A számítástudomány alapjai

KATONA GYULA Y. — RECSKI ANDRÁS — SZABÓ CSABA

A számítástudomány alapjai

Typotex Kiadó ◇ Budapest, 2002

Ez a könyv az illetékes kuratórium döntése alapján az Oktatási Minisztérium támogatásával a Felsőoktatási Pályázatok irodája által lebonyolított Tankönyvtámogatási Program keretében jelent meg.

ISBN 963 9326 24 0

Kiadja a Typotex Elektronikus Kiadó Kft.
www.typotex.hu
Felelős kiadó Votisky Zsuzsa
Felelős szerkesztő Gerner József
A borítót tervezte Tóth Norbert
Terjedelem 13 (A/5 ív)
Készült a pécsi Bornus Nyomdában
Felelős vezető Borbély Gábor

Tartalomjegyzék

Előszó

A véges matematika különféle lehetőségek összeszámlálásával, különféle struktúrákkal (pl. a gráfelmélettel) és algoritmusokkal foglalkozik. A számítógépek elterjedése óta mind a matematikában, a számítástudományban, mind azok (műszaki, közgazdaságtani, biológiai stb.) alkalmazásaiban különösen fontos szerepet játszik.

Ez a tankönyv a véges matematika alábbi területeire nyújt bevezetést:

1. Klasszikus leszámlálási problémák, módszerek

   Nagyon rövid átismétlés, mert ezt legtöbben már a középiskolában megtanulták. Aki bonyolultabb eljárásokra is kíváncsi, a 7. fejezetben talál ilyeneket.

2. Gráfelmélet

   Ez a könyv legfontosabb – egyben leghosszabb – része. A gráfelméletnek nemcsak az alapfogalmait tartalmazza, hanem számos fejezetéből aránylag mély eredményeket is. Törekszünk az algoritmikus szemléletre; a tételekhez legtöbbször algoritmikus bizonyítást adunk.

3. Adatkezelési eljárások, gráfelméleti adatstruktúrák, a bonyolultságelmélet elemei

   Ezt a fejezetet elsősorban a villamosmérnök hallgatóknak szánjuk. A matematikusok és az informatikusok ezekről jóval többet fognak hallani későbbi tanulmányaik során; ehhez Rónyai Lajos, Ivanyos Gábor és Szabó Réka „Algoritmuselmélet” *című könyvét ajánljuk (Typotex, Budapest, 1999).*

4. A számelmélet elemei

   A matematikus hallgatóknak természetesen ennél sokkal többet kell tudniuk számelméletből – itt csak a következő fejezet megértéséhez szükséges alapismereteket tárgyaljuk.

5. Nyilvános kulcsú titkosírások

   A számítógépes adatvédelembe épp csak bepillantunk. Az érdeklődő hallgatóknak Györfi László, Győri Sándor és Vajda István „Információ- és kódelmélet” *című könyvét (Typotex, Budapest, 2000) ajánljuk.*

6. Csoportok, gyűrűk, testek, hálók

   Ez a fejezet elsősorban a műegyetemistáknak készült – a matematikus hallgatóknak az absztrakt algebrából sokkal többet kell tudniuk.

7. Rekurziók, generátorfüggvények

   Ez és a következő fejezet csak a matematikus kurzusokon szokott törzsanyag lenni, de az érdeklődő mérnökhallgatóknak is ajánljuk.

8. Extremális halmazrendszerek

Ezen témák közül az első öt és az utolsó kettő lefedi az ELTE és a BME alkalmazott matematikus hallgatói számára tartott „Véges matematika” vagy „Kombinatorika és gráfelmélet” című előadások anyagának nagy részét; az első hat pedig a BME villamosmérnök hallgatói számára tartott „Számítástudomány elemei” című tárgy anyagát. Végül a BME műszaki informatikus hallgatói számára tartott „Bevezetés a számításelméletbe” című tárgy anyaga (a más tankönyvből elsajátítandó lineáris algebrán kívül) az itteni 1–2. és 4–6. témák.

Az önállóan is olvasható 6. fejezetet Szabó Csaba írta, a többi Katona Gyula Y. és Recski András munkája. A számelméleti eredmények jelentős része így a 4. fejezetben is és a 6.8. szakaszban is előjön. Tudatosan döntöttünk a teljes könyv terjedelmét mintegy 2%-kal növelő átfedés mellett – így az olvasók megismerhetik a hagyományos tárgyalásmódot is, amikor az egész számokat egy speciális gyűrűként tekintjük, és azt a megközelítést is, amikor a számokkal végzett algoritmusok gyorsításához, bonyolultságuk vizsgálatához használjuk fel a számelmélet néhány klasszikus elemét.

Felhasználtuk korábbi jegyzeteinket, melyeket az ELTE-n és a BME-n tartott előadásainkhoz írtunk,[1] valamint számos kollégánk, elsősorban Friedl Katalin, Rónyai Lajos és Simonyi Gábor észrevételeit. Rajtuk kívül köszönet illeti hallgatóinkat is, akik a jegyzetek korábbi változataiban számos elírást, sajtóhibát, stb. találtak és kérdéseikkel, megjegyzéseikkel segítették a szöveg véglegesítését.

Budapest, 2001. szeptember 30.

[1] Jórészt a nyári szünetekben, mint azt (az akkor 9 és fél éves) Recski Júlia költeménye mutatja:
Balatoni édes ritmus
Ihlette az algoritmus
T.

1. fejezet

Klasszikus leszámlálási problémák

1.1. Permutációk, variációk, kombinációk

Az itt következő fogalmakat és tételeket valószínűleg már sokan ismerik középiskolai tanulmányaikból. Ezért a definíciókon kívül csak egy–egy feladaton mutatjuk be a fogalmakat.

1.1.1. Feladat. *Egy egyetemi hallgatónak n vizsgát kell letennie. Hány különböző sorrendben teheti ezt meg? (minden vizsgát pontosan egyszer kell letenni)*

MEGOLDÁS: Az első vizsgát n-féleképpen választhatjuk ki. Ha az első vizsgát letette a hallgató, akkor akármelyik is volt az első vizsga, a második vizsgánál $n-1$ választási lehetőségünk van. Tehát az első két vizsgát $n(n-1)$-féleképpen választhatjuk ki. A harmadik vizsgánál további $n-2$ választási lehetőség van. Az okoskodást így folytatva látható, hogy az utolsó előtti vizsgánál 2 választási lehetőség van, míg az utolsónál már nincs választási lehetőségünk. Tehát n vizsgát $n(n-1)(n-2)(n-3)\cdots 2\cdot 1$-féle különböző sorrendben lehet letenni. □

1.1.2. Definíció. *Az $n(n-1)(n-2)(n-3)\cdot\ldots\cdot 2\cdot 1$ szorzatot n* ***faktoriálisnak*** *nevezzük. Jele: $n!$. Definíció szerint: $0!=1$.*

1.1.3. Definíció. *n elem összes lehetséges sorrendje: n (ismétlés nélküli)* ***permutációi****. Ezek száma $n!$.*

Az előbbi feladatban tehát n vizsga permutációinak számát határoztuk meg.

1.1.4. Feladat. *Tegyük fel, hogy az előbbi hallgató k_1 vizsgájára 1-est, k_2 vizsgájára 2-est, k_3-ra 3-ast, k_4-re 4-est és k_5-re 5-öst kapott. Hányféle sorrendben írhatja fel a jegyeket egy papírra, ha nem írja mellé, melyik vizsgára kapta?*

MEGOLDÁS: Először tegyük fel, hogy odaírtuk a jegyek mellé, hogy melyik vizsgára adták. Így a fentiek szerint $n!$ sorrend lehet. Viszont így többször számoltuk azokat a jegysorozatokat, amelyikben csak például a 3-asok sorrendje különbözik. Mivel a 3-asokat $k_3!$-féleképpen cserélhetjük fel, pontosan ennyiszer számoltuk ezeket. Hasonlóan $k_1!$-szor azokat, amelyekben csak az 1-esek sorrendje különbözik, stb. Tehát a jegyek különböző sorrendjeinek száma

$$\frac{(k_1+k_2+k_3+k_4+k_5)!}{k_1!\cdot k_2!\cdot k_3!\cdot k_4!\cdot k_5!}.$$

□

1.1.5. Definíció. *k_1 darab első típusú elem, k_2 darab második típusú elem, …, k_n darab n-dik típusú elem lehetséges sorbaállításai a $k_1+k_2+\ldots+k_n$ elem* ***ismétléses permutációi****. Ezek száma:*

$$\frac{(k_1+k_2+\ldots+k_n)!}{k_1!\cdot k_2!\cdot\ldots\cdot k_n!}$$

Most olyan problémákat vizsgálunk, amelyekben nem kell minden elemnek szerepelnie a sorban.

1.1.6. Feladat. *Az egyetemen összesen n különböző óránk van. Ezek közül k darabot akarunk hétfőre tenni. Hányféle lehet a hétfői órarend?*

MEGOLDÁS: Kövessük az ismétlés nélküli permutációnál megismert módszert. Az első órát n-féleképpen választhatjuk ki. A második órát már csak $n-1$-féleképpen választhatjuk ki. És így tovább, végül a k-adik órát $n-k+1$-féleképpen választhatjuk ki. Több választási lehetőség nincs, hiszen ekkor már megvan a hétfői órarend. Tehát a lehetséges órarendek száma $n(n-1)(n-2)\cdot\ldots\cdot(n-k+1)$. □

1.1.7. Definíció. *n elemből az összes lehetséges sorrendben k darab különböző kiválasztása: az n elem k-adosztályú (ismétlés nélküli)* ***variációi****. Ezek száma*

$$n(n-1)(n-2)\cdot\ldots\cdot(n-k+1)=n!/(n-k)!.$$

(A baloldalon k szorzótényező szerepel.)

Megjegyezzük, hogy a permutáció a variáció speciális esete, $k=n$-re épp a permutációt kapjuk.
A most következő feladatban ismét lehetnek egyformák a kiválasztott elemek között.

1.1.8. Feladat. *Egy k tagú évfolyamot hányféleképpen oszthatunk be az 1-es, 2-es, …, n-es sorszámú csapatokba? Lehetnek olyan csapatok is, ahova senki nem kerül.*

MEGOLDÁS: Hogy az első hallgató melyik csapatba tartozzon, azt n-féleképpen választhatjuk ki. Ugyanígy azt is n-féleképpen dönthetjük el, hogy melyik csapatba járjon a második, harmadik, ..., k-adik hallgató. Így a választási lehetőségek száma n^k. □

1.1.9. Definíció. *n elemből képezhető k tagú sorozatok (egy-egy elem többször is szerepelhet): az n elem k-adosztályú* ***ismétléses variációi****. Ezek száma n^k.*

Az eddigi feladatokban mindig fontos volt a kiválasztott elemek sorrendje. A következőkben viszont nem törődünk a sorrenddel.

1.1.10. Feladat. *Egy n tagú csapatból k-an kaphatnak kiemelt ösztöndíjat. Hányféleképpen választhatók ki az ösztöndíjat kapók?*

MEGOLDÁS: Először rangsoroljunk k hallgatót. Ez egy ismétlés nélküli variációs feladat, tehát ezt $n(n-1)\cdot\ldots\cdot(n-k+1)$-féleképpen tehetjük meg. Mivel a sorrend nem számít abban, hogy ki kap ösztöndíjat és ki nem, minden lehetőséget többször számoltunk. Éppen annyiszor, ahányféleképpen a már rangsorolt k diákot permutálhatjuk, azaz $k!$-szor. Tehát az ösztöndíjat kapó k diákot

$$\frac{n(n-1)\cdot\ldots\cdot(n-k+1)}{k!}$$

módon választhatjuk ki. □

1.1.11. Definíció. *Egy n elemű halmaz k elemű részhalmazai: n elem k-adosztályú (ismétlés nélküli)* ***kombinációi****. Ezek számát jelöljük $\binom{n}{k}$-val. Azaz*

$$\binom{n}{k} = \frac{n(n-1)\cdot\ldots\cdot(n-k+1)}{k!}.$$

$\binom{n}{k}$-t ***binomiális együtthatónak*** *nevezzük.*

Megjegyzés: A definícióból következően $\binom{n}{0} = \binom{n}{n} = 1$ és $\binom{n}{k} = 0$, ha $k > n$.

1.1.12. Feladat. *A büfében n-féle sütemény kapható. Hányféleképpen vehetünk k darabot?*

MEGOLDÁS: Minden lehetséges vásárlást egy a 0 és 1 számjegyekből álló rendezett sorozattal fogunk jellemezni. Először írjunk fel annyi egyest, ahány darabot az első féle süteményből vásároltunk. Ezután írjunk egy 0-t, majd annyi egyest, ahányat a második féle süteményből választottunk. Majd ismét írjunk egy 0-t, és folytassuk ezt a módszert. A sorozat végén annyi egyes áll, ahány darabot a n-edik süteményből vettünk. Ha valamelyik süteményből nem vettünk, akkor ott két 0 áll egymás mellett. Tehát így minden lehetséges vásárlásnak megfeleltettünk egy ilyen sorozatot, és minden sorozathoz is pont egy vásárlás tartozik. Elég tehát meghatározni

a különböző sorozatok számát. Vagyis, hány olyan sorozat van, amelyben k darab egyes és $n-1$ darab nulla van. Ez éppen $n+k-1$ elem k-adosztályú kombinációja, ezek száma pedig $\binom{n+k-1}{k}$. □

1.1.13. Definíció. *n elemből k kiválasztása, ha a sorrend nem számít, de az elemek többször is szerepelhetnek: n elem k-adosztályú* ***ismétléses kombinációi****. Számuk* $\binom{n+k-1}{k}$.

Eddig tehát megismertük az ismétléses és ismétlés nélküli permutációkat, variációkat és kombinációkat. Ezek során többször is találkoztunk binomiális együtthatókkal. Most ezeknek néhány tulajdonságát ismertetjük. Legelőször Newton binomiális tételét bizonyítjuk be.

1.1.14. Tétel (binomiális tétel). *Tetszőleges valós x,y-ra és nemnegatív egész n-re*

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \\ + \binom{n}{k}x^{n-k}y^k + \ldots + \binom{n}{n}y^n. \qquad (1.1)$$

BIZONYÍTÁS: Írjuk fel $(x+y)^n$-t a következő alakban:

$$(x+y)^n = (x+y)(x+y)\cdot\ldots\cdot(x+y).$$

Bontsuk fel sorban a zárójeleket, miközben ügyeljünk arra, hogy az összes szorzókat abban a sorrendben írjuk fel, amelyben adódtak. Például $n=3$ esetén

$$(x+y)^3 = xxx+xxy+xyx+xyy+yxx+yxy+yyx+yyy.$$

Látható, hogy a zárójelek felbontása után az x és y elemekből készíthető összes n-edosztályú ismétléses variáció fellép, mégpedig pontosan egyszer. Most számoljuk meg, hány olyan tag van, amelyikben pont k darab x van az n darab szorzótényező között. Ez éppen az n elem k-adosztályú kombinációinak száma, azaz $\binom{n}{k}$. Ha tehát összevonjuk az ugyanannyi x-et tartalmazó tagokat, akkor (1.1)-et kapjuk. □

A most következő tételek egyszerűen adódnak a binomiális tételből, ha az x és y helyére megfelelő számértékeket helyettesítünk. Mi azonban itt kombinatorikai bizonyításokat adunk.

1.1.15. Tétel. *Minden n nemnegatív egész számra*

$$\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{n-1}+\binom{n}{n} = 2^n.$$

BIZONYÍTÁS: Számoljuk meg kétféleképpen, hány n hosszú 0–1 sorozat van. Ez egyrészt 2 elem n-edosztályú ismétléses variációja, amelyek száma 2^n. Másrészt számoljuk meg, hány olyan n hosszú 0–1 sorozat van, amelyben pontosan $0,1,2,\dots,n-1$, illetve n darab 1-es van. Ez pedig éppen az a szám, ahányféleképpen n elem közül kiválaszthatunk k darabot, vagyis $\binom{n}{k}$. Mivel ugyanazokat a sorozatokat számoltuk meg, a két mennyiség egyenlő, és ez épp a tétel állítása. □

Ha most a $0,1,2$ elemekből álló n hosszú sorozatokat számoljuk össze, hasonlóan kétféleképpen, akkor a következőt kapjuk:

$$\sum_{i=0}^{n} 2^i \binom{n}{i} = 3^n.$$

Nyilvánvaló, hogy megegyezik a k darab 1-est tartalmazó n hosszúságú 0–1 sorozatok, és az $n-k$ darab 0-t tartalmazó n hosszúságú sorozatok száma. Így

$$\binom{n}{k} = \binom{n}{n-k}.$$

Számoljuk meg, hány olyan n hosszúságú, k darab 1-est tartalmazó 0–1 sorozat van, amelynek első tagja 1-es. Ilyen $\binom{n-1}{k-1}$ van, hiszen a többi $n-1$ helyen épp $k-1$ darab 1-esnek kell állnia. Viszont olyan sorozat, amelynek első helyén 0 áll, $\binom{n-1}{k}$ darab van. Így viszont összeszámoltuk az összes n hosszúságú, k darab 1-est tartalmazó sorozatot. Tehát

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}. \tag{1.2}$$

A továbbiakban bemutatunk néhány összetettebb leszámlálási feladatot és megoldásaikat.

1.1.16. Feladat. *Bizonyítsuk be, hogy*

$$\sum_{k=0}^{n} \binom{m+k}{k} = \binom{m+n+1}{n}.$$

MEGOLDÁS: Az egyelőség bal oldalán álló összeget kifejtve az első két tag $\binom{m}{0} + \binom{m+1}{1}$. Mivel $\binom{m}{0} = 1$, helyettesíthetjük $\binom{m+1}{0}$-val, ami szintén 1. Így viszont az első két tagra alkalmazhatjuk az (1.2) azonosságot. Tehát az első két tag helyett írhatunk $\binom{m+2}{1}$-t. Ekkor ismét alkalmazhatjuk az (1.2) azonosságot az új összeg első két tagjára: $\binom{m+2}{1} + \binom{m+2}{2} = \binom{m+3}{2}$. A továbbiakban is mindig összeadhatjuk a keletkező első két tagot. Az utolsó lépésben: $\binom{m+n}{n-1} + \binom{m+n}{n} = \binom{m+n+1}{n}$. □

1.1.17. Feladat. *Bizonyítsuk be, hogy*

$$\sum_{k=0}^{\infty} \binom{r}{k} \binom{s}{n-k} = \binom{r+s}{n}.$$

Megjegyzés: Furcsának tűnhet, hogy a bal oldalon az összegzés $k=0$-tól végtelenig történik. Vegyük észre azonban, hogy ha $k>r$ vagy $n-k>s$, akkor a megfelelő tag 0 lesz, ezért nem kell vesződnünk vele, hogy meghatározzuk, adott r,s és n esetén mely tagok „értelmesek”.

MEGOLDÁS: Tegyünk egy dobozba r piros és s kék színű különböző tárgyat. Nyilván igaz, hogy összesen $\binom{r+s}{n}$–féleképp választhatunk ki n tárgyat. Most számoljuk össze, hogy hányféleképp választhatunk ki n tárgyat úgy, hogy közöttük éppen k darab legyen piros. Világos, hogy a k piros tárgyat $\binom{r}{k}$–féleképp választhatjuk ki. Akárhogy is választottunk, ki kell még választanunk pontosan $n-k$ kék tárgyat is, amit $\binom{s}{n-k}$–féleképp tehetünk meg, ezért az ilyen kiválasztások száma $\binom{r}{k}\binom{s}{n-k}$. Ha ezt összegezzük minden lehetséges k-ra, akkor megint csak azt számoltuk össze, hogy hányféleképp választhatunk ki n tárgyat. □

1.1.18. Feladat. *Hányféleképp állíthatunk sorba n fiút és n lányt, ha két fiú nem állhat egymás mellett, de két lány esetleg igen?*

MEGOLDÁS: Először számoljuk meg hány sorrend lehetséges, ha a fiúkat, illetve a lányokat egymás között nem különböztetjük meg. Ha n fiú és $n-1$ lány lenne, akkor nyilván csak a $FLFL\ldots FLF$ sorrend jön szóba. Viszont az n-edik lányt állíthatjuk az első fiú elé, vagy az első és második közé (ahol ekkor 2 lány áll), vagy a második és harmadik közé, ..., vagy az utolsó fiú után. Ez $n+1$ lehetőség. Ha most megkülönböztetjük a fiúkat egymástól, akkor egymás között $n!$-féleképp cserélhetik fel a sorrendet. Ugyanez a helyzet az n lánnyal is. Tehát az összes lehetőségek száma $(n+1)(n!)^2$. □

1.1.19. Feladat. *Hányféleképp választható ki 3 különböző szám az $1,2,\ldots,100$ számok közül úgy, hogy az összegük osztható legyen 3-mal?*

MEGOLDÁS: Vegyük észre, hogy az összeg csak úgy lehet 3-mal osztható, ha mindhárom szám azonos maradékot ad 3-mal osztva, vagy pedig mindhárom különbözőt. Mivel a számok közül 33 darab ad 0 maradékot, $\binom{33}{3}$-féleképp választhatunk ki 3 különböző 0 maradékot adót. Hasonlóan, $\binom{34}{3}$-féleképp választhatunk ki 3 különböző 1 maradékot adót és $\binom{33}{3}$-féleképp 3 különböző 2 maradékot adót. Amikor 3 különböző maradékot adót akarunk kiválasztani, akkor $33\cdot 34\cdot 33$-féleképp választhatunk. Tehát az összes lehetőségek száma

$$\binom{33}{3}+\binom{34}{3}+\binom{33}{3}+33\cdot 34\cdot 33.$$

□

1.1.20. Feladat. *Hányféleképp lehet kiosztani az 52 lapos franciakártya-csomagot 4 játékosnak úgy, hogy mindenki 13 lapot kapjon, és András pontosan 2 ászt és 5 treffet (♣) kapjon?*

MEGOLDÁS: Két alapvető esetet kell megkülönböztetnünk a szerint, hogy András kapja-e a treff ászt vagy sem.
Ha nem, akkor először Andrásnak $\binom{3}{2}$-féleképp választhatunk két ászt, majd bármely ilyen választás esetén $\binom{12}{5}$-féleképp választhatunk ki 5 treffet a maradék 12 treff közül (hiszen a treff ászt nem választhatjuk). András maradék 6 lapját úgy kell választanunk, hogy azok között sem ász, sem treff nem lehet. Ilyen lap $52-4-13+1=36$ van, ezért a lehetőségek száma $\binom{36}{6}$. Miután Andrásnak már kiválasztottunk 13 lapot, a második játékosnak a maradék 39 lapból választhatunk $\binom{39}{13}$, a harmadik játékosnak már csak 26 lapból választhatunk $\binom{26}{13}$-féleképp, míg a negyedik játékos megkapja a maradék lapokat.
A másik esetben András megkapja a treff ászt. $\binom{3}{1}$-féleképp kaphat még egy ászt és $\binom{12}{4}$-féleképp még 4 treffet. Végül $\binom{36}{7}$-féleképp kaphat további lapokat. A többiek az előző esettel megegyező módon $\binom{39}{13}\binom{26}{13}$-féleképp kaphatják meg a lapjaikat.
Tehát az összes lehetőségek száma:

$$\left[\binom{3}{2}\binom{12}{5}\binom{36}{6}+\binom{3}{1}\binom{12}{4}\binom{36}{7}\right]\binom{39}{13}\binom{26}{13}=$$
$$=\left[\binom{4}{2}\binom{12}{5}\binom{36}{6}+\binom{3}{1}\binom{12}{4}\binom{36}{7}\right]\frac{39!}{(13!)^3}$$

□

1.2. Skatulya–elv

Skatulya-elv: Ha van n darab gyufásdobozunk és $n+1$ gyufaszálunk, akkor akárhogy rakjuk bele az összes gyufát a skatulyákba, valamelyik skatulyába legalább 2 gyufa jut.
Két tételt fogunk mutatni, amelynek bizonyítása a skatulya–elven alapszik.

1.2.1. Tétel (Erdős–Szekeres, 1935). *Bármelyik $nk+1$ darab különböző számból álló sorozatban van vagy egy n-nél hosszabb csökkenő részsorozat, vagy egy k-nál hosszabb növekvő részsorozat.*

BIZONYÍTÁS: Legyen az eredeti sorozat $x_1, x_2, \ldots, x_{nk+1}$. Jelöljük a_i-vel a leghosszabb, x_i-vel kezdődő csökkenő részsorozat hosszát, b_i-vel pedig a leghosszabb, x_i-vel kezdődő növekvő részsorozat hosszát. Ha $i<j$ esetén $x_i>x_j$, akkor nyilvánvaló, hogy $a_i>a_j$. Hasonlóan, ha $x_i<x_j$, akkor $b_i>b_j$. Ebből következik, hogy ha $i\neq j$, akkor az (a_i,b_i) pár különbözik az (a_j,b_j) pártól, hiszen vagy $a_i\neq a_j$ vagy $b_i\neq b_j$. Így tehát minden $1\leq i\leq nk+1$-re különböző párt kell kapnunk. Ha azonban minden i-re $a_i\leq n$ és $b_i\leq k$, akkor csak nk különböző párt kaphatunk, vagyis a skatulya–elv miatt ellentmondásra jutottunk. (Ebben az esetben a gyufák szerepét az $nk+1$ különböző index, a skatulyákét pedig az nk darab pár játsza.) □

1.2.2. Tétel (Erdős–Hajnal, 1966). *Vegyünk egy X halmazt ($|X| = n$), és ennek különböző pontosan 3 elemű részhalmazait úgy, hogy ha $F_1, F_2 \in \mathcal{F}$ két részhalmaz a kiválasztott részhalmazok közül, akkor $|F_1 \cap F_2| \neq 2$. Ekkor létezik olyan $Y \subseteq X$, hogy $|Y| \geq \lfloor \sqrt{2n} \rfloor$ és minden $F \in \mathcal{F}$ -re $F \not\subset Y$.*

BIZONYÍTÁS: Tegyük fel, hogy van egy olyan k elemű Y részhalmaz, amit nem lehet tovább bővíteni, azaz akárhogy veszünk hozzá egy új elemet, akkor Y' már tartalmazni fog egy $F \in \mathcal{F}$ -et. Ez csak úgy lehet, hogy ennek az F-nek két pontja benne van Y-ban, a harmadik pont pedig az, amit hozzá akartunk venni. Minden külső ponthoz tartozik tehát egy Y-beli pontpár. Két különböző külső ponthoz nem tartozhat ugyanaz a pár, mert ekkor ennek a két $\mathcal{F}$ -beli halmaznak a metszete kételemű lenne. Tehát a külső pontok száma legfeljebb annyi, mint a párok száma:

$$\binom{k}{2} \geq n - k.$$

Ez pozitív k-ra csak úgy lehetséges, ha

$$k \geq \frac{-1+\sqrt{1+8n}}{2} = \sqrt{\frac{1}{4}+2n} - \frac{1}{2}.$$

Az pedig világos, hogy

$$\left\lceil \sqrt{\frac{1}{4}+2n} - \frac{1}{2} \right\rceil \geq \left\lfloor \sqrt{2n} \right\rfloor,$$

vagyis Y megfelel a feltételeknek. (A skatulya-elv egyszerű következményét használtuk, hogy ha kevesebb gyufa van, mint doboz, akkor marad üres doboz.) □

1.3. Szita módszer

Szokásos feladat, hogy hány olyan 1000-nél kisebb természetes szám van, amely nem osztható sem 2-vel, sem 3-mal, sem 5-tel. Összesen 999 darab ezernél kisebb természetes szám van, ebből le kell vonnunk a 2-vel oszthatók számát, $\lfloor 999/2 \rfloor$ darabot, majd a 3-mal, illetve 5-el oszthatókat, $\lfloor 999/3 \rfloor$ darabot, illetve $\lfloor 999/5 \rfloor$ darabot. Így azonban kétszer is levontuk azokat, amik $2 \cdot 3$-mal, $3 \cdot 5$-tel, illetve $2 \cdot 5$-tel oszthatók, hiszen például a 12-t levontuk akkor is, amikor a 2-vel oszthatókat vontuk le, és akkor is, amikor a 3-mal oszthatókat. Tehát hozzáadunk $\lfloor 999/2 \cdot 3 \rfloor + \lfloor 999/2 \cdot 5 \rfloor + \lfloor 999/3 \cdot 5 \rfloor$-t.
Most nézzük meg, mi történt a $2 \cdot 3 \cdot 5$-tel oszthatókkal! Levontuk háromszor, majd hozzáadtuk háromszor, hiszen minden tagba beleszámoltuk. Ezért le kell vonnunk még $\lfloor 999/2 \cdot 3 \cdot 5 \rfloor$-t. Tehát a keresett számok száma

$$999 - \left\lfloor \frac{999}{2} \right\rfloor - \left\lfloor \frac{999}{3} \right\rfloor - \left\lfloor \frac{999}{5} \right\rfloor + \left\lfloor \frac{999}{2 \cdot 3} \right\rfloor + \left\lfloor \frac{999}{3 \cdot 5} \right\rfloor + \left\lfloor \frac{999}{2 \cdot 5} \right\rfloor - \left\lfloor \frac{999}{2 \cdot 3 \cdot 5} \right\rfloor = 266.$$

Ezt a módszert nevezik szita módszernek. Hasonló módszerrel megadhatjuk az n számnál kisebb, n-hez relatív prím számok $\varphi(n)$ számát.

$$\varphi(n) = n - \sum_{p_i|n} \frac{n}{p_i} + \sum_{p_i,p_j|n} \frac{n}{p_i p_j} - \sum_{p_i,p_j,p_k|n} \frac{n}{p_i p_j p_k} + \ldots = n \prod_{p_i|n} \left(1 - \frac{1}{p_i}\right)$$

Ugyanígy megadható az $A_1, A_2, \ldots A_n$ halmazok uniójának elemszáma.

$$|\cup A_i| = \sum_{i=1}^{n} |A_i| - \sum_{i,j=1}^{n} |A_i \cap A_j| + \sum_{i,j,k=1}^{n} |A_i \cap A_j \cap A_k| - \ldots$$

Az utolsó példa a szita módszerre, hogy hány olyan permutációja van az $1, 2, \ldots,$ n számoknak, amikor egyik sincs a helyén, azaz $a_i \neq i$:

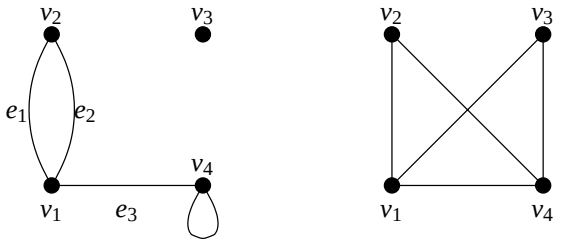
$$n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \ldots = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \approx \frac{n!}{e}.$$

2. fejezet

Gráfelmélet

2.1. Alapfogalmak

A matematika számos területén gyakran előfordul, hogy egy bizonyos halmaz elemeiből vett párokkal foglalkozunk. Szokásos, hogy a halmaz elemeit pontokkal jelöljük a síkon, és a tekintett pároknak megfelelő pontokat egy vonallal összekötjük. Nem érdekes sem a pontok elhelyezkedése a síkon, sem a vonalak formája, de a vonalak nem mehetnek keresztül egy harmadik ponton. Ilyen rajzok láthatók a 2.1. ábrán.



2.1. ábra.

Ezeket fogjuk gráfoknak nevezni. Most definiáljuk formálisan a gráfot, és néhány további alapfogalmat.

2.1.1. Definíció. *Egy **gráf** egy rendezett pár, $G = (V,E)$, ahol V egy nem-üres halmaz, E pedig ebből a halmazból képezhető párok egy halmaza. V elemeit **pontoknak** vagy **csúcsoknak**, E elemeit **éleknek** nevezzük. Ha egy G gráfról beszélünk, akkor $V(G)$-vel illetve $E(G)$-vel jelöljük a gráf pontjainak illetve éleinek halmazát, míg a pontok illetve élek számát $v(G)$-vel ill. $e(G)$-vel jelöljük.*
*Ha az $e \in E$ él a $\{v_1, v_2\}$ párnak felel meg, akkor ez a két pont e **végpontja**. 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.*

Ha $e, f \in E$ végpontjai $\{v_1, v_2\}$ ill. $\{w_1, w_2\}$, és $\{v_1, v_2\} \cap \{w_1, w_2\} \neq \emptyset$, akkor e, f ***szomszédos élek****. Hasonlóan, v_1 és v_2* ***szomszédos pontok****, ha $\{v_1, v_2\} \in E$. v_1* ***illeszkedik*** *e-re, ha annak egyik végpontja.*
Egy pont ***izolált pont****, ha nincsen vele szomszédos másik pont, vagyis nem illeszkedik egyetlen élre sem. Egy pontra illeszkedő élek száma a pont* ***fokszáma****. Egy esetleges hurokél kettővel növeli a fokszámot. A v pont fokszámát $d(v)$-vel jelöljük. A maximális fokszámot Δ-val, a minimálist δ-val fogjuk jelölni.*
*k-****reguláris*** *egy gráf, ha minden pontjának foka k.*
Ha egy n pontú egyszerű gráf tetszőleges két pontja szomszédos, akkor n-pontú ***teljes gráfnak*** *nevezzük, és K_n-nel jelöljük.*

2.1.2. Állítás. *Minden gráfra igaz, hogy a fokszámok összege az élszám kétszerese:*

$$\sum_{v_i \in V(G)} d(v_i) = 2e(G).$$

Ebből következően a fokszámok összege páros szám.

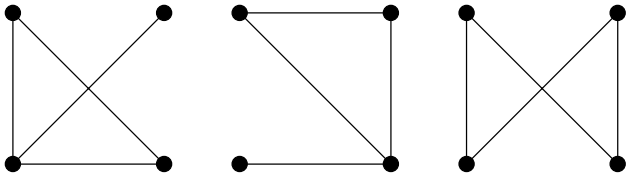
BIZONYÍTÁS: Amikor a fokszámokat összegezzük, minden pontra megszámoljuk a hozzá illeszkedő élek számát és ezeket összegezzük. Mivel minden élnek két végpontja van, így minden élet pontosan kétszer számolunk meg, egyszer-egyszer mindkét végénél. □

Nézzük meg, mit jelentenek ezek a fogalmak a 2.1. ábrán látható gráfokon. Az első gráf $G = (V, E)$, ahol $V = \{v_1, v_2, v_3, v_4\}$ és $E = \{e_1, e_2, e_3, e_4\}$. A v_3 pont izolált pont. e_1 és e_2 párhuzamos élek, e_4 hurokél. Így az első gráf nem egyszerű, míg a második az. A második gráfon szomszédos például az v_1 és v_2, de nem szomszédos v_2 és v_3. v_4 fokszáma 3, v_3-é 2. Az első gráfon v_4 fokszáma 3, v_3-é pedig 0.
Említettük már, hogy egy gráfot több különböző módon le lehet rajzolni. A következő definíció épp azt fejezi ki, hogy ezek a rajzok ugyanazt a gráfot jelölik.

2.1.3. Definíció. *A $G = (V, E)$ és a $G' = (V', E')$ gráfok* ***izomorfak****, ha van olyan egy–egy értelmű megfeleltetés – bijekció – V és V' között, hogy G-ben pontosan akkor szomszédos két pont, ha G'-ben a nekik megfelelő pontok szomszédosak, és szomszédos pontpárok esetén ugyanannyi él fut közöttük.*

A 2.2. ábrán látható három gráf közül az első kettő izomorf, a harmadik viszont nem izomorf velük.
Könnyű ellenőrizni, hogy két gráf izomorf-e, ha adva van egy megfelelő bijekció. Azonban találni egy megfelelő bijekciót, vagy bebizonyítani, hogy nincs ilyen, nagyon nehéz. Előfordulhat, hogy $v!$ esetet kell végignézni. Ez pedig már $v = 22$-nél is eltart kb. 35641 évig egy másodpercenként 10^9 műveletet végző számítógéppel.

2.1.4. Definíció. *A $G' = (V', E')$ gráf a $G = (V, E)$ gráf* ***részgráfja****, ha $V' \subseteq V$, $E' \subseteq E$ valamint egy pont és egy él pontosan akkor illeszkedik egymásra G'-ben, ha G-ben is illeszkedők.*



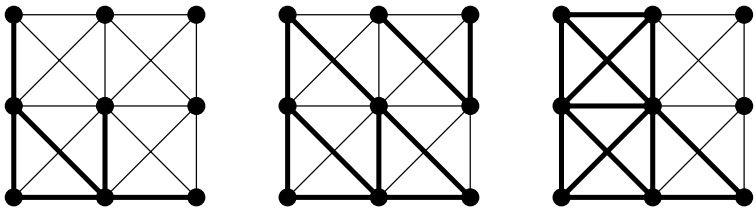
2.2. ábra.

Ez utóbbi azért szükséges, mert különben előfordulhatna, hogy egy él végpontja nem tartozik a gráfhoz. Részgráfot kapunk, ha elhagyunk néhány pontot a hozzá illeszkedő élekkel együtt, valamint esetleg még néhány élet is.

2.1.5. Definíció. *Egy $G' = (V', E')$ gráf a $G = (V, E)$ gráf* ***feszítő részgráfja****, ha G' részgráfja G-nek és $V' = V$, azaz ha a részgráf G összes pontját tartalmazza.*

2.1.6. Definíció. *Ha E' pontosan azokból az E-beli élekből áll, amelyeknek mindkét végpontja V'-ben van, és E' az összes ilyen élet tartalmazza, akkor G' a G gráf V' által* ***feszített részgráfja****.*

A 2.3. ábra bal oldalán a vastag vonalak egy részgráfot alkotnak, amely se nem feszítő, se nem feszített részgráf. A középső ábrán viszont feszítő részgráfot láthatunk, míg a jobb oldalon egy feszített részgráfot.



2.3. ábra.

2.1.7. Definíció. *A G'* ***részgráf komplementere*** *az a $G'' = (V'', E'')$ gráf, melyre $V'' = V$ és $E'' = E - E'$. Egy G gráf* ***komplementerén*** *azt a $\overline{G}$ gráfot értjük, amelyet akkor kapunk, ha G-t a $K_{v(G)}$ teljes gráf részgráfjának tekintjük. Vagyis $\overline{G}$-ben azok a pontpárok vannak összekötve, amelyek G-ben nincsenek.*

2.1.8. Definíció. *Egy $(v_0, e_1, v_1, e_2, v_2, \ldots, v_{k-1}, e_k, v_k)$ sorozatot* ***élsorozatnak*** *nevezünk, ha e_i a v_{i-1}-t és v_i-t összekötő él. Ha $v_0 = v_k$, akkor az élsorozat* ***zárt****. Ha a csúcsok mind különbözőek, akkor egy* ***utat*** *definiáltunk. Ha $v_0 = v_k$ és különben a csúcsok mind különbözőek, akkor ez egy* ***kör*** *a gráfban. Az út vagy kör* ***hosszán*** *az őt alkotó élek számát értjük. Egyszerű gráfban $(v_0, v_1, \ldots, v_k)$-val írjuk le az utat.*

2.1.9. Tétel. *Definiáljuk a $p \equiv q$ relációt úgy, hogy $p \equiv q$ akkor és csak akkor, ha $p,q \in V(G)$ és vezet út p és q között, vagy $p = q$. Ez egy ekvivalencia reláció.*

BIZONYÍTÁS: A reflexivitás és a szimmetria triviális. Csak a tranzitivitást kell belátnunk. Legyen $(p,e_0,p_1,e_1,\ldots,q)$ a p-t és q-t összekötő, $(q,f_0,q_1,f_1,\ldots,r)$ a q-t és r-et összekötő út. Legyen p_i a legkisebb indexű p, amely előfordul a q-k között. Mondjuk $p_i = q_j$. Ekkor a $(p,e_0,p_1,e_1,\ldots,p_i,f_j,q_{j+1},\ldots,r)$ egy p-t és r-et összekötő út. □

2.1.10. Definíció. *A fenti reláció ekvivalencia osztályokat határoz meg G pontjain. Az egy osztályba eső pontok által feszített részgráfokat a G gráf **összefüggő komponenseinek** hívjuk, számukat $c(G)$-vel jelöljük. Ha a komponensek száma 1, vagyis ha G bármely két pontja között vezet út, akkor a G gráf **összefüggő**.*

A későbbiekben szükség lesz a következő fogalmakra is.

2.1.11. Definíció. *Egy $X \subseteq E$ élhalmazt **elvágó élhalmaznak** nevezünk, ha az X-beli élek elhagyásával nő a gráf komponenseinek száma, azaz a gráf több komponensre esik, mint ahányból eredetileg állt. X **vágás**, ha elvágó, de semelyik valódi részhalmaza nem az. Az egyelemű vágásokat **elvágó éleknek** nevezzük.*
*Néha szükségünk lesz arra, hogy **irányított gráfokkal** foglalkozzunk, vagyis olyanokkal, amelyeknek élei nem $\{v_1,v_2\}$ alakú rendezetlen párok, hanem (v_1,v_2) alakú rendezett párok. Egy ilyen (v_1,v_2) élnek v_1 a **kezdőpontja**, v_2 a **végpontja**. Rajzban az élet egy v_1-ből v_2-be mutató nyíllal ábrázoljuk. **Forrásnak** hívunk egy pontot, ha egyetlen élnek sem végpontja, **nyelőnek**, ha egyetlen élnek sem kezdőpontja.*
*Irányított gráfban egy $(v_0,e_1,v_1,e_2,v_2,\ldots,e_k,v_k)$ utat akkor hívunk **irányított útnak**, ha $e_1 = (v_0,v_1), e_2 = (v_1,v_2),\ldots,e_k = (v_{k-1},v_k)$. Az **irányított kör** definíciója hasonló. Egy irányított gráf **erősen összefüggő**, ha bármely pontjából bármely más pontjába vezet irányított út.*

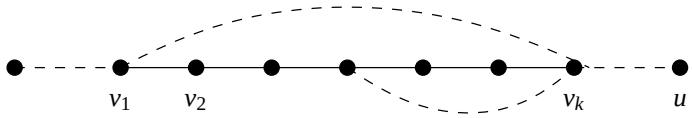
2.2. Fák és tulajdonságaik

2.2.1. Definíció. *Az összefüggő körmentes gráfokat **fáknak** nevezzük.*

Most a fákra vonatkozó néhány egyszerű tételt bizonyítunk be.

2.2.2. Tétel. *Minden legalább 2 pontú fában van legalább két elsőfokú pont.*

BIZONYÍTÁS: Tekintsük a fában található leghosszabb utat, legyen ez $(v_1,v_2,\ldots,v_k)$. Belátjuk, hogy ennek mindkét végpontja, v_1 és v_k, elsőfokú. Tegyük fel, hogy v_k nem elsőfokú, azaz vezet belőle még egy él a fa valamely pontjába. Az út többi pontjába nem vezethet, hiszen ekkor kört tartalmazna a fa. Ha pedig egy új u pontba vezet az él, akkor az eredeti utat evvel megtoldva egy hosszabb utat kapnánk, $(v_1,\ldots,v_k,u)$-t, ez pedig ellentmond a feltevésünknek (2.4. ábra). □



2.4. ábra.

2.2.3. Tétel. *Egy n pontú fa éleinek száma $n-1$.*

BIZONYÍTÁS: Bizonyítsunk a pontszámra vonatkozó teljes indukcióval. $n=2$-re az állítás triviálisan teljesül. Tegyük fel, hogy az állítás igaz minden $n<n_0$-ra. Az előző tétel szerint minden n_0 pontú fában van elsőfokú pont. Ha elhagyjuk ezt a pontot és a hozzá tartozó egyetlen élet, akkor mivel a maradék n_0-1 pontú fára már igaz az állítás, látható, hogy az n_0 pontú eredeti fának n_0-1 éle van. □

2.2.4. Definíció. *Az F gráf a G gráf **feszítőfája**, ha F fa, és részgráfja G-nek.*

2.2.5. Tétel. *Minden összefüggő G gráf tartalmaz feszítőfát.*

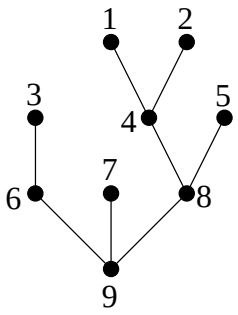
BIZONYÍTÁS: Ha G-ben van kör, akkor hagyjuk el a kör egy tetszőleges élét. Ha a maradék gráfban megint van kör, ismét hagyjuk el ennek egy élét, és ezt az eljárást folytassuk egészen addig, amíg találunk kört. Ha már nincs több kör, akkor nézzük meg, mit kaptunk. Az eljárás folyamán soha sem sérült meg az összefüggőség, hiszen mindig egy kör egyik élét hagytuk el. Nem hagytuk el a gráfnak egy pontját sem. Így a maradék gráf láthatóan G egy feszítőfája. □

2.2.6. Definíció. *A körmentes gráfokat **erdőnek** nevezzük. Egy F gráf a G gráf **feszítőerdője**, ha F erdő és minden komponense feszítőfája G megfelelő komponensének.*

Könnyen látható, hogy egy erdő összefüggő komponensei fák. Így teljesen hasonlóan a fentiekhez belátható, hogy ha az F erdő pontjainak száma n, komponenseinek száma k, akkor F-nek pontosan $n-k$ éle van. Ennek speciális esete, amikor F fa, hiszen ekkor 1 komponensből áll.
Cayley bebizonyította, hogy az $\{1,2,\ldots,n\}$ pontokon – ha most különbözőknek tekintjük az egyébként izomorf gráfokat – pontosan n^{n-2} darab különböző fa adható meg. Ennek a tételnek a bizonyításához lesz szükségünk a Prüfer-kódra.
Az $\{1,2,\ldots,n\}$ pontokon adott fához rendeljünk egy számsorozatot a következőképpen. Hagyjuk el a fa *elsőfokú* pontjai közül a legkisebb indexűt, és jegyezzük fel a szomszédja (a vele összekötött egyetlen pont) indexét. Legyen ez v_1. Ismételjük az eljárást a maradék fára, majd folytassuk egészen addig, amíg csak egy pont marad. Világos, hogy az utolsó pont az n sorszámú. Ugyanis ezt biztosan nem hagytuk el soha, hiszen mindig legalább két elsőfokú pont volt, és nyilván nem lehetett a kisebb sorszám az n. Ezért nem is kell, hogy a számsorozat végén feltüntessük.

2.2.7. Definíció. *Az így kapott $v_1, v_2, \ldots, v_{n-2}$ sorozatot a fa* ***Prüfer-kódjának*** *nevezzük.*

Például a 2.5. ábrán látható fa Prüfer-kódja $4,4,6,8,8,9,9$.



2.5. ábra.

2.2.8. Tétel (Cayley). *Az $\{1,2,\ldots,n\}$ pontokon n^{n-2} különböző fa adható meg.*

BIZONYÍTÁS: A definícióból könnyen látható, hogy egy fához nem tartozhat két különböző Prüfer-kód, és az is, hogy minden fához tartozik Prüfer-kód. Azt kell még belátnunk, hogy minden sorozathoz tartozik egy fa, melynek a Prüfer-kódja épp az adott sorozat, valamint azt, hogy a kapott sorozatok száma épp n^{n-2}.
Abból, hogy hány számból áll a Prüfer kód, könnyen meghatározhatjuk v_{n-1}-et, hiszen az biztosan n-nel egyenlő. Legyen w_k az a pont, amelyik elhagyásánál v_k-t feljegyeztük. Elég tehát meghatározni w_k-t minden k-ra, ebből már egyértelműen rekonstruálható a fa. w_1 a legkisebb szám, ami nem fordul elő a Prüfer-kódban, pontosabban $v_1, v_2, \ldots, v_{n-1}$ között. Általában w_k pedig a legkisebb szám, ami nem fordul elő a $w_1, w_2, \ldots, w_{k-1}, v_k, v_{k+1}, \ldots, v_{n-1}$ számok között. Mivel ez legfeljebb $n-1$ darab különböző szám, mindig van ilyen legkisebb szám.
Így megkaptuk a $\{v_1, w_1\}, \{v_2, w_2\}, \ldots, \{v_{n-1}, w_{n-1}\}$ éleket. Belátjuk, hogy ezek az élek tényleg fát határoznak meg, és akkor persze könnyen látható, hogy ennek a fának Prüfer-kódja éppen $v_1, v_2, \ldots, v_{n-1}$. Indirekt tegyük fel, hogy nem, azaz a kapott gráfban van kör. Minden egyes újabb w_i felírásakor egy újabb pontját és egy újabb élét kapjuk a gráfnak. Kell lenni egy olyan lépésnek, amikor éppen a kör utolsó élét kapjuk meg, de ekkor olyan w_i-t kellene felírnunk, amit már korábban felírtunk. Ez azonban nem lehetséges a fenti eljárásban.
Tehát minden olyan $n-1$ elemű sorozathoz, amelyben az első $n-2$ elem mindegyike lehet $\{1,2,\ldots,n\}$, és az utolsó elem n, tartozik egy-egy fa, és különböző sorozathoz különböző fa tartozik. Mivel ilyen sorozat n^{n-2} van, ennyi a különböző fák száma is. □

2.2.1. A mohó algoritmus

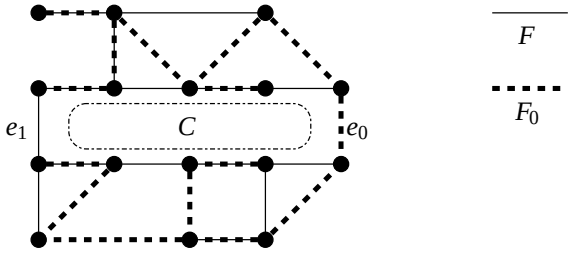
Rendeljünk egy G gráf éleihez súlyokat, nemnegatív valós számokat. Jelöljük $s(e)$-vel az e-hez rendelt súlyt. Ha $X \subseteq E(G)$, akkor X súlya $\sum_{e \in X} s(e)$. Adjunk algoritmust, amely megkeresi a minimális súlyú feszítőerdőt G-ben.

2.2.9. Algoritmus (Kruskal). *Az éleket egyesével választjuk ki a következők szerint. Először válasszuk ki a gráfból a legkisebb súlyú élek egyikét. Tegyük fel, hogy már kiválasztottunk néhány élet. Ekkor válasszuk ki a legkisebb súlyú olyan élek egyikét, amely nem alkot kört az eddig már kiválasztottakkal. Ha ilyen nincs, megállunk, ha van, akkor ezt az eljárást ismételjük.*

Egy algoritmust **mohó algoritmusnak** nevezünk, ha végrehajtása folyamán minden lépésben az éppen a legjobbnak tűnő lehetőséget választjuk és nem törődünk azzal, hogy esetleg egy most rosszabbnak tűnő választással végül jobb eredményt kaphatnánk. A Kruskal algoritmus nyilván egy mohó algoritmus a legkisebb súlyú feszítőerdő megkeresésére. A mohó algoritmus azonban más feladatok, például a legkisebb súlyú kör megkeresése vagy páros gráfban a maximális párosítás megkeresése (lásd 2.9.1) esetén nem feltétlenül ad jó megoldást.

2.2.10. Tétel. *Az előbbi algoritmus G minimális súlyú feszítőerdőjét adja.*

BIZONYÍTÁS: Nyilvánvaló, hogy az algoritmus végén a kiválasztott élek egy F feszítőerdőt alkotnak. Tegyük fel indirekt, hogy F_0 minimális súlyú feszítőerdő, és $s(F_0) < s(F)$. Ha több ilyen ellenpélda van, akkor ezek közül azt válasszuk F_0-nak, amelynek a lehető legtöbb közös éle van F-fel. Legyen $e_0 \in E(F_0) - E(F)$. (Lásd a 2.6. ábrát.)



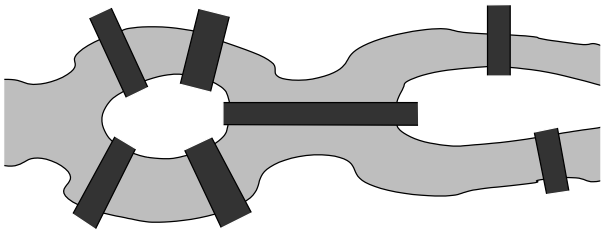
2.6. ábra.

Ha e_0-t hozzávesszük F-hez, akkor kapunk egy C kört. Ha valamely $e \in E(C) - \{e_0\}$ élre $s(e) > s(e_0)$ állna, akkor az algoritmus során e helyett e_0-t választottuk volna. Így $s(e) \leq s(e_0)$ minden $e \in E(C)$-re. Mivel $F_0 - e_0$ két komponensből áll, van legalább egy olyan $e_1 \in E(C) - \{e_0\} \subseteq E(F)$ él, melynek két végpontja $F_0 - e_0$ két különböző komponenséhez tartozik. Nyilván feszítőerdő $F_1 = (F_0 - e_0) \cup \{e_1\}$ is. Már láttuk, hogy $s(e_1) \leq s(e_0)$. Nem lehet azonban $s(e_1) < s(e_0)$, mert

ekkor $s(F_1) < s(F_0)$ volna, ami ellentmond F_0 minimalitásának. Csak $s(e_1) = s(e_0)$ lehetne, de ekkor F_1 olyan ellenpélda lenne, amelynek eggyel több közös éle van F-fel, mint F_0-nak. Ez pedig ellentmond a feltevésnek. □

2.3. Euler- és Hamilton körök

Ismert történet, hogy Eulertől megkérdezték Königsberg lakói, hogy miért nem tudnak átmenni a város hídjain úgy, hogy mindegyiken pontosan egyszer mentek át (2.7. ábra).



2.7. ábra.

Ebből ered a következő definíció és tétel.

2.3.1. Definíció. *A G gráf **Euler-körének** nevezünk egy zárt élsorozatot, ha az élsorozat pontosan egyszer tartalmazza G összes élét. Ha az élsorozat nem feltétlenül zárt, akkor **Euler-utat** kapunk.*

Megjegyezzük, hogy a fenti definíció értelmében tehát minden Euler-kör egyben Euler-út is. Fontos még megjegyezni, hogy az Euler-kör és -út általában nem „rendes" kör és út a gráfban, hiszen egy ponton többször is áthalad. Precízebb lenne tehát Euler-vonalnak vagy Euler-sétának nevezni ezt a fogalmat, de ez a hagyományos elnevezése.

2.3.2. Tétel. *Egy összefüggő G gráfban akkor és csak akkor van Euler-kör, ha G minden pontjának fokszáma páros.*

BIZONYÍTÁS: Először lássuk be, hogy ha van a gráfban Euler-kör, akkor minden pont foka páros. Induljunk el a gráf egy tetszőleges pontjából, és járjuk körbe az Euler-kör mentén. Így nyilvánvalóan minden pontba pontosan annyiszor „mentünk be", ahányszor „kimentünk", de a „kimenések" és „bemenések" számának összege épp a pont fokszáma. Ez pedig így biztosan páros.
A másik irányt G pontszámára való indukcióval bizonyítjuk. Tegyük fel, hogy minden $k < n$-re igaz az állítás, és legyen G egy n pontú gráf. Induljunk el a gráf egy

tetszőleges pontjából, és haladjunk az élek mentén úgy, hogy egy élen kétszer nem megyünk át. Ha egy olyan pontba érünk, amelyből nem vezet ki olyan él, amelyen még nem haladtunk át, akkor ez csak a kiinduló pont lehet, mivel minden pont foka páros. Így tehát egy zárt élsorozatot kapunk. Legyen a H egy olyan zárt élsorozata G-nek, amelyben az előforduló élek száma maximális. Mivel a kiindulópontból már nem tudtunk tovább menni, az ebből a pontból kiinduló minden él H-beli. Indirekt tegyük fel, hogy H nem egy Euler-köre G-nek. Vizsgáljuk a G' gráfot, amelyet úgy kaptunk, hogy a G gráfból elhagytuk a H-ban szereplő éleket. G' nem feltétlenül összefüggő, viszont összesen n-nél kevesebb pontja van, hiszen a kiindulópont nincs benne. Az indukciós feltevés miatt minden komponensében van Euler-kör. Mivel G összefüggő, G' valamelyik komponensének van olyan pontja, amelyik H-ban szerepel. Nevezzük az ebben a komponensben található Euler-kört H'-nek. Tehát ha elindulunk az előbb talált közös pontból, és először bejárjuk H-t majd H'-t, akkor egy H élszámánál nagyobb élszámú zárt élsorozatot találtunk, ami ellentmond a feltevésünknek. Vagyis H Euler-kör. □

2.3.3. Tétel. *Egy összefüggő G gráfban akkor és csak akkor van Euler-út, ha G-ben a páratlan fokú pontok száma* 0 *vagy* 2.

BIZONYÍTÁS: A 2.3.2. tétel bizonyításához hasonlóan belátható, hogy ha G-ben van Euler-út, akkor az Euler-út két végpontjának kivételével minden pont foka páros.
A másik irány bizonyításához viszont felhasználhatjuk a 2.3.2. tételt. Ha nincs páratlan fokú pont, akkor készen vagyunk. Ha 2 darab páratlan fokú pont van, akkor kössük össze ezeket egy újabb e éllel (párhuzamos éleket is megengedünk). A keletkező G' gráfban minden pont foka páros lesz, így a 2.3.2. tétel értelmében van benne Euler-kör, ami definíció szerint tartalmazza az e élet is. Hagyjuk el ebből az Euler-körből az e élet, így egy Euler-utat kaptunk G-ben. □

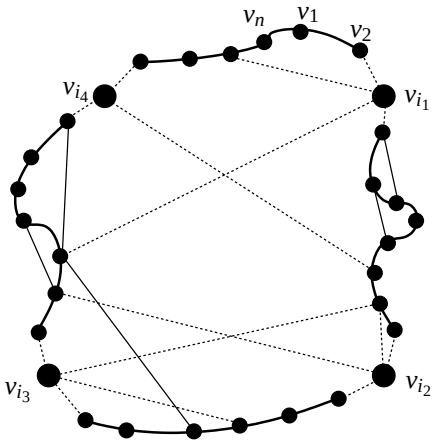
2.3.4. Definíció. *Egy G gráfban* ***Hamilton-körnek*** *nevezünk egy H kört, ha G minden pontját (pontosan egyszer) tartalmazza. Egy utat pedig* ***Hamilton-útnak*** *nevezünk, ha G minden pontját pontosan egyszer tartalmazza.*

Megjegyezzük, hogy a Hamilton-kör és a Hamilton-út egy speciális kör, illetve út a gráfban, ellentétben az Euler-körrel és -úttal.
A Hamilton-kör létezésének kérdése speciális esete a széles körben felmerülő Utazó Ügynök problémának: Egy ügynöknek meg kell látogatnia bizonyos városokat útja során (és végül haza kell térnie). Adott, hogy valamelyik városból egy másik városba milyen költséggel tud eljutni (repülőjegy, autóút ára). Természetesen szeretné az utak összköltségét minimalizálni. Ez a feladat sok alkalmazás során felmerül, és csak bizonyos speciális esetekben ismeretesek jó algoritmusok a megoldására.
Ha most feltesszük, hogy bizonyos városokból nem lehet közvetlenül eljutni egyes másik városokba, míg a többi városba egységnyi költséggel lehet eljutni, és az ügynöknek minden várost meg kell látogatnia, akkor a feladat a Hamilton-kör létezésére

redukálódik. Hiszen vegyük azt a gráfot, melynek pontjai a városoknak megfelelő n pont, és amelyben két pont akkor és csak akkor van összekötve, ha a nekik megfelelő városok között közvetlen összeköttetés van. Ebben a gráfban akkor és csak akkor van Hamilton-kör, ha az ügynök n összköltséggel meg tud látogatni minden várost.
Hamilton-kör létezésére több elégséges feltételt adtak. Néhányat megemlítünk itt, bár csak kettőt bizonyítunk be. Természetesen mindenhol egyszerű gráfról van szó, és úgyis csak akkor érdekes a kérdés, ha $n \geq 3$. Ismertetünk egy szükséges feltételt is, azonban nem ismeretes olyan jól kezelhető feltétel, amely egyszerre szükséges és elégséges is.

2.3.5. Tétel. *Ha a G gráfban létezik k olyan pont, amelyeket elhagyva a gráf több mint k komponensre esik, akkor nem létezik a gráfban Hamilton-kör. Ha létezik k olyan pont, amelyeket elhagyva a gráf több mint $k+1$ komponensre esik, akkor nem létezik a gráfban Hamilton-út.*

BIZONYÍTÁS: Indirekt tegyük fel, hogy van a gráfban Hamilton-kör, legyen ez $(v_1, v_2, \ldots, v_n)$ és legyen $v_{i_1}, v_{i_2}, \ldots, v_{i_k}$ az a k pont, melyet elhagyva a gráf több mint k komponensre esik. Vegyük észre azonban, hogy az elhagyott pontok közötti „ívek” biztosan összefüggő komponenseket alkotnak. Pl. a $(v_{i_1+1}, v_{i_1+2}, \ldots, v_{i_2-1})$ ív is összefüggő lesz, hiszen két szomszédos pontja között az eredeti Hamilton-kör egy éle fut. Mivel éppen k ilyen ívet kapunk, nem lehet több komponens k-nál. (Kevesebb lehet, hiszen különböző ívek között futhatnak élek, lásd a 2.8. ábrát.)



2.8. ábra.

Ugyanígy bizonyíthatjuk be a Hamilton-útra vonatkozó feltételt is. Ha egy Hamilton-útból elhagyunk k pontot, legfeljebb $k+1$ összefüggő ív marad. □

2.3.6. Tétel (Ore). *Ha az n pontú G gráfban minden olyan $x,y \in V(G)$ pontpárra, amelyre $\{x,y\} \in E(G)$ teljesül az is, hogy $d(x)+d(y) \geq n$, akkor a gráfban van Hamilton-kör.*

A fenti feltétel tehát a nem szomszédos pontpárok fokszámainak összegéről nem mond semmit. Ki lehet mondani a tételt kissé más fogalmazásban is: *Ha az n pontú G gráfban nincs olyan $x,y \in V(G)$ pontpár, amelyre $d(x)+d(y) < n$ és $\{x,y\} \notin E(G)$, akkor G-ben van Hamilton-kör.*

BIZONYÍTÁS: Indirekt tegyük fel, hogy a gráf kielégíti a feltételt, de nincsen benne Hamilton-kör. Vegyünk hozzá a gráfhoz éleket úgy, hogy továbbra se legyen benne Hamilton-kör. Ezt egészen addig csináljuk, amikor már akárhogyan is veszünk hozzá egy élet, lesz a gráfban Hamilton-kör. Az így kapott G' gráfra továbbra is teljesül a feltétel, hiszen új élek behúzásával „rossz pontpárt" nem lehet létrehozni. Biztosan van két olyan pont, hogy $\{x,y\} \notin E(G')$. Ekkor a $G'+\{x,y\}$ gráfban van egy Hamilton-kör, tehát G'-ben van Hamilton-út. Legyen ez $P=(z_1,z_2,\ldots,z_n)$, ahol $z_1=x$ és $z_n=y$.
Ha x szomszédos a P út valamely z_k pontjával, akkor y nem lehet összekötve z_{k-1}-el , mert $(z_1,\ldots,z_{k-1},z_n,z_{n-1},\ldots,z_k,z_1)$ egy Hamilton-kört adna. Így tehát y nem lehet összekötve legalább $d(x)$ darab ponttal, ezért

$$d(y) \leq n-1-d(x)$$

ami viszont ellentmondás, mert $\{x,y\} \notin E(G)$. □

2.3.7. Tétel (Dirac). *Ha egy n pontú G gráfban minden pont foka legalább $n/2$, akkor a gráfban létezik Hamilton–kör.*

BIZONYÍTÁS: Ez az előző tételből következik, hiszen ha minden pont foka legalább $n/2$, akkor teljesül az Ore-tétel feltétele, mivel bármely x,y pontpárra $d(x)+d(y) \geq n$. □

2.3.8. Tétel (Pósa). *Jelöljük G pontjai fokszámát nagyság szerint rendre $d_1 \leq d_2 \leq \ldots \leq d_n$-nel. Ha minden $k < n/2$-re $d_k \geq k+1$, akkor G-ben van Hamilton-kör.*

2.3.9. Tétel (Chvátal). *Az előbbi jelöléssel, ha minden k-ra, amelyre $d_k \leq k < n/2$, teljesül, hogy $d_{n-k} \geq n-k$, akkor a gráfban van Hamilton-kör.*

2.4. Gráfok és mátrixok

2.4.1. Szomszédsági mátrix

Egy n pontú gráf mátrixszal való reprezentálásának egyik legtermészetesebb módja (feltéve, hogy az esetleges párhuzamos éleket nem kell megkülönböztetni), ha defi-

niálunk egy $n \times n$-es $A(G) = (a_{ij})$ mátrixot az alábbi módon:

$$a_{ij} = \begin{cases} 0, & \text{ha az } i\text{-edik és } j\text{-edik pont nem szomszédos} \\ k, & \text{ha az } i\text{-edik és } j\text{-edik pont között } k \text{ darab párhuzamos él halad} \\ l, & \text{ha } i = j \text{ és az } i\text{-edik ponthoz } l \text{ darab hurokél illeszkedik.} \end{cases}$$

Irányított gráfokat is megadhatunk ilyen módon, csak ott a_{ij} az i-edik pontból a j-edik pontba vezető élek száma. Ezt az $A(G)$ mátrixot a G gráf **szomszédsági mátrixának** nevezzük.

2.4.1. Tétel. *Nyilvánvaló, hogy a szomszédsági mátrix t-edik hatványa olyan $A^t = \left(m_{ij}^{(t)}\right)$ mátrix, melynek $m_{ij}^{(t)}$ eleme az i-ből j-be vezető t hosszúságú élsorozatok száma. Ezen élsorozatok között nem csak az utakat, hanem az azonos ponton többször átmenő sorozatokat is számoljuk.*

BIZONYÍTÁS: Először lássuk be a tételt $t = 2$-re. Az A^2 mátrix egy $m_{ij}^{(2)}$ elemét az A mátrix i-edik sorának és j-edik oszlopának skalárszorzataként kapjuk meg. Ebben a skalárszorzatban az k-adik összeadandó a gráf v_i-ből v_k-ba vezető és v_k-ból v_j-be vezető élei számának szorzata. Így a skalárszorzat ezeknek az összegzése minden k-ra, beleértve, hogy lehet $k = i$ vagy $k = j$ is. Ilyenkor számoljuk a hurokéleket is. Tehát $m_{ij}^{(2)}$ a v_i és v_j közötti 2 élből álló élsorozatok száma.
$t > 2$ esetében teljes indukcióval bizonyítunk, a fenti gondolatmenetet használva. Tegyük fel, hogy $t-1$-re már bizonyítottuk az állítást. A definíció szerint $A^t = A^{t-1} \times A$. Az A^t mátrix egy $m_{ij}^{(t)}$ elemét ezért az A^{t-1} mátrix i-edik sorának és az A mátrix j-edik oszlopának skalárszorzataként kapjuk meg. Ebben a skalárszorzatban az k-adik összeadandó a gráf v_i-ből v_k-ba vezető $t-1$ hosszú élsorozatai számának és a v_k-ból v_j-be vezető élek számának szorzata. Így a skalárszorzat ezeknek az összegzése minden k-ra, tehát $m_{ij}^{(t)}$ a v_i és v_j közötti t élből álló élsorozatok száma. □

Megjegyzés: A hurokéleket nem tartalmazó gráfoknál A^3 diagonális elemeinek összege a gráfban található három hosszúságú körök számának hatszorosa (hisz minden kört minden pontból mindkét irányban be lehet járni).

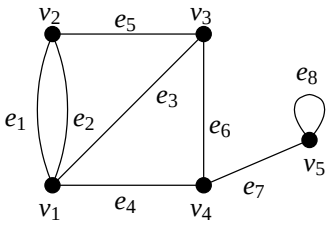
2.4.2. Illeszkedési mátrix

Ez a villamosságtani alkalmazások szempontjából legfontosabb mátrixreprezentáció. Legyen az n-pontú G gráfnak e éle és definiáljuk az $n \times e$-es $B(G) = (b_{ij})$ mátrix elemeit úgy, hogy

$$b_{ij} = \begin{cases} 0, & \text{ha a } j\text{-edik él nem illeszkedik az } i\text{-edik ponthoz} \\ 1, & \text{ha a } j\text{-edik élnek az } i\text{-edik pont a kezdőpontja} \\ -1, & \text{ha a } j\text{-edik élnek az } i\text{-edik pont a végpontja} \end{cases}$$

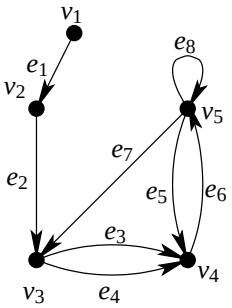
Legyen – megállapodás szerint – $b_{ij} = 1$ akkor is, ha a j-edik él az i-edik ponthoz illeszkedő hurokél. Irányítatlan esetben is ez a definíció, csak ott a j-edik él mindkét

végpontjának megfelelő mátrixelem 1. Ezt a $B(G)$ mátrixot a G gráf **illeszkedési mátrixának** nevezzük. A 2.9. ábrán egy irányítatlan és egy irányított gráf, valamint illeszkedési és szomszédsági mátrixa látható.



$$\mathbf{B} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$\mathbf{A} = \begin{pmatrix} 0 & 2 & 1 & 1 & 0 \\ 2 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$



$$\mathbf{B} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & -1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 1 & 1 \end{pmatrix}$$

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

2.9. ábra.

2.4.2. Tétel. *Az n pontú, c darab összefüggő komponensből álló, hurokélmentes irányított G gráf illeszkedési mátrixának rangja $n-c$.*

BIZONYÍTÁS: Ha $c > 1$, akkor komponensenként sorolva fel a pontokat és éleket, $B(G)$ blokkdiagonális szerkezetű lesz. Elég tehát egy p pontú összefüggő komponensre belátni, hogy a neki megfelelő blokk rangja $p-1$. Mivel a blokk sorainak száma p és az összes sor összege a $(0,0,\ldots,0)$ vektor (hiszen minden élnek megfelelő oszlopban egy $+1$, egy -1 és $p-2$ darab zérus található), nyilvánvaló, hogy a rang legfeljebb $p-1$ lehet. (Itt használtuk fel a hurokélmentességet.)
Legyen F egy p pontú, $p-1$ élű feszítőfa ebben a komponensben. Legyen v_1 egy elsőfokú pont F-ben és e_1 a hozzá illeszkedő él. Legyen v_2 egy elsőfokú pont $(F-$

$\{v_1\}$)-ben és e_2 a hozzá illeszkedő él, stb. Ha a blokk sorait $v_1, v_2, \ldots$ sorrendben soroljuk fel, oszlopait pedig $e_1, e_2, \ldots$ felsorolásával kezdjük, akkor egy $p \times (p-1)$ méretű részmátrixot kapunk, amelyből az utolsó sor elhagyásával olyan mátrixot kapunk, melynek diagonális elemei ± 1 értékűek és az átló felett csupa zérus áll. Mivel így találtunk $p-1$ lineárisan független oszlopot, a rang pontosan $p-1$. □

2.4.3. Tétel. *Válasszunk ki az n pontú, összefüggő, hurokélmentes irányított G gráf illeszkedési mátrixában $n-1$ oszlopot. Ezek akkor és csak akkor lesznek lineárisan függetlenek, ha a megfelelő $n-1$ él G-nek egy fáját alkotja.*

BIZONYÍTÁS: Az előző tétel bizonyításakor láttuk, hogy ha az élek fát alkotnak, akkor a megfelelő oszlopvektorok lineárisan függetlenek. Megfordítva, megmutatjuk, hogy ha bizonyos élek kört alkotnak, akkor a nekik megfelelő oszlopvektorok lineárisan összefüggőek. Csakugyan, ezek az oszlopok és a kört alkotó pontoknak megfelelő sorok alkalmas sor- ill. oszloppermutációk után az alábbi alakú mátrixot alkotják.

$$\begin{pmatrix} a & 0 & \cdots & -x \\ -a & b & \cdots & 0 \\ 0 & -b & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & x \end{pmatrix},$$

ahol az $a, b, \ldots, x$ betűk mindegyike $+1$ vagy -1. Képezzük az oszlopvektoroknak azt a lineáris kombinációját, melyben az első oszlop együtthatója 1, ha $a = 1$ és -1, ha $a = -1$; a második oszlopé 1, ha $b = 1$ és -1, ha $b = -1$ stb. □

Az első tétel bizonyítása alapján nem csak az következik, hogy a fáknak megfelelő $p-1$ oszlop lineárisan független, hanem az is, hogy ezek az oszlopok és B bármelyik $p-1$ sora által alkotott mátrix determinánsa ± 1.

2.4.4. Tétel. *Hagyjunk el az n pontú összefüggő irányított G gráf illeszkedési mátrixából egy tetszőleges sort. A keletkező B_0 mátrixból képzett $B_0 \cdot B_0^T$ mátrix determinánsa épp a G gráf feszítőfáinak száma.*

BIZONYÍTÁS: Felhasználhatjuk az alábbi, Binet-től és Cauchy-tól származó tételt: Ha M egy $p \times r$-es, N egy $r \times p$-es mátrix (ahol $p \leq r$), akkor az $M \cdot N$ determinánsa

$$\sum det(M_i) det(N_i),$$

ahol az M_i az M alkalmas p db oszlopából, N_i pedig az N ugyanilyen sorszámú soraiból áll, és a szummázás mind az $\binom{r}{p}$-féle ilyen kiválasztásra történik. Például

$$\left| \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \begin{pmatrix} g & h \\ i & j \\ k & l \end{pmatrix} \right| =$$

$$= \begin{vmatrix} a & b \\ d & e \end{vmatrix} \begin{vmatrix} g & h \\ i & j \end{vmatrix} + \begin{vmatrix} a & c \\ d & f \end{vmatrix} \begin{vmatrix} g & h \\ k & l \end{vmatrix} + \begin{vmatrix} b & c \\ e & f \end{vmatrix} \begin{vmatrix} i & j \\ k & l \end{vmatrix}.$$

Ezek után a tétel állítása nyilvánvaló: B_0-ból mindenféleképp kiválasztva $n-1$ oszlopot, épp a fának megfelelő részmátrixok determinánsa lesz zérustól különböző. A tétel előtti megjegyzés szerint akkor ez a determináns ± 1, a négyzete tehát $+1$. (Felhasználtuk, hogy B_0^T megfelelő részmátrixa épp a B_0 vizsgált részmátrixának transzponáltja, tehát determinánsaik egyenlőek.) □

A tétel felhasználásához nem szükséges a B_0 mátrixot felírnunk. Az egyszerűség kedvéért tegyük fel, hogy B utolsó (n-edik) sorát elhagyva kaptuk a B_0 mátrixot. A mátrixszorzás tulajdonságából és B_0 definíciójából következik, hogy $B_0 B_0^T = (d_{ij})$ elemeit az alábbi képlet is előállítja:

$$d_{ij} = \begin{cases} \text{az } i\text{-edik pont foka,} & \text{ha } i = j \\ \text{az } i\text{-edik és } j\text{-edik pont között} \\ \text{oda- és visszavezető élek számának } (-1)\text{-szerese,} & \text{ha } i \neq j. \end{cases}$$

Így például az n pontú teljes gráfra

$$B_0 B_0^T = \begin{pmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{pmatrix}.$$

Ebből azonnal új bizonyítást kaptunk Cayley tételére (2.2.8. tétel), hisz ennek determinánsa

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ -1 & n-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{vmatrix} = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & n & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & n \end{vmatrix} = n^{n-2}.$$

2.4.3. Körmátrix

Az előzőekben megismert illeszkedési mátrix gyakorlati jelentőségét többek között az adja, hogy ha egy villamos hálózat minden alkatrésze 2 pólusú (tehát a hálózat összekapcsolását természetes módon megadhatjuk egy G irányított gráffal, ahol az élek irányítása a „mérőiránynak” felel meg), akkor a Kirchhoff–féle áramegyenletek röviden $B\mathbf{i} = \mathbf{0}$ alakba írhatók, ahol az $\mathbf{i}$ vektor elemei az alkatrészek áramai. Ugyanígy röviden $C\mathbf{u} = \mathbf{0}$ alakba írhatjuk fel a Kirchhoff–féle feszültségegyenleteket is, a $C(G)$ **körmátrix** segítségével. Ennek definiálásához írjuk elő minden kör „körüljárását”, tehát határozzuk el, hogy a kör pontjait milyen ciklikus sorrendben

soroljuk fel. Ezek után a $C(G) = (c_{ij})$ mátrixot úgy definiáljuk, hogy

$$c_{ij} = \begin{cases} 0, & \text{ha a } j\text{-edik él nem eleme az } i\text{-edik körnek} \\ 1, & \text{ha a } j\text{-edik él benne van az } i\text{-edik körben és irányítása megegyezik a kör körüljárásával} \\ -1, & \text{ha a } j\text{-edik él benne van az } i\text{-edik körben és irányítása ellentétes a kör körüljárásával.} \end{cases}$$

A körmátrixra hasonló tételek érvényesek, mint az illeszkedési mátrixra. Egyszerűség kedvéért ezeket csak összefüggő gráfokra mondjuk ki.

2.4.5. Tétel. *Az n pontú, e élű, összefüggő irányított gráf körmátrixának rangja $e-n+1$.* □

2.4.6. Tétel. *Válasszunk ki az n pontú, e élű, összefüggő irányított G gráf körmátrixában $e-n+1$ oszlopot. Ezek akkor és csak akkor lesznek lineárisan függetlenek, ha a megfelelő $e-n+1$ él G egy fájának komplementerét alkotja.* □

Ha egy kétpólusú alkatrészekből álló villamos hálózatra fel akarjuk írni a Kirchhoff–féle áramegyenleteket, akkor gépiesen n egyenletet kaphatnánk (minden pontra egyet). Láttuk (2.4.2. tétel), hogy ezek közül csak $n-c$ darab lenne lineárisan független. A gyakorlatban ezért a hálózat gráfjában (pontosabban: annak minden összefüggő komponensében) egy-egy pontot figyelmen kívül hagyunk az áramegyenletek felírásakor.
A feszültségegyenleteknél a helyzet bonyolultabb. Egy n pontú gráfban akár közel $n!$ darab kör is található és a 2.4.5. tétel épp arra mutat rá, hogy ha mindegyikre felírnánk egy feszültségegyenletet, akkor nagyon sok felesleges (a többi következményeképp előálló) egyenlet adódnék. Ha pl. a hálózat gráfja K_6 lenne, akkor a 6 áramegyenletből 1, viszont a 165 feszültségegyenletetből 150 lenne felesleges!
Ha egy összefüggő G gráf valamely lerögzített F fájához minden lehetséges módon hozzáveszünk egy további $e \notin F$ élt, akkor $F \cup \{e\}$ egyetlen C_e kört tartalmaz. Ezen körök $\{C_e \mid e \notin F\}$ együttesét az F fához tartozó **alapkörrendszernek** vagy **fundamentális körrendszernek** nevezzük. A villamosmérnöki gyakorlatban valamely alapkörrendszer elemeihez érdemes felírni a Kirchhoff–féle feszültségtörvényeket.
Könnyű végiggondolni, hogy az F fához tartozó alapkörrendszer köreinek megfelelő sorvektorok és az F-hez nem tartozó éleknek megfelelő oszlopok $C(G)$-ben egy olyan $(e-n+1)\times(e-n+1)$ méretű négyzetes részmátrixot határoznak meg, mely a sorok és az oszlopok esetleges permutációi után az előjelektől eltekintve egységmátrix.
Ebből azonnal adódik, hogy $r(C) \geq e-n+1$. A 2.4.5. tételhez még szükséges $r(C) \leq e-n+1$ irány, valamint a 2.4.6. tétel bizonyítását nem részletezzük. **Nem igaz** viszont az, hogy ha a körmátrixból tetszőlegesen kiválasztunk $e-n+1$ darab lineárisan független sort, akkor az így kapott mátrix $(e-n+1)\times(e-n+1)$ méretű

részmátrixai közül a nemszingulárisok determinánsa mind ± 1 (csak az, hogy mind $\pm k$, ahol k értéke csak a sorok kiválasztásától függ). Belátható az is, hogy ez a közös érték ± 1, ha nem tetszőlegesen választjuk ki az $e-n+1$ darab lineárisan független sort, hanem úgy, hogy egy lerögzített F fához tartozó alapkörrendszer sorait használjuk.

2.4.4. Egyéb gráfreprezentációk

A $C(G)$ körmátrixhoz hasonlóan definiálható a $Q(G)$ **vágásmátrix** is, ha a körök „körüljárásához" hasonlóan definiáljuk a vágás „irányítását". Egy vágást alkotó élek mind a gráf ugyanazon komponensében vannak és ennek a komponensnek a pontjait választják szét két X_1, X_2 részhalmazra. Akkor mondjuk, hogy a vágás valamely (u,v) élének irányítása megegyezik a vágás irányításával, ha $u \in X_1$ és $v \in X_2$; és akkor ellentétes az irányításuk, ha $u \in X_2$ és $v \in X_1$.
A 2.9. ábrán látható irányított gráf körmátrixa és vágásmátrixa ennek megfelelően

$$C = \begin{pmatrix} 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & -1 & 0 \\ 0 & 0 & 1 & 1 & 1 & -1 & 0 & 0 \end{pmatrix},$$

ha a körök „körüljárását" a 2.9. ábrán látható rajzon az óramutató járásával ellentétesnek definiáljuk, ill. a vágásokat úgy irányítjuk, hogy $v_1 \in X_1$ mindig teljesüljön.
A 2.4.2. és a 2.4.3. tételek az illeszkedési mátrix helyett a vágásmátrixra is teljesülnek, sőt, még a hurokélmentességet sem kell kikötni. Ezek bizonyítását nem részletezzük.

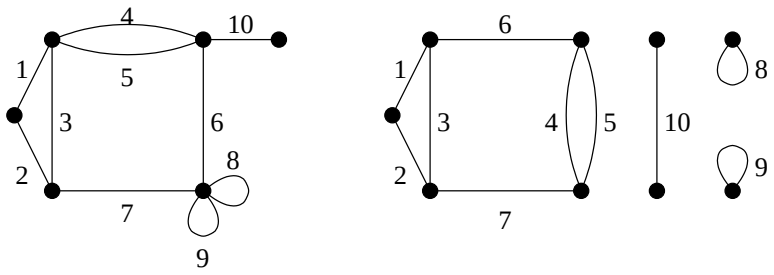
2.4.7. Tétel. *Legyen B, C és Q rendre egy hurokélmentes irányított G gráf illeszkedési, kör- ill. vágásmátrixa. Tegyük fel, hogy oszlopaik ugyanolyan sorrendben felelnek meg G éleinek. Ekkor*

$$B \cdot C^T = \mathbf{0} \quad \text{és} \quad Q \cdot C^T = \mathbf{0}.$$

□

A fenti négy mátrix elsősorban gráfelméleti (és a gráfok alkalmazásai során felmerülő) tételek bizonyításához használható. Ha gráfelméleti algoritmusokat kívánunk beprogramozni, akkor a gráfokat általában nem célszerű ezekkel a mátrixokkal

reprezentálni: egyéb adatstruktúrák (pl. szomszédossági lista, láncolt szomszédossági lista stb.) alkalmazásával nagyságrendekkel kevesebb lépésszámú algoritmusokhoz juthatunk. Ezekkel a 3.4. szakaszban ismerkedhetünk meg.



2.10. ábra.

A körmátrix nemcsak, hogy nem hatékony, de nem is alkalmas eszköz gráfok reprezentálására, hisz nem izomorf gráfoknak is lehet azonos körmátrixa. Két gráfot **gyengén izomorfnak** nevezünk, ha élei között kölcsönösen egyértelmű és körtartó leképezés hozható létre. A 2.10. ábrán gyengén izomorf (de nem izomorf) gráfok láthatók. Ezeknek alkalmas irányítás esetén azonos a körmátrixuk. A gyenge izomorfiát szokták 2**–izomorfiának** is nevezni, de mi az előbbi elnevezést használjuk. Ugyanez a probléma merül fel a vágásmátrixokkal kapcsolatban is. Megjegyezzük viszont, hogy a kör- ill. vágásmátrixok egymást egyértelműen meghatározzák, így a gyenge izomorfia definíciójában körtartás helyett vágástartást is mondhattunk volna.

2.5. Síkbarajzolható gráfok

2.5.1. Definíció. *Ha egy gráf lerajzolható a síkba úgy, hogy az élei ne messék egymást, akkor a gráf* ***síkbarajzolható****. A síkbarajzolt gráf a síkot* ***tartományokra*** *osztja. Hasonlóan definiáljuk a* ***gömbre rajzolható*** *gráfot.*

2.5.2. Tétel. *Egy G gráf pontosan akkor síkbarajzolható, ha gömbre rajzolható.*

BIZONYÍTÁS: Egy síkban levő gráf leképezhető egy gömbfelületre oly módon, hogy ezt a gömbfelületet valamelyik pontjával a síkra helyezzük, az érintkezési pontot tekintjük a gömbfelület déli pólusaként, és az északi pólusból, mint vetítési pontból oly egyenes vonalakat húzunk, amelyek a síkban levő gráf minden egyes pontját összekötik az északi pólussal. Ezeknek a vonalaknak egy-egy további metszéspontja van a gömbfelülettel, ezek szolgáltatják a kívánt vetítést. Ez az ún. **sztereografikus projekció**. Ez az eljárás megfordítható, ha az északi pólus nem pontja a gráfnak és nem halad át rajta él, így a gömbre rajzolt gráfok is leképezhetők a síkba. □

Evvel a módszerrel beláthatjuk, hogy bármely síkbarajzolható gráf tetszőleges tartománya egy másik lerajzolásban lehet külső tartomány. Először vetítsük a gráfot

egy gömbre úgy, hogy a déli pólus a kiválasztott tartomány belső pontjában legyen. Majd a visszavetítés előtt forgassuk el a gömböt úgy, hogy az északi pólus legyen a kiválasztott tartomány belsejében.
Természetesen nem minden gráf rajzolható síkba. Kuratowski tétele meghatározza, mely gráfok rajzolhatók síkba. Ehhez a tételhez azonban szükség lesz néhány önmagában is fontos eredményre.

2.5.3. Tétel (Euler-formula). *Ha egy összefüggő síkbeli gráfnak n csúcsa, e éle és t tartománya van (beleértve a külső, nem korlátos tartományt is), akkor eleget tesz az Euler-formulának: $n-e+t=2$.*

BIZONYÍTÁS: Tekintsük a gráf egy C körét (ha van) és ennek egy a élét. A C kör a síkot két részre osztja. Ezeket egyéb élek további tartományokra oszthatják, de mindkét részben van egy-egy olyan tartomány, amelynek a határa. Ha a-t elhagyjuk, a két tartomány egyesül, azaz a tartományok száma eggyel csökken. A csúcsok száma nem változik, tehát a elhagyásával az $n-e+t$ érték nem változik.
Ezt az eljárást addig folytassuk, amíg a gráfban nem marad kör. Ekkor viszont egy feszítőfa maradt. Elég az állítást erre belátni, ez viszont triviális, hiszen $t=1$ és a 2.2.3. tétel alapján $e=n-1$. □

Megjegyezzük, hogy a fenti tétel nem csak egyszerű gráfokra igaz, hanem párhuzamos- és hurokéleket tartalmazó gráfokra is. Az Euler-formula segítségével könnyen bizonyítható a következő két tétel.

2.5.4. Tétel. *Ha G egyszerű, síkbarajzolható gráf és pontjainak száma legalább 3, akkor az előbbi jelölésekkel $e \leq 3n-6$.*

BIZONYÍTÁS: Vegyük G egy tetszőleges síkbarajzolását és jelöljük az egyes tartományokat határoló élek számát $c_1, c_2, \ldots, c_t$-vel. Mivel a gráf egyszerű, minden tartományát legalább 3 él határolja, ezért $c_i \geq 3$. Nyilvánvaló, hogy egy él viszont legfeljebb két tartomány határához tartozik (ha az él elvágó él, akkor csak egyhez), tehát ha összegezzük a tartományokat határoló élek számát minden tartományra, akkor minden élet legfeljebb kétszer számoltunk. Így

$$3t \leq c_1 + c_2 + \ldots + c_t = \sum_{i=1}^{t} c_i \leq 2e.$$

Az Euler-formulát felhasználva az

$$3(e-n+2) \leq 2e$$

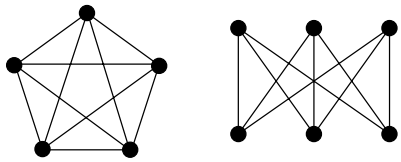
egyenlőtlenséget kapjuk. Ebből átrendezéssel következik, hogy $e \leq 3(n-2) = 3n-6$. □

2.5.5. Tétel. *Ha G egyszerű, síkbarajzolható gráf, minden körének a hossza legalább 4 és pontjainak száma legalább 4, akkor az előbbi jelölésekkel $e \leq 2n-4$.*

BIZONYÍTÁS: Nyilvánvaló, hogy minden tartományt legalább 4 él határol. A 2.5.4. tétel bizonyításához hasonló gondolatmenettel kapjuk ebből, hogy $4t \leq 2e$ és az Euler-formula alkalmazásával, hogy $e \leq 2n-4$. □

2.5.6. Tétel. *Ha G egyszerű, síkbarajzolható gráf, akkor $\delta = \min_{x \in V(G)} d(x) \leq 5$, azaz a minimális fokszám legfeljebb* 5.

BIZONYÍTÁS: Feltehetjük, hogy a gráf pontjainak a száma legalább 3. Tegyük fel, hogy $\delta \geq 6$. Mivel a fokszámok összege egyenlő az élszám kétszeresével, $6n \leq 2e$. A 2.5.4. tétel miatt azonban $2e \leq 6n-12$. Így viszont ellentmondásra jutunk, hiszen $6n \not\leq 6n-12$. □



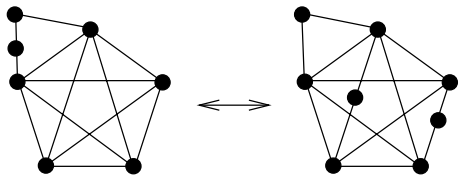
2.11. ábra.

A 2.11. ábrán látható két gráfot **Kuratowski-gráfoknak** nevezzük. Az első K_5, az öt pontú teljes gráf. A másik $K_{3,3}$, a „három ház – három kút" gráf. Ez az elnevezés a következő problémából ered. Adott három ház és három kút, kössük össze utakkal a három ház mindegyikét a három kút mindegyikével úgy, hogy az utak ne messék egymást. Ezt nem lehet megtenni, amit a következő tétel bizonyít.

2.5.7. Tétel. *A Kuratowski-gráfok, K_5 és $K_{3,3}$ (2.11. ábra) nem rajzolhatók síkba.*

BIZONYÍTÁS: Ha K_5 síkbarajzolható volna, akkor teljesülne rá a 2.5.4. tétel. Azonban K_5 pontjainak száma 5, éleinek száma 10 és $10 > 3 \cdot 5 - 6 = 9$, azaz ellentmondásra jutottunk. Tehát K_5 nem síkbarajzolható.
Belátjuk, hogy $K_{3,3}$ minden körének hossza legalább 4. Ha volna 3 hosszú kör, akkor ennek pontjai között vagy két háznak vagy két kútnak kell szerepelnie, amelyek össze vannak kötve. Ez viszont ellentmond a definíciónak. Ezért, ha $K_{3,3}$ síkbarajzolható volna, akkor teljesülne rá a 2.5.5. tétel. Azonban $K_{3,3}$ pontjainak száma 6, éleinek száma 9 és $9 > 2 \cdot 6 - 4 = 8$, azaz ellentmondásra jutottunk. Tehát $K_{3,3}$ nem síkbarajzolható. □

Egy gráf síkbarajzolhatóságát nyilván nem befolyásolja, hogyha egy élet egy 2 hosszú úttal helyettesítünk, azaz egy élet egy új 2 fokú csúcs felvételével két élre bontunk, vagy ha egy 2 fokú csúcsra illeszkedő éleket egybeolvasztjuk, és a csúcsot elhagyjuk. (2.12. ábra)



2.12. ábra.

2.5.8. Definíció. *A G és H gráfok **topológikusan izomorfak**, ha a fent említett transzformációk ismételt alkalmazásával izomorf gráfokba transzformálhatók.*

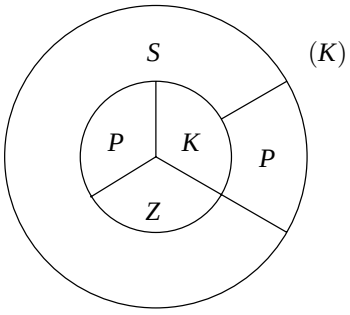
2.5.9. Tétel (Kuratowski). *Egy gráf akkor és csak akkor síkbarajzolható, ha nem tartalmaz olyan részgráfot, amely topológikusan izomorf $K_{3,3}$-mal vagy K_5-tel.*

A tételben szereplő feltétel szükségességét láttuk, az elégségesség bizonyítása elég bonyolult, ezért nem részletezzük. Szintén bizonyítás nélkül megemlítjük a következő tételt.

2.5.10. Tétel (Fáry-Wagner). *Ha G egy egyszerű, síkbarajzolható gráf, akkor létezik olyan síkbeli ábrázolása is, melyben minden élet egy egyenes szakasszal rajzoltunk le.*

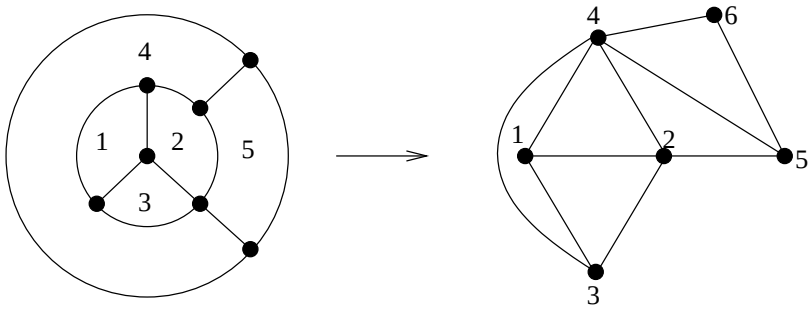
2.6. Síkbarajzolható gráfok duálisa

Közel másfél évszázada vették észre, hogy ha egy politikai térképet készítve az egyes országokat ki kell színezni és közben szomszédos (közös határvonallal rendelkező) országok nem lehetnek egy színűek, akkor a feladat 4 színnel mindig megoldható. Például a 2.13. ábrán látható térkép négy színnel (Piros, Kék, Zöld és



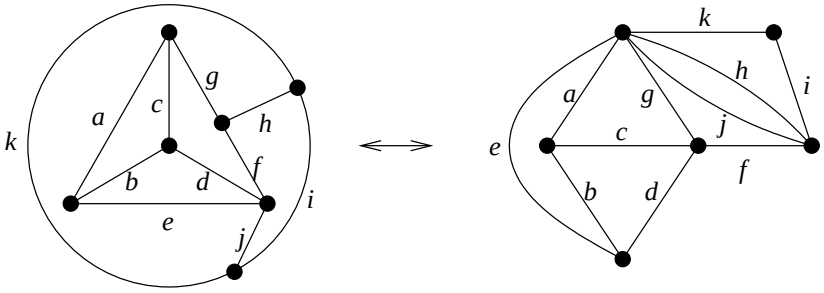
2.13. ábra.

Sárga) megszínezhető, még akkor is, ha a „külvilágot” (az összes korlátos tartomány egyesítésének komplementerét) is meg kell színezni. Számos (később hibásnak bizonyult) kísérletet tettek ennek bebizonyítására, de a probléma (a híres „négyszín sejtés”) sokáig nyitott volt és számos gráfelméleti kutatási területet inspirált. Végül 1977-ben sikerült Appel és Haken amerikai matematikusoknak a sejtés bizonyítása. A 2.11.3. pontban bebizonyítjuk, hogy öt színnel kiszínezhető minden térkép.
A későbbiekben (2.9., 2.11. és 3.5. szakasz) többször fogunk gráfok színezésével találkozni, ott azonban a gráf pontjaihoz rendelünk színeket (és az éllel összekötött pontok nem kaphatnak azonos színt). Azonban a térképszínezési feladatot könnyen átfogalmazhatjuk ez utóbbira: Minden síkbarajzolható G gráfhoz gyártsunk egy G^* gráfot az alábbi utasítással: G tartományaihoz (az „országokhoz”) rendeljük az új G^* gráf pontjait és G^*-ban akkor kössünk össze két pontot éllel, ha a megfelelő két G-beli tartománynak van közös határvonala (ld. a 2.14. ábrát).



2.14. ábra.

Az így gyártott G^* gráfot szokás a G **duálisának** is nevezni (főleg a villamos hálózatok elméletében, ld. később). Vegyük észre, hogy G^* is síkbarajzolható (az élei nem keresztezik egymást) és tartományai épp G pontjainak felelnek meg, így szokás G-t és G^*-ot egymás duálisának is nevezni.
Hamarosan látni fogjuk, hogy ez a „definíció” matematikailag problematikus, vegyük azonban előbb szemügyre a jó tulajdonságait! Az előző G és G^* gráfokat újrarajzoltuk a 2.15. ábrán. Ezúttal az éleiket jelöltük be, ügyelve arra, hogy ha G^* két pontját azért kötjük össze egy x éllel, mert a G megfelelő tartományainak volt egy közös y éle, akkor a G-beli y és a G^*-beli x éleket ugyanazzal a betűvel jelöljük. Írjuk most fel G néhány körét, pl. az $\{a,b,c\},\{a,b,d,f,g\}$ és az $\{i,k\}$ köröket. A G^* gráfban a megfelelő élhalmazok vágást alkotnak: ismét a 2.14. ábra pont–számozását használva az $\{a,b,c\}$ élek az 1. pontot, az $\{i,k\}$ élek a 6. pontot választják el a többitől, míg az $\{a,b,d,f,g\}$ élek az $\{1,2\}$ és a $\{3,4,5,6\}$ ponthalmazokat. Megfordítva, ha G vágásait tekintjük, azoknak G^* körei felelnek meg – ellenőrizzük pl. az $\{f,g,i,k\}$, az $\{f,g,j\}$ és a $\{h,j\}$ élhalmazokon.
Általában is belátható az alábbi állítás:



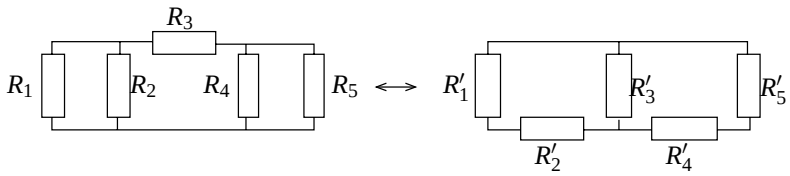
2.15. ábra.

2.6.1. Tétel. *Legyen C és Q egy síkbarajzolható G gráf valamely körének, ill. valamely vágásának az élhalmaza. Ekkor a most látott módon elkészített G^* gráfban C egy vágás, Q pedig egy kör élhalmaza lesz.*

Ugyancsak belátható, hogy ha G összefüggő is és F egy feszítő fája, akkor az F-nek megfelelő élek G^* egy feszítőfájának komplementerét alkotják.
Ennek segítségével is belátható a 2.5.3. Tétel (az Euler-féle $n-e+t=2$ formula): Válasszuk ki egy F feszítő fa éleit ($n-1$ darab), a többi él a duális gráf egy feszítőfáját alkotja. Mivel a duális gráfnak t pontja van, szükségképpen $e-(n-1)=t-1$ teljesül.
A 2.6.1. Tétel következménye az alábbi:

2.6.2. Tétel. *Legyen G egy síkbarajzolható gráf és G^* a fent definiált módon elkészített duálisa. Ekkor kör– és vágásmátrixaikra $C(G)=Q(G^*)$ és $C(G^*)=Q(G)$.*

Ismeretes, hogy egy kétpólusú alkatrészekből összerakott áramkör analízise során a Kirchhoff–féle hurok– és csomóponti törvények $C\mathbf{u}=0$, ill. $Q\mathbf{i}=0$ alakba írhatók (ahol az **u** és **i** vektorok komponensei az egyes alkatrészek feszültségei, ill. áramai).



2.16. ábra.

Így például a 2.16. ábrán látható első hálózat alkatrészeinek feszültségei között ugyanolyan kapcsolatok érvényesek, mint a második hálózat alkatrészeinek áramai között, és fordítva. Ha ez lenne a helyzet az egyes alkatrészeket leíró egyenletekre

is, tehát az $u_k = R_k i_k$ egyenletek helyett formálisan $i_k = R_k u_k$-t írnánk (vagyis a második hálózat ellenállásaira $R'_k = R_k^{-1}$ teljesülne), akkor a két hálózatot leíró egyenletrendszer matematikailag azonos lenne. Ez a villamos hálózatok elméletéből jól ismert dualitási elv:
Legyenek G és G^* egymás duálisai és a megfelelő élek helyére helyezzünk olyan ellenállásokat, melyek értéke egymás reciproka. Ekkor az első hálózat k-adik alkatrészének árama megegyezik a második hálózat k-adik alkatrészének feszültségével és viszont.
Például a 2.16. ábra baloldali hálózatára – többek között – felírhatók az $u_1 = u_2$ vagy az $i_3 = i_4 + i_5$ egyenletek (megfelelő „mérőirányok” rögzítése után) a jobboldali hálózatban ugyanekkor $i_1 = i_2$ és $u_3 = u_4 + u_5$ teljesülnek.
Nyilván nem szükséges ellenállás–hálózatokra szorítkozni – tetszőleges kétpólusú alkatrész szóba jöhet, csak a feszültség és áram szerepét kell felcserélni. Így lesz az $u = L\frac{di}{dt}$ egyenletű induktivitás „duálisa” az $i = C\frac{du}{dt}$ egyenletű kapacitás, vagy az „u adott, i tetszőleges” egyenletű feszültségforrás „duálisa” az „i adott, u tetszőleges” egyenletű áramforrás.

2.1. táblázat. Néhány „duális” fogalompár a villamos hálózatok elméletében

Feszültség	Áram
Feszültségforrás	Áramforrás
Rövidzár	Szakadás
Párhuzamos kapcsolás	Soros kapcsolás
Ellenállás	Vezetés (reciprok ellenállás)
Induktivitás	Kapacitás

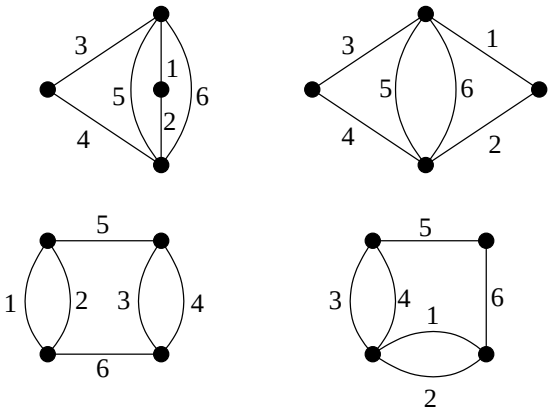
Hasonló táblázatban foglalhatjuk össze gráfok és duálisaik egymásnak megfelelő tulajdonságait.

2.2. táblázat. Néhány „duális” fogalompár a síkbarajzolható gráfok körében

Él	Él
Pont	Tartomány
Kör	Vágás
Fa	Fa komplementere
Párhuzamos élek	Soros élek
Hurokélek	Elvágó élek

Az eddig látottak a gráfelméletben legalább két évszázada ismertek (sőt egyes részeit már a régi görögök is valószínűleg tudták); a villamosságtani dualitás is kb. 150 éve ismert. Azonban már több, mint 70 éve észrevették, hogy az eddig elmondottak matematikailag nem teljesen korrektek.

Az az eljárás ugyanis, amivel egy síkbarajzolható G gráfhoz egy G^* duálist rendeltünk, tulajdonképpen nem G-hez, hanem G konkrét lerajzolásához rendelt egy új gráfot. Például a 2.17. ábra első sorának két rajza nyilván ugyanazon gráf két különböző lerajzolása. Ha viszont megszerkesztjük a duálisukat (az ábra második sora), azok már nem lesznek izomorfak: a baloldalinak nincs, a jobboldalinak van 2– és 4–edfokú pontja. Mivel a „rajz” csak szemléltető eszköz és nem tehetünk különbséget két, különféleképp rajzolt, de izomorf gráf között, nem mondhatjuk a két alsó gráf egyikéről sem, hogy a felsők duálisa.



2.17. ábra.

Másik probléma, hogy a dualitás–fogalomtól elvárhatnánk, hogy duális duálisa ismét az eredeti(vel izomorf) legyen. Nyilván ez sem teljesül, mert ha a 2.17. ábra két alsó gráfja közül a baloldali duálisát valaki úgy rajzolja le, ahogy az a felső sor jobboldalán látható, akkor az ismételt duális–képzés a jobb alsó gráfhoz fog vezetni. A problémát az előző szakasz végén bevezetett fogalom, a gyenge izomorfia segítségével oldhatjuk meg. Igazak ugyanis az alábbi – bizonyítás nélkül közölt – állítások.

2.6.3. Tétel (Whitney). *Legyen G síkbarajzolható gráf és H vele gyengén izomorf. Ekkor H is síkbarajzolható, G^* és H^* szintén gyengén izomorfak, végül $(G^*)^*$ és $(H^*)^*$ gyengén izomorfak G-vel, ill. H-val.*

Ha felidézzük, hogy a gyenge izomorfiát élek közötti körtartó megfeleltetésként definiáltuk, természetes ötletnek tűnik, hogy a dualitást is definiálhatnánk élek közötti, kört vágásba vivő megfeleltetésként. Az eddigi definícióktól való megkülönböztethetőség érdekében mondjuk azt, hogy a G és G^* gráfok egymás **absztrakt duálisai**, ha éleik közt létesíthető olyan, kölcsönösen egyértelmű leképezés, mely kört vágásba, vágást körbe visz. Nyilvánvaló, hogy ha G síkbarajzolható, akkor a lerajzolás után nyert „régi” duálisa egyben absztrakt duálisa is lesz. Megmutatható, hogy síkba nem rajzolható gráfhoz más eljárással sem lehet duálist rendelni:

2.6.4. Tétel (Whitney, 1932). *Egy gráfnak akkor és csak akkor létezik absztrakt duálisa, ha síkbarajzolható.*

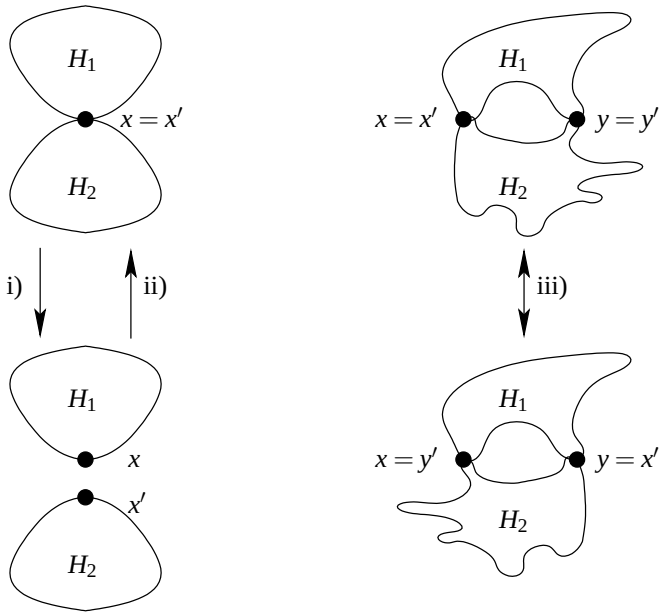
Jól használható az alábbi tétel gyengén izomorf gráfok felismerésére.

2.6.5. Tétel (Whitney). *Egy H gráf akkor és csak akkor gyengén izomorf G-vel, ha H-ból az alábbi három lépés ismételgetésével G-vel izomorf gráfot kaphatunk (2.18. ábra):*

i) Ha x olyan pontja H-nak, hogy $H-\{x\}$ két komponensre, H_1-re és H_2-re esik, akkor „húzzuk szét” H-t két komponensre.

ii) Az előző lépés fordítottja, ha H két komponensből álló gráf, akkor válasszunk ki mindkét komponensből egy-egy pontot és „ragasszuk össze” ezeknél a pontoknál.

iii) Ha x és y olyan pontjai H-nak, hogy $H-\{x\}$ és $H-\{y\}$ is összefüggő, de $H-\{x,y\}$ már nem, akkor „húzzuk szét” a két részt, majd ragasszuk össze fordítva (azaz x-hez y'-t, y-hoz x'-t ragasszuk).



2.18. ábra.

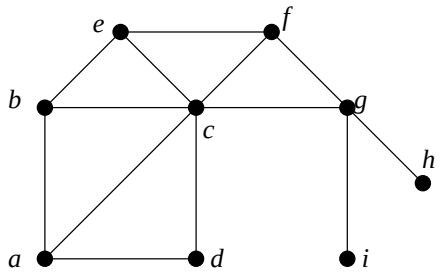
BIZONYÍTÁS: Csak azt bizonyítjuk be, hogy az ilyen lépésekkel mindig gyengén izomorf gráfot kapunk. Ebből következik az állítás egyik iránya, a másik irány bizonyítása lényegesen bonyolultabb.

Az élek közötti megfeleltetés mindhárom esetben értelemszerűen adódik, mindkét részben feleljenek meg az élek a széthúzás illetve összeragasztás előtti gráfban a megfelelő élnek. Be kell látnunk, hogy ez a megfeleltetés körtartó.
Ha az i) lépést használtuk és néhány él kört alkot H-ban, akkor ennek a körnek minden éle vagy H_1-ben van, vagy mindegyik H_2-ben. Nyilvánvaló, hogy ezek a széthúzás után is kört fognak alkotni. Ha pedig néhány él nem alkot kört H-ban, akkor a széthúzás után sem alkothatnak.
Ugyanígy látszik, hogy a ii) lépés alkalmazása is gyengén izomorf gráfot ad.
A iii) lépésnél, ha néhány él kört alkot H-ban, akkor vagy minden él az egyik részben van, vagy a kör tartalmazza x-et és y-t is, melyek két ívre bontják a kört. Az első esetben ugyanúgy következik az állítás, mint az előbb. A másik esetben pedig az egyik oldal megfordításával a kör x és y közötti egyik íve is megfordul, de így is kört fognak alkotni. □

2.7. Hogyan járjunk be egy gráfot?

2.7.1. Szemléletes előkészítés

A gráfelméleti algoritmusok során (ha tehát meg akarjuk állapítani, rendelkezik-e a gráf egy bizonyos tulajdonsággal, vagy konstruálni akarunk egy bizonyos tulajdonságú részgráfot stb.) nyilván fel kell használnunk a gráf szerkezetéről rendelkezésre álló információkat. Mint korábban említettük és a 3.4. szakaszban részletesen látni fogjuk, a gráfokat gyakran úgy tároljuk, hogy a pontokhoz megadjuk a szomszédaikat. Így a gráf szerkezetét leggyakrabban úgy „derítjük fel”, hogy – valamilyen sorrendben, valamilyen stratégia szerint – pontról szomszédos pontra lépve bejárjuk a gráfot. Ebben a fejezetben két különösen fontos keresési formáról, a szélességi keresésről (breadth–first–search, BFS) és a mélységi keresésről (depth–first–search, DFS) lesz szó. A következő három fejezetben látni fogjuk, hogy számos fontos algoritmus ezekre épül.



2.19. ábra.

A bejárási algoritmusok formális leírása előtt szemléltessük mindkettőt a a 2.19. ábrán látható gráfon. Tegyük fel, hogy az a pontból kiindulva akarjuk „bejárni” a

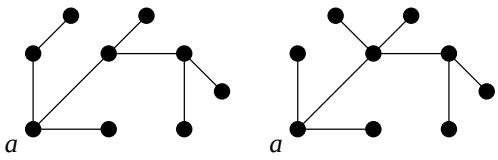
gráfot. Először járjuk be sorban a összes szomszédját: b, c, d. Utána járjuk be a első szomszédjának összes olyan szomszédját, ahol még nem jártunk (e), majd a második szomszédjának összes szomszédját (f, g) és így tovább. Ha már bejártuk a összes szomszédainak összes szomszédját, akkor menjünk abba a pontba, ahol legrégebben jártunk azok közül, amelyeknek még nem néztük végig a szomszédait (ez most f, de annak nincs már más szomszédja). Ezt az eljárást folytatjuk, amíg tudjuk. (A példánkon g-ből még bejárjuk h-t és i-t.)

Az eljárást szemléltethetjük úgy is, hogy a „bejáró” nem egy ember, hanem pl. egy minden irányban 1 él/sec sebességgel haladó „hullám”, akkor első körben a b, c és d pontokhoz jutunk el, a második körben az e, f, g, míg a harmadikban a h, i pontokhoz.

Ha viszont a gráf egy labirintus térképe és az a pontból egy „ember” kezdi bejárni a gráfot, akkor minden pontból egy új pontba próbál menni és csak akkor lép vissza, ha ez nem lehetséges. Ha pl. az a-ból először b-be megy, akkor a b, c, d utat követheti. Miután d-ből már nem tud tovább menni, visszalép egyet és c-ből megy tovább e-be, majd onnan f, g, h-ba. Onnan megint nem tud továbbmenni, de egy visszalépéssel g-ből eljut i-be.

Mindkét bejárás folyamán előfordulhat, hogy több lehetőség közül választhatunk, merre megyünk tovább. A szélességi keresésnél azt nem határoztuk meg, hogy egy pont szomszédait milyen sorrendben kell bejárni, a mélységi keresésnél pedig azt nem, hogy ha többfelé lehet továbbmenni, akkor merre menjünk. Az algoritmus konkrét végrehajtásakor ezt persze el kell döntenünk. Ezt tehetjük véletlenszerűen is, vagy például elhatározhatjuk, hogy mindig az ábécében előrébb állót választjuk.

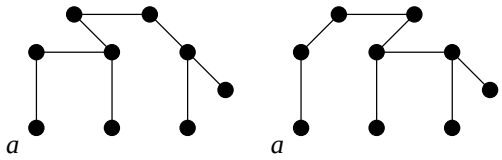
Könnyen látható, hogy egyik bejárás során sem „érünk körbe”, hiszen egy már bejárt pontba nem lépünk be még egyszer, ezért egy fát kapunk. A 2.20. ábrán látható két fát szélességi kereséssel kaptuk, az elsőnél az ábécét vettük figyelembe, a másiknál véletlenül döntöttünk. A 2.21. ábrán látható két fát pedig a mélységi kereséssel kaptuk ugyanígy.



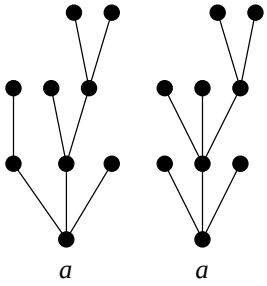
2.20. ábra.

Ha a két-két fát a 2.22. ill. a 2.23. ábrán újrarajzoljuk, intuitíve érthetővé válik, hogy az első esetben viszonylag „széles” és alacsony, a második esetben viszonylag keskeny és magas (vagy fordítva nézve „mély”) fákhoz jutunk.

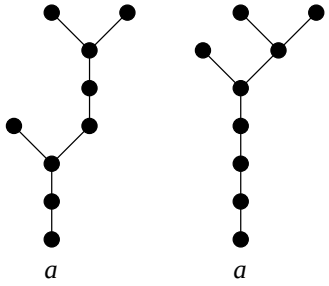
Ezeket fogjuk a továbbiakban BFS-, ill. DFS-fáknak, a bejárási-keresési módokat szélességi (vagy BFS-) ill. mélységi (vagy DFS-) bejárásnak vagy keresésnek nevezni.



2.21. ábra.



2.22. ábra.



2.23. ábra.

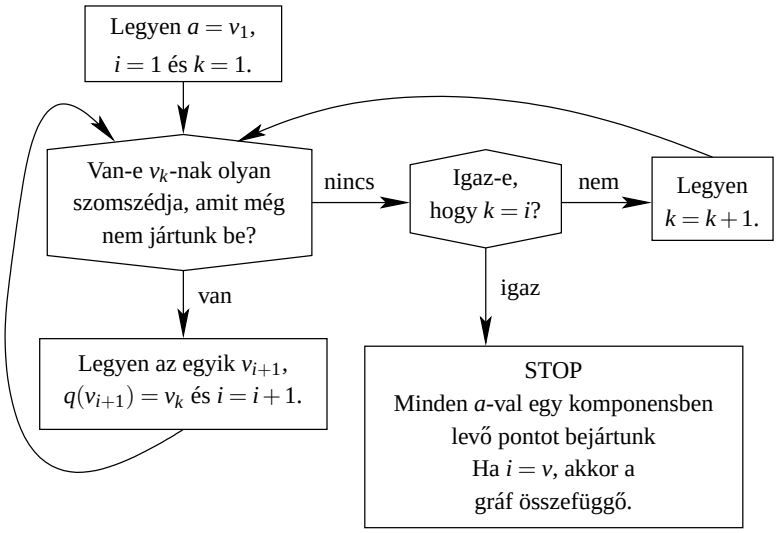
2.7.2. A kétféle bejárás leírása

A két bejárási algoritmust egységes jelölésrendszerrel fogjuk formálisan leírni. Így a leírások a szükségesnél valamivel hosszabbak lesznek, de később könnyebben hivatkozhatunk rájuk.

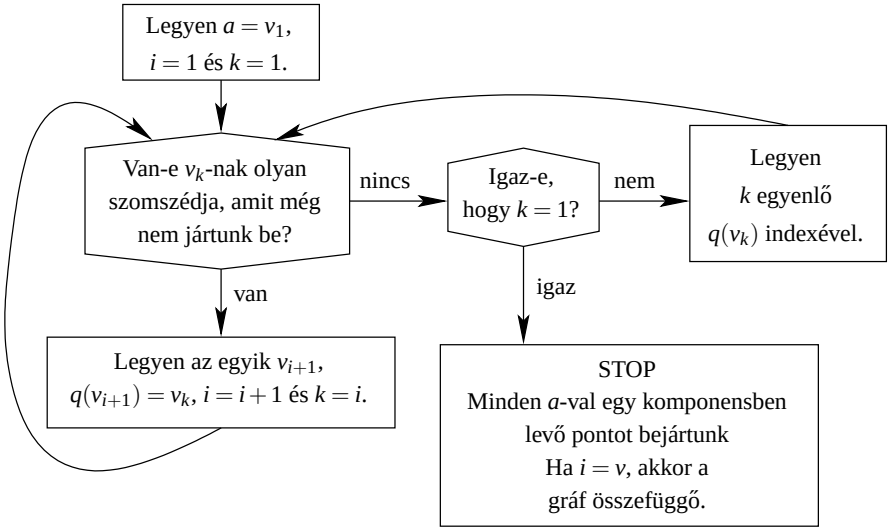
Mikor sorban bejárjuk a gráf pontjait, akkor tulajdonképpen sorszámokat adunk a pontoknak abban a sorrendben, ahogy bejártuk őket. Jelöljük az i-ediknek bejárt pontot v_i-vel. Az i értéke persze először 1 lesz, majd minden újabb pontnál eggyel növeljük. Tudnunk kell, hogy mi a sorszáma annak a pontnak, ahonnan éppen tovább akarunk lépni. Ezt jelölje k (mint **k**iinduló pont). Először ez is 1 lesz, majd a kétféle algoritmusban különbözőképpen változik. Hogy a bejárás végeztével felrajzolhassuk a bejárt fát, meg kell jegyezni, hogy v_x-re melyik pontból léptünk. Ezt a pontot jelölje $q(v_x)$. A gráf pontszámát pedig jelölje v.

Ezek után a kétféle bejárási eljárást a 2.24. és a 2.25. ábra mutatja. A 2.26. és a 2.27. ábrán megismételjük a BFS– ill. a DFS-bejárások egy-egy lehetséges eredményét a 2.19. ábrán látható gráfra. Az a-tól különböző pontok mellé zárójelben először v_i-t, majd $q(v_i)$-t tüntettük fel.

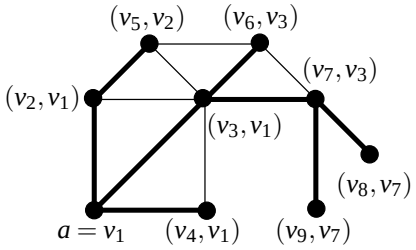
Jóllehet a leírások során irányítatlan gráfokkal foglalkoztunk, mindezek irányított gráfokra is elmondhatóak. Az egyik különbség ott van, hogy a „Van-e v_k-nak olyan szomszédja, amit még nem jártunk be?” helyett azt kell kérdeznünk, hogy „Mutat-e v_k-ból irányított él még be nem járt szomszédba?”. A másik különbség a STOP értelmezésében van: Ha $i = v$, akkor a-ból G minden más pontja irányított úton elérhető és mindent be is jártunk, ha nem, akkor csak azokban a pontokban jártunk, amelyek a-ból irányított úton elérhetőek.



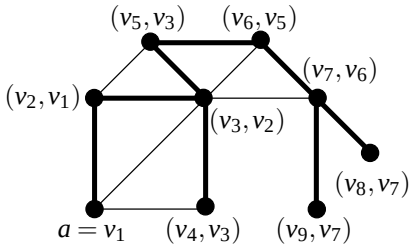
2.24. ábra. Szélességi keresés



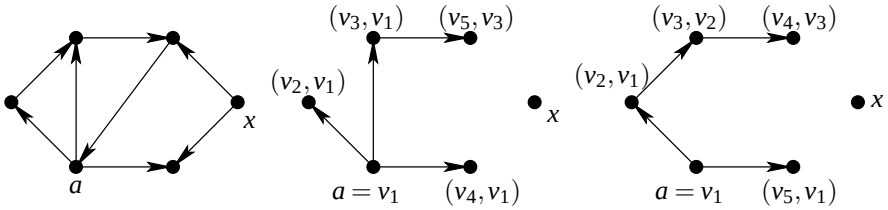
2.25. ábra. Mélységi keresés



2.26. ábra.

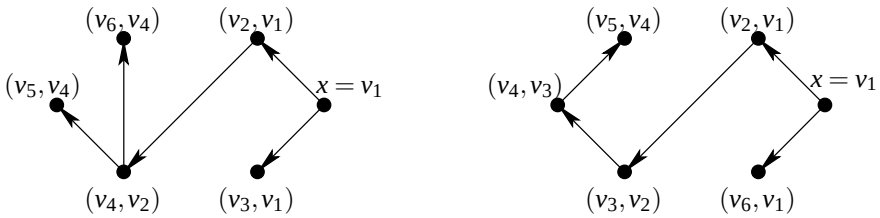


2.27. ábra.



2.28. ábra.

Szemléltessük a kétféle bejárást irányított gráfokra is. A 2.28. ábra első gráfjának az a pontból való egy-egy BFS-, ill. DFS-bejárása látható az ábra középső, ill. jobboldali részén. Az x pontba nyilván nem juthatunk el az a-ból irányított úton. Ugyanakkor az x pontból mindenhová eljuthatnánk, így onnét egy-egy BFS-, ill. DFS-bejárás egészen másképp néz ki, ld. a 2.29. ábrát.



2.29. ábra.

Vizsgáljuk meg a kétféle bejárás lépésszám-igényét! A szélességi keresés esetén sorra kell vennünk v_k összes szomszédját. A mélységi keresés esetén ugyan nem kell az összeset sorba vennünk az előrelépéshez, de v_k-ról vissza csak akkor léphetünk, ha már az összeset sorba vettük. Így minden pontban az eltöltött idő a pont fokszámával arányos. A teljes bejárás lépésszám-igénye tehát a gráf éleinek e számával arányos (hisz $d_1+d_2+\ldots+d_v=2e$). Pontosabban fogalmazva, figyelembe véve, hogy a gráf nem feltétlenül összefüggő, helyesebb azt mondani, hogy a tel-

jes lépésszám-igény $\max(v,e)$-vel arányos, vagy ami ugyanaz, $(e+v)$-vel arányos. (Általában is mindegy, hogy $\max(x,y)$-nal vagy $(x+y)$-nal arányos mennyiségről beszélünk, persze az arányossági tényezők különbözőek lehetnek.)
Vegyük észre (ld. a 3.1. Táblázat első sorát), hogy a legtöbb gráfelméleti adatstruktúra tárigénye is $(e+v)$-vel arányos. Ha az arányossági tényezőktől eltekintünk (és ezt mindig megtehetjük, hisz különben a felhasznált programozási nyelvek közti különbségeket és a felhasznált számítógépek műveleti sebessége közötti különbséget is figyelembe kellene venni), akkor megállapíthatjuk, hogy a BFS és DFS bejárásoknál gyorsabb nem is lehetséges, hisz lépésszámuk ugyanazzal az $(e+v)$-vel arányos, amennyivel arányos időre már ahhoz is szükségünk van, hogy pusztán beolvassuk a gráfot.

2.8. Legrövidebb utat kereső algoritmusok

2.8.1. Élsúlyozatlan eset

Adott egy összefüggő $G=(V,E)$ gráf és egy kitüntetett $s \in V$ pontja. Kérdezhetjük, mi a legrövidebb út s-ből egy másik kiválasztott t pontba, vagy akár azt is, hogy mi a legrövidebb út s-ből minden más pontba.
Egyelőre feltesszük, hogy az út hossza az utat alkotó élek száma (tehát nincsenek hosszabb és rövidebb élek). Ekkor s összes szomszédja egységnyi távolságra van s-től, ezen szomszédok minden olyan szomszédja, ami maga nem szomszédja s-nek, két egységnyi távolságra van s-től stb.[1]
Természetes gondolat tehát, hogy a szélességi keresést alkalmazzuk $a=s$ választással. Amikor az algoritmus véget ér, a kiválasztott t ponthoz határozzuk meg a $q(t)=u_1$ pontot; ha $u_1 \neq s$, akkor a $q(u_1)=u_2$ pontot; ha $u_2 \neq s$, akkor a $q(u_2)=u_3$ pontot stb. Nyilvánvaló, hogy előbb-utóbb eljutunk egy olyan k indexhez, melyre $u_k=s$, és akkor belátható, hogy az

$$(s=u_k,u_{k-1},u_{k-2},\ldots,u_1,t)$$

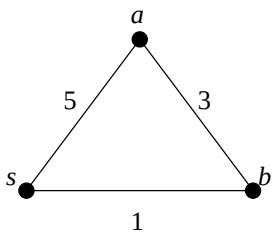
a legrövidebb út s-ből t-be.
Ha a gráf irányított volt, akkor ugyanez az algoritmus az s-ból t-be vezető legrövidebb irányított utat határozza meg.
Mennyi ennek az algoritmusnak a lépésszám-igénye? A bejáráshoz – mint már láttuk – $(e+v)$-vel arányos lépésszám kell, utána még annyi lépés, amilyen hosszú a keresett út. Mivel elképzelhető, hogy az út hossza e (gondoljunk arra, hogy a gráf egyetlen út is lehet), általában ennél gyorsabb algoritmus nem lehet.

2.8.2. Dijkstra algoritmusa

Számos alkalmazásnál az egyes élek különböző hosszúságú szakaszokat modellezneknek. Ilyenkor az út hosszán nem az utat alkotó élek számát, hanem ezen élek hosszá-

[1] „Apu, ugye ha majomtól származunk, akkor Te jobban hasonlítasz a majmokra, mint én?” (Recski Gábor, 6 éves)

nak összegét értjük. Ebben az esetben a fenti algoritmus nyilván nem alkalmazható: Például a 2.30. ábrán az s-ből a-ba vezető él hossza 5 egység, tehát rövidebb a b ponton át menni a-ba.



2.30. ábra.

Mind a mostani, mind a következő szakaszban $l(e)$-vel jelöljük az e él hosszát. Valamennyi algoritmusunk úgy fog kezdődni, hogy definiálunk egy v hosszúságú $d(\ )$ tömböt. Szemléletesen az u pontra $d(u)$ értéke azt fogja jelenteni, hogy az algoritmus során eddig talált, az s kezdőpontból u-ba vezető utak közül a legrövidebb hossza $d(u)$. Ennek megfelelően először $d(s)$ a 0 értéket kapja, a tömb minden más eleme a végtelent, vagyis minden algoritmusunk 0. lépése tartalmazni fogja a

$$d(s) \leftarrow 0 \text{ és minden } u \neq s\text{-re } d(u) \leftarrow \infty \qquad (*)$$

utasításokat. Nyilvánvaló továbbá, hogy minden algoritmus kulcslépése az lesz, hogy

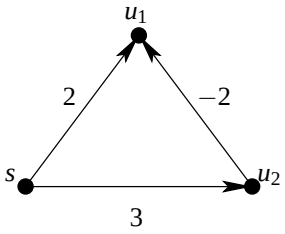
$$\text{ha } x\text{-ből vezet egy } e \text{ él } y\text{-ba és } d(y) > d(x) + l(e)$$

$$\text{akkor } d(y) \leftarrow d(x) + l(e) \qquad (**)$$

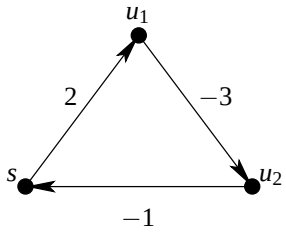
Nem túl nehéz belátni, hogy ha a $(**)$ javítás semmilyen élre nem működik már, akkor megállhatunk. Csak az a probléma, hogy ugyanaz az e él sokszor is javíthat (ha $d(x)$ értéke sokszor csökken a különféle x-be vezető élek miatt).
Ebben a szakaszban feltesszük, hogy minden él hossza nem negatív. Legyen az s-ből kiinduló és a szomszédos $u_1, u_2, u_3, \ldots$ pontokba vezető élek hossza rendre $l_1, l_2, l_3, \ldots$ és tegyük fel, hogy ezek közül l_1 a legkisebb (vagy az egyik legkisebb). Ekkor biztos, hogy u_1 -nek az s-től való távolsága l_1, hisz bármilyen más irányba indulva legalább ennyivel kezdődik az út, és a hossza csak nőhet. (Most használtuk ki, hogy $l(e) \geq 0$ minden e-re. A 2.31. ábra mutatja, hogy különben nem feltétlenül lenne így.) Ezt az észrevételt általánosítva elkészíthetjük a következő – még nem túl gyors – algoritmust:

0. lépés: $S \leftarrow \{s\}, T \leftarrow V - \{s\}$ és $(*)$

1. lépés: Minden S-beli pontból minden T-beli pontba vezető e élre végezzük el a $(**)$ javítást



2.31. ábra.



2.32. ábra.

2. lépés: A T-beli pontok közül legyen u_0 az, amelyiken a $d(u)$ érték a legkisebb. Tegyük át u_0-t T-ből S-be

3. lépés: Ha T üres, STOP. Különben folytassuk az 1. lépésnél.

Sajnos ennek az algoritmusnak a lépésszáma akár v^3-bel arányos is lehet (hisz az 1. lépés k-ik elvégzésekor $|S| = k$, $|T| = v - k$, és így az összes $(**)$ javítások száma $\sum k(v-k) = \sum kv - \sum k^2$, és az első szumma kb. $v^3/2$, a második kb $v^3/3$. Kis változtatással azonban egy nagyságrenddel gyorsabb algoritmushoz juthatunk (Dijkstra): Ennek az az alapötlete, hogy egy e él mentén a $(**)$ javítást csak egyszer kell elvégezni, ha „elég későn” végezzük el, vagyis csak akkor, ha már biztosak vagyunk abban, hogy az e él kezdőpontjának d értéke utána már nem fog tovább csökkenni:

0. lépés: $S \leftarrow \{s\}, T \leftarrow V - \{s\}$ és $(*)$, valamint u_0 legyen s

1. lépés: Csak az u_0-ból a T-beli pontokba vezető e élekre végezzük el a $(**)$ javítást.

2. lépés: A T-beli pontok közül legyen u_0 az, amelyiken a $d(u)$ érték a legkisebb. Tegyük át u_0-t T-ből S-be.

3. lépés: Ha T üres, STOP, különben folytassuk az 1. lépésnél.

Világos, hogy ennek lépésszáma legfeljebb v^2 -tel arányos (hisz az 1. lépésnél a minimum megkeresése mindig $|T|$ lépést igényel, és $\sum |T|$ értéke kb. $v^2/2$, míg a 2. lépés mindig u_0 fokszámával arányos lépésszámot igényel, és a fokszámok összege $(= 2e)$ is legfeljebb v^2-tel arányos).
A leálláskor ha egy u pontra $d(u) = \infty$, akkor irányítatlan gráfok esetén u és s a gráf két különböző komponensében van, irányított gráfok esetén ez csak azt jelenti, hogy s-ből irányított úton nem lehet u-ba eljutni.

2.8.3. Ford algoritmusa

Megengedhető-e, hogy az élek hossza negatív legyen? A 2.32. ábra azt sugallja, hogy nem, hisz az $(s_1,u_1),(u_1,u_2),(u_2,s)$ sorrendben örökké csökkenthetnénk a

$d(u_i)$ értékeket (és persze a $d(s)$ értéket is) a $(**)$ javításokkal. Ugyanakkor, a 2.31. ábrán a $d(s) = 0, d(u_1) = 1, d(u_2) = 3$ értékeket nyilván nem lehet tovább javítani, tehát semmi okunk nincs ezt kizárni.
Nyilván nem a negatív élhosszakat kell kizárnunk, hanem azt, hogy egy irányított kör mentén az élhosszak összege legyen negatív. (Irányítatlan gráfok esetén persze ez automatikusan kizár minden negatív hosszúságú élt, hisz azon oda-vissza haladva örökké csökkenthetnénk a $d(u)$ értékeket.) Tekintsünk tehát egy irányított gráfot, melyben az élhosszak között lehetnek negatív számok, de bármely irányított kör mentén az élhosszak összege nem negatív kell, hogy legyen.
Az ilyen gráfokban Ford alábbi algoritmusa alkalmazható:

0. lépés: Számozzuk meg az éleket 1-től e-ig (tetszőleges lehet ez a sorrend, de rögzítsük le). Legyen $i \leftarrow 1$ és $(*)$

1. lépés: A rögzített sorrendben végezzük el a $(**)$ javítást minden élen.

2. lépés: $i \leftarrow i+1$. Ha $i > v$, akkor STOP, különben folytassuk az 1. lépésnél.

Ez az egyszerű algoritmus (melynek lépésszáma nyilván ev-vel arányos) könnyen beláthatóan megtalálja a legrövidebb utak hosszát. Az ev általában jóval nagyobb a v^2-nél, ezt az árat kell fizetnünk azért, hogy negatív élhosszúságokat is megengedünk.
Ennek az algoritmusnak még egy jó tulajdonsága van. Tegyük fel, hogy az élhosszúságok beadása során valami input hiba történt és a gráfban mégis van egy negatív összhosszúságú irányított C_0 kör. Hogy lehet ezt észrevenni? (Egy v pontú egyszerű irányított gráfban az irányított körök száma 2^v-nél több is lehet – sőt akár $v!$ körüli nagyságrend is elképzelhető –, ezért az összes irányított kör ebből a szempontból való ellenőrzése nyilván nem jöhet szóba.) Mivel bármely kör hossza legfeljebb v, ezért az algoritmus során az 1. lépés legkésőbb v-szeri ismétlése után C_0 elkezdi éreztetni a 2.32. ábrán szemléltetett hatását. Ha tehát van ilyen C_0 kör, akkor még $i = v+1$ mellett is szeretne valamelyik él $(**)$ javítást végezni.
Ennek alapján a 2. lépést érdemes az alábbiak szerint módosítani:

2'. lépés: Ha az 1. lépés során egyetlen javítás sem történt, akkor STOP (és megtaláltuk a minimális úthosszakat). Különben $i \leftarrow i+1$. Ha $i \leq v+1$, folytassuk az 1. lépésnél; ha $i > v+1$, akkor STOP (és van negatív összhosszúságú irányított kör).

2.8.4. Floyd algoritmusa

Ebben a szakaszban is egy legrövidebb utakat kereső algoritmust ismertetünk. Az előző két szakaszban eredetileg csak két adott pont távolságát akartuk meghatározni, de „melléktermékként" megkaptuk egy adott pont és az összes többi pont távolságát. Most azonban az összes pontpár távolságát szeretnénk meghatározni egy adott súlyozott gráfban, amiben nincsen negatív összsúlyú irányított kör. Természetesen ha

a Ford algoritmust végigcsináljuk minden pontból kiindulva, akkor minden távolságot megkapunk, de így ev^2-nel lesz arányos az algoritmus lépésszáma. A következő algoritmus viszont ugyanezt a feladatot v^3-nal arányos lépésszámmal hajtja végre.
Tegyük fel tehát, hogy adott a G irányított gráf a $V(G) = \{v_1, \ldots, v_n\}$ pontokon. A v_i-ből v_j-be mutató él hosszát, azaz súlyát, jelöljük $l(i,j)$-vel és tegyük fel, hogy nincs a gráfban negatív összsúlyú irányított kör. Ha nincs él v_i-ből v_j-be, akkor legyen $l(i,j) \leftarrow \infty$. Legyen továbbá $l(i,i) \leftarrow 0$ minden $i = 1,2,\ldots,n$-re. Jelölje $d^{(k)}(i,j)$ a v_i-ből v_j-be vezető legrövidebb olyan irányított út hosszát, ami (v_i-n és v_j-n kívül) csak k-nál szigorúan kisebb indexű pontokon megy át. Így $d^{(1)}(i,j) = l(i,j)$ lesz és az is nyilvánvaló, hogy $d^{(n+1)}(i,j)$ pedig az eredetileg keresett legrövidebb irányított út hossza lesz v_i-ből v_j-be.
Világos, hogy a v_i-ből v_j-be vezető legrövidebb olyan út, ami csak $k+1$-nél szigorúan kisebb indexű pontokon megy át, vagy átmegy v_k-n, vagy nem. Ha nem megy át, akkor nyilván $d^{(k+1)}(i,j) = d^{(k)}(i,j)$. Ha viszont átmegy v_k-n, akkor könnyen látható, hogy $d^{(k+1)}(i,j) = d^{(k)}(i,k) + d^{(k)}(k,j)$. Csak azt kell megnéznünk, hogy melyik esetben találunk rövidebb utat. Ezek után világos, hogy a következő algoritmus a kívánt eredményre vezet v^3-nal arányos lépésszámban.

0. lépés: Minden i,j rendezett párra legyen $d^{(1)}(i,j) \leftarrow l(i,j)$. Legyen továbbá $k \leftarrow 2$.

1. lépés: Minden i,j rendezett párra

$$d^{(k+1)}(i,j) \leftarrow \min\left\{d^{(k)}(i,j), \quad d^{(k)}(i,k) + d^{(k-1)}(k,j)\right\}.$$

2. lépés: Ha $k = n+1$, akkor STOP. Különben $k \leftarrow k+1$ és folytassuk az 1. lépésnél.

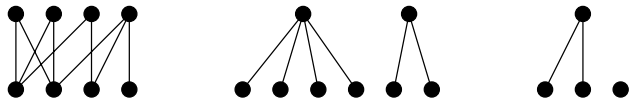
2.9. Párosítások és folyamok

2.9.1. Párosítás páros gráfban

2.9.1. Definíció. *Egy G gráfot **páros gráfnak** nevezünk, ha a G pontjainak $V(G)$ halmaza két részre, egy A és B halmazra osztható úgy, hogy G minden élének egyik végpontja A-ban, másik végpontja B-ben van. Ennek jelölése: $G = (A,B)$. A $K_{a,b}$-vel jelölt **teljes páros gráf** olyan $G = (A,B)$ páros gráf, ahol $|A| = a$ és $|B| = b$, és amelyben minden A-beli pont össze van kötve minden B-beli ponttal.*

Páros gráfok láthatók a 2.33. ábrán.
Páros gráf a már korábban megismert $K_{3,3}$ Kuratowski-gráf is.

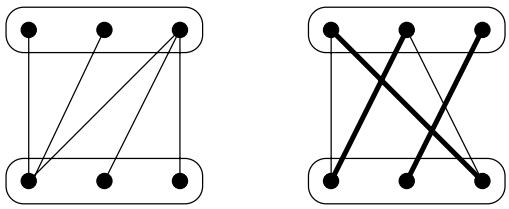
2.9.2. Tétel. *Egy G gráf akkor és csak akkor páros gráf, ha minden G-ben levő kör páros hosszúságú.*



2.33. ábra.

BIZONYÍTÁS: Ha G páros gráf, és C egy kör G-ben, akkor C pontjai felváltva vannak A-ban és B-ben. Így $|V(C)|$ nyilván páros.
Ha G minden köre páros hosszú, akkor megadhatjuk az A és B halmazt. Válasszunk egy tetszőleges $v \in V(G)$ pontot. Legyen ez A első pontja. v minden szomszédját tegyük B-be, majd minden eddig B-ben levő pont minden szomszédját tegyük A-ba. Most minden A-beli minden eddig még nem szerepelt szomszédját tegyük B-be, és ezt az eljárást folytassuk addig, amíg minden pontot el nem helyeztünk. Ez biztosan jó elosztás, hiszen ha most lenne például A-ban két szomszédos pont, akkor kell lennie a gráfban páratlan körnek is, ami viszont ellentmondás volna. Ha a gráf nem összefüggő, akkor ezt az eljárást komponensenként hajtsuk végre. □

Legyenek most A pontjai fiúk, B pontjai lányok. Egy fiút összekötünk egy lánnyal, ha ismerik egymást. Hány párt lehet összehozni? Könnyen látható, hogy a 2.34. ábra második gráfján 3 párt össze lehet állítani, az első gráfban viszont csak kettőt. Ennek az az oka, hogy bár a 3 fiú együtt ismer 3 lányt, de van két fiú, akik csak ugyanazt az egy lányt ismerik. Tehát nyilván csak akkor van olyan párosítás, hogy minden fiúnak jut pár, hogyha akárhogy is választunk ki k fiút, ők összesen legalább k lányt ismernek. Ez általánosan is igaz, sőt elégséges feltétel is.



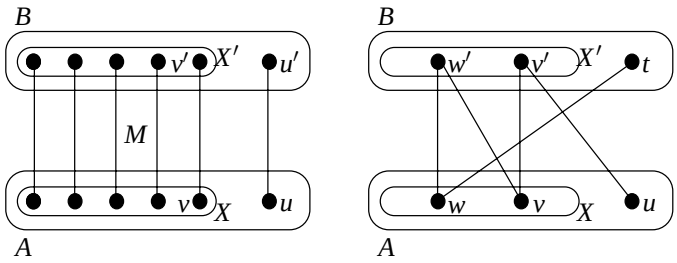
2.34. ábra.

2.9.3. Definíció. ***Párosításnak**, vagy **részleges párosításnak** nevezünk egy M élhalmazt, ha semelyik két élnek nincs közös pontja. Az ilyen éleket **független éleknek** is nevezzük. A részleges párosítás **lefedi** éleinek végpontjait. Egy párosítást **teljes párosításnak** nevezünk, ha a gráf minden pontját lefedi.*

$N(X)$-szel jelöljük egy $X \subseteq V(G)$ ponthalmaz szomszédainak halmazát, vagyis $N(X)$ azon y pontok halmaza, amelyekhez van olyan él, melynek egyik végpontja y, másik pedig egy X-beli pont.

2.9.4. Tétel. [Hall] *Egy $G = (A,B)$ páros gráfban akkor és csak akkor van A-t lefedő párosítás, ha minden $X \subseteq A$ részhalmazra $|N(X)| \geq |X|$. (Ezt a feltételt **Hall-feltételnek** nevezzük.)*

BIZONYÍTÁS: Nyilvánvaló, hogy ha van A-t lefedő párosítás, akkor teljesül a feltétel, hiszen ekkor a párosítás élei minden ponthoz egyértelműen hozzárendelnek egy B-beli pontot.
Tegyük most fel, hogy teljesül a Hall-feltétel, és lássuk be, hogy ekkor van A-t lefedő párosítás. Tegyük fel, hogy már van egy M párosításunk, ami lefedi az $X \subset A$ halmazt, de még van olyan $u \in A - X$ pont, amit nem (2.35. ábra). Minden $v \in X$ pont M-beli párját jelöljük v'-vel, X' pedig legyen a B-beli, M által lefedett pontok halmaza. Ha u-nak van szomszédja $B - X'$-ben, akkor egy élet hozzávehetünk M-hez.



2.35. ábra.

Lehetséges azonban, hogy u-nak minden szomszédja X'-ben van. Ekkor is előfordulhat, hogy növelni tudjuk a párosítás élszámát. Ha van egy olyan P út, ami egy $A - X$-beli pontból indul, egy $B - X'$-beli pontban végződik, és minden második éle M-beli, de a többi nem M-beli (2.35. ábra), akkor növelhetjük a párosítást, ekkor ugyanis a P út első és utolsó éle nem M-beli, tehát eggyel több nem M-beli él szerepel benne, mint az M-beliek száma. Az ilyen P utakat **javító útnak** nevezzük. Ha tehát $M' = (M - (M \cap P)) \cup (P - M)$, vagyis ha M-ből elhagyjuk a P-ben szereplő éleket és hozzávesszük a többi P-beli élet, akkor az így kapott M' párosítás élszáma eggyel nagyobb lesz. A „javító utakat és részeiket", vagyis az olyan utakat, amelyek $A - X$-beli pontból indulnak és minden második élük M-beli, de a többi nem, **alternáló útnak** nevezzük.
Tegyük fel, hogy már javító úttal sem növelhetjük a párosítást. Belátjuk, hogy ekkor már M lefedi A-t. Legyen T' azon B-beli pontok halmaza, amelyek elérhetők u-ból alternáló úttal. Ekkor feltevésünk szerint $T' \subseteq X'$. Jelölésünk szerint T a T'-beli pontok párjai, és nyilván $T \subseteq X$ (ld. a 2.36. ábrát). Belátjuk, hogy $N(T) = T'$. A párosításból világos, hogy $T' \subseteq N(T)$. Tegyük fel tehát, hogy van egy olyan $\{x,y\}$ él, hogy $x \in T$ és $y \notin T'$. Legyen P egy alternáló út u-ból x'-be. Ekkor P nem megy át x-en, hiszen P utolsó éle nem lehet az M-beli $\{x,x'\}$ él, és ha egy közbeeső pont volna x, akkor P-nek kétszer kellene átmennie x'-n. Így azonban P-t

folytatva $\{x',x\}$-szel majd $\{x,y\}$-nal egy javító utat kaptunk u-ból $y \notin T'$-be. Ez pedig ellentmond T' definíciójának.
Tehát $N(T) = T'$. Mivel azonban u-nak is minden szomszédja csak T'-ben lehet, a $T \cup \{u\} \subseteq A$ halmazra $N(T \cup \{u\}) = T'$, de $|T'| = |T| < |T \cup \{u\}|$, vagyis nem teljesül a Hall-feltétel. □

Ennek a tételnek egy egyszerű következménye Frobenius tétele.

2.9.5. Tétel (Frobenius). *Egy $G = (A,B)$ páros gráfban akkor és csak akkor van teljes párosítás, ha $|A| = |B|$ és $|N(X)| \geq |X|$ minden $X \subseteq A$-ra.*

BIZONYÍTÁS: A két feltétel szükségessége nyilvánvaló. Ha viszont teljesül a második feltétel, akkor a Hall-tétel miatt van A-t lefedő párosítás. Mivel azonban $|A| = |B|$, ez lefedi B-t is. □

A Hall-tétel bizonyításában leírtak alkalmazásával, javító utak keresésével hatékony algoritmust kapunk a maximális élszámú párosítás megtalálására. Ez az algoritmus **magyar módszer** néven vált ismertté. Az algoritmus lényege a következő.
Amíg tudunk, egy párosításhoz hozzáveszünk további független éleket, így kapunk egy M párosítást, ami még nem feltétlenül maximális. Ha ez már nem lehetséges, akkor keresünk egy javító utat, és ennek segítségével növeljük a párosítást. A 2.9.11. tétel bizonyítása során adódni fog, hogy ha a javító utak módszerével az M párosítás nem növelhető, akkor M-nél több élű párosítás a gráfban nem létezhet.
Hogyan keressük a javító utat? Induljunk ki egy A-beli, M által le nem fedett u pontból és mintha szélességi keresést végeznénk, menjünk el ennek összes szomszédjába, amelyeket $b_1,\ldots,b_d$ jelöljön. Ezek nyilván mind B-beli pontok és mindet lefedi M, hiszen ellenkező esetben ennek a pontnak u lehetne a párja, vagyis M-hez hozzávehetnénk még egy független élet. Miután M lefedi a $b_1,\ldots,b_d$ pontokat, jelölje $a_1,\ldots,a_d$ ezek M által meghatározott párjait. Most minden $a_1,\ldots,a_d$ pontból kiinduló, nem M-beli élen elérhető pontjába menjünk el. Látható, hogy ezek éppen azok a pontok, amelyekbe vezet u-ból 3 élből álló alternáló út. Folytassuk ezt az eljárást, amíg lehet. Tehát lényegében a BFS algoritmust alkalmazzunk, csak minden páros sorszámú szintről M-beli és minden páratlan sorszámú szintről nem M-beli éleken haladhatunk tovább.
Ha eljutunk egy B-beli M által le nem fedett pontig, akkor találtunk javító utat, ha pedig nem, akkor nincs u-ból kiinduló javító út. Ha tehát ezt az eljárást minden szóba jövő u-ra elvégezzük, akkor vagy találunk egy javító utat vagy belátjuk, hogy nincs ilyen.

2.9.2. König és Gallai tételei

2.9.6. Definíció. *Jelöljük $\nu(G)$-vel a G gráfban található **független élek** maximális számát. $X \subseteq V(G)$ egy **lefogó ponthalmaz**, ha G minden élének legalább egyik végpontját tartalmazza. A lefogó pontok minimális számát $\tau(G)$-vel jelöljük. $Y \subseteq E(G)$ **lefogó élhalmaz**, ha minden pontot lefog. A lefogó élek minimális számát $\rho(G)$ jelöli. $X \subseteq V(G)$ **független ponthalmaz**, ha nincs benne két szomszédos pont. A független pontok maximális száma $\alpha(G)$.*

A „lefogó ponthalmaz ill. élhalmaz” helyett használják a **lefedő ponthalmaz ill. élhalmaz** kifejezést is.

2.9.7. Tétel. $\nu(G) \leq \tau(G)$ *minden G gráfra.*

BIZONYÍTÁS: Legyen M egy maximális méretű független élhalmaz. Mivel pusztán M éleinek lefogásához már $\nu(G) = |M|$ pontra van szükség, ezért $\tau(G) \geq |M|$. □

Könnyen látható, hogy például $\nu(K_3) = 1 < \tau(K_3) = 2$.
Ugyanígy látható be a következő is.

2.9.8. Tétel. $\alpha(G) \leq \rho(G)$ *minden G gráfra.* □

Két újabb összefüggést adnak meg ezek között a számok között a következő tételek.

2.9.9. Tétel (Gallai). $\tau(G) + \alpha(G) = v(G) = |V(G)|$ *minden hurokmentes G gráfra.*

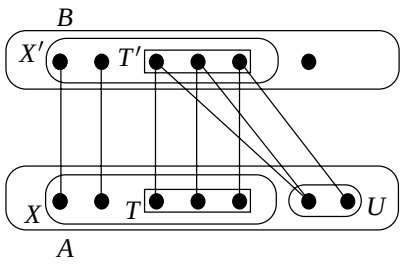
BIZONYÍTÁS: Egy X halmaz pontjai akkor és csak akkor függetlenek, ha a $V(G) - X$ halmaz lefogó ponthalmaz. Hiszen ha X nem független, akkor van két összekötött pont, és így $V(G) - X$ nem fogja le ezt az élet. Fordítva, ha $V(G) - X$ nem fog le egy huroktól különböző élet, akkor X-ben ennek az élnek mindkét végpontja szerepel. Tehát $\tau(G) \leq |V(G) - X|$ teljesül minden X független ponthalmazra. Ebből pedig következik, hogy $\tau(G) + \alpha(G) \leq v(G)$. Hasonlóan $\alpha(G) \geq |V(G) - Y|$ minden Y lefogó ponthalmazra, amiből $\tau(G) + \alpha(G) \geq v(G)$ következik. □

2.9.10. Tétel (Gallai). $\nu(G) + \rho(G) = v(G)$ *minden G gráfra, amelyben nincs izolált pont.*

BIZONYÍTÁS: Egy $\nu(G)$ elemű X független élhalmaz lefog $2\nu(G)$ különböző pontot. A többi pont (mivel nincs köztük izolált) nyilván lefogható $v(G) - 2\nu(G)$ éllel, így $v(G) - \nu(G) \geq \rho(G)$. Másrészt, ha Y egy minimális lefogó élhalmaz, akkor Y néhány (mondjuk k darab) diszjunkt csillag egyesítése. Ha ugyanis Y tartalmazna kört, akkor annak bármely élét, ha pedig 3 hosszú utat, akkor annak középső élét el lehetne hagyni Y-ból, mert a többi él még mindig lefogná az összes pontot. Így $\rho(G) = v(G) - k$ (hiszen k komponensű erdőről van szó). Ha minden csillagból kiválasztunk egy élet, az így kapott élhalmaz nyilván független. Tehát $\nu(G) \geq k = v(G) - \rho(G)$. □

2.9.11. Tétel (König). *Ha* $G = (A, B)$ *páros gráf, akkor* $\nu(G) = \tau(G)$. *Ha nincs G-ben izolált pont, akkor* $\alpha(G) = \rho(G)$ *is teljesül.*

BIZONYÍTÁS: Először $\nu(G) = \tau(G)$-t bizonyítjuk. Legyen M egy olyan párosítás, mely a javító utak módszerével már nem bővíthető és használjuk a 2.36. ábra jelöléseit. Legyen $U = A - X$, T' azon B-beli pontok halmaza, amelyek elérhetők U-ból alternáló úton, T pedig ezek párjainak halmaza.



2.36. ábra.

Legyen $Y = T' \cup (X - T)$. Ennek a halmaznak éppen $|M|$ pontja van. Ezek minden élet lefognak, hiszen $N(T \cup U) = T'$, ugyanúgy mint a Hall–tétel bizonyításában. Így $\tau(G) \leq |M| \leq \nu(G)$, amiből viszont a 2.9.7. tétel miatt már következik az állítás. Most már könnyű belátni, hogy $\alpha(G) = \rho(G)$. Gallai két tétele miatt ugyanis $\nu(G) + \rho(G) = \tau(G) + \alpha(G)$, és az imént láttuk, hogy $\nu(G) = \tau(G)$. □

Következmény: A 2.9.5. tétel bizonyítása után megismert magyar módszer hatékony algoritmus $\nu(G)$ és $\tau(G)$ értékének meghatározására (sőt, egy maximális független élhalmaz, illetve egy minimális lefogó ponthalmaz megtalálására) bármely G páros gráfban.

2.9.3. Párosítás tetszőleges gráfban

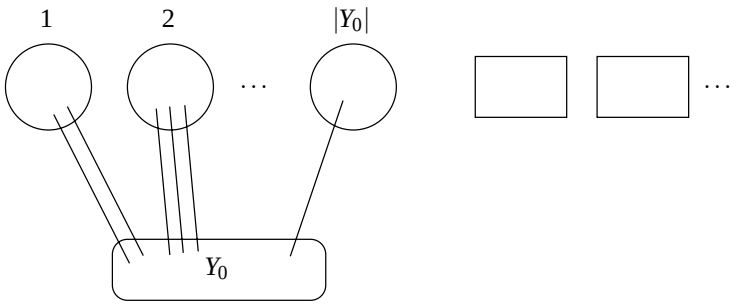
Páros gráfok esetén a Hall–feltétel elégséges teljes párosítás létezéséhez, ha $|A| = |B|$. Tutte olyan feltételt talált, ami szükséges és elégséges tetszőleges gráfra. Itt Gallai bizonyítását közöljük. Mindenekelőtt egy jelölés: $c_p(H)$-val jelöljük a H gráf páratlan (vagyis páratlan sok pontot tartalmazó) komponenseinek számát.

2.9.12. Tétel (Tutte). *Egy G gráfban akkor és csak akkor létezik teljes párosítás, ha minden $X \subseteq V(G)$-re $c_p(G - X) \leq |X|$, azaz akárhogy hagyunk el a gráfból néhány pontot, a maradékban a páratlan komponensek száma ennél több nem lehet.*

BIZONYÍTÁS: Ha G-ben van teljes párosítás, akkor nyilvánvalóan teljesül a feltétel. Hiszen ha elhagyjuk a gráfból X-et, akkor a páratlan komponensek mindegyikéből az eredeti gráfban indul ki legalább egy párosításbeli él, és ezek az élek csak egy-egy (különböző) X-beli pontba mehetnek. Tehát $c_p(G - X) \leq |X|$.
A feltétel elégséges voltának bizonyítása már jóval bonyolultabb.
Tegyük fel tehát, hogy teljesül a feltétel. Ekkor $X = \emptyset$-re is igaz, vagyis $c_p(G) \leq |X| = 0$, tehát G csak páros komponensekből áll, így $|V(G)|$ páros. Ebből következik, hogy $c_p(G - X) \neq |X| - 1$. Ha ugyanis $|X|$ páros, akkor ebből az következne, hogy G pontjainak száma páratlanszor páratlan plusz a páros komponensek plusz $|X|$, vagyis $|V(G)|$ páratlan volna. Ha $|X|$ páratlan, akkor pedig G pontszáma párosszor páratlan plusz a páros komponensek plusz a páratlan $|X|$, vagyis ekkor is ellentmondásra jutunk.

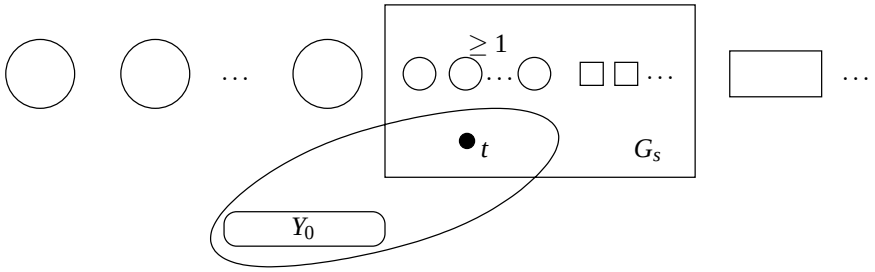
(1) Indirekt tegyük fel, hogy van olyan gráf, amelyre teljesül a feltétel, de nincs benne teljes párosítás. Legyen G egy minimális pontszámú ilyen ellenpélda.

(2) Egy $Y \subseteq V(G)$ ponthalmazt **gátnak** hívunk, ha $c_p(G-Y) = |Y|$. Például az $\emptyset$ és minden egyelemű halmaz ilyen. Legyen Y_0 egy maximális pontszámú gát G-ben. (2.37. ábra)



2.37. ábra.

(3) Belátjuk, hogy a $G-Y_0$-ban nincsenek páros komponensek. Ha létezik ugyanis egy ilyen G_s komponens, annak egy t pontját Y_0-hoz véve $c_p(G-Y_0-\{t\} \geq |Y_0|+1$ lenne, hiszen G_s-ből t elhagyásával legalább egy újabb páratlan komponens keletkezik. Ekkor viszont az eredeti feltétel miatt egyenlőségnek kell állnia, tehát $Y_0 \cup \{t\}$ is gát lenne (2.38. ábra).

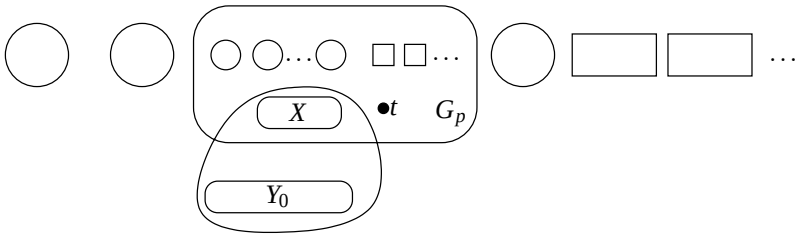


2.38. ábra.

(4) Most azt látjuk be, hogy egy G_p páratlan komponensből egy tetszőleges t pontot elhagyva létezik teljes párosítás a komponensben. Ellenkező esetben, mivel G minimális ellenpélda, kell lennie egy $X \subseteq G_p - \{t\}$ halmaznak, amelyre $c_p(G_p - \{t\} - X)$ nagyobb, mint $|X|$, tehát legalább $|X|+2$. Ekkor viszont

$$c_p(G-X-Y_0-\{t\}) \geq |Y_0|-1+|X|+2 = |X \cup Y_0 \cup \{t\}|,$$

vagyis $X \cup Y_0 \cup \{t\}$ egy Y_0-nál nagyobb gát, ami ellentmond a feltevésünknek (2.39. ábra).



2.39. ábra.

(5) Helyettesítsünk minden páratlan komponenst egyetlen ponttal. Belátjuk, hogy ezek a pontok és Y_0 összepárosíthatók.
Hagyjuk el az Y_0-on belüli éleket. Így egy páros gráfunk marad, amelynek egyik osztálya Y_0 pontjai, a másik pedig a páratlan komponenseknek megfelelő pontok. Ez utóbbi pontokból bárhogy választunk ki p darabot, azok együtt legalább p darab Y_0-beli ponttal szomszédosak, hiszen különben Y_0-nak (és így $V(G)$-nek) egy p-nél kevesebb elemű részhalmazát elhagyva p darab páratlan komponens keletkeznék az eredeti G gráfban. Így a Hall tételből következik, hogy a páros gráfban van $|Y_0|$ elemű független élhalmaz, vagyis egy teljes párosítás.
Most már könnyen megkonstruálható G-ben a teljes párosítás. Húzzuk be az iménti éleknek megfelelő éleket. Egy ilyen él egy páratlan komponensből lefoglal egy pontot. A (4) pont szerint a páratlan komponensek ezeket kihagyva párosíthatók. Páros komponensek pedig a (3) pont szerint nem is voltak. □

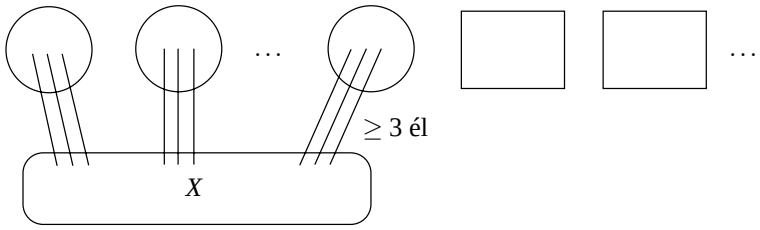
A következő tétel előtt meg kell említenünk egy definíciót.

2.9.13. Definíció. *Egy gráf 2-szeresen **élösszefüggő**, ha bárhogy hagyunk el a gráfból 2-nél kevesebb élet, a maradék gráf összefüggő.*

Evvel kapcsolatos kérdésekkel máshol bővebben foglalkozunk.

2.9.14. Tétel (Petersen). *Ha G 3-reguláris, 2-szeresen élösszefüggő gráf, akkor létezik benne teljes párosítás.*

BIZONYÍTÁS: A Tutte tétel bizonyításánál használt jelölésekkel, ebben az esetben az X halmaz és egy páratlan komponens között legalább három él fut. Pontosan kettő ugyanis nem futhat (a páratlan komponens minden pontjából 3 él indul ki, ez összesen páratlan, a komponensen belül futó éleket kétszer kell levonni, így páratlan szám marad), ha viszont csak egy futna, akkor ezt az élet elhagyva szétesne a gráf, vagyis nem lenne 2-szeresen élösszefüggő (2.40. ábra). Jelöljük t-vel az összes olyan él számát, amely az X halmaz és valamelyik páratlan komponens között fut. Az előbbiek szerint így $t \geq 3c_p(G-X)$. Mivel G 3-reguláris, $t \leq 3|X|$. Ezeket összevetve kapjuk, hogy $c_p(G-X) \leq |X|$. Így pedig a Tutte–tételből következik az állítás. □



2.40. ábra.

2.9.15. Tétel (Berge). *Akkor és csak akkor létezik G-ben javító út egy M párosításra nézve, ha M nem maximális élszámú párosítás.*

BIZONYÍTÁS: Ha van javító út, akkor M nyilván nem maximális, hiszen a javító út mentén megcserélve az éleket, eggyel nagyobb párosításhoz jutunk. Tegyük most fel, hogy nem létezik javító út, de van egy N párosítás, hogy $|N| > |M|$. Feltehetjük, hogy $|N| = |M| + 1$. Tekintsük az $M \triangle N = (M \cup N) - (M \cap N)$ élhalmaz által meghatározott H részgráfot. Ez csak izolált pontokból, páros körökből és utakból állhat. Mivel azonban $|N| = |M| + 1$, $|E(H)|$ páratlan, így H-ban kell lenni páratlan útnak is. De $|N| > |M|$, így van olyan páratlan út is amelynek első és utolsó éle N-beli. Ez pedig épp egy javító út. □

2.9.16. Tétel (Berge). *Tetszőleges G gráfra a független élek maximális száma*

$$\nu(G) = \min_{X \subseteq V(G)} \frac{v(G) - (c_p(G - X) - |X|)}{2}.$$

Ennek a tételnek nem közöljük a bizonyítását, mivel elég nehéz.

2.9.4. Hálózati folyamok

2.9.17. Definíció. *Legyen G egy irányított gráf. Rendeljünk minden éléhez egy $c(e)$ nemnegatív valós számot, amit az él* ***kapacitásának*** *nevezünk. Jelöljünk ki továbbá két s,t pontot G-ben, melyeket* ***termelőnek*** *illetve* ***fogyasztónak*** *hívunk. Ekkor a $(G;s;t;c)$ négyest* ***hálózatnak*** *nevezzük.*

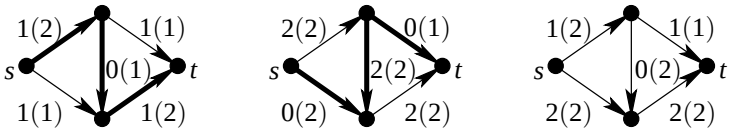
Szemléltetésképp feltehetjük, hogy a hálózattal egy vízvezetékrendszert ábrázolunk. A kapacitások a vezeték vastagságát jelentik, vagyis azt, hogy egységnyi idő alatt mennyi víz folyhat át azon a vezetékdarabon. A kérdés az, hogy egy adott hálózaton mennyi víz folyhat át s-ből t-be. Szoktak beszélni úthálózatokról is, ahol a kapacitás az utak áteresztőképessége, és árukat kell eljuttatni a termelőtől a fogyasztókhoz.

2.9.18. Definíció. *Legyen $f(e)$ az a vízmennyiség, ami az e élen folyik át. Ez az f függvény* ***megengedett függvény****, ha $f(e) \leq c(e)$ minden élre, és*

$$m(v) = \sum\{f(e) \mid e \text{ végpontja } v\} - \sum\{f(e) \mid e \text{ kezdőpontja } v\} = 0$$

minden $v \in V(G)$-re, kivéve az s és t pontokat. Egy megengedett függvényt ***folyamnak*** *hívunk. Könnyen belátható, hogy $m(t) = -m(s)$. Ezt a közös értéket a* ***folyam értékének*** *nevezzük és m_f-el jelöljük. Egy élet* ***telítettnek*** *hívunk egy folyamban, ha $f(e) = c(e)$, és* ***telítetlennek****, ha $f(e) < c(e)$.*

A feladat tehát a maximális értékű folyam meghatározása. Nézzünk néhány példát. A 2.41. ábrán az éleken szereplő első szám a folyam értéke azon az élen, míg a második (zárójelben) az él kapacitása.



2.41. ábra.

Nyilvánvaló, hogy ha van egy olyan irányított út s-ből t-be, amelynek minden élén a folyam értéke kisebb mint az él kapacitása, vagyis minden él telítetlen, akkor ezen út mentén a folyam értékét minden élen megnövelhetjük annyival, hogy az egyik él telített legyen. Ezt szemlélteti a 2.41. ábra első gráfja.
Ilyen javításra azonban nem mindig van lehetőség. Legyen a gráfban $s = v_0, v_1, \ldots, v_{k-1}, v_k = t$ egy út, aminek most nem kell feltétlenül az irányítás szerint haladnia. Növelhetjük a folyam értékét abban az esetben, ha minden $i = 0, 1, 2, \ldots, k-1$-re vagy $e_i = (v_i, v_{i+1})$ és $f(e_i) < c(e_i)$, vagy $e_i = (v_{i+1}, v_i)$ és $f(e_i) > 0$. Ekkor az első típusú éleken – mint a következő tételben látni fogjuk – növeljük a folyam értékét, míg a második típusúakon csökkentjük, így az össz folyamérték nő. Az ilyen utakat **javító útnak** hívjuk. Egy ilyet szemléltet a 2.41. ábra második gráfja, míg a harmadik gráfban nincs javító út.

2.9.19. Tétel. *Egy folyam értéke akkor és csak akkor maximális, ha nincs javító út s-ből t-be.*

BIZONYÍTÁS: Legyen P egy javító út. Ekkor P minden első típusú élére a $c(e_i) - f(e_i)$, a második típusúra pedig az $f(e_i)$ érték szigorúan pozitív. Legyen ezeknek a minimuma d. Az első típusú élekre növeljük $f(e_i)$-t d-vel, a második típusúaknál pedig csökkentsük $f(e_i)$-t d-vel. Ekkor a módosított folyam is megengedett marad, értéke viszont d-vel nőtt.
Tegyük most fel, hogy nincs javító út s-ből t-be. Lehetnek azonban olyan pontok a gráfban amelyek elérhetők s-ből javító úton. (Most nem követeljük meg, hogy a javító út t-be érjen, azaz, hogy $v_k = t$ legyen.) Legyen az ilyen pontok halmaza $X \subset V(G)$. Ekkor sem X, sem $V(G) - X$ nem üres, hiszen $s \in X, t \in V(G) - X$. Tekintsünk egy olyan e élet, amely egy X-beli x pontból egy nem X-beli y-ba mutat. Ekkor $f(e) = c(e)$, hiszen ellenkező esetben az s-ből x-be vezető javító út e-vel meghosszabbítva egy s-ből y-ba vezető javító utat szolgáltatna. Ugyanígy egy olyan

élre, amelyik egy nem X-beliből egy X-belibe mutat, teljesül, hogy $f(e) = 0$. Tehát az X és $V(G) - X$ között futó élek mind telítettek, és a visszafelé mutató éleket nem használjuk, tehát ezen a vágáson nem folyhat át több víz. Vagyis f maximális folyam. □

Ez a tétel más formában vált igazán híressé.

2.9.20. Definíció. *Legyen $s \in X \subseteq V(G) - \{t\}$, így nyilvánvaló, hogy sem X, sem $V(G) - X$ nem üres halmaz. Azoknak az éleknek a C halmazát, amelyeknek egyik végpontja X-beli, másik $V(G) - X$-beli, a hálózati folyam egy (s,t)-**vágásának** nevezzük. A **vágás értéke**, $c(C)$, azon éleken levő kapacitások összege, amelyek egy X-beli pontból egy $V(G) - X$-beli pontba mutatnak. Ezeket előremutató éleknek nevezzük. Tehát a vágás értékében nem játszanak szerepet a visszafelé mutató élek, vagyis azok, amelyek egy X-beli pontba mutatnak.*

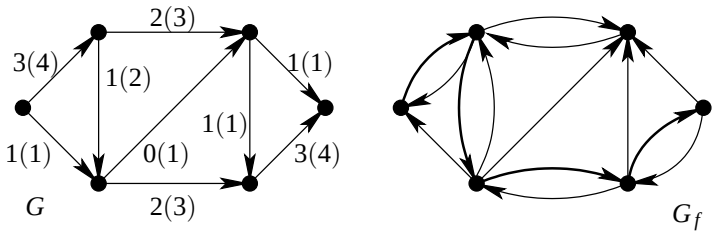
Megjegyezzük, hogy ez a definíció nem azonos a a 2.1. és a 2.6. szakaszokban található vágás definícióval.
Így az előző tétel egyszerű következménye a következő, ebben a témakörben leggyakrabban felhasznált tétel.

2.9.21. Tétel (Ford–Fulkerson). *A maximális folyam értéke egyenlő a minimális vágás értékével, azaz*

$$\max\{m_f \mid f \text{ egy folyam } s\text{-ből } t\text{-be}\} = \min\{c(C) \mid C \text{ vágás}\}.$$

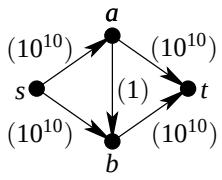
BIZONYÍTÁS: A maximális folyam nyilván nem lehet nagyobb a minimális vágásnál, hiszen ha minden előremutató él telített, a visszafelé mutatókon pedig 0 a folyam értéke, akkor ezen a vágáson nem folyhat át több víz. Az előző tételben pedig láttuk, hogy ha létezik egy f maximális folyam, akkor van ilyen értékű vágás. Azt, hogy maximális folyam mindig létezik, a következőkben bemutatott algoritmus segítségével bizonyíthatjuk. □

E tétel segítségével könnyen bebizonyítható egy adott folyamról (amit valahogy megsejtettünk), hogy az maximális. Ha megsejtünk egy ugyanilyen értékű vágást, akkor a Ford–Fulkerson tétel biztosítja, hogy a folyam értéke maximális. Ha viszont nem tudjuk megsejteni a maximális folyamot, akkor rendelkezésre áll egy algoritmus. Ez lényegében abból áll, hogy a kiindulási folyamra vonatkozólag (ha ilyen nem volt, akkor az azonosan 0 folyam használható) keresünk egy javító utat, és a már ismert módszer szerint e mentén növeljük a folyam értékét. Hogyan tudunk, ilyen javító utat keresni, illetve hogyan jövünk rá, hogyha nincs javító út?
Az irányított G gráfon adott f folyamhoz definiálunk egy G_f irányított gráfot: Legyen $V(G_f) = V(G)$ és G_f-ben fusson egy irányított él x-ből y-ba, ha vagy (1) $(x,y) \in E(G)$ és $f(x,y) < c(x,y)$, vagy (2) $(y,x) \in E(G)$ és $f(y,x) > 0$. (2.42. ábra). Könnyen látható, hogy ha G_f-ben van egy irányított út s-ből t-be, akkor az ennek az útnak megfelelő élek G-ben épp egy javító utat adnak az f folyamra nézve. Ha pedig van javító út G-ben, akkor lesz irányított út s-ből t-be G_f-ben.



2.42. ábra.

Így tehát elegendő megnézni, hogy az így kapott G_f gráfban van-e út s-ből t-be. Ezt viszont a BFS algoritmussal könnyen eldönthetjük. Ha van ilyen út, akkor találtunk egy javító utat G-ben, ha nincs, akkor viszont nincs javító út. Ekkor viszont a fenti tétel miatt tudjuk, hogy a folyam maximális.



2.43. ábra.

Nem mindegy azonban, hogy melyik javító utat vesszük. Például a 2.43. ábrán látható hálózati folyamon felváltva az s,a,b,t és s,b,a,t utakat vesszük, akkor minden lépésben csak 1-gyel tudjuk növelni a folyam értékét, és így a maximális folyam értékéhez csak $2 \cdot 10^{10}$ lépésben jutunk el, míg ha az első lépésben az s,a,t javító utat vesszük, akkor 2 lépésben jutunk a maximumhoz. Sőt, konstruálható olyan példa is, ahol a javító utak ügyetlen sorrendben való alkalmazása esetén sohasem ér véget az algoritmus.

2.9.22. Tétel (Edmonds-Karp). *Ha mindig a legrövidebb javító utat vesszük, akkor a maximális folyam meghatározásához szükséges lépések száma felülről becsülhető a pontok számának polinomjával.*

Ezt a tételt itt nem bizonyítjuk be. Ha tehát az előbbi algoritmusban a G_f segédgráfban szélességi kereséssel a legrövidebb utat határozzuk meg s-ből t-be, akkor polinomiális idejű algoritmust kapunk.
Megemlítünk még egy fontos következményt.

2.9.23. Tétel. *Ha a kapacitások egész számok, akkor a maximális folyam értéke egész szám, és ez olyan f függvénnyel is megvalósítható, mely minden élen egész értéket vesz fel.*

BIZONYÍTÁS: Az állítás nyilvánvaló, hiszen a kiindulási, azonosan 0 folyam rendelkezik a kívánt tulajdonsággal, majd az algoritmus során minden lépésben a folyamértékek minden élen csak egész számmal változhattak. □

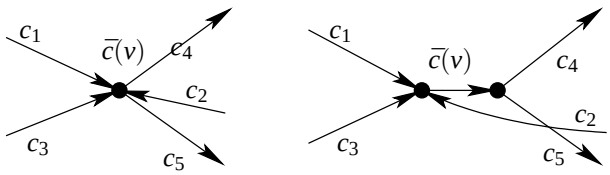
2.9.5. A folyamprobléma általánosításai

Az eredeti problémának több általánosítása is van. Például legyen a hálózatban több termelő $s_1, s_2, \ldots, s_k$ és több fogyasztó $t_1, t_2, \ldots, t_l$. A feladat az összes termelőtől az összes fogyasztóig eljutó termékmennyiség maximalizálása. Vegyünk fel két új s', t' pontot, és kössük össze s'-t $s_1, \ldots, s_k$-val, $t_1, \ldots, t_l$-t pedig t'-vel, az új élek mindegyikének kapacitása legyen ∞. Ha ebben a hagyományos hálózatban meghatározzuk a maximális folyamot, akkor az eredeti éleken szereplő folyamértékek pontosan a keresett értékek.

Most úgy módosítjuk a feladatot, hogy nem csak az élekhez, hanem a pontokhoz is rendelünk $\bar{c}(v)$ kapacitásokat, és megköveteljük, hogy a ponton csak ennyi víz folyhat át, azaz minden v-re

$$\sum_{\{u|(u,v)\in E\}} f(u,v) \leq \bar{c}(v).$$

Ezt a problémát is úgy oldjuk meg, hogy konstruálunk hozzá egy hagyományos hálózatot. Minden v pontot helyettesítsünk két v', v'' ponttal. Ha egy él az u pontból a v pontba mutatott, akkor helyette vegyünk fel egy u''-ből v'-be mutató élet a hozzá tartozó kapacitással együtt. Ezenkívül pedig minden v'-ből mutasson egy él v''-be és ennek kapacitása $\bar{c}(v)$ legyen (lásd a 2.44. ábrát).



2.44. ábra.

Ezek után már könnyű megtalálni a maximális folyamot. Még könnyebb a visszavezetés abban az esetben, amikor megengedünk irányítatlan éleket. Ekkor az ilyen c kapacitású $\{u,v\}$ él helyett felveszünk két c kapacitású (u,v) és (v,u) irányított élet. Már említettük, hogy ha a kapacitások egész számok, akkor van olyan maximális folyam, melyben minden élen a folyam értéke egész. Így nyilvánvaló, hogy ha a kapacitás minden élen 1 vagy 0, akkor van olyan maximális folyam, melynek minden élén a folyam értéke vagy 1 vagy 0. Ha elhagyjuk ez utóbbi éleket, akkor diszjunkt utakat kapunk s-ből t-be. (Esetleg maradhatnak további irányított körök is.)

2.9.6. Menger tételei

Ebben a szakaszban a hálózati folyamok segítségével irányított és irányítatlan gráfokról bizonyítunk be néhány tételt.

2.9.24. Tétel (Menger). *Ha G egy irányított gráf, $s,t \in V(G)$, akkor az s-ből t-be vezető páronként élidegen irányított utak maximális száma megegyezik az összes irányított $s-t$ utat lefogó élek minimális számával.*

BIZONYÍTÁS: Ha létezik G-ben k darab ilyen irányított $s-t$ út, akkor az $s-t$ utakat lefogó élek száma nyilvánvalóan legalább k. Tehát $\max\{\} \leq \min\{\}$. Most lássuk a fordított egyenlőtlenséget. Tegyük fel, hogy az $s-t$ utakat lefogó élek minimális száma k. Legyen minden él kapacitása 1. Az így kapott hálózatban a minimális vágás értéke tehát legalább k. Ekkor a Ford–Fulkerson tétel miatt a maximális folyam is legalább k értékű. Azt is láttuk már, hogy van olyan maximális folyam, melyben minden élen a folyamérték 0 vagy 1. Lássuk be, hogy G-ben van k élidegen irányított $s-t$ út. Egy ilyen út mindenképpen van, hiszen különben nem lehetne k a folyam értéke. Az ebben az útban szereplő élek kapacitását változtassuk 0-ra. Így a folyam értéke legalább $k-1$ lesz. Ekkor viszont ismét kell lennie $s-t$ útnak, és ennek nyilván nincs közös éle az előbbi úttal. A gondolatmenetet folytatva k élidegen irányított $s-t$ utat kapunk. □

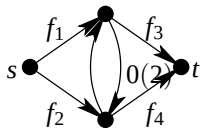
Ennek a tételnek több változata is van.

2.9.25. Tétel (Menger). *Ha G egy irányított gráf, $s,t \in V(G)$ két nem szomszédos pont, akkor az s-ből t-be vezető, végpontoktól eltekintve pontidegen irányított utak maximális száma megegyezik az összes irányított $s-t$ utat s és t felhasználása nélkül lefogó pontok minimális számával.*

BIZONYÍTÁS: Készítsünk egy új G' gráfot. Minden pontot húzzunk szét két ponttá, a 2.44. ábrán látható módon. Ha a G gráfban egy minimális ponthalmaz lefogja az irányított $s-t$ utakat, akkor a lefogó pontoknak megfelelő (v',v'') élek G'-ben lefogják az irányított $s-t$ utakat. Kevesebb él nem lehet elég a lefogáshoz, mert ha a lefogó élek között lennének (a'',b') típusú élek, akkor ezeket helyettesíthetjük (b',b'')-vel, ha $b' \neq t$, illetve (a',a'')-vel, ha $b' = t$. Így pedig G-ben egy kisebb lefogó ponthalmazt nyernénk. Vagyis a G-beli lefogó pontok és a G'-beli lefogó élek minimális száma egyenlő. Az is könnyen látható, hogy G-beli pontdiszjunkt utaknak G'-ben éldiszjunkt utak felelnek meg, és fordítva G'-beli élidegen utaknak G-ben pontidegen utak felelnek meg. Így az előző tétel bizonyítja állításunkat. □

2.9.26. Tétel (Menger). *Ha G egy irányítatlan gráf, $s,t \in V(G)$, akkor az s-ből t-be vezető élidegen irányítatlan utak maximális száma megegyezik az összes irányítatlan $s-t$ utat lefogó élek minimális számával.*

BIZONYÍTÁS: Vezessük vissza a problémát a hasonló, irányított gráfos problémára. Készítsünk egy G' gráfot úgy, hogy minden élet két, egy oda és egy vissza mutató irányított éllel helyettesítünk. Az már visszavezetés nélkül is világosan látszik, hogy k darab diszjunkt utat nem lehet lefogni k-nál kevesebb éllel, vagyis a maximum nem nagyobb a minimumnál. Most tegyük fel, hogy G-ben k a diszjunkt utakat lefogó élek minimális száma. Ha G'-ben ennél kevesebb él lefogná az irányított utakat, akkor az ezeknek az éleknek G-ben megfelelő élek lefognák az utakat G-ben, tehát ellentmondásra jutunk.
Világos, hogy egy G-beli $s-t$ útnak G'-ben megfelel egy irányított $s-t$ út. Azonban két élidegen G'-beli irányított $s-t$ útnak G-ben megfelelő utak nem feltétlenül élidegenek. Előfordulhat, hogy az egyik irányított út (2.45. ábra) tartalmazza az f_1, e_2, f_4 irányított utat, a másik pedig az f_2, e_1, f_3 utat, ahol az f_i szimbólumok nem csak irányított éleket, hanem irányított rész-utakat is jelölhetnek. Ezek ugyan élidegenek, de a G-ben nekik megfelelő utaknak van közös éle. Ezt a két diszjunkt utat helyettesítsük az f_1, f_3 és f_2, f_4 utakkal. Az ezeknek G-ben megfelelő utak már diszjunktak. Evvel a helyettesítéssel csökken az utakban szereplő élek száma, tehát véges lépés után már nem fog ilyen helyzet előállni. Ebből tehát látszik, hogy a diszjunkt utak maximális száma G-ben és G'-ben megegyezik.



2.45. ábra.

Így sikerült visszavezetnünk a feladatot a korábbi problémára, hiszen G'-ben már bizonyítottuk, hogy a minimum nem nagyobb a maximumnál, G-ben pedig a lefogó élek száma nem lehet nagyobb, mint G'-ben. □

2.9.27. Tétel (Menger). *Ha G egy irányítatlan gráf, $s,t \in V(G)$ két nem szomszédos pont, akkor az s-ből t-be vezető pontidegen irányítatlan utak maximális száma megegyezik az összes irányítatlan $s-t$ utat s és t felhasználása nélkül lefogó pontok minimális számával.*

BIZONYÍTÁS: Ezt a tételt könnyen visszavezethetjük az előző tételre, ha az irányítatlan élek helyett mindkét irányban húzunk egy irányított élet. □

2.9.7. Többszörös összefüggőség

2.9.28. Definíció. *Egy G gráfot k-**szorosan összefüggőnek** nevezünk, ha legalább $k+1$ pontja van, és akárhogy hagyunk el belőle k-nál kevesebb pontot, a maradék gráf összefüggő marad. A gráf k-**szorosan élösszefüggő**, ha akárhogy hagyunk el belőle k-nál kevesebb élet, összefüggő gráfot kapunk.*

Azonnal következik a definícióból, hogy mind az egyszeres összefüggőség, mind az egyszeres élösszefüggőség a korábban definiált összefüggőséggel egyezik meg. Azt is láthatjuk, hogy $k \geq 2$ esetén a k-szoros összefüggőség „erősebb” a k-szoros élösszefüggőségnél. Például ha két p pontú teljes gráfot veszünk, amelyeknek egyik pontja közös, az így kapott gráf csak 1-szeresen összefüggő, de $(p-1)$-szeresen élösszefüggő.

2.9.29. Tétel. *A G gráf akkor és csak akkor k-szorosan összefüggő, ha legalább $k+1$ pontja van, és bármely két pontja között létezik k pontidegen út. Hasonlóan G akkor és csak akkor k-szorosan élösszefüggő, ha bármely két pontja között létezik k élidegen út.*

BIZONYÍTÁS: Először a második részt bizonyítjuk. Ha G k-szorosan élösszefüggő, akkor az $u-v$ utakat lefogó élek minimális száma nyilván legalább k. Így Menger idevágó tétele szerint az élidegen $u-v$ utak maximális száma legalább k. Ennek a résznek a megfordítása is következik a Menger tételből.
Ha G k-szorosan összefüggő, akkor bármely két $u,v \in V(G)$ pontot választva legalább k darab, u-tól és v-től különböző pontra van szükség ahhoz, hogy lefogjuk az összes u és v közötti utat (az esetleges $\{u,v\}$ éltől eltekintve). Így a 2.9.27. tétel szerint létezik u és v között k pontidegen út.
Ha G bármely két pontja között létezik k pontidegen út, akkor nyilván nem lehet ezeket k-nál kevesebb ponttal lefogni, tehát a k-szoros összefüggőség következik. □

Egy egyszerű következmény, amely szintén Mengertől származik.

2.9.30. Tétel (Menger). *A legalább 3 pontú G gráf akkor és csak akkor 2-szeresen összefüggő, ha tetszőleges két pontján át vezet kör. Igaz az is, hogy akkor és csak akkor 2-szeresen összefüggő, ha bármely két élén át vezet kör.*

BIZONYÍTÁS: Az első állítás triviális, hiszen két pontidegen $u-v$ út együtt egy kört ad, amely átmegy u-n és v-n.
A második állítás pedig az elsőből következik. Lássuk be, hogy ha G 2-szeresen összefüggő, akkor az e, f éleken keresztül van kör. Vegyünk fel két pontot úgy, hogy ezekkel osszuk két részre az e illetve az f élet. Az így kapott gráf is 2-szeresen összefüggő. Az első állítás szerint ezen a két ponton át megy kör, és ez a kör az eredeti gráfban átmegy e-n és f-en. A megfordítás pedig nyilvánvaló. □

Ennek a tételnek egyik irányát általánosította Dirac.

2.9.31. Tétel (Dirac). *Ha $k \geq 2$ és a G gráf k-szorosan összefüggő, akkor bármely $x_1, x_2, \ldots, x_k$ pontján át vezet kör.*

BIZONYÍTÁS: k-ra való teljes indukcióval bizonyítunk. $k = 2$-re éppen ezt mondja ki Menger előbbi tétele. Tegyük fel most, hogy a C kör már tartalmazza az $x_1, x_2, \ldots, x_{k-1}$ pontokat (feltehető, hogy ebben a sorrendben), de nem megy át x_k-n.

Vegyünk fel egy z pontot a gráfon kívül és kössük össze C minden pontjával. A keletkező új gráfban z és x_k között a végpontoktól eltekintve pontidegen utak maximális száma legyen t. Jelöljük $y_1, y_2, \ldots, y_t$-vel azokat a pontokat, amelyekben az x_k-ból induló t darab pontidegen út először találkozik a C körrel.
Ha $t \geq k$, akkor a skatulya-elv szerint van olyan i, hogy x_i és x_{i+1} közé a körön két különböző y – mondjuk y_1 és y_2 – is esik. Ekkor az $x_1, \ldots, x_i, \ldots, y_1, \ldots, x_k, \ldots, y_2, \ldots, x_{i+1}, \ldots, x_{k-1}, \ldots, x_1$ kör tartalmazza a kijelölt k darab pontot.
Ha $t < k$, akkor alkalmas t darab pont elhagyásával szétesik az új gráf, x_k és z különböző komponensbe kerül. Mivel az eredeti gráf k-szorosan összefüggő volt, ez csak úgy lehetséges, ha z egyedül alkot egy komponenst. Ez viszont csak úgy lehet, ha a kör minden pontját elhagytuk. Ekkor azonban $t = k-1$ és $V(C) = \{x_1, x_2, \ldots, x_{k-1}\}$. Így bármely két szomszédos x_i közötti él kicserélhető egy x_k-n keresztül haladó úttal. □

2.10. A mélységi keresés alkalmazásai

2.10.1. Alapkörrendszer keresése

A 2.4.3. pontban látottak szerint a villamosságtani alkalmazások során fontos, hogy gyorsan elő tudjuk állítani az összefüggő G gráf F feszítőfájához tartozó alapkörrendszert, vagyis minden $e, f, g, \ldots \in E - F$ élhez az

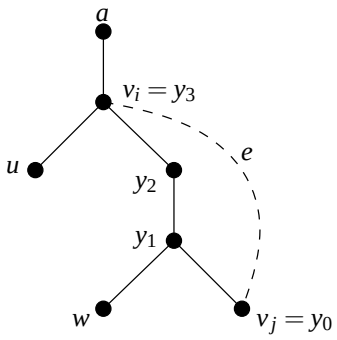
$$F \cup \{e\},\ F \cup \{f\},\ F \cup \{g\}, \ldots$$

részgráfok által tartalmazott egyértelmű $C_e, C_f, C_g, \ldots$ kört.
A 2.7.2. szakaszban található mélységi keresés segítségével ez különösen egyszerűen megoldható. Összefüggő gráf esetén az algoritmus meghatározott egy fát (t.i. minden $y \neq a$ pontra adódik egy $\{q(y), y\}$ él és ezek együtt egy F fát alkotnak). Legyen $e = \{v_i, v_j\}$ egy olyan él, mely nem tartozik ehhez a fához. Hogy kaphatjuk meg a hozzá tartozó C_e kört?
Emlékezzünk vissza, hogy i azt mutatja, hányadik pont volt v_i a mélységi bejárás során. Ha ezek után pl. $i < j$ (amit az általánosság korlátozása nélkül feltehetünk, hisz e irányítatlan él), akkor az

$$y_0 = v_j, \quad y_1 = q(y_0), \quad y_2 = q(y_1), \quad y_3 = q(y_2), \ldots \qquad (*)$$

sorozat előbb-utóbb eljut a v_i-hez (ld. 2.46. ábra). Az nem fordulhat elő, hogy az e él két végpontja egymáshoz képest olyan helyzetben lenne, mint a 2.46. ábrán az u és w pontok, hisz u-ból épp azért kellett v_i-be visszalépnünk, mert u-ból sehova nem vezetett él.
Így az alapkörrendszer meghatározásához egyszerűen az alábbi kiegészítés szükséges (a STOP helyére):

STOP: minden $e \notin F$-re $C_e = (y_0, y_1, \ldots, y_k, y_0)$, ld. $(*)$

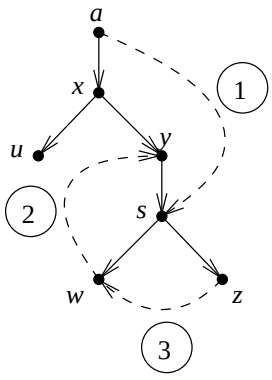


2.46. ábra.

Az eljárás egyszerűségét biztosító fenti észrevételt újra kimondjuk. Előtte vezessük be a következő szóhasználatot: Ha $u = q(w)$, akkor az u pontot w **apjának** vagy a w pontot u **fiának** nevezzük: általánosabban a $(*)$ sorozatban $i < j$ esetén y_j az y_i **őse**, ill. y_i az y_j **leszármazottja**. Ezután megállapíthatjuk, hogy

2.10.1. Lemma. *Irányítatlan összefüggő gráf mélységi bejárása esetén tetszőleges él két végpontja közül az egyik, amelyiknek sorszáma nagyobb) a másik leszármazottja.*

2.10.2. Irányított körök felismerése, emeletekre bontás



2.47. ábra.

Irányított gráfok esetén a a 2.10.1. Lemma helyett egy bonyolultabb állítás mondható csak ki. Induljunk ki egy tetszőleges a pontból és végezzünk mélységi bejárást. Ha nem jutottunk el így minden ponthoz, akkor válasszunk ki egy tetszőleges még

be nem járt pontot és ismét végezzünk mélységi bejárást. Ezt az eljárást addig folytassuk, amíg minden pontot bejárunk. Az így kapott fák unióját nevezzük DFS erdőnek.
A 2.47. ábrán jól látható módon három csoportba oszthatjuk (a konkrét mélységi bejárás szempontjából) egy irányított gráf éleit. A (p,p') irányított él lehet

(1) előre–él, ha p őse p'-nak (ekkor persze p sorszáma kisebb mint p' sorszáma),

(2) vissza–él, ha p' őse p-nek (ekkor p' sorszáma kisebb), vagy

(3) kereszt–él, ha p és p' közül egyik sem őse a másiknak.

Például a 2.47. ábra gráfjában az (a,s) él előre-él, a (w,y) él vissza–él, a (z,w) él pedig kereszt–él. Világos, hogy a mélységi erdőhöz tartozó élek mind előre–élek, a gráf többi éle bármilyen lehet. Az is könnyen látható, hogy egy (p,p') kereszt–élre p' sorszámának kell kisebbnek lennie. Ha ugyanis lenne a gráfban például egy (u,y) él, akkor u-ból nem léptünk volna vissza x-be az y meglátogatása nélkül.
Az élek fenti osztályozásának jelentősége rögtön kitűnik az alábbi észrevételből:

2.10.2. Lemma. *Egy irányított gráfban akkor és csak akkor van irányított kör, ha a mélységi bejárás során találunk vissza–élt.*

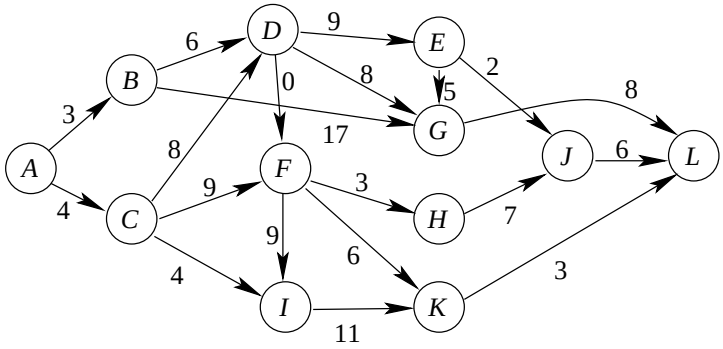
A feltétel elégségessége persze triviális, a szükségessége a szakasz végén következő algoritmusból fog adódni.
Nevezzük **emeletekre bontásnak** az irányított gráf V ponthalmazának azt a $V = V_1 \cup V_2 \cup \cdots \cup V_m$ partícióját (ha ilyen létezik), melyben bármely (x,y) irányított élre, ha $x \in V_i$ és $y \in V_j$, akkor $i < j$ teljesül és nincs olyan él ami két V_i-beli pont között fut. Világos, hogy ilyenkor V_1 elemei **források** (vagyis be–fokuk zérus) és V_m elemei **nyelők** (vagyis ki-fokuk zérus), de a források és nyelők létezése még nem garantálja az emeletekre bonthatóságot.

2.10.3. Lemma. *Egy irányított gráfban akkor és csak akkor van irányított kör, ha ponthalmaza nem bontható emeletekre.*

A feltétel szükségessége triviális. Elégségességét (a 2.10.2. Lemma feltételének szükségességével együtt) azzal látjuk be, hogy megadunk egy olyan algoritmust, mely tetszőleges irányított gráfra vagy emeletekre bontja a ponthalmazát, vagy talál benne egy irányított kört.
Ez az algoritmus azonban a mélységi keresés triviális módosításával megkapható: Amikor v_k szomszédjait tekintjük át, észrevesszük, ha van köztük olyan v_l, hogy a (v_k,v_l) él vissza–él (hisz akkor v_l-t már korábban bejártuk és $l < k$ teljesül), akkor megállunk, és a a 2.10.2 Lemma triviális iránya alapján találtunk egy irányított kört. Ha viszont v_k szomszédjai között nem volt ilyen pont, akkor előbb–utóbb v_k-ról visszalépünk. Az a pont, amelyikből legelőször visszalépünk, alkossa egyedül a V_m halmazt, az a pont, amelyikből másodszor lépünk vissza, alkossa az ugyancsak egyelemű V_{m-1} halmazt stb. Ha a DFS erdő több fából áll, akkor ezt folytassuk a következő fával, stb. Így persze $k = v$ és minden ponthalmaz egyelemű lesz. Ez azonban csak egy speciális módja az emeletekre bontásnak, legtöbb esetben sokféleképpen lehet emeletekre bontani egy gráfot.

2.10.3. A kritikus út módszere (PERT-módszer)

Az előző szakaszban látott „emeletekre bontás” fontos alkalmazása az úgynevezett PERT–módszer. Az elnevezés az angol „Program Evaluation and Review Technique” rövidítéséből származik.
Tegyük fel, hogy egy összetett feladatot több alvállalkozóval kell elvégeztetni. Az egyes részfeladatok nem végezhetőek el egymástól függetlenül: pl. egy házépítés során a kőművesmunkák nyilván megelőzik a festési munkákat. A helyzetet egy G gráffal szemléltethetjük, melynek pontjai a részfeladatok, és egy l hosszúságú (x,y) irányított él azt fejezi ki, hogy az y részfeladat nem kezdhető el korábban, mint az x kezdése után l idővel. $l=0$ is lehetséges: x és y ilyenkor kezdhető egyszerre, vagy y később.

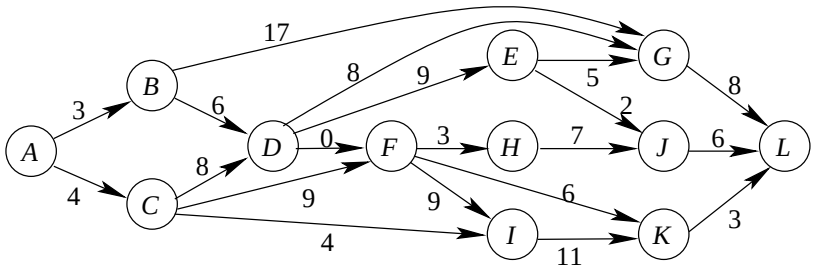


2.48. ábra.

A feladat jellegénél fogva egy ilyen gráf (ld. pl. a 2.48. ábrát) nem tartalmazhat irányított kört. Az egyszerűség kedvéért feltesszük, hogy G egyetlen forrást és egyetlen nyelőt (az ábrán A, ill. L) tartalmaz. A gráf a 2.10.2. lemma értelmében emeletekre bontható, de most ezt nem az előző szakasz végén leírt algoritmussal végezzük. Először a nyelőt helyezzük a jobbszélső halmazba, az ennek elhagyása után keletkező (és szintén irányított kört nem tartalmazó) gráf nyelőit a jobbról második halmazba és így tovább, ld. a 2.49. ábrát).
Ezek után balról jobbra haladva, meghatározhatjuk minden tevékenység elkezdésének lehetséges legkorábbi időpontját. Az eljárást a a 2.50. ábra szemlélteti: A bal szélső tevékenység azonnal (0. időpontban) megkezdhető, később egy y tevékenységhez tekintsük át az összes olyan $x_1,x_2,\ldots$ tevékenységet, melyre $(x_i,y)\in E(G)$, és ha ezek legkorábban a $t_1,t_2,\ldots$ időpontban kezdhetőek el, akkor y elkezdésére legkorábban a

$$\max(t_1+l(x_1,y),\ t_2+l(x_2,y),\ldots)$$

időpontban kerülhet sor.
Végezetül érdemes megjelölni L-ből visszafelé azokat az (x_i,y) éleket, melyeken a fenti maximumok felvétetnek. (A a 2.50. ábrán aláhúzással jelöltük meg a maxi-



2.49. ábra.

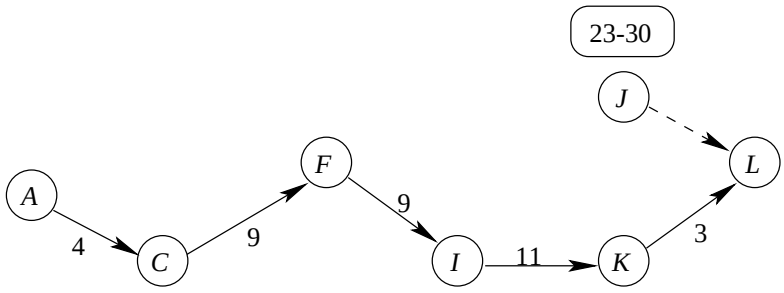
$A \to \underline{0}$
$B \to \underline{3}, C \to \underline{4}$
$D \to \max(3+6, \underline{4+8}) = 12$
$F \to \max(\underline{9+4}, 12+0) = 13$
$E \to \underline{12+9} = 21$, $H \to \underline{13+3} = 16$, $I \to \max(\underline{9+13}, 4+4) = 22$
$G \to \max(17+3, 8+12, \underline{5+21}) = 26$, $J \to \max(\underline{21+2}, \underline{16+7}) = 23$ $K \to \max(13+6, \underline{\underline{22+11}}) = 33$
$L \to \max(26+8, 23+6, \underline{33+3}) = \underline{\underline{36}}$

2.50. ábra.

mális összegeket.) A megjelölt élek a G gráf kritikus élei, az ezek által meghatározott részgráf mindig tartalmaz legalább egy irányított utat a forrásból a nyelőbe. (A 2.51. ábrán pontosan egy ilyen út van, de általában több is lehet.) Ezeket az utakat kritikus útnak nevezzük, nyilván ezek a leghosszabb utak a forrásból a nyelőbe.

Az ilyen kritikus utakon lévő pontoknak megfelelő részfeladatok bármelyikének késedelmes elvégzése az egész összetett feladat befejezését késleltetné (innét a kritikus út elnevezés). Ha viszont egy pont nincs kritikus úton (pl. a J. pont a 2.51. ábrán), akkor a megfelelő feladat késedelmes elvégzése bizonyos határon belül még elfogadható. Pl. a J feladat legkorábban a 23. időegységben kezdhető el, és legfeljebb 7 egységnyi késedelem még nem veszélyezteti a teljes munka eredeti terv szerint való befejezését. Ugyanis az L kezdésének időpontja (36) előtt legkésőbb 6 egységgel kell J-t elkezdeni.

Jól látható, hogy a részfeladatok „beprogramozásához” (vagyis a kezdési időpontok meghatározásához) szükséges lépések száma a G pontjainak fokszámösszegével (vagyis e-vel) arányos. Végül megjegyezzük, hogy a leghosszabb út meghatározása – ellentétben a legrövidebb útéval – általában nem végezhető el polinom időben (ld. a köv. fejezetet). Ebben a speciális esetben azért tudtunk gyors algoritmust adni, mert G-ben nincsenek irányított körök.



2.51. ábra.

2.10.4. További alkalmazások

A mélységi keresés segítségével számos további nevezetes gráfelméleti feladatot lehet polinom–időben, sőt, $(e+v)$-vel arányos lépésszámban megoldani. Ilyeneket tartalmaz a 2.3. Táblázat 2. oszlopa. Az utolsó 4 feladat azonban az eddigieknél bonyolultabb, ezeket nem részletezzük.

2.3. táblázat. Polinomrendben megoldható nevezetes gráfelméleti feladatok

A szélességi keresés (BFS) alkalmazásával	A mélységi keresés (DFS) alkalmazásával
Összefüggő-e egy gráf?	Összefüggő-e egy gráf?
Fa konstruálása	Fa konstruálása
Legrövidebb út és kör keresése	Alapkörrendszer előállítása
Legrövidebb irányított út ill. kör keresése	Tartalmaz-e egy irányított gráf irányított kört?
Maximális párosítás gráfban	Erősen összefüggő-e egy irányított gráf?
Maximális folyam egytermékes hálózatban	Gráf erősen összefüggővé irányítása
	2–összefüggőség és 2–él–összefüggőség ellenőrzése
	Síkbarajzolhatóság ellenőrzése

2.11. Gráfok színezése

2.11.1. Alsó és felső korlátok

2.11.1. Definíció. *Egy G hurokmentes gráf **k színnel kiszínezhető**, hogyha minden csúcsot ki lehet színezni k szín felhasználásával úgy, hogy bármely két szomszédos csúcs színe különböző legyen. G **kromatikus száma** $\chi(G) = k$, ha G k színnel kiszínezhető, de $k-1$ színnel nem. Egy ilyen színezésnél az azonos színt kapott pontok halmazát **színosztálynak** nevezzük.*

Ha hurokél csatlakozna egy ponthoz, akkor azt a pontot nem lehetne kiszínezni. Másrészt a színezés szempontjából a többszörös élek nem játszanak szerepet, ezért ebben a szakaszban csak egyszerű gráfokkal foglalkozunk. Nyilvánvaló, hogy $\chi(G) \leq v(G)$, hiszen ha minden csúcsot különböző színűre színezünk, az jó színezés. K_n-et ennél kevesebbel nem is lehet kiszínezni, tehát $\chi(K_n) = n$.

2.11.2. Tétel. *Egy legalább egy élet tartalmazó G gráf akkor és csak akkor páros, ha $\chi(G) = 2$.*

BIZONYÍTÁS: Ha a gráf páros, akkor az egyik oldalon levő pontokat pirossal, a másik oldalon levőket kékkel színezve 2 színnel színeztük a gráfot. Ha a gráfnak van legalább egy éle, akkor ennek két végpontját nem színezhetjük ugyanolyan színűre, így $\chi(G) = 2$.
Ha $\chi(G) = 2$, akkor a két színosztály épp a páros gráf definíciójában szereplő felbontásnak megfelelő két halmaz lesz (ld. 2.9.1. definíció). □

2.11.3. Definíció. *G egy teljes részgráfját* **klikknek** *nevezzük. A G-ben található maximális méretű klikk méretét, azaz pontszámát $\omega(G)$-vel jelöljük és a gráf **klikkszámának** nevezzük.*

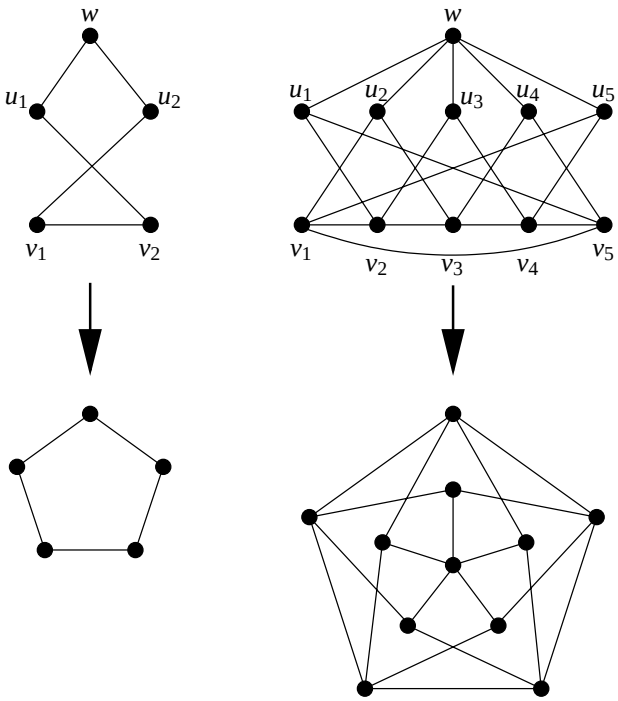
Ha van a gráfban egy klikk, akkor ennek semelyik két pontja nem lehet azonos színű:

2.11.4. Tétel. *Minden G gráfra $\chi(G) \geq \omega(G)$.* □

Ez az alsó korlát a kromatikus számra éles például olyankor, ha a gráf egy teljes gráf. Másrészt van olyan gráf is, amire nagyon rossz ez a korlát.

2.11.5. Tétel (Mycielski konstrukciója). *Minden $k \geq 2$ egész számra van olyan G_k gráf, hogy $\omega(G_k) = 2$ és $\chi(G_k) = k$.*

BIZONYÍTÁS: G_2-nek nyilván megfelel a 2 pontot és egy élet tartalmazó gráf. Tegyük fel, hogy már megkonstruáltuk a fenti tulajdonságokkal rendelkező G_k-t. Ebből konstruáljuk meg G_{k+1}-et. Jelöljük G_k pontjait $v_1, v_2, \ldots, v_n$-nel. Vegyünk fel $n+1$ darab új pontot, $u_1, u_2, \ldots, u_n$-t és w-t, valamint új éleket a következőképp.



2.52. ábra.

Minden u_i-t kössük össze v_i minden G_k-beli szomszédjával, de magával v_i-vel ne. Végül w-t kössük össze minden u_i-val (de a $v_1, \ldots, v_n$ pontokkal ne). Belátjuk, hogy az így kapott G_{k+1} gráf kielégíti a feltételeket. A 2.52. ábrán látható G_3, ami egy 5 hosszú kör és G_4, amit Grötzsch gráfnak is neveznek.

Először lássuk be, hogy ha G_k-ban nem volt háromszög, akkor G_{k+1}-ben sincs, azaz $\omega(G_{k+1}) = 2$. Tegyük fel, hogy mégis van háromszög G_{k+1}-ben. Ennek nyilván nem lehet mindhárom csúcsa G_k-ban, hiszen ekkor volna háromszög G_k-ban. Ha w a háromszög egyik csúcsa, akkor a másik kettő csak u_i és u_j lehet, ezek viszont nem szomszédosak. Ha u_i a háromszög egyik csúcsa, akkor már csak az az eset maradt, hogy a másik két csúcs v_x és v_y. Mivel azonban u_i szomszédai megegyeznek v_i szomszédaival, ekkor nem csak u_i, v_x és v_y, hanem v_i, v_x és v_y is egy háromszöget alkotna G_k-ban, ami ellentmond a feltevésünknek.

Nyilvánvaló, hogy $\chi(G_{k+1}) \leq k+1$. Színezzünk ki ugyanis minden v_i pontot ugyanolyan színnel, mint G_k egy k színnel való kiszínezésében, majd minden u_i-t színezzünk ugyanolyanra, mint v_i-t, végül w-t színezzük ki a $k+1$-edik színnel. Így G_{k+1}-et jól színeztük $k+1$ színnel.

Tegyük fel indirekt, hogy $\chi(G_{k+1}) = k$. (Ennél kisebb nem lehet, hisz G_{k+1} részgráfként tartalmazza a k-kromatikus G_k gráfot.) Jelöljük az x pont színét $c(x)$-szel, a

színeket pedig $1,2,\ldots,k$-val. Azt is feltehetjük, hogy $c(w)=k$. Mivel w minden u_i-vel össze van kötve, az u_i pontok mindegyikére $c(u_i)\in\{1,2,\ldots,k-1\}$. Megadunk egy c' színezést a v_i pontok által feszített részgráfon. (Ez éppen G_k-val izomorf részgráf.) Ha $c(v_i)=k$, akkor legyen $c'(v_i)=c(u_i)$, különben $c'(v_i)=c(v_i)$, vagyis a k színűeket színezzük át a „párjuk” színére.
Belátjuk, hogy c' egy $k-1$ színnel való jó színezése G_k-nak, ami ellentmondás, hiszen $\chi(G_k)>k-1$. Az olyan élekkel nem lehet probléma, amelyeknek egyik végpontja sem volt k színű, hiszen ezek végpontjainak színét nem változtattuk meg. Tegyük fel, hogy $c(v_i)=k$ és v_i-nek van egy olyan v_j szomszédja, amelyre $c'(v_j)=c'(v_i)$. Mivel $c(v_j)\neq k$ (hiszen az eredeti színezés jó volt), ezért $c'(v_j)=c(v_j)$, másrészt $c'(v_i)=c(u_i)$. Így $c(v_j)=c(u_i)$, ami viszont ellentmondás, hiszen v_j és u_i szomszédosak G_{k+1}-ben, ha v_j és v_i szomszédosak G_k-ban. □

Ezzel beláttuk, hogy a klikkszám segítségével nem adható felső korlát a kromatikus számra. Könnyen látható viszont, hogy ha a maximális fokszám a G gráfban Δ, akkor $\chi(G)\leq\Delta+1$. Ha ugyanis mohó algoritmussal tetszőleges sorrendben elkezdjük színezni a gráf pontjait, akkor nem kell $\Delta+1$-nél több színt felhasználnunk. Amikor egy újabb pontot akarunk kiszínezni, akkor ennek legfeljebb Δ szomszédja van már kiszínezve, így a $\Delta+1$-edik színt felhasználhatjuk a színezésre.
Vannak azonban olyan gráfok is, amikor ez a színezés sokkal több színt használ a kromatikus számnál. Vegyük például a következő gráfot: $V(G)=\{a_1,\ldots,a_n,b_1,\ldots,b_n\}$, $E(G)=\{\{a_i,b_j\}\mid i\neq j\}$, vagyis a $K_{n,n}$ teljes gráfból elhagyjuk az $\{a_i,b_i\}$ éleket. Mivel ez páros gráf, kromatikus száma 2. Ha azonban az $a_1,b_1,a_2,b_2,a_3,\ldots$ sorrendben akarjuk színezni a gráfot mohón, akkor n színt fogunk használni.
A $\Delta+1$ korlát azonban olykor pontos: Ha G teljes gráf vagy egy (húr nélküli) páratlan kör, akkor $\chi(G)=\Delta+1$. A következő tétel arról szól, hogy minden más esetben már Δ szín is elég a színezéshez.

2.11.6. Tétel (Brooks). *Ha G egyszerű, összefüggő gráf, nem teljes gráf, és nem egy páratlan hosszúságú kör, akkor $\chi(G)\leq\Delta=\max_{x\in V(G)}d(x)$, azaz ekkor a kromatikus szám nem nagyobb, mint a maximális fokszám.*

BIZONYÍTÁS: Először is könnyen látható, hogy $\Delta=2$ esetén a gráf csak egy egyszerű út vagy egy kör lehet. Ha út, illetve páros hosszúságú kör, akkor nyilván kiszínezhető két színnel. A fennmaradó eset a páratlan kör. Ez pedig megfelel a tétel állításának.
A továbbiakban feltesszük, hogy $\Delta\geq 3$. A bizonyítást a pontszámra vonatkozó indukcióval végezzük, vagyis feltesszük, hogy minden G pontszámánál kisebb pontszámú gráfra már igaz az állítás.
Először belátjuk, hogy elég 2–szeresen összefüggő gráfokkal foglalkoznunk. Tegyük fel, hogy G nem 2–szeresen összefüggő, vagyis az x pont elhagyásával legalább két komponensre esik a gráf. Ha éppen két komponensre esik, akkor legyen G_1, ill. G_2 az a gráf, amelyet a komponensekből az x pont és persze az x-ből G_1, ill. G_2 pontjaiba eredetileg is vezető élek hozzávételéből kapunk. Ha több mint két

komponenesre esik, akkor legyen G_1 az egyik komponens, míg G_2 a többi komponens uniójából és x-ből álljon a megfelelő élekkel összekötve. Tehát $G_1 \cup G_2 = G$ és $V(G_1) \cap V(G_2) = \{x\}$. G_1-ben és G_2-ben x-től eltekintve minden pont fokszáma ugyanannyi maradt, mint G-ben, tehát Δ-nál nem nagyobb. Mivel x-nek volt szomszédja mindkét komponensben, x fokszáma határozottan kisebb lesz Δ-nál G_1-ben és G_2-ben is. Így nem lehet $\Delta+1$ pontú teljes gráf egyik sem. Ekkor azonban az indukciós feltevés szerint kiszínezhetők Δ színnel. Sőt az egyik színezésben a színeket permutálva azt is elérhetjük, hogy x színe mindkét részben ugyanolyan legyen. Ezután pedig a két részt ismét „összerakva” megkaptuk G egy megfelelő színezését.

Most megmutatjuk, hogy elég 3–szorosan összefüggő gráfokkal foglalkozni. Tegyük fel, hogy x és y elhagyásával két részre esik a gráf, G_1-re és G_2-re, amelyekhez most is hozzátartoznak x,y és a megfelelő élek. Ugyanúgy járunk el, mint az előbb, csak előfordulhat, hogy mondjuk G_1 minden színezése olyan, hogy x és y egyforma színűek, míg G_2 minden színezésénél x és y színe különböző. Ekkor nem tudjuk ismét „összerakni” a két részt. A többi esetnél nincs probléma. Ha tehát ez az eset áll fenn, akkor nézzük a $G_1+\{x,y\}$ és a $G_2+\{x,y\}$ gráfokat (azaz behúzzuk az $\{x,y\}$ élet is). Mivel x-nek és y-nak is volt szomszédja mindkét komponensben, így G_1-ben, ill. G_2-ben is teljesül rájuk, hogy a fokszámuk legfeljebb Δ. A többi pontra pedig nyilván igaz a feltétel. Az indukciós feltevés szerint ekkor mindkét rész vagy kiszínezhető Δ színnel, vagy teljes gráfot kaptunk. (A másik kivétel, a páratlan kör, nem okoz gondot, hisz $\Delta \geq 3$.) Ha mindkét rész kiszínezhető, az azt jelenti, hogy G_1-ben és G_2-ben is különböző színe van x-nek és y-nak. Ekkor pedig a már ismert módon „összerakjuk” a részeket. Ha viszont mondjuk $G_1+\{x,y\}$ egy $\Delta+1$ pontú teljes gráf, akkor az azt jelenti, hogy x-nek és y-nak is csak egy szomszédja van G_2-ben. Ha ezeket x'-vel ill. y'-vel jelöljük, akkor az eredeti gráf két részre esik akkor is, ha x'-t és y-t hagyjuk el. Ha most ugyanezt végigcsináljuk, akkor nem jutunk teljes gráfhoz, hanem valamelyik másik esethez, amikor megkapjuk a gráf egy jó színezését.

Most tehát a tételt már csak 3–szorosan összefüggő nem teljes gráfokra kell belátnunk. Legyenek v_1,v_2,v_n olyan pontjai G-nek, amelyekre $\{v_1,v_n\} \in E(G)$, $\{v_2,v_n\} \in E(G)$, de $\{v_1,v_2\} \notin E(G)$. Ilyen pontok biztosan vannak, ha G nem teljes gráf és összefüggő.

A gráf többi pontját úgy akarjuk megjelölni $v_3,v_4,\ldots,v_{n-1}$-gyel, hogy minden pontnak legyen nagyobb indexű szomszédja is. Mivel G 3–szorosan összefüggő, a $G-\{v_1,v_2\}$ gráf még biztosan összefüggő. Ennek a maradék gráfnak van feszítőfája (2.2.5. tétel) és ennek a feszítőfának van v_n-től különböző elsőfokú pontja (2.2.2. tétel). Ez legyen v_3. A $G-\{v_1,v_2,v_3\}$ gráf összefüggő marad, így hasonlóan kapjuk v_4-et stb. Az így kapott sorrend nyilván megfelel a feltételünknek.

Most megadunk egy színezést Δ színnel. Színezzük v_1-et és v_2-t mondjuk pirosra. Majd sorban színezzük ki mohó módon $v_3,v_4,\ldots,v_{n-1}$-et is. Mindig lesz megfelelő szín v_i-hez, mert eddig v_i-nek csak az i-nél kisebb indexű szomszédait színeztük ki, amiből viszont Δ-nál kevesebb van. (Összesen legfeljebb Δ szomszédja van, de van közte i-nél nagyobb indexű.) v_n-nek ugyan lehet, hogy éppen Δ szomszédja van, de ezek között van két piros színű is, v_1 és v_2. Tehát marad szín v_n-nek is. □

Láttuk már, hogy ez a felső korlát lehet nagyon rossz. Egy másik példa erre egy n pontú csillag (egy középső ponthoz csatlakozik $n-1$ él), ekkor $\Delta = n-1$, viszont $\chi = 2$.

2.11.2. Perfekt gráfok

Láttuk, hogy egy gráf kromatikus száma és klikkszáma között általában nem tételezhetünk fel egyenlőséget (sőt még ennél sokkal lazább összefüggést sem). Mégis igen sok olyan példa van, amikor ez a két paraméter egyenlő, csak a legegyszerűbb példát említve, ilyen az összes páros gráf. Felmerül a kérdés, hogy vajon érdemes-e közelebbről is megvizsgálni azokat a gráfokat, melyekre az egyenlőség teljesül. A válasz abban az esetben lesz igen, ha még valamit kikötünk, nevezetesen azt, hogy a szóban forgó egyenlőség ne csak a gráfra magára, hanem minden feszített részgráfjára is igaz legyen. Enélkül ugyanis egy tetszőleges gráfot kiegészíthetnénk egy elegendően nagy klikk hozzávételével (amit esetleg még egy éllel összekötünk az eredeti gráf egy tetszőleges pontjával, hogy az összefüggőséget se rontsuk el) olyanná, amire a kromatikus szám és a klikkszám egyenlő. Vagyis ez a kikötés önmagában még nem sokat árulna el a gráf struktúrájáról. Ugyanez az ellenvetés azonban már nem tehető meg, ha a feszített részgráfokra is vonatkozik a feltétel. Ez a meggondolás indokolja a következő definíciót, mely egy igen fontos gráfosztályt vezet be.

2.11.7. Definíció (Berge). *Egy G gráf **perfekt**, ha $\chi(G) = \omega(G)$ és G minden G' feszített részgráfjára is teljesül, hogy $\chi(G') = \omega(G')$.*

2.11.8. Tétel. *Minden páros gráf perfekt.*

BIZONYÍTÁS: Mivel egy páros gráf minden feszített (és nem feszített) részgráfja szintén páros gráf, ezért elég belátni, hogy minden $G = (A,B)$ páros gráfra $\chi(G) = \omega(G)$. Ez viszont nyilván igaz, hiszen a legalább egy élet tartalmazó gráfokra $\omega(G) = 2$, mert páros gráfban nincs háromszög, másrészt ha A pontjait pirossal, B pontjait pedig kékkel színezzük, akkor G egy 2–színezését kapjuk. Az egy élet sem tartalmazó páros gráfra pedig $\chi(G) = 1 = \omega(G)$. □

Másik nevezetes példa perfekt gráfokra az ún. intervallumgráfok osztálya.

2.11.9. Definíció. *Legyenek $I_1 = [a_1, b_1], I_2 = [a_2, b_2], \ldots$ korlátos zárt intervallumok, és minden a_i, b_i legyen pozitív egész. Legyenek $p_1, p_2, \ldots$ egy G gráf pontjai és $\{p_i, p_j\}$ akkor és csak akkor legyen él G-ben, ha $I_i \cap I_j \neq \emptyset$. Az így előálló gráfokat **intervallumgráfoknak** nevezzük.*

2.11.10. Tétel. *Minden intervallumgráf perfekt.*

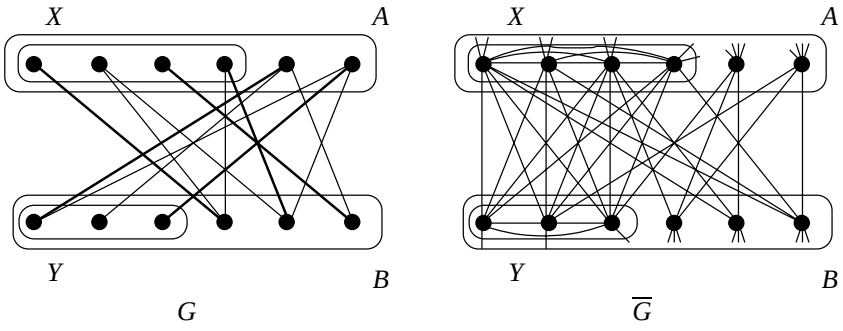
BIZONYÍTÁS: Mivel az intervallumgráfok feszített részgráfjai is intervallumgráfok, ezért itt is elég belátni, hogy az intervallumgráfok kromatikus száma megegyezik a klikkszámukkal.

Legyen $\omega(G) = k$. Mivel $\chi(G) \geq \omega(G)$, elég belátni, hogy $\chi(G) \leq k$. Kezdjük el színezni a pontoknak megfelelő intervallumokat balról jobbra. A még színezetlen intervallumok közül mindig azt színezzük ki, amelyiknek baloldali végpontja a legbalrább van. Ha egy intervallumot a $k+1$-dik színnel kellene kiszíneznünk, akkor az azt jelenti, hogy ennek az intervallumnak a bal vége benne van már k intervallumban, amelyeket már kiszíneztünk az $1, 2, \ldots, k$ színekkel. Így van $k+1$ intervallum, amelyek közül bármely kettő metszi egymást, azaz van az intervallumgráfban egy $k+1$ méretű klikk, ez viszont ellentmond feltevésünknek. □

Valamivel nehezebben látható, hogy perfekt minden páros gráf komplementere is, és az a gráf is, amit úgy kapunk, hogy egy páros gráf minden élének megfeleltetünk egy pontot és két ilyen pontot akkor kötünk össze, ha a megfelelő éleknek van közös pontjuk (ez a páros gráf **élgráfja**). Csak az első állítást bizonyítjuk most be.

2.11.11. Tétel. *Minden G páros gráf $\overline{G}$ komplementere perfekt.*

BIZONYÍTÁS: Mivel egy páros gráf komplementerének minden feszített részgráfja is egy páros gráf komplementere (ez nem feszített részgráfra nem igaz!), elég belátni, hogy $\chi(\overline{G}) = \omega(\overline{G})$. Sőt, mivel $\chi(\overline{G}) \geq \omega(\overline{G})$, elég bizonyítani, hogy $\overline{G}$ kiszínezhető $\omega(\overline{G})$ színnel.
Legyen G-ben a két színosztály A és B. Egy maximális méretű klikk $\overline{G}$-ben pedig legyen $X \cup Y$ úgy, hogy $X \subseteq A$ és $Y \subseteq B$ teljesüljön. ($X \cup Y$ a G gráfban egy független ponthalmazt alkot.)
Belátjuk, hogy létezik G-ben egy olyan párosítás, ami $A - X$ minden pontjához egy Y-beli pontot párosít. Tegyük fel indirekt, hogy nem létezik ilyen párosítás. Ekkor a 2.9.4. Hall tétel szerint létezik egy olyan $Z \subseteq A - X$ ponthalmaz az $((A - X) \cup Y)$ által feszített páros gráfban, amelyre $|N(Z)| < |Z|$. Így azonban könnyen látható, hogy az $(X \cup Z) \cup (Y - N(Z))$ halmaz egy $X \cup Y$-nál nagyobb klikk $\overline{G}$-ben, ami ellentmondás. Ehhez csak azt kell észrevennünk, hogy G-ben nincs él Z és $Y - N(Z)$ pontjai között $N(Z)$ definíciója miatt. (Lásd a 2.53. ábrát.)



2.53. ábra.

Ugyanígy megmutatható, hogy G-ben van egy olyan párosítás is, ami $B-Y$ minden pontjához egy X-beli pontot párosít. Ez és az előző párosítás $\overline{G}$-ben minden $(A-X)\cup(B-Y)$-beli ponthoz rendel egy vele nem szomszédos $X\cup Y$-beli pontot. Ha tehát $X\cup Y$ pontjait kiszínezzük $\omega(\overline{G})$ színnel, akkor minden további pontot kiszínezhetünk úgy, hogy az előbb definiált párjának színét adjuk neki. Könnyen látható, hogy ez jó színezés, hiszen minden szín legfeljebb két ponton fordul elő és ezek biztosan nem szomszédos pontok. □

Az előbbi tételnek van egy sokkal általánosabb formája is, amit itt nem bizonyítunk be.

2.11.12. Tétel (Lovász). *Egy gráf akkor és csak akkor perfekt, ha a komplementere perfekt.*

Mely gráfok nem perfektek? Nem perfekt egy legalább öt hosszú páratlan kör, hiszen ebben a maximális klikk mérete 2, viszont kromatikus száma 3. Az előbbi tétel szerint a legalább öt hosszú páratlan körök komplementerei sem perfektek. A definícióból így rögtön következik, hogy nem perfekt egy olyan gráf sem, amiben feszített részgráfként van egy páratlan kör vagy komplementere. Berge következő sejtése szerint nincs is másmilyen nem perfekt gráf.

2.11.13. Sejtés (Erős perfekt gráf sejtés). *Egy G gráf akkor és csak akkor perfekt, ha sem G, sem $\overline{G}$ nem tartalmaz feszített részgráfként páratlan kört.*

2.11.3. Síkbarajzolható gráfok kromatikus száma

A fentiekben láthattuk, hogy általában nem könnyű jó becslést adni egy gráf kromatikus számára. Ha viszont a gráf síkbarajzolható, akkor lényegesen könnyebb a helyzet.

2.11.14. Tétel (5-szín tétel). *Ha G síkbarajzolható gráf, akkor $\chi(G)\leq 5$.*

BIZONYÍTÁS: A gráf pontszámára vonatkozó indukcióval bizonyítunk. Mivel a párhuzamos élek nem befolyásolják a színezést, feltehetjük, hogy a gráf egyszerű. 2 pontú gráfra nyilván igaz az állítás. A 2.5.4. tételben beláttuk, hogy G éleinek száma legfeljebb $3n-6$, ahol $n=|V(G)|$. Így biztosan van egy olyan x pont, amelynek foka legfeljebb 5, hiszen ha minden pont foka legalább 6, akkor az élek száma legalább $\frac{1}{2}6n$ volna, ami ellentmondás. Ha x foka legfeljebb négy, akkor az indukciós feltevés miatt x-et elhagyva kiszínezhető a gráf 5 színnel, majd x-et a 4 szomszédjától eltérő ötödik színnel színezzük ki.
Tegyük most fel, hogy $d(x)=5$. Ha x-nek bármely két szomszédja között van él, akkor a gráfban egy K_6 részgráf szerepel, ami ellentmond G síkbarajzolhatóságának. Tehát x két szomszédja, y és z nincs összekötve. Húzzuk össze egy ponttá az x,y és z pontokat. Az így kapott G' gráf az indukciós feltevés miatt kiszínezhető 5 színnel. Az ennek megfelelő színezés G-ben nem jó, hiszen x,y,z egyszínűek. G-ben x-nek három szomszédja van y-on és z-n kívül. Ezek legfeljebb három színt foglalnak le,

és a további két szomszéd, y és z, egyszínű. Marad tehát az ötödik szín, amellyel kiszínezhetjük x-et. Tehát G kiszínezhető 5 színnel. □

Appel és Haken [1977] bebizonyította a 4-szín tételt is, de bizonyításuk többszáz oldalas, és felhasználtak hozzá számítógépes módszereket is.

2.11.15. Tétel (4-szín tétel). *Ha G síkbarajzolható gráf, akkor $\chi(G) \leq 4$.*

2.11.4. Élkromatikus szám

2.11.16. Definíció. *Egy G gráf élei **k színnel kiszínezhetők**, hogyha minden élet ki lehet színezni k szín felhasználásával úgy, hogy bármely két szomszédos él színe különböző legyen. G **élkromatikus száma** $\chi_e(G) = k$, ha G élei k színnel kiszínezhetők, de $k-1$ színnel nem.*

Megjegyezzük, hogy az élkromatikus szám megegyezik a gráf élgráfjának kromatikus számával. Nyilvánvaló, hogy az élkromatikus szám nem lehet kisebb a maximális fokszámnál, hiszen az egy pontra illeszkedő éleket mind különböző színekre kell színezni. Viszont egyszerű gráfokra az élkromatikus szám ennél legfeljebb eggyel lehet nagyobb.

2.11.17. Tétel (Vizing). *Ha G egyszerű gráf, akkor $\chi_e(G) \leq \Delta + 1$.*

BIZONYÍTÁS: Próbáljuk kiszínezni a gráf éleit $\Delta+1$ színnel. Tegyük fel, hogy az $\{x,y_1\}$ élet még nem színeztük ki. Mivel egy pontból legfeljebb Δ él indul ki, minden $v \in V(G)$ ponthoz rendelhetünk egy színt, $c(v)$-t, ami nem szerepel még a v-ből kiinduló élek egyikén sem. Ha $c(x) = c(y_1)$ (azaz a két szín megegyezik), akkor az $\{x,y_1\}$ élet kiszínezhetjük a $c(x)$ színnel.
Most tegyük fel, hogy $c(x) \neq c(y_1)$. Ekkor két eset lehet. Ha x-ből nem indul ki $c(y_1)$ színű él, akkor az $\{x,y_1\}$-et megint csak kiszínezhetjük $c(y_1)$ színnel. Tehát feltehetjük, hogy van x-nek olyan y_2 szomszédja, hogy az $\{x,y_2\}$ él színe $c(y_1)$. Ha x-ből nem indul ki $c(y_2)$ színű él, akkor $\{x,y_2\}$ színét $c(y_2)$-re cseréljük, ekkor viszont x-ből nem indul ki $c(y_1)$ színű él. Ellenkező esetben feltehetjük, hogy van x-nek olyan y_3 szomszédja, hogy az $\{x,y_3\}$ él színe $c(y_2)$. A gondolatmenetet folytatva hasonlóan kapjuk az $y_4, y_5, \ldots$ pontokat.
Csak akkor akadunk el, ha van olyan h, hogy az $\{x,y_h\}$ él színe $c(y_{h-1})$, és valamilyen $1 \leq j < h$ indexre $c(y_h) = c(y_j)$. Minden más esetben át tudjuk úgy alakítani a színezést, hogy ki tudjuk színezni $\{x,y_1\}$-et is. Ha viszont ez a helyzet, akkor tekintsük G-nek azt a G' részgráfját, amelyet a $c(x)$ és a $c(y_h)$ színű élek alkotnak. G'-ben minden pont foka legfeljebb 2, és mivel x-ből nem indul ki $c(x)$ színű, y_h-ból és y_j-ből pedig $c(y_h)$ színű él, x, y_h, y_j fokszáma legfeljebb 1. Tehát G' utakból, esetleg még körökből és izolált pontokból áll. x az egyik ilyen út egyik végpontja, tehát vagy y_j, vagy y_h x-től különböző komponensben van. Ha például y_j van más komponensben, akkor az ebben a komponensben szereplő élek színét cseréljük fel. Így elértük, hogy $c(y_j) = c(x)$. Most már $\{x,y_j\}$ színét kicserélhetjük $c(x)$-re, $\{x,y_{j-1}\}$ színét $c(y_{j-1})$-re, stb. és végül ki tudjuk színezni $\{x,y_1\}$-et $c(y_1)$-gyel. □

A fenti eljárás egy polinomiális algoritmushoz vezet, ami kiszínezi a gráf éleit $\Delta+1$ színnel. Annak eldöntése viszont **NP**–teljes (ld. a 3.5. szakasz), hogy egy adott gráfra $\chi_e = \Delta$ vagy $\chi_e = \Delta+1$.

2.12. Részgráfokkal kapcsolatos kérdések

2.12.1. Ramsey–típusú tételek

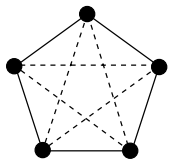
2.12.1. Tétel. *Minden* 6 *pontú gráfban van egy teljes* 3*-as vagy egy teljes üres* 3*-as, azaz vagy van* 3 *olyan pont, hogy bármely kettő között fut él, vagy van* 3 *olyan pont, hogy köztük nem fut él.*

BIZONYÍTÁS: Válasszunk ki egy tetszőleges pontot, v_1-et. Mivel rajta kívül még 5 pont van, vagy van 3 olyan pont, amibe vezet él v_1-ből, vagy 3 olyan pont, amibe nem vezet él v_1-ből. Az első esetben legyenek v_1 szomszédai v_2, v_3, v_4. Ha ezek között vezet él, például $\{v_2, v_3\} \in E(G)$, akkor v_1, v_2, v_3 egy teljes 3-as, ha viszont nem vezet köztük él, akkor v_2, v_3, v_4 egy teljes üres hármas. A másik esetben is ugyanígy következik az állítás. □

Most próbáljuk általánosítani ezt a tételt.

2.12.2. Tétel (Ramsey). *Adott k, l pozitív egészekhez létezik egy olyan legkisebb $r(k,l)$ szám, hogy $n \geq r(k,l)$ esetén az n pontú teljes gráf, K_n éleit két színnel – kékkel és pirossal – kiszínezve van a gráfban egy kék K_k vagy egy piros K_l.*

Mivel van olyan 5 pontú gráf, amelyben nincs sem teljes 3-as, sem teljes üres 3-as (2.54. ábra), az előző tételből következik, hogy $r(3,3) = 6$, hiszen egy gráfot felfoghatunk úgy is, hogy a teljes gráf azon éleit színezzük kékre, amelyek szerepelnek a gráfban, és azokat pirosra, amelyek nem.



2.54. ábra.

Ramsey tételének bizonyításával együtt belátjuk a következő tételt is.

2.12.3. Tétel (Erdős–Szekeres).

$$r(k,l) \leq r(k-1,l) + r(k,l-1) \tag{2.1}$$

BIZONYÍTÁS: Bizonyítsunk indukcióval. Nyilvánvaló, hogy létezik $r(k,2)$ és $r(2,l)$ és világos, hogy $r(k,2)=k$ és $r(2,l)=l$. Tegyük most fel, hogy létezik minden $r(t,s)$, ahol vagy $t\le k$ és $s<l$ vagy $t<k$ és $s\le l$. Valamint indirekt tegyük fel, hogy

$$n\ge r(k-1,l)+r(k,l-1), \tag{2.2}$$

és K_n élei megszínezhetők két színnel úgy, hogy a gráfban nincs sem kék K_k, sem piros K_l.
Válasszuk ki K_n egy tetszőleges pontját, v_1-et. Legyenek a v_1-ből kimenő kék élek végpontjai $k_1,k_2,\dots,k_u$, a pirosaké pedig $p_1,p_2,\dots,p_v$. Ha u nagyobb lenne $r(k-1,l)-1$-nél, akkor a k_i pontok között a feltevés miatt volna vagy egy piros K_l vagy egy kék K_{k-1} és az utóbbi esetben ehhez hozzávéve v_1-et kék K_k-t kapnánk. Tehát a feltevésekből következik, hogy $u\le r(k-1,l)-1$. Ugyanígy kapjuk, hogy $v\le r(k,l-1)-1$. Ekkor viszont $n=u+v+1\le r(k-1,l)+r(k,l-1)-2+1$, ami viszont ellentmond (2.2)-nek.
Itt tulajdonképpen azt láttuk be, hogy $r(k-1,l)+r(k,l-1)$ olyan szám, hogy minden nála nem kisebb n-re K_n-et két színnel színezve lesz a gráfban kék K_k, vagy piros K_l. Ekkor viszont a legkisebb ilyen szám kisebb vagy egyenlő $r(k-1,l)+r(k,l-1)$-vel. □

(2.1) felhasználásával könnyen adhatunk felső korlátot $r(k,l)$-re.

2.12.4. Tétel.

$$r(k,l)\le\binom{k+l-2}{k-1}$$

BIZONYÍTÁS: Teljes indukcióval bizonyítunk. Láttuk már, hogy $r(k,2)=k$ és $r(2,l)=l$. Tegyük fel, hogy már igaz az állítás minden olyan $r(t,s)$-re, ahol vagy $t<k$ és $s\le l$, vagy $s<l$ és $t\le k$. Ekkor

$$r(k,l)\le r(k-1,l)+r(k,l-1)\le\binom{k+l-3}{k-2}+\binom{k+l-3}{k-1}=\binom{k+l-2}{k-1}.$$

□

Általánosíthatjuk a Ramsey–tételt több színre is.

2.12.5. Tétel. *Adott $k_1,k_2,\dots,k_m$ egészek esetén létezik egy legkisebb olyan $r(k_1,k_2,\dots,k_m)$, hogy $n\ge r(k_1,k_2,\dots,k_m)$ esetén m színnel színezve K_n-et lesz a gráfban vagy első színű K_{k_1}, vagy második színű K_{k_2}, stb. Azt is tudjuk, hogy*

$$r(k_1,k_2,\dots,k_m)\le\frac{(\sum_{i=1}^m(k_i-1))!}{\prod_{i=1}^m(k_i-1)!}.$$

Ezt a tételt a Ramsey–tételhez hasonlóan lehet bebizonyítani.

Felső becslésünk már van $r(k,l)$-re, alsó becslésünk viszont nincs. Erre irányul Erdős tétele.

2.12.6. Tétel (Erdős). *Ha $k \geq 3$, akkor*

$$r(k,k) \geq 2^{k/2}.$$

BIZONYÍTÁS: Jelöljük g_n-el a különböző n pontú gráfok számát, $g_{n,k}$-val pedig azon n pontú gráfok számát, amelyekben van K_k részgráf. Könnyen látható, hogy $g_n = 2^{\binom{n}{2}}$ és $g_{n,k} \leq \binom{n}{k} 2^{\binom{n}{2}-\binom{k}{2}}$. Jelöljük P-vel annak a valószínűségét, hogy egy véletlen n pontú gráf tartalmaz K_k-t. Nyilván

$$P = \frac{g_{n,k}}{g_n} \leq \binom{n}{k} 2^{-\binom{k}{2}} < \frac{n^k}{k! 2^{\binom{k}{2}}}.$$

Tegyük fel tehát, hogy $n < 2^{k/2}$. Ebben az esetben

$$P < \frac{2^{\frac{k^2}{2}-\binom{k}{2}}}{k!} = \frac{2^{k/2}}{k!} < \frac{1}{2}, \tag{2.3}$$

ha $k \geq 3$. Hasonlóan kisebb $\frac{1}{2}$-nél annak a P' valószínűsége, hogy egy véletlen gráfban van üres k-as. Tehát annak a Q valószínűsége, hogy egy véletlen n pontú gráfban nincs sem teljes k-as, sem üres k-as, $Q = 1 - P - P' > 1 - \frac{1}{2} - \frac{1}{2} = 0$. Ez pedig azt jelenti, hogy biztosan van olyan n pontú gráf, amely nem tartalmaz sem teljes, sem üres k-ast vagyis $r(k,k) \geq 2^{k/2}$.
Megfogalmazhatjuk a bizonyítást valószínűségek nélkül is. Ha P-vel egyszerűen csak a $\frac{g_{n,k}}{g_n}$ hányadost jelöljük, akkor (2.3) azt jelenti, hogy $g_{n,k} < \frac{1}{2} g_n$. Vagyis az összes n pontú gráfoknak kevesebb mint a fele tartalmaz k-ast. Ugyanígy az összes n pontú gráfoknak kevesebb mint a fele tartalmaz üres k-ast. Így biztosan van olyan n pontú gráf, ami nem tartalmazza egyiket sem, és így ellentmondásra jutottunk. □

Nézzünk most a Ramsey–típusú tételeknek egy alkalmazását.

2.12.7. Definíció. *Jelöljük r_n-nel $r(\underbrace{3,3,\ldots,3}_{n \text{ darab}})$-at.*

2.12.8. Tétel (Schur). *Az $\{1,2,3,\ldots,r_n\}$ halmazt bárhogyan osztjuk fel n darab diszjunkt $S_1, S_2, \ldots, S_n$ részhalmazra ($S_1 \cup \cdots \cup S_n = \{1,\ldots,r_n\}$), valamelyik részhalmazban megoldható az $x+y=z$ egyenlet, azaz van olyan i,x,y,z számnégyes, hogy $x,y,z \in S_i$ és $x+y=z$.*

BIZONYÍTÁS: Színezzük ki K_{r_n} éleit a következőképpen. Egy $\{u,v\}$ élet az k-adik színnel színezünk ki, ha $|u-v| \in S_k$. Ekkor r_n definíciója miatt van a gráfban valamilyen színű teljes hármas. Legyenek az ennek a három csúcsnak megfelelő számok $u < v < w$, és a háromszög színe az i-edik szín. Jelöljük $w-v$-t x-szel, $v-u$-t y-nal és $w-u$-t z-vel. Definícióink miatt $x,y,z \in S_i$ és $x+y=z$. □

2.12.2. Turán–típusú tételek

Az első ilyen típusú kérdés talán az volt, hogy legfeljebb hány éle lehet egy n pontú gráfnak, amelyben nincs háromszög. Sejthető, hogy a legtöbb éle annak a páros gráfnak van, amelyben a két osztály pontszáma egyenlő, vagy legfeljebb eggyel tér el. Ezt Turán Pál általánosabban is bebizonyította.

2.12.9. Definíció. *Definiáljuk a $T_{n,m}$ ($n \geq m$) gráfot a következőképpen. Osszuk el maradékosan n-et m-mel, azaz legyen $n = qm + r$, ahol $0 \leq r < m$. A gráf n pontját osszuk m osztályra, r osztály álljon $q+1$ pontból, a többi $m-r$ pedig q pontból. A gráfban két pont akkor és csak akkor legyen összekötve, ha különböző osztályban vannak.* ***m-osztályú gráfnak*** *nevezünk egy gráfot, ha a pontjai m osztályba oszthatók úgy, hogy az egy osztályban levő pontok között nem fut él. $T_{n,m}$-et másképpen m-osztályú teljes gráfnak nevezzük.*

2.12.10. Tétel. *Ha egy n pontú G gráf nem tartalmaz K_{m+1}-et, akkor*

$$e(G) \leq e(T_{n,m}).$$

Ha pedig $e(G) = e(T_{n,m})$, akkor $G \cong T_{n,m}$.

BIZONYÍTÁS: Először lássuk be, hogy az m-osztályú gráfok közül $T_{n,m}$-nek van a legtöbb éle. Tegyük fel, hogy az a G gráf, amelyiknek a legtöbb éle van, nem a $T_{n,m}$ gráf. Ebben a gráfban kell, hogy legyen két olyan osztály, hogy az egyikben x pont van, a másikban legalább $x+2$. Ha a nagyobból a kisebbe átteszünk egy pontot, akkor legfeljebb x él szűnik meg, viszont legalább $x+1$ új élet húzunk be. Vagyis növeltük az élszámot, ez pedig ellentmond a feltevésünknek.
Most az látjuk be, hogy ha G egy K_{m+1}-et nem tartalmazó n-pontú gráf, akkor ugyanazon a ponthalmazon konstruálható egy olyan m osztályú teljes H gráf, melyben minden pont fokszáma legalább akkora mint G-ben, vagyis minden $v \in V(G) = V(H)$-ra $d_G(v) \leq d_H(v)$.
m-re való teljes indukcióval bizonyítunk. $m = 1$-re az állítás triviális. Legyen G-ben a maximális fokszám Δ_G és x olyan pont, hogy $d_G(x) = \Delta_G$. Legyen $V_1 = \{u | \{u,x\} \in E(G)\}$, vagyis x szomszédainak halmaza, V_2 pedig a többi pont, vagyis $V_2 = V(G) - V_1$ Így persze $x \in V_2$. G_1 legyen G-nek a V_1 által feszített részgráfja. Nyilván G_1-ben nincs K_m, hiszen ez x-szel együtt G-ben K_{m+1}-et alkotna. Így alkalmazhatjuk az indukciós feltevést G_1-re. Tehát van olyan teljes $m-1$-osztályú H_1 gráf, hogy minden $v \in V(G_1)$-re $d_{G_1}(v) \leq d_{H_1}(v)$.
Konstruáljuk meg a H gráfot a következőképpen. Vegyük a V_1 ponthalmazon a H_1 gráfot, majd V_1 minden pontját kössük össze V_2 minden pontjával, viszont hagyjunk el minden két V_2-beli pontot összekötő élet. Nyilvánvaló, hogy ez a H gráf m osztályú, hiszen H_1 $m-1$ osztályú teljes gráf volt, és ehhez egy újabb osztályt, V_2-t vettünk. Lássuk be, hogy $d_G(v) \leq d_H(v)$ minden pontra teljesül. Ha $v \in V_2$, akkor $d_H(v) = |V_1| = \Delta_G$, a definícióink szerint viszont $d_G(v) \leq \Delta_G$. Ha $v \in V_1$, akkor

$$d_H(v) = d_{H_1}(v) + |V_2| \geq d_{G_1}(v) + |V_2| \geq d_G(v).$$

Tehát H valóban megfelelő gráf.
Így ha egy G gráfban nincs K_{m+1}, de nem izomorf $T_{n,m}$-mel, akkor konstruálhatunk egy nála nagyobb élszámú m-osztályú teljes gráfot, ennek az élszáma pedig nem nagyobb $T_{n,m}$ élszámánál. Egyben beláttuk az állítás második részét is. □

Megjegyezzük, hogy $T_{n,m}$ élszáma

$$e(T_{n,m}) = \binom{n}{2} - r\binom{q+1}{2} - (m-r)\binom{q}{2} \approx \binom{n}{2}\left(1-\frac{1}{m}\right). \tag{2.4}$$

Megemlítünk ebből a témakörből még két tételt bizonyítás nélkül.

2.12.11. Tétel (Erdős–Stone). *Ha*

$$e(G) \geq e(T_{n,m}) + \varepsilon n^2,$$

akkor G-ben nemcsak hogy van legalább egy K_{m+1}, hanem létezik olyan $c(\varepsilon, m)$ konstans is, hogy G-ben van olyan teljes $m+1$-osztályú részgráf, amelyben az osztályok pontszáma legalább $c\log n$.

2.12.12. Tétel (Erdős–Simonovits). *Ha $G_1, G_2, \ldots, G_k$ adott gráfok, akkor létezik olyan $f(n; G_1, G_2, \ldots, G_k)$ függvény, amelyre teljesül, hogy minden olyan G gráfnak, amelyre $v(G) = n$ és $e(G) \geq f(n; G_1, G_2, \ldots, G_k)$, van valamelyik G_i gráffal izomorf részgráfja. Az f függvényre teljesül, hogy*

$$\lim_{n\to\infty} \frac{f(n; G_1, G_2, \ldots, G_k)}{\binom{n}{2}} = 1 - \frac{1}{\min_{i=1,\ldots,k} \chi(G_i) - 1}. \tag{2.5}$$

Vegyük észre, hogy $k = 1$ és $G = K_{m+1}$ esetén $\chi(K_{m+1}) = m+1$ miatt (2.5) éppen (2.4)-re redukálódik.

3. fejezet

Adatkezelési eljárások, gráfelméleti adatstruktúrák, a bonyolultságelmélet elemei

3.1. Keresés

Tegyük fel, hogy Béla gondol egy x egész számot 1 és n között. Ezt a számot akarja kitalálni Aliz. Aliz megkérdezheti Bélát, hogy az általa gondolt szám nagyobb-e egy k egésznél. Hány kérdésre van szüksége Aliznak ahhoz, hogy kitalálja a számot?

Ha sorban minden számot megkérdezne Aliz, akkor legrosszabb esetben $n-1$, de átlagosan is $n/2$ lépésre lenne szüksége. Ehelyett jobb, ha azt kérdezi, hogy x nagyobb-e $n/2$-nél. Ha igen, elég a sorozat második felével, ha nem, elég a sorozat első felével foglalkoznia. Minden ilyen lépésben megfelezi a sorozatot, így a legrosszabb esetben $\log_2 n$ lépésben végez.

Ez az eljárás nyilván akkor is használható, ha n tetszőleges szám van adva, sőt nem is mind különböző (és „növekvő” helyett „nem csökkenő” sorrendről van szó). Az sem baj, ha n nem éppen 2 valamelyik hatványa. Ekkor az eljárás során legalább egyszer egy páratlan k számot kell „feleznünk”. Ilyenkor $\lfloor k/2 \rfloor$ alsó egészrész vagy $\lceil k/2 \rceil$ felső egészrész lép $k/2$ helyébe. A lépésszám is $\lceil \log_2 n \rceil$ lesz.

Megmutatjuk, hogy nem lehetséges olyan algoritmust készíteni, ami $\lceil \log_2 n \rceil$-nél kevesebb összehasonlítással sőt, általánosabban, ennél kevesebb bármilyen típusú igennel vagy nemmel megválaszolandó kérdés feltevésével mindig megoldaná ezt a feladatot. Tegyük fel, hogy Aliz készítene egy ilyen algoritmust és Béla meg akarja mutatni, hogy ez az algoritmus rossz. Valahányszor Aliz algoritmusa feltesz egy kérdést, a még szóba jöhető számok közül bizonyosakat az „igen”, a többit a „nem” válasz zárja ki. Béla azt mondja Aliznak, hogy gondolt egy n-tagú sorozatot és egy x számot, és megkéri Alizt, alkalmazza ezekre az „algoritmusát”.

A valóságban Béla mondjuk az $1, 2, \ldots, n$ sorozatra gondol, viszont semmilyen x-re sem, hanem Aliz kérdéseire mindig úgy válaszol, hogy a válasz a még szóba jöhető számoknak legfeljebb a felét zárja ki. Így k kérdés után még mindig a számok

legalább 2^k-adrésze szóba jöhet. Ha tehát Aliz $\lceil \log_2 n \rceil$-nél kevesebb kérdést tett fel, akkor még egynél több szám jöhet szóba, tehát bármilyen „eredményt” hozna ki Aliz, Béla tudna egy másik olyan számot is mondani, amely esetén ugyanezeket a válaszokat adta volna, és erre a másik számra „fogja rá”, hogy ez volt x.

3.2. Beszúrás

Most tegyük fel, hogy $n-1$ darab különböző valós számunk van, növekvő sorrendben felsorolva, de most egy adott x számot be kell szúrnunk a sorozatba. Ez tulajdonképpen ugyanaz, mintha n intervallumból kellene kiválasztanunk a megfelelőt.
Ezúttal tehát $\lceil \log_2 n \rceil$ lépésben találjuk meg x helyét, de utána az x után következőket eggyel jobbra kell tolnunk, így a legrosszabb esetben $n-1+\lceil \log_2 n \rceil$ lépésre van szükségünk.
Számos esetben az összehasonlítás lényegesen idő– és pénzigényesebb művelet, mint a számok máshová helyezése. (Gondoljunk például arra, hogy esetleg egy összehasonlítás egy többórás fizikai vagy kémiai kísérlet elvégzését jelentheti, míg az adatok mozgatásából több millió elvégezhető egy másodperc alatt.) Ilyenkor a fenti megoldás tekinthető gyakorlatilag a lehető legjobbnak. Ha nem ez a helyzet, akkor a teljes lépésszámot (tehát nem csak az összehasonlítások számát) lecsökkenthetjük ugyan $c \cdot \log_2(n+1)$-re, de ehhez a sorozatot nem egy $a(1), a(2), \ldots, a(n)$ tömbben kell ábrázolnunk, hanem másfajta adatstruktúrát kell alkalmaznunk. Ezzel a kérdéssel itt nem foglalkozunk.

3.3. Sorba rendezés

Ezek után azonnal látszik, hogy n darab különböző valós szám sorba rendezéséhez sem kell több, mint $n \log_2 n$ darab összehasonlítás. Tekintsük ugyanis a számokat, amilyen sorrendben érkeznek, és mindig a legutoljára érkezettet szúrjuk be az addigiak közé. Világos, hogy összesen

$$a = \lceil \log_2 1 \rceil + \lceil \log_2 2 \rceil + \ldots + \lceil \log_2 n \rceil$$

darab összehasonlítást végeztünk.
Ismét könnyű belátni, hogy ha Aliz bármilyen olyan algoritmust készít, ami k darab igennel vagy nemmel megválaszolandó kérdést tesz fel, Béla tud úgy válaszolni (legalábbis elméletben), hogy az n szám $n!$ féle sorrendje közül a k-ik kérdés után még $n!/2^k$-féle sorrend szóba jöhessen. Aliz algoritmusa tehát biztos rossz, ha $n!/2^k > 1$, vagyis $k < \log_2(n!)$. Mivel

$$\log_2(n!) = \log_2 n + \log_2(n-1) + \ldots + \log_2 2 + \log_2 1$$

és ez legfeljebb n-nel kisebb a fenti a értéknél (hisz minden felső egészrész képzésnél legfeljebb egyet veszíthettünk), megállapíthatjuk, hogy a fenti a érték (ami körülbelül $n \log_2 n - n$) közel a legjobb.

Most is elmondhatjuk, hogy amennyiben az összehasonlítások sokáig tartanak a beszúrásokhoz szükséges adatmozgatásokhoz képest, akkor ez közel optimális algoritmus.

Lényegében ugyanilyen lépésszámmal működik a következő **összefésüléses rendezés** is:

Egy k és egy l hosszú rendezett tömb összefésülésekor összehasonlítjuk két tömb legkisebb elemét és a kisebbet áttesszük az új tömbbe. Utána a maradék két tömb két legkisebb eleme közül áttesszük a kisebbet az új tömbbe a következő helyre. És így tovább, amíg minden elem átkerül az összefésült tömbbe. Így pontosan $k+l-1$ összehasonlítást végeztünk.

Az összefésüléses rendezéskor először két nagyjából egyforma részre vágjuk a rendezendő tömböt és a két részt rekurzívan összefésüléses rendezéssel rendezzük, majd a két részt a fenti módszerrel összefésüljük. Megmutatható, hogy ez a rendezés is $cn\log_2 n$ összehasonlítást használ.

Léteznek olyan – bonyolultabb – algoritmusok is, például a kupacos rendezés, ahol nemcsak az összehasonlítások száma, hanem a teljes lépésszám is $cn\log_2 n$-nel becsülhető felülről a legrosszabb esetben. Ezekkel részletesebben nem foglalkozunk.

Felhívjuk viszont a figyelmet három további sorba rendező algoritmusra. Az egyik különösen egyszerűen működik. Az adott n szám közül először kiválasztjuk a legkisebbet, majd a többi közül a második legkisebbet stb. Az összehasonlítások száma nyilván

$$n-1+n-2+\ldots+2+1=n(n-1)/2\approx cn^2$$

és a további lépések száma is maximum ugyanennyi (hisz az összehasonlítás eredményétől függően vagy fel kell cserélni a két számot, vagy nem). Ha az összehasonlítások időigénye nem nagy (pl. adott számokat kell összehasonlítani, és n sem túl nagy), akkor egyszerűsége miatt gyakran használják ezt az algoritmust.

Egyszerűsége miatt igen népszerű a **buborék rendezés** is, amely szintén nem optimális, hiszen cn^2 összehasonlítást használ:

A rendezendő tömb elejétől kezdve hasonlítsuk össze az egymás mellett álló párokat. Ha a nagyobb elem van előrébb, akkor cseréljük fel őket. Ha egyszer végighaladtunk az egész tömbön, akkor nyilván a legnagyobb elem fog a tömb utolsó helyére kerülni, de a többi elem még nem feltétlenül lesz rendezve. Ezért ismét az elejéről indulva ismételjük meg az eljárást, az első $n-1$ elemre, majd ismét az első $n-2$ elemre, stb.

A harmadik algoritmus, a **láda rendezés**, még $cn\log_2 n$-nél is gyorsabb, de csak akkor használható, ha a sorba rendezendő számok egészek és értékük pl. 1-től n-ig terjed (csak ismeretlen sorrendben). Nyissunk egy n hosszúságú $b(1),b(2),\ldots,b(n)$ tömböt. Ha az i-edikként beérkező $a(i)$ szám értéke j, akkor a $b(j)$ helyre írjuk be az i értéket. Ha ezt mind az n darab $a(i)$-re befejeztük, akkor a b tömbben épp az áll, hogy milyen sorrendben kell az $a(i)$ elemeket olvasnunk, hogy növekedő sorrendbe kerüljenek. Ha pl. $n=5$ és $a=(3,1,5,2,4)$, akkor $b=(2,4,1,5,3)$ és csakugyan, az a tömb 2. eleme a legkisebb, 4. eleme a következő stb.

Világos, hogy a legutolsó algoritmus csak cn lépésszámú, és még akkor is az marad, ha a sorba rendezendő pozitív egészek nem 1-től n-ig, hanem 1-től c_0n-ig terjednek

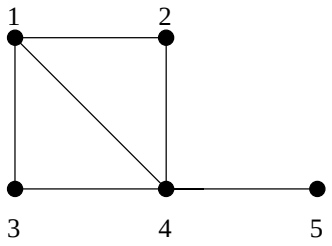
(ahol c_0 is egy konstans). Ilyenkor persze a b tömb hossza is $c_0 n$ és egy extra kinullázással kell kezdeni, majd a kiolvasáskor eltekintünk a zérus elemektől.

3.4. Hogyan tároljunk gráfokat?

3.4.1. Szomszédossági tömbök és listák

A 2.4. szakaszban már megismerkedtünk a gráfok szomszédossági és illeszkedési mátrixokkal való megadásával. Egy v pontú és e élű G gráf szomszédossági mátrixa v^2, illeszkedési mátrixa ve helyet foglal el. Egyszerűség kedvéért foglalkozzunk csak egyszerű gráfokkal (melyek nem tartalmaznak hurokéleket és többszörös éleket). Ilyenkor $e \leq v(v-1)/2$ irányítatlan gráfok esetén és $e \leq v(v-1)$ irányított gráfok esetén.
Azonnal látszik, hogy az illeszkedési mátrix mindig feleslegesen sok helyet foglal el (hisz a ve szám között $(v-2)e$ darab zérus van); és a legtöbb esetben a szomszédossági mátrixszal is ez a probléma, hisz ha egy gráf **ritka** (vagyis cv^2-nél jóval kevesebb éle van), akkor ebben a mátrixban is rengeteg a zérus. A feleslegesen nagy tárigény mellett a gráfelméleti algoritmusok lépésszámát (tehát időigényét) is növelné, ha a hasznos információkhoz csak számos felesleges zérus kiolvasásán keresztül jutnánk.
Ezért gyakran hasznos a gráfot úgy tárolni, hogy minden pontjához felsoroljuk a szomszédjait. Pl. a 3.1. ábrán látható gráfra ez az ábra melletti „táblázatot” adná.

2 3 4
1 4
1 4
1 2 3 5
4



3.1. ábra.

Mivel ezek a szomszédossági listák általában különböző hosszúságúak, érdemes őket egy nagy közös tömbben tárolni, és egy külön tömbben tárolni a „mutatókat” (pointer), hogy honnét kezdve kell olvasni egy adott pont szomszédait. Így a fenti „táblázat” az alábbi két tömbbel helyettesíthető:

2 3 4 1 4 1 4 1 2 3 5 4 és 1 4 6 8 12

Ezt a két tömböt nevezzük röviden **szomszédossági tömb**nek. Az 1-1 ponthoz tartozó listák külön-külön lehetnek rendezettek (mint példánkban is), így a 3.1. szakaszban látottak szerint hamarabb ellenőrizhetjük, hogy egy pont szomszédai között szerepel-e egy adott másik pont.
Az első tömb hossza nyilván a fokszámok összege, vagyis $2e$, a második tömbé pedig v. Így a teljes tárigény $2e+v$. Ez az elképzelhető minimális tárigénynek közel kétszerese (az $\{i,j\}$ élt i szomszédainál is, j szomszédainál is felsoroljuk); látni fogjuk azonban, hogy ez a redundancia busásan megtérül.
Irányított gráfok esetén megtehetnénk, hogy minden i ponthoz felsoroljuk azokat a j pontokat, melyekbe (i,j) irányított él vezet i-ből; vagy azokat a k pontokat, melyekből (k,i) irányított él vezet i-be. Sok esetben az a legjobb, ha mindkét listát megadjuk: a kétszeres tárigény számos algoritmusnál nagyságrenddel csökkenti a lépésszám-igényt.
Rendezett szomszédossági tömbről beszélünk, ha az egyes pontok szomszédai már növekvő sorrendben elhelyezve kerülnek tárolásra (a fenti példában is ez volt a helyzet). Világos, hogy a rendezések elvégzése további időt igényel, de ez később megtérülhet, ld. a 3.1. Táblázatot.

3.4.2. Láncolt szomszédossági listák

Már a 3.2. szakaszban láttuk, hogy hiába tudjuk $\log_2 n$ darab összehasonlítással megtalálni egy beszúrandó (vagy elhagyandó) elem helyét az n tagú sorozatban, ha az utána következők eggyel eltolása akár n darab további lépést is igényelhet. Olyan algoritmusok esetén, ahol gyakran kell a gráfból egy élt (vagy akár pontot) elhagyni, sok esetben előnyös lehet ezért egy valamivel bonyolultabb adatstruktúra. Ezért egy olyan listát adunk, aminek első tömbje a szomszédossági lista elemeit tetszőleges sorrendben tartalmazhatja.
Változatlanul a 3.1. ábra gráfján szemléltetve a $2e$ hosszú és a v hosszú tömbök helyett most két darab, egyenként $2e$ hosszú és változatlanul egy darab v hosszú tömb kell:

2	1	1	3	2	1	4	4	5	3	4	4		1	2	6	3	11
4	12	5	7	10	8	$*$	$*$	$*$	9	$*$	$*$						

Most is a v hosszú tömb i-edik eleme mutatja meg, hogy hol kezdjük el az i-edik pont szomszédainak kiolvasását az első $2e$ hosszú tömbből. Azt azonban az alatta lévő szám (tehát a második $2e$ hosszú tömb megfelelő eleme) mutatja meg, hogy hol folytassuk az olvasást, illetve egy speciális $*$ szimbólum jelzi, hogy vége van a listának.
Világos, hogy ezzel a tárigényt közel megdupláztuk. Viszont például a $\{2,4\}$ él elhagyása esetén nincs más teendőnk, csak a második tömb 12-es elemét $*$-ra és 5-ös elemét 10-re cserélni. Hasonlóképp, ha a gráfhoz hozzá akarnánk venni egy

$\{3,5\}$ élt, akkor a második tömbben a 8-adik elemet $*$-ról 13-ra és a 11-edik elemet $*$-ról 14-re változtatnánk és a 13. és 14. eleme az első tömbnek 5 ill. 3, a második tömbnek pedig $*$ és $*$ lenne.

3.4.3. További megjegyzések

Attól függően, hogy milyen gráfelméleti műveletet akarunk elvégezni, hol az egyik, hol a másik adatstruktúra bizonyul különösen jónak (ld. a 3.1. Táblázatot). Fontos látni, hogy nincs minden másnál jobb, előnyösebb tárolási mód.
Ugyanakkor az is könnyen belátható, hogy ezek az adatstruktúrák kb. cv^2 lépésben egymásba átalakíthatóak. Ha tehát csak az a kérdés, hogy egy konkrét gráfelméleti probléma polinom időben eldönthető-e, akkor az adatstruktúra megválasztása kevéssé jelentős. Ha viszont v értéke nagyon nagy (pl. a nagy bonyolultságú integrált (VLSI) áramkörök tervezésénél) és ezért csak v-vel, vagy legfeljebb $v\log v$-vel arányos lépésszámú algoritmusok felelnek meg, akkor a megfelelő adatstruktúra kiválasztása kritikus lehet.

3.1. táblázat.
Tárigény és a különféle gráfelméleti műveletek időigénye, ha a gráfot szomszédossági mátrixszal (**A**), szomszédossági tömbbel (**B**), rendezett szomszédossági tömbbel (**C**) vagy láncolt szomszédossági listával (**D**) adjuk meg.

	A	**B**	**C**	**D**
Tárigény	v^2	$2e+v$	$2e+v$	$4e+v$
Két pont szomszédosságának eldöntése	1	d	$\log d$	d
Pont szomszédainak megjelölése	v	d	d	d
Minden él megjelölése	v^2	e	e	e
Új él hozzávétele	1	e	e	1
Régi él elvétele	1	e	e	d
Régi pont elvétele	v	e	e	$\min(e,d^2)$

jelölések: v pontszám, e élszám, d maximális fokszám

3.5. NP-beli problémák

3.5.1. A P, NP és NP-teljes problémaosztályok

Eddig nem sokat foglalkoztunk kifejezetten algoritmusokkal, de sok eddig tárgyalt problémával kapcsolatban felmerül a kérdés, hogyan tudnánk számítógéppel eldönteni, hogy például rendelkezik-e egy adott tulajdonsággal egy bizonyos gráf. **El-**

döntési problémának nevezzük az olyan problémákat, amikor az input egy olyan kérdés (pl. „G összefüggő-e?”), amire az output „igen” vagy „nem”. Az eldöntési problémák azon osztályát, amelyek az input méretének polinomiális függvényével felülről becsülhető időben megoldhatók, jelöljük **P**-vel. Például egy gráf összefüggőségének eldöntése **P**-ben van.
Nézzük meg, mit is jelent a gyakorlatban, hogy egy problémát meg tudunk-e oldani polinomiális időben vagy nem. Tegyük fel, hogy az A algoritmus 2^n lépésben működik, míg a B algoritmus $3000n^5$ lépésben, és van egy számítógépünk, ami másodpercenként 10^{12} műveletet végez. (n itt például a gráf pontjainak a száma lehet.) Ha 1 percig használhatjuk a gépet, akkor az A algoritmus segítségével csak olyan problémákat tudunk megoldani, ahol $n \leq \lfloor \log_2 6 \cdot 10^{13} \rfloor = 45$, a B algoritmussal viszont olyanokat, ahol $n \leq \lfloor \sqrt[5]{6 \cdot 10^{13}/3000} \rfloor = 114$. Ha azonban egy óra áll rendelkezésünkre, akkor az A algoritmussal csak 51-re, a B-vel 260-re emelkedik a megoldható probléma mérete.
„Sajnos” vannak olyan problémák, amelyekre eddig senki sem tudott polinomiális algoritmust adni. Ilyen például a Hamilton-kör probléma:

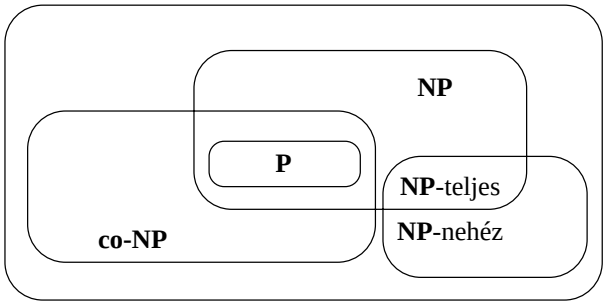
(H) Input: G gráf. **Kérdés:** Van-e a G-ben Hamilton-kör?

Ha most egy varázsló megmondja nekünk, hogy G-ben van Hamilton-kör, és meg is mutatja, melyik kör az, akkor én a vizsgán be tudom bizonyítani a tanárnak, hogy ebben a gráfban van Hamilton-kör. Ha azonban nincs a gráfban Hamilton-kör, akkor a varázsló sem tud jobbat, minthogy minden egyes körről megmutatja nekem, hogy az nem Hamilton-kör. Ezt viszont egy nagyobb gráf esetén esetleg egy egész félévig is magyarázhatnám a tanárnak. Az olyan eldöntési problémák osztályát, amelyeknél az igenlő válasz esetén a varázsló biztosan tud olyan segítséget adni, amellyel polinom időben be tudjuk bizonyítani, hogy a válasz igen, **NP**-nek nevezzük. Pontosabban, egy eldöntési probléma akkor **NP**-beli, ha minden olyan I inputhoz, melyre a válasz igenlő, létezik egy olyan, I-től függő T „tanú”, hogy egyrészt T hossza felülről becsülhető I hosszának egy polinomjával, másrészt I és T ismeretében polinom időben ellenőrizhető, hogy a válasz igenlő.
Természetesen vannak olyan problémák is, amelyeknél a nemleges választ tudjuk polinom időben bebizonyítani, ha segít a varázsló. Az ilyen problémák osztálya a **co-NP** osztály. Egyből adódik, hogy ilyen a következő.

(H') Input: G gráf. **Kérdés:** Igaz-e, hogy a G-ben nincs Hamilton-kör?

Az eddigiekből nyilvánvaló, hogy $\mathbf{P} \subseteq \mathbf{NP}$, hiszen **P**-beli problémák esetén polinom időben meg tudjuk határozni a választ és ezáltal, a varázsló segítsége nélkül, be is tudjuk bizonyítani, hogy a válasz igenlő. A bonyolultságelmélet talán legérdekesebb megoldatlan kérdése, hogy itt valódi tartalmazás vagy egyenlőség áll fenn.
A 3.2. ábrán, mely a fejezetben szereplő problémaosztályok **legvalószínűbb** (de nem biztos) viszonyát mutatja, látható, hogy nyilván vannak problémák amelyek $\mathbf{NP} \cap \mathbf{co\text{-}NP}$-ben vannak. Ilyenek például:

(P1) Input: G páros gráf. **Kérdés:** Van-e a G-ben teljes párosítás?



3.2. ábra.

(P2) **Input:** H hálózat, $k \geq 0$ valós szám **Kérdés:** H-ban van-e legalább k értékű folyam?

(P3) **Input:** G gráf. **Kérdés:** A G gráf síkbarajzolható-e?

Ezek valóban **NP**-ben vannak, hiszen ha a varázsló megmondja nekünk a párosítást, a folyamot, illetve a síkba lerajzolt gráfot, akkor ezek könnyen ellenőrizhetők. Ugyanakkor, ha a varázsló mutat egy halmazt, melyre $|N(X)| < |X|$ (P1); egy k-nál kisebb kapacitású (s,t) vágást (P2); illetve egy részgráfot, ami topológikusan izomorf valamelyik Kuratowski–gráffal (P3), akkor a nemleges választ is polinom időben bebizonyíthatjuk.
Ezek a problémák egyébként nemcsak **NP** $\cap$ **co-NP**-ben, hanem **P**-ben is benne vannak. Vannak akik azt sejtik, hogy **NP** $\cap$ **co-NP** $=$ **P**, hiszen még egyetlen ilyen problémáról sem látták be, hogy nincs **P**-ben, és a legtöbb **NP** $\cap$ **co-NP**-beli problémáról előbb-utóbb kiderült, hogy **P**-ben van.
Tegyük fel, hogy most egy olyan számítógépünk van, amely a szokásos műveletek mellett még egy P_2 problémát is meg tud oldani egységnyi idő alatt. Ha evvel a számítógéppel polinom időben meg tudjuk oldani a P_1 problémát, akkor azt mondjuk, hogy P_1 polinomiálisan **visszavezethető** a P_2 problémára.
Ha $P_2 \in$ **P**, akkor nyilván $P_1 \in$ **P**. Egy problémát **NP-nehéznek** nevezünk, ha minden **NP**-beli probléma visszavezethető rá. Ha ez a probléma maga is eleme **NP**-nek, akkor **NP-teljesnek** hívjuk. Ha egy **NP**-teljes problémát meg tudnánk oldani polinom időben, akkor minden **NP**-beli probléma is megoldható lenne polinom időben. Cook és Levin bizonyították, hogy létezik **NP**-teljes probléma. Később sikerült belátni, hogy a Hamilton-kör probléma **NP**-teljes. Ugyancsak fontos **NP**-teljes probléma a Klikk–probléma, és a pontszínezési probléma:

3.5.1. Tétel. *A következő problémák* **NP***-teljesek:*

(H) ***Input:*** *G gráf.* ***Kérdés:*** *Van-e G-ben Hamilton-kör?*

(K) ***Input:*** *G gráf,* $k \geq 1$ *egész szám.* ***Kérdés:*** *Van-e a G gráfban k-nál nagyobb pontszámú teljes részgráf?*

(S) ***Input:*** *G gráf.* ***Kérdés:*** *Legyen $p \geq 3$. Igaz-e, hogy $\chi(G) \leq p$?*

Mire lehet használni ezt az elméletet? Ha van egy problémánk (kaptuk gyakorlaton), amire nem találunk polinomiális algoritmust, viszont nyilván **NP**-ben van, akkor megpróbálunk visszavezetni a mi problémánkra egy **NP**-teljes problémát. Ez azt jelenti, hogy a mi problémánk is **NP**-teljes. Ekkor megmondhatjuk a gyakorlatvezetőnek, hogy a probléma „gyakorlatilag megoldhatatlan", mivel ha megoldottuk volna, akkor egyben polinomiális algoritmust találtunk volna a sok száz **NP**-teljes problémára is, amit már hosszú ideje sok okos ember próbál kitalálni. Ennek a gyakorlatvezető nem biztos, hogy örülni fog, de nem buktat meg amiatt, hogy nem oldottuk meg a problémát.
Nézzünk néhány példát, hogyan bizonyíthatjuk egy probléma **NP**-teljességét!

3.5.2. Tétel. *A következő probléma* **NP***-teljes:*

(HU) ***Input:*** *G gráf.* ***Kérdés:*** *Van-e G-ben Hamilton-út?*

BIZONYÍTÁS: Először belátjuk, hogy a probléma **NP**-beli. Ha a gráfban van Hamilton-út, akkor maga a Hamilton-út egy tanú, nyilván polinom méretben leírható és polinom időben belátható, hogy ő tényleg Hamilton-út.
Az **NP**-nehézség belátásához visszavezetjük a (H) Hamilton-kör problémát a (HU) Hamilton-út problémára. Inputként kapunk tehát egy gráfot, melyről meg kell mondanunk, hogy van-e benne Hamilton-kör. Ennek megválaszolásához felhasználhatjuk, hogy tetszőleges G' gráfról meg tudjuk mondani, van-e benne Hamilton-út.
Konstruáljuk meg G-ből a következő G' gráfot. Legyen $v_1 \in V(G)$ egy tetszőleges pont. Vegyünk fel egy új v_1' pontot és kössük össze v_1 összes szomszédjával. Ezek után vegyünk fel még két új pontot, az egyiket, w-t kössük össze v_1-gyel, a másikat w'-t pedig v_1'-vel.
Belátjuk, hogy az így kapott G' gráfban akkor és csak akkor van Hamilton-út, ha G-ben van Hamilton-kör. Ha $v_1, v_2, \ldots, v_n$ egy Hamilton-kör G-ben, akkor $w, v_1, v_2, \ldots, v_n, v_1', w'$ nyilván egy Hamilton-út G'-ben. Ha G'-ben van Hamilton-út, akkor ennek két végpontja csak w és w' lehet, hiszen ezek első fokúak. Legyen tehát $w, v_1, v_2, \ldots, v_n, v_1', w'$ egy Hamilton-út G'-ben, ekkor $v_1, v_2, \ldots, v_n$ nyilván egy Hamilton-kör G-ben.
Így ha megnézzük, G'-ben van-e Hamilton-út, meg tudjuk mondani azt is, hogy G-ben van-e Hamilton-kör. □

3.5.3. Tétel. *A következő probléma* **NP***-teljes:*

(Sp) ***Input:*** *G gráf.* ***Kérdés:*** *Legyen $p \geq 4$. Igaz-e, hogy $\chi(G) \leq p$?*

BIZONYÍTÁS: Először belátjuk, hogy a probléma **NP**-beli. Ha G kiszínezhető p színnel, akkor egy ilyen színezés megfelelő tanú.
Az **NP**-nehézség belátásához visszavezetjük az (S) 3-színezési problémát az (Sp) p-színezési problémára. Inputként kapunk tehát egy G gráfot, amelyről el kell döntenünk, hogy kiszínezhető-e 3 színnel. Ennek megválaszolásához felhasználhatjuk,

hogy tetszőleges G' gráfról el tudjuk dönteni, hogy kiszínezhető-e p színnel, ahol $p \geq 4$ egy rögzített szám.
Konstruáljuk meg G-ből a következő G' gráfot. Vegyünk fel $p-3$ darab új pontot $u_1, \ldots, u_{p-3}$-at, és ezeket kössük össze egymással is és G összes pontjával is.
Belátjuk, hogy az így kapott G' gráf akkor és csak akkor színezhető ki p színnel, ha G kiszínezhető 3 színnel.
Ha G pontjai kiszínezhetők 3 színnel, akkor az új pontok mindegyikét egy-egy újabb színnel kiszínezve sikerül G'-t kiszíneznünk p színnel. Ha G' kiszínezhető p színnel, akkor bármely ilyen színezés esetén az $u_1, \ldots, u_{p-3}$ pontok színe egymástól és G pontjainak színétől is különbözniük kell, hiszen páronként szomszédosak. Ezért G pontjainak a színei csak a maradék 3 szín közül kerülhetnek ki, és két azonos színű nem lehet szomszédos G-ben, hiszen G'-ben sem lehetett az.
Így ha megnézzük, hogy G' kiszínezhető-e p színnel, akkor meg tudjuk mondani azt is, hogy G kiszínezhető-e 3 színnel. □

3.5.4. Tétel. *A következő probléma* **NP***-teljes:*

(RI) ***Input:*** *G, H gráfok.* ***Kérdés:*** *Van-e G-nek H-val izomorf részgráfja?*

BIZONYÍTÁS: Először belátjuk, hogy a probléma **NP**-beli. Ha G-nek van H-val izomorf részgráfja, akkor ennek a részgráfnak a megadása, valamint a részgráf és H pontjai közötti éltartó megfeleltetés megadása megfelelő tanú.
Az **NP**-nehézség belátásához visszavezetjük a (H) Hamilton-kör problémát az (RI) részgráf-izomorfia problémára. Inputként kapunk tehát egy G gráfot, amelyről el kell döntenünk, hogy van-e benne Hamilton-kör. Ennek megválaszolásához felhasználhatjuk, hogy tetszőleges G és H gráf esetén el tudjuk dönteni, van-e G-nek H-val izomorf részgráfja.
Ha G egy n pontú gráf, akkor legyen H egy n pontú kör. Világos, hogy akkor és csak akkor van G-ben Hamilton-kör, ha G-nek van H-val izomorf részgráfja. Ha tehát ezt megnézzük, akkor meg tudjuk mondani, van-e G-ben Hamilton-kör. □

Ennél a bizonyításnál azt használtuk ki, hogy a Hamilton-kör probléma speciális esete a részgráf-izomorfia problémának. Általában is igaz, hogy ha egy probléma **NP**-teljes, akkor az ennél általánosabb **NP**-beli eldöntési problémák is **NP**-teljesek. Ha belegondolunk, nyilvánvaló, hogy ha nehéz megoldani egy problémát, akkor egy általánosabbat nem lehet könnyebben megoldani.
Nem igaz azonban, hogy ha egy probléma **NP**-teljes, akkor ennek speciális esete feltétlenül **NP**-teljes lenne. Például **NP**-teljes annak eldöntése, hogy egy gráf 5 színnel kiszínezhető-e, de síkbarajzolható gráfokról tudjuk, hogy mindig kiszínezhetőek 5 színnel (2.11.14. tétel), azaz ebben a speciális esetben könnyen megválaszolható a kérdés.

3.5.2. A nem polinomrendű algoritmus is lehet jó

A valóságban persze a történetnek nem a végét, hanem az elejét kell, hogy jelentse, ha egy problémáról belátjuk, hogy **NP**-teljes. Ilyenkor el kell ejtenünk azt a cél-

kitűzést, hogy olyan algoritmust konstruáljunk, melynek lépésszáma a legrosszabb esetben is az input hosszának polinomja, azonban még számos lehetőségünk van.

(1) A modellalkotáskor nem feledkeztünk-e el valamiről (hisz számos **NP**-teljes problémának sok polinomrendben megoldható speciális esete van)? Például a leghosszabb irányított út megkeresése egy tetszőleges irányított gráfban **NP**-nehéz (speciális esetként tartalmazza az irányított Hamilton út létezésének eldöntésére vonatkozó **NP**-teljes feladatot), de a 2.10.3. pontban láttuk, hogy létezik rá gyors algoritmus, ha a gráfban nincs irányított kör.

Másik példa, hogy – szemben a 2.9.4. pontban tanult eljárással, ami meghatározza egy hálózatban a minimális kapacitású vágást – a maximális kapacitású vágás meghatározása általában **NP**-nehéz, de síkbarajzolható gráfokra ismeretes rá polinomrendű algoritmus.

(2) Tényleg olyan nagyméretű-e a feladat, hogy exponenciális rendű algoritmus már nem jöhet szóba? Pl. a Hamilton-kör problémára már többszáz pontú gráfokra is ismert elfogadható idejű algoritmus. Másik példa, hogy az n-pontú gráfokban a maximális független ponthalmaz meghatározása **NP**-nehéz, de a minden részhalmazt megvizsgáló, lényegileg 2^n lépésszámú algoritmus helyett $1,3^n$ lépésszámú is készíthető.

(3) Sokszor olyan algoritmust használunk, melynek lépésszáma a legrosszabb esetben exponenciális, de az esetek többségében polinomiális. Tekintsük például a 3.2. Táblázat baloldali oszlopának utolsó feladatát. Léteznek rá polinomrendű algoritmusok (Hacsijan, Karmarkar), de felfedezésük idején már közel 30 éve ismeretes volt a szimplex-módszer, ami egyszerűsége révén ma is a legnépszerűbb, és ugyan konstruálható olyan input, melyre a lépésszáma exponenciális, de az átlagos lépésszáma nagyon kedvező.

(4) Gyakran exponenciális lépésszámú algoritmussal tudnánk csak megtalálni egy feladat optimális megoldását, de ismeretesek olyan polinomrendű algoritmusok, melyek az optimálishoz közeli megoldást adnak. Ha ez utóbbi megoldás bizonyíthatóan közel van az optimumhoz, akkor gyakran ez is kielégítő. Például **NP**-teljes feladat eldönteni egy egyszerű G gráfról, hogy az élkromatikus száma legfeljebb k-e, ugyanakkor Vizing 2.11.17. tételéből tudjuk, hogy az élkromatikus szám vagy Δ, vagy $\Delta+1$.

Másik példa a ládapakolási–feladat. Próbáljuk meg a $V_1, V_2, \ldots, V_k$ térfogatú tárgyakat minél kevesebb V térfogatú ládába bepakolni. (Feltesszük, hogy $V_i \leq V$ minden i-re, és hogy ha néhány tárgy össztérfogata legfeljebb V, akkor be is tehetők ugyanabba a ládába; más feltételt már nem kell kielégítenünk.) **NP**-teljes annak az eldöntése, hogy $(\sum V_i)/V$ darab láda elég-e. Ha azonban sorba vesszük a tárgyakat és mindegyiket a legelső olyan ládába tesszük, amelyikbe belefér („sietős algoritmus”), akkor legfeljebb $1,7$-szer annyi ládát fogunk felhasználni, mint amennyi az optimális megoldáshoz kellene. Sőt belátható, hogy a „hiba” 70%-ról 22%-ra szorítható le, ha a tárgyakat térfogatuk szerint csökkenő sorrendbe rendezzük és a „sietős” algoritmust a legnagyobbal kezdjük.

(5) Az is előfordul, hogy olyan polinom rendű algoritmust tudunk készíteni, mely nem biztosan, csak nagy valószínűséggel ad helyes választ. A 4.6. szakaszban fo-

gunk erre példákat látni, pl. olyan prímtesztelő algoritmust, mely vagy azt mondja egy beadott számra, hogy az összetett, és akkor ez biztos igaz, vagy azt, hogy prím, és akkor ez legfeljebb $1/2^{300}$ valószínűséggel lehet hamis.

3.2. táblázat. Nevezetes polinomrendű ill. **NP**-teljes feladatok

	P-beli	**NP**-teljes
1	Van-e G-ben legalább k darab független él?	Van-e G-ben legalább k darab független pont?
2	Lefogható-e G minden pontja legfeljebb k éllel?	Lefogható-e G minden éle legfeljebb k ponttal?
3	Van-e G-ben legfeljebb k hosszúságú út?	Van-e G-ben legalább k hosszúságú út?
4	Van-e G-ben legfeljebb k hosszúságú kör?	Van-e G-ben legalább k hosszúságú kör?
5	Kiszínezhetőek-e G pontjai legfeljebb 2 színnel?	Kiszínezhetőek-e G pontjai legfeljebb k ($k \geq 3$) színnel?
6a	Van-e egy hálózatban legfeljebb k értékű vágás?	Van-e egy hálózatban legalább k értékű vágás?
6b	Van-e egy egytermékes hálózatban legalább k értékű folyam?	Van-e egy többtermékes hálózatban legalább k értékű folyam?
7	Van-e az $\{\mathbf{Ax} \leq b, \mathbf{x} \geq 0\}$ feltételeket kielégítő valós $\mathbf{x}$ vektorok között olyan, amelyre $\mathbf{c}^T\mathbf{x} \geq k$?	Van-e az ezen feltételeket kielégítő egész koordinátájú $\mathbf{x}$ vektorok között olyan, amelyre $\mathbf{c}^T\mathbf{x} \geq k$?

Megjegyzések

(1) Az első 4 problémapár második feladata is **P**-beli, ha k rögzített (nem része az inputnak); az 5. probléma viszont már $k = 3$ esetén is **NP**-teljes.

(2) **NP**-teljes probléma, hogy adott G és H gráf esetén van-e G-nek H-val izomorf részgráfja.

(3) Nem ismeretes a bonyolultsága annak a problémának, hogy két adott gráf izomorf-e.

4. fejezet

Számelmélet, algoritmusok az egész számok körében

4.1. Az alapműveletek

Mostanra hozzászoktunk ahhoz, hogy egy algoritmust akkor tekintsünk „jónak”, ha lépésszáma a legrosszabb esetben is felülről becsülhető az input hosszának polinomjával. Mi mondható ilyen szempontból azokról az algoritmusokról, amiket az általános iskola alsó tagozatában tanultunk és írásbeli összeadásnak, kivonásnak stb. neveztünk?

Egy k-jegyű x szám nyilván 10^{k-1} és 10^k-1 között van. Így leírásához $\lceil \log_{10} x \rceil$ számjegy kellett. Ne törődjünk azzal, hogy eddig 2 alapú logaritmusokról volt szó, hisz tudjuk, hogy $\log_a x = c \cdot \log_b x$, ahol c értéke (t.i. $\frac{\lg b}{\lg a}$) csak a-tól és b-től függ (vagyis x-től nem). Így az a kijelentés, hogy egy mennyiség $c \cdot \log x$-szel becsülhető, akkor is értelmes, ha a logaritmus alapját nem rögzítjük előre le (csak persze akkor c értékét sem tudjuk megmondani).

Ha tehát megadunk két x, y számot, hogy az összegét, különbségét stb. számoljuk ki, akkor az input hossza $\lceil \log_{10} x \rceil + \lceil \log_{10} y \rceil \approx \log_{10} xy$ miatt xy logaritmusával arányos. Nyilván az írásbeli összeadás és kivonás lépésszáma a számjegyek számával arányos, ezek tehát polinom rendű (sőt, lineáris) algoritmusok. Könnyű végiggondolni, hogy az írásbeli szorzás és osztás is polinomrendű algoritmusok (csak nem lineárisak).

Ugyanakkor nyilvánvaló, hogy a hatványozás nem végezhető el polinomrendben, hisz pl. 2^x végeredményének puszta kiírásához (tehát nem a kiszámításához) már $\log 2^x = x$ lépés kell, ez pedig az input hosszának (vagyis $\log x$-nek) exponenciális függvénye.

A szakaszt annak bemutatásával zárjuk, hogy az adott két a, b egész szám legnagyobb közös osztóját, $d(a,b)$-t meghatározó ún. euklideszi algoritmus is polinomrendű. Idézzük fel az algoritmust! Ha $a > b$, akkor az $a : b$ maradékos osztást

elvégezzük, majd b-t osztjuk a maradékkal stb.:

$$\begin{array}{rcll} a & = & h_1 b + m_1 & (0 \le m_1 < b) \\ b & = & h_2 m_1 + m_2 & (0 \le m_2 < m_1) \\ m_1 & = & h_3 m_2 + m_3 & (0 \le m_3 < m_2) \\ & \vdots & & \vdots \end{array}$$

A k-ik lépésben a hányadost h_k-val, a maradékot m_k-val jelöljük. Az eljárás akkor ér véget, ha nincs az osztásnak maradéka, vagyis

$$m_{n-2} = h_n m_{n-1}$$

Ekkor persze $m_{n-3} = h_{n-1} m_{n-2} + m_{n-1} = (h_{n-1} h_n + 1) m_{n-1}$, és ugyanígy visszahelyettesítve minden kisebb indexű m, végül a és b is m_{n-1} konstansszorosa lesz, tehát m_{n-1} közös osztója a-nak és b-nek. Megfordítva, a és b tetszőleges közös osztója m_1-nek is osztója lesz (az $a = h_1 b + m_1$ összefüggés miatt), majd minden nagyobb indexű m-nek, végül m_{n-1}-nek is. Tehát $m_{n-1} = d(a,b)$.

Korábban már láttuk, hogy az osztás polinomrendű, tehát csak azt kell belátnunk, hogy n nem túl nagy. Egzakt bizonyítás helyett ezt azzal szemléltetjük, hogy végiggondoljuk, mikor a legnagyobb az n. Nyilván akkor, ha az $a, b, m_1, m_2, \ldots$ sorozat viszonylag lassan csökken, vagyis ha h_n kivételével minden hányados 1. Ekkor viszont az $m_{n-2}, m_{n-1}, \ldots m_1, b, a$ sorozatot ugyanazzal a rekurzióval képezhetjük, mint a Fibonacci-félét, tehát a t-ik tag nagyságrendben p^t konstansszorosa, ahol $p = (\sqrt{5}+1)/2$. Következésképp $n \approx log_p a$, tehát az input hosszának konstansszorosa.

Miért nagy jelentőségű az euklideszi algoritmus hatékonysága? Idézzük először fel, hogy **prímszámnak** hívunk egy egynél nagyobb pozitív p számot, ha nincs valódi osztója, vagyis ha a pozitív m szám osztója p-nek, akkor vagy $m = 1$ vagy $m = p$ teljesül. A **számelmélet alaptétele** szerint minden pozitív n szám a sorrendtől eltekintve egyértelműen előáll

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots$$

alakban, ahol a p_i számok a prímek, az α_i számok nemnegatív egészek. Ezt a szám **kanonikus alakjának** szokás nevezni. (Figyeljük meg, hogy jóllehet végtelen sok prímszám van, csak véges sok kitevő lesz pozitív, tehát csak véges sok 1-től különböző szám szorzatát képezzük.)

Ha az általános iskolában elő akartuk állítani az a és b számok legnagyobb közös osztóját, akkor először e számok $a = \prod p_i^{\alpha_1}$, ill. $b = \prod p_i^{\beta_1}$ kanonikus alakját határoztuk meg, majd a

$$d(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \ldots$$

képletet alkalmaztuk. Például $72 = 2^3 \cdot 3^2$; $378 = 2 \cdot 3^3 \cdot 7$, a legnagyobb közös osztójuk $d(72,378) = 2^1 \cdot 3^2 \cdot 7^0 = 18$.

Látszólag ez az eljárás egyszerűbb az euklideszi algoritmusnál. Látni fogjuk azonban, hogy egy n szám kanonikus alakját nem tudjuk polinom időben előállítani (tehát legfeljebb $c(\log n)^k$ lépésszámú algoritmussal, ahol c és k rögzített számok). Így

két elég nagy (többszáz számjegyből álló) egész szám legnagyobb közös osztójának tényleges előállítása mai tudásunk szerint csak az euklideszi algoritmussal lehetséges.

4.2. Kongruenciák, maradékosztályok

Legyen $m > 1$ egy rögzített egész szám. Akkor mondjuk, hogy a **kongruens** b-vel az m modulusra vonatkozólag (jelölve $a \equiv b \pmod{m}$), ha az a és a b számok m-mel osztva ugyanazt a maradékot adják. Ezzel osztályokba soroljuk az egész számok halmazát. Egy–egy ilyen osztályt hívunk **maradékosztálynak**. Más szóval egy osztályt alkot az összes m-mel osztható szám, egy másikat azok a számok, melyek m-mel osztva egy maradékot adnak, egy újabb osztályt azok, melyek kettő maradékot adnak stb.
Nyilván $a \equiv b \pmod{m}$ akkor és csak akkor teljesül, ha $a-b$ osztható m-mel. Ennek felhasználásával belátható, hogy ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$ teljesülnek, akkor

$$a+c \equiv b+d,\ a-c \equiv b-d,\ ac \equiv bd \pmod{m}.$$

A legutolsó kongruenciát például úgy látjuk be, hogy az

$$ac-bd = ac-bc+bc-bd = c(a-b)+b(c-d)$$

azonos átalakítást alkalmazzuk: Ha $a-b$ és $c-d$ is osztható m-mel, akkor $ac-bd$ is. Szabad tehát azonos modulusú kongruenciákat összeadni, kivonni, összeszorozni. Speciálisan érvényes marad egy kongruencia, ha mindkét oldalához ugyanazt az egész számot adjuk, vagy ha mindkét oldalát ugyanazzal az egész számmal szorozzuk.
Azonos modulusú kongruenciákkal tehát „majdnem ugyanúgy” számolhatunk, mint az egyenletekkel. Nem mindig oszthatjuk el azonban a kongruencia két oldalát ugyanazzal az a számmal, hiszen például $10 \equiv 70 \pmod{15}$, de $1 \not\equiv 7 \pmod{15}$.
Tegyük fel, hogy $ac \equiv bc \pmod{m}$ teljesül, vagyis szeretnénk mindkét oldalt c-vel osztani. Ha $d(c,m) = 1$, vagyis a c és m számok **relatív prímek**, akkor ebből következik, hogy $a \equiv b \pmod{m}$. Csakugyan, ha tudjuk, hogy $ac-bc = c(a-b)$ osztható m-mel, és c és m relatív prímek, akkor m minden prímtényezője szükségképp $a-b$ osztója volt. Ha viszont c és m nem relatív prímek, akkor a c-vel való osztáskor megváltozik a modulus:

4.2.1. Tétel. *Legyen $ac \equiv bc \pmod{m}$ és $d(c,m) = t$. Ekkor $a \equiv b \pmod{\frac{m}{t}}$ teljesül.*

BIZONYÍTÁS: Legyen $c = tc'$ és $m = tm'$. Ekkor a c' és m' egész számok már relatív prímek. Tudjuk, hogy $ac-bc = c(a-b) = tc'(a-b)$ osztható $m = tm'$-vel, vagyis $c'(a-b)$ osztható m'-vel. Mivel $d(c',m') = 1$, így $a-b$ osztható $m' = \frac{m}{t}$-vel. □

A fenti példában $10 \equiv 70 \pmod{15}$ miatt $c = 10$-zel akarunk osztani. Mivel $d(10,15) = 5$, ezért $1 \equiv 7 \pmod{\frac{15}{5}}$ következik.
Vegyük észre, hogy a bizonyítás során felhasználtuk az alábbi fontos észrevételt:

4.2.2. Tétel. *Ha p prím és osztója egy ab szorzatnak, akkor p osztója a-nek vagy b-nek (vagy mindkettőnek).* □

Ez a tulajdonság jellemzi is a prímszámokat, szokás ezért **prím–tulajdonságnak** is nevezni. (Gondoljunk végig, hogy ha n nem prím, hanem előáll két egynél nagyobb a és b szám szorzataként, akkor n osztója ab-nek, de nem osztója sem a-nak, sem b-nek.)
Később az absztrakt algebrában majd látunk példát olyan gyűrűkre, ahol ez a prím tulajdonság nem ekvivalens azzal a „felbonthatatlansággal”, ahogy a prímszámokat definiáltuk. Amíg azonban csak az egész számok körében vizsgálódunk, addig ez a probléma nem jelentkezik.

4.3. Műveletek maradékosztályokkal

A $\bmod m$ maradékosztályok körében is beszélhetünk az alapműveletekről, akár az egész számok esetén. Például $m = 7$ választással

$$5+6 \equiv 4, \quad 5-6 \equiv 6, \quad 5\cdot 6 \equiv 2 \pmod 7$$

hisz $5+6=11$ és ez héttel osztva 4 maradékot ad stb. Prím–modulus esetén (a nullán kívül mindennel) még osztani is lehet, pl. $5/6$ nyilván 2 (mert $2\cdot 6 \equiv 5 \pmod 7$). Ha a modulus összetett szám, akkor az

$$ax \equiv b \pmod m \qquad (*)$$

feladatnak (adott a,b,m esetén) nem mindig van megoldása: Pl. $6x \equiv 5 \pmod 7$-ről már láttuk, hogy megoldása az $x \equiv 2 \pmod 7$ maradékosztály, ugyanakkor

$$4x \equiv 3 \pmod 6 \quad \text{és} \quad 4x \equiv 2 \pmod 6$$

közül az elsőnek nincs megoldása, a másodiknak két különböző megoldása is van, nevezetesen $x \equiv 2$ és $x \equiv 5 \pmod 6$. A $(*)$ feladat általános megoldására később térünk vissza.
Nyilvánvaló, hogy ha két maradékosztály összegét, különbségét vagy szorzatát akarjuk kiszámolni, akkor ez az input (t.i. a,b és m) hosszának polinomjával arányos lépésszámban végrehajtható, hisz elvégezhetjük a „közönséges” műveletet, majd egy maradékos osztást hajtunk végre.
Megmutatjuk, hogy – az első szakaszban látottakkal ellentétben – a maradékosztályok körében a hatványozás is polinomrendben végezhető el. Gondoljuk végig, hogy pl.

$$\begin{aligned} 2^2 &= 4 \\ 2^4 &= 16 \equiv -13 \pmod{29} \\ 2^8 &\equiv 169 \equiv -5 \pmod{29} \\ 2^{16} &\equiv 25 \equiv -4 \pmod{29} \\ &\vdots \end{aligned}$$

vagyis $2^k = l$ esetén t^l nem l darab, hanem $k(= \log l)$ darab lépésben számítható ki. Általában is, ha l-nek a kettes számrendszerben felírt alakja k számjegyű, akkor t^l maradékosztályának meghatározásához k db szorzással elő tudjuk állítani az összes $t^2, t^4, t^8, t^{16}, \ldots t^{2^k}$ számokat és ezek közül épp azokat kell összeszorozni, melyeknek megfelelő helyen az l kettes számrendszer-beli előállításában egyes áll.
Bár ezzel beláttuk, hogy $t^l \pmod m$ kiszámításához csak $(\log t + \log l + \log m)$-ben polinom–sok lépés kell, érezhető, hogy ha $l \gg m$ (vagyis l sokkal nagyobb m-nél), akkor ennél sokkal gyorsabb algoritmus is elképzelhető. Nyilvánvaló, hogy a

$$t, t^2, t^3, t^4, \ldots$$

számoknak megfelelő maradékosztályok sorozata előbb–utóbb önmagát fogja ismételni (mivel csak m darab maradékosztály van). Például $\bmod 7$ esetén

$$2,\ 4,\ 8 \equiv 1,\quad 16 \equiv 2,\quad 32 \equiv 4,\quad 64 \equiv 1, \ldots$$

vagy

$$3,\ 9 \equiv 2,\quad 27 \equiv 6,\quad 81 \equiv 4,\quad 243 \equiv 5,\quad 729 \equiv 1, \ldots$$

tehát 3, illetve 6 hosszú ciklus jött létre. Így ha valaki mondjuk $3^{2002} \pmod 7$-re kíváncsi, akkor tudva, hogy $3^6 \equiv 1 \pmod 7$, először megállapítja, hogy $2002 \equiv 3 \pmod 6$, vagyis hogy $2002 = 6l + 3$ alakban áll elő, és akkor

$$3^{2002} = 3^{6l+3} = (3^6)^l \cdot 3^3 \equiv 1^l \cdot 3^3 \equiv 6 \pmod 7.$$

A következő szakaszban látni fogjuk, hogy lehet ezeknek a ciklusoknak a hosszát általában is meghatározni.

4.4. Teljes és redukált maradékrendszerek, az Euler-Fermat tétel

Ha a $\bmod m$ maradékosztályok mindegyikéből kiválasztunk egy tetszőleges elemet, a keletkező számhalmazt $\bmod m$ **teljes maradékrendszernek** nevezzük. Könnyű belátni, hogy egy $\{b_1, b_2, \ldots, b_n\}$ számhalmaz akkor és csak akkor alkot $\bmod m$ teljes maradékrendszert, ha

$$\begin{array}{ll} (1) & n = m \\ (2) & \text{bármely } i \neq j \text{ indexpárra } b_i \not\equiv b_j \pmod m \end{array} \qquad (*)$$

Ha két szám ugyanabba a $\bmod m$ maradékosztályba tartozik, akkor vagy mindkettő relatív prím m-hez, vagy egyik sem (hisz a különbségük osztható m-mel, így ha az egyiküknek van m-mel közös osztója, akkor az a másiknak is osztója). Így van értelme a $\bmod m$ maradékosztályokat két csoportba osztani: azokba, melyek minden eleme relatív prím m-hez, és azokba, melyeknek egyik eleme sem. Az előbbi csoportba épp annyi $\bmod m$ maradékosztály tartozik, ahány szám a $\{0, 1, 2, \ldots, m-1\}$ halmazból relatív prím m-hez. Ezt a számot $\varphi(m)$-mel jelöljük.

Ha fenti első csoportban tartozó minden maradékosztályból kiválasztunk egy tetszőleges elemet, a keletkező számhalmazt mod m **redukált maradékrendszernek** nevezzük. A fenti (*) tulajdonság-párhoz hasonlóan könnyű belátni, hogy egy $\{c_1, c_2, \ldots, c_k\}$ számhalmaz akkor és csak akkor alkot mod m redukált maradékrendszert, ha

$$\begin{array}{ll} (1) & k = \varphi(m) \\ (2) & \text{bármely } i \neq j \text{ indexpárra } c_i \not\equiv c_j \pmod{m} \\ (3) & \text{bármely } i \text{ indexre } d(c_i, m) = 1 \end{array} \qquad (**)$$

Például mod 5 teljes maradékrendszer a $\{0,1,2,3,4\}$ vagy a $\{0,11,22,53,59\}$ számhalmaz, és redukált maradékrendszereket kapunk, ha a 0 elemet elhagyjuk belőlük. Ugyanakkor mod 6 egy redukált maradékrendszer csak két elemből állhat, egy $6k+1$ és egy $6k+5$ alakú számból, hisz bármely más szám 2 és 3 közül legalább az egyikkel osztható, tehát nem relatív prím 6-hoz.

4.4.1. Tétel. *Legyen $d(a,m) = 1$. Ha egy* mod m *teljes vagy redukált maradékrendszer minden elemét a-val megszorozzuk, ismét egy* mod m *teljes, ill. redukált maradékrendszert kapunk.*

BIZONYÍTÁS: A maradékrendszer elemeinek számát az a-val való szorzás nyilván nem befolyásolja. Belátjuk, hogy ha $x \not\equiv y \pmod{m}$ és $d(a,m) = 1$, akkor $ax \not\equiv ay \pmod{m}$. Csakugyan, ha $ax - ax = a(x-y)$ osztható lenne m-mel, akkor a 4.2.2. tétel szerint m minden prímosztója vagy a-nak, vagy $(x-y)$-nak osztója lenne, tehát vagy $d(a,m) = 1$, vagy $x \not\equiv y \pmod{m}$ nem teljesülne. Végül redukált maradékrendszer esetén a $(**)$ tulajdonság-hármas (3) tagja is teljesül: az m-hez relatív prím a és c_i számok szorzatának sem lehet m-mel közös prímosztója. □

A 4.3. szakaszban már említettük, hogy tetszőleges t szám esetén a $t, t^2, t^3, \ldots$ hatványok mod m sorozata előbb-utóbb ismétlődni fog. Ezt most pontosan meg tudjuk fogalmazni a fenti $\varphi(m)$ függvény segítségével.

4.4.2. Tétel (Euler-Fermat tétel). *Ha $m > 1$ tetszőleges egész szám és a tetszőleges olyan szám, melyre $d(a,m) = 1$, akkor*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

BIZONYÍTÁS: Legyen $\{c_1, c_2, \ldots, c_{\varphi(m)}\}$ egy mod m redukált maradékrendszer. A 4.4.1. tétel szerint az $\{ac_1, ac_2, \ldots, ac_{\varphi(m)}\}$ számhalmaz is egy mod m redukált maradékrendszer lesz, tehát az $ac_1, ac_2, \ldots, ac_{\varphi(m)}$ szorzatok valamilyen sorrendben kongruensek a $c_1, c_2, \ldots, c_{\varphi(m)}$ számokkal (lásd a 4.1. ábrát). Így

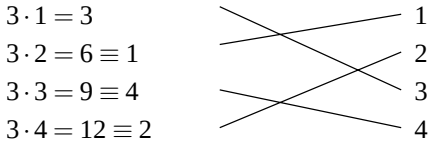
$$\prod_{i=1}^{\varphi(m)} (ac_i) = \prod_{i=1}^{\varphi(m)} (c_i) \pmod{m}$$

teljesül, vagyis

$$\left(a^{\varphi(m)-1}\right)\prod_{i=1}^{\varphi(m)}(c_i)\equiv 0 \pmod m.$$

Mivel a c_i számok m-hez relatív prímek voltak, szükségképp $a^{\varphi(m)}-1$ osztható m-mel. □

Legyen például $m=5$ és $a=3$. Ha mondjuk a redukált maradékrendszer elemei $\{1,2,3,4\}$, akkor a 4.1. ábrán látható sorrendben felelnek meg az ac_i elemek az eredeti c_i elemeknek.



4.1. ábra.

Ahhoz, hogy ezt a tételt használhassuk, ismernünk kell a φ függvény kiszámítási módját. Ha m prím, nyilván $\varphi(m)=m-1$ és ha m egy p^α alakú prímhatvány, akkor $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$, hisz az $1,2,\ldots,p^\alpha$ számok közül épp a p-vel osztható $p^{\alpha-1}$ darab szám **nem** relatív prím p^α-hoz. Ha a és b relatív prímek, akkor $\varphi(ab)=\varphi(a)\cdot\varphi(b)$ is teljesül (ezt nem bizonyítjuk). Ennek segítségével adódik

4.4.3. Tétel. *Ha $n=\prod p_i^{\alpha_i}$, akkor*

$$\varphi(n)=\prod\left(p_i^{\alpha_i}-p_i^{\alpha_i-1}\right)=n\cdot\prod\left(1-\frac{1}{p_i}\right),$$

ahol a szorzatképzés n prímosztóira vonatkozik. □

Ha például $n=2001=3\cdot 23\cdot 29$, akkor $\varphi(n)=2\cdot 22\cdot 28=1232$. A képlet második alakját használva ha például $n=1000=2^3\cdot 5^3$, akkor $\varphi(n)=1000\cdot\frac{1}{2}\cdot\frac{4}{5}=400$. Megjegyezzük, hogy erre a számelméleti tételre kombinatorikus bizonyítás is adható, lásd az 1.3. szakaszt.

4.4.4. Tétel („kis" Fermat tétel). *Tetszőleges p prímszámra és tetszőleges a egész számra $a^p\equiv a \pmod p$.*

BIZONYÍTÁS: Ha a osztható p-vel, akkor $a\equiv a^p\equiv 0 \pmod p$. Ha nem, akkor $d(a,p)=1$, tehát $a^{\varphi(p)}=a^{p-1}\equiv 1 \pmod p$. A kongruencia mindkét oldalát a-val szorozva kapjuk az állítást. □

4.5. Lineáris kongruenciák megoldása, alkalmazások

Térjünk vissza az

$$ax \equiv b \pmod{m} \tag{4.1}$$

lineáris kongruencia megoldására.

4.5.1. Tétel. *A (4.1) kongruencia akkor és csak akkor oldható meg, ha $d = d(a,m)$ osztója b-nek. Ilyenkor a megoldások száma d darab maradékosztály* mod m.

BIZONYÍTÁS: Ha (4.1) megoldható, akkor $ax - b$ osztható m-mel, így b szükségképp osztható a és m valamennyi közös osztójával. Megfordítva, ha b osztható d-vel, akkor a 4.2.1. tétel szerint (4.1)-ből következik, hogy

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}, \tag{4.2}$$

ahol $\frac{a}{d}$ és $\frac{m}{d}$ már relatív prímek. Ha tehát a mod $\frac{m}{d}$ teljes maradékrendszer minden elemét végigszorozzuk a modulushoz relatív prím $\frac{a}{d}$ számmal, akkor a 4.4.1. tétel szerint ismét teljes maradékrendszerhez jutunk, vagyis pontosan egy mod $\frac{m}{d}$ maradékosztály elemeire teljesül a (4.2) kongruencia. Végül ha $x \equiv x_0 \pmod{\frac{m}{d}}$ megoldása (4.2)-nek, akkor nyilván az

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d}, \ldots,\ x_0 + (d-1)\frac{m}{d} \tag{4.3}$$

számok által meghatározott d darab mod m maradékosztály lesz (4.1) megoldása. □

Hogyan oldjunk meg egy (4.1) kongruenciát a gyakorlatban? Először ellenőrizzük, hogy b osztható-e $d(a,m)$-mel. Ha nem, akkor (4.1) nem oldható meg. Ha igen, akkor térjünk át a (4.2) alakra, ezt oldjuk meg, majd a (4.3) képlet alkalmazásával adjuk meg az eredeti kongruencia megoldásait. Ha pl. $3x \equiv 9 \pmod{12}$, akkor $x \equiv 3 \pmod 4$, vagyis $x \equiv 3$ vagy 7 vagy 11 $\pmod{12}$.
Elég tehát (4.2) megoldásaival foglalkoznunk, vagyis legyen $ax \equiv b \pmod m$ és tegyük fel, hogy $d(a,m) = 1$. Mivel ilyenkor $a^{\varphi(m)} \equiv 1 \pmod m$ teljesül, nyilván az a megoldás, hogy

$$x \equiv b \cdot a^{\varphi(m)-1} \pmod m,$$

hisz a kongruencia mindkét oldalát a-val szorozva $ax \equiv b \cdot a^{\varphi(m)} \equiv b \pmod m$ adódik.
Ha ismerjük $\varphi(m)$-et (vagy legalábbis m kanonikus alakját, amiből a 4.4.3. tétel alapján $\varphi(m)$ kiszámítható), akkor ezt a képletet *elvileg* mindig alkalmazhatjuk. A *gyakorlatban* azonban, viszonylag kis a, b, m számok mellett egyszerűbben is célhoz juthatunk. Ezt egy példán szemléltetjük.
Ha az

$$523x \equiv 39 \pmod{23}$$

kongruenciát kell megoldanunk, akkor először is a és b értékét a velük mod m kongruens legkisebb értékkel helyettesítjük, esetünkben tehát a

$$17x \equiv 16 \pmod{23}$$

feladatra térünk át, hisz $523 = 22 \cdot 23 + 17$ és $39 = 1 \cdot 23 + 16$. Utána a kongruencia mindkét oldalát megszorozzuk egy olyan t számmal, hogy az $atx \equiv bt \pmod{m}$ baloldalán az at szorzat mod m egy a-nál kisebb számmal legyen kongruens. A példánkban $t = 2$ választással máris $34x \equiv 32 \pmod{23}$ miatt

$$11x \equiv 7 \pmod{23}$$

adódnék, még szerencsésebb a $t = 4$ választás, mert $68x \equiv 64$-ből $-x \equiv 18$, vagyis

$$x \equiv 5 \pmod{23}.$$

Előfordulhat, hogy több kongruenciát egyidejűleg kell egy számnak kielégítenie. (Ezt **szimultán kongruenciarendszernek** is hívják.) Az ilyenkor követendő eljárást egy példán mutatjuk be. Ha pl. a

$$2x \equiv 1 \pmod{5}, \quad 3x \equiv 7 \pmod{11}$$

kongruenciáknak kell egyidejűleg teljesülniük, akkor első lépésként ellenőrizzük, hogy külön-külön megoldhatóak-e (ez nyilván szükséges feltétel). Esetünkben igen, ezért (az elsőt 3-mal, a másodikat 4-gyel szorozva) megoldjuk őket:

$$x \equiv 3 \pmod{5}, \quad x \equiv 6 \pmod{11}.$$

Ezután az utóbbit átírjuk $x = 11k + 6$ alakba (ahol k tetszőleges egész szám) és behelyettesítjük az előbbibe:

$$11k + 6 \equiv 3 \pmod{5}.$$

Ennek megoldása $k \equiv 2 \pmod{5}$ tehát $k = 5l + 2$. Ezt visszahelyettesítve $x = 11k + 6 = 55l + 28$ adódik, vagyis

$$x \equiv 28 \pmod{55}.$$

Gyakran van szükség arra, hogy olyan lineáris egyenletrendszereket oldjunk meg, ahol eggyel kevesebb az egyenlet, mint az ismeretlenek száma, viszont minden egyenletben minden konstans egész szám és a megoldásoknak is egészeknek kell lenniük. (Ha csak az egészek körében keressük egy egyenlet vagy egyenletrendszer megoldásait, akkor **diofantikus** egyenlet(-rendszer)-ről beszélünk.) A lineáris diofantikus egyenletek megoldását is lineáris kongruenciák megoldására vezetjük vissza, ezt is egy példán szemléltetjük.
Ha a

$$2x + 3y + 5z = 46, \quad x - 2y + z = 2$$

diofantikus egyenletrendszert kell megoldanunk, akkor a második egyenletből

$$z = 2 - x + 2y \tag{4.4}$$

behelyettesítéssel egyetlen

$$-3x + 13y = 36 \tag{4.5}$$

egyenlethez jutunk. Mivel x,y egész számok, ez ekvivalens a $13y \equiv 36 \pmod 3$ kongruenciával, melyből $y \equiv 0 \pmod 3$, vagyis $y = 3t$, ahol t tetszőleges egész szám. (4.5)-be, majd (4.4)-be visszahelyettesítve az

$$x = 13t - 12, \quad y = 3t, \quad z = 14 - 7t$$

megoldást kapjuk.

A lineáris kongruenciák harmadik alkalmazásaképp belátjuk a következőt:

4.5.2. Tétel (Wilson-tétel). *Legyen $k \geq 2$ tetszőleges pozitív szám. Ekkor*

$$(k-1)! \equiv \begin{cases} -1 \pmod k, & \text{ha } k \text{ prím,} \\ 2 \pmod k, & \text{ha } k = 4, \\ 0 \pmod k, & \text{ha } k \geq 6 \text{ összetett szám.} \end{cases}$$

BIZONYÍTÁS: $k = 4$-re az állítás nyilvánvaló. Ha $k > 4$ és összetett, akkor található két olyan különböző $1 < a < b < k$ egész szám, melyekre $ab = k$, és akkor $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (k-1) = a \cdot b \cdot c \equiv 0 \pmod k$ teljesül.
Legyen végül k prím. Minden $1 \leq a < k$ -ra az $ax \equiv 1 \pmod k$ kongruencia egyértelműen megoldható, jelöljük a megoldást x_a-val. Ha $x_a \neq a$, akkor a $(k-1)!$ szorzatban ez a két szám (a és x_a) szorzatként egyet ad, tehát nem kell velük foglalkozni. Például $k = 7$-re

$$(k-1)! = 1 \cdot 6 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \equiv 6 \equiv -1 \pmod k,$$

mert $2 \cdot 4 \equiv 3 \cdot 5 \equiv 1 \pmod 7$. Elég belátnunk, hogy tetszőleges k prímre épp ez lesz a helyzet, tehát hogy 1 és $k-1$ kivételével a szorzótényezők párbaállíthatóak. Csakugyan, a-nak pontosan akkor nincs párja, ha $x_a = a$, vagyis ha $a^2 \equiv 1 \pmod k$. Ez átalakítva $a^2 - 1 = (a+1)(a-1) \equiv 0 \pmod k$-val ekvivalens. Felhasználva, hogy k prím, az $(a+1)(a-1)$ szorzat csak akkor lehet k-val osztható, ha vagy $a \equiv 1 \pmod k$, vagy $a \equiv -1 \pmod k$ teljesül. □

4.6. Prímszámok, prímtesztelés

Hogy lehet eldönteni egy n számról, hogy prím-e? Sok ezer éve a görög Eratoszthenész javasolta az alábbi „szita-algoritmust”: Írjuk fel az egész számokat 2-től n-ig, húzzuk ki (vagyis szitáljuk ki) a páros számokat, kivéve a 2-t, azután a maradékból a hárommal oszthatókat, kivéve a 3-t, azután az öttel oszthatókat, kivéve

az 5-öt stb. Minden ilyen lépés után a megmaradtak közül a legkisebb egy prím, őt hagyjuk meg, de a többszöröseit húzzuk ki. Így elvileg bármilyen határig előbb-utóbb elő lehet állítani az összes prímet.

Egy másik lehetőség egyszerűen minden n-nél kisebb számról megnézni, nem osztója-e n-nek. A valóságban elég csak $2,3,4,\ldots,\lfloor\sqrt{n}\rfloor$-ig próbálkozni, ha addig semmi nem osztója n-nek, akkor n biztos prímszám (hisz ha k osztója n-nek, akkor n/k is osztója, és $\min(k,n/k)\leq\lfloor\sqrt{n}\rfloor$).

Az utóbbiról azonnal látszik, hogy lépésszám-igénye $\lfloor\sqrt{n}\rfloor$-nel arányos. Figyelembe véve, hogy a feladat inputja n, az input hossza $\lceil\log n\rceil$, ennek a lépésszám nem polinomja. Az eredeti Eratoszthenész–szitáról is belátható, hogy a lépésszám az input hosszának exponenciális függvénye.

Mielőtt elvetnénk ezeket a – kétségkívül nem polinomrendű – algoritmusokat, jegyezzük meg, hogy egy nagy előnyük is van. Ha ugyanis n nem prímnek, hanem összetett számnak bizonyul, akkor rögtön n valamely osztóját is megtaláljuk. A szakasz hátralévő részében egy olyan prímtesztelő algoritmust ismertetünk, mely polinomrendben véget ér, de **egyrészt** az eredmény nem biztosan, hanem csak valószínűleg igaz, **másrészt** ha összetett számnak tartja n-et, akkor általában nem találja meg egyetlen osztóját sem.

Az algoritmus alapgondolata az előző szakaszban kimondott Euler–Fermat tételt használja fel. Ha n prím, tehát $\varphi(n)=n-1$, akkor $t^{n-1}\equiv 1 \pmod{n}$ teljesül minden olyan t-re, mely n-hez relatív prím (vagyis melyre $t\not\equiv 0 \pmod{n}$ teljesül). Ha egy konkrét t,n párra $t^{n-1}\equiv 1 \pmod{n}$ teljesül, akkor ez nem bizonyítja azt, hogy n prím (lehet, hogy n összetett szám, csak t a „cinkosa”, vagyis segíti n-t abban, hogy bennünket megtévesszen, hogy velünk elhitesse, hogy ő prím). Ha viszont $t^{n-1}\equiv 1 \pmod{n}$ nem teljesül, akkor minden további vizsgálat nélkül biztosak lehetünk abban, hogy n nem prím (tehát t az n „árulója”).

Ha egyáltalán vannak egy összetett számnak árulói (általában vannak; nagyon kevés az olyan úgynevezett Carmichael szám, amelynek minden hozzá relatív prím cinkosa), akkor legalább annyi az árulója, mint a cinkosa. Ezt könnyű belátni. Vegyük észre, hogy a cinkosok szorzata cinkos, míg egy cinkos és egy áruló szorzata áruló. Ha tehát

$$c_1,c_2,\ldots,c_s$$

az összes cinkos sorozata, és a egy áruló, akkor az

$$ac_1,ac_2,\ldots,ac_s$$

sorozat minden tagja áruló (és belátható, hogy mind különbözőek). Így már $2s$ darab különböző maradékosztályt találtunk, és lehet, hogy további árulók is vannak.

Ha tehát egymástól függetlenül véletlenszerűen választunk q darab maradékosztályt, és mindegyikre $m^{n-1}\equiv 1 \pmod{n}$ teljesül, akkor n lehet ugyan összetett szám, de ennek a valószínűsége $(1/2)^q$-nál kisebb (vagyis elég nagy q érték mellett szinte lehetetlen). Így az alábbi algoritmus – néhány Carmichael számtól eltekintve – minden n inputra működik:

0. lépés: $i\leftarrow 1$

1. lépés: Válasszunk véletlenszerűen egy $1 < m < n$ számot

2. lépés: Határozzuk meg m és n legnagyobb közös osztóját. Ha ez egynél nagyobb $\rightarrow$ STOP 1

3. lépés: Ha $m^{n-1} \not\equiv 1 \pmod{n} \rightarrow$ STOP 2

4. lépés: Ha $i = 100 \rightarrow$ STOP 3

5. lépés: $i \leftarrow i+1$ és folytassuk az 1. lépésnél.

STOP 1: n összetett szám, $d(n,m)$ egy osztója

STOP 2: n összetett szám, de egyetlen osztóját sem találtuk meg

STOP 3: n valószínűleg prím (a hiba valószínűsége $< (1/2)^{100}$)

Vegyük észre, hogy az előző szakaszokban látottak szerint a 2. és 3. lépés is elvégezhető polinom időben, így az egész algoritmus lépésszám–igénye is az input hosszának polinomjával becsülhető.
A Carmichael-féle számok esetén is működik az algoritmus, ha a 3. lépést megváltoztatjuk. A fenti algoritmus 3. lépése úgy is írható, hogy ha $m^{n-1}-1$ nem osztható n-nel, akkor STOP 2. Mivel n páratlan, nyilván

$$m^{n-1}-1 = \left(m^{\frac{n-1}{2}}+1\right)\left(m^{\frac{n-1}{2}}-1\right)$$

sőt, ha $n-1$ osztható 4-gyel, akkor a második tényező

$$m^{\frac{n-1}{2}}-1 = \left(m^{\frac{n-1}{4}}+1\right)\left(m^{\frac{n-1}{4}}-1\right)$$

alakba is írható stb. Általában, ha $n-1 = 2^t q$ (ahol q már páratlan szám), akkor

$$m^{n-1}-1 = \left(m^{\frac{n-1}{2}}+1\right)\left(m^{\frac{n-1}{4}}+1\right)\cdots\left(m^{\frac{n-1}{2^t}}+1\right)\left(m^{\frac{n-1}{2^t}}-1\right) \tag{4.6}$$

Ezek után belátható, hogy a 3. lépés helyett az alábbi állhat:

3'. lépés: Ha a (4.6) jobboldalán látható $t+1$ tényező egyike sem osztható n-nel, akkor STOP 2.

Vegyük észre, hogy így nem egy, hanem $t+1$ oszthatóságot kell ellenőriznünk, de $t = \log\frac{n-1}{q} < \log n$ miatt ez csak az algoritmus lépésszámát felülről becslő polinom fokszámát növeli eggyel (de nem rontja el a polinomialitást).
Összegezve: a fentiek alapján létezik polinomrendű prímtesztelő algoritmus. Ha azonban a beadott szám összetettnek bizonyul, akkor a szorzótényezőit nem tudjuk polinom időben meghatározni. Ha pl. p és q két egyenként 200 jegyű szám, akkor rövid idő alatt eldönthetjük $n = p \cdot q$-ról, hogy összetett, de – mai tudásunk szerint – évszázadok alatt sem lehet n-ből visszakövetkeztetni p-re és q-ra. Ez a következő fejezet kulcs–gondolata.

5. fejezet

Nyilvános kulcsú titkosírások

5.1. Mi a jelszó?

Előkészítésképp tekintsük az alábbi problémát. A számítógép memóriájában el akarunk helyezni fontos információkat azzal, hogy csak a jogosultak olvashassák ki. Ha valami jelszó igazolja a jogosultságot, akkor a számítógép belső rendszerét ismerő programozó illetéktelenül hozzájuthat a jelszóhoz, és azon keresztül az információhoz. Elképzelhető-e olyan „jelszó”, amit a rendszer maga sem ismer, és mégis tudja ellenőrizni, hogy mi ismerjük-e?

A 4.6. szakasz végén mondottak sugallják a megoldást. Válasszunk ki két 200-jegyű p és q prímszámot és csak az $n = pq$ szorzatukat adjuk meg a gépnek. Ezután rendelkezzünk úgy, hogy annak adhatják ki az adatokat, aki n valamely osztóját mondja meg. Annak ellenőrzése, hogy az adatokért jelentkező személy által mondott k szám osztója-e n-nek (vagyis $k = p$ vagy $k = q$ teljesül-e), nyilván gyorsan elvégezhető, de n-ből p és q előállítása mai tudásunk szerint reménytelenül nehéz.

Igazából még azt sem kell kérnünk a számítógéptől, hogy az n számot (a jelszónkat) tartsa titokban – a konkurencia (akitől védjük az információt) éppúgy nem tud semmit sem kezdeni az n számmal, mint a számítógép programozója. Ez indokolja a „nyilvános kulcs” elnevezést.

Ha persze egyszer közöljük a számítógéppel p vagy q értékét, akkor attól kezdve nem lehetünk biztonságban. A számítógépes adatvédelem ezért egy valamivel bonyolultabb megoldást igényel.

5.2. Kódolás és dekódolás

Nyilván bármilyen üzenet átalakítható számjegyek sorozatává. Feltehetjük tehát, hogy a titkosítandó majd továbbítandó üzenet mondjuk 400-jegyű számok sorozata. (A hosszabb üzenet nyilván feldarabolható 400-elemű blokkokra, az utolsó blokk szükség esetén kiegészíthető valamilyen szimbólummal épp 400-jegyűre.)

Ha tehát titkosítani (szokásos nevén: kódolni) akarunk egy üzenetet, akkor a kódolást tekinthetjük egy $y = C(x)$ függvénynek, mely a 400-jegyű x számhoz egy másik 400-jegyű y számot rendel. E függvény inverzét, az $x = D(y)$ függvényt dekódoló függvénynek nevezhetjük.

Tegyük fel, hogy mindenki nyilvánosságra hozza a saját C kódoló függvényét (pl. a telefonkönyvben a neve után ezt is megadja), de titokban tartja a D dekódoló függvényt. Ekkor ha az i-edik személy (a feladó) el akarja küldeni az x üzenetet a j-ik személynek (a címzettnek), akkor az általa is hozzáférhető C_j kódolófüggvényt alkalmazva az $y = C_j(x)$ üzenetet küldi el. A címzett alkalmazza a csak általa ismert D_j dekódoló függvényt és megkapja a $D_j(y) = D_j(C_j(x)) = x$ üzenetet. A rendszerben részt vevő többi ember számára y dekódolhatatlan.

Kérdés persze, hogyan lehet olyan $C_1, C_2, \ldots$ kódoló és $D_1, D_2, \ldots$ dekódoló függvényeket készíteni, hogy bármely x-re $C_i(x)$ vagy $D_i(x)$ kiszámítása gyorsan elvégezhető legyen, de a C_i ismeretében D_i-re ne lehessen következtetni. Ehhez térünk vissza a prímszámokhoz.

Tegyük fel, hogy az i-ik résztvevő választ két 200-jegyű prímszámot, jelöljük ezeket p_i-vel és q_i-vel. Legyen $n_i = p_i q_i$. Emlékeztetünk rá, hogy $\varphi(n_i) = (p_i - 1)(q_i - 1)$, jelöljük ezt a mennyiséget m_i-vel.

A résztvevő ezen kívül kiválaszt egy olyan e_i számot is, melyre $1 \leq e_i \leq n_i$ teljesül és amely relatív prím $(p_i - 1)$-hez is és $(q_i - 1)$-hez is. Végül megoldva egy (4.1) típusú kongruenciát (ld. 4.5. szakasz) meghatározza azt a d_i számot, melyre $e_i d_i \equiv 1 \pmod{m_i}$.

Ezután az i-ik résztvevő nyilvánosságra hozza az n_i és e_i számokat, viszont titokban tartja a p_i, q_i, m_i és d_i számokat. A C_i kódolófüggvény egy x üzenethez hozzárendeli azt az $y = C_i(x)$ számot, melyre

$$y \equiv x^{e_i} \pmod{n_i},$$

míg a D_i dekódolófüggvény az y-hoz annak d_i-ik hatványát rendeli $\pmod{n_i}$. Így

$$y^{d_i} \equiv x^{e_i d_i} = x^{hm_i+1} = \left[x^{\varphi(n_i)}\right]^h \cdot x \equiv x \pmod{n_i}.$$

Végül egy technikai megjegyzés. Mindez csak akkor működik, ha x relatív prím n_i-hez. Ezt pl. úgy biztosíthatjuk, hogy az üzenetet nem 400, hanem 399 jegyű számsorozatokra bontjuk, majd mindegyik sorozat utolsó elemét úgy választjuk meg, hogy e feltétel teljesüljön. Dekódolás után egyszerűen elhagyjuk az utolsó számjegyet.

5.3. További trükkök

A klasszikus titkosírásoknak több gyenge pontja is volt. Mindenekelőtt, ha két személy kódolt üzeneteket akart váltani egymással, akkor először meg kellett állapodniuk egymással a kódban (tehát találkozniuk kellett egymással még az üzenetváltás előtt, vagy ha erre nem volt módjuk, akkor biztosítaniuk kellett, hogy amikor az egyik elküldi a másiknak a kódot, az nem kerül illetéktelen kezekbe). Világos, hogy az előző pontban leírt módszer kiküszöböli ezt a hátrányt.

Másik előnye az új módszernek, hogy ha t személy akar így levelezni, akkor nem kell $\binom{t}{2}$ féle titkos kódot kitalálni, és mégis bármely üzenet rejtve marad a többi $t-2$ résztvevő előtt.
A régi titkosírások harmadik hátránya, hogy a címzett soha nem tudhatta, hogy tényleg a feladó írt-e neki, vagy „az ellenség” kezébe került a kód, és hamisítványt kap. Az előző pontban leírt módszernek látszólag ugyanez a hátránya (hisz C_j-hez mindenki hozzáfér, nem csak az i-ik résztvevő). Azonban a következő trükkel elkerülhetjük ezt a veszélyt. Az i-ik résztvevő ne x-re, hanem $z = D_i(x)$-re alkalmazza a $w = C_j(z)$ kódolást, majd ezt a w „üzenetet” küldi el. A címzett (tehát a j-ik résztvevő) először a csak általa ismert D_j, majd a nyilvánosság számára hozzáférhető C_i függvényt alkalmazza, hisz

$$C_i(D_j(w)) = C_i(D_j(C_j(z)) = C_i(z) = C_i(D_i(x)) = x.$$

Így az üzenetet csak j tudja elolvasni, és biztos lehet benne, hogy csak i küldhette.
Az új módszer negyedik előnyét akkor érthetjük meg, ha nem katonai hírszerzők titkosírásaira gondolunk, hanem egymással konkurens kereskedők, bankárok stb. titkos üzeneteire. Itt ugyanis előfordulhat, hogy i rendel valamit j-től, majd nem fizet, így j-nek „bíróság” elé kell vinnie az ügyet: Be akarja bizonyítani, hogy i feladta a rendelést, tehát valamilyen értelemben a kapott w üzenetet is, meg annak x jelentését is be kell mutatnia, de a bírónak sem akarja megmondani a saját D_j dekódoló eljárását és nyilván nem kényszerítheti az „ellenérdekelt” i-t saját D_i eljárásának felfedésére. Ez a látszólag sokkal komplikáltabb feladat is könnyen megoldható: A pert kezdeményező j nem csak w-t, hanem az $u = D_j(w)$ „félig dekódolt” üzenetet is bemutatja a „bírónak”. A „bíró” kizárólag a nyilvánosság számára is hozzáférhető C_i, C_j kódolási eljárások segítségével ellenőrizheti, hogy (1) $w = C_j(u)$, tehát tényleg j-nek jött az üzenet, és hogy (2) $x = C_i(u)$, tehát tényleg i-től jött az üzenet.

5.4. Bizonyítás információközlés nélkül

A titkosírásokkal kapcsolatos megfontolásaink mind azon alapultak, hogy az összetett számokat nem tudjuk prímtényezőkre bontani. Ha egyszer valaki találna erre a problémára polinomidejű algoritmust, akkor minden ilyen titkos kódot „fel tudna törni”.
Márpedig lehet, hogy a probléma polinom időben megoldható. Nincs olyasmi „negatív” eredményünk, mint pl. a Hamilton–kör probléma esetén az **NP**-teljesség (ami szintén nem bizonyítja ugyan a probléma **P**-n kívül levését, de legalább erősen valószínűsíti). Sőt, olyan „pozitív” eredmény is született (A. Lenstra, H. Lenstra és Lovász), hogy egy némiképp hasonló probléma (egész együtthatós polinomok irreducibilis tényezők szorzatára bontása) éppen hogy polinom időben elvégezhető.

Ezért most egy olyan konstrukciót is bemutatunk, ami nem a prímfelbontás nehézségére, hanem a Hamilton–kör létezésének **NP**-teljességére épül. Fel fogjuk használni azt is (3.2. Táblázat utáni 3. megjegyzés), hogy két adott gráf izomorf vagy nem izomorf voltának eldöntésére sem ismeretes polinomrendű algoritmus.
Nyilván könnyen tudunk konstruálni egy olyan G gráfot, melynek van Hamilton–köre. Ha utána a pontok nevét permutáljuk és így adjuk meg a gráfot, más nem tudja eldönteni, van-e benne Hamilton–kör.
Ezt a gráfot adjuk meg titkunk őrzőjének (mondjuk a banknak) azzal, hogy csak annak szolgáltassa ki titkunkat, aki ismeri G-nek egy Hamilton–körét. Hogy győzheti meg ezek után a megbízottunk a bankárt, hogy jogosult az információ megszerzésére, anélkül, hogy ezután a bankár is ismerné G-nek egy Hamilton–körét?
Megbízottunk mutat egy G_1 gráfot és azt állítja, hogy

(1) G_1 izomorf G-vel; és hogy

(2) G_1-nek van Hamilton-köre.

Ezek után a bankár kérheti, hogy a két állítás egyikét (de csak az egyikét) bizonyítsa be. Ha (1)-et kell bebizonyítani, akkor megbízottunk megad G és G_1 ponthalmaza között egy kölcsönösen egyértelmű és éltartó leképezést. Ha (2)-t kell bebizonyítani, egyszerűen megad G_1-ben egy Hamilton–kört.
Az első esetben a bankár nem jut semmilyen új információhoz, csak az általa már úgyis ismert G-nek egy izomorf G_1 leírását is látni fogja. A második esetben sem jut semmilyen információhoz – lát ugyan egy G_1 gráfot, melynek van Hamilton–köre, de mivel nem tudja eldönteni, hogy G és G_1 izomorfak-e, változatlanul nem tud G-hez Hamilton–kört rajzolni.
Ennek ellenére annak a valószínűsége, hogy megbízottunk „blöffölt”, vagyis nem ismeri G-nek egyetlen Hamilton-körét sem, legfeljebb $1/2$ lehet. Ő ugyanis nem tudhatja előre, hogy a bankár (1) vagy (2) bizonyítását fogja kérni. Így akár G-t rajzolja át G_1-gyé anélkül, hogy ismerné egy Hamilton–körét, akár egy Hamilton–körrel rendelkező G_1-et rajzol anélkül, hogy tudná, izomorf-e G-vel, $1/2$ valószínűséggel lelepleződnék. (Első esetben a (2), második esetben az (1) kérdés feltevése esetén.)
Mondhatja persze valaki, hogy az $1/2$ valószínűség túl nagy. De ha a bankár mondjuk százszor kéri a „jelszót”, vagyis száz darab $G_1, G_2, \ldots, G_{100}$ gráfot, és mindegyiknél egymástól függetlenül dönti el, hogy az (1) vagy a (2) állítás bizonyítását kéri, akkor

- vagy mind a száz bizonyítás kielégítő,
- vagy van legalább egy olyan állítás, amit a titokért jelentkező nem tud bebizonyítani.

Utóbbi esetben biztos, hogy nem ismeri a jelszót, előbbi esetben $1/2^{100}$-nál kisebb a „blöffölés” valószínűsége (tehát lényegileg zérus). Ezt a kockázatot már vállalhatja a bankár.

Ha valaki tényleg meg akarna valósítani egy ilyen rendszert, akkor G megválasztása komoly problémát vethet fel. Ha túl sok, vagy túl kevés élű gráfot választanánk, akkor esetleg könnyű lenne benne Hamilton–kört találni (mert az első esetben nagyon sok Hamilton–köre lenne, a második esetben nagyon kevés). Ezekkel a kérdésekkel nem foglalkozunk.

6. fejezet

Csoportok, gyűrűk, testek, hálók

6.1. Alapfogalmak

A matematika számos területén találkoztunk olyan körülményekkel, amikor nem számokon, hanem egészen más természetű objektumokon kellett algebrai műveletet elvégeznünk. Ilyenek voltak például a vektorok vagy a mátrixok összeadása, a mátrixok illetve a lineáris transzformációk szorzása, vagy a függvények kompozíciója. Most megadjuk a művelet általános definícióját.

6.1.1. Definíció. *Legyen H tetszőleges halmaz, jelölje H^n a H halmaz elemeiből képzett n hosszú sorozatokat. Az $f: H^n \to H$ mindenütt értelmezett függvényt n-változós* **műveletnek** *nevezzük.*

Kétváltozós művelet például az egész számok összeadása, kivonása ($f(a,b) = a + b$, $f(a,b) = a - b$). Ilyenkor az $f(a,b)$ jelölés helyett a két elem közé beírjuk a műveleti jelet. Három változós művelet például a vektorok vegyesszorzata. Nem művelet a pozitív számok kivonása ($f(a,b) = a - b$), hiszen ha $a \leq b$, akkor nincs értelmezve (például $f(2,3) = 2 - 3$ nem pozitív).

6.1.2. Definíció. *Egy H halmazon értelmezett 2-változós műveletet (jelöljük $\star$-gal)* **kommutatívnak** *nevezünk, ha tetszőleges $a, b \in H$ esetén $a \star b = b \star a$;* **asszociatívnak** *nevezünk, ha tetszőleges $a, b, c \in H$ esetén $(a \star b) \star c = a \star (b \star c)$.*

6.1.3. Definíció. *Az S halmazt a rajta értelmezett $\star$ művelettel* **félcsoportnak** *nevezzük, ha $\star$ asszociatív. Ha $\star$ kommutatív is, akkor kommutatív (vagy Abel-féle) félcsoportról beszélünk.*

Példák:

1. A pozitív számok az összeadásra nézve félcsoportot alkotnak.
2. Az $n \times n$-es mátrixok a szorzással félcsoportot alkotnak.

3. A pozitív valós számok a szorzásra nézve félcsoportot alkotnak.

Ha az S félcsoportban van olyan e elem, amelyre igaz az, hogy $e \star a = a \star e = a$ minden $a \in S$ esetén, akkor e-t neutrális vagy **egységelemnek** hívjuk, S-et pedig egységelemes félcsoportnak nevezzük.
A fenti példák közül a 2. és a 3. egységelemes, az egységmátrix illetve az 1 az egységelemek.

6.1.4. Definíció. *Egy G halmazt a $\cdot$ művelettel* **csoportnak** *nevezünk, ha*

(a) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *minden* $a, b, c \in G$ *esetén*

(b) $\exists\, e \in G$, *amelyre* $a \cdot e = e \cdot a = a \quad \forall\, a \in G$-*re*

(c) $\forall\, a \in G$-*re* $\exists\, a' \in G$ *úgy, hogy* $a \cdot a' = a' \cdot a = e$.

A csoport elemszámát $|G|$-vel jelöljük, és G **rendjének** *nevezzük.*

Megjegyzés: a $\cdot$-ot gyakran nem írjuk ki, $a \cdot b$ helyett ab-t írunk.
Az (a) pont azt jelenti, hogy a művelet asszociatív, a (b) azt, hogy létezik egységelem. Ezt gyakran 1-gyel jelöljük, ha a művelet az összeadás, akkor 0-val. A (c) pontban említett a' elemet az a elem **inverzének** nevezzük és a^{-1}-gyel jelöljük. A csoportműveletről nem követeljük meg a kommutativitási szabály teljesülését, ha ez teljesül, **kommutatív (Abel-féle) csoportról** beszélünk.

Példák:

1. Az egész, a racionális és a valós számok Abel-csoportot alkotnak az összeadásra nézve ($(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$), a természetes számok ($\mathbb{N}$) viszont nem.

2. A pozitív valós és a pozitív racionális számok Abel-csoportot alkotnak a szorzásra nézve ($(\mathbb{R}^+, \cdot)$, $(\mathbb{Q}^+, \cdot)$).

3. Az $n \times n$-es invertálható mátrixok csoportot alkotnak a szorzásra nézve.

4. A szabályos n-szög egybevágóságai csoportot alkotnak, ahol a művelet az egymás után való elvégzés. Megjegyezzük, hogy itt a csoport egységeleme a helybenhagyás, a csoport rendje $2n$, ugyanis van n darab tengelyes tükrözés és a helybenhagyással együtt n forgatás. A csoportot D_n-nel jelöljük és **diédercsoportnak** nevezzük. Általában is definiálhatjuk egy síkidom **egybevágósági csoportját**.

5. n elem permutációi (önmagára való bijektív leképezései) csoportot alkotnak a kompozícióra. A csoportot n-ed fokú **szimmetrikus csoportnak** nevezzük, S_n-nel jelöljük, rendje $n!$. Egy H halmaz elemeinek összes permutációinak csoportját S_H-val jelöljük.

6. Egy Γ gráf automorfizmusai ($\mathrm{Aut}(\Gamma)$) (csúcs és éltartó bijektív leképezései) csoport a kompozícióra, mint műveletre.

Következmények:

1. Az egységelem egyértelmű: Tegyük föl, hogy e' és e'' is eleget tesznek a (b) pont követelményeinek. Ekkor $e' = e'e'' = e''$.

2. Az inverz egyértelmű: Legyen a' és a'' az a-nak két inverze.

$$a''aa' = (a''a)\,a' = ea' = a'$$
$$a''aa' = a''\,(aa') = a'e = a'',$$

azaz $a' = a''$.

Most a csoportaxiómák „átfogalmazásait” fogjuk vizsgálni. Az első arról szól, hogy a (b) és (c) pontokban megkövetelt egység- és inverzelem helyett elég egyoldali egység- illetve inverzelem létezését előírni.

6.1.5. Állítás. (1. átfogalmazás) *Egy G halmaz a $\cdot$ művelettel pontosan akkor csoport, ha*

(a) $(ab)c = a(bc)$*;*

(b) $\exists\, e \in G$*, amelyre* $ae = a$*;*

(c) *a (b) pontban említett e-k közül van olyan* e_0*, hogy* $\forall\, a \in G$*-re* $\exists\, a' \in G$ *úgy, hogy* $aa' = e_0$.

BIZONYÍTÁS: Legyen a' az a egyik jobbinverze,

$$aa' = e_0 = e_0e_0 = e_0aa.'$$

Az $aa' = e_0aa'$ egyenlőség mindkét oldalát megszorozva a' jobboldali inverzével az $a = e_0a$ egyenlőséget kapjuk, ezért e_0 baloldali egységelem is. Tehát e_0 (kétoldali) egységelem, és mint ilyen, a fentiek miatt egyértelmű.

$$a' = a'e_0 = a'aa'$$

Mindkét oldalt jobbról szorozva a' valamely jobboldali inverzével az $e_0 = a'a$ összefüggést kaptuk, tehát a' balinverz is. Ezzel igazoltuk a csoportaxiómák teljesülését. □

A második átfogalmazás előnye, hogy nem szerepelnek benne kitüntetett elemek.

6.1.6. Állítás. (2. átfogalmazás) *Egy asszociatív művelettel ellátott G struktúra pontosan akkor csoport, ha tetszőleges a, b G-beli elemekhez található G-ben egyetlen olyan x és egyetlen olyan y elem, amelyekre*

$$ax = b \text{ és } \quad ya = b$$

BIZONYÍTÁS: Legyen $a \in G$, e_a az $ax = a$ megoldása. Legyen $b \in G$ tetszőleges, $ya = b$. Ekkor

$$b = ya = y(ae_a) = (ya)e_a = be_a,$$

azaz $e_a = e$ a csoport jobboldali egységeleme. Az $ax = e$ egyenlet megoldása a jobbinverze. Ezzel igazoltuk az előző állítás feltételeit, tehát G csoport. □

Az algebrai szempontból egyformán viselkedő csoportokat nem akarjuk megkülönböztetni. Erre szolgál a következő

6.1.7. Definíció. *A G_1, G_2 csoportokat* **izomorfaknak** *nevezzük, ha van köztük egy kölcsönösen egyértelmű művelettartó leképezés, azaz van olyan*

$$\phi: G_1 \to G_2$$

leképezés, amely bijektív és tetszőleges $g,h \in G_1$ esetén

$$\phi(g)\phi(h) = \phi(gh)$$

teljesül. Jelölése $G_1 \simeq_\phi G_2$, vagy egyszerűen $G_1 \simeq G_2$.

Példák:

1. $(\mathbb{R}^+,\cdot) \simeq (\mathbb{R},+)$, ahol a ϕ izomorfizmus minden pozitív valós számhoz hozzárendeli a logaritmusát, azaz $\phi(a) = \log a$. A bijektivitás a logaritmus függvény monotonitásából adódik, a művelettartás pedig a $\log(ab) = \log a + \log b$ összefüggés következménye.

2. $D_3 \simeq S_3$, azaz a háromszög egybevágósági csoportja izomorf a 3-adfokú szimmetrikus csoporttal. Ennek igazolásához legyenek a háromszög csúcsai A, B, C, jelöljük a csúcsokon átmenő tengelyekre való tükrözéseket rendre t_1, t_2, t_3-mal, az $A \to B \to C \to A$ forgatást f-fel, a helybenhagyást pedig e-vel. Ekkor az $A \to C \to B \to A$ forgatás éppen f^2. Vegyük észre, hogy a háromszög minden egybevágósága permutálja a csúcsokat. Feleltessük meg A-nak az 1-et, B-nek a 2-t, C-nek a 3-at. Ily módon minden transzformációnak megfeleltethetünk egy permutációt. t_1 például felcseréli B-t és C-t, ezért a neki megfelelő permutáció az $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, amely a 2-t és a 3-at cseréli fel. Ugyanígy az f^2-nek megfelelő permutáció az $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Világos, hogy különböző transzformációk képe különböző, és mivel mindkét csoportnak 6 eleme van, minden permutáció előáll képként. A művelettartás abból az észrevételből adódik, hogy a transzformációk ugyanúgy szorzódnak össze, mintha a csúcsokon vett permutációkként fognánk fel őket.

6.2. Részcsoport, mellékosztályok, Lagrange tétele

6.2.1. Definíció. *Legyen G csoport. Egy $H \subseteq G$ részhalmazt* **részcsoportnak** *nevezünk, ha H is csoport ugyanarra a műveletre nézve. Jelölése: $H \leq G$.*

Példák:

1. Minden csoportnak részcsoportja maga a csoport, és az egységelemet tartalmazó egyelemű halmaz. Ezeket a részcsoportokat **triviális részcsoportnak**, az ezektől különböző részcsoportokat **valódi részcsoportoknak** nevezzük.

2. A valós számok additív csoportjának részcsoportja a racionális számok, annak pedig az egész számok additív csoportja.

3. A háromszög egybevágóságainak (D_3) részcsoportját alkotják a forgatások.

4. Az $n \times n$-es invertálható mátrixok csoportjának részcsoportja az 1 determinánsú mátrixok.

5. n elem permutációinak részcsoportját alkotják a páros permutációk.

6. A nem 0 komplex számok ($\mathbb{C} - \{0\}$) a szorzásra nézve csoportot alkotnak. Ennek egy részcsoportját alkotják az 1 abszolút értékű komplex számok, annak pedig részcsoportját az n-edik egységgyökök.

Annak ellenőrzése végett, hogy egy G csoport H részhalmaza részcsoport-e, elég ellenőrizni, hogy $a, b \in H$ esetén ab és a^{-1} is H-beli. Az asszociativitás ugyanis automatikusan teljesül a csoportaxiómák miatt, az egységelemet pedig megkapjuk, ha valamely H-beli elemet megszorozzuk az inverzével.

6.2.2. Állítás. *Részcsoportok metszete is részcsoport, azaz legyenek $H_i \leq G$ ($i \in A$), ahol A valamilyen indexhalmaz, akkor $\bigcap H_i$ is részcsoport.*

BIZONYÍTÁS: Ha $x, y \in \bigcap H_i$, akkor $x, y \in H_i$ $\forall i \in A$ esetén, így $xy \in H_i$ $\forall i \in A$ esetén, tehát $xy \in \bigcap H_i$. Ha $x \in \bigcap H_i$, akkor $x \in H_i$ $\forall i \in A$ esetén, ezért $x^{-1} \in H_i$ $\forall i \in A$ esetén, így $x^{-1} \in \bigcap H_i$. □

6.2.3. Definíció. *Legyen $K \subseteq G$. K által* **generált részcsoportnak** *nevezzük és $\langle K \rangle$-mal jelöljük a K-t tartalmazó legszűkebb részcsoportot. Ez nem más, mint a K-t tartalmazó részcsoportok metszete.*

Érdekes példái a részcsoportnak az egy elem által generált részcsoportok. Legyen $a \in G$. Ekkor $\langle a \rangle$ nyilván tartalmazza aa-t, aaa-t, stb. Az a elem n-szer önmagával vett szorzatát a^n-nel jelöljük . Ekkor a hatványozás azonosságai teljesülnek, azaz $a^{n+k} = a^n a^k$ és $(a^n)^k = a^{nk}$ tetszőleges n, k pozitív egészekre. $\langle a \rangle$ továbbá tartalmazza a^{-1}-et is, valamint ennek hatványait. Tekintsük az $\left(a^{-1}\right)^n a^n$ szorzatot.

Kiírva tényezőnként azt kapjuk, hogy a szorzat értéke e, a csoport egységeleme, tehát $\left(a^{-1}\right)^n = (a^n)^{-1}$. Jelöljük ezt az elemet a^{-n}-nel. A hatványozás tulajdonságai ezek alapján kiterjeszthetőek negatív hatványokra is:

$$a^k a^l = a^{k+l} \text{ és } \left(a^k\right)^l = a^{kl} \qquad \text{tetszőleges } k,l \in \mathbb{Z} \text{ esetén.}$$

Ezek szerint $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, azaz egy elem által generált részcsoport az elem (negatív és pozitív kitevős) hatványaiból áll.
Különböztessünk meg két esetet:

(1) a összes hatványa különböző

(2) vannak olyan k,l egész számok, hogy $a^k = a^l$. Ekkor $a^{k-l} = 1$, azaz van a-nak olyan hatványa, amely az egységelem. Legyen n a legkisebb ilyen szám.

6.2.4. Definíció. *A legkisebb ilyen számot a* ***rendjének*** *nevezzük, és* $\mathbf{o}(\mathbf{a})$*-val jelöljük („ordó a”-nak mondjuk). Ha nincs ilyen szám, végtelen rendű elemről beszélünk.*

$o(a) = n$ esetén $\langle a \rangle = \{1, a, a^2, \ldots a^{n-1}\}$. Ezen elemek különbözőek, mert $a^j = a^i$, $i > j$ esetén $a^{i-j} = 1$ lenne, ahol $i - j < n$. Továbbá minden $k \in \mathbb{Z}$ előáll $k = qn + r$ alakban, ahol $0 \leq r < n$, és $a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = 1^q a^r = a^r$, tehát a minden hatványa szerepel az első $n-1$ között. Ezzel igazoltuk, hogy jogos volt két látszólag távoli fogalomra ugyanazt a szót használni:

6.2.5. Állítás. *Egy elem rendje megegyezik az általa generált részcsoport rendjével.*

6.2.6. Definíció. *Az egy elem által generált csoportokat* **ciklikus csoportnak** *nevezzük és* C_n*-nel jelöljük.*

Következmény: Minden $n > 0$ egész számra van n elemű csoport.
Valóban, tekintsük az $\{1, a, a^2, \ldots a^{n-1}\}$ halmazt, ahol a szorzás a fent leírt módon történik. Ez egy n elemű ciklikus csoport.
n elemű ciklikus csoportra jó példa az n-edik komplex egységgyökök a szorzásra, a szabályos n-szög forgatásai vagy a számok összeadása modulo n. Ezek a csoportok lényegében nem különböznek:

6.2.7. Állítás. *Azonos rendű ciklikus csoportok izomorfak.*

BIZONYÍTÁS: Legyen $G = \langle a \rangle$ végtelen ciklikus csoport. Tekintsük a

$$\phi: G \to \mathbb{Z}$$

$\phi(a^n) = n$ megfeleltetést. Ez nyilván bijektív és művelettartó is, mert egy elem hatványai úgy szorzódnak, hogy a kitevők összeadódnak.
Legyen most $G = \langle a \rangle$, $|G| = n$. Legyen ε primitív n-edik egységgyök. Tekintsük a $\phi\left(a^k\right) = \varepsilon^k$ leképezést. ϕ izomorfizmus volta nyilvánvaló. □

Végül megjegyezzük, hogy

6.2.8. Állítás. *Ciklikus csoport részcsoportja ciklikus.*

BIZONYÍTÁS: Legyen $G = \langle a \rangle$ ciklikus, $H \leq G$. Feltehető, hogy H valódi részcsoport, különben nincs mit bizonyítani. Ekkor van H-ban egységelemtől különböző elem, ezért szerepel a-nak pozitív kitevős hatványa is. Legyen k a legkisebb olyan pozitív szám, hogy $a^k \in H$. Belátjuk, hogy ekkor $\langle a^k \rangle = H$. $\langle a^k \rangle \subseteq H$ nyilvánvaló. Tegyük fel, hogy $a^l \in H$. Ekkor vannak olyan $q \geq 0$, $0 \leq r < n$ számok, hogy $l = kq + r$. Ekkor $a^l \left(a^k\right)^{-q} = a^r \in H$, de mivel k volt a legkisebb H-ban szereplő hatványa, $r = 0$ lehet csak, tehát $k \mid l$, más szóval $H \subseteq \langle a^k \rangle$ is teljesül. □

6.2.9. Definíció. *Legyenek K, M részhalmazok G-ben. A KM szorzaton a*

$$KM = \{km \mid k \in K, \quad m \in M\}$$

halmazt értjük. Legyen $H \leq G$ részcsoport, $g \in G$. A Hg (gH) szorzatot H g szerinti jobboldali (baloldali) **mellékosztályának**, *g- t pedig a mellékosztály* **reprezentánsának** *nevezzük.*

6.2.10. Állítás. *Legyen $H \leq G$. Ekkor*

(1) *$g \in Hg$;*

(2) *a Hg mellékosztály minden eleme reprezentálja a Hg mellékosztályt;*

(3) *két különböző jobboldali mellékosztály vagy egybeesik, vagy diszjunktak;*

(4) *ha H véges, akkor bármely mellékosztály elemszáma megegyezik H rendjével.*

BIZONYÍTÁS: (1) $1 \in H$, így $g = 1g \in Hg$
(2) Legyen $h \in Hg$. Ekkor van olyan $h_1 \in H$, hogy $h = h_1 g$. A tetszőleges $x \in H$-ra érvényes $xh = (xh_1)g$ összefüggés igazolja, hogy $Hh \subseteq Hg$, és $xg = xh_1^{-1}h$ pedig azt, hogy $Hg \subseteq Hh$.
(1)-ből és (2)-ből közvetlenül következik (3).
A $h_1 g = h_2 g$ egyenlőséget g^{-1}-zel jobbról szorozva kapjuk, hogy $h_1 \neq h_2$ esetén $h_1 g$ és $h_2 g$ különböznek, ez igazolja (4)-et. □

Most már kimondhatjuk Lagrange tételét:

6.2.11. Tétel (Lagrange). *Legyen G véges, $H \leq G$. Ekkor H rendje osztja G rendjét.*

BIZONYÍTÁS: Osztályozzuk G-t a H szerinti jobboldali mellékosztályok szerint: $G = \bigcup Hg$. Jelölje k H mellékosztályainak számát. Mivel minden elem pontosan egy mellékosztályban szerepel, ezért $|G| = |\bigcup Hg|$ miatt $|G| = \sum |Hg| = k|H|$. A $k = |G|/|H|$ számot H G-beli **indexének** nevezzük és $|G : H|$-val jelöljük. $|G : H||H| = |G|$. □

Mivel egy elem rendje megegyezik az általa generált részcsoport rendjével:
Következmény: Egy elem rendje osztja a csoport rendjét.

Legyen $|G| = p$, p prím. Ekkor egy egységelemtől különböző csoportelem által generált ciklikus csoport rendje csak p lehet, azaz:
Következmény: Minden prímrendű csoport ciklikus.

6.3. Normálosztó, faktorcsoport, homomorfizmus

6.3.1. Definíció. *Legyen G csoport, $N \leq G$. N* **normálosztó** *G-ben $(N \triangleleft G)$, ha N jobboldali és baloldali mellékosztályai megegyeznek.*

Ez azt jelenti, hogy minden Nh mellékosztály előáll h_1N alakban. Mivel $h \in Nh$ és $h \in hN$, ez csak úgy lehet, ha $hN = Nh$ minden $h \in G$-re.

6.3.2. Állítás. *Az alábbi állítások ekvivalensek:*

(1) $N \triangleleft G$;

(2) $gN = Ng$ *minden* $g \in G$*-re;*

(3) $g^{-1}Ng = N$ *minden* $g \in G$*-re;*

(4) *tetszőleges* $h \in N$, $g \in G$ *esetén* $g^{-1}hg \in N$.

BIZONYÍTÁS: (1)⇔(2) világos.
(2)⇔(3) Szorozzuk meg a $gN = Ng$ egyenlőség mindkét oldalát balról g^{-1}-zel.
(3)⇒(4) nyilvánvaló.
(4)-ből következik, hogy $g^{-1}Ng \subseteq N$, valamint, hogy $gNg^{-1} \subseteq N$. Ez utóbbi tartalmazási relációt jobbról g-vel, balról g^{-1}-zel szorozva $N \subseteq g^{-1}Ng$-t kapjuk, amiből következik (3). □

A normálosztó jobboldali és baloldali mellékosztályainak egybeesését kihasználva új csoportot definiálhatunk. Legyen $N \triangleleft G$, $g,h \in G$. Vizsgáljuk az $NgNh$ szorzatot. Mivel $g^{-1}Ng = N$ és $NN = N$, $NgNh = Ngg^{-1}Ngh = Ngh$, azaz egy normálosztó két mellékosztályának szorzata megegyezik egy harmadik mellékosztállyal.
$N(Ng) = (Ng)N = Ng$, azaz maga a normálosztó egységelemként viselkedik, továbbá $Ng^{-1}Ng = NN = N$, azaz az új műveletre nézve minden mellékosztálynak van inverze. Tehát egy normálosztó szerinti mellékosztályok csoportot alkotnak a részhalmaz-szorzásra, mint műveletre.

6.3.3. Definíció. *Ezt a csoportot a G csoport N normálosztója szerinti* **faktorcsoportjának** *nevezzük, G/N („gé per en”)-nel jelöljük. Elemszáma megegyezik az N szerinti mellékosztályok számával, vagyis N indexével, azaz $|G/N| = |G : N|$.*

Megjegyzések: Abel-csoport minden faktorcsoportja kommutatív, ciklikus csoport minden faktorcsoportja ciklikus, hiszen $Nxy = Nyx$, illetve ha $G = \langle a \rangle$, akkor

$$G/N = \langle Na \rangle.$$

Egy faktorcsoport rendje osztója a csoport rendjének.

6.3.4. Definíció. *Legyenek G_1, G_2 csoportok. A $\phi: G_1 \to G_2$ leképezést homomorfizmusnak nevezzük, ha ϕ értelmezve van G_1 minden elemén és tetszőleges $a, b \in G_1$ esetén*

$$\phi(ab) = \phi(a)\phi(b).$$

Példák:

1. Legyen $G_1 = G_2$, ϕ a helybenhagyás.
2. Legyen $G_1 = (\mathbb{C}, +)$, $G_2 = (\mathbb{R}, +)$, azaz a komplex illetve valós számok additív csoportja. Legyen

$$\begin{aligned} \phi: \mathbb{C} &\to \mathbb{R} \\ a + bi &\to a, \end{aligned}$$

   vagyis rendeljük hozzá minden számhoz a valós részét. Ez a leképezés homomorfizmus, hiszen amikor komplex számokat összeadunk, a valós részek összeadódnak.
3. Jelölje $GL(n, \mathbb{R})$ az $n \times n$-es valós elemű invertálható mátrixok csoportját a mátrixszorzásra nézve. Legyen

$$\begin{aligned} \phi: GL(n, \mathbb{R}) &\to (\mathbb{R} - \{0\}, \cdot) \\ A &\to \det(A), \end{aligned}$$

   A determinánsok szorzástétele alapján ez homomorfizmus.

6.3.5. Definíció. *Legyen $\phi: G_1 \to G_2$ homomorfizmus. Azon G_1-beli elemek halmazát, amelyek képe 1_{G_2} (vagyis a G_2-beli egységelem) a leképezés* **magjának** *nevezzük és $Ker(\phi)$-vel jelöljük. Azon G_2-beli elemek halmazát, amelyek előállnak egy G_1-beli elem képeként, a leképezés* **képének** *nevezzük és $Im(\phi)$-vel jelöljük.*

$$\begin{aligned} Ker(\phi) &= \{g \in G_1 \mid \quad \phi(g) = 1_{G_2}\}, \\ Im(\phi) &= \{g \in G_2 \mid \quad \exists h \in G_1 \quad \phi(h) = g\}. \end{aligned}$$

6.3.6. Állítás. *Homomorfizmusnál egységelem képe egységelem, inverz képe a kép inverze, a kép részcsoport, a mag normálosztó:*

$$\begin{aligned} \phi(1_{G_1}) &= 1_{G_2}, \qquad \phi\left(g^{-1}\right) = \phi(g)^{-1}, \\ Im(\phi) &\leq G_2, \qquad Ker(\phi) \triangleleft G_1. \end{aligned}$$

BIZONYÍTÁS: Tetszőleges $g \in G_1$-re

$$\phi(1_{G_1})\phi(g) = \phi(1_{G_1}g) = \phi(g),$$

azaz $\phi(1_{G_1}) = 1_{G_2}$.

$$\phi(g)\phi\left(g^{-1}\right) = \phi\left(gg^{-1}\right) = \phi(1_{G_1}) = 1_{G_2},$$

azaz $\phi\left(g^{-1}\right) = \phi(g)^{-1}$.
Legyen $\phi(g_1) = h_1$, $\phi(g_2) = h_2$. Ekkor

$$h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2) \in \mathrm{Im}(\phi),$$

azaz $\mathrm{Im}(\phi) \leq G_2$, mivel azt már korábban láttuk, hogy egy elemmel együtt az inverze is benne van a képben.
Legyen $\phi(g_1) = \phi(g_2) = 1_{G_2}$ Ekkor

$$\phi(g_1g_2) = \phi(g_1)\phi(g_2) = 1_{G_2},$$

$\phi\left(g_1^{-1}\right) \in \mathrm{Ker}(\phi)$ világos, azaz $\mathrm{Ker}(\phi) \leq G_1$. Legyen $h \in G_1$. Ekkor

$$\phi\left(h^{-1}gh\right) = \phi\left(h^{-1}\right)\phi(g)\phi(h) = \phi\left(h^{-1}\right)1_{G_2}\phi(h) = 1_{G_2},$$

tehát $\mathrm{Ker}(\phi)$ normálosztó is. □

Láttuk, hogy minden homomorfizmus magja normálosztó. Most megmutatjuk, hogy minden normálosztó előáll, mint egy homomorfizmus magja, sőt, hogy a normálosztók bizonyos értelemben egyértelműen jellemzik a csoport homomorfizmusait.

6.3.7. Állítás. *Legyen $N \triangleleft G$. Ekkor a*

$$\phi: G \to G/N$$
$$g \to Ng$$

leképezés homomorfizmus. A homomorfizmus magja N, képe G/N. Ezt a leképezést G-nek G/N-re való **természetes homomorfizmusának** *nevezzük.*

BIZONYÍTÁS: Nyilvánvaló a normálosztó definíciójából. □

6.3.8. Tétel (homomorfizmus tétel). *Legyen $\phi: G_1 \to G_2$ homomorfizmus. Ekkor*

$$G_1/Ker(\phi) \simeq Im(\phi).$$

BIZONYÍTÁS: Tekintsük a $\sigma: \mathrm{Im}(\phi) \to G_1/\mathrm{Ker}(\phi)$, $\sigma(\phi(g)) = \mathrm{Ker}(\phi)g$ leképezést. Megmutatjuk, hogy σ izomorfizmus. Legyen $g \in \mathrm{Im}(\phi)$ tetszőleges, $x \in G_1$ olyan, hogy $\phi(x) = g$, $h \in \mathrm{Ker}(\phi)$. Ekkor $\phi(h) = 1_{G_2}$ miatt $\phi(xh) = \phi(x)\phi(h) =$

g, vagyis a ϕ leképezésnél a $\mathrm{Ker}(\phi)x$ mellékosztály minden eleme ugyanabba az elembe, g-be képződik.
Legyen most $\phi(y) = g$. Ekkor $\phi\left(yx^{-1}\right) = \phi(y)\phi\left(x^{-1}\right) = gg^{-1} = 1_{G_2}$, azaz $yx^{-1} = k \in \mathrm{Ker}(\phi)$, $y = kx$, azaz y benne van az x szerinti (jobboldali) mellékosztályban, azaz $\mathrm{Im}(\phi)$ tetszőleges elemébe $\mathrm{Ker}(\phi)$ egy mellékosztálya képződik le. Tehát σ kölcsönösen egyértelmű. Másrészt σ művelettartó: Legyen ugyanis

$$\sigma\left(x'\right) = \mathrm{Ker}(\phi)x \qquad \sigma\left(y'\right) = \mathrm{Ker}(\phi)y.$$

Ekkor

$$\phi(x) = x' \qquad \phi(y) = y',$$

ezért $\phi(xy) = \phi(x)\phi(y) = x'y'$, így

$$\sigma\left(x'y'\right) = xy\mathrm{Ker}(\phi) = x\mathrm{Ker}(\phi)y\mathrm{Ker}(\phi) = \sigma\left(x'\right)\sigma\left(y'\right),$$

tehát σ izomorfizmus. □

Megjegyzés: $\mathrm{Im}(\phi) \simeq G/\mathrm{Ker}(\phi)$ miatt $|G| = |\mathrm{Im}(\phi)||\mathrm{Ker}(\phi)|$, tehát $|\mathrm{Im}(\phi)|$ osztja $|G|$-t.

Példák:

1. A homomorfizmusra adott példákból látszik, hogy tetszőleges G csoportra $G/\{1\} \simeq G$. $(\mathbb{C},+)/i(\mathbb{R},+) \simeq (\mathbb{R},+)$, hisz itt a 0-ba a tiszta képzetes számok képződnek. A 3. példában a mag az 1 determinánsú mátrixokból ($SL(n,\mathbb{R})$) áll, azaz $SL(n,\mathbb{R}) \triangleleft GL(n,\mathbb{R})$ és $GL(n,\mathbb{R})/SL(n,\mathbb{R}) \simeq (\mathbb{R}\setminus\{0\},\cdot)$.

6.4. Permutációcsoportok, Cayley-tétel

Mint egy példában említettük, n elem összes permutációja csoportot alkot a kompozícióra, mint műveletre. Ennek a csoportnak $n!$ eleme van. Az

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

permutáció, ahol $\{1,2,\dots,n\} = \{i_1,i_2,\dots,i_n\}$, azt a permutációt jelöli, amelynél az 1 képe i_1, a 2 képe i_2, stb. Ennélfogva megegyezik a

$$\begin{pmatrix} k_1 & k_2 & \dots & k_n \\ i_{k_1} & i_{k_2} & \dots & i_{k_n} \end{pmatrix}$$

permutációval, ahol $\{1,2,\dots,n\} = \{k_1,k_2,\dots,k_n\}$. Permutációk szorzását a függvénykompozícióval ellentétben balról jobbra végezzük, például:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$$

A permutációk szorzása nem kommutatív, az előző két permutációt fordított sorrendben összeszorozva:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

A permutációkat ciklikus módon is felírhatjuk. Az $(i_1, i_2, \ldots, i_k)$ **ciklus**, ahol $i_1, i_2, \ldots, i_k$ különbözőek, azt a σ permutációt jelöli, amelynél i_1 i_2-be, i_2 i_3-ba, i_{k-1} i_k-ba, i_k pedig i_1-be képződik, a többi elem helyben marad.

$$(i_1, i_2, \ldots, i_k) = \begin{pmatrix} i_1 & i_2 & \ldots & i_k \\ i_2 & i_3 & \ldots & i_1 \end{pmatrix}$$

6.4.1. Definíció. *A permutációnál helyben maradó elemeket* **fixpontoknak** *nevezzük. A „kettes” ciklusokat ((i, j), $i \neq j$)* **transzpozíciónak** *nevezzük.*

A ciklusokat ugyanúgy szorozzuk össze, mint a permutációkat általában. Diszjunkt ciklusok felcserélhetőek, hiszen különböző elemeket mozgatnak. Világos, hogy

6.4.2. Állítás. *Minden permutáció előáll diszjunkt ciklusok szorzataként. Ez a felírás sorrendtől eltekintve egyértelmű.*

Például

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 7 & 5 & 1 & 6 \end{pmatrix} = (1476)(23)(5).$$

A fixpontok (egy hosszú ciklusok) a ciklikus felírásnál elhagyhatók. Ekkor $\sigma = (1476)(23)$. Vegyük észre, hogy $(i_1, i_2, \ldots, i_k) = (i_1, i_2)(i_1, i_3)\ldots(i_1, i_k)$, azaz minden ciklus (így minden permutáció) felírható transzpozíciók szorzataként.
$(i, j) = (1, i)(1, j)(1, i)$ miatt kimondható az alábbi

6.4.3. Tétel. *Az $(1,2)$, $(1,3)$, …, $(1,n)$ transzpozíciók generálják S_n-et.*

Az $(2, \ldots, n)(1,2) = (1,2,\ldots,n)$ és $(2,\ldots,n)^{-k+1}(1,2)\,(2,\ldots,n)^{k-1} = (1,k)$ összefüggés megmutatja, hogy S_n két elemmel generálható:

6.4.4. Tétel. $S_n = \langle (1,2,\ldots,n), (1,2) \rangle$.

6.4.5. Definíció. *Legyen σ permutáció. Az $i < j$ elemek* **inverzióban** *vannak, ha $\sigma(i) > \sigma(j)$. Egy permutációt* **párosnak** *illetve* **páratlannak** *nevezünk, ha a benne lévő inverziók száma páros illetve páratlan. A páros permutációk halmazát A_n-nel jelöljük.*

A definícióból rögtön levezethető, hogy a paritás „összeszorzódik”. Ugyanis, ha egy π permutációt megszorzunk az (i, j) $(i < j)$ transzpozícióval balról, akkor az inverziók száma páratlannal változik: az $(ij)\pi$ permutációban π-hez képest helyet cserél $\pi(i)$ és $\pi(j)$, mindkettőnek megváltozik a viszonya a köztük lévő elemekkel $(\pi(i+1), \ldots, \pi(j-1))$, ez páros sok változás az inverziók számában, valamint egymáshoz képest is változnak, ez még egy, azaz összesen páratlan sok változás lesz.

Mivel minden permutáció előáll transzpozíciók szorzataként, azt kapjuk, hogy páros permutációt párossal szorozva párosat, páros permutációt páratlannal szorozva páratlant, páratlan permutációt párossal szorozva páratlant, páratlan permutációt páratlannal szorozva pedig páros permutációt kapunk. Figyelembe véve, hogy az identitás páros permutáció, adódik az alábbi

6.4.6. Tétel. *$A_n \triangleleft S_n$, $|S_n : A_n| = 2$, azaz a páros permutációk normálosztót alkotnak S_n-ben, ennek indexe 2, így ugyanannyi páros permutáció van, mint páratlan.*

BIZONYÍTÁS: Tekintsük a

$$\begin{aligned} \phi: S_n &\to C_2 \\ \pi &\to \begin{cases} 1 & \text{ha } \pi \text{ páros} \\ a & \text{ha } \pi \text{ páratlan} \end{cases} \end{aligned}$$

leképezést. (C_2 a szokásos, $C_2 = \{1, a\}$, $a^2 = 1$.) A fentiek miatt ϕ homomorfizmus. $\mathrm{Ker}(\phi) = A_n$. Lévén minden homomorfizmus magja normálosztó, adódik az állítás első fele. $\mathrm{Im}(\phi) = C_2$ miatt $S_n/A_n \simeq C_2$, tehát $|S_n : A_n| = 2$, ami igazolja az állítás második felét. □

6.4.7. Definíció. *Az S_n szimmetrikus csoport részcsoportjait n-ed fokú* **permutációcsoportoknak** *nevezzük.*

Permutációcsoportokat könnyű kezelni. Mégis csak elvi jelentőségű a következő tétel:

6.4.8. Tétel (Cayley). *Minden csoport izomorf egy permutációcsoporttal.*

BIZONYÍTÁS: Megmutatjuk hogy G izomorf S_G egy részcsoportjával, ami azt jelenti, hogy izomorf $S_{|G|}$ egy részcsoportjával is. Tekintsük a

$$\begin{aligned} \phi: G &\to S_G \\ h &\to \begin{pmatrix} g \\ gh \end{pmatrix} \end{aligned}$$

megfeleltetést, azaz minden $h \in G$-hez rendeljük hozzá G elemeinek azt a permutációját, amely bármely g-hez annak h-szorosát, gh-t rendeli. ϕ valóban a csoportelemek egy permutációja, ehhez azt kell megmutatni, hogy különböző csoportelemekhez különböző csoportelemeket rendel. Nyilvánvaló, hogy $g_1 h = g_2 h$ esetén $g_1 = g_2$. Ez a megfeleltetés injektív, hiszen minden permutáció mást rendel a csoport egységeleméhez. A leképezés művelettartó, mert

$$\phi(h_1)\phi(h_2) = \begin{pmatrix} g \\ gh_1 \end{pmatrix} \begin{pmatrix} g \\ gh_2 \end{pmatrix} = \begin{pmatrix} g \\ gh_1 h_2 \end{pmatrix} = \phi(h_1 h_2).$$

Ezzel igazoltuk állításunkat. □

A tétel azért csak elvi jelentőségű, mert ha valóban mindent tudnánk a permutációcsoportokról, mindent tudnánk az összes csoportról, ez pedig nem áll. Másrészt a tétel nem éles. A tétel alapján ugyanis D_3 izomorf S_6 egy részcsoportjával, de $D_3 \simeq S_3$ miatt már S_3-nak is van ilyen része (önmaga). A kocka egybevágósági csoportja, G, 48 elemű. A Cayley-tétel alapján ezért G része S_{48}-nak. Ha azonban a kocka oldalait megszámozzuk 1-től 6-ig, akkor minden transzformáció felfogható a hat lap, így az 1–6 számok permutációjaként. Precízen megfogalmazva tekintsük azt a

$$\phi: G \to S_6$$

leképezést, amely minden transzformációhoz hozzárendeli azt a permutációt, ahogy a lapokat permutálja. $\mathrm{Ker}(\phi) = \{1\}$, hisz ha minden lap fix, a kocka is helyben marad. Tehát $G \simeq \mathrm{Im}(\phi)$, azaz G izomorf S_6 egy részcsoportjával.

6.5. Direkt szorzat, Abel-csoportok

Ebben a fejezetben először egy csoportkonstrukciót fogunk bemutatni:
Legyenek A, B csoportok. Tekintsük az $A \times B = \{(a,b) \mid a \in A, b \in B\}$ halmazt. Legyen $(a_1,b_1)\cdot(a_2,b_2) = (a_1a_2, b_1b_2)$.

6.5.1. Állítás. *$(A \times B, \cdot)$ csoport.*

BIZONYÍTÁS: $\cdot$ asszociatív, mert koordinátánként az. $1_{A\times B} = (1_A, 1_B)$ és

$$(a,b)\cdot\left(a^{-1}, b^{-1}\right) = (1_A, 1_B)$$

igazolja álltásunkat. □

6.5.2. Definíció. *A fent leírt $(A \times B, \cdot)$ csoportot az A és B csoportok* **direkt szorzatának** *nevezzük és $A \oplus B$-vel („a kereszt bé") jelöljük. Ha nem okoz zavart, gyakran $A \oplus B$ helyett is $A \times B$-t írunk. Gyakran direkt szorzat helyett direkt összegről beszélünk, a két fogalom közt mi nem teszünk különbséget.*

6.5.3. Állítás. *$|A \oplus B| = |A||B|$. Valamint vannak olyan $N_1, N_2 \triangleleft A \oplus B$, hogy*

(1) *$N_1 \simeq A$, $N_2 \simeq B$;*

(2) *$N_1 \cap N_2 = 1_{A\oplus B}$;*

(3) *$A \oplus B = N_1 \cdot N_2$;*

(4) *$a \in N_1, b \in N_2$ esetén $a \cdot b = b \cdot a$;*

(5) *$(A \oplus B)/N_1 \simeq N_2$, és $(A \oplus B)/N_2 \simeq N_1$.*

BIZONYÍTÁS: Az állítás első fele világos. A második feléhez legyenek

$$N_1 = \{(a, 1_B) \mid a \in A\}, \qquad N_2 = \{(1_A, b) \mid b \in B\}.$$

Az (1), (2) pontok nyilvánvalóan teljesülnek. (3) az $(a,b) = (a,1_B)\cdot(1_A,b)$, (4) pedig az $(a,1_B)\cdot(1_A,b) = (a,b) = (1_A,b)\cdot(a,1_B)$ azonosságból következik. (5)-höz tekintsük a

$$\begin{aligned} \phi: A \oplus B &\to B \\ (a,b) &\to b \end{aligned}$$

leképezést. $\mathrm{Ker}(\phi) = N_1$, $\mathrm{Im}(\phi) = B$ alapján a homomorfizmus tételből $A \oplus B/N_1 \simeq B$ adódik. Hasonlóan kapjuk (5) második felét. □

Érdekes megjegyezni, hogy az előző állítás (2)-es és (3)-as pontja garantálja azt, hogy egy csoport előálljon két csoport direkt szorzataként, azaz:

6.5.4. Állítás. *Legyen G csoport, $N_1, N_2 \triangleleft G$, és teljesüljenek az előző állítás (2)-es és (3)-as pontjai, azaz $N_1 \cap N_2 = 1_G$ és $N_1 N_2 = G$. Ekkor $G \simeq N_1 \oplus N_2$. N_1 és N_2 szerepe megegyezik az előző állításbeli N_1 és N_2 szerepével.*

Az állítás bizonyítását elhagyjuk. Nem azért, mert meghaladja tudásunkat, hanem, mert nem lesz rá szükségünk a továbbiakban. Annál fontosabb a továbbiak szempontjából maga az állítás. Ha egy G csoportban van két a fenti tulajdonsággal rendelkező N_1 és N_2 normálosztó, akkor azt mondjuk, hogy G a két normálosztó direkt szorzata (összege), $G = N_1 \oplus N_2$. A két állítás közötti szoros összefüggés indokolja az azonos szóhasználatot. Ha valami véletlen folytán mégis meg akarjuk különböztetni a kétféle definíciót, az első esetben **külső direkt szorzatról**, a másodikban **belső direkt szorzatról** beszélünk. Csoportok direkt szorzatára most nem mutatunk példát, hamarosan végtelen sokat látunk rá. Előbb azonban megfogalmazunk egy természetes módon felmerülő csoportszerkesztési módszert:

6.5.5. Definíció. *Legyenek A_i, $i \in \{1,\dots,n\}$ csoportok. Tekintsük az $(a_1,\dots,a_n)$ alakú rendezett n-eseket a koordinátánként való szorzással. Ez csoportot alkot, amely az A_i csoportok direkt szorzata, jelölése $\bigoplus_{i=1}^{n} A_i$.*

Csoportok szerkezetéről általában keveset tudunk. A fenti (bizonyítás nélkül közölt) állítás azt írja le, mikor áll elő egy csoport direkt szorzatként. Kevés az ilyen csoport, de a csoportok nagy osztálya leírható a direkt szorzat segítségével:

6.5.6. Tétel (Véges Abel-csoportok alaptétele). *Legyen A véges Abel-csoport. A előáll prímhatvány rendű ciklikus csoportok direkt összegeként. Az előállításban szereplő prímhatványok egyértelműek, maguk a direkt összeadandók nem.*

Példák:

1. $C_6 = \langle a \rangle$, $6 = 2 \cdot 3$. A tétel alapján $C_6 = C_2 \oplus C_3$. Valóban, $\{a^2, a^4, e\} = C_3$, $\{a^3, e\} = C_2$, mindkét halmaz normálosztó, metszetük $\{e\}$. $e = ee$, $a = a^4a^3$, $a^2 = a^2e$, $a^3 = ea^3$, $a^4 = a^4e$, $a^5 = a^2a^3$, tehát a két normálosztó szorzata C_6.

2. Hasonlóan igaz, hogy $C_{12} = C_3 \oplus C_4$, sőt legyen $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Ekkor $C_n = C_{p_1^{\alpha_1}} \oplus \dots \oplus C_{p_k^{\alpha_k}}$.

3. A tétel alapján könnyű megszámolni, hogy adott n-re hány n-edrendű Abel-csoport létezik. Legyen $n = 100$. 100 az alábbi módokon bontható fel prímhatványok szorzatára: $4 \cdot 25 = 2 \cdot 2 \cdot 25 = 4 \cdot 5 \cdot 5 = 2 \cdot 2 \cdot 5 \cdot 5$. Így 4 féle 100 elemű Abel-csoport létezik: $C_4 \oplus C_{25} = C_{100}$, $C_2 \oplus C_2 \oplus C_{25} = C_2 \oplus C_{50}$, $C_4 \oplus C_5 \oplus C_5 = C_{20} \oplus C_5$ és $C_2 \oplus C_2 \oplus C_5 \oplus C_5 = C_{10} \oplus C_2 \oplus C_5 = C_{10} \oplus C_{10}$. Ugyanis a megjegyzések alapján $C_2 \oplus C_{25} = C_{50}$, de $C_2 \oplus C_2 \neq C_4$.

6.6. Csoportok megadása, példák

D_n a szabályos n szög szimmetriacsoportja. Jelöljük az óra járásával ellenkező irányban $2\pi/n$-nel való forgatást f-fel, a tengelyes tükrözéseket $t_1, t_2, \dots, t_n$-nel. Két szomszédos tengely szöge π/n, így két szomszédos tengelyre való tükrözés szorzata f. $t_i t_{i+1} = f$ balról t_i-vel szorozva $t_{i+1} = t_i f$-et, jobbról t_{i+1}-gyel szorozva pedig $t_i = f t_{i+1}$-et kapjuk, amiből

$$t_i = t_1 f^{i-1} \text{ és } t_1 f = f^{n-1} t_1 = f^{-1} t_1$$

adódik. Ezekből az összefüggésekből felírhatjuk a csoport művelettáblázatát, az úgynevezett Cayley-táblázatot.

6.6.1. Definíció. *Legyen $G=\{g_1, g_2, \dots, g_n\}$ csoport. Ekkor azt az $n \times n$-es táblázatot, amely i-edik sorának j-edik oszlopában $g_i g_j$ áll, a csoport* **Cayley-táblázatának** *nevezzük.*

$n = 4$ esetén ez a következő:

D_4	1	f	f^2	f^3	t_1	t_2	t_3	t_4
1	1	f	f^2	f^3	t_1	t_2	t_3	t_4
f	f	f^2	f^3	1	t_4	t_1	t_2	t_3
f^2	f^2	f^3	1	f	t_3	t_4	t_1	t_2
f^3	f^3	1	f	f^2	t_2	t_3	t_4	t_1
t_1	t_1	t_2	t_3	t_4	1	f	f^2	f^3
t_2	t_2	t_3	t_4	t_1	f^3	1	f	f^2
t_3	t_3	t_4	t_1	t_2	f^2	f^3	1	f
t_4	t_4	t_1	t_2	t_3	f	f^2	f^3	1

Nagy n-ek esetén ez a megadás kissé nehézkes. Legyen $t = t_1$. Ekkor $D_n = \{f^i, tf^i \mid 0 \le i < n\}$, ahol $ft = tf^{n-1} = tf^{-1}$. Ezen egyetlen szorzási szabály segítségével a csoport bármely két elemét össze tudjuk szorozni. Például

$$\begin{aligned}(tf^i)(tf^j) &= t\left(f^i t\right) f^j = tf^{i-1}(ft) f^j = \\ &= tf^{i-1}tf^{-1}f^j = tf^{i-1}tf^{j-1} = \ldots = ttf^{j-i} = f^{j-i}\end{aligned}$$

ahol a kitevők összeadását és kivonását modulo n értjük.
Most tekintsük át a legföljebb 10 elemszámú csoportokat (annak bizonyítását, hogy más csoport nincs, általában nem közöljük):
1 elemű csoport csak az egységelemből álló csoport van.
Mivel p prím esetén tudjuk, hogy a p-edrendű csoport ciklikus, ezért $2,3,5,7$ elemszámú csoport izomorfizmus erejéig csak egy van, a megfelelő rendű ciklikus csoport.
Izomorfizmus erejéig kétféle 4 elemű csoport van. Az egyik C_4, a másik Cayley-táblázata a következő:

V	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Mint látható, mindhárom e-től különböző elem másodrendű, a csoport kommutatív, és két másodrendű elem szorzata a harmadik. Ezt a csoportot Klein-féle csoportnak hívják, V-vel jelölik és izomorf $C_2 \times C_2$-vel. V és C_4 nem izomorfak az Abel-csoportok alaptétele miatt. Könnyű igazolni, hogy más 4-elemű csoport nincs.
Hatelemű csoportból kettőt ismerünk, $C_6 \simeq C_2 \times C_3$ és $D_3 \simeq S_3$. Ezek nem izomorfak, mert az egyik kommutatív, a másik nem. Más 6 elemű csoport nincs.
Izomorfizmus erejéig öt nyolcadrendű csoport létezik. Az Abel-félék $C_2 \times C_2 \times C_2$, $C_2 \times C_4$ és C_8. A nem kommutatívak közül D_4-et már ismerjük. A másik nem kommutatív nyolc elemű csoport a **kvaterniócsoport**:

$$Q = \{1, -1, i, j, k, -i, -j, -k\}$$

ahol

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j$$

valamint minden $g \in Q$-ra $(-1)g = g(-1) = -g$.
Ezekből az összefüggésekből bármely két elem szorzata kiszámítható. Például:

$$\begin{aligned}ji = ji1 = ji(-1)(-1) = jij^2(-1) = j(ij)j(-1) = \\ = (jk)j(-1) = ij(-1) = k(-1) = -k\end{aligned}$$

A csoport Cayley-táblázata a következő:

Q	1	-1	i	j	k	$-i$	$-j$	$-k$
1	1	-1	i	j	k	$-i$	$-j$	$-k$
-1	-1	1	$-i$	$-j$	$-k$	i	j	k
i	i	$-i$	-1	k	$-j$	1	$-k$	j
j	j	$-j$	$-k$	-1	i	k	1	$-i$
k	k	$-k$	j	$-i$	-1	$-j$	i	1
$-i$	$-i$	i	1	$-k$	j	-1	k	$-j$
$-j$	$-j$	j	k	1	$-i$	$-k$	-1	i
$-k$	$-k$	k	$-j$	i	1	j	$-i$	-1

D_4 és Q nem izomorfak, mert míg Q-ban hat negyedrendű elem van $(i, j, k, -i, -j, -k)$, addig D_4-ben csak kettő $\left(f, f^3\right)$.
9 elemű csoportból két nem izomorf létezik. Ezek C_9 és $C_3 \times C_3$.
Tíz elemű csoportok a diéder és a ciklikus csoport: D_5 és $C_{10} \simeq C_2 \times C_5$. Más 10-ed rendű csoport nincs, ezek nyilván nem izomorfak.

6.7. További alapfogalmak

Az előző fejezetben olyan struktúrákkal foglalkoztunk, amelyekben egy művelet volt értelmezve. Gyakran merülnek fel olyan algebrai objektumok, ahol lehet összeadni és szorozni is.

6.7.1. Definíció. *Az R halmaz a $+$ és $\cdot$ műveletekkel* **gyűrű**, *ha*

(1) $a+b=b+a \quad \forall\, a,b \in R$ *esetén;*

(2) $(a+b)+c=a+(b+c) \quad \forall\, a,b,c \in R$ *esetén;*

(3) *van olyan R-beli elem (jelöljük 0-val), hogy* $a+0=0+a=a \quad \forall\, a \in R$ *esetén;*

(4) $\forall\, a \in G$*-re* $\exists\, a' \in G$ *úgy, hogy* $a+a'=0$ *(ahol 0 a (3)-ban szereplő elem);*

(5) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall\, a,b,c \in R$ *esetén;*

(6) $(a+b) \cdot c = a \cdot c + b \cdot c \quad \forall\, a,b,c \in R$ *esetén;*

(7) $c \cdot (a+b) = c \cdot a + c \cdot b \quad \forall\, a,b,c \in R$ *esetén.*

Az első négy axióma azt mondja ki, hogy R Abel-csoport az összeadásra nézve, az ötödik pedig, hogy félcsoport a szorzásra nézve. A szorzás $\cdot$-ját gyakran elhagyjuk. A hatodik illetve hetedik axiómákat jobboldali illetve baloldali **disztributív** törvénynek nevezzük. Ha a szorzás is kommutatív, **kommutatív gyűrűről**, ha van a szorzásra nézve egységelem, **egységelemes gyűrűről** beszélünk. A harmadik axiómában említett elemet **nullelemnek** nevezzük. Egy R-beli a elem összeadásra vonatkozó inverzét (negyedik axióma) a **ellentettjének** hívjuk, és $-a$-val jelöljük. Az $a-b=a+(-b)$ műveletet **kivonásnak** nevezzük. Tekintsük most át a gyűrűaxiómák közvetlen következményeit. Ezek arról szólnak, hogy egy gyűrűben teljesülnek azok a műveleti tulajdonságok, amiket elvárunk egy gyűrűtől:

6.7.2. Állítás. *Legyen R gyűrű, $a,b \in R$*

(1) *a nullelem és az ellentett egyértelmű;*

(2) $0a = a0 = 0$*;*

(3) $(-a)\,b = -ab$*;*

(4) $(-a)\,(-b) = ab$*.*

BIZONYÍTÁS: Az első pont annak következménye, hogy R Abel-csoport az összeadásra. Az $a0 = a\,(0+0) = a0+a0$ egyenlőség mindkét oldalához $a0$ inverzét adva a második pont adódik. A harmadik pont az $ab+(-a)\,b = (a-a)\,b = 0b = 0$ egyenlőség következménye, a negyedik pedig ennek folyománya, hisz: $(-a)\,(-b) = -\,(a\,(-b)) = -\,(-ab) = ab$. □

Példák:

1. Az egész számok kommutatív, egységelemes gyűrűt alkotnak a szokásos összeadásra és szorzásra. Jele $\mathbb{Z}$.

2. Az m-mel osztható egész számok kommutatív, egységelemes gyűrűt alkotnak a szokásos műveletekre.

3. A racionális, a valós, a komplex számok kommutatív, egységelemes gyűrűt alkotnak a szokásos műveletekre.

4. Az $n \times n$-es komplex (valós, racionális, egész) mátrixok egységelemes nemkommutatív gyűrűt alkotnak a mátrixösszeadásra és mátrixszorzásra. Az egységelem az egységmátrix.

5. Egy H halmaz részhalmazai az

$$A+B = (A \cup B) \setminus (A \cap B) \text{ és } AB = A \cap B$$

műveletekre kommutatív gyűrűt alkotnak. Az összeadás neve szimmetrikus differencia. Az elnevezést az

$$(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$$

összefüggés indokolja. A nullelem az üres halmaz, az egységelem maga a H. Vegyük észre, hogy tetszőleges $a \in R$ esetén $a^2 = a$. Az ezzel a tulajdonsággal rendelkező gyűrűt **Boole-gyűrűnek** nevezzük. Az ilyen gyűrűkben az $a+a = 0$ egyenlőség is teljesül.

6. A komplex (valós, racionális, egész) együtthatós polinomok gyűrűt alkotnak a polinomösszeadásra és szorzásra. Jelölése $\mathbb{C}[x]$ ($\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$).

7. A valós ($[a,b]$ intervallumon értelmezett) (folytonos) függvények gyűrűt alkotnak az $(f+g)(x) = f(x)+g(x)$ és $fg(x) = f(x)g(x)$ műveletekkel.

8. Legyen n egész szám. Tekintsük az egész számok n-nel vett osztásakor vett maradékokat, $\{m_0, m_1, \ldots, m_{n-1}\}$, a $0, 1, \ldots, n-1$ maradékoknak megfelelően. Itt például m_2 az a halmaz, amely az összes n-el osztva 2 maradékot adó számot tartalmazza. Legyen

$$m_i + m_j = \begin{cases} m_{i+j} & \text{ha } i+j < n \\ m_{i+j-n} & \text{ha } i+j \geq n \end{cases}$$
$$m_i m_j = m_r, \text{ ahol } ij = km+r, \quad 0 \leq r < n$$

A nullelem m_0, az egységelem m_1. Ezt a gyűrűt $\mathbb{Z}_m$-mel jelöljük és a **modulo n maradékosztályok (maradékok) gyűrűjének** nevezzük. Ha ez nem okoz félreértést, akkor m_i helyett i-t írunk.

6.7.3. Definíció. *Legyen R gyűrű. Az $0 \neq a \in R$ elemet jobboldali (baloldali)* **nullosztónak** *nevezzük, ha van hozzá $0 \neq b \in R$, hogy $ab = 0$ ($ba = 0$).*

Világos, hogy egy gyűrűben pontosan akkor van baloldali nullosztó, ha van jobboldali is.

6.7.4. Definíció. *Az R gyűrűt* **nullosztómentesnek** *nevezzük, ha nincs benne nullosztó. A kommutatív nullosztómentes gyűrű neve* **integritási tartomány**.

Példák:

1. Az egész számok, a páros számok gyűrűje integritási tartomány.

2. $\mathbb{Z}_6$-ban $2 \cdot 3 = 0$, ezért a 2 illetve a 3 nullosztók.

3. Egy $n \times n$-es A mátrix baloldali nullosztó, ha az $AB = 0$ mátrixegyenletnek van 0-tól különböző megoldása, ami ekvivalens azzal, hogy az $A\underline{x} = 0$ lineáris egyenletrendszernek van nemtriviális megoldása, azaz, ha A nem invertálható. Ugyanezzel ekvivalens az, hogy A jobboldali nullosztó.

6.7.5. Definíció. *Legyen R gyűrű. Az $R' \subseteq R$ halmazt R* **részgyűrűjének** *nevezzük és $R' \leq R$-rel jelöljük, ha R' is gyűrű ugyanazokra a műveletekre nézve. R és $\{0\}$ mindig részgyűrűk, ezeket triviális, az ettől eltérő részgyűrűket pedig* **valódi részgyűrűknek** *nevezzük.*

A részcsoport-csoport viszonyhoz hasonlóan bizonyítható gyűrűk esetén is a következő

6.7.6. Állítás. *Legyen R gyűrű. Az $R' \subseteq R$ halmaz R részgyűrűje, ha zárt a műveletekre és minden elemmel együtt benne van annak ellentettje is.*

Példák:

1. Az egész számoknak részgyűrűjét alkotják az m-mel osztható egész számok.
2. A racionális számok részgyűrűje a valós, a valós számok részgyűrűje a komplex számok gyűrűjének.
3. Az $n \times n$-es komplex (valós, racionális, egész) mátrixoknak részgyűrűjét alkotják azon mátrixok, amelyeknek az utolsó sora és utolsó oszlopa 0.

$\mathbb{Z}$ összes részgyűrűjét írja le az alábbi

6.7.7. Állítás. *$\mathbb{Z}$ minden részgyűrűje az (1) példában leírt módon kapható.*

BIZONYÍTÁS: Legyen $R \leq \mathbb{Z}$, $R \neq \{0\}$. Ekkor R-ben van pozitív elem is. Legyen a legkisebb R-beli pozitív egész m. Megmutatjuk, hogy R m többszöröseiből áll. Legyen $s \in R$. Ekkor vannak olyan $q \in \mathbb{Z}$, $0 \leq r < m$ számok, hogy

$$s = qm + r.$$

$s \in R$ és $qm = m + \ldots + m \in R$ miatt $s - qm = r \in R$. De m volt a legkisebb pozitív R-beli szám, ezért $r = 0$ lehet csak, azaz m osztja s-t. □

6.8. Az egész számok gyűrűje

Az egész számok gyűrűjének számelmélete az oszthatóság és a prímszám fogalmán alapul.

6.8.1. Definíció. *Legyenek $a, b \in \mathbb{Z}$. Azt mondjuk, hogy b* **osztható** *a-val, vagy a* **osztója** *b-nek (a* **osztja** *b-t), ha van olyan $q \in \mathbb{Z}$, amelyre $b = aq$. Jelölése $a \mid b$.*

6.8.2. Definíció. *A p 0-tól, 1-től és -1-től különböző egész számot* **prímszámnak** *nevezzük, ha $a, b \in \mathbb{Z}$, $p \mid ab$ esetén $p \mid a$ vagy $p \mid b$.*

Oszthatóság szempontjából a negatív számok ugyanúgy viselkednek, mint a pozitívak, a és $-a$ osztói megegyeznek, valamint ha $a \mid b$, akkor $-a \mid b$ is. Ezért ezentúl csak a nemnegatív számokkal foglalkozunk, **számon mindig nemnegatív egész** (természetes) **számot értünk**.

6.8.3. Definíció. *A p 0-tól és 1-től különböző egész számot* **fölbonthatatlannak** *nevezzük, ha $a, b \in \mathbb{N}$, $p = ab$ esetén $p = a$ vagy $p = b$.*

6.8.4. Tétel. *A természetes számok körében a fölbonthatatlanok megegyeznek a prímekkel.*

Ezt a tételt nem bizonyítjuk. Nem bonyolult a bizonyítása, de számunkra érdektelen. A tétel maga azért fontos, mert ezen múlik a számelmélet alaptétele:

6.8.5. Tétel. *Minden 1-nél nagyobb szám a sorrendtől eltekintve egyértelműen előáll prímszámok szorzataként, azaz tetszőleges $n \in \mathbb{N}$ esetén*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i},$$

ahol a p_i-k prímszámok és az $\alpha_i > 0$ kitevők egyértelműek.

A fenti fölbontást n kanonikus alakjának nevezzük. Az $\alpha_i > 0$ kikötésre azért van szükség, mert különben tetszőleges n-et nem osztó prímeket hozzávehetnénk a felbontáshoz 0 kitevővel. Ekkor a felbontás nem lenne egyértelmű.

Egy szám kanonikus alakjának segítségével könnyen meghatározhatóak a szám osztói.

6.8.6. Állítás. *Legyen $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $d \mid n$. Ekkor d előáll*

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

alakban, ahol $\beta_i \leq \alpha_i$. Minden ilyen alakú szám osztója n-nek.

Megjegyzés: Természetesen a fenti alak nem feltétlenül d kanonikus alakja, hisz a β_i számok 0-k is lehetnek.
A számok kanonikus alakjának segítségével meghatározható két szám legnagyobb közös osztója és legkisebb közös többszöröse. Legyenek $n, k \in \mathbb{N}$. n kanonikus alakját „pótoljuk” ki a k-ban szereplő, n-ben nem szereplő prímekkel 0 kitevővel és fordítva. Ekkor mindkét szám fölírásában ugyanazok a prímek szerepelnek.

6.8.7. Állítás. *Legyen $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$. Ekkor n és m legnagyobb közös osztója*

$$(n,m) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}},$$

legkisebb közös többszöröse

$$[n,m] = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \cdots p_k^{\max\{\alpha_k,\beta_k\}}.$$

6.8.8. Definíció. *Az a, b számokat* **relatív prímeknek** *nevezzük, ha legnagyobb közös osztójuk 1.*

Az n szám osztóinak számát $d(n)$-nel, osztóinak összegét $\sigma(n)$-nel, a nála kisebb hozzá relatív prím számok számát $\varphi(n)$-nel jelöljük. Azaz

$$d(n) = \sum_{d \mid n} 1, \qquad \sigma(n) = \sum_{d \mid n} d \qquad \text{és} \qquad \varphi(n) = \sum_{\substack{(a,n)=1 \\ a \leq n}} 1.$$

6.8.9. Tétel. *Legyen* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. *Ekkor*

$$d(n) = \prod_{i=1}^{k} (\alpha_i + 1), \qquad \sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}, \qquad \varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

BIZONYÍTÁS: $d \mid n$ esetén $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, ahol $\beta_i \leq \alpha_i$. β_i így $\alpha_i + 1$ féle értéket vehet föl, n osztóinak száma $d(n) = \prod_{i=1}^{k} (\alpha_i + 1)$. Az i-edik helyen minden osztóban az $1, p_i, p_i^2, \ldots, p_i^{\alpha_i}$ számok valamelyike szerepel tényezőként, ezért

$$\sigma(n) = \prod_{i=1}^{k} (1 + p_i + \ldots + p_i^{\alpha_i}) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

A $\varphi(n)$-re vonatkozó képletet a szita módszerrel fogjuk kiszámolni. Az 1-től n-ig terjedő számok közül ki fogjuk szitálni az n-hez nem relatív prímeket. Azt a tényt fogjuk kihasználni, hogy két szám pontosan akkor nem relatív prím egymáshoz, ha van közös prímosztójuk. Minden p_1-edik szám nem relatív prím n-hez, hisz közös osztójuk p_1. $\frac{n}{p_1}$ ilyen szám van n-ig. Ezt minden prímre végigszámolva az $n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \ldots + \frac{n}{p_k}\right)$ számhoz jutunk. Kétszer vontuk ki azonban azon számok számát, amelyek két különböző prímmel is oszthatók, stb. Végül az

$$n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \ldots + \frac{n}{p_k}\right) + \left(\frac{n}{p_1 p_2} + \ldots + \frac{n}{p_{k-1} p_k}\right) + \ldots + (-1)^k \frac{n}{p_1 \cdot \ldots \cdot p_k} = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

értékhez jutunk. □

Megjegyzés: Mindhárom függvény rendelkezik az úgynevezett multiplikatív tulajdonsággal. Az f egészeken értelmezett függvény multiplikatív, ha $(a,b) = 1$ esetén $f(ab) = f(a)f(b)$. A d, σ, φ függvények multiplikativitása a rájuk vonatkozó képletből látszik.

6.8.1. Kongruenciák

Az egész számok körében elvégezhető a maradékos osztás. Ha $n = qk + b$, ahol $0 \leq b < k$, akkor b-t n-nek k-val való osztásakor kapott maradékának, vagy röviden n-nek k-val vett maradékának nevezzük.

6.8.10. Definíció. a **kongruens** b*-vel modulo* n*, ha* a *és* b n*-nel vett maradéka ugyanaz. Jelölése* $a \equiv b \pmod{n}$ *vagy* $a \equiv b \pmod{n}$.

6.8.11. Állítás. *A kongruencia ekvivalenciareláció.*

BIZONYÍTÁS: Az állítás közvetlenül látszik, ha észrevesszük, hogy

$$a \equiv b \pmod{n}$$

pontosan akkor, ha $n \mid a-b$. □

Legyenek most a,b,c egész számok. Az $ax \equiv b \pmod{c}$ kongruencia megoldhatóságát fogjuk vizsgálni. Ez azt jelenti, hogy keressük azon x egész számokat, amelyre $c \mid ax-b$. Nyilván ha x kielégíti a feltételt, akkor $kc+x$ is tetszőleges k egész számra, így a megoldásokat modulo c fogjuk keresni. A feltétel azzal ekvivalens, hogy van olyan $y \in \mathbb{Z}$, amelyre $cy = ax-b$, azaz $cy-ax = b$. A kétféle átfogalmazásból közvetlenül igazolható, hogy

6.8.12. Állítás. *Az $ax \equiv b \ (c)$ kongruenciában a és b leosztható és megszorozható tetszőleges c-hez relatív prím számmal, a,b,c pedig leosztható tetszőleges egész számmal, a kongruencia megoldáshalmaza nem változik. A kongruencia pontosan akkor oldható meg, ha $(a,c) \mid b$.*

BIZONYÍTÁS: A fentiek alapján csak a megoldhatóság feltétele szorul igazolásra. Ha a kongruencia megoldható, akkor $(a,c) \mid a,c$ miatt $(a,c) \mid b$. Megfordítva: Elég megmutatni, hogy az $ax \equiv (a,c) \pmod{c}$ kongruencia megoldható ami az $ax-cy = (a,c)$ egyenlet megoldhatóságával egyenértékű. Ehhez az euklideszi algoritmust kell elvégeznünk. Osszuk el maradékosan c-t a-val, majd a-t a kapott maradékkal, és így tovább. Az utolsó nem 0 maradék lesz (a,c), és ez kifejezhető a és c segítségével a kívánt módon. Ugyanis:

$$\begin{aligned} c &= aq_1 + r_1 & \qquad r_1 &= 1c - aq_1 \\ a &= r_1q_2 + r_2 & \qquad r_2 &= 1a - r_1q_2 = (1+q_1q_2)\,a - q_2c \\ &\vdots & & \vdots \\ r_{t-1} &= r_{t-2}q_{t-1} + r_t & \qquad r_t &= h_1a - h_2c \\ r_t &= r_{t-1}q_t + 0 \end{aligned}$$

Az utolsó előtti sor alapján $(a,c) \mid r_t$. Másrészt az utolsó sortól visszafelé lépegetve $r_t \mid r_{t-1}$, ezért az utolsó előtti sorból $r_t \mid r_{t-2}$, a másodikból $r_t \mid a$, majd az elsőből $r_t \mid c$ adódik. Így $r_t \mid (a,c)$, tehát $r_t = (a,c)$. □

Most már kimondható a kongruenciák megoldhatóságáról szóló:

6.8.13. Tétel. *Az $ax \equiv b \pmod{c}$ kongruencia pontosan akkor oldható meg, ha $(a,c) \mid b$. A megoldások száma (a,c) modulo c.*

BIZONYÍTÁS: Csak a megoldások számát kell vizsgálnunk. Ha a kongruencia megoldható, legyen $a = a'(a,c)$, $b = b'(a,c)$, $c = c'(a,c)$. Leosztva (a,c)-vel az $a'x \equiv b' \pmod{c}$ kongruenciát kapjuk, ahol $(a',c') = 1$. Megmutatjuk, hogy ekkor egy megoldás van modulo c'. Tegyük fel, hogy b_1 és b_2 inkongruens megoldások, azaz a $0 \le b_1, b_2 < c'$ számok kielégítik a kongruenciát. Ekkor $a'b_1 \equiv a'b_2 \bmod (c')$,

azaz $c' \mid a'(b_1 - b_2)$, de (a', c')=1 és $|b_1 - b_2| < c'$ miatt ez lehetetlen. Ezért egy megoldás van modulo c', így (a, c) számú megoldás van modulo c. □

Tekintsük most a $\mathbb{Z}_n$ gyűrűt. Ebben a gyűrűben az n-hez relatív prím maradékok csoportot alkotnak a szorzásra nézve, hiszen két n-hez relatív prím szám szorzata relatív prím n-hez, az 1 relatív prím n-hez, és inverze is van az összes relatív prím elemnek, hisz $(a, n) = 1$ esetén az $ax \equiv 1 \pmod{n}$ kongruencia megoldható. Mivel egy elem rendje osztja a csoport rendjét, adódik az Euler-Fermat tétel:

6.8.14. Tétel. *Legyen $(a, n) = 1$. Ekkor $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Ennek speciális esete $n = p$ prím esetén a „kis” Fermat-tétel:

6.8.15. Tétel. *Tetszőleges a egész számra $a^p \equiv a \pmod{p}$.*

BIZONYÍTÁS: Az állítás p-vel osztható számokra nyilván teljesül, a többire pedig az $a^{p-1} \equiv 1 \pmod{p}$ kongruencia a-val való beszorzásával adódik. □

6.9. Hálók

6.9.1. Definíció. *A H halmazt a $\leq$ relációval* **részben rendezett halmaznak** *nevezzük, ha $\leq$ reflexív, antiszimmetrikus és tranzitív, azaz*

(1) *$a \leq a$ $\forall a \in H$-ra,*

(2) *$a \leq b$ és $b \leq a$ esetén $a = b$,*

(3) *$a \leq b$ és $b \leq c$ esetén $a \leq c$.*

Példák:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, ahol $\leq$ a szokásos;
2. $\mathbb{Z}$, ahol $a \leq b$, ha $a \mid b$;
3. Egy halmaz részhalmazai, ahol $A \leq B$, ha $A \subseteq B$.

6.9.2. Definíció. *Legyen H részben rendezett halmaz, $a \leq b$, $a, b \in H$. Azt mondjuk, hogy b* **fedi** *a-t ($a \prec b$), ha nincs olyan a, b-től különböző $c \in H$, hogy $a \leq c \leq b$.*

Míg $(\mathbb{R}, \leq)$-ban bármely két elem közt van harmadik (nincsenek fedő elemek), véges halmazok esetén a rendezés jellemezhető a fedéssel. Véges halmazban ugyanis $a \leq b$ pontosan akkor, ha vannak olyan $a = a_1, a_2, \ldots, a_n = b$ elemek, hogy $a_i \prec a_{i+1}$.

6.9.3. Definíció. *Legyenek a, b elemei a H részben rendezett halmaznak. A c elemet a és b felső korlátjának nevezzük, ha $a \leq c$ és $b \leq c$. c az a és b* **legkisebb felső korlátja**, *ha felső korlát, és tetszőleges c' felső korlátra $c \leq c'$. (A* **legnagyobb alsó korlát** *hasonlóan definiálható.)*

6.9.4. Definíció. *A H részben rendezett halmazt* **hálónak** *nevezzük, ha bármely két H-beli elemnek van legkisebb felső korlátja és legnagyobb alsó korlátja. Az előbbit $a \vee b$-vel (a unió b), az utóbbit $a \wedge b$-vel (a metszet b) jelöljük. Ha a hálóban van legnagyobb elem, azt* **egységelemnek**, *ha van legkisebb elem, azt* **nullelemnek** *nevezzük.*

6.9.5. Tétel. *Legyen H háló. Ekkor a metszet és unió kétváltozós műveletek a H halmazon az alábbi tulajdonságokkal: tetszőleges $a,b,c \in H$ esetén*

$$\begin{array}{ccccc} a \vee a = a & \text{és} & a \wedge a = a & & \textit{(idempotencia)} \\ a \vee b = b \vee a & \text{és} & a \wedge b = b \wedge a & & \textit{(kommutativitás)} \\ (a \vee b) \vee c = a \vee (b \vee c) & \text{és} & (a \wedge b) \wedge c = a \wedge (b \wedge c) & & \textit{(asszociativitás)} \\ (a \vee b) \wedge a = a & \text{és} & (a \wedge b) \vee a = a & & \textit{(elnyelési tulajdonság)} \end{array}$$

A tétel bizonyítása világos, ugyanúgy, mint a megfordításáé:

6.9.6. Tétel. *Legyen H halmaz az $\vee, \wedge$ műveletekkel, amelyekre teljesül a fenti négy tulajdonság. Ekkor H háló, ahol az a,b elemek legkisebb felső korlátja (legnagyobb alsó korlátja) $a \vee b$ ($a \wedge b$). $a \leq b$ pontosan akkor, ha $a \wedge b = a$, vagy másképp $a \vee b = b$.*

Ezzel megkaptuk a háló algebrai megfogalmazását.
Példák:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, ahol $a \vee b = \max\{a,b\}$, $a \wedge b = \min\{a,b\}$ (a rendezés ekkor a szokásos);
2. $\mathbb{N}$, ahol $a \vee b = [a,b]$, a és b legkisebb közös többszöröse, $a \wedge b = (a,b)$, a és b legnagyobb közös osztója (a rendezés az „osztója” reláció);
3. Egy halmaz részhalmazai, ahol $A \vee B = A \cup B$, $A \wedge B = A \cap B$ (a rendezés a tartalmazás);
4. Legyen H a [0,1] intervallumon folytonos függvények halmaza,
$$f \vee g = \max\{f,g\}, \quad f \wedge g = \min\{f,g\}$$
(a rendezés a minden pontban kisebb-egyenlő).
5. Egy G csoport részcsoportjai, $H \vee K = \langle H,K \rangle$, $H \wedge K = H \cap K$ (a rendezés a tartalmazás). Ennek részhálóját alkotják a normálosztók, hisz két normálosztó metszete és generátuma is normálosztó.

Az első példában nincs se egység- se nullelem. A második példában nincs egységelem, nullelem az 1. Az ötödik példában az egységelem G, a nullelem $\{1\}$, vagyis az egységelemből álló csoport.
A harmadik példában bármely három elemre (részhalmazra) teljesülnek a

$$(A \wedge B) \vee C = (A \vee C) \wedge (B \vee C)$$

és

$$(A \vee B) \wedge C = (A \wedge C) \vee (B \wedge C)$$

egyenlőségek.

6.9.7. Definíció. *Az L hálót disztributívnak nevezzük, ha tetszőleges $a, b, c \in L$ esetén teljesülnek az $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$ és $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$ azonosságok.*

Könnyen látható, hogy bármelyik disztributív törvényből következik a másik.

6.9.8. Definíció. *Legyen L egység- (1) és nullelemmel (0) rendelkező háló. Az a' elemet az a elem* **komplementumának** *nevezzük, ha*

$$a \wedge a' = 0 \text{ és } a \vee a' = 1.$$

6.9.9. Állítás. *Disztributív hálóban ha van komplementum, akkor ez egyértelmű.*

BIZONYÍTÁS: Legyen L disztributív háló, $a \in L$. Tegyük föl, hogy b és c a komplementumai. Ekkor $b = b \wedge 1 = b \wedge (a \vee c) = (b \wedge a) \vee (b \wedge c) = 0 \vee (b \wedge c) = b \wedge c$ Tehát $b \leq c$. Hasonlóan megmutatható, hogy $c \leq b$, tehát $b = c$. □

6.9.10. Definíció. *Egy L disztributív hálót* **Boole-algebrának** *nevezünk, ha minden elemnek van komplementuma L-ben.*

6.9.11. Állítás. *Legyen B Boole-algebra. Ekkor*

$$(a \vee b)' = a' \wedge b', \qquad (a \wedge b)' = a' \vee b'$$

BIZONYÍTÁS: A két állítás hasonlóan bizonyítható, ezért mi csak az egyiket bizonyítjuk.

$$(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = (1 \vee b) \wedge (1 \vee a) = 1 \wedge 1 = 1,$$
$$(a \vee b) \wedge (a' \wedge b') = (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') = (0 \wedge b') \vee (0 \wedge a') = 0 \vee 0 = 0.$$

Tehát $(a \vee b)$ komplementuma $a' \wedge b'$. □

Boole-algebrákból egyszerűen nyerhetünk Boole-gyűrűt. (Boole-gyűrűnek neveztünk egy olyan gyűrűt, amelyben $a^2 = a$ teljesül minden gyűrűelemre.) Legyen B Boole-algebra, $a, b \in B$ esetén legyen

$$a + b = (a \wedge b') \vee (b \wedge a'), \qquad ab = a \wedge b \qquad (\star)$$

Ellenőrizhető a gyűrűaxiómák teljesülése. A gyűrű Boole-gyűrű, hisz $a^2 = a \wedge a = a$ teljesül minden elemre.

6.9.12. Állítás. *Egy Boole-gyűrű kommutatív, és tetszőleges a elemére $2a = 0$.*

BIZONYÍTÁS: Legyenek R Boole-gyűrű, $a,b \in R$. Ekkor $a+a=(a+a)^2=a^2+a^2+a^2+a^2=a+a+a+a$, azaz $a+a=2a=0$. Ezzel az állítás második részét beláttuk és melléktermékként azt kaptuk, hogy $a=-a$ minden $a \in R$-re. $a+b=(a+b)^2$ összefüggésből $ab=-ba$ adódik. $ab=-ab$ miatt $ab=ba$. □

A Boole-algebrákból kapott Boole-gyűrű egységelemes, az 1 az egységelem. A következő tétel arról szól, hogy minden egységelemes Boole-gyűrű megkapható Boole-algebrából, és fordítva.

6.9.13. Tétel. *Legyen R egységelemes Boole-gyűrű. Ekkor R Boole-algebra az*

$$a \vee b = a+b-ab \qquad a \wedge b = ab$$

műveletekkel. B-ből visszakapható R a $(\star)$ műveletekkel.

A tétel az eddigiekhez hasonló módszerekkel bizonyítható.
Boole-algebrára a legkézenfekvőbb példa egy halmaz részhalmazainak rendszere.

6.9.14. Definíció. *Egy H halmaz részhalmazainak metszetre és unióra zárt rendszerét* **halmazgyűrűnek** *nevezzük. A komplementumra zárt halmazgyűrűt* **halmaztestnek** *nevezzük.*

A disztributív hálókat és a Boole-algebrákat írja le a következő

6.9.15. Tétel (Stone-féle reprezentációs tétel). *Minden disztributív háló izomorf egy halmazgyűrűvel. Minden Boole-algebra izomorf egy halmaztesttel.*

6.10. Testek

A kommutativitáson és az egységelemen kívül van még egy alapvető tulajdonság, ami számos gyűrűre teljesül:

6.10.1. Definíció. *Egy R egységelemes gyűrűt* **ferdetestnek** *hívunk, ha a szorzásra nézve is van inverz, azaz $\forall\ 0 \neq a \in R$-hez $\exists a' \in R$, hogy $aa'=1$. Egy ferdetestet* **testnek** *nevezünk, ha a szorzás kommutatív.*

Megjegyzés: Gyakran a ferdetestet hívják testnek, a testet pedig kommutatív testnek.

6.10.2. Állítás. *Minden ferdetest nullosztómentes.*

BIZONYÍTÁS: Legyen K ferdetest, $a,b \in K$, $ab=0$. Balról a^{-1}-gyel szorozva $b=0$ adódik, tehát K nullosztómentes. □

Példák:

1. A racionális, a valós illetve a komplex számok ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) testet alkotnak a szokásos műveletekre.

2. A modulo 2 maradékosztályok testet alkotnak a gyűrűknél a 8-as példában leírt műveletekre. Elég ellenőrizni, hogy az 1-nek (m_1-nek) van-e inverze. $1 \cdot 1 = 1$ miatt az 1 inverze önmaga.

3. A modulo 5 maradékosztályok testet alkotnak a gyűrűknél a 8-as példában leírt műveletekre. Elég ellenőrizni, hogy az 1,2,3,4 elemeknek van-e inverze. $1 \cdot 1 = 1$, $2 \cdot 3 = 6 = 1$, $4 \cdot 4 = 16 = 1$ miatt az 1 és a 4 inverze önmaga, a 2-é a 3.

4. Az $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ alakú valós mátrixok testet alkotnak a mátrixműveletekre.

5. A valós számtest feletti racionális törtfüggvények halmaza, $\mathbb{R}(x)$, testet alkot a szokásos műveletekre, azaz

$$\mathbb{R}(x) = \left\{ \frac{p(x)}{q(x)} \;\middle|\; p(x), q(x) \in \mathbb{R}[x], \quad q(x) \not\equiv 0 \right\}$$

test, ahol

$$\frac{p_1(x)}{q_1(x)} + \frac{p_2(x)}{q_2(x)} = \frac{p_1(x)q_2(x) + p_2(x)q_1(x)}{q_1(x)q_2(x)},$$

valamint

$$\frac{p_1(x)}{q_1(x)} \cdot \frac{p_2(x)}{q_2(x)} = \frac{p_1(x)p_2(x)}{q_1(x)q_2(x)}.$$

6. Legyen d négyzetmentes szám, azaz $b = p_1 p_2 \cdots p_k$, ahol a p_i-k különbözőek. $\mathbb{Q}\left(\sqrt{d}\right) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ test a szokásos műveletekre, ugyanis

$$\left(a_1 + b_1\sqrt{d}\right) + \left(a_2 + b_2\sqrt{d}\right) = (a_1 + a_2) + (b_1 + b_2)\sqrt{d} \in \mathbb{Q}\left(\sqrt{d}\right),$$

$$\left(a_1 + b_1\sqrt{d}\right)\left(a_2 + b_2\sqrt{d}\right) = (a_1a_2 + db_1b_2) + (a_1b_2 + a_2b_1)\sqrt{d} \in \mathbb{Q}\left(\sqrt{d}\right),$$

azaz $Q\left(\sqrt{d}\right)$ gyűrű. Meg kell még mutatni a multiplikatív inverz létezését: $a^2 + db^2 \neq 0$, mert ellenkező esetben $d = -\frac{a^2}{b^2} = \frac{p^2}{q^2}$ lenne, ahol $p, q \in \mathbb{Z}$. Beszorozva q^2–tel $dq^2 = p^2$ adódna. Az egyenlet baloldalán d prímosztói páratlan, míg a jobboldalon páros hatványon szerepelnének, ez ellentmondás. Az $\left(a + b\sqrt{d}\right)\frac{a - b\sqrt{d}}{a^2 + db^2} = 1$ egyenlőség igazolja az inverz létezését minden nem nulla számra.

Példa ferdetestre, a kvaterniók. Tekintsük az $a+bi+cj+dk$ alakú számokat, ahol $a,b,c,d \in \mathbb{R}$. Legyen az összeadás a koordinátánkénti összeadás, az i,j,k elemek pedig szorzódjanak úgy, mint a kvaterniócsoportban. Ekkor a disztributív törvények meghatározzák tetszőleges két kvaternió szorzatát. Azaz legyen:

$$(a_1+b_1i+c_1j+d_1k)+(a_2+b_2i+c_2j+d_2k) = \\ (a_1+a_2)+(b_1+b_2)\,i+(c_1+c_2)\,j+(d_1+d_2)\,k$$

$$(a_1+b_1i+c_1j+d_1k)\,(a_2+b_2i+c_2j+d_2k) = \\ (a_1a_2-b_1b_2-c_1c_2-d_1d_2)+(a_1b_2+a_2b_1+c_1d_2-c_2d_1)\,i+ \\ +(a_1c_2+a_2c_1+d_1b_2-d_2b_1)\,j+(a_1d_2+a_2d_1+b_1c_2-b_2c_1)\,k.$$

Ezt a halmazt a fönti műveletekre a kvaterniók (ferde)testének, elemeit pedig kvaternióknak nevezzük. Mint a komplex számok körében, a kvaterniók közt is értelmezzük a konjugált és a norma (hossz) fogalmát.

$$\overline{a+bi+cj+dk} = a-bi-cj-dk \quad \text{és}$$

$$|a+bi+cj+dk|^2 = (a+bi+cj+dk)\left(\overline{a+bi+cj+dk}\right) = a^2+b^2+c^2+d^2.$$

Egy kvaternió reciproka is a komplex számoknál megszokott módon kapható. Hiszen, ha $k \neq 0$ kvaternió, akkor $k\cdot\overline{k}/|k|^2 = 1$. Ezzel igazoltuk a ferdetest axiómákat. A kvaterniók valóban nem test, hisz $ij \neq ji$.
Nézzük meg, miben térnek el a kvaterniók a testektől. Mint tudjuk, egy test fölött egy n-edfokú polinomnak legföljebb n gyöke lehet. Tekintsük az x^2+1 polinomot. Vegyük észre, hogy ennek a polinomnak a kvaterniók felett gyöke minden $bi+cj+dk$ alakú szám, ahol $b^2+c^2+d^2=1$, tehát végtelen sok gyöke van. Másrészt vegyük észre, hogy $x^2+1 = (x+i)(x-i) = (x+j)(x-j) = (x+k)(x-k) = (x+t)\,(x+\overline{t})$, ahol t gyöke a polinomnak. Azonban a különböző helyeken vett helyettesítési értékek különbözhetnek, pl. i-t helyettesítve az első három felbontásba: $i^2+1 = (i+i)(i-i) = 0$, $(i+j)(i-j) = -2k$, $(i+k)(i-k) = 2j$ adódik. Végül érdemes megjegyezni, hogy az $a+bi$ ($a+bj$, stb.) alakú számok a komplex számokkal izomorf résztestjét alkotják a kvaterniónak. Felmerülhet a kérdés, lehet-e még a komplex számokon és a kvaterniókon kívül – esetleg valamiféle hasonló módszerrel – más, a valós számokat tartalmazó (ferde)testet szerkeszteni. Erről szól Frobenius tétele:

6.10.3. Tétel. *Legyen K a valós számokat tartalmazó ferdetest. Ekkor K izomorf a komplex számok vagy a kvaterniók valamelyikével.*

További testekre ad példát a következő

6.10.4. Állítás. *Minden véges integritási tartomány test.*

BIZONYÍTÁS: Legyen R integritási tartomány. Meg kell mutatni az egységelem és a rá vonatkozó inverz létezését. Legyenek a gyűrű elemei $0 = a_1, a_2, \cdots a_n$. Legyen

$0 \neq a \in R$. Tekintsük az $aa_1, aa_2, \cdots aa_n$ elemeket. $aa_i = aa_j$ esetén $a(a_i - a_j) = 0$, így a nullosztómentesség miatt $a_i = a_j$ teljesül, azaz az aa_i elemek mind különbözőek. Mivel n elem van, ezért fölsoroltuk az összes elemet, így előállítottuk a-t is, azaz van olyan $e \in R$, hogy $ae = a$. Megmutatjuk, hogy e egységelem. $ae = a$ miatt tetszőleges $b \in R$-re $bae = ba$, azaz a kommutativitás szerint $abe = ab$, $a(be - b) = 0$. A nullosztómentesség és $a \neq 0$ miatt ez csak úgy lehet, ha $be - b = 0$, azaz $b = be$. Tehát e egységelem. Az aa_i elemek közt szerepel e is, azaz a-nak van inverze. □

6.10.5. Következmény. *$\mathbb{Z}_m$ pontosan akkor test, ha m prím.*

BIZONYÍTÁS: $\mathbb{Z}_m$ akkor nullosztómentes, ha $a, b \in \mathbb{Z}_m$ esetén $ab = 0$-ból $a = 0$ vagy $b = 0$ következik, azaz $m \mid ab$ esetén $m \mid a$ vagy $m \mid b$. Ez pont a prímtulajdonság, ezzel igazoltuk állításunkat. □

A $\mathbb{Z}_p$ gyűrűt, ha mint testre gondolunk rá, $\mathbb{F}_p$-vel is jelöljük.

6.10.6. Definíció. *Legyenek $L \leq K$ testek. L-et K* **résztestének**, *K-t L* **bővítésének** *nevezzük. Az $K \mid L$ párt* **testbővítésnek** *nevezzük. K vektortér L fölött. K L fölötti dimenzióját ($\dim_L(K)$) a testbővítés fokának hívjuk, $|K : L|$-lel jelöljük. Ha ez véges,* **véges bővítésről** *beszélünk. $a, b, \ldots \in K$ esetén a legszűkebb olyan testet, amely az $a, b, \ldots$ elemeket tartalmazza, $L(a, b, \ldots)$-vel jelöljük, és azt mondjuk, hogy L-ből az $a, b, \ldots$ elemek* **adjunkciója** *révén áll elő. Az egy elem adjunkciójával nyert bővítést* **egyszerű bővítésnek** *nevezzük, a megfelelő elemet* **primitív elemnek** *hívjuk.*

Ismételt testbővítések fokáról szól az alábbi

6.10.7. Tétel (fokszámok szorzástétele). *Legyenek $K \subseteq L \subseteq M$. Ekkor*

$$|M : K| = |M : L||L : K|.$$

Példák:

1. A $\mathbb{C} \mid \mathbb{R}$ pár véges testbővítés, foka 2, $\mathbb{C} = \mathbb{R}(i)$.
2. $\mathbb{Q}\left(\sqrt{d}\right) \mid \mathbb{Q}$ másodfokú bővítése $\mathbb{Q}$-nak.
3. Az $\mathbb{R}(x) \mid \mathbb{R}$ bővítés végtelen bővítés. Az $x, x^2, \ldots, x^n, \ldots$ elemek lineárisan függetlenek $\mathbb{R}$ fölött.
4. Az $\mathbb{R} \mid \mathbb{Q}$ bővítés végtelen, ezt egyelőre nem indokoljuk.

Külön szerepet játszanak azon testek, amelyeknek nincs résztestük.

6.10.8. Definíció. *Egy testet* **prímtestnek** *nevezünk, ha nincs valódi részteste.*

6.10.9. Tétel. *Minden test tartalmaz prímtestet. $\mathbb{Q}$ és $\mathbb{F}_p$ prímtestek. Más prímtest nincs.*

BIZONYÍTÁS: Legyen K a test. Az 1 mindig eleme a testnek. Ezért benne vannak az 1+1, 1+1+1, ..., $1+\ldots+1$ számok is. Különböztessünk meg két esetet:

1. A sorozatban szerepel a 0. Ekkor van olyan k természetes szám, hogy az 1-et k-szor összeadva 0-t kapunk. A sorozat elemei ekkor éppen a $\mathbb{Z}_k$ gyűrűt alkotják. De mivel a test nullosztómentes, k csak egy p prímszám lehet, azaz K tartalmazza $\mathbb{F}_p$-t.

2. A sorozatban nem szerepel a 0. Ekkor a test tartalmazza a természetes számokat. Mivel minden számmal az ellentettje is benne van, a test tartalmazza az egészeket, és a multiplikatív inverz létezése miatt bármely két elem hányadosát, így $\mathbb{Q}$-t is.

Tehát minden test tartalmazza $\mathbb{F}_p$-t vagy $\mathbb{Q}$-t, más prímtest nincs. □

Az állítás alapján minden test előáll $\mathbb{Q}$ vagy valamely $\mathbb{F}_p$ bővítéseként. Vizsgáljuk először azt az esetet, amikor $K \geq \mathbb{F}_p$. Legyen $a \in K$ tetszőleges. Tekintsük az $\underbrace{a+\ldots+a}_{p-szer} = pa$ összeget. $\underbrace{a+\ldots+a}_{p-szer} = \underbrace{1\cdot a+\ldots+1\cdot a}_{p-szer} = \underbrace{(1+\ldots+1)}_{p-szer}a = 0a = 0$, tehát tetszőleges elemet p-szer összeadva 0-t kapunk. Ezt a p számot a K test **karakterisztikájának** nevezzük. Ha nincs ilyen p, **0-karakterisztikájú** testről beszélünk.

6.10.10. Tétel. *Legyen K véges test. Ekkor K elemszáma prímhatvány.*

BIZONYÍTÁS: Van olyan p, hogy $\mathbb{F}_p \leq K$. K vektortér $\mathbb{F}_p$ fölött. Legyen $e_1, e_2, \ldots, e_n$ a K vektortér bázisa $\mathbb{F}_p$ felett. Ekkor minden elem egyértelműen előáll

$$\sum_{i=1}^{n} \alpha_i e_i \quad (\alpha_i \in \mathbb{F}_p)$$

alakban. Ezért a test elemszáma p^n. □

6.10.11. Definíció. *Legyen $L \mid K$ testbővítés, $a \in L$. Az a elemet* **algebrai elemnek** *nevezzük (Kfölött), ha van olyan $f \in K[x]$ polinom, amelyre $f \not\equiv 0$ és $f(a) = 0$. Ha nincs ilyen polinom, akkor az elemet* **transzcendens** *elemnek nevezzük. Az $L \mid K$ testbővítés* **algebrai**, *ha L minden eleme algebrai K fölött.*

Példák:

1. Az $\mathbb{R} \mid \mathbb{Q}$ testbővítésben a $\sqrt[1993]{1994}$, $\sqrt{2}+1$ elemek algebraiak, hisz gyökei az $f(x) = x^{1993} - 1994$ illetve a $g(x) = x^2 - 2x - 1$ polinomnak. Az e és a π transzcendens elemek. Ennek bizonyítása komolyabb felkészültséget igényel. $\mathbb{R} \mid \mathbb{Q}$ tehát nem algebrai bővítés.

2. A $\mathbb{C} \mid \mathbb{R}$ bővítés algebrai, hisz $z \in \mathbb{C}$ esetén z gyöke az $f(x) = x^2 - (z+\overline{z})x + z\overline{z}$ valós együtthatós polinomnak.

A második példa általánosítása az alábbi

6.10.12. Állítás. *Minden véges testbővítés algebrai.*

BIZONYÍTÁS: Legyen $\dim_K(L) = n$, $a \in L$. Ekkor az $1, a, a^2, \ldots, a^n$ elemek lineárisan összefüggőek K felett, így vannak olyan $\alpha_i \in K$ elemek, hogy $\sum_{i=0}^{n} \alpha_i a^i = 0$. Ekkor a gyöke az $f(x) = \sum_{i=0}^{n} \alpha_i x^i$ polinomnak. □

Az egyszerű algebrai bővítéseket a következőképpen lehet jellemezni:

6.10.13. Állítás. *Legyen $L \mid K$ testbővítés, $a \in L$ algebrai K fölött, gyöke az $f(x) = \sum_{i=0}^{n} \alpha_i x^i$ irreducibilis (felbonthatatlan) polinomnak. Ekkor*

$$K(a) = \left\{ \sum_{i=0}^{n-1} \beta_i a^i \;\middle|\; \beta_i \in K \right\},$$

a $K(a) \mid K$ testbővítés foka n.

BIZONYÍTÁS: Az $\sum_{i=0}^{n-1} \beta_i a^i$ alakú elemek nyilván benne vannak $K(a)$-ban. Megmutatjuk, hogy ezek testet alkotnak, ezzel igazoljuk állításunkat. A testaxiómák közül elég ellenőrizni a műveleti zártságot, az inverz, nullelem és egységelem létezését. Ez utóbbi kettő és az ellentett létezése nyilvánvaló. Két ilyen alakú szám összege ilyen alakú, mert $\sum_{i=0}^{n} \beta_i a^i + \sum_{i=0}^{n} \gamma_i a^i = \sum_{i=0}^{n} (\beta_i + \gamma_i) a^i$. Két ilyen elem szorzatában már előfordulnak magasabb kitevős tagok is, de $\sum_{i=0}^{n} \alpha_i a^i = 0$ miatt

$$a^n = -\frac{1}{\alpha_n} \sum_{i=0}^{n-1} \alpha_i a^i,$$

azaz az n-nél magasabb fokú tagok kisebb fokú kifejezésekkel helyettesíthetők, így a halmaz szorzásra zárt. Legyen most $g(x) = \sum_{i=0}^{n-1} \delta_i x^i$. Megmutatjuk, hogy $g(a)$-nak van inverze a halmazban. Mivel g foka kisebb mint f-é, és f felbonthatatlan, $(f, g) = 1$. Ezért az Euklideszi-algoritmus létezése alapján vannak olyan $p, q \in K[x]$ polinomok, hogy $f(x)q(x) + g(x)p(x) = 1$. a-t helyettesítve az $f(a)q(a) + g(a)p(a) = 1$ egyenlőséget kapjuk, $f(a) = 0$ miatt $g(a)p(a) = 1$ adódik, azaz $g(a)$ inverze $p(a)$. Ezzel igazoltuk azt is, hogy a bővítés foka legföljebb n, hisz a első

$n-1$ hatványa az 1-gyel generátorrendszer. Ezek az elemek függetlenek is. Ellenkező esetben $\sum_{i=0}^{n-1} \beta_i x^i = 0$ teljesülne, azaz a gyöke lenne egy legfeljebb $n-1$-ed fokú polinomnak, de ez ellentmond annak, hogy f irreducibilis. □

Az állítás fontos folyománya az alábbi:

6.10.14. Állítás. *Algebrai bővítés algebrai bővítése algebrai.*

BIZONYÍTÁS: Legyenek $K \mid L$, $L \mid M$ algebrai bővítések. Meg kell mutatni, hogy K minden eleme algebrai M fölött. Legyen $a \in K$. a algebrai L fölött, ezért vannak olyan $\alpha_i \in L$ elemek, hogy a gyöke az $f(x) = \sum_{i=0}^{n} \alpha_i x^i$ polinomnak. Az α_i elemek algebraiak K fölött, ezért a $K(\alpha_i) \mid K$ testbővítések végesek, ezért ezek egymásutánja is véges a fokszámok szorzástétele miatt, ezért $M(\alpha_0, \ldots, \alpha_n) \mid M$ is véges. $M(\alpha_0, \ldots, \alpha_n, a) \mid M(\alpha_0, \ldots, \alpha_n)$ is véges (legfeljebb n-edfokú), ezért a $M(\alpha_0, \ldots, \alpha_n, a) \mid M$ bővítés is véges a fokszámok szorzástétele miatt, tehát a algebrai K fölött. □

Következmény: Legyenek α, β algebraiak a K test fölött. Ekkor $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ is algebraiak K fölött. A K fölött algebrai számok testet alkotnak.
A tétel jelentőségét az adja, hogy míg az $\sqrt[1993]{1994}$, $\sqrt{2}+1$ számokról egyszerű volt egy polinom megmutatásával eldönteni, hogy algebraiak, a $\sqrt{2}+1/\sqrt[1993]{1994}$ esetén körülményes lenne ilyen polinomot mutatni (3886-od fokú polinom lenne). A tétel mégis garantálja, hogy algebrai (persze a tétel nem mondja meg, hogyan lehet ilyen polinomot találni). A következő tétel arról szól, hogy véges bővítéseket könnyű kezelni az egyszerű bővítések ismeretében.

6.10.15. Tétel. *Legyen K 0-karakterisztikájú test, $L \mid K$ véges bővítés. Ekkor L előáll egyetlen elem adjungálásával K-ból, azaz minden véges bővítés egyszerű.*

6.11. A Galois-elmélet alapjai

Ugyanebben a fejezetben $\mathbb{Q}$ bővítéseiről fogunk beszélni, minden elmondható tetszőleges 0 karakterisztikájú testre. Bár a felkészültségünk megvan hozzá, kevés állítást fogunk bizonyítani, inkább példákkal szemléltetjük a fogalmakat.

6.11.1. Definíció. *Az $L \mid \mathbb{Q}$ véges testbővítést* **normális** *bővítésnek hívjuk, ha van olyan $p \in \mathbb{Q}[x]$, hogy L $\mathbb{Q}$-ból p összes ($\mathbb{C}$-beli) gyökeinek adjungálásával áll elő.*

Mivel minden véges bővítés egyszerű, itt is található primitív elem, azaz $L = \mathbb{Q}(\alpha)$ valamilyen α-ra. Legyen f olyan irreducibilis polinom, amely gyöke α.

6.11.2. Tétel. *Ekkor L előáll $\mathbb{Q}$-ból f gyökeinek adjungálásával. A bővítés foka megegyezik f fokával.*

Példák:

1. A $\mathbb{Q}\left(\sqrt[3]{2}\right) \mid \mathbb{Q}$ bővítés nem normális. Ebben ugyanis primitív elem a $\sqrt[3]{2}$, ekkor ha $\mathbb{Q}\left(\sqrt[3]{2}\right)$ normális lenne, az $f(x) = x^3 - 2$ polinom gyökeinek adjungálásával keletkezne, de elemei az $a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{2^2}$ alakú számok, a nem valós gyökök azonban nem állnak elő ilyen módon.

2. $\mathbb{Q}\left(\sqrt{2}\right) \mid \mathbb{Q}$ normális, hisz az $x^2 - 2$ polinom egyik gyökének adjungálásával kapható, és a másik gyöke is benne van a testben.

Legyen most $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ normális bővítés, α gyöke az n-edfokú irreducibilis $f(x) = \sum_{i=0}^{n} a_i x^i$ racionális együtthatós polinomnak. Tekintsük $\mathbb{Q}(\alpha)$ azon automorfizmusait (önmagára való izomorfizmusait), amelyek $\mathbb{Q}$-t elemenként helybenhagyják, azaz azon $\sigma: \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ bijektív leképezéseket, amelyekre

(1) $\sigma(a) + \sigma(b) = \sigma(a+b)$ tetszőleges $a, b \in \mathbb{Q}(\alpha)$ esetén;

(2) $\sigma(a)\sigma(b) = \sigma(ab)$ tetszőleges $a, b \in \mathbb{Q}(\alpha)$ esetén;

(3) $\sigma(a) = a$ tetszőleges $a \in \mathbb{Q}$ esetén.

Két ilyen leképezést egymás után elvégezve ugyanilyen tulajdonságokkal rendelkező leképezést kapunk. A helybenhagyás is ilyen, és egy ilyen leképezés inverze is ilyen, tehát ezek a leképezések csoportot alkotnak az egymás utáni elvégzésre, mint műveletre.

6.11.3. Definíció. *Ezt a csoportot a $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ bővítés* **relatív automorfizmus csoportjának** *vagy más néven* **Galois-csoportjának** *nevezzük, $\Gamma(\mathbb{Q}(\alpha) \mid \mathbb{Q})$-val jelöljük.*

Legyen $\beta \in \mathbb{Q}(\alpha)$ gyöke a $b_k x^k + b_{k-1}x^{k-1} + \ldots + b_1 x + b_0 = \sum_{i=0}^{k} b_i x^i$ polinomnak. Legyen $\sigma(\beta) = \gamma$. Ekkor

$$0 = \sigma(0) = \sigma\left(b_k\beta^k + b_{k-1}\beta^{k-1} + \ldots + b_1\beta + b_0\right) = \sigma\left(\sum_{i=0}^{k} b_i\beta^i\right) =$$

$$= \sum_{i=0}^{k} \sigma\left(b_i\beta^i\right) = \sum_{i=0}^{k} \sigma(b_i)\,\sigma\left(\beta^i\right) = \sum_{i=0}^{k} b_i\sigma(\beta)^i = \sum_{i=0}^{k} b_i\gamma^i.$$

Azaz $\sum_{i=0}^{k} b_i\gamma^i = 0$. Tehát β képe gyöke ugyanannak a polinomnak, mint β. Tehát α képe csak f valamely gyöke lehet és ez egyértelműen meghatározza σ-t. Mivel egy n-ed fokú polinomnak n gyöke van, ezért $|\Gamma(\mathbb{Q}(\alpha) : (\mathbb{Q}))| \leq n$. Megmutatjuk, hogy

van n különböző automorfizmus. Legyenek az f polinom gyökei $\alpha = \alpha_1, \ldots, \alpha_n$. Ekkor a

$$\sigma_k : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$$
$$\sum_{i=0}^{k} b_i \alpha^i \to \sum_{i=0}^{k} b_i \alpha_k^i$$

leképezések automorfizmusok. Ez abból látszik, hogy f minden gyökére ugyanaz a megkötés, mégpedig, hogy gyöke f-nek, azaz kielégítik a $\sum_{i=0}^{n} a_i \alpha_k^i = 0$ összefüggést. Tehát a Galois-csoport rendje n, megegyezik a bővítés fokával. A Galois-csoport a gyököket permutálja.

Tekintsük át ezeket a fogalmakat egy konkrét példán. Legyen $f(x) = x^4 - 3$. f komplex gyökei a $\pm\sqrt[4]{3}, \pm i\sqrt[4]{3}$ számok. A keresett test tehát

$$K = \mathbb{Q}\left(\sqrt[4]{3}, -\sqrt[4]{3}, i\sqrt[4]{3}, -i\sqrt[4]{3}\right).$$

Megmutatjuk, hogy $\mathbb{Q}\left(\sqrt[4]{3}, i\right) = K$. $i = i\sqrt[4]{3}/\sqrt[4]{3} \in K$, és $\pm\sqrt[4]{3}, \pm i\sqrt[4]{3} \in \mathbb{Q}\left(\sqrt[4]{3}, i\right)$ nyilván teljesül, hisz a szorzatok tényezői már $\mathbb{Q}\left(\sqrt[4]{3}, i\right)$-beliek. Így a két test tartalmazza egymást, ezért megegyeznek. $\mathbb{Q}\left(\sqrt[4]{3}\right) \mid \mathbb{Q}$ negyedfokú bővítés $f(x)$ irreducibilitása miatt. Ez nem tartalmazza i-t, hisz része a valós számtestnek. A $\mathbb{Q}\left(\sqrt[4]{3}, i\right) \mid \mathbb{Q}\left(\sqrt[4]{3}\right)$ bővítés másodfokú, ezért a fokszámok szorzástétele miatt a $K \mid \mathbb{Q}$ bővítés foka 8. Megjegyzendő, hogy ezek szerint a $\sqrt[4]{3}$ nem primitív eleme K-nak. Igazolható, hogy a $\sqrt[4]{3} + i$ primitív elem.

Térjünk rá a Galois-csoport vizsgálatára. Ez egy 8-elemű csoport lesz, amely permutálja f gyökeit. Az i képe $\pm i$ lehet, mert gyöke az $x^2 + 1$ racionális együtthatós polinomnak, a $\sqrt[4]{3}$ képe pedig $\left(\pm\sqrt[4]{3}, \pm i\sqrt[4]{3}\right)$ lehet. Ez összesen $2 \cdot 4 = 8$ lehetőség. A $\sqrt[4]{3}$ és az i képe egyértelműen meghatározza az automorfizmust, tehát ezek a leképezések mind automorfizmusokat határoznak meg. Nézzük meg a gyökök képeit a megfelelő automorfizmusoknál.

$\sigma\left(\sqrt[4]{3}\right)$	$\sigma(i)$	$\sigma\left(\sqrt[4]{3}\right)$	$\sigma\left(-\sqrt[4]{3}\right)$	$\sigma\left(i\sqrt[4]{3}\right)$	$\sigma\left(-i\sqrt[4]{3}\right)$
$\sqrt[4]{3}$	i	$\sqrt[4]{3}$	$-\sqrt[4]{3}$	$i\sqrt[4]{3}$	$-i\sqrt[4]{3}$
$\sqrt[4]{3}$	$-i$	$\sqrt[4]{3}$	$-\sqrt[4]{3}$	$-i\sqrt[4]{3}$	$i\sqrt[4]{3}$
$-\sqrt[4]{3}$	i	$-\sqrt[4]{3}$	$\sqrt[4]{3}$	$-i\sqrt[4]{3}$	$i\sqrt[4]{3}$
$-\sqrt[4]{3}$	$-i$	$-\sqrt[4]{3}$	$\sqrt[4]{3}$	$i\sqrt[4]{3}$	$-i\sqrt[4]{3}$
$i\sqrt[4]{3}$	i	$i\sqrt[4]{3}$	$-i\sqrt[4]{3}$	$-\sqrt[4]{3}$	$\sqrt[4]{3}$
$i\sqrt[4]{3}$	$-i$	$i\sqrt[4]{3}$	$-i\sqrt[4]{3}$	$\sqrt[4]{3}$	$-\sqrt[4]{3}$
$-i\sqrt[4]{3}$	i	$-i\sqrt[4]{3}$	$i\sqrt[4]{3}$	$\sqrt[4]{3}$	$-\sqrt[4]{3}$
$-i\sqrt[4]{3}$	$-i$	$-i\sqrt[4]{3}$	$i\sqrt[4]{3}$	$-\sqrt[4]{3}$	$\sqrt[4]{3}$

A $\sqrt[4]{3}$, $i\sqrt[4]{3}$, $-\sqrt[4]{3}$, $-i\sqrt[4]{3}$ számokat rendre az 1,2,3,4 számokkal helyettesítve a

$$\sigma_1=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\sigma_2=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix},\ \sigma_3=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},$$
$$\sigma_4=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix},\ \sigma_5=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\ \sigma_6=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},$$
$$\sigma_7=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},\ \sigma_8=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

permutációkat kapjuk. Ciklikus felírásban ezek rendre a helybenhagyás, $(2,4)$, $(1,3)(2,4)$, $(1,3)$, $(1,2,3,4)$, $(1,2)(3,4)$, $(4,3,2,1)$, $(1,4)(2,3)$ permutációk. Ha egy négyzet csúcsait körbe megszámozzuk, akkor D_4 elemei a csúcsok pont ezen permutációinak felelnek meg. Tehát $\Gamma\left(\mathbb{Q}\left(\sqrt[4]{3},i\right)\mid\mathbb{Q}\right)\simeq D_4$.
Hogyan lehet egy testbővítés közbülső testeit megkapni? Azaz, ha $K\mid\mathbb{Q}$ testbővítés, melyek a $\mathbb{Q}\leq L\leq K$ testek? Erről szól a Galois-elmélet főtétele:
Legyen $K\mid\mathbb{Q}$ véges normális bővítés. Ekkor a bővítés közbülső testei kölcsönösen egyértelműen megfelelnek $\Gamma(K\mid\mathbb{Q})$ részcsoportjainak a következő módon:
Legyen $K\geq L\geq\mathbb{Q}$ test. L-hez rendeljük hozzá $\Gamma(K\mid\mathbb{Q})$ azon elemeit, amelyek elemenként helybenhagyják L elemeit, azaz

$$L^{\triangledown}=\{\sigma\in\Gamma(K\mid\mathbb{Q})\mid\sigma(a)=a,\forall a\in L\}.$$

Ez a $\Gamma(K\mid L)$ csoport, mint $\Gamma(K\mid\mathbb{Q})$ részcsoportja.
Legyen most $H\leq\Gamma(K\mid\mathbb{Q})$. H-nak megfeleltetjük K azon elemeit, amelyeket H minden eleme helybenhagy, azaz

$$H^{\triangle}=\{\alpha\in K\mid\sigma(a)=a,\ \forall\sigma\in H\}.$$

A megfeleltetésből látszik, hogy bővebb részcsoporthoz szűkebb test, bővebb testhez szűkebb részcsoport tartozik.

6.11.4. Tétel (a Galois-elmélet főtétele).

$$\left(L^{\triangledown}\right)^{\triangle}=L\ \text{és}\ \left(H^{\triangle}\right)^{\triangledown}=H$$

tetszőleges $\mathbb{Q}\leq L\leq K$ illetve $H\leq\Gamma(K\mid\mathbb{Q})$ esetén, azaz a közbülső testek kölcsönösen egyértelműen megfelelnek a részcsoportnak. Sőt, $|L^{\triangledown}|=|K:L|$, azaz $|H|=|L:H^{\triangle}|$

Esetünkben, $K=\mathbb{Q}\left(\sqrt[4]{3},i\right)$ esetén Γ részcsoportjai az alábbiak:
Elsőrendű: $H_1=\{\sigma_1\}$
Másodrendűek: $H_2=\{\sigma_1,\sigma_2\}$, $H_3=\{\sigma_1,\sigma_3\}$, $H_4=\{\sigma_1,\sigma_4\}$, $H_5=\{\sigma_1,\sigma_6\}$, $H_6=\{\sigma_1,\sigma_8\}$
Negyedrendűek: $H_7=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$, $H_8=\{\sigma_1,\sigma_3,\sigma_6,\sigma_8\}$, $H_9=\{\sigma_1,\sigma_3,\sigma_5,\sigma_7\}$
Nyolcadrendű: $\Gamma(K\mid\mathbb{Q})$.

$H_1^{\triangle} = \mathbb{Q}$ és $H_9^{\triangle} = K$ világos.
σ_2 helybenhagyja $\sqrt[4]{3}$-t, és $|\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}(\sqrt[4]{3})| = 2$, ezért $H_2^{\triangle} = \mathbb{Q}(\sqrt[4]{3})$.
$H_4^{\triangle} = \mathbb{Q}(i\sqrt[4]{3})$ hasonlóan igazolható.
Nézzünk most egy fordított esetet. $\mathbb{Q}(i)$ közbülső test. Ezt az $\sigma_1, \sigma_3\sigma_5, \sigma_7$ elemek hagyják fixen, ezért $\mathbb{Q}(i)^{\triangledown} = H_9$. Ugyanígy, a $\sqrt{3}$-at helybenhagyják azon elemek, amelyek nem mozgatják $\sqrt[4]{3}$-t (hisz ennek négyzete $\sqrt{3}$, $i\sqrt[4]{3}$-at (négyzetének -1-szerese) valamint ezen elemek szorzata, σ_3 is. Ebből látszik, hogy $\mathbb{Q}(\sqrt{3})^{\triangledown} = H_7$.
Hasonlóan igazolható a többi részcsoportra is, hogy:
$H_3^{\triangle} = \mathbb{Q}(\sqrt{3}, i)$, $H_5^{\triangle} = \mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3})$, $H_6^{\triangle} = \mathbb{Q}(\sqrt[4]{3} - i\sqrt[4]{3})$, $H_8^{\triangle} = \mathbb{Q}(i\sqrt{3})$.

7. fejezet

Rekurziók és generátorfüggvények

7.1. Homogén lineáris rekurzió

A legismertebb rekurzív összefüggés a **Fibonacci–számokra** vonatkozik. Fibonacci olasz matematikusnak 1202-ben megjelent könyvében szerepel a következő feladat.
Egy nyúlpárnak havonta egyszer születik kölyke, egy hím és egy nőstény. A kölykök születésük után két hónappal kölykeznek először. Hány nyúlpárunk lesz az év végén, ha az év elején egy nyúlpárunk volt? A feltételekből következik, hogy egy hónap múlva két pár nyulunk lesz. Két hónap múlva még csak az első pár fog kölykezni, tehát három pár nyulunk lesz. A harmadik hónapban már a két hónappal korábban született pár is kölykezik, így összesen öt pár nyulunk lesz. Jelöljük F_n-nel az n hónap után meglevő nyúlpárok számát. Láthatjuk, hogy $n+1$ hónap múlva ez az F_n pár nyulunk lesz, és még annyi újszülött pár, ahány nyúlpárunk volt az $n-1$-edik hónap végén, azaz még F_{n-1} pár.
Másszóval, fennáll a következő rekurzív összefüggés:

$$F_{n+1} = F_n + F_{n-1},$$

és $F_0 = 0, F_1 = 1$. Így $F_2 = 1, F_3 = 2, F_4 = 3$ stb. Az F_n számokat nevezzük Fibonacci–számoknak. Evvel a módszerrel azonban elég hosszadalmas kiszámítani például F_{1000}-et. Ezért most belátjuk a következő tételt, amely explicit alakban adja meg F_n-et.

7.1.1. Tétel.

$$F_k = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^k - \left(\frac{1-\sqrt{5}}{2} \right)^k \right]. \tag{7.1}$$

BIZONYÍTÁS: Legyen

$$F(x) = \sum_{k=0}^{\infty} F_k x^k.$$

Ez a függvény a Fibonacci–számok generátorfüggvénye. Ekkor

$$F(x) = F_0 + F_1 x + \sum_{k=2}^{\infty} F_k x^k = x + \sum_{k=2}^{\infty} \left(F_{k-1} x^k + F_{k-2} x^k \right) =$$
$$= x + x \sum_{k=2}^{\infty} F_{k-1} x^{k-1} + x^2 \sum_{k=2}^{\infty} F_{k-2} x^{k-2} =$$
$$= x(F(x)+1) + x^2 F(x) = x + (x + x^2) F(x).$$

Így egy egyenletet kaptunk $F(x)$-re, amiből

$$F(x) = \frac{x}{1-x-x^2} = \frac{x}{\left(1 - \frac{1+\sqrt{5}}{2} x\right)\left(1 - \frac{1-\sqrt{5}}{2} x\right)} =$$
$$= \frac{1}{\sqrt{5}} \frac{1}{1 - \frac{1+\sqrt{5}}{2} x} - \frac{1}{\sqrt{5}} \frac{1}{1 - \frac{1-\sqrt{5}}{2} x} =$$
$$= \frac{1}{\sqrt{5}} \left[\sum_{k=0}^{\infty} \left(\frac{1+\sqrt{5}}{2} \right)^k x^k - \sum_{k=0}^{\infty} \left(\frac{1-\sqrt{5}}{2} \right)^k x^k \right].$$

Ebből pedig már következik (7.1). □

Jól látható, hogy bármely $0 < r < \frac{2}{1+\sqrt{5}}$ számra $F(x)$ abszolút konvergens az $|x| \leq r$ intervallumon, így az összes átalakítás jogos volt. A későbbiekben nem fogjuk vizsgálni az átalakítások jogosságát (ez néha egyáltalán nem könnyű analízisbeli kérdésekhez vezetne), hiszen a generátorfüggvény–technikának az a lényege, hogy a rekurzió ismeretében explicit képlethez jussunk, és ha már megkaptuk a képletet, akkor annak helyességét analízis-beli módszerek nélkül is bebizonyíthatjuk (teljes indukcióval, épp a rekurziót alkalmazva).
Az előbb említettük már, mi az a generátorfüggvény, most pontosan definiáljuk.

7.1.2. Definíció. *Egy $r_0, r_1, r_2, \ldots$ valós számokból álló végtelen sorozat **generátorfüggvénye** az az $f(x)$ függvény, amelynek hatványsorában minden i-re az i-edik együttható r_i. Vagyis*

$$f(x) = \sum_{k=0}^{\infty} r_k x^k.$$

A Fibonacci–számok egy speciális esete a következőkben tárgyalt rekurzióknak.

7.1.3. Definíció. *Egy $r_0, r_1, r_2, \ldots$ végtelen sorozat **p-edrendű, állandó együtthatós homogén lineáris rekurzióval** van megadva, ha $r_0, r_1, \ldots, r_{p-1}$ adottak, és $n \geq p$-re*

$$r_n = \sum_{k=1}^{p} c_k r_{n-k}.$$

Ha ilyen rekurziónk van, akkor megadhatjuk r_i-t explicit alakban is, mint a Fibonacci–számokat. Mivel a bizonyítás könnyen általánosítható a fentiek alapján, itt csak magát a módszert ismertetjük.
Legyen $R(x)$ a sorozat generátorfüggvénye. Ekkor – a 7.1.1. tétel bizonyításában látottakhoz hasonlóan – felírható a következő formában:

$$R(x) = \frac{q(x)}{1 - \sum_{k=1}^{p} c_k x^k},$$

ahol $q(x)$ valamilyen legfeljebb $p-1$ fokú polinom. Az $x^p - \sum_{k=1}^{p} c_k x^{p-k} = 0$ egyenletet a rekurzió **karakterisztikus egyenletének** nevezzük. Az algebra alaptétele értelmében ennek pontosan p komplex gyöke van, amelyek között lehetnek azonban azonosak is. Két esetet különböztetünk meg.
Ha a karakterisztikus egyenlet gyökei $z_1, z_2, \ldots z_p$, mind különbözők, akkor $r_n = \sum_{i=1}^{p} \lambda_i z_i^n$ valamilyen λ_i állandókkal. Mivel $n = 0, 1, 2, \ldots, p-1$-re r_n adott, ezeket rendre behelyettesítve egy egyenletrendszert kapunk a λ_i együtthatókra. Mivel $z_i \neq z_j$, az ezekből képzett Vandermonde determináns nem nulla, így az egyenletrendszerből megkaphatjuk a λ_i együtthatókat, és evvel megkaptuk r_n explicit alakját.
A másik eset, ha $i = 1, 2, \ldots s$-re z_i k_i-szeres gyöke a karakterisztikus egyenletnek. Ekkor az explicit alak

$$\begin{aligned} r_n = &(\lambda_1^{(1)} + \lambda_2^{(1)} n + \ldots + \lambda_{k_1}^{(1)} n^{k_1-1}) z_1^n + \\ &+ (\lambda_1^{(2)} + \lambda_2^{(2)} n + \ldots + \lambda_{k_2}^{(2)} n^{k_2-1}) z_2^n + \ldots \\ &+ (\lambda_1^{(s)} + \lambda_2^{(s)} n + \ldots + \lambda_{k_s}^{(s)} n^{k_s-1}) z_s^n. \end{aligned}$$

7.2. Stirling–számok

7.2.1. Definíció. *Jelöljük $S(n,k)$-val azt a számot, ahányféleképpen n darab különböző tárgyat k nemüres csoportba lehet osztani (feltesszük, hogy $k \geq 1$ és $n \geq k$). Az $S(n,k)$ számokat* ***másodfajú Stirling–számoknak*** *nevezzük.*

Keressünk rekurziót a Stirling–számok meghatározására.

7.2.2. Tétel. *$S(n+1,k) = S(n,k-1) + kS(n,k)$, ha $k \geq 2$ és $n \geq k$.*

BIZONYÍTÁS: Ha $n+1$ tárgyat akarunk pontosan k osztályba osztani, akkor ezt megtehetjük úgy is, hogy először kiválasztunk egy tetszőleges tárgyat (például egy üveg sört), majd eldöntjük, hogy ez a tárgy egy külön csoport legyen, vagy más elemekkel együtt lesz egy csoportban. Az első esetben a maradék n tárgyat $S(n,k-1)$–féleképpen oszthatjuk $k-1$ csoportba, míg a második esetben $S(n,k)$–féleképpen

oszthatjuk az n tárgyat k csoportba, majd k lehetőségünk van kiválasztani azt a csoportot, ahová a sör kerül. □

Most példát mutatunk arra, hogy egy számsorozatot többféle rekurzióval is meg lehet adni.

7.2.3. Tétel.

$$S(n+1,k+1) = \sum_{p=k}^{n} \binom{n}{p} S(p,k),$$

ha $k \geq 1$ *és* $n \geq k$.

BIZONYÍTÁS: Számoljuk össze másképpen, hogy lehet $n+1$ elemet $k+1$ nemüres csoportba osztani. Válasszunk ki egy tárgyat, mondjuk egy krémest. Először döntsük el, hány tárgy lesz a krémessel egy csoportban, vagyis hány tárgy lesz más csoportban. A krémes csoportjában lehet a krémesen kívül $0,1,2,\ldots,n-k$ tárgy. Több nem lehet, mert akkor nem tudunk már $k+1$ nemüres csoportot csinálni. Ha úgy döntöttünk, hogy még $n-p$ darab ($k \leq p \leq n$) tárgy lesz egy csoportban vele, akkor ezeket a tárgyakat $\binom{n}{n-p} = \binom{n}{p}$–féleképp választhatjuk ki. Ezután a többi tárgyat $S(p,k)$–féleképp oszthatjuk k nemüres csoportba. □

Eddig még nem derült ki, miért hívjuk a Stirling–számokat másodfajúnak. Nyilván vannak **elsőfajú Stirling–számok** is. Először bevezetünk egy jelölést: $[n]_k = n(n-1)(n-2)\cdots(n-k+1)$.

7.2.4. Definíció. *Minden n-re az*

$$[x]_k = \sum_{k=1}^{n} s(n,k)x^k$$

összefüggés definiálja az $s(n,k)$ ***elsőfajú Stirling–számokat***.

Az elsőfajú Stirling–számokkal nem is foglalkozunk többet, de így már tudjuk értékelni a következő tételt.

7.2.5. Tétel. *Minden n-re teljesül*

$$x^n = \sum_{k=1}^{n} S(n,k)[x]_k.$$

BIZONYÍTÁS: Hányféleképpen lehet n tárgyat x különböző csoportba osztani, ha lehetnek üres csoportok is? Ez x elem n-ed osztályú ismétléses variációja, tehát x^n lehetőség van. Számoljuk össze most másképpen a lehetőségek számát. Mint tudjuk, n elemet $S(n,k)$–féleképpen oszthatunk k nemüres csoportba. Egy ilyen felosztás után csak azt kell meghatározni, hogy a k csoport mindegyike melyik csoportnak feleljen meg az x darab tervezett csoport közül. Ezt $x(x-1)\ldots(x-k+1)$–féleképp

tehetjük meg. Természetesen összegezni kell még k-nak megfelelően. Így látható, hogy minden pozitív egész x-re

$$x^n = \sum_{k=1}^{n} S(n,k)[x]_k. \tag{7.2}$$

Ha most x-et egy polinom változójának tekintjük, akkor azt kapjuk, hogy a két oldal végtelen sok x esetén egyenlő. Ez azonban csak akkor lehet, ha (7.2) azonosság. □

Ebből már könnyen megkaphatjuk a Stirling–számok explicit alakját, aminek segítségével sokkal gyorsabban lehet kiszámolni nagy n-ekre $S(n,k)$-t.

7.2.6. Tétel.

$$S(n,k) = \frac{1}{k!}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n.$$

BIZONYÍTÁS:

$$\begin{aligned}
\frac{1}{k!}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n &= \sum_{j=0}^{k}\frac{(-1)^{k-j}}{j!(k-j)!}\sum_{r=0}^{n}S(n,r)j(j-1)\dots(j-r+1) = \\
&= \sum_{j=0}^{k}\frac{(-1)^{k-j}}{j!(k-j)!}\sum_{r=0}^{j}S(n,r)j(j-1)\dots(j-r+1) = \\
&= \sum_{j=0}^{k}\sum_{r=0}^{j}S(n,r)\frac{(-1)^{k-j}}{(k-j)!(j-r)!} = \sum_{r=0}^{k}\frac{S(n,r)}{(k-r)!}\sum_{j=r}^{k}(-1)^{k-j}\binom{k-r}{k-j} = \\
&= \sum_{r=0}^{k}\frac{S(n,r)}{(k-r)!}(1-1)^{k-r} = S(n,k).
\end{aligned}$$

□

7.2.7. Definíció. *Az*

$$f_k(x) = \sum_{n=1}^{\infty}S(n,k)\frac{x^n}{n!} = \sum_{n=k}^{\infty}S(n,k)\frac{x^n}{n!}$$

függvényt a Stirling–számok ***exponenciális generátorfüggvényének*** *hívjuk.*

7.2.8. Tétel.

$$f_k(x) = \frac{(e^x-1)^k}{k!}. \tag{7.3}$$

BIZONYÍTÁS: $k=1$ esetén tudjuk, hogy $S(n,k)=1$, tehát (7.3) teljesül, hiszen

$$\sum_{n=1}^{\infty}\frac{x^n}{n!} = e^x - 1.$$

k szerinti teljes indukcióval fogunk bizonyítani. Tegyük fel, hogy $j = k-1$-re már igazoltuk (7.3)-at. Ha belátjuk, hogy $f_k'(x) = e^x f_{k-1}$, akkor ebből már következik (7.3) k-ra is hiszen

$$\left(\frac{(e^x-1)^k}{k!}\right)' = e^x \frac{(e^x-1)^{k-1}}{(k-1)!},$$

és az $f_k(x)$ konstans tagja 0.
Először alakítsuk át $f_k(x)$-et a 7.2.6. tételbeli rekurziós összefüggés segítségével. Felhasználjuk azt is, hogy itt már $k > 1$, és így $S(1,k) = 0$.

$$\begin{aligned} f_k(x) &= \sum_{n=1}^{\infty} \frac{S(n,k)x^n}{n!} = \sum_{n=1}^{\infty} \frac{S(n+1,k)x^{n+1}}{(n+1)!} = \\ &= \sum_{n=1}^{\infty} \frac{x^{n+1}}{(n+1)!} \left[\sum_{p=k-1}^{n} \binom{n}{p} S(p,k-1)\right] = \\ &= \sum_{p=k-1}^{\infty} S(p,k-1) \left[\sum_{n=p}^{\infty} \frac{x^{n+1}}{(n+1)!}\binom{n}{p}\right] = \\ &= \sum_{p=k-1}^{\infty} \frac{S(p,k-1)}{p!} \left[\sum_{n=p}^{\infty} \frac{x^{n+1}}{(n+1)(n-p)!}\right]. \end{aligned}$$

Ebben a formában már könnyen elvégezhetjük a deriválást.

$$f_k'(x) = \sum_{p=k-1}^{\infty} \frac{S(p,k-1)}{p!} \left[\sum_{n=p}^{\infty} \frac{x^{n-p}}{(n-p)!}\right] \cdot x^p = e^x f_{k-1}(x).$$

□

7.3. Bell–számok

7.3.1. Definíció. *Jelöljük B_n-nel azt a számot, ahányféleképpen n darab különböző tárgyat csoportokba lehet osztani, azaz ahányféle* ***partíciója*** *van egy n elemű halmaznak. A B_n számokat* ***Bell–számoknak*** *nevezzük.*

A definícióból azonnal következik, hogy $B_n = \sum_{k=1}^{n} S(n,k)$, ha $n \geq 1$. Például $B_1 = 1, B_2 = 2, B_3 = 5$, B_0-t pedig definiáljuk 1-nek. Most keressünk explicit formulát, mint a Stirling–számoknál. Először adjunk rekurziós formulát a Bell–számokra.

7.3.2. Tétel.

$$B_n = \sum_{k=0}^{n-1} \binom{n-1}{k} B_k.$$

BIZONYÍTÁS: Legyen S az a halmaz, amit csoportokra akarunk osztani, és legyen $x \in S$. Tegyük fel, hogy az a csoport, amelyikben x van, k elemű. Ezt a csoportot

$\binom{n-1}{k-1}$ féleképpen választhatjuk ki, a többi tárgyat pedig B_{n-k} féleképpen oszthatjuk csoportokba. Tehát az olyan elosztások száma, amikor x egy k elemű csoportba kerül, éppen $\binom{n-1}{k-1}B_{n-k}$. Tehát

$$B_n = \sum_{k=1}^{n} \binom{n-1}{k-1} B_{n-k} = \sum_{k=0}^{n-1} \binom{n-1}{k} B_k.$$

□

7.3.3. Tétel.

$$B_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}.$$

BIZONYÍTÁS: Mivel $k > n$ esetén $S(n,k) = 0$, a Stirling–számok explicit formuláját felhasználva

$$B_n = \sum_{k=0}^{\infty} S(n,k) = \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^n =$$
$$= \sum_{j=0}^{\infty} \frac{j^n}{j!} \sum_{k=j}^{\infty} \frac{(-1)^{k-j}}{(k-j)!} = \sum_{j=0}^{\infty} \frac{j^n}{j!} \cdot \frac{1}{e},$$

ami pedig épp az állításunk. □

Most pedig foglalkozzunk a B_n exponenciális generátorfüggvényével.

7.3.4. Tétel.

$$b(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n = e^{e^x - 1}.$$

BIZONYÍTÁS: Itt is felhasználjuk az összefüggést a Stirling–számokkal, hiszen annak az exponenciális generátorfüggvényét már ismerjük.

$$b(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n = 1 + \sum_{n=1}^{\infty} \sum_{k=1}^{\infty} \frac{S(n,k)}{n!} x^n =$$
$$= 1 + \sum_{k=1}^{\infty} \sum_{n=1}^{\infty} \frac{S(n,k)}{n!} x^n = 1 + \sum_{k=1}^{\infty} \frac{(e^x - 1)^k}{k!}.$$

Ha ezt az utolsó tagot deriváljuk, azt kapjuk, hogy $b'(x) = e^x b(x)$. Ekkor viszont $(\log b(x))' = b'(x)/b(x) = e^x$ miatt tudjuk, hogy $b(x) = e^{e^x + c}$ valamilyen c konstansra. Tudjuk azonban, hogy $e^{e^0 + c} = b(0) = 1$, amiből következik, hogy $c = -1$. □

Most vizsgáljunk egy hasonló problémát. Hányféleképpen osztható n különböző tárgy λ_1 darab 1 elemű, λ_2 darab 2 elemű, ... , λ_t darab t elemű csoportra, ahol

$n = \sum_{k=1}^{t} k\lambda_k$? Eddigi ismereteink alapján ezt már könnyen meg tudjuk válaszolni. Az ilyen partíciók száma

$$\frac{n!}{\prod_{i=1}^{t}\lambda_i!\prod_{i=1}^{t}(i!)^{\lambda_i}}.$$

Nyilván, ha ezeket minden λ_i rendszerre összegezzük, akkor B_n-et kapjuk. Ezek szerint az exponenciális generátorfüggvényüknek is meg kell egyezniük. Ezt most másképp is belátjuk.

$$\sum_{n=0}^{\infty}\sum_{\substack{\forall\lambda_i\\ \text{rendsz.}}}\frac{x^n}{n!}\frac{n!}{\prod_{i=1}^{t}\lambda_i!(i!)^{\lambda_i}} = \sum_{n=0}^{\infty}\sum_{\substack{\forall\lambda_i\\ \text{rendsz.}}}\prod_{i=1}^{t}\frac{\left(\frac{x^i}{i!}\right)^{\lambda_i}}{\lambda_i!},$$

hiszen $n = \sum_{k=1}^{n} k\lambda_k$.

$$= \prod_{i=1}^{\infty} e^{\frac{x^i}{i!}} = e^{\sum_{i=1}^{\infty}\frac{x^i}{i!}} = e^{e^x-1}.$$

Evvel a Rényitől származó módszerrel megkaphatjuk azt is, hogy hány olyan partíció van, ahol a csoportok mérete egy adott $A \subseteq \{1,2,\ldots\}$ számhalmaz elemei. Például, minden i-re $\lambda_{2i+1} = 0$ helyettesítéssel megkaphatjuk, hány olyan partíció van, ahol a halmazok mérete páros szám. Általában az exponenciális generátorfüggvény

$$e^{\sum_{k\in A}\frac{x^k}{k!}}.$$

7.4. Számelméleti partíciók

Az előbbiekben az volt a kérdés, hogy hányféleképp oszthatunk csoportokra egy halmazt bizonyos feltételek mellett. Az ilyen tipusú felosztásokat **halmazelméleti partícióknak** hívjuk. **Számelméleti partícióról** beszélünk akkor, ha az a kérdés, hányféleképpen lehet az n számot összeadandókra bontani, valamilyen megkötésekkel.
$P(n,k)$-val azt jelöljük, hogy hányféleképpen lehet az n számot k darab pozitív egész szám összegeként előállítani. Például $P(4,2) = 2, P(5,3) = 2$. A Bell–számok analógiájára jelöljük a $\sum_{k=1}^{n} P(n,k)$ mennyiséget P_n-nel.

7.4.1. Tétel.

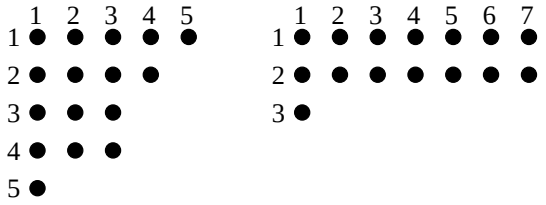
$$P(n+k,k) = \sum_{i=1}^{k} P(n,i).$$

BIZONYÍTÁS: Állítsuk elő először n-et k-nál nem több tag összegeként, és képzeljünk hozzá annyi 0 összeadandót, hogy összesen épp k darab összeadandó legyen. Most pedig adjunk hozzá minden összeadandóhoz 1-et. Így az $n+k$ számot állítottuk elő k darab összeadandóból. Innen pedig már következik az állítás. □

A most következő részben csak arról lesz szó, hogy néha különböző feltételek mellett is megegyezik a partíciók száma.

7.4.2. Tétel. *Az olyan partíciók száma, ahol a legnagyobb összeadandó k, megegyezik az olyan partíciók számával, ahol az összeadandók száma éppen k.*

BIZONYÍTÁS: Vegyünk egy olyan partíciót, ahol a legnagyobb összeadandó k. Rajzoljunk összesen n pontot egy négyzetháló pontjaira úgy, hogy az első oszlopba egymásután, felülről lefelé annyi pontot rajzolunk, amennyi a legnagyobb összeadandó értéke, a másodikba annyit, amennyi a második legnagyobb összeadandóé, stb. A 7.1. ábrán látható rajzokat **Ferrer–diagramoknak nevezik.**
Most nézzük meg, hány pont van egy-egy sorban. Így n-nek egy olyan partícióját kapjuk, ahol pontosan k összeadandónk van, hiszen pontosan k sor van. Tehát a kétféle partíció között egyértelmű megfeleltetés van, tehát számuk is megegyezik. □



7.1. ábra.

Evvel gyakorlatilag a következő tételt is bebizonyítottuk.

7.4.3. Tétel. *Az olyan partíciók száma, ahol a legnagyobb összeadandó legfeljebb k, megegyezik az olyan partíciók számával, ahol az összeadandók száma legfeljebb k.*

A következő tétel állítása hasonló formájú, a bizonyítás viszont másképp történik.

7.4.4. Tétel. *Az olyan partíciók száma, ahol minden összeadandó különböző, megegyezik az olyan partíciók számával, ahol minden összeadandó páratlan.*

BIZONYÍTÁS: Legyen $a_1 + a_2 + \ldots + a_m = n$, ahol minden a_i különböző; írjuk e számokat $a_i = 2^{\beta_i} b_i$ alakba, ahol b_i páratlan szám. Rendezzük át az így felírt összeget a b_i számok szerint. Egy d páratlan szám együtthatója $\sum_{b_i=d} 2^{\beta_i} = \gamma_d$ (a szummázás azon i indexek szerint történik, melyekre $b_i = d$). Ha tehát összeadunk γ_1 darab 1-est, γ_3 darab 3-ast, …, akkor n-nek egy olyan előállítását kaptuk, ahol minden összeadandó páratlan. Elég tehát azt megmutatnunk, hogy minden ilyen előállítást pontosan egyszer kaptunk meg a fenti módszerrel.

γ_d definíciójában minden β_i-nek különböznie kell, hiszen $\beta_i = \beta_j, b_i = b_j = d$-ből következik, hogy $a_i = a_j = 2^{\beta_i} d$. Tehát a β_i-k egyértelműen meghatározzák γ_d-t, másrészt viszont γ_d is egyértelműen meghatározza a β_i kitevőket. Ha tehát van egy előállításunk páratlan számokból, amelyben γ_i darab i-es szerepel, és felírjuk γ_d-t $\sum 2^{\beta_i(d)}$ alakban, akkor a $d2^{\beta_i(d)}$ számok egy különböző számokból álló felbontást adnak, éppen azt, amiből eredetileg kiindultunk. □

Most ismét a generátorfüggvényekkel foglalkozunk. Legyen

$$p(x) = \sum_{n=0}^{\infty} P_n x^n \quad \textbf{és } k \geq 1\textbf{-re} \quad p_k(x) = \sum_{n=k}^{\infty} P(n,k) x^n,$$

ahol $P_0 = 1$.

7.4.5. Tétel. a)

$$p(x) = \frac{1}{(1-x)(1-x^2)(1-x^3)\cdots} \tag{7.4}$$

b) $k \geq 1$*-re*

$$p_k(x) = \frac{x^k}{(1-x)(1-x^2)(1-x^3)\cdots(1-x^k)} \tag{7.5}$$

BIZONYÍTÁS: **a)** (7.4) jobb oldalát mindjárt átalakíthatjuk:

$$(7.4) = \prod_{i=1}^{\infty} \frac{1}{1-x^i} = \\ = (1+x+x^2+x^3+\ldots)(1+x^2+x^4+x^6+\ldots)(1+x^3+x^6+x^9+\ldots)\cdots$$

Ebben a szorzatban x^n együtthatója éppen annyi, ahányféleképp n előáll $k_1 + 2k_2 + \ldots + nk_n$ alakú összegként. Ez viszont éppen egy partíciónak felel meg, így (7.4)-et beláttuk.
b) Az a) rész alapján könnyen látszik, hogy ha $\overline{p}_k(x)$-szel jelöljük az olyan partíciók számának generátorfüggvényét, amelyben az összeadandók nem nagyobbak k-nál, akkor

$$\overline{p}_k(x) = \frac{1}{(1-x)(1-x^2)(1-x^3)\cdots(1-x^k)}.$$

Egy előző tétel miatt ez megegyezik az olyan partíciók $\overline{\overline{p}}_k(x)$ generátorfüggvényével, amelyekben az összeadandók száma nem több k-nál. Ekkor viszont

$$p_k(x) = \overline{\overline{p}}_k(x) - \overline{\overline{p}}_{k-1}(x) = \\ = \frac{1}{(1-x)(1-x^2)(1-x^3)\cdots(1-x^{k-1})}\left(\frac{1}{1-x^k} - 1\right) = (7.5).$$

□

Evvel a módszerrel egyébként sok hasonló, partíciók számára vonatkozó feladatot oldhatunk meg úgy, hogy közvetlenül felírjuk a generátorfüggvényét. Például a páratlan számok összegére való partíciók esetén:

$$\frac{1}{(1-x)(1-x^3)(1-x^5)\cdots},$$

különböző számok összegére:

$$(1+x)(1+x^2)(1+x^3)\cdots,$$

különböző páratlan számok összegére pedig:

$$(1+x)(1+x^3)(1+x^5)\cdots.$$

Ez utóbbiból egyébként új bizonyítást nyert Euler a 7.4.4. tételre. A kétfajta partíció generátorfüggvényei ugyanis megegyeznek.

$$\prod_{k=0}^{\infty}\frac{1}{1-x^{2k+1}}=\frac{\prod_{k=1}^{\infty}(1-x^{2k})}{\prod_{k=1}^{\infty}(1-x^k)}=\prod_{k=1}^{\infty}(1+x^k).$$

Itt jegyezzük meg, hogy az eddig tárgyalt mennyiségek nagyságrendileg mekkorák.

$$B_n\sim\frac{1}{\sqrt{n}}\beta^{n+\frac{1}{2}}e^{\beta-n-1},\ \textbf{ahol}\quad n=\beta\log\beta,$$
$$P_n\sim\frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}}.$$

Elég persze a nagyságrend érzékeléséhez annyit megjegyezni, hogy

$$\log B_n\sim n\log n$$
$$\log P_n\sim c\sqrt{n}.$$

7.5. Catalan–számok

Az alapfeladat annak a meghatározása, hogy hányféleképp zárójelezhető egy n tényezős szorzat. (Például $a(bc)d)e)f$ rossz zárójelezés.) Ezt a számot C_n-nel jelöljük. A C_n számokat **Catalan–számoknak** nevezzük. Először megadunk egy rekurziós formulát.

7.5.1. Tétel. *$C_1=1$, továbbá $n\geq 2$-re*

$$C_n=\sum_{k=1}^{n-1}C_kC_{n-k}.$$

BIZONYÍTÁS: Nyilvánvaló, hogy egy egytényezős szorzatot csak egyféleképpen lehet zárójelezni. $n \geq 2$ esetén osztályozzuk a zárójelezéseket a szerint, hányadik tényező után fordul elő először, hogy addig ugyanannyi bal és jobb zárójel van. Olyan zárójel pár, ami az összes tényezőt tartalmazza, nem lehet. Ha az i-edik tényező után fordul elő, hogy bezártunk minden megkezdett zárójelet, akkor az első i tényezőt C_i–féleképpen zárójelezhetjük, míg a többi $n-i$ darabot C_{n-i}–féleképp. Ezeket kell összegeznünk i szerint. □

Meg tudjuk határozni a Catalan–számok generátorfüggvényét is. Előbb azonban általánosabban is definiáljuk a binomiális együtthatókat.

7.5.2. Definíció. *Ha c tetszőleges valós, k pedig pozitív egész szám, akkor*

$$\binom{c}{k} = \frac{c(c-1)(c-2)\cdots(c-k+1)}{k!}.$$

Megjegyezzük, hogy $k > c$ esetén itt nem lesz feltétlenül 0 a binomiális együttható. Az egész számok esetén ugyanis ilyen esetben a számláló szorzótényezői között szerepel a 0, míg itt ez nem igaz.
Így felírhatjuk a binomiális tételt nem egész kitevő esetén is:

$$(a+b)^c = \sum_{k=0}^{\infty} \binom{c}{k} a^k b^{c-k}$$

7.5.3. Tétel.

$$C_n = \frac{1}{n}\binom{2n-2}{n-1}.$$

BIZONYÍTÁS: Legyen $c(x) = \sum_{n=1}^{\infty} C_n x^n$ a Catalan–számok generátorfüggvénye. Ekkor $[c(x)]^2 = C_1C_1x^2 + (C_2C_1 + C_1C_2)x^3 + \ldots = c(x) - x$. Ebből kifejezhetjük $c(x)$-et.

$$c(x) = \frac{1-\sqrt{1-4x}}{2}.$$

Ez a generátorfüggvény. (A gyök előjelének meghatározásához figyelembe vettük, hogy $c(x)$-ben konstans tag nem szerepel.)
Most alkalmazzuk a binomiális tétel általánosabb formáját:

$$c(x) = \frac{1}{2}\left[1 - \sum_{k=0}^{\infty} \binom{1/2}{k} (-4x)^k\right].$$

Alakítsuk át a binomiális együtthatót:

$$\binom{1/2}{k} = \frac{\left(\frac{1}{2}\right)^k (1-2)(1-4)(1-6)(1-8)\cdots(1-2k+2)}{k!} =$$
$$= (-1)^{k-1}\frac{1}{2^k}\frac{1\cdot 3\cdot 5\cdots(2k-3)}{k!} =$$

$$= (-1)^{k-1}\frac{1}{2^k}\frac{1\cdot 3\cdot 5\cdots(2k-3)}{k!}\cdot\frac{2\cdot 4\cdot 6\cdots(2k-2)}{2^{k-1}(k-1)!} =$$
$$= (-1)^{k-1}\frac{1}{k2^{2k-1}}\frac{(2k-2)!}{(k-1)!(k-1)!} = (-1)^{k-1}\frac{1}{k2^{2k-1}}\binom{2k-2}{k-1} =$$
$$= \frac{-2}{k}\left(-\frac{1}{4}\right)^k\binom{2k-2}{k-1}.$$

Ebből pedig már látszik, hogy a generátorfüggvényben x^n együtthatója

$$C_n = \frac{1}{n}\binom{2n-2}{n-1}.$$

□

Ismert feladat, hogy hányféleképpen állhat sorban egy mozi pénztáránál n ember 500 forintossal és n ember 1000 forintossal úgy, hogy a pénztáros mindig tudjon visszaadni (a jegy 500 Ft és kezdetben nincs pénz a pénztárban). A válasz C_{n+1}. Másik feladat, hogy egy konvex n szöget hányféleképpen lehet háromszögekre bontani egymást nem metsző átlókkal. A megoldás itt C_{n-1}.

8. fejezet

Extremális halmazrendszerek

8.1. Erdős–Ko–Radó tétele

Halmazrendszernek egy alaphalmaz részhalmazainak családját nevezzük. A halmazrendszereket írott nagybetűkkel jelöljük, legtöbbször F-fel. A halmazrendszer elemei az alaphalmaz részhalmazai, amiket nyomtatott nagy betűkkel jelölünk. Pl. $A \in F$. Az alaphalmaz elemeit kisbetűkkel jelöljük: $x, y \in A$. Mivel általában nem lényeges, hogy mik az alaphalmaz elemei, egy n elemű alaphalmazt $[n]$-nel jelölünk, és ennek összes részhalmazainak családját $2^{[n]}$-nel. Például halmazrendszer egy V alaphalmaz néhány kételemű részhalmaza. Ez természetesen egy gráfnak felel meg, a kételemű részhalmazok az élek. Emiatt szokás a halmazrendszereket **hipergráfoknak** is nevezni. Ha az összes részhalmaz k elemű, akkor k-**uniform** hipergráfról vagy halmazrendszerekről beszélünk. Így minden hurokmentes gráf egy 2-uniform hipergráf. Ebben a fejezetben általában arról lesz szó, hogy legfeljebb hány részhalmazt lehet megadni úgy, hogy azok kielégítsenek bizonyos feltételeket. Például bármely két halmaz messe egymást:

8.1.1. Tétel (Erdős–Ko–Radó, 1961). *Ha $F \subseteq 2^{[n]}$ k-uniform halmazrendszer ($k < n/2$) olyan, hogy minden $A, B \in F$-re $A \cap B \neq \emptyset$, akkor*

$$|F| \leq \binom{n-1}{k-1}.$$

BIZONYÍTÁS: [Katona O. H. Gyula, 1972] A házigazda és $n-1$ vendége egy köralakú asztalnál akarnak leülni. A házigazda az asztalfőre ül. F elemei olyan kisebb k tagú társaságok, akik mind egymás barátai, és ezért az asztalnál k egymásmelletti helyre akarnak ülni, azaz egy ívet alkotnak az asztal körül. Ültessük le valahogy a vendégeket. Így bizonyos társaságok ívet alkotnak, bizonyosak nem. A feltétel szerint bármely két társaságnak van közös tagja. Belátjuk, hogy legfeljebb k ív lehet az asztal körül.

Az asztalon két szomszédos hely között egy pohár van. Ha két társaság ugyanannál a pohárnál kezdődne, akkor az egyik társaság jobbra, a másik balra ül a pohártól, hiszen különben a két társaság megegyezne (minden társaság k emberből áll). Mivel

azonban $k < n/2$, ezért ennek a két társaságnak nincs közös tagja. Tehát minden pohárnál legfeljebb egy társaság kezdődik. Az első társaságnak az összes többi társasággal van közös tagja. Ekkor bármely másik társaság valamelyik vége egy olyan pohárnál van, ami az első társaság két tagja között van. Mivel az első társaság tagjai között $k-1$ pohár van, az elsőn kívül legfeljebb $k-1$ társaság alkot ívet az asztalnál.
Ülésrend összesen $(n-1)!$ van, így eddig $k(n-1)!$ társaságot számoltunk, de minden társaságot több ülésrendnél is számoltunk. Mindegyiket $k!(n-k)!$-szor, hiszen ennyiféle ülésrendnél alkot ívet egy társaság. Tehát a társaságok száma

$$|F| \leq \frac{k(n-1)!}{k!(n-k)!} = \binom{n-1}{k-1}.$$

□

Most nem elégszünk meg avval, hogy bármely két halmaz messe egymást, hanem a metszet méretét is meghatározzuk.

8.1.2. Tétel (Fischer–egyenlőtlenség). *Legyen $\{A_1, A_2, \ldots, A_m\} = F \subseteq 2^{[n]}$ olyan, hogy ha $i \neq j$, akkor $|A_i \cap A_j| = \lambda > 0$. Ekkor $m \leq n$.*

BIZONYÍTÁS: Ha van olyan A_i, amelynek elemszáma éppen λ, akkor bármely két másik halmaz metszete épp ez a halmaz, más elem nem lehet a metszetben. Tehát a többi halmaz A_i-n kívül eső része diszjunkt, így nyilván igaz az állítás, nem lehet $n-1$-nél több diszjunkt halmaz. Tehát feltehetjük, hogy minden i-re $|A_i| > \lambda$, így $\alpha_i = |A_i| - \lambda \geq 1$.
Legyen $\mathbf{a}_i$ az A_i halmaz **karakterisztikus vektora**, azaz $\mathbf{a}_i$ j-edik koordinátája 1, ha az alaphalmaz j-edik eleme benne van A_i-ben, és 0, ha nincs benne. Így a feltételek miatt

$$\mathbf{a}_i \mathbf{a}_j = \begin{cases} \lambda, & \text{ha } i \neq j \\ \lambda + \alpha_i, & \text{ha } i = j. \end{cases}$$

Lássuk be, hogy az $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m$ vektorok lineárisan függetlenek a valós számok teste felett. Tegyük fel, hogy $\sum_{i=1}^m c_i \mathbf{a}_i = \mathbf{0}$. Szorozzuk meg mindkét oldalt $\mathbf{a}_j$-vel. Így azt kapjuk, hogy $\lambda \sum_{i=0}^m c_i + c_j \alpha_j = 0$, bármely $j = 1, 2, \ldots, m$-re. Átrendezve

$$c_j = -\frac{\lambda}{\alpha_j} \sum_{i=0}^m c_i. \qquad j = 1, 2, \ldots, m$$

Ha $\sum_{i=0}^m c_i = 0$, akkor $c_j = 0$, azaz kész vagyunk. Ha $\sum_{i=0}^m c_i \neq 0$, akkor adjuk össze az m darab egyenlőséget:

$$\sum_{i=0}^m c_i = -\lambda \left(\sum_{j=1}^m \frac{1}{\alpha_j} \right) \sum_{i=0}^m c_i.$$

Mivel minden $\alpha_j \geq 1$, az egyik oldal pozitív, a másik negatív, tehát ellentmondást kaptunk.

Evvel beláttuk, hogy az $\mathbf{a}_i$ vektorok lineárisan függetlenek. Mivel azonban n-dimenziós vektorokról van szó, számuk legfeljebb n lehet. □

Most gyengítjük a feltételt a metszet méretére.

8.1.3. Tétel (Ray-Chaudhuri–Wilson, 1975). *Legyen $F \subseteq 2^{[n]}$, és legyen $\{l_1, l_2, \ldots, l_s\} = L$ nemnegatív, n-nél kisebb egészek halmaza. Ha bármely két különböző $A, B \in F$ -re $|A \cap B| \in L$, akkor*

$$|F| \leq \sum_{k=1}^{s} \binom{n}{k}.$$

BIZONYÍTÁS: Legyen $F = \{A_1, A_2, \ldots, A_m\}$ úgy, hogy $|A_1| \leq |A_2| \leq \ldots \leq |A_m|$ és A_i karakterisztikus vektora $\mathbf{v}_i = (v_{i,1}, v_{i,2}, \ldots, v_{i,n})$. Definiáljuk az n dimenziós valós $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ vektorok halmazán az $f_i(\mathbf{x})$ függvényt:

$$f_i(\mathbf{x}) = \prod_{l_j < |A_i|} (v_{i,1}x_1 + \ldots + v_{i,n}x_n - l_j).$$

Nyilvánvaló, hogy $f_i(\mathbf{v}_j) = 0$, ha $i > j$, viszont $f_i(\mathbf{v}_i) \neq 0$. Tekintsük most azokat a $g_i(\mathbf{x})$ függvényeket, amelyeket úgy kapunk, hogy f_i-ben minden j-re x_j hatványai helyére x_j-t helyettesítünk, azaz g_i-ben minden x_j csak első hatványon szerepel. Mivel a $\mathbf{v}_i$ vektorok $0,1$ vektorok voltak, teljesül, hogy $g_i(\mathbf{v}_j) = 0$, ha $i > j$, viszont $g_i(\mathbf{v}_i) \neq 0$. Ezért nyilván ezek is különböző függvények lesznek.
Belátjuk, hogy a $g_1, g_2, \ldots, g_m$ függvények lineárisan függetlenek. Tegyük fel, hogy $\sum_{i=1}^{m} \lambda_i g_i(\mathbf{x}) = 0$ minden $\mathbf{x}$-re, és van olyan λ_j, ami nem 0. Ekkor viszont

$$0 = \sum_{i=1}^{m} \lambda_i g_i(\mathbf{v}_1) = \lambda_1 g_1(\mathbf{v}_1).$$

Mivel $g_1(v_1) \neq 0$, ebből következik, hogy $\lambda_1 = 0$. Viszont ekkor

$$0 = \sum_{i=1}^{m} \lambda_i g_i(\mathbf{v}_2) = \lambda_2 g_2(\mathbf{v}_2),$$

amiből $\lambda_2 = 0$ következik. Ezt folytatva teljes indukcióval könnyen belátható, hogy minden λ_i együtthatónak nullának kell lennie. Ez viszont ellenmond a feltételünknek.
Tehát a g_i függvények lineárisan függetlenek. Minden g_i-ben minden x_j csak első hatványon szerepel, viszont g_i fokszáma legfeljebb s. Tehát ilyen lineárisan független függvény legfeljebb $\sum_{k=1}^{s} \binom{n}{k}$ van. □

8.2. Sperner–rendszerek

Mostantól másféle feltételt teszünk a halmazrendszerre.

8.2.1. Tétel (Sperner, 1928). *Legyen $F \subseteq 2^{[n]}$ olyan, hogy minden $A, B \in F$ -re $A \not\subseteq B$ és $B \not\subseteq A$. Ekkor*

$$|F| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}.$$

Most bebizonyítjuk a **LYM-egyenlőtlenséget**, amiből már következni fog a Sperner–tétel. A bizonyítás Lubelltől származik 1966-ból.

8.2.2. Tétel (Yamamoto, 1954). *Ha F teljesíti a Sperner–tétel feltételeit (F Sperner–rendszer), akkor*

$$\sum_{k=0}^{n} f_k \frac{1}{\binom{n}{k}} \leq 1, \tag{8.1}$$

ahol f_k az F -ben szereplő k elemű halmazok számát jelenti.

BIZONYÍTÁS: Legyen $2^{[n]}$-ben egy maximális lánc $L_1 \subset L_2 \subset \cdots \subset L_n = [n]$, ahol $|L_i| = i$. Egy ilyen lánc az alaphalmaz elemei egy permutációjának felel meg, tehát $n!$ darab ilyen lánc van. Egy tetszőleges maximális láncnak legfeljebb egy eleme szerepelhet F -ben, hiszen ha kettő szerepel, akkor az egyik része a másiknak, de így F nem Sperner–rendszer. Nézzük meg, hány láncban szerepelhet egy $A \in F$ halmaz. Ha $|A| = k$, akkor nyilván $k!(n-k)!$ darab maximális lánc tartalmazza A-t. Tehát ha minden A-hoz hozzárendeljük az őt tartalmazó maximális láncokat, akkor egy láncot sem számoltunk kétszer, mivel egy láncban nincs két elem a Sperner–rendszerből. Ezért

$$\sum_{k=0}^{n} f_k k!(n-k)! \leq n!,$$

amiből átrendezéssel a tétel állítását kapjuk. □

BIZONYÍTÁS: (Sperner–tétel) Könnyen látható, hogy minden k-ra igaz, hogy

$$\binom{n}{k} \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}.$$

Tehát (8.1)-ben a bal oldalt csökkentjük, ha $\binom{n}{k}$ helyett $\binom{n}{\lfloor \frac{n}{2} \rfloor}$-t írunk. Így

$$1 \geq \sum_{k=0}^{n} f_k \frac{1}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} = |F| \frac{1}{\binom{n}{\lfloor \frac{n}{2} \rfloor}}.$$

□

Ha $\emptyset \in F$, vagy az alaphalmaz szerepel F -ben akkor más halmaz nem lehet F -ben. Ezekkel nem foglalkozunk tovább. Könnyen látható, hogy ha F az összes k elemű halmazból áll, akkor Sperner–rendszer és (8.1)-ben egyenlőség teljesül. Most belátjuk, hogy csak akkor állhat egyenlőség, ha minden halmaz egyenlő méretű. Ebből pedig már könnyen kijön, hogy a Sperner–tételben csak akkor áll egyenlőség, ha az összes $\lfloor \frac{n}{2} \rfloor$ elemű halmazt (vagy páratlan n esetén az összes $\frac{n+1}{2}$ eleműt) vesszük.

8.2.3. Tétel. *A LYM-egyenlőtlenségben akkor és csak akkor teljesül egyenlőség, ha F az összes k elemű halmazból áll.*

BIZONYÍTÁS: Vegyük az alaphalmaz elemeinek egy $(x_1, x_2, \ldots, x_n)$ ciklikus permutációját (ez olyan, mint az ülésrend az Erdős–Ko–Radó–tételnél), amelyre F valamelyik eleme épp az $\{x_i, \ldots x_{k+i-1}\}$ halmaz, vagyis a permutációban épp k darab egymásután következő elemből áll, azaz egy ív. Az ilyen permutáció–halmaz párokat fogjuk kétféleképp összeszámolni.
Ha $F \in F$ és $|F| = k$, akkor pontosan $k!(n-k)!$ olyan permutáció van amelyben F egy ív. Tehát a permutáció–halmaz párok száma $\sum_{F \in F} |F|!(n-|F|)!$.
Jelöljük π_k-val, hogy egy adott π permutációban hány k hosszúságú ív szerepel F-ből. Ha két F-beli halmaznak megfelelő ív első eleme megegyezik, akkor az egyik ív tartalmazza a másikat, ekkor pedig F nem Sperner–rendszer. Tehát minden elem csak egy ív kezdőpontja lehet. Tehát $\sum_{k=1}^{n} \pi_k \leq n$. Belátjuk, hogy egyenlőség csak akkor állhat fenn, ha minden ív egyforma hosszú. Ha egyenlőség áll, akkor minden elemnél kezdődik egy ív. Ha nem volna minden ív egyforma, akkor van olyan ív, hogy a rákövetkező elemnél kezdődő ív rövidebb nála. Ekkor viszont F nem Sperner–rendszer. Mivel a ciklikus permutációk száma $(n-1)!$, a permutáció–halmaz párok száma legfeljebb $(n-1)!n$, és akkor és csak akkor pontosan ennyi, ha bármely permutációban az ívek hossza egyenlő. Mivel azonban bármely két F-beli halmazhoz van olyan permutáció, amelyben mindkettő ív, így akkor és csak akkor pontosan ennyi a permutáció–halmaz párok száma, ha bármely két halmaz mérete egyforma.
Ezt összevetjük avval, amit az előbb kaptunk.

$$\sum_{k=1}^{n} f_k k!(n-k)! = \sum_{F \in F} |F|!(n-|F|)! \leq n(n-1)! = n!$$

és egyenlőség akkor és csak akkor teljesül, ha F minden eleme egyenlő méretű halmaz, és F-ben az összes ekkora halmaz benne van. □

Ez egyben egy másik bizonyítás a LYM-egyenlőtlenségre. De ennél még egy általánosabb tételt is bebizonyítunk, amit Bollobás, Katona, Jaeger és Payan is egymástól függetlenül bebizonyított.

8.2.4. Tétel. *Legyen $|A_1| = |A_2| = \ldots |A_m| = k$, $|B_1| = |B_2| = \ldots |B_m| = l$, és $|A_i \cap B_j| = 0$ akkor és csak akkor, ha $i = j$. Ekkor*

$$m \leq \binom{k+l}{k}.$$

BIZONYÍTÁS: Legyen $(x_1, x_2, \ldots, x_n)$ az alaphalmaz egy permutációja. Ekkor legfeljebb egy i-re teljesül, hogy a permutációban A_i minden elemének az indexe kisebb B_i minden elemének az indexénél. Ha i és j is ilyen lenne, akkor $A_i \cap B_j$ vagy $A_j \cap B_i$ üres lenne, ami ellentmond a feltételnek. Mivel $n!$ permutáció van, az (A_i, B_i) párok száma legfeljebb $n!$.

Egy rögzített i-re viszont

$$\binom{n}{k+l}k!l!(n-k-l)! = \frac{n!}{\binom{k+l}{k}}$$

olyan permutáció van, amiben A_i elemeinek indexei kisebbek B_i elemeinek indexeinél. Vagyis minden (A_i, B_i) párt ennyiszer számoltunk az előbb. Tehát

$$m \leq n! \Big/ \frac{n!}{\binom{k+l}{k}} = \binom{k+l}{k}.$$

□

Ennek a tételnek egy általánosabb formája a következő tétel, amit nem bizonyítunk.

8.2.5. Tétel (Bollobás, 1964). *Legyenek $A_1, A_2, \ldots, A_m$ és $B_1, B_2, \ldots, B_m$ olyan halmazok, hogy $|A_i \cap B_j| = 0$ akkor és csak akkor, ha $i = j$. Ekkor*

$$\sum_{i=1}^{m} \frac{1}{\binom{|A_i|+|B_i|}{|A_i|}} \leq 1.$$

Ha $B_i = [n] - A_i$, akkor az előbbi feltétel épp azt jelenti, hogy A_i Sperner–rendszer, és az előbbi egyenlőtlenség a LYM-egyenlőtlenséget adja.
A LYM-egyenlőtlenség neve Yamamoto, Lubell és Meshalkin nevéből származik. Az igazság azonban az, hogy YBL M.-egyenlőtlenségnek is lehetne nevezni, hiszen Yamamoto 1954-ben bizonyította be a tételt algebrai módszerekkel, 1964-ben Bollobás belátta az előbbi tételt, 1966-ban Lubell adta meg az egyenlőtlenségnek az itt ismertett bizonyítását, végül Meshalkin 1968-ban egy további általánosítást adott.

Tárgymutató

Ajánlott irodalom

A témakör hallatlanul gazdag irodalmából csak néhány, jórészt magyar nyelvű könyvet emelünk ki.

[1] Andrásfai Béla: *Ismerkedés a gráfelmélettel* (Tankönyvkiadó, Budapest, 1985) és *Gráfelmélet (folyamok, mátrixok)* (Akadémiai Kiadó, Budapest, 1983)

[2] Bondy, J. A. és U. S. R. Murty: *Graph theory with applications* (McMillan Press, London, 1976)

[3] Diestel, R: *Graph theory* (Springer, Berlin, 2000)

[4] Elekes György: *Véges matematika példatár* (Eötvös Kiadó, Budapest, 1992)

[5] Freud Róbert és Gyarmati Edit: *Számelmélet* (Nemzeti Tankönyvkiadó, Budapest, 2000)

[6] Fuchs László: *Algebra* (Tankönyvkiadó, Budapest, 1991)

[7] Györfi László, Győri Sándor és Vajda István: *Információ- és kódelmélet* (Typotex, Budapest, 2000)

[8] Hajnal Péter: *Gráfelmélet* (Polygon, Szeged, 1997) és *Összeszámlálási problémák* (Polygon, Szeged, 1997)

[9] König Dénes: *Theorie der endlichen und unendlichen Graphen* (Leipzig, 1936)

[10] Lovász László: *Kombinatorikus problémák és feladatok* (Typotex, Budapest, 1999)

[11] Lovász László és Gács Péter: *Algoritmusok* (Tankönyvkiadó, Budapest, 1991)

[12] Lovász László és M. D. Plummer: *Matching theory* (North-Holland, Amsterdam, 1986)

[13] Rónyai Lajos, Ivanyos Gábor és Szabó Réka: *Algoritmusok* (Typotex, Budapest, 1999)

[14] Simonovits Miklós és T. Sós Vera: *Kombinatorika* (ELTE sokszorosított jegyzet, Budapest, 1981-82)

[15] Szendrei Ágnes: *Diszkrét matematika* (Polygon, Szeged, 1994)