Eötvös Loránd Tudományegyetem
Természettudományi Kar

Fejezetek a kombinatorikus számelméletből

Szakdolgozat

Madarasi Adrienn
Matematika BSc
Alkalmazott matematikus szakirány

Témavezető:

Dr. Gyarmati Katalin

Algebra- és számelmélet tanszék

Budapest
2016

Tartalomjegyzék

1. Köszönetnyilvánítás

Szeretnék köszönetet mondani témavezetőmnek, Gyarmati Katalinnak azért, hogy hasznos formai és tartalmi tanácsaival, magyarázataival nagy segítséget nyújtott a szakdolgozat írásában.

2. Bevezetés

A kombinatorikus számelméletben szereplő problémák gyakran visszavezethetőek gráfelméletre. A bizonyítások sokszor elemiek, ugyanakkor a nyert eredmények általában élesek és jól használhatóak.

Szakdolgozatom célja, hogy betekintést nyújtson a gráfelmélet egyik alapvető területébe, a Ramsey-elmélet alapjaiba, a kombinatorika egy érdekes ágába. Ezt követően megmutatom a Ramsey-tételnek néhány alkalmazhatóságát érdekes és fontos számelméleti tételek bizonyításaiban. Például többek közt így is igazolható, hogy a Fermat kongruenciának mindig van nem triviális megoldása.

A Ramsey témakör az 1920-as évek végén született Frank Plumpton Ramsey Facts an Propositions és On a problem of formal logic cikkeiben közölt eredmények alapján. Az elmélet filozófiája a következőképpen fogalmazható meg: ha egy struktúra elég nagy, akkor elkerülhetetlen, hogy ne tartalmazzon szabályos részstruktúrákat.

A téma tárgyalásához szükségünk lesz néhány alapvető gráfelméleti fogalomra, amelyet a 3. fejezetben ismertetek. A 4. fejezet a Ramsey-elméletet tárgyalja majd, a 5. fejezetben következnek a számelméleti alkalmazások.

3. Gráfelméleti bevezető

Ebben a részben [1] szerint ismertetem a definíciókat.

3.1. Definíció. Gráfnak nevezzük a $G = (V, E)$ rendezett párokat, ahol V egy nem-üres halmaz, E pedig ebből a halmazból képezhető párok egy részhalmaza. V elemeit **szögpontoknak** vagy **csúcsoknak**, E elemeit **éleknek** nevezzük. Ha egy G gráfról beszélünk, akkor $V(G)$-vel illetve $E(G)$-vel jelöljük a gráf szögpontjainak illetve éleinek halmazát.

3.2. Definíció. Ha az $e \in E$ él a v_1, v_2 párnak felel meg, akkor ez a két szögpont e **végpontjai**. Ha $v_1 = v_2$, akkor e **hurokél**. Ha két különböző nem hurokélnek a végpontjai azonosak, a két élet **párhuzamos** vagy **többszörös élnek** nevezzük. Azokat a gráfokat, amelyekben nincsenek hurokélek és többszörös élek, **egyszerű gráfnak** nevezzük.

3.3. Definíció. Ha $e, f \in E$ végpontjai $\{v_1, v_2\}$ illetve $\{w_1, w_2\}$, és $\{v_1, v_2\} \cap \{w_1, w_2\} \neq \emptyset$, akkor e, f **szomszédos élek**. Hasonlóan v_1 és v_2 **szomszédos szögpontok**, ha $\{v_1, v_2\} \in E$. v_1 **illeszkedik** e-re, ha annak egyik végpontja.

3.4. Definíció. Egy szögpont **izolált szögpont**, ha nincsen vele szomszédos másik szögpont, vagyis nem illeszkedik egyetlen élre sem. Egy szögpontra illeszkedő élek száma a szögpont **fokszáma**. Egy esetleges hurokél kettővel növeli a fokszámot. A v szögpont fokszámát $d(v)$-vel jelöljük. A maximális fokszámot Δ-val, a minimálisat δ-val jelöljük.

3.5. Definíció. **k-reguláris** egy gráf, ha minden szögpontjának foka k.

3.6. Definíció. Ha egy n szögpontú egyszerű gráf tetszőleges két szögpontja szomszédos, akkor n-szögpontú **teljes gráfnak** nevezzük, és K_n-nel jelöljük.

4. Ramsey-tételkör

A következő rész [1], [2], [4], [6], [7], [8], [10], [11] felhasználásával készült.

4.1. Bevezető példa

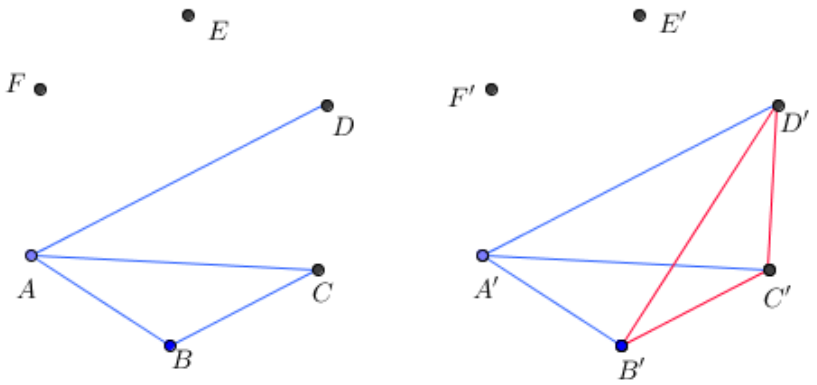
Első lépésként tekintsünk egy közismert példát ([6], [7]):

Mutassuk meg, hogy hat ember között biztosan van vagy három olyan, akik közül bármelyik kettő ismeri egymást, vagy három olyan, akik közül semelyik kettő nem ismeri egymást, az ismertségeket kölcsönösnek tekintve!

Bizonyítás. Könnyen látszik, hogy a példa átfogalmazható a gráfelmélet nyelvezetére. Nézzük azt a 6 szögpontú teljes gráfot, aminek a szögpontjai az emberek, és két csúcsot összekötő él piros, ha az emberek ismerik egymást, egyébként kék. A feladat ekkor így szól: mutassuk meg, hogy akárhogyan is színezzük ki egy 6 szögpontú teljes gráf éleit pirossal és kékkel, biztosan keletkezik benne egyszínű háromszög!

Ennek bizonyításához tekintsük a gráf egy tetszőleges A csúcsát. Az ezen csúcsból kiinduló 5 él között biztosan van legalább 3 azonos színű, például kék. Ha ezen 3 kék él másik végpontja B, C és D között vezet kék él, például a BC él kék, akkor van egyszínű háromszög, ugyanis az ABC háromszög kék, ellenkező esetben, ha a BC, CD és AD élek mindegyike piros, akkor BCD piros háromszög, vagyis ez esetben is van egyszínű háromszög. □

A bizonyítás szemléltetésére tekinthetjük az alábbi ábrákat.



4.2. Ramsey tétel

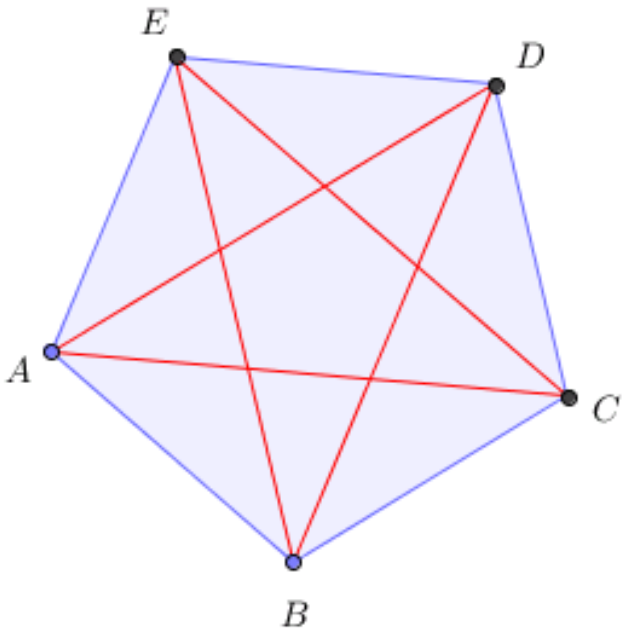
A Ramsey tétel az előző példánknak egy általánosítását adja.

4.1. Tétel. (Ramsey tétel) *Adott k, l pozitív egészekhez létezik egy olyan legkisebb $R(k,l)$ egész szám, hogy $n \geq R(k,l)$ esetén bárhogyan színezzük az n szögpontú teljes K_n gráf éleit két színnel – kékkel és pirossal – mindig van a gráfban egy kék K_k, vagy egy piros K_l.*

Speciális esetek: $R(k,2) = k$, $R(2,l) = l$.

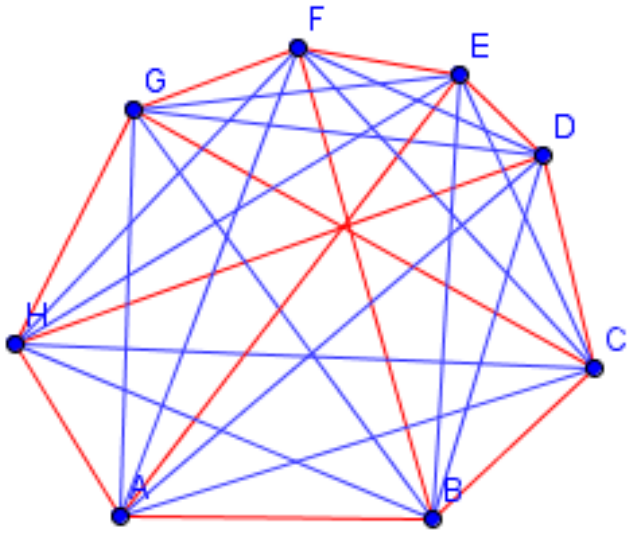
4.2. Megjegyzés. Nyilvánvaló, hogy $R(k,l) = R(l,k)$.

Az előbb megoldott feladatunkból az derült ki, hogy $R(3,3) \leq 6$. Ha K_5-nek tudunk mutatni egy olyan élszínezését (piros és kék színekkel), amelyben nincs sem kék, sem piros háromszög, akkor az is igaz, hogy $R(3,3) > 5$, tehát $R(3,3) = 6$. Az alábbi ábra egy ilyen színezést szemléltet, tehát $R(3,3) = 6$.



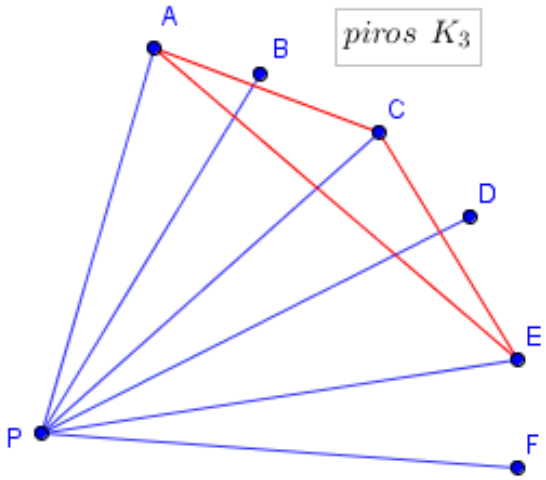
4.3. $R(3,4)$ meghatározása

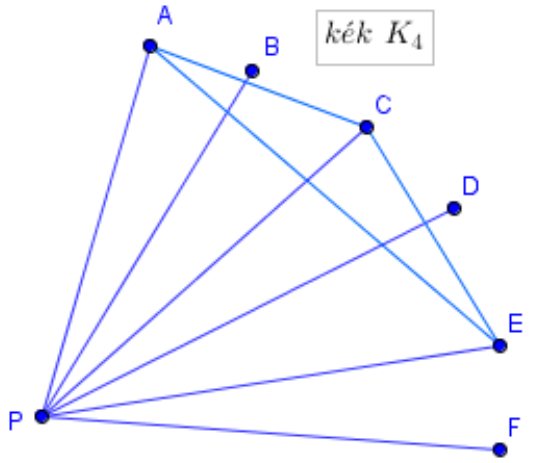
Nézzünk még egy konkrét példát, határozzuk meg az $R(3,4)$ értéket! (Ennek kiszámítását [7] -ből vettem.) Vagyis arra vagyunk kíváncsiak, hogy mi az a legkisebb pozitív egész szám, hogy az annyi csúcsú teljes gráf éleit két színnel színezve biztosan lesz a gráfban első színű K_3 vagy második színű K_4. Most a két szín legyen piros és kék. Először megmutatjuk, hogy a 8 csúcsú teljes gráf élei még kiszínezhetőek úgy pirossal és kékkel, hogy ne legyen a gráfban sem piros háromszög, sem 4 csúcsú kék teljes részgráf. Az alábbi ábra egy ilyen színezést szemléltet, tehát ezzel beláttuk, hogy $R(3,4) > 8$.



Most belátjuk, hogy a 9 csúcsú teljes gráf éleit akárhogyan is színezzük ki pirossal és kékkel, lesz a gráfban vagy piros háromszög vagy kék 4 csúcsú teljes gráf. Két eset van.

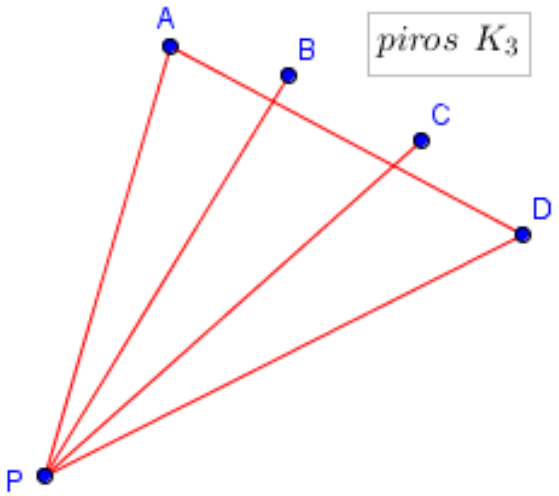
Az első eset, ha van olyan P csúcsa a gráfnak, amelyből 6 kék él indul ki, akkor tekintsük ezek végpontjai alkotta 6 csúcsú teljes gráfot. Az előzőek szerint itt lesz vagy piros háromszög, ekkor készen vagyunk, vagy lesz kék háromszög. Ennek csúcsaihoz vegyük hozzá a P csúcsot, így van kék színű, 4 csúcsú teljes gráf. Ezt az esetet az alábbi ábrák szemléltetik.

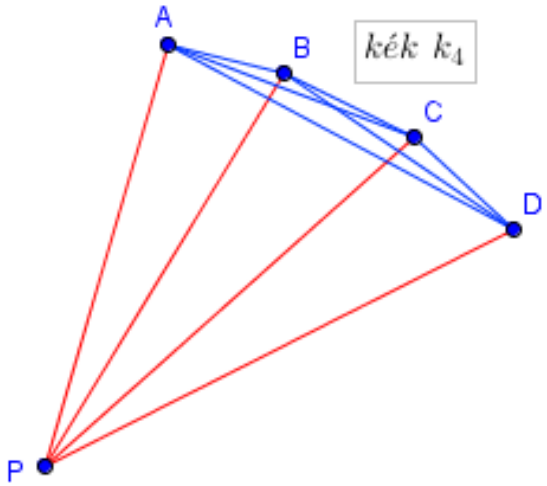




Második eset, ha nincs olyan csúcs, amelyből 6 kék él indul ki. Ekkor minden csúcsból legalább három piros él indul. Pontosan 3 piros él viszont nem indulhat minden csúcsból, ugyanis ha összeadjuk a csúcsokból kiinduló piros élek számát, akkor megkapjuk a gráfban szereplő összes piros él kétszeresét. Ezesetben azonban $3 \cdot 9 = 27$, ami páratlan szám, és így nem lehet a piros élek számának kétszerese. Vagyis lesz olyan csúcs, amelyből 4 piros él indul.

Nézzük ezen élek végpontjait! Ha valamelyik kettő pirossal van összekötve, akkor van piros háromszög, ha nem, akkor 4 csúcsú teljes gráfot alkotnak, tehát van kék K_4. Ezen eseteket az alábbi ábrák személtetik.





Mindkét esetben beláttuk, hogy vagy van a gráfban piros háromszög vagy van 4 csúcsú kék teljes gráf. Tehát $R(3,4) = 9$.

A Ramsey tétel bizonyításához szükségünk lesz az Erdős-Szekeres tételre.

4.4. Erdős-Szekeres tétel és következményei

4.3. Tétel. (Erdős-Szekeres tétel [1]) *Ha $k, l \geq 3$, akkor*

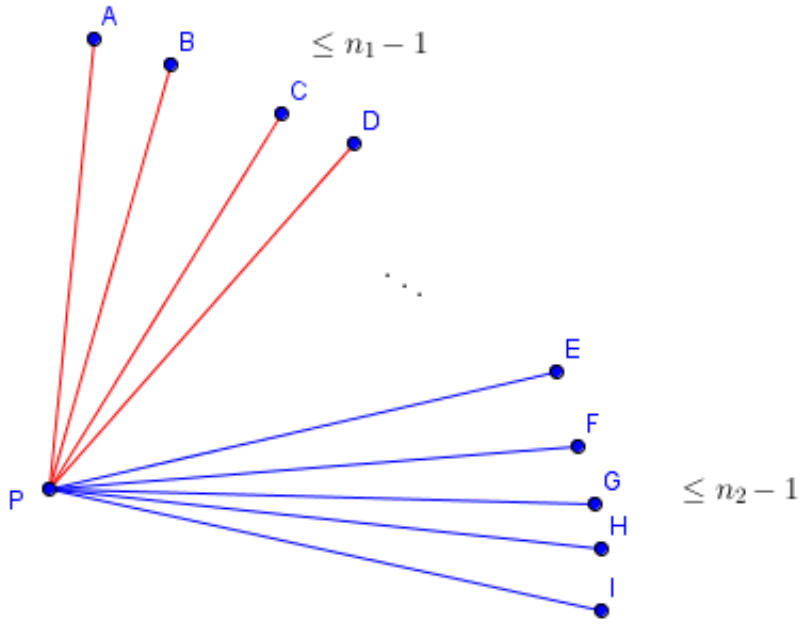
$$R(k,l) \leq R(k-1,l) + R(k,l-1).$$

Mielőtt a tételt bebizonyítanánk, nézzük meg, hogy miért következik belőle a Ramsey tétel! Az egyenlőtlenség jobb oldalán lévő összeget tovább lehet bontani, szintén az Erdős-Szekeres tételt alkalmazva a következő módon:

$$\begin{aligned} &R(k-1,l) + R(k,l-1) \leq \\ &\leq R(k-2,l) + R(k-1,l-1) + R(k-1,l-1) + R(k,l-2) \leq \dots \end{aligned}$$

Ezt a bontogatást minden tagnál addig végezzük, amíg $R(p,q)$-nál p vagy q egyenlő nem lesz 2-vel. Tudjuk, hogy $R(a,2) = R(2,a) = a$. Tehát véges sok lépésben eljutunk addig, hogy minden tagban szerepel 2-es. Vagyis $R(k,l)$-et felülről tudtuk becsülni egy pozitív egész számmal, vagyis létezik a Ramsey szám.

Bizonyítás. Most pedig térjünk rá az Erdős-Szekeres tétel bizonyítására. Legyen $n_1 = R(k-1,l), n_2 = R(k,l-1)$. Azt kell belátnunk, hogy ha van egy (n_1+n_2) csúcsú teljes gráf, azt bárhogy színezve van piros K_k vagy kék K_l. Ehhez indirekt tegyük fel, hogy van egy (n_1+n_2) csúcsú teljes gráfunk és nincs benne sem piros K_k sem kék K_l. Tekintsünk egy P csúcsot! Nézzük meg, hogy mi a helyzet, ha ebből kiindul n_1 darab piros él! Ekkor n_1 definíciója miatt a P-ből kiinduló piros élek P-től különböző végpontjai által alkotott gráf vagy tartalmaz egy kék K_l-et vagy ezek a pontok és P által meghatározott gráfban van piros K_k. Ebből következik, hogy P-ből maximum $n_1 - 1$ darab piros él indulhat. Most vizsgáljuk azt, hogy mi történik akkor, ha P-ből n_2 darab kék él indul! Ekkor n_2 definíciója miatt a P-ből kiinduló kék élek P-től különböző végpontjai által alkotott gráf vagy tartalmaz piros K_k-t vagy ezek a pontok és P által meghatározott gráfban van kék K_l. Ebből következik, hogy P-ből maximum $n_2 - 1$ darab kék él indulhat.



Vagyis a feltevés miatt a gráfnak maximum $1+n_1-1+n_2-1 = n_1+n_2-1$ csúcsa lehet. Ezzel tehát ellentmondásra jutottunk, ugyanis a gráfunknak $n_1 + n_2$ csúcsa volt.

□

1. Következmény. ([1]) *Az Erdős-Szekeres tétel következményeként egy rekurzió mentes felső becslést is kaphatunk $R(k, l)$-re:*

$$R(k,l) \leq \binom{k+l-2}{k-1}$$

Bizonyítás. $w = k + l$-re vonatkozó teljes indukcióval bizonyítunk, $k = 2$ és $l = 2$ kezdőlépésekkel. Nézzük meg tehát, hogy ezen értékekre igaz-e az egyenlőtlenség!

$$R(2,l) = l,$$
$$\binom{2+l-2}{2-1} = \binom{l}{1} = l.$$

Tehát $k = 2$ esetén a két oldal megegyezik, vagyis az egyenlőtlenség ez esetben igaz.

$$R(k, 2) = k,$$
$$\binom{k+2-2}{k-1} = \binom{k}{k-1} = k.$$

$l = 2$ esetén is egyenlő lesz a két oldal, vagyis ebben az esetben is igaz a következmény. Tehát kis értékekre teljesül az egyenlőtlenség, alkalmazhatjuk az indukciós lépést. Tegyük fel, hogy az állítás minden olyan $R(t, s)$-re teljesül, ahol $t < k$ és $s < l$ vagy $s < k$ és $t < l$. Felhasználva az Erdős-Szekeres tételt és az ismert azonosságot, hogy $\binom{a}{b} = \binom{a-1}{b} + \binom{a-1}{b-1}$, kapjuk, hogy a következmény valóban igaz.

$$\begin{aligned}
R(k, l) &\leq R(k-1, l) + R(k, l-1), \\
R(k, l) &\leq \binom{k-1+l-2}{k-2} + \binom{k+l-1-2}{k-1}, \\
R(k, l) &\leq \binom{k+l-3}{k-2} + \binom{k+l-3}{k-1}, \\
R(k, l) &\leq \binom{k+l-2}{k-1}.
\end{aligned}$$

Ami a kívánt egyenlőtlenség. □

A tétel bizonyításából adódik egy felső korlát $R(k, l)$-re, alsó korlátok pedig máshonnan, azonban a legjobb alsó korlátok és a legjobb felső korlátok között elég nagy űr tátong. Nagyon kevés k és l számra ismerjük $R(k, l)$ pontos értékét. Az L alsó korlát kiszámítása $R(k, l)$-re általában a K_{L-1} olyan kék-piros színezéséből áll, ami nem tartalmaz kék K_k részgráfot, sem piros K_l részgráfot. Egy K_n gráf összes lehetséges kiszínezésének a vizsgálata hamar számításigényessé válik, ahogy n értéke növekszik, a színezések száma exponenciálisan növekszik.

Az $R(k, l)$ értékei 8-nál kisebb k-kra és l-ekre megtalálhatók a lenti táblázatban. Ahol a pontos érték ismeretlen, az eddigi legjobb alsó és felső korlátokat adjuk meg. $R(k, l)$ értékét, ahol akár k vagy l 3-nál kisebb, megadják az $R(1, l) = 1$ és $R(2, l) = l$ képletek minden l-re. A Ramsey-számok kutatását Stanisław Radziszowski tekintette át, aki Brendan McKay-jel együtt kiszámította az $R(4, 5)$ pontos értékét.

k,l	1	2	3	4	5	6	7	8
1	1							
2	1	2						
3	1	3	6					
4	1	4	9	18				
5	1	5	14	25	43–49			
6	1	6	18	36–41	58–87	102–165		
7	1	7	23	49–61	80–143	113–298	205–540	
8	1	8	28	56–84	101–216	127–495	216–1031	282–1870

Triviális, hogy a táblázat szimmetrikus az átlóra nézve, ezért az áttekinthetőség kedvéért az átló fölötti elemeket elhagytuk.

Az $R(k,k)$ átlós Ramsey-számok meghatározása a kombinatorika egyik legnehezebb problémája. Ismert, hogy $R(3,3)=6$ és $R(4,4)=18$. De $R(5,5)$ pontos értéke már ismeretlen, csak azt tudjuk róla, hogy 43 (Geoffrey Exoo) és 49 (Brendan McKay és Stanisław Radziszowski) között található; hacsak nem találunk az összes eset szisztematikus végigvizsgálásánál lényegesen hatékonyabb eljárást, valószínű, hogy az $R(6,6)$ pontos értéke örökre ismeretlen marad számunkra.

„Képzeljük el, hogy az embernél sokkal hatalmasabb idegen faj landol a Földön, és az $R(5,5)$ értékét követelik, vagy elpusztítják a bolygót. Ebben az esetben hadra kéne fognunk minden számítógépet és matematikust, hogy megtaláljuk az értéket. De tegyük fel, hogy ehelyett az $R(6,6)$ értékére kíváncsiak; ebben az esetben minden erőnkkel meg kéne próbálnunk legyőzni őket." –Erdős Pál

Nézzünk még egy alsó, illetve felső becslést $R(k,k)$-ra.

4.4. Tétel. ([7]) *Ha $k \geq 2$, akkor $2^{\frac{k}{2}} \leq R(k,k) \leq 2^{2k-3}$.*

Bizonyítás. A jobb oldali reláció bizonyításánál a binomiális együtthatók tulajdonságait használjuk fel:

$$\begin{aligned} R(k,k) &\leq \binom{k+k-2}{k-1} = \binom{2k-2}{k-1} = \\ &= \binom{2k-3}{k-1} + \binom{2k-3}{k-2} \leq \\ &\leq \sum_{i=0}^{2k-3} \binom{2k-3}{i} = 2^{2k-3}. \end{aligned}$$

A bal oldali reláció és bizonyítása Erdős Páltól származik:

Az állítás $k = 2$-re és $k = 3$-ra igaz, hiszen $R(2,2) = 2$ és $R(3,3) = 6$, mint már láttuk. Legyen $k \geq 4$. Vegyünk egy $n < 2^{\frac{k}{2}}$ csúcsú gráfot, és tekintsük az összes piros-kék színezését. Azt bizonyítjuk be, hogy ha ezek közül véletlenszerűen választunk egyet, akkor nem 0 annak a valószínűsége, hogy a választott színezés nem tartalmaz sem k csúcsú piros, sem k csúcsú kék teljes gráfot. Ez nyilván azt jelenti, hogy van ilyen színezés.

Az n csúcsú teljes gráf összes színezéseinek száma: $2^{\binom{n}{2}}$, hiszen $\binom{n}{2}$ darab él van, és egymástól függetlenül mindegyik piros vagy kék. Így minden színezés választásának valószínűsége $2^{-\binom{n}{2}}$. Legyen X egy k darab csúcsból álló halmaz. Annak valószínűsége, hogy az ezeket összekötő élek mind pirosak $2^{-\binom{k}{2}}$. Mivel ilyen X halmaz $\binom{n}{k}$ féleképpen választható, ezért annak valószínűsége, hogy lesz közöttük piros k csúcsú teljes gráf:

$$P(\exists \text{k csúcsú teljes piros}) \leq \binom{n}{k} 2^{-\binom{k}{2}}.$$

Itt $\binom{n}{k} \leq \frac{n^k}{k!} \leq \frac{n^k}{2^{k-1}}$, és $n < 2^{\frac{k}{2}}$, ezért

$$P(\exists \text{k csúcsú teljes piros}) \leq \frac{n^k}{2^{k-1}} \cdot 2^{-\binom{k}{2}} < \frac{2^{\frac{k^2}{2}}}{2^{k-1}} \cdot 2^{-\frac{k^2}{2}+\frac{k}{2}} = 2^{-\frac{k}{2}+1} \leq \frac{1}{2}.$$

(Az utolsó reláció $k \geq 4$ miatt teljesül.) Vagyis annak a valószínűsége, hogy az összes színezésben lesz k csúcsú piros teljes gráf kisebb, mint $\frac{1}{2}$. Szimmetria alapján annak a valószínűsége, hogy az összes színezésben lesz k csúcsú kék teljes gráf is kisebb, mint $\frac{1}{2}$. Tehát annak a valószínűsége, hogy lesz vagy piros vagy kék k csúcsú teljes gráf 1-nél kisebb. □

4.5. További becslések

4.5. Megjegyzés. ([11], [14], [15], [16]) Említés szinten felsorolok még néhány alsó- és felső becslést:

1935–Erdős: $R(k,k) < \frac{c_1}{(\log k)^{c_2}}\binom{2k-2}{k-2}$, megfelelő pozitív c_1, c_2 konstansokkal.

1947–Erdős: $(1+\mathcal{O}(1))\frac{1}{e\sqrt{2}} \cdot k \cdot 2^{\frac{k}{2}} < R(k,k)$.

1980–Ajtai-Komlós-Szemerédi, és 1995–Kim: Megfelelő pozitív c_1 és c_2 konstansok esetén

$$c_1 \cdot \frac{n^2}{\log n} \leq R(3,n) \leq c_2 \cdot \frac{n^2}{\log n}.$$

1986–Rödl: $R(k,l) < \frac{c}{\log(k+l))^d}\binom{k+l-2}{k-1}$, megfelelő $c, d > 0$ konstansokkal.

1987–Graham–Rödl (az előzőnél gyengébb becslés): $R(k,l) \leq \binom{k+l+2}{k-1}\frac{6}{\log\log(k+l-2)}$.

1987–Thomason: $R(k,k) < \frac{1}{k}\binom{2k-2}{k-1}$.

2009–Conlon: $R(k,k) < \frac{1}{k^{\frac{c\cdot\log k}{\log\log k}}}\binom{2k-2}{k-1}$ megfelelő $c > 0$ konstanssal.

4.6. Ramsey tétel általános alak

Az alábbiakban a Ramsey tétel általánosítása fog következni. Most 2-nél több színnel is színezhetjük az n szögpontú, teljes gráf éleit, mondjuk $s \geq 2$ darab színnel.

4.6. Tétel. (Ramsey tétel általános alak) *Minden $k_1, k_2, \ldots k_s \geq 2$-re van olyan $R(k_1, k_2, \ldots k_s)$ szám, hogy egy legalább $R(k_1, k_2, \ldots k_s)$ szögpontú teljes gráf éleit s darab színnel tetszőlegesen színezve keletkezik 1. színű K_{k_1} részgráf vagy 2. színű K_{k_2} részgráf vagy ... s. színű K_{k_s} részgráf.*

A tétel bizonyításánál hasonlóan járunk el, mint előbb, egy egyenlőtlenség igazságából következtetünk rá. Nézzük először tehát ezt az egyenlőtlenséget.

4.7. Állítás. *Ha* $k_1, k_2 \dots k_s \geq 3$, *akkor* $R(k_1, k_2, \dots k_s) \leq R(R(k_1, k_2), k_3, \dots k_s)$, *ahol* $R(k_1, k_2)$ *azt mutatja az egyenlőtlenség jobb oldalán, hogy az 1-es és 2-es színt összevontuk azonos színné.*

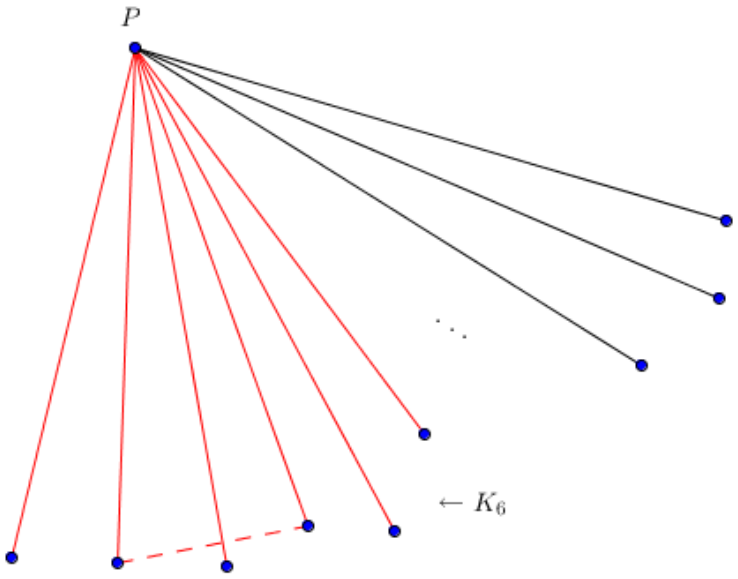
Az állítás bizonyítása előtt gondoljuk meg, hogy abból miért következik az általános Ramsey-tétel is. Az egyenlőtlenség jobb oldalán álló kifejezésben az $R(k_1, k_2)$-ről már beláttuk, hogy létezik. Ha igaz az állítás, akkor az egyenlőtlenség jobb oldalán lévő kifejezés addig bontható tovább, amíg már csak 2 darab színnel való színezésre vezethetjük vissza bizonyításunkat. Erről viszont a két színnel színezett gráfokra kimondott Ramsey-tétel alapján tudjuk, hogy létezik. Tehát lesz egy felső becslésünk $R(k_1, k_2, \dots k_s)$-re, vagyis létezik $R(k_1, k_2, \dots k_s)$. Miután láttuk, hogy az állítás igazságából miért következik az általános Ramsey-tétel, lássunk neki az állítás bizonyításának.

Bizonyítás. Az 1-es és a 2-es színből egy időre azonos, mondjuk lila színt készítünk. A gráf most $s-1$ színnel van színezve. $R(R(k_1, k_2), k_3, \dots k_s) := n$. Az n szögpontú, $s-1$ színnel színezett gráfban definíció szerint van lila $K_{R(k_1,k_2)}$ vagy 3. színű K_{k_3} vagy $\dots$s. színű K_{k_s}. Ha itt a 3.,4., $\dots$s. színből volt a megfelelő részgráf, akkor készen vagyunk, hiszen az eredetileg színezett gráfban is van ugyanilyen részgráf. Baj akkor lehet, ha lila részgráfot találtunk. De ekkor is készen vagyunk, hiszen ha visszaállítjuk az eredeti színezést, akkor ebben az $R(k_1, k_2)$ méretű egyes vagy kettes színnel színezett teljes gráfban lesz piros K_{k_1} vagy kék K_{k_2}. □

4.8. Megjegyzés. ([8]) A fenti állítás egy gyenge becslést ad, ugyanis például

$$R(3,3,3) \leq R(R(3,3),3) = R(6,3) \leq \binom{6+3-2}{5} = 21.$$

Megjegyezzük, hogy a pontos érték $R(3,3,3)$-ra viszont 17 (ld. [8]). K_{16} éleinek találni egy olyan három színnel való színezését, amelyben nincs egyszínű háromszög, nem könnyű feladat, de létezik ilyen három színezés. Azt viszont könnyen be tudjuk látni, hogy $R(3,3,3) \leq 17$, ugyanis K_{17} éleinek három színnel (mondjuk pirossal, zölddel és kékkel) való színezésekor egy tetszőleges P csúcsot kiválasztva, lesz olyan színű él (pl. piros) a skatulya elv miatt, amiből legalább 6 darab megy ki P-ből.



Ha ezen 6 él végpontjai közül van kettő, amelyek között szintén piros él megy, akkor van piros háromszög. Ellenkező esetben egy hat csúcsú teljes gráf élei két színnel (zölddel és kékkel) vannak színezve, erre pedig már beláttuk, hogy lesz vagy zöld, vagy kék háromszög benne. Tehát K_{17} éleinek 3 színnel való színezésekor fogunk találni egyszínű háromszöget, azaz $R(3,3,3) \leq 17$.

4.7. $R(3,3,\ldots 3)$ becslése

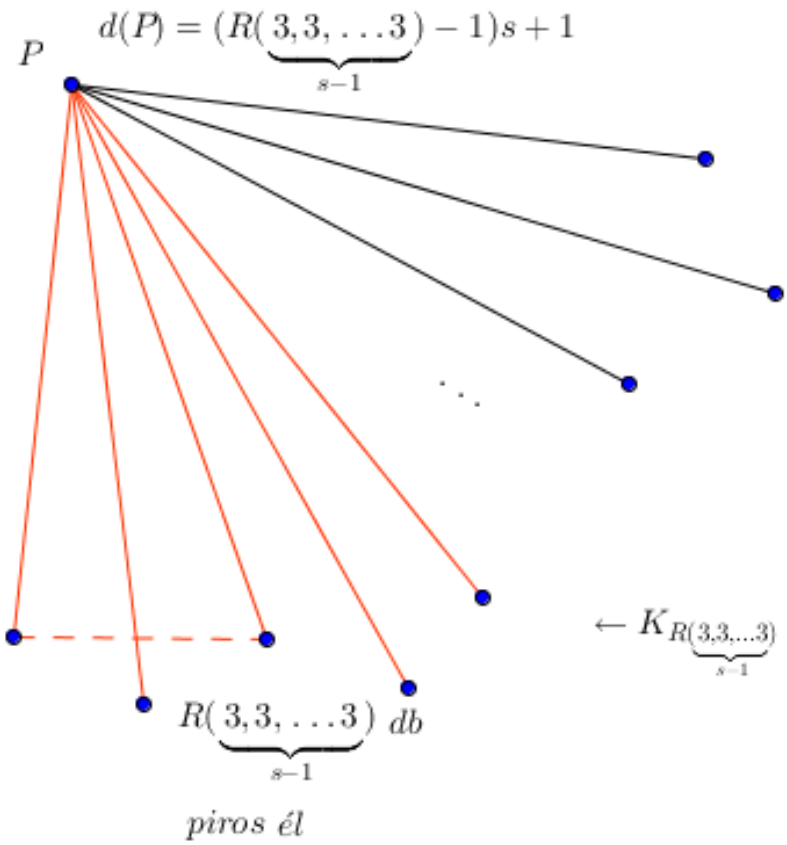
Az első érdekes eset az $R(3,3,\ldots 3)$.

4.9. Állítás. ([11]) $R(\underbrace{3,3,\ldots 3}_{s}) \leq (R(\underbrace{3,3,\ldots 3}_{s-1}) - 1)s + 2.$

Bizonyítás. Vegyünk egy $(R(\underbrace{3,3,\ldots 3}_{s-1}) - 1)s + 2$ csúcsú teljes gráfot. Kiszíneztük az éleit s darab színnel. Azt kell belátnunk, hogy van egyszínű

háromszög. Válasszunk egy tetszőleges P csúcsot. A belőle kiinduló élek száma $(R(\underbrace{3,3,\dots 3}_{s-1})-1)s+1$. A skatulya elv alapján létezik olyan színű él, mondjuk piros, amelyből legalább $R(\underbrace{3,3,\dots 3}_{s-1})$ darab van. Tekintsük ezen piros élek végpontjai által alkotott G részgráfot. Ekkor két eset lehet. Vagy van a G részgráf élszínezésében piros él, és ekkor az eredeti gráfban van piros háromszög. (A P szögpont és a piros él végpontjai által alkotott háromszög piros.) Vagy nincs, ekkor a G részgráf színezésében $(s-1)$ darab színt használtunk, viszont ennek a G részgráfnak $R(\underbrace{3,3,\dots 3}_{s-1})$ darab szögpontja van, így definíció szerint van benne egyszínű háromszög. □

Az alábbi ábra a fenti bizonyítást szemlélteti:



4.10. Tétel. ([11]) $R(\underbrace{3,3,\dots 3}_{s}) \leq 1 + \lfloor es! \rfloor$

4.11. Megjegyzés. Itt e a természetes logaritmus alapszámát jelenti.

Bizonyítás. A bizonyítás s szerinti teljes indukcióval fog történni. Nézzük meg tehát először, hogy $s = 2$-re és $s = 3$-ra igaz-e az állítás.

$$6 = R(3,3) \leq 1 + \lfloor \mathrm{e}2! \rfloor = 6$$
$$17 = R(3,3,3) \leq 1 + \lfloor \mathrm{e}3! \rfloor = 17.$$

Tegyük fel, hogy $s = n-1$-ig teljesül az állítás. $s = n$-re

$$R(\underbrace{3,3,\dots 3}_{n}) \leq 1 + \lfloor \mathrm{e}n! \rfloor,$$

vagyis egy tetszőleges u csúcsnak $\lfloor en! \rfloor$ szomszédja van, melyek n osztályba vannak sorolva. Ekkor:

$$\lfloor \mathrm{e}n! \rfloor = \lfloor \textstyle\sum_{i=0}^{\infty} \frac{n!}{i!} \rfloor = \sum_{i=0}^{n} \frac{n!}{i!} = 1 + n \sum_{i=0}^{n-1} \frac{(n-1)!}{i!} = 1 + n \lfloor \mathrm{e}(n-1)! \rfloor,$$

vagyis ezen n különböző szín között a skatulya elv miatt van olyan, amihez $\lfloor e(n-1)+1 \rfloor$ csúcs tartozik. Legyen például ez a szín a kék. Ha ezen csúcsok között van kék él, akkor kék háromszöget kapunk, ha pedig nincs közöttük kék él, akkor az $\lfloor e(n-1)+1 \rfloor$ csúcs közötti él színezésére csak $(n-1)$ színt használunk, vagyis teljesül az indukciós feltétel, és találtunk egyszínű háromszöget. □

5. A Ramsey-tétel alkalmazása bizonyításokban

Ehhez a részhez szükségünk lesz az alábbi definíciókra, amelyeket [1] könyv alapján ismertetek.

5.1. Definíció. Legyen $p > 2$ prím és $(a, p) = 1$. Az a számot aszerint nevezük **kvadratikus maradék**nak, illetve **kvadratikus nemmaradék**nak modulo p, hogy az $x^2 \equiv a \ (p)$ kongruencia megoldható-e, vagy sem.
Az $a \equiv 0 \ (p)$ számokat nem soroljuk sem a kvadratikus maradékok, sem a kvadratikus nemmaradékok közé.

5.2. Definíció. Az $\left(\frac{a}{p}\right)$ **Legendre-szimbólum**ot a következőképpen értelmezzük:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ kvadratikus maradék mod } p \\ -1, & \text{ha } a \text{ kvadratikus nemmaradék mod } p. \end{cases}$$

5.1. Speciális halmazokról, amelyek csak kvadratikus maradékokat tartalmaznak

A következő rész Sárközy András 1977-ben megjelent [5] cikke alapján kerül ismertetésre.

5.3. Definíció. Legyen p tetszőleges prímszám. Egészek egy $v_1, v_2, \ldots, v_t$ sorozatát $\mathcal{M}_p$ halmaznak fogjuk hívni, ha a következők teljesülnek:

$$(v_i, p) = 1, \text{ ha } 1 \le i \le t,$$
$$v_i \not\equiv v_j \quad (p), \text{ ha } 1 \le i < j \le t,$$
$$\text{és } \left(\frac{v_i - v_j}{p}\right) = -1, \text{ ha } 1 \le i < j \le t.$$

Itt $\left(\frac{v_i - v_j}{p}\right)$ Legandre-szimbólumot jelöl.

Nézzünk erre egy egyszerű példát. $p := 5, t := 2, v_1 := 2, v_2 := 9$.
–Az első tulajdonság teljesül, ugyanis $(2, 5) = 1, (9, 5) = 1$.
–A második tulajdonság is teljesül, mert $2 \not\equiv 9$ (5).
–A harmadik tulajdonság is igaz, $\left(\frac{2-9}{5}\right) = \left(\frac{(-7)}{5}\right) = (-1)$, mert $1^2 \not\equiv (-7)$ $(5), 2^2 \not\equiv (-7)$ $(5), 3^2 \not\equiv (-7)$ $(5), 4^2 \not\equiv (-7)$ (5).

Jelölje M_p azt a legnagyobb egész számot, amit ki lehet választani az $1, 2, \ldots, p-1$ számok közül, hogy az $\mathcal{M}_p$ halmazt alkosson $v_1, v_2, \ldots, v_t$-vel.

5.4. Lemma. ([5]) *Ha egy p prímre teljesül, hogy*

$$p \equiv 1 \quad (4), \text{ akkor}$$
$$M_p \ge \left[\frac{\log(p-1)}{\log 4} + 1\right].$$

Bizonyítás. Definiáljuk a G_{p-1} gráfot, aminek $p-1$ pontja $P_1, P_2, \ldots, P_{p-1}$ a következőképp:

A P_i és P_j $(i \ne j)$ pontok között menjen piros él, ha

$$\left(\frac{i-j}{p}\right) = -1,$$

és menjen kék él, ha

$$\left(\frac{i-j}{p}\right) = 1.$$

Vezessük be a következő jelölést:

$$T \stackrel{\text{def}}{=} \left[\frac{\log(p-1)}{\log 4} + 1\right].$$

Az alábbi becslésekből látható, hogy G_{p-1} vagy a komplementere tartalmaz részgráfként egy T szögpontú teljes gráfot, vagyis $R(T,T) \leq p-1$.

$$R(T,T) \leq \binom{T+T-2}{T-1} = \binom{2T-2}{T-1} \leq \sum_{i=0}^{2T-2} \binom{2T-2}{i} = 2^{2T-2} \leq 4^{T-1}.$$

Behelyettesítve T értékét:

$$R(T,T) \leq 4^{T-1} = 4^{\left[\frac{\log p}{\log 4}+1\right]-1} = 4^{\left[\frac{\log p}{\log 4}\right]} < 4^{\frac{\log p}{\log 4}} = p,$$

vagyis

$$R(T,T) \leq p-1.$$

Ha ez a T szögpontú egyszínű teljes gráf piros, akkor készen vagyunk, ugyanis ez azt jelenti, hogy találtunk $\left[\frac{\log(p-1)}{\log 4}+1\right]$ méretű $\mathcal{M}_p$ halmazt. Ha a T szögpontú teljes gráf színe kék, akkor T szögpontjait jelöljük $P_{\omega_1}, P_{\omega_2} \ldots, P_{\omega_T}$-vel.

Ezekre teljesülnek:

$$(\omega_i, p) = 1,\ \omega_i \neq \omega_j,\ \left(\frac{\omega_i - \omega_j}{p}\right) = 1\ \forall 1 \leq i \leq j \leq T.$$

Rögzítsünk egy n kvadratikus nem maradékot, vagyis $\left(\frac{n}{p}\right) = -1$. Legyen $v_i \overset{\text{def}}{=} n\omega_i$. Ekkor a $n \cdot T$ szögpontú teljes kék részgráf csúcsaira teljesülni fognak az $\mathcal{M}_p$ halmaz tulajdonságai:

$$(v_i, p) = (n\omega_i, p) = 1$$

$$v_i \neq v_j \Leftrightarrow n\omega_j \neq n\omega_j \Leftrightarrow \omega_j \neq \omega_j$$

$$\left(\frac{v_i - v_j}{p}\right) = \left(\frac{n\omega_i - n\omega_j}{p}\right) = \left(\frac{n(\omega_i - \omega_j)}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{\omega_i - \omega_j}{p}\right) = -1$$

Tehát ebben az esetben is készen vagyunk, ugyanis ez szintén azt jelenti, hogy találtunk $\left[\frac{\log(p-1)}{\log 4}+1\right]$ méretű $\mathcal{M}_p$ halmazt.

□

A következő tételt témavezetőm, Dr. Gyarmati Katalin 2001-ben, On a problem of Diophantus címmel megjelent cikke ([12]) alapján ismertetem.

5.5. Tétel. *Létezik olyan p_0 konstans, hogy ha $p = 4k + 1$ alakú prím, és $p > p_0$, akkor létezik $A \subseteq \mathbb{Z}_p$ halmaz, amelyre*

$$|A| \geq \frac{1}{6 \log 3} \log p,$$

valamint $a \cdot a' + 1$, mindig kvadratikus maradék mod p, vagy $0 \mod p$, ha a, $a' \in A$ és $a \neq a'$.

A bizonyítás érdekessége, hogy gráfelméleten alapul, a Ramsey tételnek a következő általánosítása a kulcsa:

5.6. Lemma. ([4]) *Minden s_1, s_2, s_3 nem negatív számokra létezik egy r egész szám az alábbi tulajdonsággal:*

Ha G olyan teljes gráf, amelyre $V(G) \geq r$, és C tetszőleges három színezése G gráfnak a c_1, c_2, c_3 színekkel, akkor létezik $1 \leq i \leq 3$, hogy G-nek van egyszínű G' részgráfja, ahol $|V(G')| \geq s_i$. Jelöljük az ilyen r számok közül a legkisebbet $R(a, b, c)$-vel. Ekkor:

$$R(s_1, s_2, s_3) \leq \frac{(s_1 + s_2 + s_3)!}{s_1! s_2! s_3!}.$$

Bizonyítás. Ha az $R(s_1, s_2, s_3)$ számok valamelyike 0, akkor az állítás triviális, mert $R(s_1, s_2, s_3) = 0$. $s_1, s_2, s_3 > 0$ esetén igaz az alábbi egyenlőtlenség, ami az Erdős-Szekeres tétel általánosítása:

$$R(s_1, s_2, s_3) \leq R(s_1 - 1, s_2, s_3) + R(s_1, s_2 - 1, s_3) + R(s_1, s_2, s_3 - 1).$$

Ebből $s_1 + s_2 + s_3$-ra vonatkozó indukcióval kapjuk:

$$R(s_1, s_2, s_3) \leq \frac{(s_1 + s_2 + s_3)!}{s_1! s_2! s_3!}.$$

□

Nézzük most azt a gráfot, amelynek pontjai a $\mod p$ maradékosztályok. Mivel $p = 4k + 1$ alakú prím, ezért létezik i maradékosztály, hogy $i^2 \equiv -1$ (p). Az élek színét a Legendre szimbólum segítségével határozzuk meg, $\left(\frac{0}{p}\right)$ értékét vegyük 0-nak.

Az a és b maradékosztályokat összekötő élt színezzük
c_1 színnel, ha $\left(\frac{ab+1}{p}\right) = 1$ vagy 0,
c_2 színnel, ha $\left(\frac{-ab+1}{p}\right) = 1$ vagy 0, és $\left(\frac{ab+1}{p}\right) = -1$,
c_3 színnel, ha $\left(\frac{-a^2b^2+1}{p}\right) = 1$ vagy 0 és $\left(\frac{ab+1}{p}\right) = \left(\frac{-ab+1}{p}\right) = -1$.
Ekkor minden élt megszíneztünk, ellenkező esetben ugyanis:

$$\left(\frac{ab+1}{p}\right) = \left(\frac{-ab+1}{p}\right) = \left(\frac{-a^2b^2+1}{p}\right) = -1.$$

Tehát:

$$-1 = \left(\frac{(ab+1)(-ab+1)(-a^2b^2+1)}{p}\right) = \left(\frac{(a^2b^2-1)^2}{p}\right).$$

De ez ellentmond a nyilvánvaló ténynek, hogy

$$\left(\frac{(a^2b^2-1)^2}{p}\right) = 1 \quad \text{vagy} \quad 0.$$

Legyen $c = \left[\frac{1}{3\log 3}\log p\right] + 1$. Az előző lemma szerint:

$$R(c,c,c) \leq \frac{(3c)!}{c!c!c!}.$$

Az egyenlőtlenség jobboldalát Stirling formulával becsüljük. Elég nagy c esetén:

$$\frac{(3c)!}{c!c!c!} \leq (1+o(1))\frac{\left(\frac{3c}{e}\right)^{3c}\sqrt[2]{2\pi 3c}}{\left(\left(\frac{c}{e}\right)^{c}\sqrt[2]{2\pi c}\right)^3} \leq 3^{3c-3} \leq p.$$

Azaz, ha p elég nagy, akkor $R(c,c,c) \leq p$. Tehát van a gráfban egy c darab szögpontból álló egyszínű G' részgráf.

Legyen

$$A = \begin{cases} V(G'), & \text{ha a } G' \text{ éleit } c_1 \text{ színnel színeztük,} \\ ig : g \in V(G'), & \text{ha a } G' \text{ éleit } c_2 \text{ színnel színeztük,} \\ ig^2 : g \in V(G'), & \text{ha a } G' \text{ éleit } c_3 \text{ színnel színeztük.} \end{cases}$$

Ekkor $|A| \geq \frac{1}{2}|V(G')|$. A színezés definíciója miatt A halmaz bármely két elemének szorzatához 1-et adva mindig kvadratikus maradékot vagy 0-t kapunk mod p.

5.2. Az első N egész szám összegmentes csoportokra bontása

5.7. Tétel. ([9]) *Ha az első N egész szám beosztható r csoportba úgy, hogy egyikben se szerepeljen semelyik két elemének a különbsége, akkor*

$$N < r!e.$$

5.8. Megjegyzés. Itt e a természetes logaritmus alapszámát jelenti.

Az alábbi bizonyítást Erdős Pál és Surányi János Válogatott fejezetek a számelméletből című könyvéből ismertetem.

Bizonyítás. Induljunk ki az első N természetes szám egy, a feltételeknek megfelelő beosztásából r darab csoportba. Legyen az előforduló legnagyobb elemszám egy csoportban n_1, ekkor

$$N \leq n_1 \cdot r.$$

Egy n_1 elemű csoport elemei legyenek

$$a_1 < a_2 < a_3 < \ldots < a_{n_1},$$

nevezzük ezt a csoportot elsőnek.

Ez a csoport nem tartalmazhatja az

$$a_2 - a_1, a_3 - a_1, \ldots, a_{n_1} - a_1$$

számokat, így azok a további $r-1$ darab csoport közt oszlanak el. Közülük n_2 legyen a legtöbb, amennyi egy csoportba kerül. Legyen többek közt

$$b_1 < b_2 < b_3 < \ldots < b_{n_2}$$

ugyanabban a csoportban, nevezzük ezt a csoportot másodiknak. Ekkor egyrészt n_2 jelentése szerint

$$n_1 - 1 \leq n_2(r-1),$$

másrészt

$$b_i = a_{k_i} - a_1 \quad (i = 1, 2, \ldots, n_2)$$

alkalmas $k_1, k_2, \ldots, k_{n_2}$ indexekkel. Ismét nem lehetnek a második csoportban

$$b_i - b_1 \quad (i = 2, 3, \ldots, n_2)$$

számok, de az elsőben sem, mert

$$b_i - b_j = a_{k_i} - a_{k_j}$$

két első csoportbeli elemnek is különbsége. Ezek a számok tehát a maradó $r-2$ darab csoportban oszlanak el. Ha egybe közülük maximálisan n_3 esik, akkor

$$n_2 - 1 \leq n_3(r-2),$$

és az eljárás folytatható tovább egészen addig, míg az $s-1$-edik lépésben kiválasztott n_{s-1} elemből képezett $n_{s-1}-1$ különbség már úgy oszlik el abban az $r-s+1$ darab csoportban, amelybe még kerülhet belőlük, hogy mindegyikbe legfeljebb $1 = n_s$ elem kerül közülük. Ekkor

$$n_{s-1} - 1 \leq n_s(r-s+1) = r-s+1.$$

Nyilvánvalóan $s \leq r$, és az így definiált $n_1, n_2, \ldots, n_s = 1$ sorozat bármely két szomszédos elemére fennáll, hogy

$$n_i - 1 \leq n_{i+1}(r-i),$$

ha $i = 1, 2, \ldots, s-1$, sőt még $i = 0$-ra is érvényes az egyenlőtlenség, ha n_0-n $N+1$-et értünk.

Sorra alkalmazva ezt $i = 0, 1, 2, \ldots, s-1$-re és használva e értelmezését, nyerjük a következő egyenlőtlenségeket:

$$\begin{aligned}
N &\leq ((n_1 - 1) + 1)r \leq n_2(r-1)r + r \leq n_3(r-2)(r-1)r + (r-1)r + r \leq \\
&\leq \ldots \leq n_{s-1}(r-s+2)(r-s+3)\ldots(r-1)r + (r-s+3)\ldots(r-1)r + \\
&\ldots + \ldots + (r-1)r + r \leq \\
&\leq (r-s+1)(r-s+2)\ldots(r-1)r + (r-s+2)\ldots(r-1)r + \ldots \\
&\ldots + (r-1)r + r \leq \\
&\leq r! + 2\cdot 3\cdot \ldots \cdot (r-1)r + 3\cdot \ldots \cdot (r-1)r + \ldots + (r-1)r + r = \\
&= r!\left(1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{(r-2)!} + \frac{1}{(r-1)!}\right) < r!e,
\end{aligned}$$

és ez volt a bizonyítandó. □

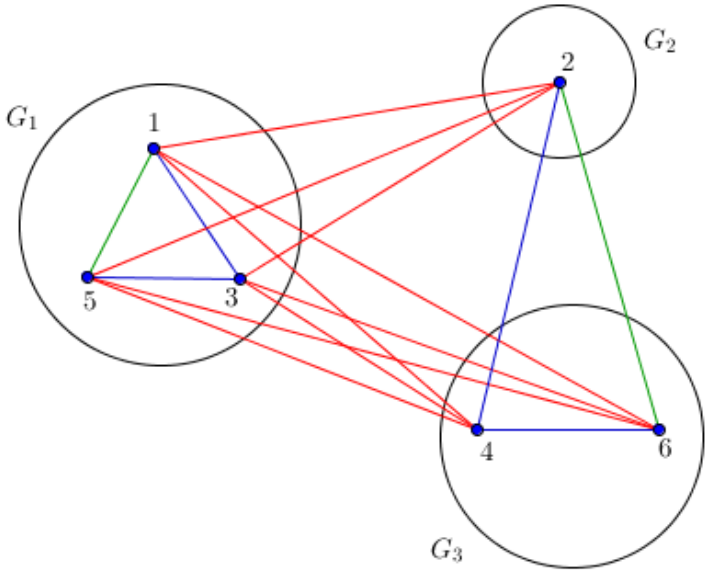
Most pedig jöjjön ugyanennek a tételnek a Ramsey-tétellel való bizonyítása.

Bizonyítás. Definiáljunk egy N szögpontú gráfot, szögpontjai $1, 2, \ldots, N$ legyenek. Az r darab csoportot, amelybe a gráf csúcsait a tétel feltételének megfelelően beosztjuk jelölje $G_1, G_2, \ldots, G_r$. A gráf éleit színezzük r darab színnel a következőképpen: az i és j pontot összekötő él színe legyen az a k. szín, amelyre $|i-j| \in G_k$. Ha be tudnánk látni, hogy

$$R(\underbrace{3, 3, \ldots 3}_{r}) \leq N - 1,$$

azzal a tételt is bebizonyítanánk. Viszont a fenti egyenlőtlenség a 4.10 tétel következménye, tehát felhasználhatjuk. Ez pedig azt jelenti, hogy az N szögpontú, a fenti módon definiált gráf éleit a feltételeknek megfelelően színezve van olyan G_k csoport, amelyben van egyszínű hármoszög. Ebből pedig az következik, hogy $\exists \quad h, i, j$, amelyekre $|h-i|, |h-j|, |i-j| \in G_k$, azaz $|h-i|$, $|h-j|$ és $|i-j|$ számok azonos színnel lettek szinezve. Itt szimmetrikus okokból feltesszük, hogy $h < i < j$. Ez viszont ellentmond annak, hogy egy csoportban csak olyan számok vannak, amelyeknek a különbsége nincs a csoportban, itt ugyanis $(i-h)+(j-i) = (j-h)$, tehát két csoportbeli szám összege egy harmadik, ami átfogalmazva azt is jelenti, hogy az egyik elemet megkapjuk két csoportbeli elem különbségeként. $\square$

A könnyebb elképzelhetőség kedvéért nézzünk egy konkrét példát is. Legyen most $N = 6$, $r = 3$, és a csoportok, $G_1 = \{1, 3, 5\}$, $G_2 = \{2\}$, $G_3 = \{4, 6\}$. Ellenőrizhető, hogy ez valóban megfelelő beosztás, egyik halmazban sem szerepel két elemének a különbsége. A gráf éleit pirossal, kékkel és zölddel színezzük. Az i és j szögpontot összekötő él színe legyen piros, ha $|i-j| \in G_1$, kék, ha $|i-j| \in G_2$, és zöld, ha $|i-j| \in G_3$. Látszik, hogy ennél a példánál teljesül a tétel feltétele, vagyis az első 6 egész szám beosztható 3 csoportba úgy, hogy egyikbe se szerepeljen semelyik két elemének a különbsége. Az is ellenőrizhető, hogy $6 < 3!e$, vagyis itt igaz a tétel állítása.



5.3. A Fermat kongruenciáról

Most pedig néhány szükséges definíció bevezetése és tétel kimondása után (ezeket bizonyítás nélkül közöljük [6] alapján) rátérünk a Fermat kongruencia megoldhatóságának egy elemi bizonyítására a 5.7 tétel felhasználásával. A bizonyítást Erdős Pál és Surányi János, Válogatott fejezetek a számelméletből című könyve alapján végezzük.

Először nézzük, hogy mi is az a Fermat sejtés, amely évszázadokon át izgatta a matematikusokat.

Az $x^2 + y^2 = z^2$ egyenlet Pitagorasz tételét jelenti, ahol x, y egy derékszögű háromszög befogóinak oldalhosszúságait, z pedig az átfogó hosszúságát jelenti, tehát pozitív valós számok. Az olyan pozitív egész számokat, amelyek kielégítik a Pitagorasz tételt, pitagoraszi számhármasoknak nevezzük. Ilyen számhármasból végtelen sok van. Ezek után a matematikusokat elkezdte ér-

dekelni, hogy van-e megoldása az egész számok körében az $x^3 + y^3 = z^3$ egyenletnek, sőt általában az $x^n + y^n = z^n$ egyenletnek.

Fermat miután elolvasta Diophantosz Arithmetica című művében azt a részt, amely az $x^2 + y^2 = z^2$ egyenlet megoldásairól szól az egész számok körében (Pitagoraszi számhármasok), a következő tartalmú feljegyzést írta ennek a kiadványnak a margójára.

„... Ugyanakkor teljesen lehetetlen a köb felbontása két köb összegére, vagy a negyedik hatványoké két negyedik hatvány összegére, de nem lehet semmilyen más magasabb hatványt sem felbontani két ugyanolyan hatványkitevőjű szám összegére. E tételnek valóban bámulatos bizonyítására jöttem rá, de nincs elég hely, hogy ide leírjam." (Lásd: Jelenski: Pitagorasz nyomában 135. old.)

Azaz nincs megoldása az $x^n + y^n = z^n$ diophantoszi egyenletnek az egész számok körében $n > 2$ természetes szám esetén. Ezzel a széljegyzetével azonban Fermat egy évszázadokon átnyúló versengést indított el a matematikusok között. Fermat $n = 4$ esetére szóló bizonyítását később megtalálták, és az itt használt módszert átvéve sikerült Euler-nek bizonyítani $n = 3$ esetére is. Csak 1993-ban sikerült Andrew Wiles-nak, egy angol matematikusnak a tétel bizonyítása.

A történeti áttekintés után következzenek a szükséges definíciók.

5.9. Definíció. $\varphi(n)$-nel jelöljük az 1 és n közé eső, n-hez relatív prím számok számát.

5.10. Definíció. Legyen $(a, m) = 1$. Az a rendje k modulo m, ha teljesülnek a következők:

$$\begin{gathered} k \in \mathbb{Z}^+, \\ a^k \equiv 1 \quad (m), \\ a^t \not\equiv 1 \quad (m)\ \forall 1 \leq t \leq k-1\text{-re}. \end{gathered}$$

Az a rendjét $o_m(a)$-val jelöljük.

5.11. Példa. 3 rendje modulo 10, 4, mert

$$\begin{aligned} 3^1 = 3 &\not\equiv 1 \quad (10) \\ 3^2 = 9 &\not\equiv 1 \quad (10) \\ 3^3 = 27 &\not\equiv 1 \quad (10) \\ 3^4 = 81 &\equiv 1 \quad (10). \end{aligned}$$

5.12. Definíció. Egy g számot primitív gyöknek nevezünk modulo m, ha $o_m(g) = \varphi(m)$.

5.13. Példa. A 3 primitív gyök modulo 10, mert $o_{10}(3) = \varphi(10) = 4$.

A 2 nem primitív gyök modulo 31, mert $o_{31}(2) = 5 < \varphi(31) = 30$.

5.14. Definíció. Legyen g primitív gyök mod p és $(a, p) = 1$. Ekkor az a-nak a g alapú diszkrét logaritmusán vagy indexén azt a $0 \leq k \leq p-2$ számot értjük, amelyre $a \equiv g^k \ (p)$.

Jelölés: $ind_{p,g}(a)$. Mivel a p modulus általában rögzített, ezért legtöbbször az erre utaló jelzést elhagyjuk: $ind_g(a)$. Ha a g primitív gyök is egyértelmű, akkor simán *inda*-t írunk.

5.15. Definíció. Az a maradékosztály redukált maradékosztály modulo m, ha $(a, m) = 1$.

5.16. Példa. Az 5 redukált maradékosztály modulo 12, de nem redukált maradékosztály modulo 10.

5.17. Definíció. Adott egész számok halmazát modulo m redukált maradékrendszernek hívjuk, ha minden elem m-hez relatív prím, és a halmaz minden modulo m redukált maradékosztályból pontosan egy elemet tartalmaz.

5.18. Példa. Az 1, 5, 7, 11 halmaz redukált maradékrendszer modulo 12.

Az 1, 13, 27, 39 halmaz redukált maradékrendszer modulo 10.

5.19. Tétel. *g primitív gyök modulo m akkor és csak akkor, ha $1, g, g^2, g^3, \ldots, g^{\varphi(m)-1}$ redukált maradékrendszer modulo m.*

5.20. Tétel. *A modulo p n-edrendű elemek száma $\varphi(n)$, ha $n|p-1$, különben 0. Így modulo p vannak primitív gyökök, számuk $\varphi(p-1)$.*

És most következzen az a tétel, amelynek bizonyításánál látni fogjuk a 5.7 tétel egy alkalmazhatóságát.

5.21. Tétel. ([9]) *Tetszés szerint megadva egy m pozitív egész számot, minden p prímszámhoz, amelyik nagyobb egy csak m-től függő korlátnál, vannak olyan p-vel nem osztható a, b, c egészek, amelyekre*

$$a^m + b^m \equiv c^m \quad (p). \tag{1}$$

Ez azt jelenti, hogy egyetlen m kitevőre sem kilátásos a Fermat sejtést úgy bizonyítani, hogy a prím modulusú kongruenciákra bizonyítjuk, mert minden m egészre és elég nagy p prímszámra megoldható az (1) kongruencia.
Bizonyítás. A bizonyításban felhasználjuk a primitív kongruenciagyök és az index fogalmát, illetve a 5.20 tételt, amely szerint prím modulushoz van primitív gyök.

Legyen m pozitív egész szám, p egy $m!e$-nél nagyobb prím, g primitív kongruenciagyök $\mod p$. Osszuk a p-nél kisebb pozitív egészeket csoportokba úgy, hogy a g-re vonatkozó indexük maradéka m-mel osztva $0, 1, 2, \ldots$ vagy $m-1$. Ezzel a p-nél kisebb pozitív egészeket beosztottuk m darab csoportba. Az i-edik csoport tehát:

$$Cs(i) = \{u : \exists t, \quad \text{hogy} \quad u \equiv g^{tm+i} \quad (p)\},$$

ahol $0 \leq tm + i \leq p - 1$, és $0 \leq i \leq m - 1$. A 5.7 tétel szerint van olyan csoport, amelyiknek három alkalmas elemére fennáll az

$$u_1 - u_2 = u_3$$

összefüggés. Ekkor a

$$u_1 - u_2 \equiv u_3 \quad (p)$$

kongruencia is fennáll. Mivel u_1, u_2 és u_3 ugyanannak a csoportnak a tagja, $\exists \;\; 0 \leq i \leq m - 1$, melyre $u_1,\ u_2,\ u_3 \in Cs(i)$. Így van olyan $t_1,\ t_2,\ t_3$, amelyekkel

$$u_j \equiv g^{t_j m+i} \quad (p),\ j = 1, 2, 3.$$

Ezt a $u_1 - u_2 \equiv u_3\ (p)$ kongruenciába helyettesítve:

$$g^{t_1 m+i} \equiv g^{t_2 m+i} + g^{t_3 m+i} \quad (p),$$

majd g^i-nel egyszerűsítve azt kapjuk, hogy

$$g^{t_1 m} \equiv g^{t_2 m} + g^{t_3 m} \quad (p),$$

vagyis az

$$a = g^{t_2},$$
$$b = g^{t_3},$$
$$c = g^{t_1}$$

értékekkel teljesül az (1) kongruencia. Tehát találtunk végtelen sok p prímet, amelyre az $a^m + b^m \equiv c^m \ (p)$ kongruenciának csak triviális megoldása van, hiszem a Fermat kongruencia, ellentétben a Fermat sejtéssel, az egészek körében mindig megoldható. □

Végül [6] alapján nézzünk még egy tételbizonyítást a Ramsey-tétel alkalmazhatóságára. A tétel Issai Schurtól származik, aki egy Németországban dolgozó orosz matematikus volt.

5.4. Schur tétel

5.22. Tétel. (Schur [9]) *Bármely t esetén létezik olyan $n = S(t)$, hogy ha az $1, 2, \ldots, n+1$ számokat akárhogyan színezzük ki t színnel, lesz olyan azonos színű a és b, amelyek $a+b$ összege is ugyanilyen színű ($a = b$ is megengedett).*

A továbbiakban $S(t)$-vel a legkisebb ilyen tulajdonságú n-et fogjuk jelölni, vagyis $S(t)$ a legnagyobb „rossz" szám: $1, 2, \ldots, S(t)$ még kiszínezhető t színnel úgy, hogy az $x+y = z$ egyenletnek ne legyen egyszínű megoldása. (A Ramsey-tételnél $R(k, t)$ a legkisebb „jó" számot jelentette; a két kissé eltérő szellemű jelölés hagyományosan így alakult ki, ezért mi is ezekhez tartjuk magunkat.)

$S(1) = 1$, mert az 1, 2 számokat 1 színnel színezve lesz olyan azonos színű a és b szám, amelyeknek az összege is ugyanilyen színű. Most speciálisan $a := b := 1$, $a + b = 2$. És mivel egy színnel színeztünk, ezek szükségképpen egyszínűek. Könnyen kiszámítható még $S(2) = 4$ is. Ezeken kívül pontos értékként viszont csak $S(3) = 13$ és $S(4) = 44$ ismert.

És most következzen Schur tételének bizonyítása.

Bizonyítás. A könnyebbség kedvéért vezessük be az $R(\underbrace{3, 3, \ldots 3}_{t}) := R(3, t)$ jelölést. Megmutatjuk, hogy $S(t) < R(3, t)$, azaz az $1, 2 \ldots R(3, t)$ számokat akárhogyan színezzük ki t színnel, teljesül az előírt tulajdonság. Tekintsük azt a teljes gráfot, amelynek csúcsai a fenti számok, és az (i, j) él (gráf)színe legyen az $|i-j|$ (szám)színe. Ekkor a Ramsey-tétel alapján keletkezik a gráfban egyszínű hároszög, azaz van olyan $i < j < m$, amelyre az (i, j), (j, m) és

(i, m) gráfélek azonos színűek, vagyis $a = j - i$, $b = m - j$ és $a + b = m - i$ (szám)színe azonos. $\square$

Hivatkozások

[1] Katona Gyula Y., Recski András, Szabó Csaba, A számítástudomány alapjai, Typotex Kft, 2006., 21-22. oldal, 86-89. oldal

[2] Internetes hivatkozás: http://people.inf.elte.hu/nebsabi/2013-2014-1/Grafelmelet/ramsey.pdf (letöltés dátuma: 2016. 02. 04.)

[3] Lovász László, Kombinatorikai problémák és feladatok, Typotex Kft, Budapest, 1999.

[4] Gyarmat Katalin, Szakdolgozat: Hatvány-, hatványteli és hatványmentes számok összegsorozatokban és multiplikatív struktúrákban

[5] Sárközy András: On difference sets of sequences of integers, II., 1977., 49-50. oldal

[6] Freud Róbert, Gyarmati Edit: Számelmélet, Nemzeti Tankönyvkiadó, Budapest, 2006., 106-120. oldal, 529-532. oldal

[7] Mike János, Tanári továbbképzés, 2011. augusztus

[8] Internetes hivatkozás: http://www.cut-the-knot.org/arithmetic/combinatorics/Ramsey333.shtml (letöltés dátuma: 2016. 02. 14)

[9] Erdős Pál, Surányi János: Válogatott fejezetek a számelméletből, Polygon, Szeged, 1996., 212-214. oldal

[10] Internetes hivatkozás: https://hu.wikipedia.org/wiki/Ramsey-tétel (letöltés dátuma: 2016.03. 28.)

[11] Internetes hivatkozás: Tamaga István, Ramsey-típusú tételek című diplomamunkája, 2012.

[12] Gyarmati Katalin: On a problem of Diophantus, Acta Arith. 97.1, (2001.), 53-65. oldal

[13] Szczepan Jelenski: Pitagorasz nyomában, Móra Ferenc Könyvkiadó, 1966., 135. oldal

[14] David Conlon: A new upper bound for diagonal Ramsey numbers, Ann. of Math. 170 (2009), 941-960.

[15] P. Erdos, Some remarks on the theory of graphs, Bull. Amer. Math. Soc. 53 (1947), 292-294.

[16] P. Erdős, G. Szekeres: A combinatorial problem in geometry, Compositio Math. 2 (1935), 463–470; Zentralblatt 12,270.