafelé nem igaz a tétel állítása. $10 = 9 + 1$, viszont 10-edrendű projektív sík nem létezik.

Térjünk vissza a trükk magyarázatára.



5.3. ábra.

A kártyákat a trükk megkezdése előtt az ábrán látható módon úgy oszjuk szét a 13 kupacba, hogy bármely 4 azonos értékű kártya a 2. ill. 3. ábrán berajzolt teljesen szabálytalan négyszög egy elforgatottjának a csúcsait adja. Például az 1.,3.,4.,8. kupacokba kerüljenek az ászok, a 2.,4.,5.,9. kupacokba a 2-esek, ... végül a 13.,2.,3.,7. kupacokba a királyok.

Ekkor az az állítás, hogy a 3. kupacban szerepel ász, úgy is megfogalmazható, hogy a 3. kupacnak megfelelő pont rajta van az ászok által meghatározott egyenesen. Tulajdonképpen minden kártyalap megfeleltethető a 3-rendű ciklikus síkon egy pont-egyenes illeszkedés

párnak. Ezek száma valóban 52, hiszen a síkon 13 pont van, melyek mindegyike pontosan 4 különböző egyenesre illeszkedik.

Amikor a néző kiválaszt két kupacot, az egyértelműen meghatározza a négyszög egyik elforgatottját. A bűvésznek csak oda kell képzelnie a négyszög másik két csúcsát és az ott található két kupacot kell választania. Mivel az így kiválasztott 2-2 kupac egy egyenesre esik, ezért mindkét kupacpárban ugyanaz az érték fog megegyezni. A bűvésznek ki kell választania saját kupacaiból a két egyforma kártyát és ezeket kell a kezében tartania. Mivel csak a kártyák egymáshoz viszonyított helyzete számít, ezért az asztal elforgatása semmiben sem befolyásolja a mutatványt.

Az alábbi táblázat azt mutatja, hogy a fenti módszerrel mely kártyák kerülnek az egyes kupacokba. Természetesen sok más elrendezés is lehetséges, nem számít ugyanis, hogy az egyes értékeket, a négyszög mely elforgatottjához rendeljük. A táblázat k. oszlopában a k. kupacban szereplő lapok szerepelnek, a színek feltüntetése nélkül.

7	8	9	10	J	D	K	A	2	3	4	5	6
J	D	K	A	2	3	4	5	6	7	8	9	10
D	K	A	2	3	4	5	6	7	8	9	10	J
A	2	3	4	5	6	7	8	9	10	J	D	K

Végül álljon itt néhány egyszerűbb, a trükkhöz kapcsolódó feladat:

5.2.11 Feladat: Keressünk teljesen szabálytalan

(a) 5-szöget, a szabályos 21-szögben.

(b) Hány db, forgatással egymásba nem vihető, teljesen szabálytalan 4-szög választható ki a szabályos 13-szög csúcsai közül?

Az (a) feladatban legyenek a 21-szög csúcsai rögzített körüljárás mellett: $P_1, P_2, \ldots, P_{21}$. Ekkor nem nehéz belátni, hogy a $\{P_1, P_2, P_5, P_{15}, P_{17}\}$ csúcsok egy teljesen szabálytalan 5-szöget határoznak meg.

A (b) feladatban legyenek a 13-szög csúcsai rögzített körüljárás mellett: $P_1, P_2, \ldots, P_{13}$. Ekkor $\{P_1, P_2, P_4, P_{10}\}$ és $\{P_1, P_2, P_5, P_7\}$, valamint tükörképeik: $\{P_1, P_2, P_6, P_{12}\}$ és $\{P_1, P_2, P_9, P_{11}\}$, négy különböző teljesen szabálytalan 4-szög. Az általánosság megszorítása nélkül feltehetjük, hogy a keresett négyszög tratalmazza a $\{P_1, P_2\}$ csúcsokat, ezek után szisztematikus próbálgatással könnyen megmutatható, hogy az összes lényegesen különböző megoldást megtaláltuk.

5.2.12 Feladat: Előadható-e a trükk olyan kártya-elrendezés mellett, ahol minden kupacban négy különböző színű kártya szerepel?

Igen. Vegyük észre, hogy a fenti táblázat minden sorában minden elem különböző. Így, ha az egyes sorokba egyforma színű kártyákat teszünk, és ennek megfelelően alakítjuk ki a kupacokat, akkor teljesül a kívánt feltétel.

5.2.13 Feladat: Mutassuk meg, hogy a néző és a bűvész által kiválosztott 4 kupacban minden érték szerepel.

A kiválasztott 4 kupac megfelel a 3-rendű projektív sík egy egyenesének. Így a feladat állítása a P2 axiómából következik.

5.2.14 Feladat: A trükk úgy is elvégezhető, hogy a bűvész nem két kupacot, hanem egyből 2 kártyát választ, melyek értéke megegyezik a néző által félretett lapok értékével. Hogyan lehetséges ez?

A kártyák szétosztásánál ügyeljünk arra, hogy a táblázat 4. sorában szereplő lapok kerüljenek alulra, a 3. sorban lévők alulról a második helyre, a 2. sorban lévők alulról a harmadik helyre, míg az 1. sorban lévő lapok legfelülre.

Így ha a bűvésznek a k-adik és $(k+1)$-edik kupacokból kell húznia, modulo 13 (mert a néző a $(k-2)$-edik és $(k+5)$-ödik kupacokat választotta), akkor minden k érték esetén felülről a 3. ill. 2. lapokat kell választania.

Ezeket az értékeket azonban nem kell mind a hat fellépő távolsághoz megjegyeznünk, elég ha azt tudjuk, hogy mindig a teljesen szabálytalan négyszög (vagyis a szóbanforgó egyenes) azon csúcsában (abban a kupacban) van legalul az egyenest reprezentáló lap (az a lap, amely az egyenes mind a négy kupacában szerepel), melynél a 6 és a 2 hosszú oldalak találkoznak. A négyszög csúcsain az óramutató járásával ellentétes irányba haladva, mindig az előző csúcsnál lévőnél eggyel magasabb szinten lesz a reprezentáns lap (modulo 4 számolva).

5.3. Additív kombinatorikai feladatok

Az alábbi feladatokat, ugyanebben a sorrendben, a 8. osztályosok szakkörén oldottuk meg. Nem a szakdolgozatom korábbi fejezeteiben használt tételeket néztük meg, hanem annál jóval egyszerűbb állításokat, de a problémák jellege hasonló. Összeghalmazok méretéről szeretnénk valamit mondani. A feladatok természetes módon általánosíthatók tetszőleges rendezett csoportra, mi erről az órán nem beszéltünk, végig az egész számok additív csoportjában dolgoztunk.

5.3.1 Feladat: Két szokásos dobókockával dobva, hányféle lehet a dobott számok összege?

5.3.2 Feladat: Az 1, 2, 3, 4, 5, 6 számok helyett tudnál-e úgy írni számokat a kockákra (mindkét kockára ugyanazt a hat számot), hogy a dobott számok összege többféle lehessen? Így legfeljebb hányféle különböző összeg lehetséges?

Az első feladattal természetesen nem volt sok probléma, bár volt akinek figyelmetlenségből 12 jött ki, 11 helyett. A 2. feladatnál először senki sem talált olyan megoldást, ahol 21 különböző összeg lehetséges. Egyelőre én sem mutattam nekik ilyen példát, hanem biztattam őket felső korlát találására. Először $6 \cdot 6 = 36$-ot tippeltek. Megbeszéltük ennek a gondolatmenetnek a hibáját, hogy bizonyos összegeket kétszer számol. Rögtön jött a következő tipp, a $36/2 = 18$. Ez sem volt jó, hiszen

az előbb nem minden esetet számoltunk kétszer. Itt rájöttek, hogy külön kellene számolni azokat az összegeket, melyek két különböző szám összegeként állnak elő, és azokat, melyeket akkor kapunk, ha mindkét kockával ugyanazt a számot dobjuk. Így végül kitalálták a $\binom{6}{2} + 6 = 21$-es felső korlátot. Példánk viszont még nem volt, ezért elmondtam egy másik bizonyítást:

Legyen a dobókockákra írt számok halmaza $A = \{a_1, a_2, a_3, a_4, a_5, a_6\}$, ahol $i \neq j$ esetén $a_i \neq a_j$. Azt vizsgáljuk, hogy az $A + A = \{a_i + a_j | i, j = 1, 2, \ldots, 6\}$ halmaz elemszáma milyen nagy lehet. Természetesen ezt a kérdést nem csak 6 elemű halmazok esetén tehetjük fel. Hogyha $A = \{a_1\}$, akkor világos, hogy $|A+A| = 1$. $A = \{a_1, a_2\}$ esetén legfeljebb 2-vel nő $A+A$ elemszáma, hiszen két új összeg jelenik meg, melyekben a_2 szerepel. Általában ha $A = \{a_1, a_2, \ldots a_k\}$, akkor $A + A$ elemszáma legfeljebb k-val nő az $A = \{a_1, a_2, \ldots, a_{k-1}\}$ esethez képest. Így felső korlátnak szintén $1 + 2 + 3 + 4 + 5 + 6 = 21$-et kapunk az $|A| = 6$ esetben. Arra a kérdésemre, hogy mégis hogyan válasszuk meg az $a_1, a_2, \ldots, a_6$ számokat ennek elérésére, már érkezett a válasz a gyerekektől, hogy legyen $a_2 + a_1 > a_1 + a_1$, $a_3 + a_1 > a_2 + a_2$, $\ldots$, $a_6 + a_1 > a_5 + a_5$.

Ha $a_1 = 1$-ből indulunk ki és $a_2, a_3, \ldots, a_6$-nak mindig az előbb kitalált feltételeknek megfelelő legkisebb egész számot választjuk, akkor az $A = 1, 2, 4, 8, 16, 32$ halmazhoz jutunk, amire valóban teljesül, hogy $|A + A| = 21$. Hiszen a $2^k + 2^l$ alakú számok egyféleképpen írhatók fel két kettőhatvány összegeként ($k, l \in \mathbb{N}$). Ugyanígy jó választás lenne például $A = 1, 3, 9, 27, 81, 243$.

Azt is megfigyelhetjük, hogy ha egy $A = \{a_1, a_2, \ldots, a_n\}$ halmaz esetén $|A+A| = M$, akkor az $A' = A + \{k\} = \{a_1 + k, a_2 + k, \ldots, a_n + k\}$ halmazra is teljesül, hogy $|A' + A'| = M$. Ezt az állítást már a gyerekek igazolták, és így végtelen sok példát sikerült megadnunk, ahol az összeghalmaz mérete maximális.

5.3.3 Feladat: Legfeljebb hányféle lehet az összeg, ha nem kell mindkét kockára ugyanazt a hat számot írni?

Úgy látszik az előző feladat megoldása során ráéreztek a tanulók erre a feladattípusra, mert hamar kaptam a visszajelzéseket, miszerint 36 a megoldás. Egy lehetséges példa a felsőkorlát elérésére, ha $A = \{1, 2, 3, 4, 5, 6\}$ és $B = \{1, 7, 13, 19, 25, 31\}$ (ahol A és B az egyes kockákra írt számok halmaza).

5.3.4 Feladat: Lehetséges-e úgy írni számokat a kockákra, hogy a dobott számok összege kevesebb mint 11-féle lehessen?

Ez a feladat viszont nehéznek bizonyult. Próbálgatások útján ugyan kialakult a gyerekekben a sejtés, hogy nem lehet, de bizonyítani nem tudták. Segítségül azt tanácsoltam, hogy rendezzék növekvő sorrendbe az egyes kockákra írt számokat. Legyenek ezek:
$a_1 < a_2 < a_3 < a_4 < a_5 < a_6$ és $b_1 < b_2 < b_3 < b_4 < b_5 < b_6$.

Ekkor biztos, hogy pl. $a_1 + b_1 < a_6 + b_6$. Ha sikerülne e közé a két összeg közé még 9-et találnunk, szigorúan növekvő sorrendben, akkor készen lennénk. Ezt már ki tudták találni a gyerekek. 11 biztosan különböző elem pl. a következő:
$a_1 + b_1 < a_1 + b_2 < a_1 + b_3 < \ldots < a_1 + b_6 < a_2 + b_6 < a_3 + b_6 < \ldots < a_6 + b_6$.

Megbeszéltük, hogy ugyanez a bizonyítás működik $a_k = b_k$ ($k = 1, 2, \ldots, 6$) esetén is, tehát a felső korláttal ellentétben az alsó korlátnál nincs különbség, ha a két kocka számozásának meg kell egyeznie.

5.3.5 Feladat: Igaz-e, hogy minden $11 \leq k \leq 21$, $k \in \mathbb{Z}$ szám esetén megadható úgy egy 6 elemű $A \subset \mathbb{Z}$ halmaz, hogy mindkét kockára az A-beli számokat írva, a dobott számok összege pontosan k-féle lehet?

A $k = 11$ és $k = 21$ esetre már tudjuk, hogy létezik ilyen A halmaz. A második feladatnál a maximális megoldás keresése közben több más k értékre találtak példákat a gyerekek. Ezeket összegyűjtöttük, a hiányzó 4 eset megoldásához pedig 4-5 fős csapatokat jelöltem ki. A hangzavar ugyan nagy volt, de a csoportok eredményesek voltak, így végül sikerült minden lehetséges értékre példát találnunk. Az óra végén eddigi tapasztalataink alapján a következő sejtést sikerült megfogalmazni:

5.3.6 Állítás: Minden $k \in \mathbb{Z}$, $2n - 1 \leq k \leq \binom{n+1}{2}$ szám esetén megadható olyan n elemű $A \subset Z$ halmaz, hogy $|A + A| = k$.

A következőkben a témakör lehetséges folytatását dolgoztam ki. Segítő feladatokon keresztül eljutunk pár bonyolultabb feladat, például az előző sejtés, bizonyításához.

5.3.7 Feladat: Valaki azt állította, hogy meg tud adni úgy egy n elemszámú A halmazt, hogy $|A + A| = k$. Mutassuk meg, hogy ekkor meg lehet adni egy $n + 1$ elemszámú A' halmazt úgy, hogy $|A' + A'| = k + n + 1$.

Az ötlet ugyanaz, mint az első óra második feladatában: ha az A halmaz $a_1 < a_2 < \ldots < a_n$ elemeihez egy elég nagy a_{n+1} elemet veszünk hozzá ($a_{n+1} > a_n + a_n - a_1$), akkor a k db $A + A$-beli összeg mellé $n + 1$ db új összeg fog megjelenni $A' + A'$-ben. Nézzünk egy példát, hogy ez mit is jelent:

Az $n = 6$ esetben minden $11 \leq k \leq 21$, $k \in \mathbb{Z}$ szám esetén megadtunk egy megfelelő A halmazt. De így az $n = 7$ esetben is tudunk ilyen halmazt mutatni, valahányszor $18 \leq k \leq 28$. Tehát az $n = 7$ esetben már csak a $k = 13, 14, \ldots, 17$ esetekre kell koncentrálnunk. $k = 13$ esetén $A = \{1, 2, \ldots, 7\}$ megfelelő, erre könnyű rájönni, hiszen az $n = 6$ esetben $A = \{1, 2, \ldots, 6\}$ a minimumot adta. Elég a 7-est megváltoztatni $8, 9, \ldots, 11$-re és ez megoldja a maradék 4 esetet.

Az eddigiek alapján feladatunkat az alábbi két állítás bizonyítására bonthatjuk:

1. Legyen $k \in \mathbb{Z}$ és $2n - 1 \leq k \leq 3n - 4$. Ekkor megadható olyan n elemű A halmaz, hogy $|A + A| = k$.

2. Legyen $k \in \mathbb{Z}$ és $3n - 3 \leq k \leq \binom{n+1}{2}$. Ekkor megadható olyan n elemű A halmaz, hogy $|A + A| = k$.

Az elsőt könnyű megoldani, ugyanaz a trükk működik, mint az $n = 7$ esetben. Vagyis az $A = \{1, 2, \ldots, n-1\} \cup \{a_n\}$, $a_n = n, n+1, \ldots, 2n-3$ halmazok megfelelők lesznek. Méghozzá úgy, hogy $a_n = n + k$ esetén $|A + A| = 2n - 1 + k$, valahányszor $k \in \{0, 1, \ldots, n - 3\}$. Részletesebben: $a_n = n + k$ esetén $A + A = \{2, 3, \ldots, 2n + k - 1, 2n + 2k\}$.

A 2. állítást $n = 6$-ra és 7-re már beláttuk, és könnyen láthatjuk, hogy $n = 1$ és 2 esetén is igaz. Szeretnénk megmutatni, hogy ha $|A| = n$ esetén teljesül az állítás, akkor abból következik, hogy $|A| = n + 1$ esetén is teljesül. Ha ez sikerül, készen leszünk, hiszen így $n = 2$-ből következik a hiányzó $n = 3$ eset, abból a hiányzó $n = 4$ eset és így tovább. Ezzel minden pozitív egész n-re sikerülne belátni az állítást.

Természetesen, ha a hallgatóság már sok teljes indukciós bizonyítást látott, akkor ezt nem részletezném ennyire, de középiskolában ez még egyáltalán nem biztos.

Mit is jelent az, hogy $|A| = n$-re teljesül az állítás? Azt jelenti, hogy a $3n - 3 \leq k \leq \binom{n+1}{2}$ esetekben meg tudunk adni olyan A halmazt, hogy $|A + A| = k$. A már igazolt 1. állítás miatt ez akkor is igaz, ha $2n - 1 \leq k \leq 3n - 4$. Ekkor az előző feladatot használva, minden $2n - 1 + (n + 1) = 3n \leq k \leq \binom{n+1}{2} + (n + 1) = \binom{n+2}{2}$ esetben meg tudunk adni úgy egy $n + 1$ elemszámú A' halmazt, hogy $|A' + A'| = k$, ez pedig pont a 2. állítás az $|A| = n + 1$ esetben.

Úgy gondolom ez a feladat azért is tanulságos lehet, mert a teljes indukció nem oldja meg egyből a feladatot, csupán annak egy jelentős részét.

Az első óra feladatainak felelevenítésére szolgálhat a következő:

5.3.8 Feladat: Legyen A és B két nem feltétlenül azonos elemszámú halmaz. Bizonyítsuk be, hogy $|A| + |B| - 1 \leq |A + B| \leq |A||B|$.

Az alsó korlát igazolását azért érdemes átismételni, mert ehhez kapcsolódik a következő:

5.3.9 Feladat: Bizonyítsuk be, hogy $2 \leq |A|, |B|$ esetén ha $|A+B| = |A|+|B|-1$, akkor A és B azonos differenciájú számtani sorozat.

Jusson eszünkbe, hogy a szokásos dobókockánál, ahol a lapokon az $\{1, 2, 3, 4, 5, 6\}$ számok szerepelnek, valóban $6 + 6 - 1 = 11$-féle lehet a két kockával dobott számok összege.

Legyen $|A| = k$ és $|B| = m$. Az általánosság megszorítása nélkül feltehetjük, hogy $k \leq m$. Legyen $A = \{a_1 < a_2 < \ldots < a_k\}$ és $B = \{b_1 < b_2 < \ldots < b_m\}$. Az alábbi táblázatban $A + B = \{a + b \mid a \in A,\ b \in B\}$ összes lehetséges eleme szerepel, olyan elrendezésben, hogy bármely elem felső, illetve jobb oldali szomszédja nagyobb az adott elemnél. Ezt a tulajdonságot nem árulnám el a gyerekeknek, inkább megvárnám amíg maguktól felfedezik. Az előző feladathoz kapcsolódóan, többféleképpen is mutathatunk $m + k - 1$ db biztosan különböző elemet táblázatunkban.

$$\begin{array}{cccccc}
a_k + b_1 & a_k + b_2 & a_k + b_3 & \ldots & a_k + b_{m-1} & a_k + b_m \\
a_{k-1} + b_1 & a_{k-1} + b_2 & a_{k-1} + b_3 & \ldots & a_{k-1} + b_{m-1} & a_{k-1} + b_m \\
\vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\
a_2 + b_1 & a_2 + b_2 & a_2 + b_3 & \ldots & a_2 + b_{m-1} & a_2 + b_m \\
a_1 + b_1 & a_1 + b_2 & a_1 + b_3 & \ldots & a_1 + b_{m-1} & a_1 + b_m
\end{array}$$

Tegyük fel, hogy $|A + B| = m + k - 1$. Ilyenkor rengeteg egybeesésnek kell szerepelni az $m \cdot k$ db elem között, a gyerekeket meg lehet kérni, hogy keressenek ilyen egybeeséseket. Vegyünk négy tetszőleges elemet, melyek egy 2×2-es négyzet négy csúcsát alkotják:

$$\begin{array}{cc}
a_{i+1} + b_j & a_{i+1} + b_{j+1} \\
a_i + b_j & a_i + b_{j+1}
\end{array}$$

Hogy ha $a_{i+1}+b_j = a_i+b_{j+1}$ nem teljesülne, akkor $a_i+b_j < a_{i+1}+b_j < a_{i+1}+b_{j+1}$ és $a_i + b_j < a_i + b_{j+1} < a_{i+1} + b_{j+1}$ miatt ez négy különböző értékű elem, melyeket könnyen kiegészíthetünk összesen $k+m$ db különböző értékű elemre, ami ellentmond

a feltételünknek. Pl.: $\{a_i + b_j, a_{i+1} + b_j, a_i + b_{j+1}, a_{i+1} + b_{j+1}\} \cup \{a_{i-1} + b_j, a_{i-2} + b_j, \ldots, a_1 + b_j\} \cup \{a_1 + b_{j-1}, a_1 + b_{j-2}, \ldots, a_1 + b_1\} \cup \{a_{i+2} + b_{j+1}, a_{i+3} + b_{j+1}, \ldots, a_k + b_{j+1}\} \cup \{a_k + b_{j+2}, a_k + b_{j+3}, \ldots, a_k + b_m\}$ egy ilyen kiegészítés.

Ebből az észrevételből már következik, hogy az egyforma elemek átlós egyenesek mentén helyezkednek el: $a_i + b_j = a_{i'} + b_{j'}$ pontosan akkor, ha $i + j = i' + j'$.

Nézzük, hogy ez milyen egyenlőségeket jelent az első két oszlopra nézve: $a_k + b_1 = a_{k-1} + b_2$, $a_{k-1} + b_1 = a_{k-2} + b_2$, $\ldots$, $a_2 + b_1 = a_1 + b_2$. Ezt a $k - 1$ db egyenletet átrendezve kapjuk, hogy: $b_2 - b_1 = a_2 - a_1 = a_3 - a_2 = \ldots = a_k - a_{k-1}$. Tehát A elemei $b_2 - b_1$ differenciájú számtani sorozatot alkotnak.

Az alsó két sort vizsgálva az alábbi $m-1$ db egyenleteket kapjuk: $a_2+b_1 = a_1+b_2$, $a_2 + b_2 = a_1 + b_3$, $\ldots$, $a_2 + b_{m-1} = a_1 + b_m$. Ezeket átrendezve adódik: $a_2 - a_1 = b_2 - b_1 = b_3 - b_2 = \ldots = b_m - b_{m-1}$. Tehát B elemei $a_2 - a_1$ differenciájú számtani sorozatot alkotnak. Mivel $b_2 - b_1 = a_2 - a_1$, ezzel a feladat állítását beláttuk.

5.4. Összefoglalás

Az additív kombinatorikai feladatokkal szívesen foglalkoztak a gyerekek. Szerencsés véletlen, hogy a Matematika Határok Nélkül versenyen "Kockacsata" néven, a legtöbb gyerek már találkozott olyan feladattal, ahol saját számozású dobókockákat kellett készíteniük. A rendes tanórák kombinatorika és valószínűségszámítás anyagrészét, úgy érzem, jól egészítették ki a kipróbált feladatok. Új trükköket is tanultunk, és úgy gondolom, a felvázolt folytatás is hasznos lehet pl. a teljes indukció gyakorlásához, vagy a versenyekre való felkészüléshez.

Véges geometriákkal a 8. osztályban keveset foglalkoztunk, és tulajdonképpen ki se mondtuk, hogy erről lenne szó. Amit csináltunk, az viszont tetszett a gyerekeknek, mivel segítségével meg tudtak oldani egy olyan feladatot, ami elsőre nehéznek tűnt. Itt is hallottak olyan ötleteket, melyek később alkalmazásra kerültek, pl. körmérkőzések szervezésére, egy másik órán ismét egy szabályos sokszögbe rajzolt alakzat elforgatottjait használtuk.

A 12. osztályosok közül volt, aki már hallott véges geometriákról, és a többiek is különösen érdeklődők voltak. Arra az órára nagyon sok feladattal készültem, és ezek közül néhányra nem maradt idő. Mégis, úgy gondolom, sikerült egy kis betekintést nyújtanom a témába, miközben még egy szép, euklideszi tételt is bebizonyítottunk. A táborba való lejutásért egész évben nagy versengés és készülődés van a gyerekek között, így nem csoda, hogy a gyerekek a legkülönfélébb matematikai témákra is nyitottak. Ennek a kíváncsiságnak a kielégítésére néha szükség van olyan problémák bemutatására is, melyek túlmutatnak a középiskolai matematikán. Biztos vagyok benne, hogy ez, főleg a 12. évfolyamon, a gyerekek pályaválasztását is befolyásolja. Információt, és reményeim szerint, kedvet kapnak a matematikával foglalkozó szakokhoz.

A bemutatott kártyatrükk bevezetést nyújt a véges projektív síkok, ezen belül főként a ciklikus síkok vizsgálatához. Továbbá bízom benne, hogy ha olyan tanulónak mutatja be valaki a trükköt, aki a matematikával nem nagyon, viszont a kártyatrükkökkel szimpatizál, és utánaolvas a megoldásnak, máris tanult valami matematikát, ráadásul önszántából.

Irodalomjegyzék

[1] Ambrus András: *Bevezetés a matematika-didaktikába*, Egyetemi jegyzet, ELTE Eötvös Kiadó, 2004.

[2] Bérczi Gergely, Gács András és Szőnyi Tamás: Véges projektív síkok, *Új matematikai mozaik* (szerk.: Hraskó András), Typotex Kiadó, Budapest, 2002. vagy http://www.tankonyvtar.hu/konyvek/uj-matematikai-mozaik/uj-matematikai-mozaik-081030-26

[3] A. Blokhuis, Kiss Gy., Kovács I., A. Malnic, D. Marusic és Ruff J.: *Semiovals contained in the union of three concurrent lines*, J. Comb. Designs 15 (2007), 491-501.

[4] Csajbók Bence: *Egy kártyatrükk és ami mögötte van*, Középiskolai Matematikai és Fizikai Lapok 60 (2010), 258-263.

[5] Csajbók Bence és Kiss György: *Notes on semiarcs*, Mediterr. J. Math. (2010) közlésre benyújtva

[6] J. M. Dover: *Semiovals with large collinear subsets*, J. Geom. 69 (2000), 58-67.

[7] Elekes György: *Véges matematika*, Egyetemi jegyzet, ELTE, 2002.

[8] D. J. Grynkiewicz: *On extending Pollard's Theorem for t-representable sums*, Israel J. Math. 177 (2010), 413-440.

[9] X. Hubaut: *Limitation du nombre de points d'un (k,n)-arc regulier d'un plan projectif fini*, Atti. Accad. Naz. Lincei Rend. 8 (1970), 490-493.

[10] Kárteszi Ferenc: *Bevezetés a véges geometriákba*, Akadémiai Kiadó, Budapest, 1972.

[11] Kiss György: *Small semiovals in PG(2,q)*, J. Geom. 88 (2008), 110-115.

[12] Kiss György: *A survey on semiovals*, Contrib. Discrete Math. 3 (2008), 81-95.

[13] Kiss György és Ruff János: *Notes on small semiovals*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 47 (2004), 97-105.

[14] Kiss György és Szőnyi Tamás: *Véges Geometriák*, Polygon Kiadó, Szeged, 2001.

[15] J. M. Pollard: *A generalization of the Theorem of Cauchy and Davenport*, J. London Math. Soc. 8 (1974), 460-462.

[16] Pólya György: *Indukció és analógia*, Gondolat Kiadó, Budapest, 1988.

[17] Pólya György: *A gondolkodás iskolája*, Akkord Kiadó, Budapest, 2000.

[18] T. Tao és V. Vu: *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics 105, Cambridge University Press, 2009.

[19] J. A. Thas: *On semi ovals and semi ovoids*, Geom. Dedicata 3 (1974), 229-231.