Ajánlott és felhasznált irodalom: [Fleiner Tamás: Nagy, egyesített szuperjegyzet](http://www.cs.bme.hu/~fleiner/jegyzet/NESZ.pdf). Nagy segítségemre volt továbbá Vőneki Balázs korábbi, kézzel írt [jegyzete](https://wiki.sch.bme.hu/images/d/db/Bsz2_tetelkidolgozas_2009tavasz.pdf), saját előadásjegyzetek, Wikipédiás anyagok, valamint számtalan más, helyenként lábjegyzetben feltüntetett forrás. Igyekeztem hiteles(nek tűnő) szakirodalomra támaszkodva ellenőrizni a definíciókat, tételeket, bizonyításokat, de hiányosságok, pontatlanságok (bővebb kifejtésre szoruló dolgok), elgépelési vagy egyéb hibák természetesen maradhattak a jegyzetben. Ezekért a hibákért felelősséget nem vállalok, de kérlek, javítsátok, amint ilyet felfedeztek. Sok sikert kívánok a vizsgához! Haraszin Péter (harapetiATschDOTbmeDOThu)

Tartalomjegyzék

[1.) Hamilton-körök és -utak. Szükséges feltétel Hamilton-kör/út létezésére. Elégséges feltételek: Dirac és Ore tétele. Euler-körséták és -séták, ezek létezésének szükséges és elégséges feltétele. 3](#_Toc378079941)

[Hamilton-körök és -utak 3](#_Toc378079942)

[Szükséges feltétel Hamilton-kör/út létezésére 3](#_Toc378079943)

[Elégséges feltételek: Dirac és Ore tétele 3](#_Toc378079944)

[Euler-körséták és -séták, ezek létezésének szükséges és elégséges feltétele 4](#_Toc378079945)

[2.) Gráfok színezése. fogalma és viszonya -hez, illetve -hez. Brooks tétele (biz. nélkül). Mycielski konstrukciója. 5](#_Toc378079946)

[Gráfok színezése, fogalma 5](#_Toc378079947)

[viszonya -hez, illetve -hez 5](#_Toc378079948)

[Brooks tétele 6](#_Toc378079949)

[Mycielski konstrukciója 6](#_Toc378079950)

[3.) Síkbarajzolható gráfok kromatikus száma, ötszíntétel. Élkromatikus szám: viszonya -hez, Vizing-tétel (biz. nélkül), páros gráfok élkromatikus száma. 7](#_Toc378079951)

[Síkbarajzolható gráfok kromatikus száma, ötszíntétel 7](#_Toc378079952)

[fogalma és viszonya -hez 7](#_Toc378079953)

[Vizing-tétel 7](#_Toc378079954)

[Páros gráfok élkromatikus száma (Kőnig tétele) 8](#_Toc378079955)

[4.) Perfekt gráfok: erős perfekt gráf tétel (csak a szükségesség bizonyításával), Lovász tétele (biz. az erős perfekt gráf tételből). Intervallumgráfok perfektsége. 9](#_Toc378079956)

[Perfekt gráfok 9](#_Toc378079957)

[Erős perfekt gráf tétel 9](#_Toc378079958)

[Lovász tétele 10](#_Toc378079959)

[Intervallumgráfok perfektsége 10](#_Toc378079960)

[5.) Páros gráf fogalma, kapcsolat a páratlan körökkel. Párosítások páros gráfban, a javítóutak módszere, Kőnig, Hall és Frobenius tételei. 11](#_Toc378079961)

[Páros gráf fogalma 11](#_Toc378079962)

[Kapcsolat a páratlan körökkel 11](#_Toc378079963)

[Párosítások páros gráfban, Kőnig tétele 11](#_Toc378079964)

[Hall tétele 12](#_Toc378079965)

[Frobenius tétele 13](#_Toc378079966)

[A javítóutak módszere 13](#_Toc378079967)

[6.) Párosítások tetszőleges gráfban, Tutte tétele (csak a szükségesség bizonyításával). Gallai tételei. 15](#_Toc378079968)

[Párosítások tetszőleges gráfban, Tutte tétele 16](#_Toc378079969)

[Gallai tételei 16](#_Toc378079970)

[7.) Hálózat, hálózati folyam és vágás fogalma, folyam értéke, vágás kapacitása. Algoritmus a maximális folyam és a minimális vágás megkeresésére, Ford-Fulkerson tétel, Edmonds-Karp tétel (biz. nélkül), egészértékűségi lemma. A folyamprobléma általánosításai. 17](#_Toc378079971)

[Hálózat 17](#_Toc378079972)

[Hálózati folyam 17](#_Toc378079973)

[Folyam értéke 17](#_Toc378079974)

[Vágás 17](#_Toc378079975)

[Vágás kapacitása 18](#_Toc378079976)

[Algoritmus a maximális folyam és a minimális vágás megkeresésére 18](#_Toc378079977)

[Ford-Fulkerson-tétel 19](#_Toc378079978)

[Edmonds-Karp tétel 19](#_Toc378079979)

[Egészértékűségi lemma 19](#_Toc378079980)

[A folyamprobléma általánosításai 19](#_Toc378079981)

[8.) Menger pontpárok közötti diszjunkt utakra vonatkozó tételei. Többszörös összefüggőség és élösszefüggőség fogalma, Menger ezekre vonatkozó tételei. 21](#_Toc378079982)

[Menger pontpárok közötti diszjunkt utakra vonatkozó tételei 21](#_Toc378079983)

[Az él-összefüggőségi változat irányított gráfokban 21](#_Toc378079984)

[Az él-összefüggőségi változat irányítatlan gráfokban 21](#_Toc378079985)

[A csúcs-összefüggőségi változat irányított/irányítatlan gráfokban 21](#_Toc378079986)

[Többszörös összefüggőség és élösszefüggőség fogalma, Menger ezekre vonatkozó tételei 22](#_Toc378079987)

[9.) Gráfok szomszédossági mátrixa, a szomszédossági mátrix hatványainak jelentése. Irányított gráf illeszkedési mátrixa. 23](#_Toc378079988)

[Gráfok szomszédossági mátrixa 23](#_Toc378079989)

[A szomszédossági mátrix hatványainak jelentése 23](#_Toc378079990)

[Irányított gráf illeszkedési mátrixa 23](#_Toc378079991)

[10.) Oszthatóság, felbonthatatlan és prímtulajdonságú számok, ezek kapcsolata (bizonyítás csak az egyik irányban), a számelmélet alaptétele. Osztók száma. Prímek száma, hézag a szomszédos prímek között, nagyságrendje (biz. nélkül). Kongruencia fogalma, alapműveletek kongruenciákkal 26](#_Toc378079992)

[Oszthatóság, felbonthatatlan és prímtulajdonságú számok, ezek kapcsolata 26](#_Toc378079993)

[A számelmélet alaptétele 26](#_Toc378079994)

[Osztók száma 26](#_Toc378079995)

[Prímek száma 27](#_Toc378079996)

[Hézag a szomszédos prímek között 27](#_Toc378079997)

[nagyságrendje 27](#_Toc378079998)

[Kongruencia fogalma, alapműveletek kongruenciákkal 28](#_Toc378079999)

[11.) Lineáris kongruenciák: a megoldhatóság szükséges és elégséges feltétele, a megoldások száma. Euklideszi algoritmus, ennek alkalmazása lineáris kongruenciák megoldására is. Wilson tétele 29](#_Toc378080000)

[Lineáris kongruenciák: a megoldhatóság szükséges és elégséges feltétele, a megoldások száma 29](#_Toc378080001)

[Euklideszi algoritmus (ennek alkalmazása lineáris kongruenciák megoldására is) 29](#_Toc378080002)

[Wilson tétele 30](#_Toc378080003)

[12.) Euler-féle ϕ-függvény, redukált maradékrendszer, Euler-Fermat-tétel, kis Fermat-tétel. Kétismeretlenes, lineáris diofantikus egyenlet megoldása (konkrét példán). Két kongruenciából álló kongruenciarendszer megoldása (konkrét példán) 32](#_Toc378080004)

[Euler-féle ϕ-függvény 32](#_Toc378080005)

[Redukált maradékrendszer 32](#_Toc378080006)

[Euler-Fermat-tétel, kis Fermat-tétel 32](#_Toc378080007)

[Kétismeretlenes, lineáris diofantikus egyenlet megoldása (konkrét példán) 33](#_Toc378080008)

[Két kongruenciából álló kongruenciarendszer megoldása (konkrét példán) 33](#_Toc378080009)

[13.) Számelmélet és algoritmusok: alapműveletek, hatványozás az egészek körében és modulo m. Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosítás. 34](#_Toc378080010)

[Számelmélet és algoritmusok: alapműveletek, hatványozás az egészek körében és modulo m 34](#_Toc378080011)

[Prímtesztelés 34](#_Toc378080012)

[Carmichael számok 35](#_Toc378080013)

[Nyilvános kulcsú titkosítás 35](#_Toc378080014)

[14.) Művelet fogalma, csoport, Abel-csoport. Példák: csoportok számokon, mátrixokon, rajzok szimmetriacsoportja, diédercsoport. Példák véges és végtelen, kommutatív és nem kommutatív csoportra mind a négy lehetséges variációban. 36](#_Toc378080015)

[Művelet fogalma 36](#_Toc378080016)

[Csoport, Abel-csoport 36](#_Toc378080017)

[Csoportok számokon 37](#_Toc378080018)

[Csoportok mátrixokon 37](#_Toc378080019)

[Rajzok/alakzatok szimmetriacsoportja 37](#_Toc378080020)

[Diédercsoport 39](#_Toc378080021)

[15.) Elem rendje (ez véges csoportban véges), ciklikus csoport. Részcsoport. Szimmetrikus csoport. Csoportok izomorfiája. 40](#_Toc378080022)

[Elem rendje (ez véges csoportban véges) 40](#_Toc378080023)

[Ciklikus csoport 40](#_Toc378080024)

[Részcsoport. Csoportok izomorfiája 41](#_Toc378080025)

[Szimmetrikus csoport 41](#_Toc378080026)

[16.) Mellékosztály fogalma, példák. Lagrange tétele, elemrend és csoport rendjének kapcsolata. 44](#_Toc378080027)

[Mellékosztály fogalma, példák 44](#_Toc378080028)

[Lagrange tétele, elemrend és csoport rendjének kapcsolata 45](#_Toc378080029)

[17.) Gyűrű, ferdetest és test fogalma. Nullosztómentes gyűrű, test nullosztómentessége. Példák:, , , , , -es mátrixok, polinomok, (ez milyen -re test), kvaterniók, . 46](#_Toc378080030)

[Gyűrű, ferdetest és test fogalma 46](#_Toc378080031)

[Példák:, , , , , -es mátrixok, polinomok 46](#_Toc378080032)

[Nullosztómentes gyűrű, test nullosztómentessége 47](#_Toc378080033)

[(ez milyen -re test) 47](#_Toc378080034)

[Kvaterniók 48](#_Toc378080035)

[, azaz is test (a racionális számok kibővítve -vel) 48](#_Toc378080036)

1.) Hamilton-körök és -utak. Szükséges feltétel Hamilton-kör/út létezésére. Elégséges feltételek: Dirac és Ore tétele. Euler-körséták és -séták, ezek létezésének szükséges és elégséges feltétele.

## Hamilton-körök és -utak

**Def.:** A gráf Hamilton-köre (Hamilton-útja) a G gráf olyan köre (útja), ami a gráf minden **csúcsát** pontosan egyszer tartalmazza. (egyszer: egy körben/útban szereplő minden csúcs különböző.) Ha G-ben van Hamilton-kör, akkor van benne Hamilton-út is.

Pl.: a -ban egy H-kör:

## Szükséges feltétel Hamilton-kör/út létezésére

1. Ha ∃ ***H-kör*** ⇒ -ből akárhogy  db csúcsot törölve ***legfeljebb*** komponensre esik szét.
2. Ha ∃ ***H-út*** ⇒ -ből akárhogy  db csúcsot törölve ***legfeljebb***  komponensre esik szét.

Bizonyítás: H-kör

A ***H-kör*** pontjai legyenek és legyen az a  ***pont***, amit elhagyunk.

v2

vn

v1

vi1







Vegyük észre, hogy az elhagyott pontok közötti „ívek” biztosan összefüggő komponenseket alkotnak!

Pl.: (, , ) ív is összefüggő lesz, hiszen két szomszédos pontja között az eredeti ***H-kör*** egy éle fut.

Mivel éppen ilyen ívet kapunk, nem lehet több komponens ***-nál***. (Kevesebb lehet, hiszen különböző ívek között lehetnek élek. Pl.: piros él.)

Bizonyítás: H-út  
A bizonyítás nagyon hasonló azt előzőhöz. Pl. hagyjuk el a gráfból a élet, hogy csak H-utunk legyen! Amíg az előző példában a pontok elhagyása után a , …, , , , ív összefüggő volt, itt már nem, mert ∉. tehát legfeljebb komponens keletkezhetett.  ✓

Példa arra, hogy a szükséges feltétel nem elégséges:  
***Petersen-gráf***: A Petersen-gráfnak nincs H.-köre, pedig teljesíti a szükséges feltételt (akárhogyan törlök db pontot, max. komponensre esik szét). Ha volna H.-köre, akkor 3 színnel színezhetnénk az éleit úgy, hogy az **azonos színű élek páronként diszjunktak** legyenek. (A H.-kör 10 élére kell 2 szín, a kimaradó élek pedig diszjunktak, mivel a Petersen-gráf 3-reguláris ( csúcs fokszáma 3).) Márpedig a külső ötszög és a hozzá csatlakozó élek 3-színezése (a szimmetria miatt) lényegében egyértelmű, és ez nem terjeszthető ki globális 3-színezéssé.  
Ha a Petersen-gráf külső köréből , a belső köréből pedig csúcsot hagyunk el, akkor a külső ill. a belső körön keletkező komponensek száma legfeljebb ill , vagyis a gráfnak nem keletkezhet összességében -nél több komponense. (Ha v. , akkor az adott körön egy komponens keletkezik, de ennek a komponensnek a „másik” körből is lesz pontja.)

## Elégséges feltételek: Dirac és Ore tétele

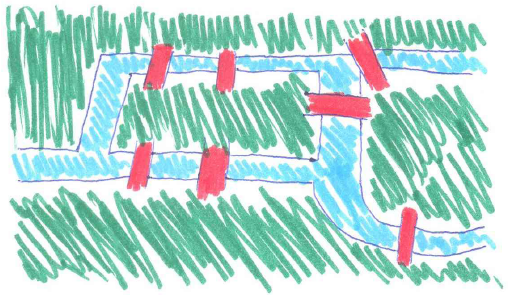
**Tétel**: (Ore) Ha az -pontú (), **egyszerű** gráfban ∀ két, nem szomszédos csúcsra ⇒ ∃ ***H-kör.***

Bizonyítás:  
Indirekt. Tfh. a két feltétel teljesülése ellenére ∄ ***H-kör*** a gráfban.  
A gráfhoz vegyünk hozzá éleket úgy, hogy továbbra se legyen benne ***H-kör***. Ezt ismételjük addig, amíg lehet. Az így kapott gráfot jelöljük -vel, amire szintén teljesül a feltétel.  
-ben biztosan van két nem szomszédos pont. Legyen ez . gráfban ∃ ***H-kör*** ⇒ ***G’***-ben ∃ ***H-út***.  
Legyen ez . Ha  szomszédos -val ⇒  nem szomszédos -gyel, mert H-kör lenne, tehát ⇒ ⭍  **ELLENTMONDÁS.**

Tétel: (Dirac) Ha az -pontú (), egyszerű gráfban ∀ pont foka legalább   ⇒ ∃ H-kör.

Bizonyítás: Teljesül az Ore-feltétel: pontpárra

## Euler-körséták és -séták, ezek létezésének szükséges és elégséges feltétele

*Königsbergi hidak problémája*:  
← Feladat: ∀ hídon pontosan egyszer átkelni.

A feladat gráfelméleti megfelelője: a folyók által határolt területeknek pontok, a hidaknak élek felelnek meg.

**3**

**3**

**5**

**3**

Def.: -ben ***Euler-kör*** (Euler-körséta) egy olyan zárt élsorozat, ami a gráf ∀ **élét** pontosan egyszer tartalmazza. Ha az élsorozat nem feltétlenül zárt, akkor ***Euler-ut***at (Euler-sétát) kapunk.

Megjegyzés:  
∀ Euler-kör egyben Euler-út is.  
Az Euler-kör/út általában nem „rendes” kör/út a gráfban, mert egy ponton többször is áthalad.

Tétel: (szükségesség)  
1.) Ha összefüggő (véges) gráfban ∃ E-kör ⇒ ∀ pont foka páros.  
2.) Ha összefüggő (véges) gráfban ∃ E-út ⇒ -nek 0 vagy 2 páratlan fokú csúcsa van.

Bizonyítás:  
1.) Induljunk el a gráf egy tetszőleges pontjáról és járjunk körbe az E-kör mentén. Minden pontban pontosan annyiszor mentünk be, ahányszor kimentünk. A kimenések és bemenések számának összege a pont fokszáma, ami így biztosan páros.  
2.) Az előzőhöz hasonlóan belátható, hogyha G-ben ∃ E-út, akkor az E-út két végpontjának kivételével ∀ pont foka páros.

Tétel (elégségesség):

1. Ha összefüggő (véges) gráfban ∃ E-kör ⇔ ∀ pont foka páros.
2. Ha összefüggő (véges) gráfban ∃ E-út ⇔ -nek 0 vagy 2 páratlan fokú csúcsa van.

Bizonyítás:

A *szükségesség*et előbb bebizonyítottuk.

*Elégségesség*

1. Legyen a gráf tetszőleges pontja, pedig egy -ből induló élismétlés nélküli séta, amíg elakadunk. Mivel ∀ pont foka páros ⇒

v

P

G

 -ben akad el

 -nek ∀ élét használja

 ∀ csúcsból páros sok élet használt

Legyen P’ az ilyen séták közül a leghosszabb.

**Állítás**: E-kör

Bizonyítás:

(indirekt) : -ből elhagyjuk a -beli éleket. Tudjuk, hogy -ban ∀ fokszám páros ()

legyen olyan csúcs, amire illeszkedik a -beli és -beli él is (megtehetjük, mert a gráf összefüggő.)

legyen egy -ből induló -ban élismétlésmentes -ben elakadó séta.

P’

Q

P’

v

v

w

w

Ez hosszabb -nél: **ELLENTMONDÁS**. 🗲

1. Ha ∀ fokszám páros ⇒ OK (Euler-kör)

Ha van két páratlan fokú pont: , akkor húzzunk élet közé. Így ∀ pont foka páros lesz. Tehát lesz E-kör. Ha ebből a gráfból elhagyjuk -t, akkor lesz E-út.

2.) Gráfok színezése. fogalma és viszonya -hez, illetve -hez. Brooks tétele (biz. nélkül). Mycielski konstrukciója.

## Gráfok színezése, fogalma

**Def.:** egy gráf színnel színezhető, ha a csúcsok színnel színezhetők úgy, hogy szomszédos csúcsok különböző színt kapnak.

kromatikus száma k, ha színnel színezhető, de -gyel nem. Jele

Pl.:

. . . .

🡪

üres gráfnál:

páros gráfnál: (akkor , ha üres a gráf)

## viszonya -hez, illetve -hez

**Def.**: egy teljes részgráfját klikknek nevezzük.

**Def.**: maximális klikkmérete (azaz a legnagyobb klikkben lévő pontok száma) , ha -ben van db csúcs, hogy közülük bármely kettő szomszédos, de nem. Ezt a gráf klikkszámának nevezzük.  
**Jele:**

**Állítás**: gráfban

Bizonyítás: Ha , akkor a csúcshoz kell db szín

Példa:

**Mohó színezés**: csúcsokat jelöljük -nel

a színeknek adjunk számokat: **➀** **➁** **➂** …

v1  → **➀**

Ha már színezett → színe legyen a legkisebb sorszámú olyan szín, amilyen szomszéd még nincs.

Pl.:

v5

v1       v2        v3      v4

Tétel: (ahol a gráf maximális fokszáma)

Bizonyítás:  
Ha *mohó színezéssel* elkezdjük tetszőleges sorrendben színezni a gráf pontjait, akkor nem kell -nél több színt felhasználnunk, mert amikor egy újabb pontot akarunk kiszínezni, akkor ennek legfeljebb szomszédja van már kiszínezve. Így a -ediket felhasználhatjuk.

## Brooks tétele

Tétel: (Brooks) Ha (véges) egyszerű összefüggő gráf, nem teljes gráf (), nem páratlan hosszú kör ()  .

## Mycielski konstrukciója

Tétel: (Mycielski konstrukciója) egész számra gráf, hogy és ,   
Azt mutatja meg, hogy sokszor a alsó becslés nem sokat ér.

Bizonyítás:  
G2-nek megfelel: .  
Tegyük fel, hogy már -t megalkottuk, készítünk ebből -et! pontjai: . Vegyünk fel új pontot: t a következőképp: -t kössünk össze -beli szomszédjával (de -vel ne), -t pedig -vel.

Állítás**:**

Bizonyítás: (indirekt)  
Tegyük fel, hogy -ben háromszög (Δ). Ennek nem lehet mind a 3 csúcsa -ban. Ha a Δ egyik csúcsa, a másik kettő csak és lehet, de ezek nem szomszédosak. Ha a Δ egyik csúcsa, akkor a másik két csúcs és lehet. Mivel szomszédjai megegyeznek szomszédjaival, ekkor nemcsak , hanem is Δ lenne. **🡪 ELLENTMONDÁS**.

Állítás:

Bizonyítás: Színezzük ki -t ugyanolyan színnel, mint egy színnel való színezésében, majd -t színezzük színűre, kapja a -edik színt.

Állítás:

Bizonyítás: (indirekt)

Tfh. ! (Ennél kisebb pont nem lehet, mert részgráfként tartalmazza -t és  ).

Jelöljük pont színét -szel. Legyen

Megadunk egy színezést az pontok által feszített részgráfban (ami -val iztomorf).

Beláthatjuk, hogy egy színnel való jó színezése ***Gk***-nak, ami ***ellentmondás***, mert .

Az olyan élekkel nem lehet probléma, amelyeknek egyik végpontja sem volt színű.

Tfh. és szomszédos egy olyan -vel, hogy !

Mivel az eredeti színezés jó volt:

⇒⇒⇒

⇒

De szomszédok -ban ⇒ szomszédok -ben

**🡪Ellentmondás**⭍

⇒⇒

⇒⇒ egy színezése -nak

🡪🡪**ELLENTMONDÁS**⭍

3.) Síkbarajzolható gráfok kromatikus száma, ötszíntétel. Élkromatikus szám: viszonya -hez, Vizing-tétel (biz. nélkül), páros gráfok élkromatikus száma.

## Síkbarajzolható gráfok kromatikus száma, ötszíntétel

Általában nem könnyű becslést adni egy gráf kromatikus számára. Ha viszont a gráf síkba rajzolható, akkor lényegesen könnyebb a helyzet.

Tétel: (5-szín tétel) Ha síkbarajzolható gráf (lerajzolható a síkba úgy, hogy az élei ne messék egymást (gömbre is rajzolható)), akkor .

Bizonyítás:  
A párhuzamos élek nem befolyásolják a színezést, ezért feltehetjük, hogy a gráf **egyszerű**.  
2 pontú gráfra nyilván igaz az állítás. Nagyobb gráfokra *pontszám szerinti indukcióval* bizonyítjuk.  
Tegyük fel, hogy a legfeljebb pontú gráfokra a tétel igaz. Legyen egy pontú egyszerű síkba rajzolható gráf. Ha ∀ pont foka legalább 6 lenne, akkor ez teljesülne rá (tétel: ):  
 ⭍  **ELLENTMONDÁS** ⇒ -nek legfeljebb 5-ödfokú csúcsa. Jelöljük -szel.  
Ha is egyszerű síkba rajzolható gráf, az indukciós feltevés miatt 5-színezhető.  
Ha szomszédjai max. 4 színt kapnak, akkor megkaphatja az 5. színt.  
Ez akkor nem működik, ha és mind az 5 szomszéd különböző színű.  
Ha -nek bármely két szomszédja között lenne él, akkor -ben lenne , ami ellentmond síkba rajzolhatóságának.  
Tehát két szomszédja, és nincs összekötve.  
Húzzuk össze egy ponttá pontokat. Az így kapott ***G’*** gráf – az indukciós feltétel miatt – 5 színezhető.  
Az ennek megfelelő színezés ***G***-ben nem jó, mert egyszínűek. ***G***-ben -nek 3 szomszédja van -on és -n kívül, ezek max. 3 színt foglalunk le, és további két szomszéd, és egyszínű. (Ez megtehető, mert szomszédosak.)  
Tehát -nek marad az ötödik szám. ∎

Tétel: (4-szín tétel) Ha síkbarajzolható gráf ⇒ Ezt a tételt Appel és Haken bizonyította be először 1977-ben. Itt alkalmaztak először bizonyításhoz számítógépes módszereket.

Def.: A gráf élgráfja az az gráf, aminek a csúcsai G éleinek felelnek meg, és 2 csúcsa pontosan akkor van éllel összekötve, ha megfelelő élei szomszédosak.

## fogalma és viszonya -hez

Def.: A gráf -élszínezhető, ha élei  db színnel kiszínezhetőek úgy, hogy bármely két szomszédos él színe különböző legyen. A G gráf élkromatikus száma (vagy ), ha -élszínezhető, de nem -élszínezhető (ha élei színnel színezhetők, de -gyel nem).

Megj.: -élszínezhető ⟺ -színezhető, továbbá .

Példa:

Állítás: tetsz. G gráfra , továbbá, ha , akkor .

Biz.: az egy csúcsból induló éleknek megfelelő pontok klikket alkotnak -ben. Másfelől minden klikkje vagy G egy csúcsból induló néhány élének, vagy G egy háromszögének felel meg.

Állítás: tetszőleges G gráfra.

Biz.: az egy csúcsból induló élek egymástól különböző színt kapnak, és ez speciálisan a max. fokszámú csúcsból induló élekre is igaz. Formálisan: .

Tekintsük a gráf egy max. fokú csúcsát! ()  
Ennek Δ db szomszédja van. Az ezekhez húzott élek különböző színt kell, hogy kapjanak.

v1

## Vizing-tétel

Tétel: (Vizing) Ha egyszerű ⇒ .

Ellenpélda (ha nem egyszerű):

vagy : , .

(nem egyszerű, ld. párh. élek)

## Páros gráfok élkromatikus száma (Kőnig tétele)

Tétel: (Kőnig) Ha páros gráf, akkor .

Biz.: az előző állítás miatt elegendő azt igazolni, hogy , azaz csupán egy -élszínezést kell mutatni.  
∃ olyan ps. gráf, melynek részgráfja, és minden csúcsának fokszáma . (Ilyen -t pl. úgy kaphatunk, hogy mellé felvesszük még -nek egy másolatát, színosztályai és lesznek, és ∀ csúcs és annak másolata közé behúzunk további párhuzamos élt.) Ha sikerül a -reguláris gráf éleit színnel kiszínezni, akkor egyúttal a részgráf éleinek is megkapjuk egy ugyanennyi színnel való színezését.  
A gráf élszínezéséhez pedig elegendő azt megmutatni, hogy tetszőleges reguláris gráfban van teljes psítás. Ugyanis akkor egy teljes psítását kiszínezve az első színnel, a színezetlen élek egy -reguláris páros gráfot alkotnak, abban is találunk egy teljes psítást, ez a második színt kapja, stb.  
Miért ∃ tehát egy -reguláris ps gráfnak teljes psítása? A Hall-feltétel teljesülését kell csupán ellenőrizni. Ha az egyik színosztályból kiválasztunk egy pontú halmazt, akkor az X-beli csúcsokból összesen él indul ki. Mindezen élekből a másik színosztály bármely csúcsa legfeljebb -t fogadhat be, tehát a darab él megérkezéséhez legalább pontra van szükség: . A Hall-feltétel az -reguláris gráf bármelyik színosztályára teljesül, tehát csakugyan ∃ teljes psítás, és pontosan ezt kellett bizonyítanunk.

4.) Perfekt gráfok: erős perfekt gráf tétel (csak a szükségesség bizonyításával), Lovász tétele (biz. az erős perfekt gráf tételből). Intervallumgráfok perfektsége.

Egy gráf kromatikus száma és klikkszáma között általában nem tételeztünk fel egyenlőséget. Mégis igen sok példa van arra, amikor ez a két paraméter egyenlő (pl. páros gráfok). Felmerül a kérdés: érdemes-e közelebbről is megvizsgálni ezeket a gráfokat.  
A válasz igen, ha még kikötjük, hogy ne csak magára a gráfra, hanem ∀ feszített részgráfjára is igaz legyen. Enélkül ugyanis tetszőleges gráfot kiegészíthetnénk egy elegendően nagy klikk hozzá vételével.

## Perfekt gráfok

Def.: perfekt, ha minden feszített részgráfjára

Megjegyzés: Ez a halmaz tartalmazza magát -t is!

Példák:

:

nem perfekt ✖

+

∀ fesz. részgráfjára

perfekt ✓

DE nem perfekt, mert tartalmazza feszített részgráfként az előző -öt ✖

**páros gráfok**:

- ha van éle:

- ha nincs éle:

ps. gráfok részgráfja is ps. 🡪 ezek perfektek ✓

**Tétel:** Ha komplementere () páros gráf, akkor perfekt.

**Biz.**: Ha G páros gráf komplementere, akkor ∀ feszített részgráfja is páros gráf komplementere, ezért elegendő azt bizonyítani, hogy , ha G komplementere páros. Kőnig és Gallai tételei alapján (ps. gráfban nincs hurokél)  
A egyenlőség igazolásához a triviális egyenlőtlenség miatt elegendő a bizonyítása, azaz G egy színnel történő színezésének megadása. Ilyet pedig úgy kapunk, hogy rögzítjük -nek egy élből álló, maximális psítását, és ∀ csúcsot kül. színnel színezünk, kivéve, hogy M ∀ élének végpontjai azonos színt kapnak. Ezáltal a felhasznált színekben az -hez képest megtakarítást érünk el.

(NEM KELL) **Tétel:** Páros gráf élgráfja perfekt.

Biz.: Ha páros gráf, akkor élgráfjának tetszőleges feszített részgráfja azonos egy alkalmas részgráfjának élgráfjával, azaz szintén egy páros gráf élgráfja. Elegendő tehát azt bizonyítani, hogy tetszőleges G páros gráfra .  
Mivel G háromszög-mentes, ezért ∀ klikkje G egy csúcsból induló éleinek felel meg, így . Kőnig páros gráfok élszínezéséről szóló tételének felhasználásával következik. ∎

(NEM KELL) **Tétel:** Páros gráf élgráfjának komplementere perfekt.

Biz.: Ha páros gráf, akkor feszített részgráfja nem más, mint , ahol a alkalmas részgráfja. Mivel páros, ezért elegendő azt igazolni, hogy tetszőleges gráfra (a másik irányú egyenlőtlenség triviális).  
A Kőnig-tétel alapján , ezért elegendő színnel kiszínezni -t. Legyen egy pontból álló lefogó ponthalmaz, és válasszunk ∀ éléhez -nek egy -beli végpontját. Ha ∀ élt a kiválasztott végpontnak megfelelően színezünk, akkor színt használunk, és az azonos színű élek páronként szomszédosak, azaz a nekik megfelelő pontok -ben függetlenek. Tehát ez csakugyan egy színnel történő színezése -nek.

## Erős perfekt gráf tétel

**Tétel:** (Erős perfekt gráf tétel) perfekt ⇔ sem , sem nem feszít (nem tart. fesz. részgr.-ként) min. 5-hosszú páratlan kört.

Bizonyítás: (**szükségesség**)  
A tétel állítása átfogalmazható: perfekt ⇔  nem tartalmaz feszített részgráfként vagy  –t ()

Állítás:   nem perfekt.

Bizonyítás:

:

nem perfekt ✖

🡪

Állítás:   nem perfekt.

Bizonyítás:  
Ebben csúcsból álló klikk, ha ∀ második pontot kiválasztjuk. De  csúcsú nincs, mert akkor az először és utoljára kiválasztott pont nem lenne szomszédos. ⇒   
Mivel ∀ színt legfeljebb kétszer használhatjuk ⇒  színnel csak csúcs lefesthető ⇒  . **Ebből és az előbbiből következik, hogy nem perfekt.**(Valójában szín elég is, tehát )

****

## Lovász tétele

Tétel: (Lovász gyenge perfekt gráf tétele)  perfekt ⇔  perfekt.

Megjegyzés:  
Elég csak az egyik oldalt bebizonyítani, mert „az állítás szimmetrikus”. Ha már bebizonyítottuk a perfekt ⇒ perfekt irányt, akkor jelöléssel a perfekt ⇒ perfekt átírható perfekt ⇒ alakra. (, illetve )

Bizonyítás: (e. f. g. t. segítségével) Ha perfekt ⇒ nem tartalmaz feszített részgráfként vagy  –t  
⇒⇒  nem tartalmaz feszített részgráfként vagy  –t ⇒  perfekt

## Intervallumgráfok perfektsége

I1

I2

I3

I4

I4

I3

I1

I2

Def.: Legyenek korlátos és zárt intervallumok a számegyenesen.

szomszédos -vel ⇔ ha ezek metszők (), tehát . Az így előálló gráfokat intervallumgráfoknak nevezzük.

Tétel: ∀ intervallumgráf **perfekt**.

Bizonyítás:  
Mivel az intervallumgráfok feszített részgráfjai is intervallumgráfok, elég azt belátni, hogy .  
Legyen , mivel , ezért elég azt belátni, hogy .  
Kezdjük el színezni az intervallumokat balról jobbra! A még színezetlen intervallumok közül mindig azt színezzük ki, amelyiknek baloldali végpontja a legbalrább van. Ha egy intervallumot -edik színnel kellene színezni, akkor ez azt jelenti, hogy ennek az intervallumnak a bal vége benne van már intervallumban, amik már elhasználták az színt. Így van intervallum, amelyek közül bármely kettő metszi egymást. ⇒ -ben méretű klikk. **ELLENTMONDÁS 🗲**

5.) Páros gráf fogalma, kapcsolat a páratlan körökkel. Párosítások páros gráfban, a javítóutak módszere, Kőnig, Hall és Frobenius tételei.

## Páros gráf fogalma

Def.: páros gráf, ha G két színnel színezhető, azaz ha .

Def.: páros gráf, ha felvágható két diszjunkt és részre úgy, hogy ∀ éle -beli csúcsot köt össze -belivel. (G ∀ élének egyik végpontja A-ban, másik B-ben van)

Jele:

**🡪 nem páros!**

Ellenpélda:

A

B

Példa:

## Kapcsolat a páratlan körökkel

Tétel: G páros ⇔ nincs benne páratlan hosszú kör.

Bizonyítás:   
⇒: Ha páros gráf és egy kör -ben, akkor pontjai felváltva vannak -ban és -ben.  
⇐: Ha ∀ köre páros hosszú, akkor megadhatjuk az , és halmazt. Válasszunk egy tetszőleges pontot.

Legyen ez első pontja, majd ∀ szomszédját tegyük -be, majd ∀ eddig -ben lévő pont ∀ szomszédját tegyük -ba stb. Ezt addig végezzük. amíg ∀ pontot el nem helyeztünk.  
Ez biztosan jó elosztás, hiszen, ha lenne pl. -ban két szomszédos pont, akkor lenne páratlan kör is. 🡪 🗲 **ELLENTMONDÁS.**Ha a gráf nem összefüggő, akkor az eljárást *komponensenként* hajtjuk végre.

## Párosítások páros gráfban, Kőnig tétele

Def.:  
Egy élhalmazt (részleges) párosításnak nevezünk, ha semelyik két élnek **nincs közös pontja** (semelyik két éle nem illeszkedik ugyanazon ponthoz). A párosítás tehát független élhalmazt jelent, a halmaz éleit független éleknek is nevezzük (páronként pontdiszjunktak). (Megjegyzés: ez a fogalom bármely gráfra értelmes, nem csak a páros gráfokra![[1]](#footnote-1))

Teljes párosítás: olyan () párosítás, ami a gráf ∀ pontját lefedi.

Bevezető/emlékeztető:  
: független élek maximális száma (legnagyobb független élhalmaz elemszáma): semelyik két élnek nincs közös pontja.  
 lefogó ponthalmaz, ha ∀ élének legalább egyik végpontját tartalmazza.  
: lefogó pontok minimális száma (legkisebb lefogó ponthalmaz elemszáma).  
 független ponthalmaz, ha nincs benne két szomszédos pont.  
: független pontok maximális száma (legnagyobb független ponthalmaz (semelyik 2 pont nincs közös élen) elemszáma).  
 lefogó élhalmaz, ha ∀ pontját lefogja.  
: lefogó élek minimális száma (legkisebb lefogó élhalmaz elemszáma).  
**.  
.**

Tétel: (Kőnig) Ha véges páros gráf ⇒  (Ha nincs -ben izolált pont, akkor is teljesül.)

Bizonyítás:

Állítás**:** véges gráf ⇒

Bizonyítás:

Legyen -nek egy max. párosítása (a javító utak módszerével már nem bővíthető). Ha egy min. méretű lefogó ponthalmaz, akkor lefogja ∀ élét is, de ∀ pontja max. egy párosításélt fog le. ⇒

1

1

1

1

B

t

A

s

1

1

1

1

∞1

∞1

∞1

Készítsük el -t az alábbiak szerint. Irányítsunk ∀ élét -ból -be, vegyünk fel egy-egy élt ∀ pontjából -be.

Adjunk ∀ élnek kapacitásokat: az -ből induló, illetve -be érkezőké legyen 1, az -ból -be futóké pedig **∞** (páratlan ).

Tekintsük a hálózatot, ahol **c** előbb definiált kapacitást jelenti. Ha -ben méretű párosítás ⇒ nagyságú egészfolyam. Tehát a max. egészfolyam értéke és az egészértékűségi lemma miatt a max. folyamérték is ugyanannyi. A **Ford-Fulkerson tétel** szerint kapacitású vágás. Definiálja ezt az -t tartalmazó ! -nek nem futhat éle -ból ()-be, mert akkor a vágás kapacitása végtelen volna (pontosabban min. ). Tehát egy lefogó ponthalmaz:

Tehát:  ✓

A

s

1

1

1

1

B

1

1

1

1

t

∞

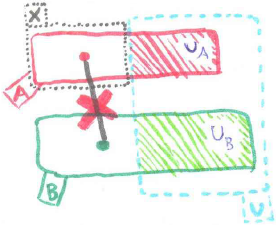
X

Összefoglalva:  
 **, ha G páros (Kőnig-tétel)** (azaz a legnagyobb független élhalmaznak ugyanannyi eleme van, mint a legkisebb lefogó ponthalmaznak) **, ha G páros, és G-ben nincs izolált pont (Kőnig-tétel)**

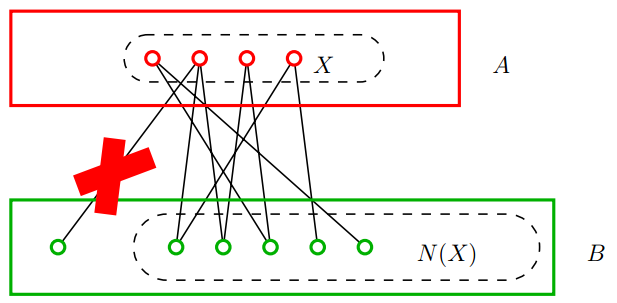
|  |  |  |  |
| --- | --- | --- | --- |
|  | független ~ max. | lefogó ~ min. | (Gallai) |
| élek |  |  | ~ + ~ = n, ha nincs izolált pont |
| pontok |  |  | ~ + ~ = n, ha nincs hurokél |

## Hall tétele

Def.: Egy gráfban jelöli az ponthalmaz szomszédainak halmazát (tehát azon pontok halmaza, amelyekhez van olyan él, melynek egyik végpontja , a másik pedig egy -beli pont).

****Tétel: (Hall) véges páros gráf, -t fedő párosítás  ha  ponthalmazra   (Hall-feltétel)

Bizonyítás:  
⇒: A **szükségesség** nyilvánvaló: ha -t fedő párosítás, akkor ∀ **A**-beli pontnak különböző párja van. (Tehát tetszőleges esetén az -beli elemek -beli párjai az egy méretű részhalmazát alkotják.)  
⇒: Tudjuk, hogy -ra . Azt kell igazolni, hogy . Legyen **U** minimális lefogó ponthalmaz, tehát méretű és , .  
Mivel **U** lefogja az -ból induló éleket ⇒ , azaz . Felhasználva a Kőnig-tételt adódik:



## Frobenius tétele

Tétel: (Frobenius) véges páros gráf, ∃ teljes párosítás ⇔ és -ponthalmazra .

Bizonyítás:  
⇒: Triviális.  
⇐: teljesül a Hall-feltétel  ⇒  -t fedő párosítás, de  ⇒ ez TP

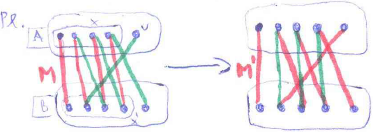
## A javítóutak módszere

Def.: páros gráf, párosítás.

Alternáló út: párosítatlan **A**-beliből indul és ∀ második éle M-beli.

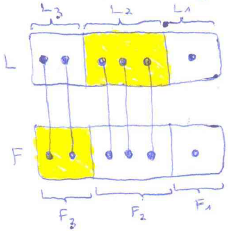
Javító út: olyan alternáló út, ami párosítatlan **B**-beliben ér véget.

Magyar módszer: (Hatékony algoritmus max. élszám párosítás megtalálására.)  
***I.*** független élek felvétele, amíg lehet.  
***II.*** javítóút keresése és e mentén a párosítás növelése, amíg lehet.

****A módszer általános megfogalmazására tegyük fel, hogy már van egy párosításunk, ami lefedi az halmazt, de még van olyan -beli pont, amit nem.  
 jelölje elemeinek -beli párját! Ha -nak van szomszédja -ben, akkor egy élet hozzávehetünk -hez, erről szólt az ***I.*** lépés.  
Ha -nak ∀ szomszédja -ben van és van egy -vel jelölt javító út, ami tehát -beliből indul, -beli pontban végződik és ∀ második éle -beli, akkor növelhetjük a párosítást: ( szimmetrikus különbsége -vel) vagyis -ből elhagyjuk a -ben szereplő éleket és hozzávesszük a többi -beli élet  
***III.*** ha nincs javító út ⇒ STOP

Tétel: , párosítás. Ha nincs javító út ⇒ max. párosítás.

Bizonyítás:  
Tfh. az algoritmus élű párosítást adott. Cél: pontú lefogó ponthalmazt találni! Ha találunk, akkor teljesül ez:   
: párosítatlan -beliek, : párosítatlan -beliek,  
: azon -beliek, amikhez -ből alternáló úton el lehet jutni (ekkor , mert ∄ javító út),  
: -beliek párjai szerint; : maradék -beliek



Állítás: -ből nem vezet él -ba

Bizonyítás: (indirekt)  
Tegyük fel, hogy...

1.) ∃ F1L1 él:

1 élű javítóút lenne ⭍

F1

L1

2.) ∃ F1L3 él: ⭍

L3

F1

L3 → rossz helyen van! L2-ben kéne lennie

1 élű altern. út

⭍

3.) ∃ F2L1 él:

F2: L2 lányok párjai

L2: vmelyik párosítatlan F1-ből elérhető alt. úton

🡪

L1 elérhető lenne F1-ből jav. úton ⭍

L2

F1

L1

F2

  🡪   lefogó ponthalmaz, és ez méretű!  ✓

4.) ∃ F2L3 él:

F2

L3

L3 → rossz helyen van! L2-ben kéne lennie

1 élű altern. út

⭍

Még egy kérdés.

Hogyan keressünk javítóutat?  
Induljunk ki egy -beli, által le nem fedett **u** pontból és mintha szélességi keresést végeznénk, menjünk el ennek összes szomszédjába, amiket jelöljön.  
Ezek nyilván mind -beli pontok és mindet lefedi . Miután lefedi a pontokat, jelölje ezek által meghatározott pontját.  
Most pontból kiinduló, nem -beli élen elérhető pontjába menjünk el.  
Látható, hogy ezek éppen azok a pontok, amelyekbe vezet -ból 3 élből álló alternáló út. Lényegében BFS-t alkalmazunk.

Másként[[2]](#footnote-2):  
A javítóutak módszere arra szolgál, hogy egy **párosításról** eldöntsük, hogy **maximális-e**, illetve ha nem, hogyan növeljük meg.  
Legyen egy adott **páros** gráf, melyben már meg van adva egy **M párosítás**. Rajzoljuk le a gráfot úgy, hogy **M éleit folytonos**, a gráf **többi élét pedig szaggatott vonallal** kötjük össze. Ha egy A-beli, az M párosítás által nem lefedett pontból elindulva, **felváltva szaggatott illetve folytonos éleken** át vezető úton **el tudunk jutni egy B-beli, M által le nem fedett pontba**, akkor találtunk javítóutat, és a párosítás növelhető úgy, hogy az úton lévő **szaggatott éleket folytonos, a folytonosakat pedig szaggatott élekre** cseréljük. Így, mivel a javító út első és utolsó éle is szaggatott volt, növeltük a párosítást. Ha **nem találunk javítóutat**, akkor a megadott párosítás maximális.

6.) Párosítások tetszőleges gráfban, Tutte tétele (csak a szükségesség bizonyításával). Gallai tételei.

ld. még előző tételt!!

|  |  |  |
| --- | --- | --- |
|  | **ftlen ~ max.** | **lef. ~ min.** |
| **élek** |  |  |
| **pontok** |  |  |

**Def.:** független élhalmaz: olyan élhalmaz, hogy semelyik két élének nincs közös pontja. (Diszjunkt.)  
: **független élek max. száma** -ben (legnagyobb független élhalmaz elemszáma): semelyik két élnek nincs közös pontja.  
 lefogó ponthalmaz, ha élének legalább egyik végpontját tartalmazza (***G*** éle tartalmaz -beli csúcsot)  
: lefogó pontok min. száma (legkisebb lefogó ponthalmaz elemszáma)  
 független ponthalmaz, ha nincs benne 2 szomszédos pont (az -beli csúcsok nem szomszédok)  
: független pontok max. száma (legnagyobb független ponthalmaz (semelyik 2 pont nincs közös élen) elemszáma).  
 lefogó élhalmaz, ha pontját lefogja (***G*** pontjára illeszkedik -beli él)  
: lefogó élek min. száma (legkisebb lefogó élhalmaz elemszáma).

Tétel: gráfra.

biz.: legyen M egy max. méretű ftlen élhalmaz. Mivel pusztán M éleinek lefogásához már pontra van szükség, ezért . ∎  
pl.: .

Tétel: gráfra. (biz. mint előző)

Tétel: (Kőnig) Ha véges páros gráf ⇒  (Ha nincs -ben izolált pont, akkor is teljesül.)

Bizonyítás:

Állítás**:** véges gráf ⇒

Bizonyítás:

Legyen -nek egy max. párosítása (a javító utak módszerével már nem bővíthető). Ha egy min. méretű lefogó ponthalmaz, akkor lefogja ∀ élét is, de ∀ pontja max. egy párosításélt fog le. ⇒

1

1

1

1

B

t

A

s

1

1

1

1

∞1

∞1

∞1

Készítsük el -t az alábbiak szerint. Irányítsunk ∀ élét -ból -be, vegyünk fel egy-egy élt ∀ pontjából -be.

Adjunk ∀ élnek kapacitásokat: az -ből induló, illetve -be érkezőké legyen 1, az -ból -be futóké pedig **∞** (páratlan ).

Tekintsük a hálózatot, ahol **c** előbb definiált kapacitást jelenti. Ha -ben méretű párosítás ⇒ nagyságú egészfolyam. Tehát a max. egészfolyam értéke és az egészértékűségi lemma miatt a max. folyamérték is ugyanannyi. A **Ford-Fulkerson tétel** szerint kapacitású vágás. Definiálja ezt az -t tartalmazó ! -nek nem futhat éle -ból ()-be, mert akkor a vágás kapacitása végtelen volna (pontosabban min. ). Tehát egy lefogó ponthalmaz:

Tehát:  ✓

A

s

1

1

1

1

B

1

1

1

1

t

∞

X

## Párosítások tetszőleges gráfban, **Tutte tétele**

Def.: -val jelöljük a H gráf páratlan sok pontot tartalmazó komponenseinek számát (röviden: páratlan komponensek).

Tétel: (Tutte) *G*-ben  **teljes párosítás**  ha -re   (: -ből -beli csúcsok elhagyása)  
🡪 Akárhogy hagyunk el a gráfból néhány pontot, a maradékban a páratlan komponensek száma ennél nem lehet több.  
Másként: ha a G véges gráfnak létezik k olyan pontja, amelyek elhagyása után több, mint k páratlan komponens keletkezik (azaz valamely -re), akkor G-nek **NINCS** teljes párosítása.

Bizonyítás: (***szükségesség***)

Ha elhagyjuk a gráfból -et, akkor az eredeti gráfban a páratlan komponensek mindegyikéből legalább egy párosításbeli él indul ki, és ezek az élek csak egy-egy különböző -beli pontban mehetnek. Tehát a  . ✓

X

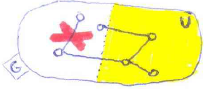
**ptlan komponensek**

**páros komponensek**

## Gallai tételei

Tétel: (Gallai) *G* tetszőleges, n csúcsú  
1.) , ha G hurokélmentes  
2.) , ha G-ben ∄ izolált pont.

Bizonyítás:

**1.)** Könnyen belátható, hogy pontosan akkor lefogó ponthalmaz, ha független ponthalmaz. Az állítás innen közvetlenül adódik.

**2.) *G***-nek diszjunkt éle, ezek két pontot fognak le. A maradék db pont mindegyike lefogható egy-egy új éllel (mert nincs izolált pont) ⇒ éllel ∀ pont lefogható ⇒ .

Ha F egy min. mértékű lefogó élhalmaz, akkor körmentes és nem tartalmaz három hosszú utat sem. Tehát diszjunkt csillagok uniója. (A csillagok összefüggő gráf, amelyek legfeljebb egy híján ∀ pont foka 1.) Ha a min. lefedő élhalmazban csillag van, akkor a halmaz élet tartalmaz, hiszen komponensű erdőből van szó: .  
Másrészt a halmaz tartalmaz diszjunkt élt: .  
Ehhez hozzáadjuk az előző egyenlőséget . Tehát

Összefoglalva:  
 **, ha G páros (Kőnig-tétel)** (azaz a legnagyobb független élhalmaznak ugyanannyi eleme van, mint a legkisebb lefogó ponthalmaznak) **, ha G páros, és G-ben nincs izolált pont (Kőnig-tétel)**

|  |  |  |  |
| --- | --- | --- | --- |
|  | független ~ max. | lefogó ~ min. | (Gallai) |
| élek |  |  | ~ + ~ = n, ha nincs izolált pont |
| pontok |  |  | ~ + ~ = n, ha nincs hurokél |

7.) Hálózat, hálózati folyam és vágás fogalma, folyam értéke, vágás kapacitása. Algoritmus a maximális folyam és a minimális vágás megkeresésére, Ford-Fulkerson tétel, Edmonds-Karp tétel (biz. nélkül), egészértékűségi lemma. A folyamprobléma általánosításai.

## **Hálózat**

Def.: Hálózatnak nevezünk egy olyan négyest, amelyben egy irányított gráf, aminek és különböző csúcsai, továbbá minden élét jellemzi egy nemnegatív szám, az él kapacitása. Az és különböző csúcsokat termelőnek és fogyasztónak hívjuk.

Röviden: ha irányított gráf, ,

Példa:

t

(3)

(4)

(1)

(4)

(2)

(3)

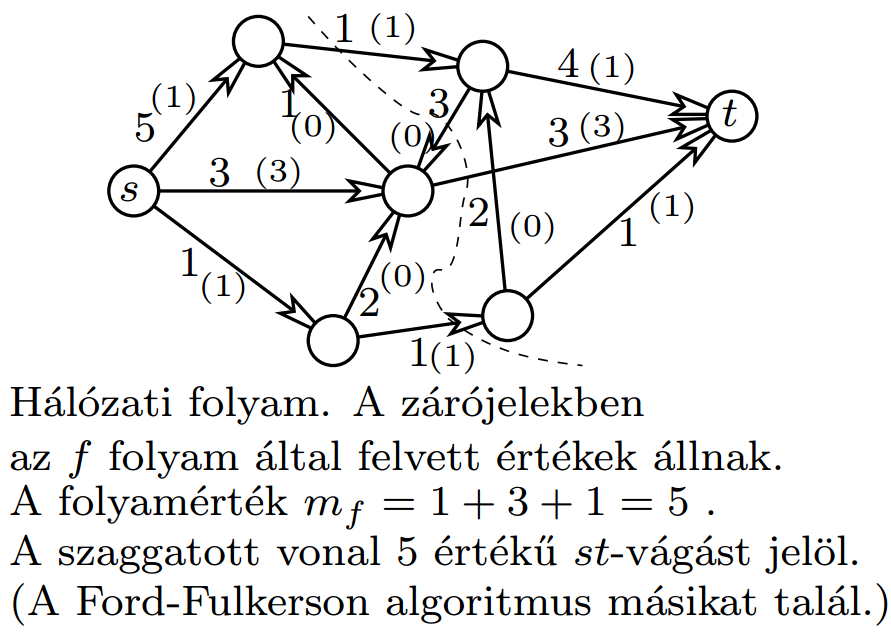
(4)

s

## Hálózati folyam

**Def.**: A hálózatban folyamnak mondunk egy olyan függvényt, amely éléhez egy számot rendel (pl. poz. valós számokat: ), amire teljesül:  
1.) teljesül élre -ben (kapacitás-feltétel: a folyam minden élen legfeljebb kapacitásnyi lehet), valamint  
2.) () áll   
, csúcsára (). Ez a Kirchhoff-szabály (csomóponti törvény; elektromos hálózatoknál is használatos): minden, -től és -től különböző, csúcsra csúcsra a **befolyó folyam összmennyisége azonos a kifolyó összfolyammal**, tehát egyetlen csúcsban sem keletkezik vagy tűnik el folyadék.

Példa:  fvérték(kapacitás) alakban:



0(3)

1(4)

1(1)

0(4)

1(2)

1(1)

0(4)

s

t

## Folyam értéke

**Def.:** folyam értéke ( folyam nagysága) az a nettó folyammennyiség, ami -ből kifolyik:   
(le kell vonni azt, ami s-be érkezik, mert nem kizárható, hogy fog ide befolyni (bár általában nem ez a helyzet, hiszen onnan minél többet akarunk kijuttatni), de nem zárhatjuk ki ezt a lehetőséget sem., ezért az -t elhagyó összfolyammennyiség kiszámításához le kell vonni azt, ami s-be érkezik)  
 vagy  
,   
Egy élet egy folyamban telítettnek hívunk, ha , és telítetlennek, ha .

## Vágás

**Def.:** Legyen csúcsainak -t tartalmazó, de -től diszjunkt részhalmaza (, ).  
Az  és  között futó élek halmazát a hálózat egy st-vágásának nevezzük (jele: ).

## Vágás kapacitása

**Def.:** vágás kapacitása, vagyis *C értéke*:   
Az által meghatározott -vágás kapacitása az -ből -be futó (előremutató) élek kapacitásösszege, azaz .  
Az által meghatározott st-vágás kapacitása **felső korlát a lehetséges folyamnagyságra**. Sőt, tetszőleges folyam folyamnagysága meghatározható úgy, hogy az -ből –be futó éleken haladó összfolyam-mennyiségből levonjuk a -ből -be továbbított folyammennyiséget.

, továbbá

.

## Algoritmus a maximális folyam és a minimális vágás megkeresésére

**Állítás:** Ha egy hálózatban folyam, C vágás ⇒ ,  
tehát

A feladat tehát a **maximális értékű folyam meghatározása**.

**Algoritmus:**

1. Kiindulunk egy tetszőleges folyamból (Pl.: )
2. Javítás (amíg lehet) ⇒  nő
3. Ha nincs több javítás ⇒ STOP

A javítást egy ún. segédgráffal tudjuk elvégezni.

**Def.:** a hálózat f folyamához tartozó segédgráf:  
, tehát segédgráf csúcsai megegyeznek csúcsaival.  
, azaz ha -ben az él értéke kevesebb, mint az él kapacitása, akkor -ben is fusson él -ből -ba., azaz ha -ben az él értéke nagyobb, mint 0, akkor -ben fusson „**visszaél**” -ból -be.**Javítóút**: -ben **irányított út -ből -be**.  
Ha   javítóút, akkor ***növelhetjük* a folyam értékét**:  
, megnézzük, az eredeti gráfban mennyi a minimális érték, amennyivel lehet növelni a javítóút élein átmenő folyam értékét.  
, tehát „előreél” esetén növelni, „visszaél” esetén csökkenteni kell az adott él értékét. Így meg is növeljük a folyam értékét, majd újabb javítóutat keresünk.

Fontos kiegészítés az „algoritmus” III. pontjához:  
Ha van egy olyan irányított út -ből -be, amelynek éle telítetlen (vagyis  ), akkor ezen út mentén a folyam értékét ∀ élen megnövelhetjük annyival, hogy az egyik él telített legyen. Ha nincs erre lehetőség, akkor ezután alkalmazzuk a segédgráfos módszert.  
Amennyiben nincs további javítóút, megtaláltuk az -ből -be futó maximális folyamot (ld. még később). A minimális vágás pedig azon pontok halmaza, melyek az utolsó felrajzolt segédgráfon még elérhetőek -ből.

Állítás: a segédgráfos javítás után folyam marad.

Bizonyítás:

Az biztos, hogy az egyik élet sem „terhelhettük túl”, mert direkt így lett megválasztva a minimumfüggvényes előállítása által; és a csomóponti törvény is igaz marad:

(1)

(2)

v

(2)

(1)

v

(2)

(2)

v

(1)

(1)

v

:

+d

+d

v

+d

-d

v

-d

+d

v

-d

-d

v

:

Tétel: Ha nincs javítóút -ben ⇔  maximális folyam

Bizonyítás:  
Tfh. az algoritmus értékű folyamot adott: .  
Cél: mutassunk értékű vágást.  
 azon pontok halmaza, ahová -ben -ből vezet irányított út ⇒

f(e)=c(e), mert különben  **⭍**  **ELLENTMONDÁS**

f(e)=0, mert különben   **⭍** **ELLENTMONDÁS**

X

Hf

e

e

t

s

A fentiekből következik:

## **Ford-Fulkerson-tétel**

Tétel: (Ford-Fulkerson)  
, vagyis a maximális folyamnagyság egyenlő a minimális vágás kapacitásával.  
(, max-flow=min-cut)  
Másként: ha véges hálózat, egy f folyam és egy részhalmaz úgy, hogy az folyamnagyság egyenlő az által definiált -vágás kapacitásával.

Bizonyítás:  
A maximális folyam nyilván nem lehet nagyobb a minimális vágásnál (), hiszen ha ∀ előremutató él telített, a visszafelé mutatókon pedig a folyam értéke, akkor ezen a vágáson nem folyhat át több. Az előző tételben pedig láttuk, hogyha létezik egy maximális folyam, akkor van ilyen értékű vágás. ✓

## **Edmonds-Karp tétel**

Tétel: (Edmonds-Karp)  
Ha Hf-ben mindig a legrövidebb javítóutat választjuk, akkor az algoritmus véges sok lépésben leáll és polinomiális lépésszámú.

## **Egészértékűségi lemma**

Tétel: (Egészértékűségi lemma): Ha élre egész (kapacitások egész számok) ⇒ olyan max. folyam, amire élre egész.

Bizonyítás: Az algoritmus nem lép ki -ből (csupa -ból indítva).

## **A folyamprobléma általánosításai**

1. **több termelő/fogyasztó is van**

megoldás

    s1      t1

 :               :

 :               :

     sk      tl

    s1     t1

 :  s2      t2  :

 :                :

     sk      tl

ss

t

ezek kapacitása legyen ∞

Felveszünk egy „szupertermelőt”(S)/„szuperfogyasztót”(T), amelyeket összekötünk a termelőkkel/fogyasztókkal végtelen kapacitású éleken. Az így kapott gráfban keresünk maximális folyamot (S-ből T-be), majd ha megtaláltuk, letöröljük a két pontot.

1. **irányítatlan élek is vannak**

megoldás

          u

   s      (c)  t

        v

     u

 s (c)   (c)    t

        v

Az irányítatlan él helyett felveszünk két irányított élet azonos kapacitással, az egyik él az egyik, a másik a másik irányba mutat. Abban az esetben, ha a folyam meghatározásakor mindkét helyettesítő élen 0-nál nagyobb a folyamérték, a két él folyamértékét ki kell vonni egymásból, és az lesz az irányítatlan él értéke, míg az iránya a két helyettesítő élből a nagyobb folyamértékűnek az irányával egyezik meg.

1. **kapacitással rendelkező csúcsok**

megoldás

         (b1)       (k1)

          (c)

(b2)

v

  (b3)                    (k2)

      (b1)         (k1)

(b2) (c)

v1 v2  
  (b3)                     (k2)

A probléma azt jelenti, hogy az adott pontba belépő élek kapacitásának összege nem lehet nagyobb a pont kapacitásánál. Ez is visszavezethető hagyományos hálózatra, ha a kapacitással rendelkező pontot két másik ponttal helyettesítjük, amiket egy kapacitású él köt össze. A két új pontból az egyikbe futnak a -be bejövő élek, a másikból futnak ki a -ből kimenő élek.

8.) Menger pontpárok közötti diszjunkt utakra vonatkozó tételei. Többszörös összefüggőség és élösszefüggőség fogalma, Menger ezekre vonatkozó tételei.

Def.: a irányított/irányítatlan gráf pontjából pontjába futó és útjait éldiszjunktaknak (élidegennek) nevezzük, ha , vagyis ha nincs közös élük.

Def.: a irányított/irányítatlan gráf pontjából pontjába futó és útjait pontdiszjunktaknak (pontidegennek/függetlennek) nevezzük, ha , vagyis ha nincs közös csúcsuk, a kezdő- és végpontjukat leszámítva.

Def.: a irányított/irányítatlan gráf **ponthalmaza** (ill. **élhalmaza**) lefog -utat, ha a (ill. ) gráfban -ból -be (irányított) út.

## Menger pontpárok közötti diszjunkt utakra vonatkozó tételei

### **Az él-összefüggőségi változat irányított gráfokban**

Tétel: (Menger I.)  
 *irányított* gráf, és a gráf különböző csúcsai. Az -ből t-be menő, (páronként) éldiszjunkt irányított -utak maximális száma = az -utakat lefogó élek minimális számával.

Bizonyítás:  
Ha ∃ **G**-ben db ilyen irányított út, akkor az utakat lefogó élek száma nyilvánvalóan legalább , tehát .  
Tfh. az utakat lefogó élek minimális száma. Legyen ∀ él kapacitása 1. Az így kapott hálózatban a minimális vágás értéke legalább . Ekkor a Ford-Fulkerson tétel értelmében a maximális folyam is értékű.  
Van olyan maximális folyam, melyben ∀ élen a folyamérték 0 vagy 1 (egészértékűségi lemma miatt). Lássuk be, hogy **G**-ben éldiszjunkt irányított út! Egy ilyen út mindenképpen van, különben nem lehetne a folyam értéke. Az ebben az útban szereplő élek kapacitását változtassuk 0-ra, így a folyamérték lesz. Ekkor viszont innen kell lennie útnak, és ennek nyilván nincs közös éle az előbbi úttal. Ezt -szor végrehajtva éldiszjunkt irányított utat kapunk.

### **Az él-összefüggőségi változat irányítatlan gráfokban**

Tétel: (Menger II.)  
G *irányítatlan* gráf, .  
Az -ből -be menő (páronként) *éldiszjunkt irányítatlan -utak maximális száma* = az -utakat *lefogó élek minimális számá*val.

u v

s t

Az összes ilyen megszüntetése után az utak ősképei adnak G-ben k db st páronként éld. irtl. utat ✓

G

hogy alkalmaz­has­suk Menger I-et

u  
s t  
  
 v

G’

u  
s t  
  
 v

előfordulhat ilyen probléma...

megoldás

Bizonyítás**:**  
Készítsük el a -t -ből úgy, hogy ∀ élét irányítjuk oda és vissza.  
Ha -ben van él, melyek lefognak irányított éldiszjunkt utat ⇒ ezek ősei lefogják az utakat -ben.

### **A csúcs-összefüggőségi változat irányított/irányítatlan gráfokban**

Tétel: (Menger III./IV.)  
G irányított/irányítatlan gráf, . Az (páronként) pontdiszjunkt irányított/irányítatlan utak maximális száma = az utakat lefogó(, irányított esetben -től és -től különböző) pontok minimális számával.

Bizonyítás:

M.III.:  
  
Ha -ben van éldiszjunkt út ⇒ -ben van db pontdiszjunkt út.  
*Probléma*: ha -ben van  db él, melyek lefogják az utakat, akkor ezek -ben pontok vagy élek?  
*Megoldás*: válasszunk  db piros lefogó élt! ⇒ ezek képei -ben  db lefogó pont.  ✓

s v1 v2 t

ev

s v t

hogy alkalmazhassuk M. I.-et

M.IV:  
     ✓

u

v

u

v

M. I. alkalm.

## Többszörös összefüggőség és élösszefüggőség fogalma, Menger ezekre vonatkozó tételei

**Def:**  
 -szorosan élösszefüggő (-élösszefüggő), ha bárhogyan legfeljebb élét elhagyva összefüggő marad.  
 -szorosan pontösszefüggő (-összefüggő) ha bárhogyan legfeljebb pontját elhagyva összefüggő marad és legalább pontja van.

-élösszefüggő ⇒ -élösszefüggő és  
-(pont)összefüggő ⇒ -(pont)összefüggő.

(Ha külön nem emeljük ki, hogy pont- vagy élösszefüggőségről beszélünk, akkor az alapértelmezett a pontösszefüggőség.)

Állítás: -összefüggő ⇒ -élösszefüggő.

*Ellenpélda*:  
nem 2-öf., de 100-élöf.:

K100

K100

Tétel: (Menger V., VI.)  
M. V.:  G -élösszefüggő ⇔ bármely 2 pont között ∃ db páronként éldiszjunkt út.  
M. VI.: G -(pont)összefüggő ⇔ bármely 2 pont között ∃ db páronként pontdiszjunkt út és pontja van.

Bizonyítás:  
⇐: (M. V., M. VI.): él/pont elhagyásakor tetszőleges ből be van út, mert volt db éldiszjunkt/pontdiszjunkt út, törlése csak et ronthatott el.  
⇒: (M. V.): Tfh. ,között nincs db éldiszjunkt út ⇒irányítatlan utak maximális száma ⇒utakat lefogó élek minimális száma ⇒ le lehet fogni éllel azutakat ⇒ élt törölve nincsút!  
         🡪 *ELLENTMONDÁS* ⭍  
⇒: (M. VI..): Tfh. ből be legfeljebb pontdiszjunkt út van!  
Hanem szomszédos, akkor M. IV. miatt azutak lefoghatók maximum ponttal. Ezek elhagyásakor G szétesne.  
         🡪 *ELLENTMONDÁS* ⭍  
Haszomszédos, akkorél törlése után keletkező G’ gráf legfeljebb pontdiszjunktutat tartalmaz, tehát M. IV. szerint létezik pontja, aminek elhagyásakor szétesik. A szétesett gráfban ismét összekötve azéspontokat egy legalább 3-pontú gráfot kapunk (mert G-nek minimum pontja volt), mely azél törlésétől szétesik. De ekkor azél helyettvagyvalamelyike is törölhető, hogy a gráf szétessen. Ismét azt kaptuk, hogy G legfeljebb alkalmas pont törlésével szétesik, ami a szoros összefüggőségnek ELLENTMOND.

Tétel: (Dirac) Ha -**összefüggő** és ⇒ bármely pontján keresztül található kör -ben.

9.) Gráfok szomszédossági mátrixa, a szomszédossági mátrix hatványainak jelentése. Irányított gráf illeszkedési mátrixa.

## Gráfok szomszédossági mátrixa

Def**.:** A gráf szomszédossági mátrixa (adjacenciamátrixa) az a méretű mátrix, aminek pozícióján az és közti élek száma áll ( esetén a hurokélek számának kétszerese). A gráf véges, ha és is véges halmazok.  
Megjegyzés:  
Ha nincs hurokél a gráfban, akkor a főátló csupa 0. Ha a gráf egyszerű gráf (nincsenek többszörös élek), akkor a mx.-ban csak 0 és 1 szerepelhet.  
Ha G irányítatlan, akkor szimmetrikus a főátlóra: (uaz, mint a transzponáltja, vagyis főátlóra történő tükrözése, vagyis ).  
Ha irányított (, jelentése: az csúcsból csúcsba hány él mutat), pontjának ki-/befoka a mátrix sorában/oszlopában lévő elemek összege. Ha a gráfban vannak többszörös élek, akkor is lehet a mx. csupa 0, ill. 1. A főátlóra való szimmetria itt már nem feltétlenül igaz (lehet olyan, hogy , ha -ből nem vezet -be él, de -ből -be igen, vagy fordítva).

Példa:

1

4

2

3

## A szomszédossági mátrix hatványainak jelentése

Tétel: Ha *irányított* gráf, akkor az mátrix pozíciójában álló eleme az **-ből -be vezető élű séták** ( hosszú élsorozatok) száma (út, amely ismétlést tartalmazhat).

Bizonyítás: Teljes indukcióval:  
-re *A* definíciójából nyilvánvaló. Tfh. -ra már bebizonyítottuk az állítást.  
Az -ből -be vezető élű séták száma:

Következmény:  
🡆 egyszerű, irányítatlan gráf ⇒ : a közös szomszédok számát adja. Másképp: megadja, hányféleképpen juthatunk el az egyik csúcsról a másikra 2 lépésben. A főátló esetén a két csúcs azonos, tehát az érték pont a fokszámmal egyenlő. (Tehát -re .)  
🡆A hurokélmentes gráfoknál főátlóbeli elemeinek összege a gráfban található 3-hosszú körök (háromszögek) számának 6-szorosa.

(NEM KELL) **Tétel:** Ha irányítatlan gráf és az legnagyobb sajátértéke, akkor a   ; továbbá    reguláris gráfokban.

Bizonyítás:  
Legyen egy -hez tartozó sajátvektor, és -adik eleme a legnagyobb.  
Mivel , ezért (esetleg a sv.-ra áttérve) feltehető, hogy pozitív.  
Ekkor:  
    ✓  
Ha G Δ-reguláris, akkor az egységvektor a Δ sajátértékhez tartozó sajátvektor, mert a fenti egyenlőtlenségek egyenlőséggel teljesülnek.  ✓

## Irányított gráf illeszkedési mátrixa

**Def**: A *irányított* gráf illeszkedési mátrixa (incidenciamátrixa) , amire:  
ha *irányítatlan*, akkor:

Példa:

1

2

3

*3*

*4*

*1*

*2*

(NEM KELL) Tétel: A  pontú irányított hurokél mentes komponensű gráfnál .

Bizonyítás:  
Ha , akkor komponensenként sorolva fel a pontokat és éleket, blokkdiagonális szerkezetű lesz.  
Elég tehát egy pontú komponensre belátni, hogy a neki megfelelő blokk rangja .  
Mivel a blokk sorból áll és összege a -t adja, a rang .  
Legyen egy pontú, élű feszítőfa ebben a komponensben.  
Legyen egy elsőfokú pont -ben és a hozzáilleszkedő él.  
Legyen egy elsőfokú pont -ben és a hozzáilleszkedő él, stb.  
Ha a blokk sorait , , sorrendben soroljuk fel, oszlopait felsorolásával kezdjük, akkor egy méretű részmátrixot kapunk, amelyből az utolsó sor elhagyásával egy alsóháromszög mátrixot kapunk, melynek főátlóbeli elemei értékűek ⇒ találtunk lineárisan független oszlopot.

Egy példa a blokkdiagonális szerkezetű mátrixra:

**Tétel**: Az pontú öf. hurokélmentes ir. G gráf illeszkedési mátrixában oszlop akkor és csak akkor lineárisan független, ha a megfelelő él G-nek egy fáját alkotja.

Bizonyítás:  
Az előző tétel bizonyításánál láttuk, hogyha az élek fát alkotnak, akkor a megfelelő oszlopvektorok lineárisan függetlenek. Megmutatjuk a fordítottját: ha néhány él kört alkot ⇒ nekik megfelelő oszlopvektorok lineárisan összefüggőek. Csakugyan ezek az oszlopok és a kört alkotó pontoknak megfelelő sorok alkalmas sor-, ill. oszloppermutációk után a baloldali alakú mátrixot alkotják.  
Képezzük azt a lineáris kombinációt, ahol az első oszlop lineáris kombinációja **a**, a másodiké **b**, stb. ⇒ összegük **0**-t adja.

(NEM KELL) Def: redukált illeszkedési mátrix: az eredeti ill. mx. egy sorának elhagyásával kapott ill. mx. Jele:

(NEM KELL) Tétel: Az pontú öf. ir. gráfnál = feszítőfák száma.

Bizonyítás:   
Felhasználjuk a Cauchy—Binet -tételt:  
,  
ahol M’-t/N’-t úgy, ahol M’-t/N’-t úgy kapjuk, hogy az eredetiből elhagyunk oszlopot/sort, hogy méretű mx-ot kapjunk.

b

b

a

a

a

a

MN

M

N

Pl.:

Ezek után a tétel állítása nyilvánvaló: B0-ból mindenképp kiválasztva oszlopot, épp a fának megfelelő részmátrixok determinánsa lesz ≠ 0, és egy ilyen determináns értéke ±1, tehát a négyzete 1.

Példa: pontú teljes gráf

A tétel felhasználásához nem szükséges a B0 mátrixot felírnunk. A elemeit az alábbi képlet előállítja:

(utsó végösszeg):   🡪  újabb bizonyítást kaptunk Cayley tételére  ✓

10.) Oszthatóság, felbonthatatlan és prímtulajdonságú számok, ezek kapcsolata (bizonyítás csak az egyik irányban), a számelmélet alaptétele. Osztók száma. Prímek száma, hézag a szom­szédos prímek között, nagyságrendje (biz. nélkül). Kongruencia fogalma, alapműveletek kongruenciákkal

## Oszthatóság, felbonthatatlan és prímtulajdonságú számok, ezek kapcsolata

Def.: osztója -nek, ha , melyre . Jele: . (Pongyolán: „ megvan -ben valahányszor”.)  
 felbonthatatlan (), ha   🡪   vagy , (p felbonthatatlan, ha minden olyan esetben, amikor előáll két egész szám szorzataként, a szorzatnak legalább az egyik tényezőjének abszolútértéke 1. Csak triviális osztói vannak.)  
 prímszám (), ha 🡪 vagy (minden olyan esetben amikor p két egész szám szorzatának osztója, akkor p a szorzat legalább egyik tényezőjének is osztója. Vagy: p osztója ab szorzatnak, és egyben p osztója a-nak vagy b-nek)

Példa: a nem prím, mert .  
Felbonthatatlan: , , , nem az: ,

Tétel: prím felbonthatatlan

Bizonyítás:  
prím, ha  
1.) és a ✓  
2.) és  ✓

## A számelmélet alaptétele

Tétel: (számelmélet alaptétele) természetes számok körében: minden egész szám (, 1-nél nagyobb természetes szám) a sorrendtől és előjelektől eltekintve egyértelműen felbontható felbonthatatlanok sorozatára.  
egész számok körében: ha egy egész számra , akkor előáll felbonthatatlan számok szorzataként, és a ilyen előállításai csak a tényezők sorrendjében és előjeleiben különbözhetnek.  
Pl.:

Bizonyítás:  
(felbonthatóság)  
(egyértelműség)  
Tfh. két különböző módon felbontható:  
 prím;   
Pl.: prím, nem lehet 1! ⭍  
*vagy*  
 ez azt jelenti, hogy   
🡪visszavezettük a problémát egy egyszerűbb esetre:  
🡪erre ismét alkalmazzuk az algoritmust, egészen addig, amíg mindegyiknél ki nem derül, hogy egyenlőek. ✓

Következmény: prímtényezős felbontás / kanonikus alak:   
kan. alakban kül. pozitív felbonthatatlanok, ; ált.   
Figyeljük meg, hogy jóllehet sok prímszám van, csak véges sok kitevő lesz pozitív, tehát csak véges sok 1-től különböző szám szorzatát képezzük.  
(Megj.: prímszám kanonikus alakja megegyezik önmagával (önmaga első hatványával).)

## Osztók száma

Osztók száma: jele:   
pl.:   
, ha ,   
vagy .  
általánosan: ,         
Tehát: a szám kanonikus alakjában szereplő hatványkitevők eggyel növelt értékeinek szorzata megaja a szám osztóinak számát.

Osztók összege: jele: (csak a pozitív osztókat vesszük figyelembe)

pl.: ,   
   
általánosan: ,

## Prímek száma

Tétel: ∞ sok prímszám (Euklidész).

Biz.: (indirekt) tfh. véges sok van: 🡪 nagyobb 🡪 A-nak van prímosztója, de A  –nel osztva 1 maradékot ad. ⭍  
Másképp: elegendő megmutatni, hogy -re ∃ -nél nagyobb prím. Mivel az számok mindegyikével osztható az számok mindegyikéhez relatív prím, tehát nem osztható egyetlen -nél kisebb prímmel sem. kan. alakjában csak -nél nagyobb prímek fordulnak elő.  
  
Vagy: legyen a prímszámok darabszáma m, tfh. véges. Szorozzuk össze mind az m db prímet, majd adjunk hozzá 1-et. A kapott szám egyik prímmel sem osztható a halmazunkból, hiszen bármelyikkel osztva 1-es maradékot kapunk, az 1 pedig egy prímmel sem osztható. A szorzat tehát vagy maga is prím, vagy osztható egy olyan számmal, ami nincs benne a fenti véges halmazban. (Mert minden 1-nél nagyobb egésznek van prímosztója.) Mindkét esetben legalább m+1 darab prímszám létezik. Az érvelés viszont nem függ m értékétől, így (m+1)-re is ugyanúgy felírható. Így tehát a prímszámok darabszáma nagyobb bármely adott véges számnál.

## Hézag a szom­szédos prímek között

Tétel: -re  szomszédos prímek, amelyekre .  
Tetsz. hosszú sorozat képezhető szomszédos összetett számokból 🡪 bármely -re olyan , melyre az számok mindegyike összetett.

Biz.: azaz: db szomszédos összetett szám  
  
 db, mindegyik összetett  ✓  
Legyen . 🡪 tetsz. esetén 🡪 számok mindegyike összetett.

p

q

N

Hézag mérete szomszédos számok között: bármilyen hosszúságú intervallum, ami nem tartalmaz prímszámot. Vagy: két „szomszédos” prímszám között tetszőleges lehet a távolság (hézag).  
Másképp: tetszőleges n-re található n darab egymást követő összetett szám. Adott -re például nyilván osztható -vel, osztható -mal, és így tovább -ig, ami osztható -gyel. Ezért ***n*** darab egymást követő szám.

## nagyságrendje

Def.: : -től -ig a prímek száma ( pozitív), pl.

Tétel: „nagy prímszámtétel”: a prímszámok eloszlását írja le (eredetileg Gauss vette észre, később Csebisev bizonyította).  
; (: természetes logaritmus), a  jelölés azt jelenti, hogy a két oldal hányadosa 1-hez tart, ha végtelenhez tart (aszimptotikusan egyenlőek)  
tehát jelentése:

Tétel: (Dirichlet - prímek számtani sorozatokban) ha (a, b)=1 🡪 ∞ sok ak+b alakú prím van  
pl.: ∞ sok 4k+1, 4k+3, 10k+1, 10k+3, 10k+7, 10k+9 alakú prím van

Def.: LNKO: .  
 és LNKO-ja a legnagyobb olyan szám, amely osztója -nak és -nek is.  
Jel.: . Pl.: , , , de .  
relatív prím:

Def.: LKKT: legkisebb közös többszöröse az a legkisebb szám, melyre és áll.  
Jel.: . Pl.: , , .

Def.: Csebisev-tétel: tetszőleges pozitív egészre , amelyre . Bármely 0-tól és 1-től különböző szám és a kétszerese közt van prímszám.

## Kongruencia fogalma, alapműveletek kongruenciákkal

Def.: [a kongruens b-vel modulo m]; ha és -mel osztva ugyanazt a maradékot adja.  
 alakú.  
   
Pl.:

Tétel:

Biz.:

1. Speciális esete:
2. , összeszervezzük őket (mert (2)-t már bizonyítottuk)

Tétel:  
ha és és (tehát -vel osztásnál -et leosztjuk és LNKO-jával)

Biz.:

**11.) Lineáris kongruenciák: a megoldhatóság szükséges és elégséges feltétele, a megoldások száma. Euklideszi algoritmus, ennek alkalmazása lineáris kongruenciák megoldására is. Wilson tétele**

## Lineáris kongruenciák: a megoldhatóság szükséges és elégséges feltétele, a megoldások száma

Def.: lineáris kongruencia: , adottak: ; kérdés:

Pl.: 6,

Tétel: Az ,  lineáris kongruencia megoldható    
A kongruencia megoldáshalmaza darab maradékosztály modulo m.

Biz.: Legyen   
Ha  , megoldható ⇒ és miatt   
Elégségesség bizonyítása: tfh. . A kongruenciát -vel végigosztva   
Az euklideszi algoritmus segítségével kiszámítható olyan , amire , -nak és -nek nem lehet közös prímosztója, hiszen ha lenne, akkor állna .  
Hátravan még, hogy a megoldásokat adjuk meg. Mivel , ezért ∀ szerinti maradékosztály pontosan darab szerinti maradékosztály uniója, a megoldások tehát:

## Euklideszi algoritmus (ennek alkalmazása lineáris kongruenciák megoldására is)

Euklideszi algoritmus: hatékony módszer két szám legnagyobb közös osztójának (LNKO) meghatározására.  
Input: , Output:   
Legyen , . Ha már meghatároztuk az számokat, akkor legyen .  
Az tehát az -vel történő osztásakor keletkező maradék (C nyelven:  ), tehát teljesül. Az eljárás akkor ér véget, ha , ekkor .  
  
Másként: első lépésként elosztjuk a-t maradékosan b-vel: . Ezután már -et keressük: . A további lépések: . Az algoritmus addig megy, amíg lesz, ekkor megkapjuk, hogy .

Pl.:   
. Tehát .

Pl. 2:   
. Tehát .

Az euklideszi algoritmus azért ér véget, azaz lesz, mert nemnegatív egészek szig. mon. csökkenő sorozata, tehát az eljárás lépésszáma felső becslés.

Lineáris kongruencia megoldása euklideszi algoritmus segítségével:adott lineáris kongruencia. Először meg kell vizsgálni, hogy megoldható-e: az euklideszi algoritmus segítségével kiszámoljuk -et, és ha ez osztható -vel, akkor van megoldás (tehát **megoldható**). Ezután az algoritmus során kapott maradékokat fordított sorrendben kifejezzük az egyenletekből, és így megkapjuk az -et.

Példa:  
Megoldható, ha   
Először meghatározzuk LNKO-t:  
(Tehát mivel teljesül (, pedig osztója -nek), ezért a lin. kongruencia megoldható, egy megoldása van.)Ezután az egyenletekből kifejezzük a maradékokat:  
 🡪   
  (marad mod 101, mivel )∎

Példa 2.:. Vizsgálat: ?  
. Tehát . 2 pedig osztója 24-nek, tehát 2 megoldásunk lesz.  
  
 🡪   
 🡪 , osztunk:  
 🡪   
 🡪   
,  
 🡪 (7 rel. prím a 18-hoz!)  
, 🡪 ()  
 🡪   
 🡪 36 modulusra áttérünk  
 VAGY  
. ∎

## Wilson tétele

Tétel: (Wilson):  
Ha prímszám, akkor .  
Összetett számra ez nem teljesülhet, mivel ha összetett, akkor -nak és -nak van közös osztója, sőt, minden -nél nagyobb összetett számra .  
Ha , akkor .  
Összefoglalva tehát -re:

biz.:  
-re nyilvánvaló:   
Ha összetett, akkor vagy található két ilyen különböző egész, melyekre , és akkor , vagy , és ilyenkor és szerepel a tényezők között.  
Legyen végül prím:  
 egészhez tartozik egy egész, melyre , hiszen az kongruenciát pontosan egy maradékosztály oldja meg.  
Látható, hogy ha -hoz , akkor -hez a tartozik, tehát az számok úgy rendezhetők párokba, hogy ∀ pár szorzata 1-et ad maradékul -vel osztva. A párokba rendezés azért nem egészen pontos, mert bizonyos számok esetleg önmagukkal állnak párban. Ezekre az a számokra teljesül, azaz az önmagukkal párban álló számok kizárólag az 1 és (p-1) lesznek. Átrendezve a -t, ∀ prím szorzata 1 lesz, és lesznek még a páratlanul maradt 1 és  .

12.) Euler-féle ϕ-függvény, redukált maradékrendszer, Euler-Fermat-tétel, kis Fermat-tétel. Kétismeretlenes, lineáris diofantikus egyenlet megoldása (konkrét példán). Két kongruenciából álló kongruenciarendszer megoldása (konkrét példán)

## Euler-féle ϕ-függvény

Def.: : és között az -hez relatív prímek száma.

Pl.:, mert 1, 2, 3, 4, 5, 6, 7, 8, 9, 10  
ha prím: , mert 1-től -ig ∀ szám relatív prím prímhez

Tétel: haHa

Pl.:

## Redukált maradékrendszer

Def.: redukált maradékrendszer modulo (röv. )  
ez egy halmaz, úgy, hogy teljesülnek a következők:  
(1) számuk/elemeik   
(2) ,  
 (inkongruensek egymással mod m)  
(3)  -re (relatív prímek mod m)  
  
Szavakkal: legyen modulus rögzített. A -vel reprezentált maradékosztályt **redukált maradékosztály**nak nevezzük, ha és relatív prímek. Ha minden redukált maradékosztályt egy számmal reprezentálunk RMR-t alkotnak. A redukált maradékosztályok száma (Euler-függvény). Tehát a RMR-ek eleműek.

Pl.: :  vagy , (✓), , , stb., , , stb.

Állítás: ha RMR mod m és is RMR mod m

Pl.: **/**∙7, mert   
 is

biz.:  
(1) a két halmaz elemszáma nyilván megegyezik ✓  
(2) ha /:a (a, m)=1  
 tudjuk, hogy volt   
(3) tudjuk:  
✓

## Euler-Fermat-tétel, kis Fermat-tétel

Tétel: (Euler-Fermat)   
Mivel ⟹tehát az szorzatok valamilyen sorrendben kongruensek a számokkal /: ; ... /:, ..., /:  
✓

Tétel: („kis” Fermat tétel) prím, a tetszőleges egész ⟹

Biz.: prím  
 ✓

## Kétismeretlenes, lineáris diofantikus egyenlet megoldása (konkrét példán)

Példa: kétismeretlenes, lineáris diofantikus (diofantoszi) egyenlet megoldása  
általánosan: adott az egyenlet és , kérdés:   
 🡪 . Tehát visszavezettük a problémát egy lin. kongr. megoldására.  
Előzőleg láttuk, hogy ennek megoldása az , tehát  
Ellenőrzés:

## Két kongruenciából álló kongruenciarendszer megoldása (konkrét példán)

Példa: Két kongruenciából álló kongruenciarendszer megoldása  
Az elsőből következik, hogy alakú , ezt helyettesítsük be a másodikba!  
 alakú alakú

13.) Számelmélet és algoritmusok: alapműveletek, hatványozás az egészek körében és modulo m. Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosítás.

## Számelmélet és algoritmusok: alapműveletek, hatványozás az egészek körében és modulo m[[3]](#footnote-3)

Egy algoritmust akkor tekintünk jónak, ha lépésszáma felülről becsülhető az input hosszának polinomjával.  
Vizsgáljuk meg az alapműveletek lépésszámigényét!

Nyilván az összeadás és kivonás lépésszáma a számjegyek számával arányos, ezek tehát lineáris, azaz polinomrendű algoritmusok.

Könnyű végiggondolni, hogy az írásbeli szorzás és osztás is polinomiális (de már nem lineáris).

Viszont a hatványozás nem végezhető el polinomrendben, hiszen pl. végeredményének puszta kiírásához már lépés kell, ami az inputnak (vagyis -nek) exponenciális függvénye. ( szám hossza , és ez nem polinomiális függvénye a ()-nek)

Az euklideszi algoritmus hatékony, mert polinomiális lépésszámú.

Ezekből következik, hogy a maradékszámítás is polinomiális, mert kiszámításához egy osztásra, egy szorzásra és egy kivonásra van szükség: (C szintaxissal)

Tehát a is polinomiális!

Mi a helyzet a hatványozással?  
Az alábbi példa bemutatja, hogy a hatványozás elvégezhető polinomidőben:

Példa: Most írjuk fel a 100-at binárisan:

...

## Prímtesztelés

200-szor

Eukl. alg.

n nem prím!

STOP

n nem prím!

STOP

Prímtesztelés:  
Egy egyszerű módszer, hogy -től -ig ellenőrizzük az -nel való oszthatóságot. Előnye, hogy ha szám összetettnek bizonyul, akkor ez megadja egy osztóját is, viszont exponenciális lépésszámú.

Ssokkal hatékonyabb (gyorsabb), polinomrendű algoritmus is létezik erre: a Fermat-teszt.  
Fermat-teszt: kérdés: prím-e?  
Kis Fermat-tételen alapul (aminek az RSA-eljárásban is szerepe van), ami kimondja, hogy ha p prím, és , akkor .

1. lépés: felveszünk egy tetszőleges számot, amire igaz, hogy .

2. lépés: kongruenciák ellenőrzése:  
ha, akkor tanúja/árulója -nek 🡪 n NEM prím! STOP,  
ha , akkor cinkosa -nek 🡪 valószínűleg prím

A Fermat-teszt problémája, hogy hibázhat, azaz egy összetett számot is prímnek tekinthet. Ennek kiküszöbölésére sokszor, sok -ra kell végrehajtani a tesztet. Ha a teszt kb. 200-szor lefutva (ha korábban nem állt le) is azt adja ki, hogy prím (), akkor nagy valószínűséggel igaza van.

Tétel: ha -nek **∃ tanúja** ⟹ legalább fele tanú! (RMR=redukált maradékrendszer)

Biz.: legyen „” egy tanú, cinkosok  
Állítás: : tanú  
biz.:   
Állítás:   
Biz.: ha /, mert

Következmény: ha van tanú, akkor a Fermat-teszt legfeljebb valószínűséggel téved

## Carmichael számok

Def.: Carmichael-szám, ha **összetett** szám, de ∄ tanúja, csak cinkosa (ami arra utalna, hogy valószínűleg prím) a RMR-ben,  
azaz ∀ a -re .  
pl.:   
De van olyan teszt, aminek a működése olyan, hogy kiszűri a Carmichael-számokat.

Prímgenerálás: legyen pl. egy -jegyű random szám 🡪 prímtesztelés. Ha összetett, megnézzük A függvény szerint rövid időn belül prímre fogunk találni.

## Nyilvános kulcsú titkosítás

Bármilyen üzenet átalakítható számjegyek szorzatává, feltehetjük tehát, hogy a titkosítandó üzenet sokszámjegyű számok szorzata. A rejtjelezés alapja, hogy legyen egy kódoló és dekódoló függvény:  
, , amire teljesül a visszafejthetőség:

RSA-kód: , ahol , sokszámjegyű prímek  
 választása úgy, hogy -hez relatív prím legyen:   
kódolás: nyilvános: (mindenki számára ismert, ennek segítségével kódolhatják mások nekünk szánt üzeneteiket. A nyílt kulccsal kódolt üzenetet csak a titkos kulccsal tudjuk „megfejteni”.)titkos:

Megjegyzés: ez az egész azért működik, mert számok prímtényezős felbontására hatékony algoritmus nem ismert!

Dekódolás:   
 jól van megválasztva ⟺-re

Segédtétel: cél: valamely -ra, azaz lin. konguencia 🡪   
kongr. az euklideszi algoritmussal megoldható!   
A -t azért nem tudja bárki kiszámolni, mert nem tudja felírni a lin. kongruenciát, ugyanis a kiszámolásához szükséges és ismerete: .

Digitális aláírás  
Előnye, hogy ha üzenetet küld -nek, akkor meg tud bizonyosodni arról, hogy az üzenetet csakis -tól kaphatta.  
 🡪

14.) Művelet fogalma, csoport, Abel-csoport. Példák: csoportok számokon, mátrixokon, rajzok szimmetriacsoportja, diédercsoport. Példák véges és végtelen, kommutatív és nem kommutatív csoportra mind a négy lehetséges variációban.

lásd még: <http://www.cs.elte.hu/~ewkiss/bboard/07t.mat/Alg2_art_12.pdf>

## Művelet fogalma

Def.: az függvényt műveletnek hívjuk, ahol alaphalmaz és a -ból készíthető rendezett párok halmaza.  
  
Ellenpélda: a skaláris szorzás egy „öszvér” művelet, mert vektorokat kap, és skalárt ad vissza;

művelet

/

\

\

*Másképp*: Művelet: Egy H nemüres halmazon értelmezett (kétváltozós) műveleten egy függvényt értünk, azaz egy olyan leképezést, amely bármely elempárhoz egyértelműen hozzárendel egy H-beli elemet.  
Vagy: a halmazon értelmezett n-változós műveleten (0-változós műv.: 5. 1-változós műv.: (ellentettképzés), (deriválás), stb.) egy tetszőleges leképezést értünk, azaz minden, elemeiből képzett, rendezett -eshez (pl. -hez) -nak egy bizonyos elemét (itt -t) rendeljük.  
A **művelet** **ne vezessen ki adott struktúrából**!

Def.: A  halmazon értelmezett, 2-változós  művelet:  
- kommutatív (felcserélhető), ha teljesül elemekre  
- asszociatív (átzárójelezhető), ha teljesül –ra  
-  struktúra félcsoport, ha asszociatív művelet a H-n.  
- ha \* asszociatív **ÉS kommutatív** is, akkor S Abel-félcsoport (vagy kommutatív félcsoport).

Pl.:

* A valós számokon értelmezett + művelet asszociatív és kommutatív 🡪 Abel-félcsoport.
* Az -es mátrixok a szorzással félcsoportot alkotnak: mátrixok szorzása asszociatív, de nem kommutatív)
* A pozitív számokon értelmezett hatványozás nem asszociatív és nem kommutatív (hisz , ill. ),
* a polinomok kompozíciója (egymásba helyettesítése) asszociatív, de nem kommutatív (hisz , de általában).

Def.: , egységelem, ha elemére (helybenhagyja az elemet).  
Összeadás esetén az egységelemet nullelemnek vagy nullának nevezzük, és 0-val jelöljük.

Állítás: az egységelem egyértelmű (ha van)

biz.: tfh. , különböző egységelemek: ⭍

Def.: az inverze , ha , ahol az egységelem.  
Jele: . Tehát

## Csoport, Abel-csoport

Def.: csoport, ha *művelet* -n **és**:  
- **asszociatív** (értelmezve van G-n egy asszoc. művelet, elemre; tehát *félcsoport*)  
- ∃ **egységelem**  
- ∀ elemnek ∃ **inverz**e a \* műveletre.

Állítás: egy csoportban egyértelmű (ha van)

biz.: tfh. az két különböző inverze:  
 ⭍

másképp:

Def.: ha csoport és kommutatív, akkor Abel-csoport

Csoportok számokon:  
- **egész számok** : Abel-csoportot alkotnak az egész számok az összeadásra nézve: komm., asszoc.: , egységelem: , inv.: ,

- **rac. sz.**: Abel-csoport,

- **valós sz.** : Abel-csoport: egységelem a 0, inverz az ellentett (-x), asszoc. komm.,

- **komplex sz.**[[4]](#footnote-4) : Abel-csoport: egységelem a 0, inverz az ellentett (-x), assz. (), komm. ()  
- De pl. **term. számok** **NEM** csoport, mert a pozitív tagoknak inverze!  
- **valós számok a szorzásra nézve** **NEM** csoport, mert 0-nak inverze!  
- Viszont **kivéve a 0-t** már csoportok lesznek a következők:  
 - nemnulla valósak, a szorzásra nézve Abel-csoportot alkotnak: komm., asszoc., egységelem az , inverz a reciprok .  
,

Csoportok mátrixokon:  
Adott: , a művelet legyen a **mátrixszorzás**. Csoportot alkot? Vizsgáljuk meg:

1. **zártság**: a determinánsok szorzástétele miatt
2. **asszociativitás** (átzárójelezhetőség)   (Az -es mátrixok a szorzással félcsoportot alkotnak: mátrixok szorzása asszociatív, de *nem kommutatív*!)
3. **egységelem**:=egységmátrix
4. **inverz**:=inverzmátrix : ez is H-beli, és biztosan , mert  (invertálás csak a nem nulla determinánsú mátrixokra értelmezett)

 IGEN, csoport

Rajzok/alakzatok szimmetriacsoportja:[[5]](#footnote-5)  
a sík azon egybevágósági transzformációi, amelyek ezt az alakzatot önmagába viszik, és a **művelet** ezen transzformációk egymás utáni elvégzése.  
  
Most tekintsük egy rajznak, pl. egy szabályos háromszögnek a szimmetriáit/egybevágódási transzformációit!  
 (3 forgatás, 3 tükrözés (a felezőmerőlegesekre); az identitás, vagyis helybenhagyás, 0 fokkal való forgatás)  
A háromszög szimmetriája a sík egy olyan egybevágósági transzformációja, ami a háromszöget önmagába képzi.Legyen , a művelet pedig a **függvénykompozíció**!  
A függvénykompozícióról (, az és kompozíciója vagy szorzata, jele néha ) tudjuk, hogy rendelkezik az **asszociativitás** (átzárójelezhetőség) tulajdonsággal:  
:

:, :, :

O

B

C

A

f

O

A

B

C

f

O

C

A

B

f

: , : , :

O

C

B

A

f

O

B

A

C

f

O

A

C

B

f

az körüli 120°-os forgatás, a +240°-os forgatás

a felezőmerőlegesére tükrözés

, mivel A🡪A🡪B;  B🡪C🡪A;  C🡪B🡪C

, forgatás a tengelyek szögének 2x-esével, A🡪A🡪B;  B🡪C🡪C;  C🡪B🡪A

egységelem/identitás: (360°-kal forgatás), ,

inverz (első transzformáció hatását „visszacsinálja”): ()

A csoport szorzástáblája (**Cayley-táblázat**): A sorának és oszlopának metszéspont-jában .

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Tehát a csoport elemei: , ahol , , .  
, , . (inverz: )  
Példa:

Állítás: az  **szimmetriacsoport** (rajzot önmagába vivő egybevágósági transzformációk halmaza a kompozícióra, mint műveletre nézve) **csoport**.

biz.:  
- a függvénykompozíció **asszociatív**  ✓  
- **egységelem** := identitás (, 0 fokkal forgatás, helybenhagyás)  ✓  
- **inverz**:= inverzfüggvény (, azt jelenti, hogy )  ✓

## Diédercsoport

Def.: diédercsoportnak nevezzük az -oldalú szabályos sokszög szimmetriacsoportját (szabályos n-szög egybevágóságai). Jele:   
, és (a szabályos n-szögnek 2n szimmetriája van – csoport rendje , ugyanis van darab tengelyes tükrözés és a helybenhagyással együtt darab forgatás)Az előzőekben említett háromszöges példa a -nak felel meg.  
, ,

15.) Elem rendje (ez véges csoportban véges), ciklikus csoport. Részcsoport. Szimmetrikus csoport. Csoportok izomorfiája.

## Elem rendje (ez véges csoportban véges)

Def.: csoport rendje = az elemszámával, ezért jele: , pl.: (első 10 szám permutációja), ()

Def.: csoport,   
Példa: -nál

Tétel: véges, , hogy

biz.: Soroljuk fel hatványait: Mivel G véges , hogy .  
Szorozzuk ezt be -gyel jobbról: . Ezt a -es szorzást hajtsuk végre annyiszor, hogy végül egyenlőséget kapjunk, ekkor . ✓

Def.: , a g rendje k, ha k a legkisebb olyan kitevő, hogy , jele: (elemet k-szor összeszorozva önmagával egységelemhez jutunk)  
 Ha nincs ilyen szám, végtelen rendű elemről beszélünk.  
VAGY: A G csoport g elemének rendje a g által generált <g> részcsoport elemszáma. Másképp g elem rendje az a legkisebb szám, amelyre . Ha ugyanis ilyen , akkor , és a elemek különbözőek (hiszen ha , akkor ), ezért <g> n-elemű. Ha ilyen , akkor a elemek mind különbözőek, <g> végtelen.  
Ha ciklikus csoport, melyet generál, akkor G eleme előáll (= [i-szer] alakban), ahol . Ha G rendje véges, elegendő a pozitív i kitevőkre szorítkozni. Ha G végtelen, akkor a generátorelemnek semelyik hatványa sem egységelem, mert egyébként a generátorelem csak véges sok elemet generálna.  
Ha két ciklikus csoport rendje különböző, akkor nem izomorfak.  
Ha azonban G és H ciklikus csoportra .[[6]](#footnote-6)

Pl.: -nál (360°-os forgatás), (2x-es tükrözés)-nál

## Ciklikus csoport

Def.: G ciklikus csoport, ha generátorelem, hogy -ből eleme kifejezhető a művelet és az inverzképzés segítségével, jele: .  
Másként: az olyan csoportot, melyet valamely eleme generál, ciklikus csoportnak nevezzük.

Állítás: véges, ciklikus , amire .

biz.:  
⟸: tartalmazza -t és annak hatványait, g kül. hatványainak száma , ami egyenlő -kel, tehát generálni tudja ∀ elemét ⟹ ciklikus  ✓  
⟹:Mivel ciklikus, ∃ egy g generátoreleme, amivel elő lehet állítani ∀ elemét ⟹   ✓

Pl.: ciklikus, ciklikus.

Állítás: ciklikus 🡪 Abel

biz.:   
  ✓

Állítás: minden párosrendű csoport ciklikus.

biz.: Legyen prím. A Lagrange-tétel miatt -re   ✓

## Részcsoport. Csoportok izomorfiája

Def.: izomorf -rel (, körrel) [jele: ≅], ha kölcsönösen egyértelmű függvény úgy, hogy:  
-re , másképpen: -re   
Vagy: G és H csoport izomorf, ha van köztük művelettartó bijekció, azaz létezik egy bijekció, melyre tetszőleges esetén áll. (a baloldali szorzás a G, a jobboldali pedig H művelete)

Pl.:   
   
 } vegyük észre, hogy a logaritmusfüggvény!

Def.: csoport, , részcsoportja -nek, ha is csoport a G csoportműveletére nézve. Jele: .  
Tetszőleges G csoport részcsoportjainak metszete is G részcsoportja.

Tétel:   
 részcsoport ⟺

biz.:  
⟹: a szükségesség nyilvánvaló  
⟸: -ra művelet:  
🡆asszociatív (mert -ben is az)  ✓  
🡆 egységelem  ✓  
🡆 miatt -nak inverze is -ban van  ✓

f90

f270

f270

t3

t1

t4

t2

Pl.:

Állítás: ciklikus csoport részcsoportja ciklikus.

biz.: G ciklikus csoport generátoreleme legyen g, és legyen valódi részcsoport. Tekintsük a minimális -t, melyre . A cél belátni, hogy generálja H-t.  
Tfh. a -t nem generálja, vagyis .  
Legyen Mivel 🗲

Állítás: azonos rendű ciklikus csoportok izomorfak

biz.: . Legyen a generátoreleme, ekkor izomorfizmus.  ✓

Tétel: (Cayley) G véges csoport , hogy valamelyik részcsoportjára .

## Szimmetrikus csoport

Def.: Az kölcsönösen egyértelmű függvényt permutációnak nevezzük.  
 halmaz permutációján annak önmagára vett bijektív leképezését értjük. a legtöbb vizsgálatban véges, így permutáción elemeinek egy meghatározott átrendezéseit vagy sorbarendezését értjük. (Ha pl. egy csomag kártya, akkor a kártyák megkeverésével egy permutációját állítjuk elő. VAGY: ha elemei egy futóversseny résztvevői, akkor a verseny minden lehetséges végeredménye egy permutációját képviseli.)  
-elemű -halmaz elemei: első pozitív egész szám -nak egy permutációja: zárójelben, egymás alá írva, sorbarendezve felsoroljuk az értelmezési tartományát és értékkészletét.  
Pl. 1.: , , , , . Permutáció rövidebben:  
   
még rövidebben: (Descartes-féle alak)  
Permutációk száma:   
Mivel az 1 képe n különböző érték lehet, ezek mindegyikére különböző értéket választhatunk a 2 képéül a fennmaradó számokból, ezek mellé a párok mellé -féleképpen választhatjuk a 3 képét, stb. Az db szám képeként tehát -féleképpen választhatjuk meg a rendezett értékeket.  
  
Pl. 2.:

Def.: szimmetrikus csoport: halmaz permutációi alkotta csoport a függvénykompozíció műveletre nézve.  
*elemei*: permutációi, *művelet*: kompozíció;   
  
**Permutációk szorzása**: megfelelő leképezések egymás utáni végrehajtása.  
Az n elem feletti permutációk csoportja az n elemű szimmetrikus csoport, . Mivel egy tetszőleges csoport összes elemének egy adott elemmel végzett megszorzása a csoport elemeinek egy permutációját adja, a szimmetrikus csoport bármely más csoportot képes „szimulálni”, azaz bármely n elemű csoport izomorf egy legfeljebb elemű szimmetrikus csoport valamelyik részcsoportjával, lásd Cayley-tétel (Cayley-tétel: véges csoport izomorf egy alkalmas permutációcsoporttal ( részcsoportjai).).  
(Minden permutáció felbontható diszjunkt ciklikus permutációk szorzatára. Ez a felbontás a ciklushosszakat nézve egyértelmű: az azonos hosszú ciklusokból álló permutációk egymás konjugáltjai. Minden permutáció felbontható továbbá kettő hosszú ciklikus permutációk (cserék) szorzatára.)  
,   
,   
   
Fontos (lásd Fleiner-jegyzet): egy permutáció kiszámításakor először alkalmazzuk a permutációt, és aztán a -t.  
Pl. 1.  
   
   
 adódik.  
Így: szorzat ():   
   
   
   
   
   
  
Pl. 2.[[7]](#footnote-7):  
   
először alkalmazzuk a permutációt, és aztán az -t.  
Tudjuk, hogy x elemre (ez a leképezés szorzás-definíciója). Tehát   
,   
   
   
   
Másik oldalról megvizsgálva:  
Tudjuk, hogy x elemre szorzat (ez a leképezés szorzás-definíciója). Tehát:   
   
   
   
   
, tehát a permutációk szorzata NEM kommutatív.  
  
 Mivel , ezért   
 és szorzata az identikus leképezés:  
   
  
Pl. 3.:  
, jobbról balra szorozva (, először g, majd f), balról jobbra szorozva (, először f, majd g)  
Pl. 3.:  
 ( pl. így áll elő: )

lásd még perm., szimm. csop., fv.komp.:

<http://www.math.u-szeged.hu/~mmaroti/okt/2010o/permutaciok.pdf>

<http://www.math.unideb.hu/~turjanyi/Komb_j/K_Win_Doc/g0602.doc>

Állítás: csoport.

biz.:  
- a függvénykompozíció **asszociatív**  ✓  
- **egységelem** := identitás    ✓ (az identikus (mindent helybenhagyó leképezés) egy permutáció, és ezzel akár jobbról, akár balról komponálunk, egységként viselkedk)  
- **inverz** := inverzfüggvény (), ,  
pl.: ;   
  ✓

**16.) Mellékosztály fogalma, példák. Lagrange tétele, elemrend és csoport rendjének kapcsolata.**

## Mellékosztály fogalma, példák

Def.: csoport,   
A halmaz a H részcsoport szerinti bal oldali mellékosztálya, jele:   
Másként: ha adott egy csoport, ennek egy eleme, valamint egy részcsoportja, akkor a részcsoport adott elem szerinti mellékosztálya azoknak az elemeknek a halmaza, amelyek a részcsoport elemeinek az adott elemmel való szorzatából (csoportra értelmezett műveletéből, ez lehet összeadás is) adódnak.

G g

H

Pl.:

y

x

(2,3)

(5,0)

(3,-1)

(-5,3)

0

Pl. 2.: , ahol az többszöröseit jelöli. Egy adott esetén a G csoport k szerinti baloldali mellékosztálya a halmaz lesz, vagyis mindazon egészek, amelyek -val kongruensek modulo .

Pl.: (emlékezzünk vissza, hogy a diédercsoportot úgy definiáltuk, hogy a művelet a fv.kompozíció, amit jobbról balra kell végrehajtani!)

t1

t3

t2

Tulajdonságok:

1.)   
biz.: mivel   ✓

2.)   
biz.:   
; cél:   
 /   ✓

3.) H véges   
biz.: ha / balról  
  ✓  
Mivel a H és g\*H között létesíthető kölcsönösen egyértelmű hozzárendelés (, egyértelmű hozzárendelés (függvény)), a két halmaz számossága egyenlő:

## Lagrange tétele, elemrend és csoport rendjének kapcsolata

Tétel: (Lagrange) Ha véges csoport, akkor -re , azaz H rendje osztója G rendjének minden H részcsoportra.   
Elem és csoport rendjének kapcsolata: speciálisan, bármely elemének rendje [] (amely gyakorlatilag a által generált részcsoport elemszáma) osztja G rendjét, azaz -re.  
  
 szerinti mellékosztályok, számuk: i  
  ✓(a tartalmazó csoport rendje megegyezik a részcsoport rendjének és indexének szorzatával.)  
Szövegesen:  
Az előző megfigyelés szerint a csoport néhány szerinti (jobb oldali) mellékosztály uniója, és minden mellékosztály elemet tartalmaz.  ✓  
A tétel második felének bizonyítása:  
Ha csoportnak egy eleme, akkor álljon a hatványaiból: Állítás: részcsoport.  
biz.:  
(i)   
ha , akkor   
ha , akkor   ✓  
(ii)   ✓

G

17.) Gyűrű, ferdetest és test fogalma. Nullosztómentes gyűrű, test nullosztómentessége. Példák:, , , , , -es mátrixok, polinomok, (ez milyen -re test), kvaterniók, .

## Gyűrű, ferdetest és test fogalma

Eddig egyműveletes stuktúrákkal foglalkoztunk. Ha azonban a ℤ, ℚ, ℝ, ℂ számhalmazokról szeretnénk többet tudni, érdemes mindkét alapműveletet: az összeadást és a szorzást is figyelembe venni.

Def.: legyen R tetszőleges halmaz (≠0), R-en két művelet értelmezett: +, ⦁ (struktúra: ).  
A két művelet disztributív (kb. szétválasztható) ha -re: és .

|  |  |
| --- | --- |
| (1) (**kommutatív**) | (I) (**kommutatív**) |
| (2) (**asszociatív** 🡪 félcsoport) | (II) (**asszociatív**) |
| (3) , amire (**nullelem** (összeadás egységeleme vagy additív semleges elem)) | (III) (**egységelem** vagy multiplikatív semleges elem) |
| (4) -re ; (additív **inverz** vagy ellentett**)** | (IV) ; (multiplikatív **inverz** vagy reciprok (0-hoz nincs)) |
| (5) ; (a művelet **disztributív** a műveletre nézve) | |

Gyűrű: (1-5)+(II)  
 Abel-csoport (összeadás komm., asszoc., van nullelem, additív inverz) és  
 félcsoport (szorzás asszoc.) és  
disztributivitás

Kommutatív gyűrű: (1-5)+(I-II)  
gyűrű ÉS még kommutatív is

Ferdetest: (1-5)+(II-IV)  
A T gyűrű ferdetest, ha csoport (szorzás nem komm.; de asszoc., egys.e., mult.inverz; tehát *ferdetest=gyűrű+egységelem+mult.inverz*).

Test: (1-5)+(I-IV)  
A T gyűrű test, ha a szorzás kommutatív is (tehát *test=ferdetest+szorzás kommutativitása*).

## Példák:, , , , , -es mátrixok, polinomok

* **végtelen test**: (komm. gyűrű, és minden nemnulla számnak van reciproka, így a szorzás is csoport a nemnulla számokon)
* NEM test, mert ∄ inverze ∀ elemnek, hanem csak kommutatív gyűrű.
* NEM gyűrű, mert nem csoport az összeadásra, nincs inverze.
* gyűrűk még: tetszőleges szám többszörösei ();
* **véges test**: modulo p maradékosztályok , ahol p prím ; ( kommutatív gyűrű; -vel szokás jelölni; a szorzás invertálhatóságát kivéve minden testaxióma következik az egész számok és a kongruencia megfelelő tulajdonságából (a reciprok kiszámítása az Euler-Fermat-tételből () adódik), azt pedig elemi számelmélettel meg lehet mutatni). Ha m nem prím (összetett), akkor -ben (modulo n maradékosztályok ) van nullosztó, tehát nem test, csak **véges gyűrű** (összeadhatók, kivonhatók és szorozhatók, de az osztás nem végezhető el reprezentáns elemekkel. Multiplikatív inverze ugyanis pontosan a redukált maradékosztályoknak van. Ezek minden eleme relatív prím -hez.)  
  - **végtelen gyűrű**: (mxszorzás nem komm., 0 det. mx. inverze, többi stimmel) vizsgálata:

|  |  |
| --- | --- |
| (1) mátrixok összeadása kommutatív  ✓ | ~~(I)~~ mátrixszorzás NEM kommutatív ✖ |
| (2) mátrixok összeadása asszociatív  ✓ | (II) mátrixszorzás asszociatív  ✓ |
| (3) nullelem legyen a nullmátrix:   ✓ | (III) egységelem legyen az egységmátrix:   ✓ |
| (4) additív inverz:   ✓ | ~~(IV)~~ a 0 determinánsú mátrixoknak ∄ inverze! ✖ |
| (5) disztributivitás teljesül  ✓ |  |
|  | ~~(I)~~ és ~~(IV)~~ miatt ez csak gyűrű, egészen pontosan **egységelemes gyűrű**; egységelemes, mert a szorzásra nézve ∃ egységelem |

* az egész vagy a valós együtthatós polinomok (ℤ[x],ℝ[x]) kommutatív gyűrűt alkotnak a szokásos p.összeadásra, szorzásra nézve. Testet azért nem alkothatnak, mert pl. az x polinomnak az felelne meg multiplikatív inverznek, de az sem polinom!
* a valós polinomok hányadosteste test:  
  , a műveletek:  
  , ill. .

## Nullosztómentes gyűrű, test nullosztómentessége

Def.: R gyűrűben az elem nullosztó, ha olyan , amelyre .

Def.: R gyűrű nullosztómentes, ha R-ben nullosztó, azaz  
ha -re az csak akkor teljesül, ha .  
Pl.:

Tétel: ∀ test nullosztómentes.

biz.:   
🡆ha   ✓  
🡆ha / balról  
  ✓

Def.: A **kommutatív nullosztómentes** **gyűrű** neve integritási tartomány. (Pl. komm. és nullosztómentes. De mátrixgyűrűben nullosztó, ha olyan mátrix, amelyre (ha egyenletnek van nemtriviális megoldása).)

Pl.: az egész számok, a páros számok gyűrűje integritási tartomány.  
 NEM integritási tartomány, mert pl. és , tehát a 2 ill. a 3 nullosztók.

## (ez milyen -re test)

Def.: -nel jelöljük és modulo n maradékosztályok gyűrűjének nevezzük a  
 halmazt a modulo összeadásra, ill. szorzásra nézve:

Pl.: -nél:  
   
, de a 2 és az 5 sem 0 ⟹ nem nullosztómentes ⟹ **nem test**.

Tétel: test ⟺ prím

biz.:  
⟹: tfh. összetett: ekkor szorzattá alakítható az előző példához hasonlóan, vagyis nem nullosztómentes ⟹ nem test! ⭍  
⟸: prím:  
(1), (2), (3), (4)  ✓ (komm.,assz.,nullelem,additív inverz)  
(I)  ✓ (komm.)  
(II)  ✓ (assz.)  
(III)  ✓ (egységelem)  
(IV): egyedül ez nem triviális (mult. inverz):   
 (v)  ✓ (disztr.)

## Kvaterniók

🡪 a válasz: kvaterniók. A kvaterniók a komplex számok négy dimenzióra történő nem kommutatív kiterjesztései. A kvaterniócsoport elemei , , , , , , , .

i

j

k

Def.: ,  
de , , 🡪 tehát az már biztos, hogy NEM kommutatív.

A kvaterniók ferdetestet alkotnak, (*ferdetest*: összea.: komm., assz., van nullelem, additív inverz; szorzás: assz., van egységelem, multiplikatív inverz; szorzás disztr. az összea. műv.-re; szorzás NEM kommutatív), mert:  
(1), ..., (4) (összea.: komm., assz., van nullelem (), additív inverz ( ellentettje ))  ✓  
~~(I)~~ (szorzás nem komm.) (, DE , , )✖  
(II) (szorzás asszociatív) ✓  
(III) (van egységelem):  ✓  
(IV) (multiplikatív inverz): ha akkor  
(5) (szorzás disztr. az összea. műv.-re) ✓

## , azaz is test (a racionális számok kibővítve -vel)

Ez is testet alkot (test=ferdetest+szorzás kommutativitása), mert:  
könnyen látható, hogy ez is teljesíti az összes kritériumot, az egyedüli nemtriviális itt is az (IV) pont, vagyis a multiplikatív inverz:

1. <http://www.cs.bme.hu/~kiskat/sza/tanacs.pdf> [↑](#footnote-ref-1)
2. <https://wiki.sch.bme.hu/images/0/04/Bsz2_tetelkidolgozas_2012tavasz.pdf> [↑](#footnote-ref-2)
3. Korábbi cím: „Számelmélet és algoritmusok: összeadás, szorzás, maradékos osztás, hatványozás lépésszáma. Modulo m hatványozás polinomiális időben.” [↑](#footnote-ref-3)
4. emlékeztető: <http://www.math.bme.hu/~szilagyi/01_komplex.pdf> [komplex számok () összeadása a vektorösszeadás szabályai szerint történik (eltolás; ); szorzás: ; egyébként komplex szám inverze:  stb.] [↑](#footnote-ref-4)
5. <http://www.cs.elte.hu/~ewkiss/bboard/07t.mat/Alg2_art_12.pdf> [↑](#footnote-ref-5)
6. Fleiner, 36. o. [↑](#footnote-ref-6)
7. forrás: <http://www.math.u-szeged.hu/~katai/disz3ea/permutaciok.pdf> [↑](#footnote-ref-7)