Ajánlott és felhasznált irodalom: Fleiner Tamás: Nagy, egyesített szuperjegyzet. Nagy segítségemre volt továbbá Vőneki Balázs korábbi, kézzel írt jegyzete, 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)

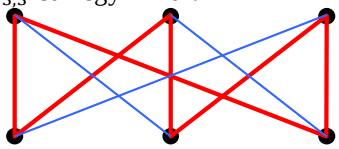
Tartalomjegyzék

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.

Hamilton-körök és -utak

Def.: A G 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.

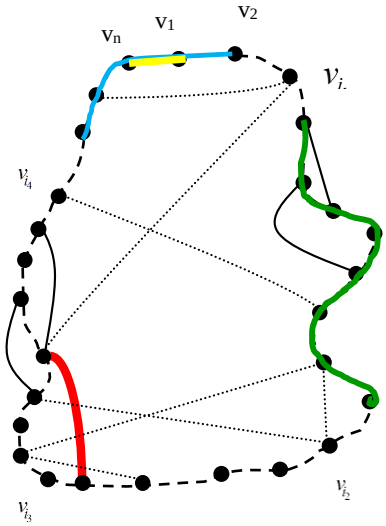
Pl.: a $K_{3,3}$-ban egy H-kör:



Szükséges feltétel Hamilton-kör/út létezésére

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

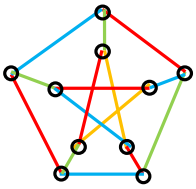
Bizonyítás: **H-kör**



A ***H-kör*** pontjai legyenek $V_1, V_2, V_3, \dots, V_n$ és legyen $V_{i_1}, V_{i_2}, V_{i_3}, \dots, V_{i_k}$ az a ***k pont***, amit elhagyunk.
Vegyük észre, hogy az elhagyott pontok közötti „ívek" biztosan összefüggő komponenseket alkotnak!
Pl.: (V_{i_1+1}, V_{i_1+2}, V_{i_2-1}) ív is összefüggő lesz, hiszen két szomszédos pontja között az eredeti ***H-kör*** egy éle fut.
Mivel éppen ***k*** ilyen ívet kapunk, nem lehet több komponens ***k-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 V_nV_1 élet, hogy csak H-utunk legyen! Amíg az előző példában a pontok elhagyása után a V_{i_4+1}, …, V_n, V_1, V_2, ív összefüggő volt, itt már nem, mert $V_nV_1 \notin E(G)$. tehát legfeljebb $k+1$ 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 k db pontot, max. k 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, a belső köréből pedig b csúcsot hagyunk el, akkor a külső ill. a belső körön keletkező komponensek száma legfeljebb a ill b, vagyis a gráfnak nem keletkezhet összességében $a+b$-nél több komponense. (Ha $a = 0$ v. $b = 0$, 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 n-pontú ($n \geq 3$), **egyszerű** G gráfban ∀ két, nem szomszédos x, y csúcsra $d(x) + d(y) \geq n \Rightarrow$ ∃ ***H-kör.***

Bizonyítás:
Indirekt. Tfh. a két feltétel teljesülése ellenére ∄ ***H-kör*** a ***G*** gráfban.
A gráfhoz vegyünk hozzá éleket úgy, hogy továbbra se legyen benne ***H-kör***. Ezt ismételjük addig, amíg lehet. Az így kapott gráfot jelöljük ***G'***-vel, amire szintén teljesül a feltétel.
G'-ben biztosan van két nem szomszédos pont. Legyen ez x, y. ***G'*** $+ \{x, y\}$ gráfban ∃ ***H-kör*** ⇒ ***G'***-ben ∃ ***H-út***.
Legyen ez $P = (\underbrace{Z_1}_{=x}, \dots, Z_2, \dots, \underbrace{Z_n}_{=y})$. Ha x szomszédos Z_k-val ⇒ y nem szomszédos Z_{k-1}-gyel, mert

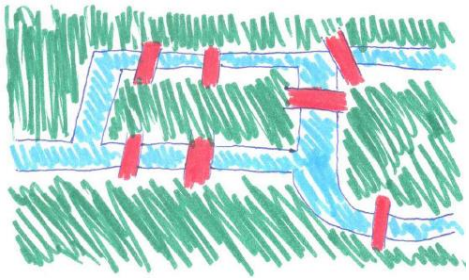
$(Z_1, \dots, Z_{k-1}, Z_n, Z_{n-1}, Z_k, Z_1)$ H-kör lenne, tehát $d(y) \leq n - 1 - d(x) \Rightarrow d(x) + d(y) < n \Rightarrow$ ↯ **ELLENTMONDÁS.**

Tétel: (**Dirac**) Ha az n-pontú ($n \geq 3$), egyszerű gráfban $\forall$ pont foka legalább $\frac{n}{2}$ $\left(d(x) \geq \frac{n}{2}\right) \Rightarrow \exists$ H-kör.

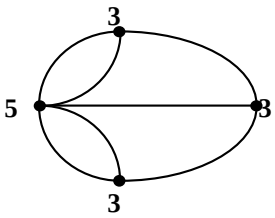
Bizonyítás: Teljesül az Ore-feltétel: $\forall\, x, y$ pontpárra $d(x) + d(y) \geq n$

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

Königsbergi hidak problémája:



← Feladat: $\forall$ hídon pontosan egyszer átkelni.
A feladat gráfelméleti megfelelője: a folyók által határolt területeknek pontok, a hidaknak élek felelnek meg.



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

Megjegyzés:
$\forall$ 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 ***G*** összefüggő (véges) gráfban $\exists$ E-kör $\Rightarrow$ $\forall$ pont foka páros.
2.) Ha ***G*** összefüggő (véges) gráfban $\exists$ E-út $\Rightarrow$ ***G***-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 $\exists$ E-út, akkor az E-út két végpontjának kivételével $\forall$ pont foka páros.

Tétel (elégségesség):

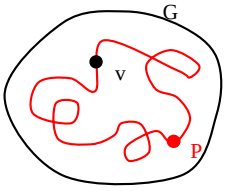
1.) Ha ***G*** összefüggő (véges) gráfban $\exists$ E-kör $\Leftrightarrow$ $\forall$ pont foka páros.
2.) Ha ***G*** összefüggő (véges) gráfban $\exists$ E-út $\Leftrightarrow$ ***G***-nek 0 vagy 2 páratlan fokú csúcsa van.

Bizonyítás:

A *szükségesség*et előbb bebizonyítottuk.

Elégségesség

1.) Legyen $v \in V(G)$ a gráf tetszőleges pontja, P pedig egy v-ből induló élismétlés nélküli séta, amíg elakadunk. Mivel $\forall$ pont foka páros $\Rightarrow$
   - P v-ben akad el
   - v-nek $\forall$ élét használja
   - $\forall$ csúcsból páros sok élet használt



   Legyen P' az ilyen séták közül a leghosszabb.
   Állítás: P' E-kör
   Bizonyítás:
   (indirekt) ***H***: ***G***-ből elhagyjuk a P'-beli éleket. Tudjuk, hogy H-ban $\forall$ fokszám páros ($páros - páros = páros$)
   w legyen olyan csúcs, amire illeszkedik a H-beli és P'-beli él is (megtehetjük, mert a gráf összefüggő.)
   Q legyen egy ***w***-ből induló ***H***-ban élismétlésmentes ***w***-ben elakadó séta.
   Ez 

   hosszabb P'-nél: **ELLENTMONDÁS.** ↯

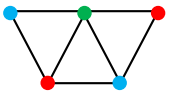
2.) Ha $\forall$ fokszám páros $\Rightarrow$ OK (Euler-kör)
   Ha van két páratlan fokú pont: u, v, akkor húzzunk élet uv közé. Így $\forall$ pont foka páros lesz. Tehát lesz E-kör. Ha ebből a gráfból elhagyjuk uv-t, akkor lesz E-út.

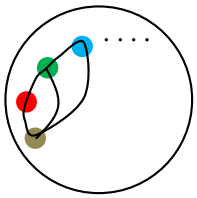
2.) Gráfok színezése. $\chi(G)$ fogalma és viszonya $\omega(G)$-hez, illetve $\Delta(G)$-hez. Brooks tétele (biz. nélkül). Mycielski konstrukciója.

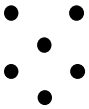
Gráfok színezése, $\chi(G)$ fogalma

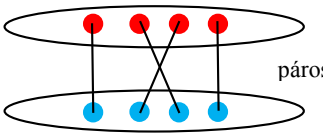
Def.: egy gráf k színnel színezhető, ha a csúcsok k színnel színezhetők úgy, hogy szomszédos csúcsok különböző színt kapnak.
G kromatikus száma k, ha G k színnel színezhető, de $k-1$-gyel nem. Jele $\chi(G) = k$

Pl.:






üres gráfnál: $\chi = 1$


páros gráfnál: $\chi(G) \leq 2$ (akkor < 2, ha üres a gráf)

$\chi(G)$ viszonya $\omega(G)$-hez, illetve $\Delta(G)$-hez

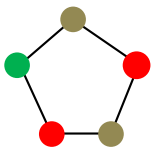
Def.: G egy teljes részgráfját **klikk**nek nevezzük.

Def.: G **maximális klikkmérete** (azaz a legnagyobb klikkben lévő pontok száma) k, ha G-ben van k db csúcs, hogy közülük bármely kettő szomszédos, de $k+1$ nem. Ezt a gráf **klikkszámá**nak nevezzük.
Jele: $\omega(G) = k$

Állítás: $\omega(G) \leq \chi(G)$, $\forall$ G gráfban

Bizonyítás: Ha $\omega(G) = k$, akkor a k csúcshoz kell k db szín

Példa:



C_5:
$\omega(C_5) = 2$
$\chi(C_5) = 3$

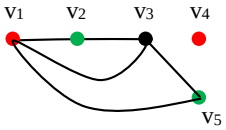
Mohó színezés: csúcsokat jelöljük $v_1, v_2, \dots, v_n$-nel

a színeknek adjunk számokat: ① ② ③ …

$v_1 \rightarrow$ ①

Ha már $v_1, \dots, v_i$ színezett $\rightarrow v_i + 1$ színe legyen a legkisebb sorszámú olyan szín, amilyen szomszéd még nincs.

Pl.:



Tétel: $\chi(G) \leq \Delta(G) + 1$ (ahol $\Delta(G)$ a G gráf maximális fokszáma)

Bizonyítás:
Ha *mohó színezéssel* elkezdjük tetszőleges sorrendben színezni a gráf pontjait, akkor nem kell $\Delta + 1$-nél több színt felhasználnunk, mert amikor egy újabb pontot akarunk kiszínezni, akkor ennek legfeljebb Δ szomszédja van már kiszínezve. Így a $\Delta + 1$-ediket felhasználhatjuk.

Brooks tétele

Tétel: (**Brooks**) Ha G (véges) egyszerű összefüggő gráf, nem teljes gráf (K_n), nem páratlan hosszú kör (C_{2k+1}) $\Rightarrow \boldsymbol{\chi(G) \leq \Delta(G)}$.

Mycielski konstrukciója

Tétel: (**Mycielski** konstrukciója) $\forall\, k \geq 2$ egész számra $\exists\, G_k$ gráf, hogy $\boldsymbol{\omega(G_k) = 2}$ és $\boldsymbol{\chi(G_k) = k}$, $\chi(G_{k+1}) = \mathrm{k} + 1$
Azt mutatja meg, hogy sokszor a $\omega(G_k) \leq \chi(G_k)$ alsó becslés nem sokat ér.

Bizonyítás:
G_2-nek megfelel: ●—●.
Tegyük fel, hogy már $\boldsymbol{G_k}$-t megalkottuk, készítünk ebből $\boldsymbol{G_{k+1}}$-et! $\boldsymbol{G_k}$ pontjai: $a_1, a_2, \ldots, a_n$. Vegyünk fel $n+1$ új pontot: $b_1, b_2, \ldots, b_n, c$ −t a következőképp: $\forall\, b_i$ -t kössünk össze a_i G_k-beli szomszédjával (de a_i-vel ne), c-t pedig $\forall\, b_i$ -vel.

Állítás: $\omega(\boldsymbol{G_k + 1}) = 2$

Bizonyítás: (indirekt)
Tegyük fel, hogy $\exists$ $\boldsymbol{G_{k+1}}$-ben háromszög (Δ). Ennek nem lehet mind a 3 csúcsa $\boldsymbol{G_k}$-ban. Ha c a Δ egyik csúcsa, a másik kettő csak b_i és b_j lehet, de ezek nem szomszédosak. Ha b_i a Δ egyik csúcsa, akkor a másik két csúcs $\boldsymbol{a_x}$ és $\boldsymbol{a_y}$ lehet. Mivel $\boldsymbol{b_i}$ szomszédjai megegyeznek $\boldsymbol{a_i}$ szomszédjaival, ekkor nemcsak $\boldsymbol{b_i a_x a_y}$, hanem $a_i a_x a_y$ is Δ lenne.
→ **ELLENTMONDÁS**.

Állítás: $\boldsymbol{\chi(G_{k+1}) \leq k + 1}$

Bizonyítás: Színezzük ki $\forall\, a_i$-t ugyanolyan színnel, mint $\boldsymbol{G_k}$ egy k színnel való színezésében, majd $\forall\, b_i$-t színezzük a_i színűre, c kapja a $\boldsymbol{k+1}$-edik színt.

Állítás: $\boldsymbol{\chi(G_{k+1}) \neq k}$

Bizonyítás: (indirekt)

Tfh. $\boldsymbol{\chi(G_{k+1}) = k}$! (Ennél kisebb pont nem lehet, mert $\boldsymbol{G_{k+1}}$ részgráfként tartalmazza $\boldsymbol{G_k}$-t és $\boldsymbol{\chi(G_k) = k}$).

Jelöljük x pont színét $f(x)$-szel. Legyen $f(i) = k \Longrightarrow f(b_i) \in \{1,\ 2,\ \ldots,\ k-1\}$

Megadunk egy f' színezést az a_i pontok által feszített részgráfban (ami $\boldsymbol{G_k}$-val iztomorf).

$$f'(a_i) = f(x) = \begin{cases} f(b_i), & \text{ha } f(a_i) = k \\ f(a_i), & \text{egyébként} \end{cases}$$

Beláthatjuk, hogy f' egy $k-1$ színnel való jó színezése $\boldsymbol{G_k}$-nak, ami ***ellentmondás***, mert $\boldsymbol{\chi(G_k) = k}$.

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

Tfh. $f(a_i) = k$ és a_i szomszédos egy olyan a_j-vel, hogy $f'(a_i) = f'(a_j)$!

$$f(a_i) = k \ \Longrightarrow\ f'(a_i) = f(b_i)$$

Mivel az eredeti színezés jó volt: $f(a_j) \neq k \Longrightarrow\ f'(a_j) = f(a_j)$

$\Rightarrow\Rightarrow\Rightarrow f(b_i) = f'(a_i) = f'(a_j) = f(a_j)$

$\Rightarrow f(b_i) = f(a_j)$

De $a_i a_j$ szomszédok G_k-ban $\Rightarrow$ $b_i a_j$ szomszédok G_{k+1}-ben

→Ellentmondás ↯

$\Rightarrow\Rightarrow \boldsymbol{\chi(G_k) = k}$

$\Rightarrow\Rightarrow f'$ egy $k-1$ színezése $\boldsymbol{G_k}$-nak

→→ELLENTMONDÁS ↯

3.) Síkbarajzolható gráfok kromatikus száma, ötszíntétel. Élkromatikus szám: $\chi_e(G)$ viszonya $\Delta(G)$-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 G síkbarajzolható gráf (lerajzolható a síkba úgy, hogy az élei ne messék egymást (gömbre is rajzolható)), akkor $\boldsymbol{\chi(G) \leq 5}$.

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 $n-1$ pontú gráfokra a tétel igaz. Legyen $\boldsymbol{G}$ egy $3 \leq n$ pontú egyszerű síkba rajzolható gráf. Ha $\forall$ pont foka legalább 6 lenne, akkor ez teljesülne rá (tétel: $e \leq 3n-6$):
$3n-6 \geq e = \frac{\sum d(v)}{2} \geq \frac{6n}{2} = 3n$ ↯ **ELLENTMONDÁS** $\Rightarrow \exists$ $\boldsymbol{G}$-nek legfeljebb 5-ödfokú csúcsa. Jelöljük x-szel.
Ha $\boldsymbol{G-x}$ is egyszerű síkba rajzolható gráf, az indukciós feltevés miatt 5-színezhető.
Ha $\boldsymbol{x}$ szomszédjai max. 4 színt kapnak, akkor x megkaphatja az 5. színt.
Ez akkor nem működik, ha $d(x)=5$ és mind az 5 szomszéd különböző színű.
Ha x-nek bármely két szomszédja között lenne él, akkor $\boldsymbol{G}$-ben lenne K_6, ami ellentmond síkba rajzolhatóságának.
Tehát x két szomszédja, y és z nincs összekötve.
Húzzuk össze egy ponttá x, y, z pontokat. Az így kapott $\boldsymbol{G'}$ gráf – az indukciós feltétel miatt – 5 színezhető.
Az ennek megfelelő színezés $\boldsymbol{G}$-ben nem jó, mert x, y, z egyszínűek. $\boldsymbol{G}$-ben x-nek 3 szomszédja van y-on és z-n kívül, ezek max. 3 színt foglalunk le, és további két szomszéd, y és z egyszínű. (Ez megtehető, mert szomszédosak.)
Tehát x-nek marad az ötödik szám. ■

Tétel: (**4-szín tétel**) Ha G síkbarajzolható gráf $\Rightarrow$ $\boldsymbol{\chi(G) \leq 4}$
Ezt a tételt Appel és Haken bizonyította be először 1977-ben. Itt alkalmaztak először bizonyításhoz számítógépes módszereket.

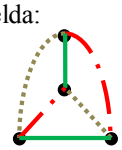
Def.: A G gráf **élgráf**ja az az $\boldsymbol{L(G)}$ gráf, aminek a csúcsai G éleinek felelnek meg, és $L(G)$ 2 csúcsa pontosan akkor van éllel összekötve, ha G megfelelő élei szomszédosak.

$\chi_e(G)$ fogalma és viszonya $\Delta(G)$-hez

Def.: A G gráf **k-élszínezhető**, ha G élei k db színnel kiszínezhetőek úgy, hogy bármely két szomszédos él színe különböző legyen. A G gráf **élkromatikus száma** $\boldsymbol{\chi_e(G) = k}$ (vagy $\chi'(G) = \chi(L(G)) \leq k$), ha G k-élszínezhető, de G nem $(k-1)$-élszínezhető (ha G élei k színnel színezhetők, de $k-1$-gyel nem).

Megj.: G k-élszínezhető $\Leftrightarrow$ $L(G)$ k-színezhető, továbbá $\boldsymbol{\chi_e(G) = \chi(L(G))}$.

Példa:



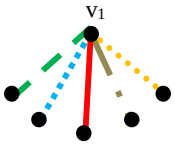
K_4
$\chi_e(K_4) = 3$

Állítás: tetsz. G gráfra $\boldsymbol{\omega(L(G)) \geq \Delta(G)}$, továbbá, ha $\boldsymbol{\Delta(G) \geq 3}$, akkor $\boldsymbol{\omega(L(G)) \geq \Delta(G)}$.

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

Állítás: $\boldsymbol{\chi_e(G) \geq \Delta(G)}$ 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: $\boldsymbol{\chi_e(G) = \chi(L(G)) \geq \omega(L(G)) \geq \Delta(G)}$.

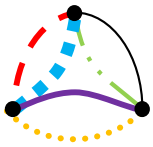


Tekintsük a gráf egy max. fokú csúcsát! (v_1)
Ennek Δ db szomszédja van. Az ezekhez húzott élek különböző színt kell, hogy kapjanak.

Vizing-tétel

Tétel: (**Vizing**) Ha G egyszerű $\Rightarrow$ $\boldsymbol{\chi_e(G) \leq \Delta + 1}$.

Ellenpélda (ha G nem egyszerű):



$\chi_e(G) = 6$
$\Delta(\mathrm{G}) = 4$
(nem egyszerű, ld. párh. élek)

vagy $\boldsymbol{C_5}$: $\chi_e(G) = 3$, $\Delta(\mathrm{G}) = 2$.

Páros gráfok élkromatikus száma (Kőnig tétele)

Tétel: (**Kőnig**) Ha $G = (A, B; E)$ páros gráf, akkor $\boldsymbol{\chi_e(G) = \Delta(G)}$.

Biz.: az előző állítás miatt elegendő azt igazolni, hogy $\boldsymbol{\chi_e(G) \leq \Delta(G)}$, azaz csupán egy $\boldsymbol{\Delta(G)}$-élszínezést kell mutatni.
∃ olyan H ps. gráf, melynek G részgráfja, és H minden csúcsának fokszáma $\boldsymbol{\Delta(G)}$. (Ilyen H-t pl. úgy kaphatunk, hogy G mellé felvesszük még G-nek egy $G' = (A', B'; E')$ másolatát, H színosztályai $A \cup B'$ és $B \cup A'$ lesznek, és $\forall\ v$ csúcs és annak v' másolata közé behúzunk további $\boldsymbol{\Delta(G) - d(v)}$ párhuzamos élt.) Ha sikerül a $\boldsymbol{\Delta(G)}$-reguláris H gráf éleit $\boldsymbol{\Delta(G)}$ színnel kiszínezni, akkor egyúttal a G részgráf éleinek is megkapjuk egy ugyanennyi színnel való színezését.
A H gráf élszínezéséhez pedig elegendő azt megmutatni, hogy tetszőleges reguláris gráfban van teljes psítás. Ugyanis akkor H egy teljes psítását kiszínezve az első színnel, a színezetlen élek egy $\boldsymbol{(\Delta(G) - 1)}$-reguláris páros gráfot alkotnak, abban is találunk egy teljes psítást, ez a második színt kapja, stb.
Miért ∃ tehát egy r-reguláris ps gráfnak teljes psítása? A Hall-feltétel teljesülését kell csupán ellenőrizni. Ha az egyik színosztályból kiválasztunk egy k pontú X halmazt, akkor az X-beli csúcsokból összesen kr él indul ki. Mindezen élekből a másik színosztály bármely csúcsa legfeljebb r-t fogadhat be, tehát a kr darab él megérkezéséhez legalább k pontra van szükség: $|N(X)| \geq |X|$. A Hall-feltétel az r-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.

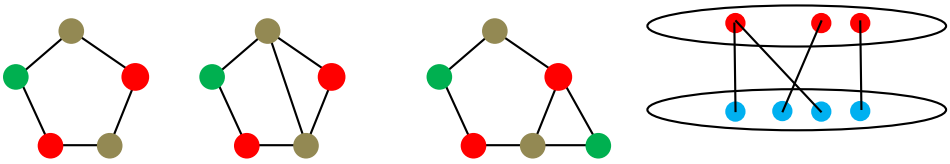
Egy gráf kromatikus száma és klikkszáma között általában nem tételeztünk fel egyenlőséget. Mégis igen sok példa van arra, amikor ez a két paraméter egyenlő (pl. páros gráfok). Felmerül a kérdés: érdemes-e közelebbről is megvizsgálni ezeket a gráfokat.
A válasz igen, ha még kikötjük, hogy ne csak magára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

Perfekt gráfok

Def.: G **perfekt**, ha G minden feszített G' részgráfjára $\chi(G') = \omega(G')$

Megjegyzés: Ez a halmaz tartalmazza magát $\boldsymbol{G}$-t is!

Példák:



$\boldsymbol{C_5}$:
$\chi(C_5) = 3$
$\omega(C_5) = 2$
nem perfekt ✖

$\omega(C_5) = 3$
$\chi(C_5) = 3$
+
∀ fesz. részgráfjára
$\chi' = \omega'$
perfekt ✓

$\chi(C_5) = 3$
$\omega(C_5) = 3$
DE nem perfekt,
mert tartalmazza
feszített részgráfként
az előző C_5-öt ✖

páros gráfok:
- ha van éle:
$\chi = \omega = 2$
- ha nincs éle:
$\chi = \omega = 1$
ps. gráfok részgráfja is
ps. → ezek perfektek ✓

Tétel: Ha G komplementere ($\bar{G}$) páros gráf, akkor G perfekt.

Biz.: Ha G páros gráf komplementere, akkor G ∀ feszített részgráfja is páros gráf komplementere, ezért elegendő azt bizonyítani, hogy $\chi(G) = \omega(G)$, ha G komplementere páros. Kőnig és Gallai tételei alapján (ps. gráfban nincs hurokél)

$$\omega(G) = \alpha(\overline{G}) = n - \tau(\overline{G}) = n - \nu(\overline{G})$$

A $\chi(G) = \omega(G)$ egyenlőség igazolásához a triviális $\chi(G) \geq \omega(G)$ egyenlőtlenség miatt elegendő a $\chi(G) \leq \omega(G)$ bizonyítása, azaz G egy $\omega(G) = n - \nu(\overline{G})$ színnel történő színezésének megadása. Ilyet pedig úgy kapunk, hogy rögzítjük $\overline{G}$-nek egy $\nu(\overline{G})$ élből álló, M maximális psítását, és ∀ csúcsot kül. színnel színezünk, kivéve, hogy M ∀ élének végpontjai azonos színt kapnak. Ezáltal a felhasznált színekben az n-hez képest $\nu(\overline{G})$ megtakarítást érünk el.

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

Biz.: Ha G páros gráf, akkor $L(G)$ élgráfjának tetszőleges feszített részgráfja azonos G egy alkalmas részgráfjának élgráfjával, azaz szintén egy páros gráf élgráfja. Elegendő tehát azt bizonyítani, hogy tetszőleges G páros gráfra $\chi(L(G)) = \omega(L(G))$. Mivel G háromszög-mentes, ezért $L(G)$ ∀ klikkje G egy csúcsból induló éleinek felel meg, így $\omega(L(G)) = \Delta(G)$. Kőnig páros gráfok élszínezéséről szóló tételének felhasználásával $\omega(L(G)) = \Delta(G) = \chi'(G) = \chi(L(G))$ következik. ■

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

Biz.: Ha G páros gráf, akkor $\overline{L(G)}$ feszített részgráfja nem más, mint $\overline{L(G')}$, ahol G' a G alkalmas részgráfja. Mivel G' páros, ezért elegendő azt igazolni, hogy $\chi\left(\overline{L(G)}\right) \leq \omega\left(\overline{L(G)}\right)$ tetszőleges G gráfra (a másik irányú egyenlőtlenség triviális).

A Kőnig-tétel alapján $\omega\left(\overline{L(G)}\right) = \alpha(L(G)) = \nu(G) = \tau(G)$, ezért elegendő $\tau(G)$ színnel kiszínezni $\overline{L(G)}$-t. Legyen $U \subset V(G)$ egy $\tau(G)$ pontból álló lefogó ponthalmaz, és válasszunk G ∀ éléhez e-nek egy U-beli végpontját. Ha ∀ élt a kiválasztott végpontnak megfelelően színezünk, akkor $\tau(G)$ színt használunk, és az azonos színű élek páronként szomszédosak, azaz a nekik megfelelő pontok $\overline{L(G)}$-ben függetlenek. Tehát ez csakugyan egy $\tau(G)$ színnel történő színezése $\overline{L(G)}$-nek.

Erős perfekt gráf tétel

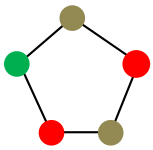
Tétel: (**Erős perfekt gráf tétel**) $\boldsymbol{G}$ perfekt ⇔ sem $\boldsymbol{G}$, sem $\overline{G}$ nem feszít (nem tart. fesz. részgr.-ként) min. 5-hosszú páratlan kört.

Bizonyítás: **(szükségesség)**

A tétel állítása átfogalmazható: $\boldsymbol{G}$ perfekt $\Leftrightarrow$ $\boldsymbol{G}$ nem tartalmaz feszített részgráfként C_{2k+1} vagy $\overline{C_{2k+1}}$ –t $(2 \leq k)$

Állítás: $(2 \leq k)$ C_{2k+1} nem perfekt.

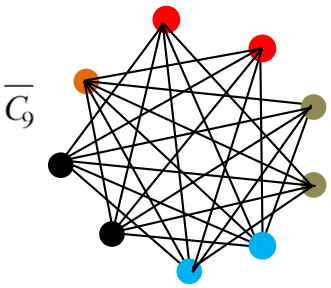
Bizonyítás:



C_5:
$\chi(C_5) = 3$
$\omega(C_5) = 2$
nem perfekt ✖
$\rightarrow \chi(C_5) \neq \omega(C_5)$

Állítás: $(2 \leq k)$ $\overline{C_{2k+1}}$ nem perfekt.

Bizonyítás:



$\overline{C_9}$

Ebben $\exists$ k csúcsból álló klikk, ha $\forall$ második pontot kiválasztjuk. De $k+1$ csúcsú nincs, mert akkor az először és utoljára kiválasztott pont nem lenne szomszédos. $\Rightarrow \omega\left(\overline{C_{2k+1}}\right) = k$
Mivel $\forall$ színt legfeljebb kétszer használhatjuk $\Rightarrow$ k színnel csak $2k$ csúcs lefesthető $\Rightarrow$ $\chi\left(\overline{C_{2k+1}}\right) \geq k+1$. **Ebből és az előbbiből következik, hogy nem perfekt.**
(Valójában $k+1$ szín elég is, tehát $\chi\left(\overline{C_{2k+1}}\right) = k+1$)

Lovász tétele

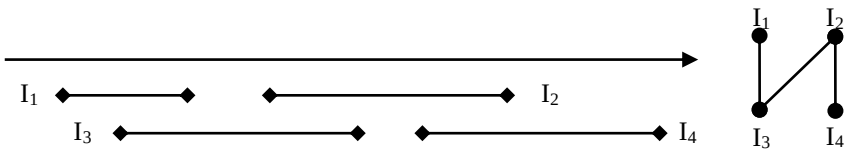
Tétel: (**Lovász gyenge perfekt gráf tétele**) G perfekt $\Leftrightarrow$ $\overline{G}$ perfekt.

Megjegyzés:

Elég csak az egyik oldalt bebizonyítani, mert „az állítás szimmetrikus”. Ha már bebizonyítottuk a $\boldsymbol{G}$ perfekt $\Rightarrow$ $\overline{G}$ perfekt irányt, akkor $H \coloneqq \bar{G}$ jelöléssel a $\bar{G}$ perfekt $\Rightarrow$ $\boldsymbol{G}$ perfekt átírható $\boldsymbol{H}$ perfekt $\Rightarrow$ $\bar{H}$ alakra. ($H = \overline{G}$, illetve $\bar{H} = \bar{\bar{G}} = G$)

Bizonyítás: (e. f. g. t. segítségével) Ha $\boldsymbol{G}$ perfekt $\Rightarrow$ $\boldsymbol{G}$ nem tartalmaz feszített részgráfként C_{2k+1} vagy $\overline{C_{2k+1}}$ –t
$\Rightarrow\Rightarrow$ $\bar{G}$ nem tartalmaz feszített részgráfként C_{2k+1} vagy $\overline{C_{2k+1}}$ –t $\Rightarrow \bar{G}$ perfekt

Intervallumgráfok perfektsége



Def.: Legyenek $I_1 = [a_1, b_1], I_2 = [a_2, b_2], \ldots, I_k = [a_k, b_k]$ korlátos és zárt intervallumok a számegyenesen.

$V(\boldsymbol{G}) \coloneqq \{I_1, I_2, \ldots, I_k\}$

I_i szomszédos I_j-vel $\Leftrightarrow$ ha ezek metszők $(i \neq j)$, tehát $I_i \cap I_j \neq 0$. Az így előálló gráfokat intervallumgráfoknak nevezzük.

Tétel: $\forall$ intervallumgráf **perfekt.**

Bizonyítás:

Mivel az intervallumgráfok feszített részgráfjai is intervallumgráfok, elég azt belátni, hogy $\chi = \omega$.
Legyen $\omega(\boldsymbol{G}) = k$, mivel $\omega(\boldsymbol{G}) \leq \chi(G)$, ezért elég azt belátni, hogy $\chi(G) \leq k$.
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 $k+1$-edik színnel kellene színezni, akkor ez azt jelenti, hogy ennek az intervallumnak a bal vége benne van már k intervallumban, amik már elhasználták az $1, 2, \ldots, k$ színt.
Így van $k+1$ intervallum, amelyek közül bármely kettő metszi egymást. $\Rightarrow \exists$ $\boldsymbol{G}$-ben $k+1$ méretű klikk.
ELLENTMONDÁS ↯

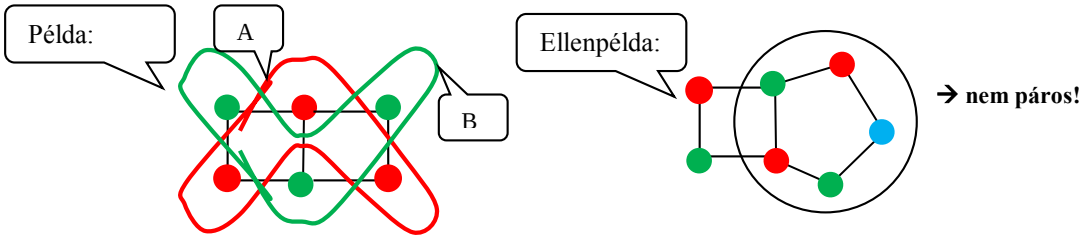
5.) Páros gráf fogalma, kapcsolat a páratlan körökkel. Párosítások páros gráfban, a javítóutak módszere, Kőnig, Hall és Frobenius tételei.

Páros gráf fogalma

Def.: G **páros gráf**, ha G két színnel színezhető, azaz ha $\chi(G) \leq 2$.

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

Jele: $G(A, B;\ E)$



Kapcsolat a páratlan körökkel

Tétel: G páros ⇔ nincs benne páratlan hosszú kör.

Bizonyítás:

⇒: Ha G páros gráf és C egy kör G-ben, akkor C pontjai felváltva vannak A-ban és B-ben.

⇐: Ha $\boldsymbol{G}$ ∀ köre páros hosszú, akkor megadhatjuk az $\boldsymbol{A}$, és $\boldsymbol{B}$ halmazt. Válasszunk egy tetszőleges $v \in V(G)$ pontot.

Legyen ez A első pontja, majd v ∀ szomszédját tegyük $\boldsymbol{B}$-be, majd ∀ eddig $\boldsymbol{B}$-ben lévő pont ∀ szomszédját tegyük $\boldsymbol{A}$-ba stb.

Ezt addig végezzük. amíg ∀ pontot el nem helyeztünk.

Ez biztosan jó elosztás, hiszen, ha lenne pl. $\boldsymbol{A}$-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 M élhalmazt (részleges) **párosítás**nak 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 élek**nek is nevezzük (páronként pontdiszjunktak). (Megjegyzés: ez a fogalom bármely gráfra értelmes, nem csak a páros gráfokra![1])

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

Bevezető/emlékeztető:

$\boldsymbol{\nu(G)}$: független élek maximális száma (legnagyobb független élhalmaz elemszáma): semelyik két élnek nincs közös pontja.

$\boldsymbol{X \subseteq V(G)}$ lefogó ponthalmaz, ha G ∀ élének legalább egyik végpontját tartalmazza.

$\boldsymbol{\tau(G)}$: lefogó pontok minimális száma (legkisebb lefogó ponthalmaz elemszáma).

$\boldsymbol{X \subseteq V(G)}$ független ponthalmaz, ha nincs benne két szomszédos pont.

$\boldsymbol{\alpha(G)}$: független pontok maximális száma (legnagyobb független ponthalmaz (semelyik 2 pont nincs közös élen) elemszáma).

$\boldsymbol{Y \subseteq E(G)}$ lefogó élhalmaz, ha G ∀ pontját lefogja.

$\boldsymbol{\rho(G)}$: lefogó élek minimális száma (legkisebb lefogó élhalmaz elemszáma).

$\boldsymbol{\nu(G) \leq \tau(G)}$.

$\boldsymbol{\alpha(G) \leq \rho(G)}$.

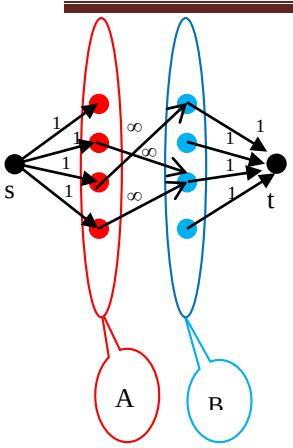
Tétel: (**Kőnig**) Ha $G = (A, B;\ E)$ véges páros gráf $\Rightarrow \boldsymbol{\nu(G) = \tau(G)}$ (Ha nincs G-ben izolált pont, akkor $\boldsymbol{\alpha(G) = \rho(G)}$ is teljesül.)

Bizonyítás:

Állítás: $\boldsymbol{G}$ véges gráf $\Rightarrow\ \nu(G) \leq \tau(G)$

Bizonyítás:

[1] http://www.cs.bme.hu/~kiskat/sza/tanacs.pdf



Legyen M G-nek egy max. párosítása (a javító utak módszerével már nem bővíthető). Ha V egy min. méretű lefogó ponthalmaz, akkor lefogja M $\forall$ élét is, de V $\forall$ pontja max. egy párosításélt fog le. $\Rightarrow |M| = \nu(\boldsymbol{G}) \leq \tau(\boldsymbol{G}) = |V|$

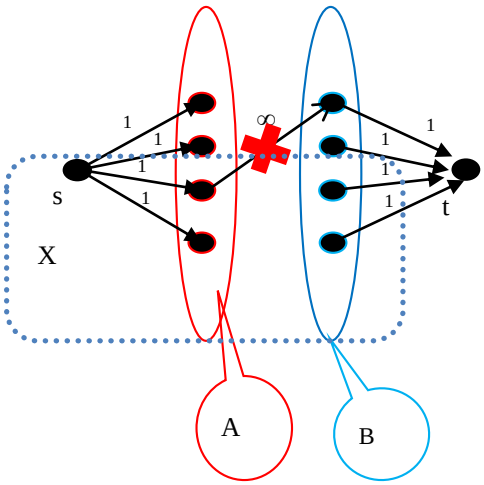
Készítsük el $\boldsymbol{G'}$-t az alábbiak szerint. Irányítsunk $\boldsymbol{G}$ $\forall$ élét $\boldsymbol{A}$-ból $\boldsymbol{B}$-be, vegyünk fel egy-egy élt $\boldsymbol{B}$ $\forall$ pontjából $\boldsymbol{t}$-be.

Adjunk $\forall$ élnek kapacitásokat: az s-ből induló, illetve t-be érkezőké legyen 1, az $\boldsymbol{A}$-ból $\boldsymbol{B}$-be futóké pedig $\boldsymbol{\infty}$ (páratlan $|\boldsymbol{A}| + 1$).

Tekintsük a $(\boldsymbol{G'}, \boldsymbol{s}, \boldsymbol{t}, \boldsymbol{c})$ hálózatot, ahol **c** előbb definiált kapacitást jelenti. Ha $\boldsymbol{G}$-ben $\exists$ $\boldsymbol{k}$ méretű párosítás $\Rightarrow \exists$ $\boldsymbol{k}$ nagyságú egészfolyam. Tehát a max. egészfolyam értéke $\nu(\boldsymbol{G})$ és az egészértékűségi lemma miatt a max. folyamérték is ugyanannyi. A **Ford-Fulkerson tétel** szerint $\exists$ $\nu(\boldsymbol{G})$ kapacitású vágás. Definiálja ezt az $\boldsymbol{s}$-t tartalmazó X! $\boldsymbol{G'}$-nek nem futhat éle $\boldsymbol{X} \cap \boldsymbol{A}$-ból $(\boldsymbol{B} \backslash \boldsymbol{X})$-be, mert akkor a vágás kapacitása végtelen volna (pontosabban min. $|A| + 1$). Tehát $(\boldsymbol{A} \backslash \boldsymbol{X}) \cup (\boldsymbol{B} \cap \boldsymbol{X})$ egy lefogó ponthalmaz:

$$\tau(\boldsymbol{G}) \leq |\boldsymbol{A} \backslash \boldsymbol{X}| + |\boldsymbol{B} \cap \boldsymbol{X}| = \nu(\boldsymbol{G})$$

Tehát: $\nu(\boldsymbol{G}) \leq \tau(\boldsymbol{G}) \wedge \tau(\boldsymbol{G}) \leq \nu(\boldsymbol{G}) \implies \nu(\boldsymbol{G}) = \tau(\boldsymbol{G})$ ✓



Összefoglalva:

$\boldsymbol{\nu(G) \leq \tau(G)}$

$\boldsymbol{\alpha(G) \leq \rho(G)}$

$\boldsymbol{\nu(G) = \tau(G)}$**, ha G páros (Kőnig-tétel)** (azaz a legnagyobb független élhalmaznak ugyanannyi eleme van, mint a legkisebb lefogó ponthalmaznak)

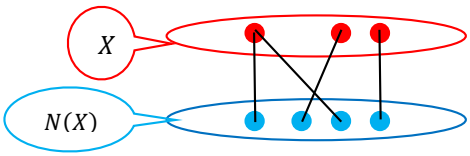
$\boldsymbol{\alpha(G) = \rho(G)}$**, ha G páros, és G-ben nincs izolált pont (Kőnig-tétel)**

	független ~ max.	lefogó ~ min.
élek	$\boldsymbol{\nu(G)}$	$\boldsymbol{\rho(G)}$
pontok	$\boldsymbol{\alpha(G)}$	$\boldsymbol{\tau(G)}$

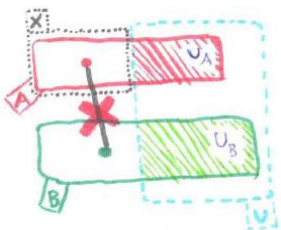
(Gallai)
~ + ~ = n, ha nincs izolált pont
~ + ~ = n, ha nincs hurokél

Hall tétele

Def.: Egy G gráfban $N(X)$ jelöli az $X \subseteq V$ ponthalmaz szomszédainak halmazát (tehát azon y pontok halmaza, amelyekhez van olyan él, melynek egyik végpontja y, a másik pedig egy X-beli pont).



Tétel: (**Hall**) $G = (A, B;\ E)$ véges páros gráf, $\exists$ A-t fedő párosítás $\Leftrightarrow$ ha $\forall$ $X \subseteq A$ ponthalmazra $|X| \leq |N(x)|$ (**Hall-feltétel**)



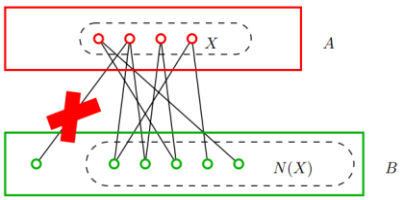
Bizonyítás:

$\Rightarrow$: A **szükségesség** nyilvánvaló: ha $\exists$ $\boldsymbol{A}$-t fedő párosítás, akkor $\forall$ **A**-beli pontnak különböző párja van. (Tehát tetszőleges $\boldsymbol{X} \subseteq \boldsymbol{A}$ esetén az $\boldsymbol{X}$-beli elemek $\boldsymbol{B}$-beli párjai az $N(x)$ egy $|\boldsymbol{X}|$ méretű részhalmazát alkotják.)

$\Rightarrow$: Tudjuk, hogy $\forall$ $\boldsymbol{X} \subseteq \boldsymbol{A}$-ra $|X| \leq |N(x)|$. Azt kell igazolni, hogy $\nu(\boldsymbol{G}) \geq |\boldsymbol{A}|$. Legyen **U** minimális lefogó ponthalmaz, tehát $\tau(\boldsymbol{G})$ méretű és $\boldsymbol{U_A} := \boldsymbol{U} \cap \boldsymbol{A}$, $\boldsymbol{U_B} := \boldsymbol{U} \cap \boldsymbol{B}$.

Mivel **U** lefogja az $\boldsymbol{X} := \boldsymbol{A} \backslash \boldsymbol{U_A}$-ból induló éleket $\Rightarrow N(x) \subseteq \boldsymbol{U_B}$, azaz $|N(x)| \leq |\boldsymbol{U_B}|$. Felhasználva a Kőnig-tételt adódik:

$$\nu(G) = \tau(\boldsymbol{G}) = |\boldsymbol{U}| = |\boldsymbol{U_A}| + |\boldsymbol{U_B}| \geq |\boldsymbol{U_A}| + |N(x)| \geq |\boldsymbol{U_A}| + |\boldsymbol{X}| = |\boldsymbol{A}|$$



Frobenius tétele

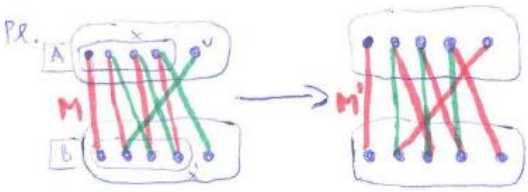
Tétel: (**Frobenius**) $G = (A, B;\ E)$ véges páros gráf, ∃ teljes párosítás ⇔ $|A| = |B|$ és ∀ $\boldsymbol{X \subseteq A}$-ponthalmazra $|X| \leq |N(x)|$.

Bizonyítás:
⇒: Triviális.
⇐: teljesül a Hall-feltétel ⇒ ∃ A-t fedő párosítás, de $\boldsymbol{|A| = |B|}$ ⇒ ez TP

A javítóutak módszere

Def.: $G(A, B;\ E)$ páros gráf, M párosítás.
Alternáló út: párosítatlan **A**-beliből indul és ∀ második éle M-beli.
Javító út: olyan alternáló út, ami párosítatlan **B**-beliben ér véget.

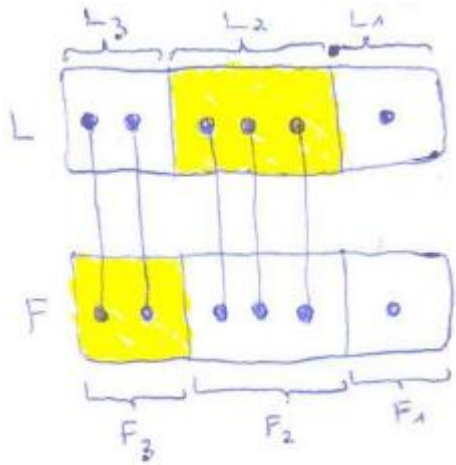
Magyar módszer: (Hatékony algoritmus max. élszám párosítás megtalálására.)
I. független élek felvétele, amíg lehet.
II. javítóút keresése és e mentén a párosítás növelése, amíg lehet.



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

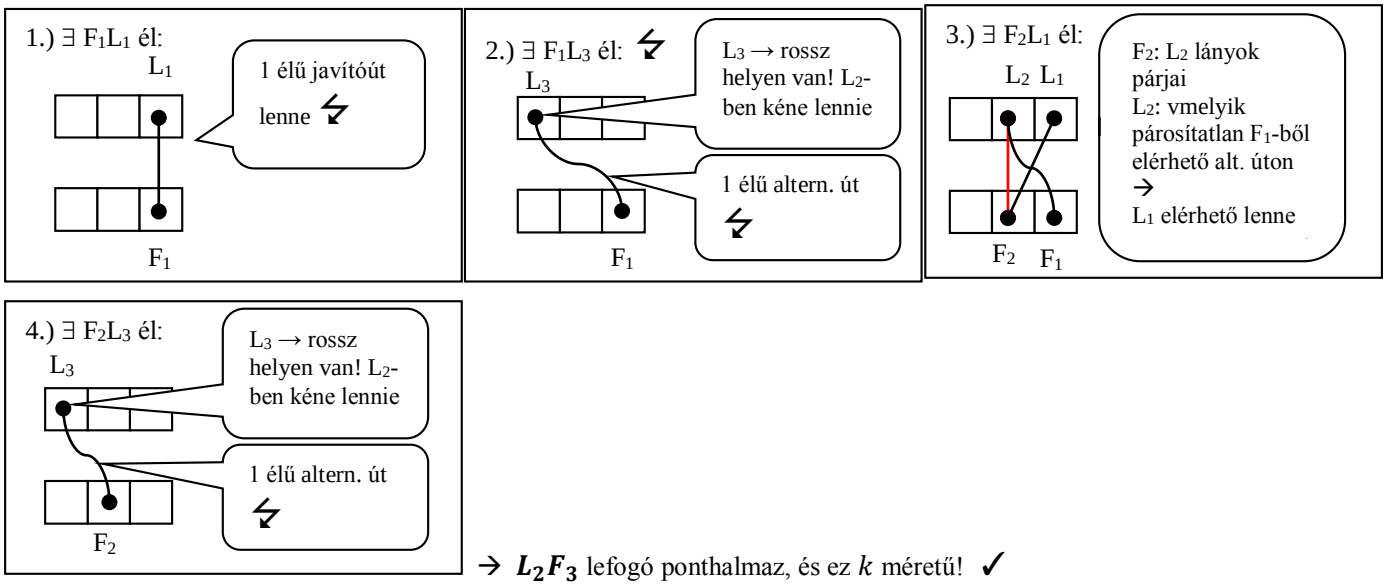
Tétel: $G(F, L;\ E)$, M párosítás. Ha nincs javító út ⇒ M max. párosítás.

Bizonyítás:
Tfh. az algoritmus k élű párosítást adott. Cél: k pontú lefogó ponthalmazt találni! Ha találunk, akkor teljesül ez: $k \leq \boldsymbol{\nu(G)} \leq \tau(\boldsymbol{G}) \leq k \implies k = \boldsymbol{\nu(G)}$
$\boldsymbol{F_1}$: párosítatlan $\boldsymbol{F}$-beliek, $\boldsymbol{L_1}$: párosítatlan $\boldsymbol{L}$-beliek,
$\boldsymbol{L_2}$: azon $\boldsymbol{L}$-beliek, amikhez $\boldsymbol{F_1}$-ből alternáló úton el lehet jutni (ekkor $\boldsymbol{L_1 \cap L_2 = \varnothing}$, mert ∄ javító út),
$\boldsymbol{F_2}$: $\boldsymbol{L_2}$-beliek párjai M szerint; $\boldsymbol{L_3 F_3}$: maradék $\boldsymbol{L \backslash F}$-beliek



Állítás: $F_1 \cup F_2$-ből nem vezet él $L_1 \cup L_3$-ba

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



→ $\boldsymbol{L_2F_3}$ lefogó ponthalmaz, és ez k méretű! ✓

Még egy kérdés.

Hogyan keressünk javítóutat?

Induljunk ki egy $\boldsymbol{A}$-beli, $\boldsymbol{M}$ által le nem fedett **u** pontból és mintha szélességi keresést végeznénk, menjünk el ennek összes szomszédjába, amiket $b_1, \ldots, b_d$ jelöljön.
Ezek nyilván mind $\boldsymbol{B}$-beli pontok és mindet lefedi $\boldsymbol{M}$. Miután $\boldsymbol{M}$ lefedi a $b_1, \ldots, b_d$ pontokat, jelölje $a_1, \ldots, a_d$ ezek M által meghatározott pontját.
Most $\forall\, a_1, \ldots, a_d$ pontból kiinduló, nem M-beli élen elérhető pontjába menjünk el.
Látható, hogy ezek éppen azok a pontok, amelyekbe vezet $\boldsymbol{u}$-ból 3 élből álló alternáló út. Lényegében BFS-t alkalmazunk.

Másként[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**.

[2] https://wiki.sch.bme.hu/images/0/04/Bsz2_tetelkidolgozas_2012tavasz.pdf

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

ld. még előző tételt!!

Def.:

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

Tétel: $\boldsymbol{\nu(G) \leq \tau(G)}$ $\forall$ $\boldsymbol{G}$ gráfra.

	ftlen ~ max.	**lef. ~ min.**
élek	$\nu(G)$	$\rho(G)$
pontok	$\alpha(G)$	$\tau(G)$

biz.: legyen M egy max. méretű ftlen élhalmaz. Mivel pusztán M éleinek lefogásához már $\nu(G) = |M|$ pontra van szükség, ezért $\tau(G) \geq M$. ■
pl.: $\nu(K_3) = 1 < \tau(K_3) = 2$.

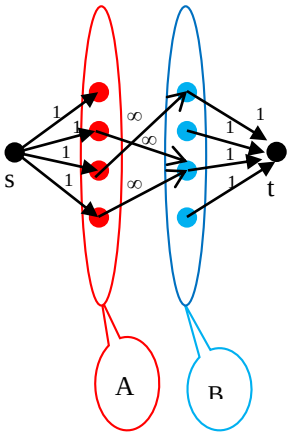
Tétel: $\boldsymbol{\alpha(G) \leq \rho(G)}$ $\forall$ $\boldsymbol{G}$ gráfra. (biz. mint előző)

Tétel: (Kőnig) Ha $G = (A, B;\ E)$ véges páros gráf $\Rightarrow \boldsymbol{\nu(G) = \tau(G)}$ (Ha nincs G-ben izolált pont, akkor $\alpha(G) = \rho(G)$ is teljesül.)

Bizonyítás:

Állítás: $\boldsymbol{G}$ véges gráf $\Rightarrow$ $\nu(G) \leq \tau(G)$

Bizonyítás:



Legyen M G-nek egy max. párosítása (a javító utak módszerével már nem bővíthető). Ha V egy min. méretű lefogó ponthalmaz, akkor lefogja M $\forall$ élét is, de V $\forall$ pontja max. egy párosításélt fog le. $\Rightarrow |M| = \boldsymbol{\nu(G) \leq \tau(G)} = |V|$

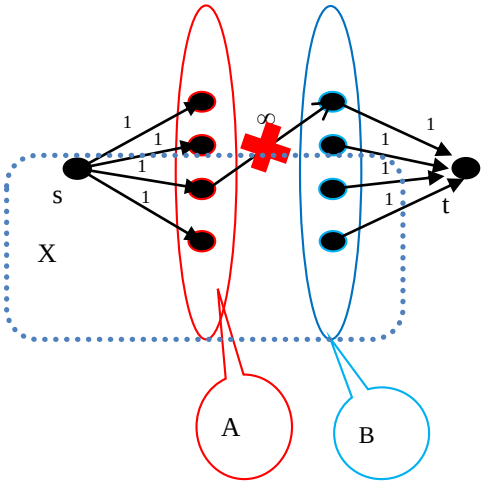
Készítsük el $\boldsymbol{G'}$-t az alábbiak szerint. Irányítsunk $\boldsymbol{G}$ $\forall$ élét $\boldsymbol{A}$-ból $\boldsymbol{B}$-be, vegyünk fel egy-egy élt $\boldsymbol{B}$ $\forall$ pontjából $\boldsymbol{t}$-be.

Adjunk $\forall$ élnek kapacitásokat: az s-ből induló, illetve t-be érkezőké legyen 1, az $\boldsymbol{A}$-ból $\boldsymbol{B}$-be futóké pedig $\boldsymbol{\infty}$ (páratlan $|\boldsymbol{A}| + 1$).

Tekintsük a $(\boldsymbol{G'}, \boldsymbol{s}, \boldsymbol{t}, \boldsymbol{c})$ hálózatot, ahol **c** előbb definiált kapacitást jelenti. Ha $\boldsymbol{G}$-ben $\exists$ $\boldsymbol{k}$ méretű párosítás $\Rightarrow \exists$ $\boldsymbol{k}$ nagyságú egészfolyam. Tehát a max. egészfolyam értéke $\nu(\boldsymbol{G})$ és az egészértékűségi lemma miatt a max. folyamérték is ugyanannyi. A **Ford-Fulkerson tétel** szerint $\exists$ $\nu(\boldsymbol{G})$ kapacitású vágás. Definiálja ezt az $\boldsymbol{s}$-t tartalmazó X! $\boldsymbol{G'}$-nek nem futhat éle $\boldsymbol{X} \cap \boldsymbol{A}$-ból $(\boldsymbol{B} \backslash \boldsymbol{X})$-be, mert akkor a vágás kapacitása végtelen volna (pontosabban min. $|A| + 1$). Tehát $(\boldsymbol{A} \backslash \boldsymbol{X}) \cup (\boldsymbol{B} \cap \boldsymbol{X})$ egy lefogó ponthalmaz:

$$\boldsymbol{\tau(G) \leq |A \backslash X| + |B \cap X| = \nu(G)}$$

Tehát: $\boldsymbol{\nu(G) \leq \tau(G) \wedge \tau(G) \leq \nu(G) \implies \nu(G) = \tau(G)}$ ✓

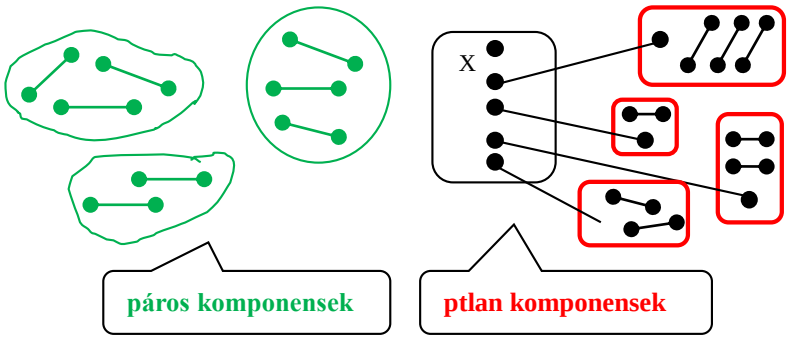


Párosítások tetszőleges gráfban, Tutte tétele

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

Tétel: (**Tutte**) G-ben ∃ **teljes párosítás** ⇔ ha ∀ $X \subseteq V(G)$-re $\boldsymbol{C_p(G-X) \leq |X|}$ ($G-X$: G-ből X-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 $\boldsymbol{C_p(G-X) > |X|}$ valamely $X \subseteq V(G)$-re), akkor G-nek **NINCS** teljes párosítása.

Bizonyítás: (***szükségesség***)



Ha elhagyjuk a gráfból X-et, akkor az eredeti gráfban a páratlan komponensek mindegyikéből legalább egy párosításbeli él indul ki, és ezek az élek csak egy-egy különböző X-beli pontban mehetnek. Tehát a $C_p(G-X) \leq |X|$. ✓

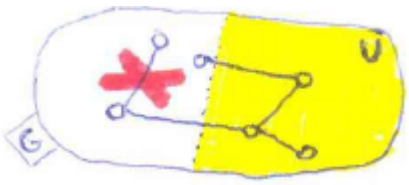
Gallai tételei

Tétel: (**Gallai**) G tetszőleges, n csúcsú
1.) $\alpha(G) + \tau(G) = n$, ha G hurokélmentes
2.) $\nu(G) + \rho(G) = n$, ha G-ben ∄ izolált pont.

Bizonyítás:

1.) Könnyen belátható, hogy $U \leq \nu(G)$ pontosan akkor lefogó ponthalmaz, ha $\nu(G) \setminus U$ független ponthalmaz. Az állítás innen közvetlenül adódik.

2.) ***G***-nek ∃ $\nu(G)$ diszjunkt éle, ezek két $\nu(G)$ pontot fognak le. A maradék $n-2$ db $\nu(G)$ pont mindegyike lefogható egy-egy új éllel (mert nincs izolált pont) ⇒ $\nu(G) + n - 2 \cdot \nu(G) = n - \nu(G)$ éllel ∀ pont lefogható ⇒ $\rho(G) \leq n - \nu(G) \implies \nu(G) + \rho(G) \leq n$.



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

Összefoglalva:
$\boldsymbol{\nu(G) \leq \tau(G)}$
$\boldsymbol{\alpha(G) \leq \rho(G)}$
$\boldsymbol{\nu(G) = \tau(G)}$**, ha G páros (Kőnig-tétel)** (azaz a legnagyobb független élhalmaznak ugyanannyi eleme van, mint a legkisebb lefogó ponthalmaznak)
$\boldsymbol{\alpha(G) = \rho(G)}$**, ha G páros, és G-ben nincs izolált pont (Kőnig-tétel)**

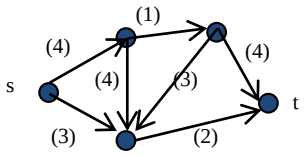
	független ~ max.	lefogó ~ min.	(Gallai)
élek	$\boldsymbol{\nu(G)}$	$\boldsymbol{\rho(G)}$	~ + ~ = n, ha nincs izolált pont
pontok	$\boldsymbol{\alpha(G)}$	$\boldsymbol{\tau(G)}$	~ + ~ = n, ha nincs hurokél

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.: **Hálózat**nak nevezünk egy olyan $(\vec{G}, s, t, c)$ négyest, amelyben $\vec{G}$ egy irányított gráf, aminek s és t különböző csúcsai, továbbá $\vec{G}$ minden e élét jellemzi egy nemnegatív $c(e)$ szám, az e él **kapacitása**. Az s és t különböző csúcsokat **termelő**nek és **fogyasztó**nak hívjuk.
Röviden: ha $\vec{G}$ irányított gráf, $s, t \in V(\vec{G})$, $c\colon E(\vec{G}) \to \mathbb{R}^+$

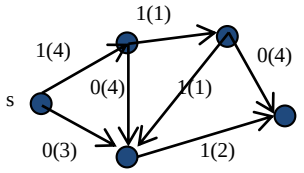
Példa:

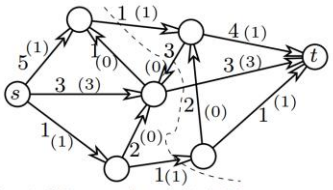


Hálózati folyam

Def.: A (G, s, t, c) hálózatban **folyam**nak mondunk egy olyan f függvényt, amely G $\forall$ éléhez egy számot rendel (pl. poz. valós számokat: $f\colon E \to \mathbb{R}^+$), amire teljesül:
1.) $0 \le f(e) \le c(e)$ teljesül $\forall\, e \in E(\vec{G})$ élre G-ben (**kapacitás-feltétel**: a folyam minden élen legfeljebb kapacitásnyi lehet), valamint
2.) $\sum\{f(uv)\colon uv \in E(G)\} = \sum\{f(vu)\colon vu \in E(G)\}$ ($\sum\{f(uv)\colon uv \in E(G)\} - \sum\{f(vu)\colon vu \in E(G)\} = 0$) áll $\forall\, v \in V(\vec{G})$, $v \neq s, t$ csúcsára ($\sum_{ve}^{\bullet\rightarrow} \mathrm{f(e)} = \sum_{ev}^{\rightarrow\bullet} \mathrm{f(e)}$). Ez a **Kirchhoff-szabály** (csomóponti törvény; elektromos hálózatoknál is használatos): minden, s-től és t-től különböző, v csúcsra csúcsra a **befolyó folyam összmennyisége azonos a kifolyó összfolyammal**, tehát egyetlen csúcsban sem keletkezik vagy tűnik el folyadék.

Példa: fvérték(kapacitás) alakban:





Hálózati folyam. A zárójelekben az f folyam által felvett értékek állnak. A folyamérték $m_f = 1 + 3 + 1 = 5$. A szaggatott vonal 5 értékű st-vágást jelöl. (A Ford-Fulkerson algoritmus másikat talál.)

Folyam értéke

Def.: f **folyam értéke** (f folyam m_f nagysága) az a nettó folyammennyiség, ami s-ből kifolyik:

$$\mathrm{m_f} = \sum\{f(sv)\colon sv \in E(G)\} - \sum\{f(vs)\colon vs \in E(G)\} = \sum_{\mathrm{se}}^{\bullet\rightarrow} \mathrm{f(e)} - \sum_{\mathrm{es}}^{\rightarrow\bullet} \mathrm{f(e)} = \sum_{\mathrm{et}}^{\rightarrow\bullet} \mathrm{f(e)} - \sum_{\mathrm{te}}^{\bullet\rightarrow} \mathrm{f(e)}$$

(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 s-t elhagyó összfolyammennyiség kiszámításához le kell vonni azt, ami s-be érkezik)
$m_f = \sum_{xe}^{\bullet\rightarrow} f(e) - \sum_{ex}^{\rightarrow\bullet} f(e)$ vagy
$m_f \coloneqq \sum\{f(sv)\} - \sum\{f(vs)\}$, $v \in V(G)$
Egy e élet egy folyamban **telített**nek hívunk, ha $f(e) = c(e)$, és **telítetlen**nek, ha $f(e) < c(e)$.

Vágás

Def.: Legyen G csúcsainak s-t tartalmazó, de t-től diszjunkt részhalmaza ($X \subseteq V(\vec{G})$, $s \in X \not\ni t$).
Az X és $V(\vec{G}) \setminus X$ között futó élek C halmazát a hálózat egy **st-vágás**ának nevezzük (jele: C).

Vágás kapacitása

Def.: vágás kapacitása, vagyis *C értéke*:

$$c(C) = \sum_{\substack{\rightarrow \\ xe}} c(e)$$

Az X által meghatározott ***st*-vágás kapacitása** az X-ből $V \setminus X$-be futó (előremutató) élek kapacitásösszege, azaz $\sum\{c(xv)\colon\ x \in X \not\ni v \in V(G)\}$.

Az X által meghatározott st-vágás kapacitása **felső korlát a lehetséges folyamnagyságra**. Sőt, tetszőleges f folyam m_f folyamnagysága meghatározható úgy, hogy az X-ből $V(\vec{G}) \setminus X$ –be futó éleken haladó összfolyam-mennyiségből levonjuk a $V(\vec{G}) \setminus X$-ből X-be továbbított folyammennyiséget.

$m_f = \sum\{f(xv) : x \in X \not\ni v \in V(G)\} - \sum\{f(vx) : x \in X \not\ni v \in V(G)\}$, továbbá

$m_f \leq \sum\{c(xv)\colon\ x \in X \not\ni v \in V(G)\}$.

Algoritmus a maximális folyam és a minimális vágás megkeresésére

Állítás: Ha egy hálózatban f folyam, C vágás $\Rightarrow$ f értéke $(= mf) \leq C$ vágás értéke $(= c(C))$,
tehát $mf \leq c(C)$

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

Algoritmus:

I. Kiindulunk egy tetszőleges folyamból (Pl.: $f \equiv 0$)

II. Javítás (amíg lehet) $\Rightarrow$ m_f nő

III. Ha nincs több javítás $\Rightarrow$ STOP

A javítást egy ún. **segédgráf**fal tudjuk elvégezni.

Def.: a $(\vec{G}, s, t, c)$ hálózat f folyamához tartozó $\overrightarrow{H_f}$ segédgráf:

$V(\overrightarrow{H_f}) = V(\vec{G})$, tehát $\overrightarrow{H_f}$ segédgráf csúcsai megegyeznek $\vec{G}$ csúcsaival.

1.) $\left.\begin{matrix} \overrightarrow{xy} \in E(\vec{G}) \\ f(\overrightarrow{xy}) < c(\overrightarrow{xy}) \end{matrix}\right\} \Rightarrow \overrightarrow{xy} \in \overrightarrow{H_f}$, azaz ha $\vec{G}$-ben az $\overrightarrow{xy}$ él értéke kevesebb, mint az él kapacitása, akkor $\overrightarrow{H_f}$-ben is fusson él x-ből y-ba.

2.) $\left.\begin{matrix} \overrightarrow{xy} \in E(\vec{G}) \\ f(\overrightarrow{xy}) > 0 \end{matrix}\right\} \Rightarrow \overrightarrow{yx} \in \overrightarrow{H_f}$, azaz ha $\vec{G}$-ben az $\overrightarrow{xy}$ él értéke nagyobb, mint 0, akkor $\overrightarrow{H_f}$-ben fusson „**visszaél**” y-ból x-be.

Javítóút: $\overrightarrow{H_f}$-ben **irányított út s-ből t-be**.

Ha $\exists\ P$ javítóút, akkor ***növelhetjük* a folyam értékét**:

$d := \min(\{c(e) - f(e)\colon e \in P,\ e(1)\text{-es}\} \cup \{f(e)\colon e \in P,\ e(2)\text{-es}\})$, megnézzük, az eredeti $\vec{G}$ gráfban mennyi a minimális érték, amennyivel lehet növelni a javítóút élein átmenő folyam értékét.

$$f(e) = \begin{cases} f(e) + d, & \text{ha } e \in P,\ e(1)\text{-es} \\ f(e) - d, & \text{ha } e \in P,\ e(2)\text{-es, tehát „előreél” esetén növelni, „visszaél” esetén csökkenteni kell az adott él értékét.} \\ f(e), & \text{ha } e \notin P \end{cases}$$

Így meg is növeljük a folyam értékét, majd újabb javítóutat keresünk.

Fontos kiegészítés az „algoritmus” III. pontjához:

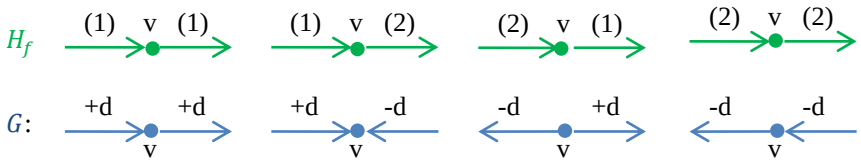
Ha van egy olyan irányított út s-ből t-be, amelynek $\forall$ éle telítetlen (vagyis $f(e) < c(e)\ \forall\ e \in P$), akkor ezen út mentén a folyam értékét $\forall$ élen megnövelhetjük annyival, hogy az egyik él telített legyen. Ha nincs erre lehetőség, akkor ezután alkalmazzuk a segédgráfos módszert.

Amennyiben nincs további javítóút, megtaláltuk az s-ből t-be futó maximális folyamot (ld. még később). A minimális vágás pedig azon pontok halmaza, melyek az utolsó felrajzolt segédgráfon még elérhetőek s-ből.

Állítás: a segédgráfos javítás után f folyam marad.

Bizonyítás:

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



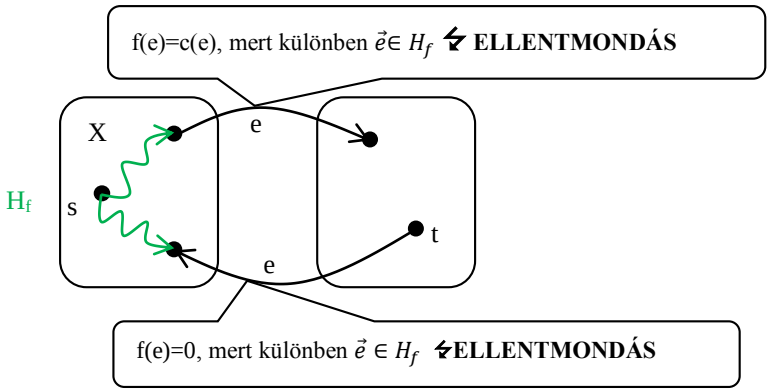
Tétel: Ha nincs javítóút H_f-ben $\Leftrightarrow$ f maximális folyam

Bizonyítás:

Tfh. az algoritmus t értékű folyamot adott: $m_f = t$.

Cél: mutassunk t értékű vágást.

X ≔ azon pontok halmaza, ahová H_f-ben s-ből vezet irányított út $\Rightarrow s \in X \not\ni t$



A fentiekből következik:

$$m_f = \sum_{\substack{\bullet\rightarrow \\ x}} f(e) - \sum_{\substack{\rightarrow\bullet \\ x}} f(e) = \sum_{\substack{\bullet\rightarrow \\ x}} c(e) - \sum_{\substack{\rightarrow\bullet \\ x}} 0 = c(C) = t$$

Ford-Fulkerson-tétel

Tétel: (**Ford-Fulkerson**)

$\underbrace{\max m_f}_{f\ folyam} = \underbrace{\min c(C)}_{c\ vágás}$, vagyis a maximális folyamnagyság egyenlő a minimális vágás kapacitásával.

($MF = MC$, max-flow=min-cut)

Másként: ha (G, s, t, c) véges hálózat, ∃ egy f folyam és egy $s \in X \subseteq V\backslash\{t\}$ részhalmaz úgy, hogy az m_f folyamnagyság egyenlő az X által definiált st-vágás kapacitásával.

Bizonyítás:

A maximális folyam nyilván nem lehet nagyobb a minimális vágásnál ($\max m_f \leq \min c(C)$), hiszen ha ∀ előremutató él telített, a visszafelé mutatókon pedig 0 a folyam értéke, akkor ezen a vágáson nem folyhat át több. Az előző tételben pedig láttuk, hogyha létezik egy f maximális folyam, akkor van ilyen értékű vágás. ✓

Edmonds-Karp tétel

Tétel: (**Edmonds-Karp**)

Ha H_f-ben mindig a legrövidebb javítóutat választjuk, akkor az algoritmus véges sok lépésben leáll és polinomiális lépésszámú.

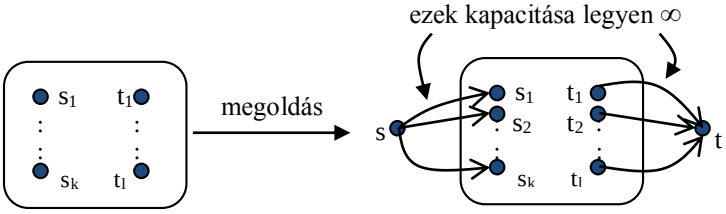
Egészértékűségi lemma

Tétel: (**Egészértékűségi lemma**): Ha ∀ e élre $c(e)$ egész (kapacitások egész számok) $\Rightarrow$ ∃ olyan m_f max. folyam, amire ∀ e élre $f(e)$ egész.

Bizonyítás: Az algoritmus nem lép ki ℕ-ből (csupa 0-ból indítva).

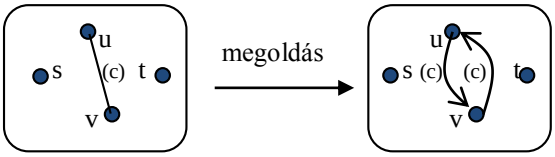
A folyamprobléma általánosításai

1.) **több termelő/fogyasztó is van**



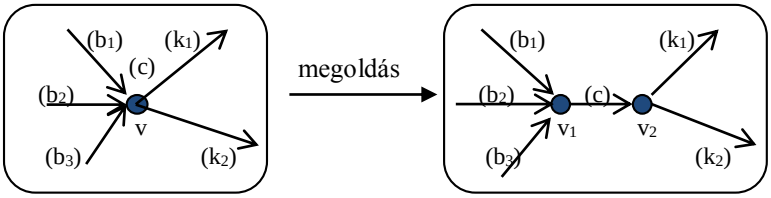
Felveszünk egy „szupertermelőt”(S)/„szuperfogyasztót”(T), amelyeket összekötünk a termelőkkel/fogyasztókkal végtelen kapacitású éleken. Az így kapott gráfban keresünk maximális folyamot (S-ből T-be), majd ha megtaláltuk, letöröljük a két pontot.

2.) **irányítatlan élek is vannak**



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.

3.) **kapacitással rendelkező csúcsok**



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 k kapacitással rendelkező v pontot két másik ponttal helyettesítjük, amiket egy k kapacitású él köt össze. A két új pontból az egyikbe futnak a v-be bejövő élek, a másikból futnak ki a v-ből kimenő élek.

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

Def.: a G irányított/irányítatlan gráf u pontjából v pontjába futó P és Q útjait **éldiszjunkt**aknak (**élidegen**nek) nevezzük, ha $E(P) \cap E(Q) = 0$, vagyis ha nincs közös élük.

Def.: a G irányított/irányítatlan gráf u pontjából v pontjába futó P és Q útjait **pontdiszjunkt**aknak (**pontidegen**nek/függetlennek) nevezzük, ha $V(P) \cap V(Q) = \{u, v\}$, vagyis ha nincs közös csúcsuk, a kezdő- és végpontjukat leszámítva.

Def.: a G irányított/irányítatlan gráf U **ponthalmaza** (ill. F **élhalmaza**) **lefog** $\forall\, uv$**-utat**, ha a $\boldsymbol{G - U}$ (ill. $\boldsymbol{G - F}$) gráfban $\nexists\, u$-ból v-be (irányított) út.

Menger pontpárok közötti diszjunkt utakra vonatkozó tételei

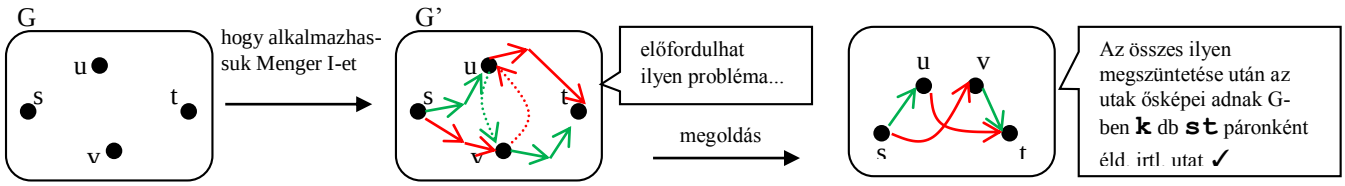
Az él-összefüggőségi változat irányított gráfokban

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

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

Az él-összefüggőségi változat irányítatlan gráfokban

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



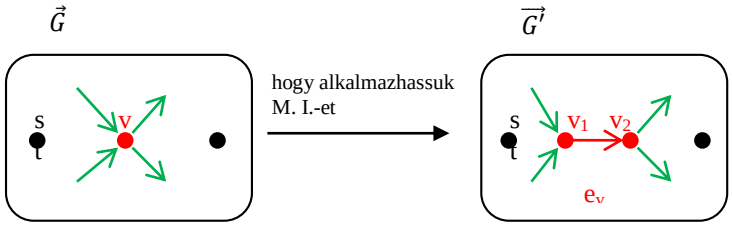
Bizonyítás:
Készítsük el a $\boldsymbol{G'}$-t $\boldsymbol{G}$-ből úgy, hogy $\boldsymbol{G}$ $\forall$ élét irányítjuk oda és vissza.
Ha $\boldsymbol{G'}$-ben van $\boldsymbol{k}$ db él, melyek lefognak $\boldsymbol{k}$ db $\boldsymbol{st}$ irányított éldiszjunkt utat ⇒ ezek ősei lefogják az $\boldsymbol{st}$ utakat $\boldsymbol{G}$-ben.

A csúcs-összefüggőségi változat irányított/irányítatlan gráfokban

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

Bizonyítás:

M.III.:

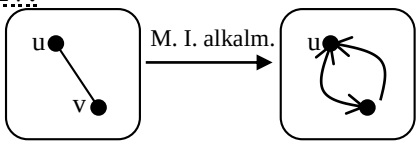


Ha $\overrightarrow{G'}$-ben van k éldiszjunkt st út ⇒ $\vec{G}$-ben van k db pontdiszjunkt út.

Probléma: ha $\overrightarrow{G'}$-ben van k db él, melyek lefogják az st utakat, akkor ezek $\vec{G}$-ben pontok vagy élek?

Megoldás: válasszunk k db piros lefogó élt! $\Rightarrow$ ezek képei $\vec{G}$-ben k db lefogó pont. ✓

M.IV:



✓

Többszörös összefüggőség és élösszefüggőség fogalma, Menger ezekre vonatkozó tételei

Def:

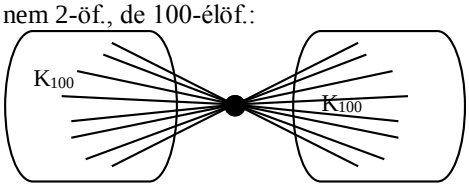
G k-szorosan élösszefüggő (k-élösszefüggő), ha bárhogyan legfeljebb $k-1$ élét elhagyva összefüggő marad.
G k-szorosan pontösszefüggő (k-összefüggő) ha bárhogyan legfeljebb $k-1$ pontját elhagyva összefüggő marad és legalább $\boldsymbol{k+1}$ pontja van.

k-élösszefüggő $\Rightarrow k-1$-élösszefüggő és
k-(pont)összefüggő $\Rightarrow k-1$-(pont)összefüggő.

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

Állítás: k-összefüggő $\Rightarrow$ k-élösszefüggő.

Ellenpélda:
nem 2-öf., de 100-élöf.:



Tétel: (**Menger V., VI.**)

M. V.: G k-élösszefüggő $\Leftrightarrow$ bármely 2 pont között $\exists$ k db páronként éldiszjunkt út.
M. VI.: G k-(pont)összefüggő $\Leftrightarrow$ bármely 2 pont között $\exists$ k db páronként pontdiszjunkt út és $\boldsymbol{k+1}$ pontja van.

Bizonyítás:

$\Leftarrow$: (**M. V.**, **M. VI.**): $k-1$ él/pont elhagyásakor tetszőleges s −ből t −be van út, mert volt k db éldiszjunkt/pontdiszjunkt út, $k-1$ törlése csak $k-1$ −et ronthatott el.
$\Rightarrow$: (**M. V.**): Tfh. s, t között nincs k db éldiszjunkt út $\Rightarrow$ st irányítatlan utak maximális száma $\leq k-1 \Rightarrow$ st utakat lefogó élek minimális száma $\leq k-1 \Rightarrow$ le lehet fogni $\leq k-1$ éllel az st utakat $\Rightarrow$ $k-1$ élt törölve nincs st út!
→ *ELLENTMONDÁS* ↯
$\Rightarrow$: (**M. VI.**): Tfh. s −ből t −be legfeljebb $k-1$ pontdiszjunkt út van!
Ha st nem szomszédos, akkor **M. IV.** miatt az st utak lefoghatók maximum ponttal. Ezek elhagyásakor G szétesne.
→ *ELLENTMONDÁS* ↯
Ha st szomszédos, akkor st él törlése után keletkező G' gráf legfeljebb $k-2$ pontdiszjunkt st utat tartalmaz, tehát **M. IV.** szerint létezik $k-2$ pontja, aminek elhagyásakor szétesik. A szétesett gráfban ismét összekötve az s és t pontokat egy legalább 3-pontú gráfot kapunk (mert G-nek minimum $k+1$ pontja volt), mely az st él törlésétől szétesik. De ekkor az st él helyett s vagy t valamelyike is törölhető, hogy a gráf szétessen. Ismét azt kaptuk, hogy G legfeljebb $k-1$ alkalmas pont törlésével szétesik, ami a k −szoros összefüggőségnek ELLENTMOND.

Tétel: (**Dirac**) Ha G **k-összefüggő** és $2 \leq k \Rightarrow G$ bármely k pontján keresztül található kör G-ben.

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

Gráfok szomszédossági mátrixa

Def.: A G gráf **szomszédossági mátrixa** (adjacenciamátrixa) az a $V(G) \times V(G)$ méretű mátrix, aminek (i,j) pozícióján az i és j közti élek száma áll ($i = j$ esetén a hurokélek számának kétszerese). A G gráf véges, ha $V(G)$ és $E(G)$ is véges halmazok.

Megjegyzés:

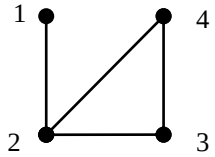
Ha nincs hurokél a gráfban, akkor a főátló csupa 0. Ha a gráf egyszerű gráf (nincsenek többszörös élek), akkor a mx.-ban csak 0 és 1 szerepelhet.

Ha G irányítatlan, akkor A szimmetrikus a főátlóra: $A = A^T$ (uaz, mint a transzponáltja, vagyis főátlóra történő tükrözése, vagyis $a_{i,j} = a_{j,i}$).

Ha G irányított ($A(G) = (a)_{i,j} \in \mathbb{R}^{V \times V}$, $\boldsymbol{a_{i,j}}$ jelentése: az i csúcsból j csúcsba hány él mutat), v_i pontjának ki-/befoka a mátrix $i.$ 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 $a_{i,j} \neq a_{j,i}$, ha i-ből nem vezet j-be él, de j-ből i-be igen, vagy fordítva).

$$\boldsymbol{a_{i,j}} = \begin{cases} 0, \text{ ha } v_i \text{ és } v_j \text{ nem szomszédos,} \\ k, \text{ ha } v_i \text{ és } v_j \text{ között k db pontdiszjunkt él fut,} \\ l, \text{ ha } i = j \text{ és } l\ db \text{ hurokél illeszkedik rá.} \end{cases}$$

Példa:



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

A szomszédossági mátrix hatványainak jelentése

Tétel: Ha $G = (V,E)$ *irányított* gráf, akkor az $\underline{A^k}$ **mátrix** (i,j) pozíciójában álló $(A^k)_j^i$ eleme az i**-ből** j**-be vezető** k **élű séták** (k hosszú élsorozatok) száma (út, amely ismétlést tartalmazhat).

Bizonyítás: **Teljes indukcióval**:

$k = 1$-re A definíciójából nyilvánvaló. Tfh. A^k-ra már bebizonyítottuk az állítást.

Az i-ből j-be vezető $k+1$ élű séták száma:

$$\sum_{w \in V} (k \text{ élű } iw \text{ séták száma}) \cdot (wj \text{ élek száma}) \underbrace{=}_{\text{indukciós feltevésből}} \sum_{w \in V} (A^k)_i^w \cdot (A^k)_w^j \underbrace{=}_{\text{mx.szorzás}} (A^{k+1})_i^j$$

Következmény:

➡G egyszerű, irányítatlan gráf $\Rightarrow A^2$: 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 $\forall\, v \in V(G)$-re $(A^2)_v^v = d(v)$.)

➡A hurokélmentes gráfoknál A^3 főátlóbeli elemeinek összege a gráfban található 3-hosszú körök (háromszögek) számának 6-szorosa.

(NEM KELL) **Tétel:** Ha G irányítatlan gráf és λ_1 az A legnagyobb sajátértéke, akkor a $\lambda_1 \leq \Delta$; továbbá $\lambda_1 = \Delta$ reguláris gráfokban.

Bizonyítás:

Legyen $\underline{\boldsymbol{x}} = (x_1, \dots, x_n)$ egy λ_1-hez tartozó sajátvektor, és k-adik eleme a legnagyobb.

Mivel $\underline{\boldsymbol{x}} \neq \underline{\boldsymbol{0}}$, ezért (esetleg a $-\underline{\boldsymbol{x}}$ sv.-ra áttérve) feltehető, hogy x_k pozitív.

Ekkor:

$\lambda_1 \cdot x_k = (A)_k \cdot \bar{x} = \sum_{i=1}^n a_{k,i} \cdot x_i \leq \sum_{i=1}^n a_{k,i} \cdot x_k = x_k \cdot \sum_{i=1}^n a_{k,i} = x_k \cdot d(v_k) \leq x_k \cdot \Delta \implies \lambda_1 \leq \Delta$ ✓

Ha G Δ-reguláris, akkor az egységvektor a Δ sajátértékhez tartozó sajátvektor, mert a fenti egyenlőtlenségek egyenlőséggel teljesülnek. ✓

Irányított gráf illeszkedési mátrixa

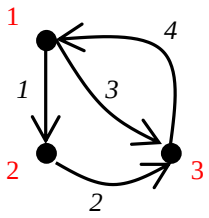
Def: A $G = (V,E)$ *irányított* gráf **illeszkedési mátrixa** (incidenciamátrixa) $B(G) \in \mathbb{R}^{V \times E}$, amire:

$$\big(B(G)\big)_v^e = \begin{cases} 1, & \text{ha } v \text{ az } e \text{ kezdőpontja} \\ -1, & \text{ha } v \text{ az } e \text{ végpontja} \\ 0, & \text{egyébként} \end{cases}$$

ha G *irányítatlan*, akkor:

$$(B)_v^e = \begin{cases} 1, & ha\ v\ az\ e\ végpontja \\ 0, & egyébként \end{cases}$$

Példa:



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

(NEM KELL) **Tétel**: A $\boldsymbol{G}$ n pontú irányított hurokél mentes c komponensű gráfnál $\boldsymbol{r(B) = n - c}$.

Bizonyítás:

Ha $1 < c$, akkor komponensenként sorolva fel a pontokat és éleket, B blokkdiagonális szerkezetű lesz.
Elég tehát egy p pontú komponensre belátni, hogy a neki megfelelő blokk rangja $p - 1$.
Mivel a blokk p sorból áll és összege a **0**-t adja, a rang $\leq \boldsymbol{p - 1}$.
Legyen F egy p pontú, $p - 1$ élű feszítőfa ebben a komponensben.
Legyen v_1 egy elsőfokú pont F-ben és $e1$ a hozzáilleszkedő él.
Legyen v_2 egy elsőfokú pont $F - \{v_1\}$-ben és $e2$ a hozzáilleszkedő él, stb.
Ha a blokk sorait $v_1, v_2, \ldots$ sorrendben soroljuk fel, oszlopait $e_1, e_2, \ldots$ felsorolásával kezdjük, akkor egy $p \times (p-1)$ méretű részmátrixot kapunk, amelyből az utolsó sor elhagyásával egy alsóháromszög mátrixot kapunk, melynek főátlóbeli elemei ± 1 értékűek $\Rightarrow$ találtunk $p - 1$ lineárisan független oszlopot.

Egy példa a blokkdiagonális szerkezetű mátrixra:

$$\begin{pmatrix} 7 & 9 & 0 & 0 \\ 4 & 2 & 0 & 0 \\ 0 & 0 & 8 & 6 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Tétel: Az n pontú öf. hurokélmentes ir. G gráf illeszkedési mátrixában $n - 1$ oszlop akkor és csak akkor lineárisan független, ha a megfelelő $n - 1$ 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 $\Rightarrow$ 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. $\Rightarrow$ összegük **0**-t adja.

$$A = \begin{pmatrix} a & 0 & \cdots & -x \\ -a & b & \cdots & 0 \\ 0 & -b & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \cdots & 0 \end{pmatrix};\ a, b, \ldots, x \in \{-1, +1\}$$

(NEM KELL) **Def**: **redukált illeszkedési mátrix**: az eredeti ill. mx. egy sorának elhagyásával kapott ill. mx. Jele: $B_0(\vec{G})$

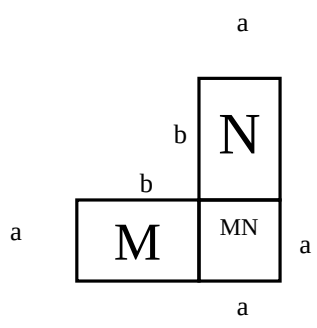
(NEM KELL) **Tétel**: Az n pontú öf. ir. G gráfnál $\det(B_0 \cdot B_0^t)$ = feszítőfák száma.

Bizonyítás:

Felhasználjuk a **Cauchy—Binet -tétel**t:

$$\det(MN) = \sum \binom{b}{a} - féleképp \det(M') \cdot \det(N'),$$

ahol M'-t/N'-t úgy, ahol M'-t/N'-t úgy kapjuk, hogy az eredetiből elhagyunk $(b - a)$ oszlopot/sort, hogy $a \times a$ méretű mx-ot kapjunk.



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

Ezek után a tétel állítása nyilvánvaló: B_0-ból mindenképp kiválasztva $n-1$ oszlopot, épp a fának megfelelő részmátrixok determinánsa lesz $\neq 0$, és egy ilyen determináns értéke ± 1, tehát a négyzete 1.

Példa: $G = K_n$ n pontú teljes gráf

$$B_0 \cdot B_0^t = \begin{pmatrix} n-1 & n-1 & \cdots & -1 \\ -1 & n-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ -1 & n-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & n & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & n \end{pmatrix}$$

A tétel felhasználásához nem szükséges a B_0 mátrixot felírnunk. A $B_0 \cdot B_0^t = (d_{i,j})$ elemeit az alábbi képlet előállítja:

$$d_{i,j} = \begin{cases} d(P_i), & ha\ i = j \\ -(az\ i\ és\ j\ élek\ közt\ vezető\ élek\ száma), & ha\ i \neq j \end{cases}$$

(utsó végösszeg): $det(B_0 \cdot B_0^t) = n^{n-2}$ → 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, $\pi(n)$ nagyságrendje (biz. nélkül). Kongruencia fogalma, alapműveletek kongruenciákkal

Oszthatóság, felbonthatatlan és prímtulajdonságú számok, ezek kapcsolata

Def.: a osztója b-nek, ha $\exists\, c \in \mathbb{Z}$, melyre $a \cdot c = b$. Jele: $a|b$. (Pongyolán: „a megvan b-ben valahányszor".)

p **felbonthatatlan** ($|p| \neq 1$), ha $p = a \cdot b \rightarrow |a| = 1$ vagy $|b| = 1, a, b \in \mathbb{Z}$ (p felbonthatatlan, ha minden olyan esetben, amikor előáll két egész szám szorzataként, a szorzatnak legalább az egyik tényezőjének abszolútértéke 1. Csak triviális osztói vannak.)

p **prímszám** ($|p| \neq 1$), ha $p|a \cdot b \rightarrow p|a$ vagy $p|b$ (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 6 nem prím, mert $6|8 \cdot 9, de\ 6 \nmid 8$ és $6 \nmid 9$.
Felbonthatatlan: $2, -5, 11$, nem az: $-1, -9 = 3 \cdot (-3)$

Tétel: p prím$\Leftrightarrow$ p felbonthatatlan

Bizonyítás:

$\Longrightarrow$: p prím, $p = a \cdot b$
$p|a \cdot b \Rightarrow p$ prím, ha
1.) $p|a$ és a$|p \Rightarrow |a| = |p| \Rightarrow |b| = 1$ ✓
2.) $p|b$ és $b|p \Rightarrow |b| = |p| \Rightarrow |a| = 1$ ✓
$\Longleftarrow$: nem kell vizsgán

A számelmélet alaptétele

Tétel: (**számelmélet alaptétele**) természetes számok körében: minden n egész szám ($2 \leq n \in \mathbb{N}$, 1-nél nagyobb természetes szám) a sorrendtől és előjelektől eltekintve egyértelműen felbontható felbonthatatlanok sorozatára.
egész számok körében: ha egy z egész számra $|z| > 1$, akkor z előáll felbonthatatlan számok szorzataként, és a z ilyen előállításai csak a tényezők sorrendjében és előjeleiben különbözhetnek.
Pl.: $-24 = 2 \cdot 3 \cdot (-2) \cdot 2 = (-3) \cdot (-2) \cdot (-2) \cdot 2 = (-2)^3 \cdot 3$

Bizonyítás:

(felbonthatóság)

n ∴ felbonthatatlan ✓
∵ a, b felbonthatatlan ✓
$n = a \cdot b$ ∴ ∴ $a_1 \cdot a_2 \cdot b$ felbonthatatlan ✓
∵ $n = a_1 \cdot a_2 \cdot b$ ∵
...

(egyértelműség)
Tfh. n két különböző módon felbontható:
$n = p_1 \cdot p_2 \cdot \ldots p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l$
p_1 prím; $p_1|q_1 \cdot q_2 \cdot \ldots \cdot q_l \Rightarrow p_1 q_1$ vagy $p_1 q_2$ vagy ... vagy $p_1 q_l$
Pl.: $p_1|q_1$, de q_1 felbonthatatlan , $q_1 = p_1 \cdot c \Longrightarrow |p_1| = 1$, de $|p_1|$ prím, nem lehet 1! ↯
vagy
$|c| = 1 \Longrightarrow$ ez azt jelenti, hogy $|p_1| = |q_1|$
→visszavezettük a problémát egy egyszerűbb esetre:

$$p_2 \cdot p_3 \cdot \ldots p_k = q_2 \cdot q_3 \cdot \ldots \cdot q_l$$

→erre ismét alkalmazzuk az algoritmust, egészen addig, amíg mindegyiknél ki nem derül, hogy egyenlőek. ✓

Következmény: prímtényezős felbontás / **kanonikus alak**: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$
kan. alakban $p_1 \cdot p_2 \cdot \ldots p_k$ kül. pozitív felbonthatatlanok, $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{Z}^+$; ált. $p_1 < p_2 < \cdots < p_k$
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: $d(n)$
pl.: $n = 2^3 \cdot 3^2 \cdot 7^4$

		0
0		1
1	0	2
2	1	3

$d|n$, ha $d = 2^3 \cdot 3^2 \cdot 7^4$, $d(172\,872) = d(2^3 \cdot 3^2 \cdot 7^4) = (3+1)(2+1)(4+1)$
vagy $d(72) = d(2^3 \cdot 3^2) = (3+1)(2+1) = 12.$
általánosan: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, $\boldsymbol{d(n) = (\alpha_1+1)\cdot(\alpha_2+1)\cdot\ldots\cdot(\alpha_k+1) = \prod_{i=1}^{k}(\alpha_i+1)}$
Tehát: a szám kanonikus alakjában szereplő hatványkitevők eggyel növelt értékeinek szorzata megaja a szám osztóinak számát.

Osztók összege: jele: $\sigma(n)$ (csak a pozitív osztókat vesszük figyelembe)

pl.: $n = 36 = 2^2 \cdot 3^2$,
$\sigma(36) = (2^0+2^1+2^2)(3^0+3^1+3^2) = 91$
általánosan: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$,

$$\sigma(n) = (1+p_1+p_1^2+\cdots+p_1{}^{\alpha_1})\cdot(1+p_2+p_2^2+\cdots+p_2{}^{\alpha_1})\cdot\ldots\cdot(1+p_k+p_k^2+\cdots+p_k{}^{\alpha_1}) = \frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\ldots\cdot\frac{p_k^{\alpha_k+1}-1}{p_k-1}$$
$$= \prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1}$$

Prímek száma

Tétel: ∞ sok prímszám ∃ (Euklidész).

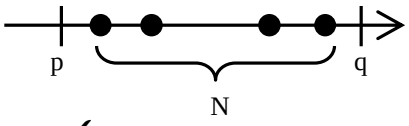
Biz.: (indirekt) tfh. véges sok van: $p_1, p_2, \ldots, p_n$. $A := p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ → nagyobb → A-nak van prímosztója, de A $p_1 \cdot p_2 \cdot \ldots \cdot p_n$ –nel osztva 1 maradékot ad. ↯
Másképp: elegendő megmutatni, hogy $\forall 2 \le n \in \mathbb{N}$-re ∃ n-nél nagyobb prím. Mivel $n!$ az $1,2,\ldots,n$ számok mindegyikével osztható ⇒ $N := n! + 1$ az $1,2,\ldots,n$ számok mindegyikéhez relatív prím, tehát N nem osztható egyetlen n-nél kisebb prímmel sem. N kan. alakjában csak n-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: $\forall N$-re ∃ p, q szomszédos prímek, amelyekre $N \le |p-q|$.
Tetsz. hosszú sorozat képezhető szomszédos összetett számokból → bármely $n \in \mathbb{N}$ -re ∃ olyan N, melyre az $N+1, N+2, \ldots, N+n$ számok mindegyike összetett.

Biz.: azaz: ∃ N db szomszédos összetett szám



$2|(N+1)!+2$
$3|(N+1)!+3$
⋮
$N+1|(N+1)!+N+1$
} N db, mindegyik összetett ✓

Legyen $N := (n+1)! + 1$. → tetsz. $2 \le k \le n+1$ esetén $k|(n+1)! + k = N + (k-1)$ → $N+1, N+2, \ldots, N+n$ számok mindegyike összetett.

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 n-re például $(n+1)! + 2$ nyilván osztható 2-vel, $(n+1)! + 3$ osztható 3-mal, és így tovább $(n+1)! + n + 1$-ig, ami osztható $n+1$-gyel. Ezért $(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + n + 1$ ***n*** darab egymást követő szám.

$\pi(n)$ nagyságrendje

Def.: $\pi(n)$: 1-től n-ig a prímek száma (n pozitív), pl. $\pi(10) = 4$

Tétel: **„nagy prímszámtétel"**: a prímszámok eloszlását írja le (eredetileg Gauss vette észre, később Csebisev bizonyította).
$\pi(n) \sim \frac{n}{\ln(n)}$; ($\ln(n)$: természetes logaritmus), a ~ jelölés azt jelenti, hogy a két oldal hányadosa 1-hez tart, ha n végtelenhez

tart (aszimptotikusan egyenlőek)
tehát jelentése: $\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$

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**: $a, b \in \mathbb{Z}, a \neq 0, b \neq 0$.
a és b LNKO-ja a legnagyobb olyan szám, amely osztója a-nak és b-nek is.
Jel.: (a, b). Pl.: $(15{,}24) = 3$, $(-20{,}0) = 20$, $(-22{,}18) = 2$, de $(0{,}0) =$ nem értelmezett.
relatív prím: $(a, b) = 1$

Def.: **LKKT**: $a, b \in \mathbb{Z}$ legkisebb közös többszöröse az a legkisebb $n \in \mathbb{N}$ szám, melyre $a|n$ és $b|n$ áll.
Jel.: $[a, b]$. Pl.: $[-5, -17] = 85$, $[-9, 0] = 0$, $[0{,}0] = 0$.

Def.: **Csebisev-tétel**: tetszőleges n pozitív egészre $\exists\, p$, amelyre $n < p \leq 2n$. Bármely 0-tól és 1-től különböző szám és a kétszerese közt van prímszám.

Kongruencia fogalma, alapműveletek kongruenciákkal

Def.: $a \equiv b(mod\ m)$ [a **kongruens** b-vel modulo m]; ha a és b m-mel osztva ugyanazt a maradékot adja.
$a = m \cdot k + b$ alakú.
$a \equiv b(m) \Leftrightarrow m|a - b$
Pl.: $17 \equiv 52 \equiv -4\ (mod\ 7)$

Tétel:

$$\left.\begin{array}{l} a \equiv b(m) \\ c \equiv d(m) \\ k \in \mathbb{N} \end{array}\right\} \Rightarrow \begin{array}{l} (1)\ a + c \equiv b + d\ (m) \\ (2)\ \ ac \equiv bd\ (m) \\ (3)\ \ a^k \equiv b^k\ (m) \end{array}$$

Biz.:

1.) $\left.\begin{array}{l} m|a - b \\ m|c - d \end{array}\right\} \Rightarrow m|(a + c) - (b + d) \Rightarrow a + c \equiv b + d(m)$ ✓

2.) $\left.\begin{array}{l} m|a - b \overset{\cdot c}{\Rightarrow} m|ac - bc \\ m|c - d \overset{\cdot b}{\Rightarrow} m|bc - bd \end{array}\right\} \oplus\Rightarrow m|ac - bd \Rightarrow ac \equiv bd(m)$ ✓ Speciális esete: $\left.\begin{array}{l} a \equiv b(m) \\ c \equiv c(m) \end{array}\right\} \Rightarrow ac \equiv bc(m)$ ✓

3.) $\left.\begin{array}{l} a \equiv b(m) \\ a \equiv b(m) \\ \vdots \\ a \equiv b(m) \end{array}\right\} \Rightarrow k$ db , összeszervezzük őket (mert (2)-t már bizonyítottuk) ✓

Tétel:
ha $c|a$ és $c|b$ és $ac \equiv bc(m) \Leftrightarrow a \equiv b\left(\frac{m}{(m,c)}\right)$ (tehát c-vel osztásnál m-et leosztjuk m és c LNKO-jával)

Biz.:
$m \coloneqq m' \cdot (m, c)$,
$c \coloneqq c' \cdot (m, c)$
$\Rightarrow (m', c') = 1$
$m|ac - bc \Leftrightarrow m|c(a - b) \Leftrightarrow m'|c'(a - b) \Leftrightarrow m'|a - b$ ✓

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**: $ax \equiv b\ (m)$, adottak: $a, b, m \in \mathbb{Z}$; kérdés: $x =$?

Pl.: $6x \equiv 7\ (15)$,
$3|\ 15|\ \underbrace{6}_{3|6}\ x - \underbrace{7}_{3\nmid 7} \Longrightarrow \nexists$ megoldása!

Tétel: Az $ax \equiv b\ (m),\ a \neq 0$ **lineáris kongruencia megoldható** $\Leftrightarrow (a, m)|b$
A kongruencia **megoldáshalmaz**a (a, m) darab maradékosztály modulo m.

Biz.: Legyen $d := (a, m), a = a'd, m = m'd, b = b'd$
Ha $ax \equiv b\ (m)$, megoldható $\Rightarrow d|m|ax - b$ és $d|a|ax$ miatt $d|ax - (ax - b) = b$ ✓
Elégségesség bizonyítása: tfh. $d|b$. A kongruenciát d-vel végigosztva $a'x \equiv b'(m')$ és $(a', m') = 1$
Az euklideszi algoritmus segítségével kiszámítható olyan $k, l \in \mathbb{Z}$, amire $ka' + lm' = 1$, k-nak és m-nek nem lehet közös p prímosztója, hiszen ha lenne, akkor $p|ka' + lm' = 1$ állna $\Longrightarrow (k, m') = 1$.
$a'x \equiv b'\ (m') \overset{(k,m')=1}{\Longleftrightarrow} ka'x \equiv kb'(m') \Leftrightarrow \left.\begin{matrix}(1 - lm')x \equiv kb'(m') \\ lm'x \equiv 0\ (m')\end{matrix}\right\} \oplus \Longrightarrow x \equiv kb'\ (m')$
Hátravan még, hogy a megoldásokat $mod\ m$ adjuk meg. Mivel $m = m'd$, ezért $\forall$ m' szerinti maradékosztály pontosan d darab m szerinti maradékosztály uniója, a megoldások tehát:
$x \equiv kb' + dm'\ (m),\ \ d = 0,1, \dots, (d - 1)$

Euklideszi algoritmus (ennek alkalmazása lineáris kongruenciák megoldására is)

Euklideszi algoritmus: hatékony módszer két szám legnagyobb közös osztójának (LNKO) meghatározására.
Input: $a, b \in \mathbb{Z}\ \ (a \geq b)$, Output: (a, b)
Legyen $a_0 := a$, $a_1 := b$. Ha már meghatároztuk az $a_0 \geq a_1 \geq \cdots \geq a_i$ számokat, akkor legyen $a_{i-1} = q_i a_i + a_{i+1}$.
Az a_{i+1} tehát az a_{i-1} a_i-vel történő osztásakor keletkező maradék (C nyelven: $a_{i+1} = a_{i-1}\%a_i$), tehát $0 \leq a_{i+1} < a_i$ teljesül.
Az eljárás akkor ér véget, ha $a_{k+1} = 0$, ekkor $(a, b) = a_k$.

Másként: első lépésként elosztjuk a-t maradékosan b-vel: $a = k_1 \cdot b + m_1$. Ezután már (b, m_1)-et keressük: $b = k_2 \cdot m_1 + m_2$. A további lépések: $m_{i-2} = k_i \cdot m_{i-1} + m_i$. Az algoritmus addig megy, amíg $m_i = 0$ lesz, ekkor megkapjuk, hogy $(a, b) = m_{i-1}$.

Pl.: $(360, 225) =$?
$360 = 1 \cdot 225 + 135$
$225 = 1 \cdot 135 + 90$
$135 = 1 \cdot 90 + 45$
$90 = 2 \cdot 45 + 0$. Tehát $(360{,}225) = 45$.

Pl. 2: $(200, 72) =$?
$200 = 2 \cdot 72 + 56$
$72 = 1 \cdot 56 + 16$
$56 = 3 \cdot 16 + 8$
$16 = 2 \cdot 8 + 0$. Tehát $(200, 72) = 8$.

Az euklideszi algoritmus azért ér véget, azaz $a_{k+1} = 0$ lesz, mert (a_i) nemnegatív egészek szig. mon. csökkenő sorozata, tehát az eljárás lépésszáma $|a_0|$ felső becslés.

$$(a, b) = (a_0, a_1) = \left(\underbrace{a_0 - q_1 a_1}_{a_2}, a_1\right) = (a_1, a_2) = \left(\underbrace{a_1 - q_2 a_2}_{a_3}, a_2\right) = (a_2, a_3) = \cdots = \left(a_k, \overbrace{a_{k+1}}^{0}\right) = a_k \quad ✓$$

Lineáris kongruencia megoldása euklideszi algoritmus segítségével:
adott $ax \equiv b\ (m)$ lineáris kongruencia. Először meg kell vizsgálni, hogy megoldható-e: az euklideszi algoritmus segítségével kiszámoljuk (a, m)-et, és ha ez osztható b-vel, akkor van megoldás (tehát **megoldható** $\Leftrightarrow (\boldsymbol{a, m})|\boldsymbol{b}$). Ezután az algoritmus során kapott maradékokat fordított sorrendben kifejezzük az egyenletekből, és így megkapjuk az x-et.

Példa:
$59x \equiv 1\ (101), \qquad x =$?
Megoldható, ha $(59{,}101)|1$
Először meghatározzuk LNKO-t:
$(101{,}59) =$?
$101 = 1 \cdot 59 + \mathbf{42}$

$59 = 1 \cdot 42 + \mathbf{17}$
$42 = 2 \cdot 17 + \mathbf{8}$
$17 = 2 \cdot 8 + \mathbf{1}$
$8 = 8 \cdot \underbrace{1}_{1|1} + 0$ ✓
$\exists$ 1 mo.!

(Tehát mivel $(59{,}101)|1$ teljesül ($(59{,}101) = 1$, 1 pedig osztója 1-nek), ezért a lin. kongruencia megoldható, egy megoldása van.)
Ezután az egyenletekből kifejezzük a maradékokat:
$\mathbf{42} = 101 - 1 \cdot 59 \equiv (-1) \cdot 59\ (mod\ 101)$
$\mathbf{17} = 59 - 1 \cdot 42 \equiv 59 - (-1) \cdot 59 = 59 + 59 = 2 \cdot 59\ (mod\ 101)$
$\mathbf{8} = 42 - \mathbf{2} \cdot 17 \equiv (-1) \cdot 59 - \mathbf{2} \cdot 2 \cdot 59 = (-5) \cdot 59\ (mod\ 101)$
$\mathbf{1} = 17 - \mathbf{2} \cdot 8 \equiv 2 \cdot 59 - \mathbf{2} \cdot (-5) \cdot 59 = 12 \cdot 59\ (mod\ 101)$ →
$1 \equiv 12 \cdot 59\ (mod\ 101)$
$59x \equiv 1 \equiv 12 \cdot 59\ (mod\ 101)\ /:59$
$\boldsymbol{x \equiv 12\ (mod\ 101)}$ (marad mod 101, mivel $\frac{101}{(101,59)} = \frac{101}{1} = 101$)■

Példa 2.: $62x \equiv 24\ (36)$. Vizsgálat: $(62{,}24)|24$?
$62 = 2 \cdot 24 + \mathbf{14}$
$24 = 1 \cdot 14 + \mathbf{10}$
$14 = 1 \cdot 10 + \mathbf{4}$
$10 = 2 \cdot 4 + \mathbf{2}$
$4 = 2 \cdot 2 + 0$. Tehát $(62, 24) = 2$. 2 pedig osztója 24-nek, tehát 2 megoldásunk lesz.

$\mathbf{14} = 62 - 2 \cdot 24 \equiv \cdots (mod\ 36)$
$\mathbf{10} = 24 - 1 \cdot 14 \equiv \cdots (mod\ 36)$
$\mathbf{4} = 14 - 1 \cdot 10 \equiv \cdots (mod\ 36)$
$\mathbf{2} = 10 - 2 \cdot 4 \equiv \cdots (mod\ 36)$

$62x \equiv 24\ (36)$ → $62 \equiv 26\ (36)$
$26x \equiv 24\ (36)$ → $(26{,}36) = 2$, osztunk:
$13x \equiv 12\ (18)$ → $13 \equiv -5\ (18)$
$-5x \equiv 12\ (18)$ → $\cdot (-1)$
$5x \equiv -12\ (18)$,
$5x \equiv 6\ (18)$ → $\cdot 7$ (7 rel. prím a 18-hoz!)
$35x \equiv 42\ (18)$, → $(42 = 36 \cdot 2 + \mathbf{6})$
$-x \equiv 6\ (18)$ → $\cdot (-1)$
$x \equiv -6 \equiv 12(18)$ → 36 modulusra áttérünk
$\boldsymbol{x \equiv 12(36)}$ VAGY
$\boldsymbol{x \equiv 12 + 18 = 30(36)}$. ■

Wilson tétele

Tétel: (**Wilson**):
Ha p prímszám, akkor $(p-1)! \equiv -1(mod\ p)$.
Összetett számra ez nem teljesülhet, mivel ha $k > 1 \in \mathbb{Z}$ összetett, akkor k-nak és $(k-1)!$-nak van közös osztója, sőt, minden 4-nél nagyobb k összetett számra $(k-1)! \equiv 0\ (mod\ k)$.
Ha $k = 4$, akkor $(k-1)! \equiv 2\ (mod\ k)$.
Összefoglalva tehát $2 \leq k \in \mathbb{Z}$-re:

$$(k-1)! \equiv f(x) = \begin{cases} -x, & x < 0 \\ x, & x \geq 0 \end{cases} \begin{cases} -1\ (mod\ k), & \text{ha } k \text{ prím} \\ 2\ (mod\ k), & \text{ha } k = 4 \\ 0\ (mod\ k), & \text{ha } 6 \leq k \text{ összetett szám} \end{cases}$$

biz.:
$k = 4$-re nyilvánvaló: $3! = 2 \cdot 3 = 6 \equiv 2\ (4)$
Ha $6 \leq k$ összetett, akkor vagy található két ilyen különböző $1 < a < b < k$ egész, melyekre $ab = k$, és akkor $1 \cdot 2 \cdot \ldots \cdot (n-1) = abc \equiv 0\ (k)$, vagy $k = l^2$, és ilyenkor l és $2l$ szerepel a tényezők között.
Legyen végül $k = p$ prím:
$\forall\ 1 \leq a \leq p-1$ egészhez tartozik egy $1 \leq b \leq p-1$ egész, melyre $ab \equiv 1\ (p)$, hiszen az $ax \equiv 1\ (p)$ kongruenciát pontosan egy $mod\ p$ maradékosztály oldja meg.
Látható, hogy ha a-hoz b, akkor b-hez a tartozik, tehát az $1, 2, \ldots, p-1$ számok úgy rendezhetők párokba, hogy $\forall$ pár szorzata 1-et ad maradékul p-vel osztva. A párokba rendezés azért nem egészen pontos, mert bizonyos számok esetleg önmagukkal állnak párban. Ezekre az a számokra $a^2 \equiv 1\ (p)$ teljesül, azaz $p|a^2 - 1 \Leftrightarrow p|(a+1)(a-1)$
$\overset{p\ prím}{\Longrightarrow} p|a+1\ vagy\ p|a-1 \Rightarrow$ az önmagukkal párban álló számok kizárólag az 1 és (p-1) lesznek. Átrendezve a $(p-1)!$-t,

∀ prím szorzata 1 lesz, és lesznek még a páratlanul maradt 1 és $(p-1) \Longrightarrow (p-1!) \equiv 1 \cdot 1 \cdot \ldots \cdot 1 \cdot (p-1) \equiv p-1 \equiv -1\ (p)$ ■.

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.: $\varphi(m)$: 1 és m között az m-hez relatív prímek száma.

Pl.: $\varphi(10) = 4$, mert 1, ~~2~~, 3, ~~4~~, ~~5~~, ~~6~~, 7, ~~8~~, 9, ~~10~~

ha p prím: $\varphi(p) = p - 1$, mert 1-től $(p-1)$-ig ∀ szám relatív prím p prímhez

$\varphi(p^\alpha) = \underbrace{p^\alpha}_{összes} - \underbrace{p^{\alpha-1}}_{"rossz"}$

Tétel: ha $(a,b) = 1 \Rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

Ha $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \Rightarrow$

$\boldsymbol{\varphi(n) = \varphi\left(p_1^{\alpha_1}\right) \cdot \varphi\left(p_2^{\alpha_2}\right) \cdot \ldots \cdot \varphi\left(p_k^{\alpha_k}\right) =}$

$\boldsymbol{\left(p_k^{\alpha_1} - p_k^{\alpha_1-1}\right) \cdot \left(p_k^{\alpha_2} - p_k^{\alpha_2-1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k-1}\right) =}$

$\underbrace{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}}_{n} \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_n}\right) =$

$\boldsymbol{n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)}$

Pl.: $\varphi(100) = ?$ $\quad 100 = 2^2 \cdot 5^2$

$\varphi(100) = (2^2 - 2^1) \cdot (5^2 - 5^1) = (4-2) \cdot (25-5) = 40$

Redukált maradékrendszer

Def.: **redukált maradékrendszer** modulo m (röv. $RMR\ mod\ m$)

ez egy $\{c_1, c_2, \ldots, c_k\}$ halmaz, úgy, hogy teljesülnek a következők:

(1) számuk/elemeik $k = \boldsymbol{\varphi(m)}$

(2) $1 \le i, j \le k$,

$i \ne j$

$\Rightarrow \boldsymbol{c_i \not\equiv c_j\ (mod\ m)}$ (inkongruensek egymással mod m)

(3) $\boldsymbol{(c_i, m) = 1}$ ∀ i-re (relatív prímek mod m)

Szavakkal: legyen m modulus rögzített. A c -vel reprezentált maradékosztályt **redukált maradékosztály**nak nevezzük, ha c és m relatív prímek. Ha minden redukált maradékosztályt egy számmal reprezentálunk ⇒ RMR-t alkotnak. A redukált maradékosztályok száma $\varphi(m)$ (Euler-függvény). Tehát a RMR-ek $\varphi(m)$ eleműek.

Pl.: $RMR\ mod\ 10$: {1,3,7,9} vagy {37,29,−59,33}, $\varphi(10) = 4$ (✓), $1 \not\equiv 3\ (mod\ 10)$, $3 \not\equiv 9\ (mod\ 10)$, stb., $(1,10) = 1$, $(3,10) = 1$, stb.

Állítás: ha $\{c_1, c_2, \ldots, c_k\}$ RMR mod m és $(a,m) = 1 \Rightarrow \{ac_1, ac_2, \ldots, ac_k\}$ is RMR mod m

Pl.: $\{1,3,7,9\}\ RMR\ mod\ 10$ /·7, mert $(7,10) = 1$

{7,21,49,63} is $RMR\ mod\ 10$

biz.:

(1) a két halmaz elemszáma nyilván megegyezik ✓

(2) ha $ac_i \equiv ac_j\ (m)$ /:a (a, m)=1

$c_i \equiv c_j\ (m)$ tudjuk, hogy $\{c_1, c_2, \ldots, c_k\}\ RMR\ mod\ 10$ volt $\Rightarrow i = j$ □

(3) tudjuk:

$\left.\begin{matrix}(a,m) = 1\\ (c_i,m) = 1\end{matrix}\right\} (ac_i, m) = 1$✓

Euler-Fermat-tétel, kis Fermat-tétel

Tétel: (**Euler-Fermat**) $(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1\ (m)$

Mivel $(a,m) = 1 \Rightarrow \{ac_1, ac_2, \ldots, ac_k\}\ is\ RMR\ mod\ m \Rightarrow$ tehát az $ac_1, ac_2, \ldots, ac_k$ szorzatok valamilyen sorrendben kongruensek a $\{c_1, c_2, \ldots, c_k\}$ számokkal $\Rightarrow (ac_1) \cdot (ac_2) \cdot \ldots \cdot (ac_k) \equiv c_1 \cdot c_2 \cdot \ldots \cdot c_k\ (m)$ /:c_1 ; … /:c_2, …, /:c_k

$a^{\varphi(m)} \equiv 1\ (m)$✓

Tétel: (**„kis" Fermat tétel**) p prím, a tetszőleges egész $\Rightarrow a^p \equiv a\ (p)$

Biz.: p prím

$$\varphi(p) = p - 1 \underbrace{\overset{E-F}{\Rightarrow}}_{\substack{mert \\ (a,p)=1}} a^{p-1} \equiv 1\ (p) \overset{\cdot a}{\Rightarrow} a^p \equiv a\ (p)\ \checkmark$$

Kétismeretlenes, lineáris diofantikus egyenlet megoldása (konkrét példán)

Példa: **kétismeretlenes, lineáris diofantikus** (diofantoszi) **egyenlet megoldása**

általánosan: adott az $ax + by = c$ egyenlet és $a, b, c \in \mathbb{Z}$, kérdés: $x, y =?,\ x, y \in \mathbb{Z}$

$by = c - ax$

$b|c - ax \rightarrow ax \equiv c\ (b)$. Tehát visszavezettük a problémát egy lin. kongr. megoldására.

$$59x + 101y = 1$$
$$101y = 1 - 59x$$
$$101|1 - 59x \implies 59x \equiv 1\ (101)$$

Előzőleg láttuk, hogy ennek megoldása az $x \equiv 12\ (101)$, tehát

$$x = 101l + 12\ \ alakú\ \ (k \in \mathbb{Z}), \qquad y = \frac{1 - 59x}{101} = \frac{1 - 59(101k + 12)}{101} = \frac{1 - 59 \cdot 12}{101} - 59k = -7 - 59k\ \ alakú$$

Ellenőrzés: $59x + 101y = 59(101k + 12) + 101(-7 - 59k) = 59 \cdot 101k + 59 \cdot 12 - 7 \cdot 101 - 101 \cdot 59k = 1$ ✓

Két kongruenciából álló kongruenciarendszer megoldása (konkrét példán)

Példa: **Két kongruenciából álló kongruenciarendszer megoldása**

$$\left.\begin{array}{l} x \equiv 3\ (7) \\ x \equiv -1\ (8) \end{array}\right\} x =?$$

Az elsőből következik, hogy $x = 7k + 3$ alakú $k \in \mathbb{Z}$, ezt helyettesítsük be a másodikba!

$7k + 3 \equiv -1\ (8) \quad /-3$

$7k \equiv -4\ (8) \quad /-8k$

$-k \equiv -4\ (8)\ /\cdot(-1)$

$k \equiv 4\ (8) \implies k = 8l + 4$ alakú $l \in \mathbb{Z} \implies$

$x = 7k + 3 = 7(8l + 4) + 3 = 56l + 31$ alakú $\implies$

$x \equiv 31\ (56)$

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]

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. 2^x végeredményének puszta kiírásához már $\log 2^x = x$ lépés kell, ami az inputnak (vagyis $\log x$-nek) exponenciális függvénye. (n^m szám hossza $m \cdot \log n$, és ez nem polinomiális függvénye a $(\log n + \log m)$-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: $a\%b \Leftrightarrow a - \left(\frac{a}{b}\right) * b$ (C szintaxissal)

Tehát a $mod\ m\ +, -, \cdot, /$ is polinomiális!

Mi a helyzet a $mod\ m$ **hatványozás**sal?
Az alábbi példa bemutatja, hogy a $mod\ m$ hatványozás elvégezhető polinomidőben:

Példa: $3^{100} \equiv ?\ (7)$
$3^1 \equiv 3(7)$
$3^2 \equiv 9 \equiv 2(7)$
$3^4 \equiv 2^2 = 4(7)$
$3^8 \equiv 4^2 = 16 \equiv 2(7)$
$3^{16} \equiv 2^2 = 4\ (7)$
$3^{32} \equiv 4^2 = 16 \equiv 2(7)$
$3^{64} \equiv 4\ (7)$
Most írjuk fel a 100-at binárisan: $100_{(10)} = 1100100_{(2)}$
$\Longrightarrow 3^{100} \equiv 3^{2^6} \cdot 3^{2^5} \cdot 3^{2^2} = 3^{64} \cdot 3^{32} \cdot 3^4\ (7)$
$3^{100} \equiv 4 \cdot 2 \cdot 4 = 32 \equiv 4\ (7)$

...

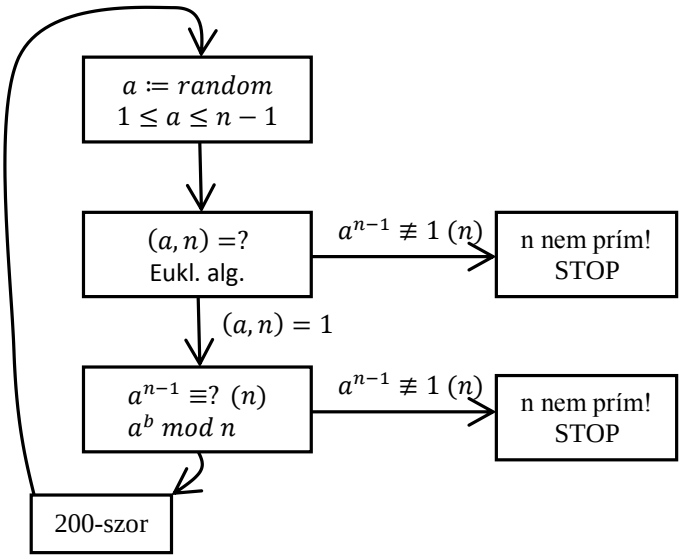
Prímtesztelés

Prímtesztelés:
Egy egyszerű módszer, hogy 1-től $\sqrt{n}$-ig ellenőrizzük az n-nel való oszthatóságot. Előnye, hogy ha n 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: n prím-e?
Kis Fermat-tételen alapul (aminek az RSA-eljárásban is szerepe van), ami kimondja, hogy ha p prím, $a \in \mathbb{Z}$ és $(a,p) = 1$, akkor $a^{p-1} \equiv 1(mod\ p)$.

1. lépés: felveszünk egy tetszőleges a számot, amire igaz, hogy $1 \leq a < n$.

2. lépés: kongruenciák ellenőrzése:
ha $a^{n-1} \not\equiv 1\ (n)$, akkor a **tanúja/árulója** n-nek → n NEM



[3] Korábbi cím: „Számelmélet és algoritmusok: összeadás, szorzás, maradékos osztás, hatványozás lépésszáma. Modulo m hatványozás polinomiális időben."

prím! STOP,
ha $a^{n-1} \equiv 1\ (n)$, akkor a **cinkosa** n-nek → n valószínűleg prím

A Fermat-teszt problémája, hogy hibázhat, azaz egy összetett számot is prímnek tekinthet. Ennek kiküszöbölésére sokszor, sok a-ra kell végrehajtani a tesztet. Ha a teszt kb. 200-szor lefutva (ha korábban nem állt le) is azt adja ki, hogy n prím ($a^{n-1} \equiv 1\ (n)$), akkor nagy valószínűséggel igaza van.

Tétel: ha n-nek **∃ tanúja** $\Longrightarrow RMR\ mod\ n$ legalább fele tanú! (RMR=redukált maradékrendszer)

Biz.: legyen „a" egy tanú, $c_1, \dots, c_k$ cinkosok
Állítás: $a \cdot c$: tanú
biz.: $(a \cdot c_i)^{n-1} \equiv \underbrace{a^{n-1}}_{\equiv 1} \cdot \underbrace{c_i^{n-1}}_{\equiv 1}\ (n) \Longrightarrow (a \cdot c_i)^{n-1} \not\equiv 1\ (n)$ ✓
Állítás: $a \cdot c_i \not\equiv a \cdot c_j\ (n), ha\ c_i \not\equiv c_j\ (n)$
Biz.: ha $a \cdot c_i \equiv a \cdot c_j\ (n)$ /: a, mert $(a, n) = 1$
$c_i \equiv c_j\ (n)$ ✓

Következmény: ha van tanú, akkor a Fermat-teszt legfeljebb $\left(\frac{1}{2}\right)^{200}$ valószínűséggel téved

Carmichael számok

Def.: n **Carmichael-szám**, ha **összetett** szám, de ∄ tanúja, csak cinkosa (ami arra utalna, hogy valószínűleg prím) a RMR-ben, azaz ∀ a $(a, n) = 1$-re $a^{n-1} \equiv 1\ (n)$.
pl.: 561
De van olyan teszt, aminek a működése olyan, hogy kiszűri a Carmichael-számokat.

Prímgenerálás: m legyen pl. egy 200-jegyű random szám → prímtesztelés. Ha összetett, megnézzük $(n+1) - et,\ (n+2) - t, \dots$ A $\Pi(n) \approx \frac{n}{\ln n}$ 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:
$x \xrightarrow{c} c(x),\ y \xrightarrow{D} D(y)$, amire teljesül a visszafejthetőség: $D\big(c(x)\big) = x$

RSA-kód: $N \coloneqq p \cdot q$, ahol p, q sokszámjegyű prímek
c választása úgy, hogy $\varphi(n) = (p-1)(q-1)$-hez relatív prím legyen: $\big(c, \varphi(N)\big) = 1$
kódolás: $x \to x^C mod\ N$
nyilvános: N, c; (mindenki számára ismert, ennek segítségével kódolhatják mások nekünk szánt üzeneteiket. A nyílt kulccsal kódolt üzenetet csak a titkos kulccsal tudjuk „megfejteni".)
titkos: $p, q, d, \varphi(N)$

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

Dekódolás: $y \to y^d mod\ N$
d jól van megválasztva $\Leftrightarrow x^{c \cdot d} = (x^c)^d \equiv x(N)\ \forall\ x$-re

Segédtétel: $(X, N) = 1 \Longrightarrow x^{\varphi(N)} \equiv 1\ (N) \Longrightarrow x^{k \cdot \varphi(N)} \equiv 1(N) \Longrightarrow x^{k \cdot \varphi(N)+1} \equiv x(N)$
cél: $c \cdot d = k \cdot \varphi(N) + 1$ valamely k-ra, azaz $c \cdot d \equiv 1\ (\varphi(N))$ lin. konguencia → $\big(c, \varphi(N)\big) = 1$ ✓
kongr. az euklideszi algoritmussal megoldható! $d \equiv \_\_\ (\varphi(N))$
A d-t azért nem tudja bárki kiszámolni, mert nem tudja felírni a lin. kongrueniát, ugyanis a $\varphi(N)$ kiszámolásához szükséges p és q ismerete: $\varphi(N) = (p-1)(q-1)$.

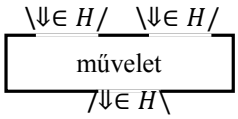
Digitális aláírás
Előnye, hogy ha A üzenetet küld B-nek, akkor B meg tud bizonyosodni arról, hogy az üzenetet csakis A-tól kaphatta.
$A \quad \to \quad B$
$C_A \qquad C_B$ } kódoló függvények nyilvánosak → $x \to y \coloneqq D_A(C_B(x))$
$D_A \qquad D_B$ } dekódoló függvények titkosak $\quad y \to x \coloneqq D_B(C_A(y))$

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 $f: H^2 \to H$ függvényt **művelet**nek hívjuk, ahol $H \neq 0$ alaphalmaz és H^2 a H-ból készíthető rendezett párok halmaza.



Ellenpélda: a skaláris szorzás egy „öszvér” művelet, mert vektorokat kap, és skalárt ad vissza; $u, v \to c \in \mathbb{R}$

*Máskép*p: **Művelet**: Egy H nemüres halmazon értelmezett (kétváltozós) műveleten egy $\boldsymbol{H \times H \to H}$ függvényt értünk, azaz egy olyan leképezést, amely bármely $\boldsymbol{a, b \in H}$ elempárhoz egyértelműen hozzárendel egy H-beli elemet.
Vagy: a H halmazon értelmezett n-változós **művelet**en (0-változós műv.: 5. 1-változós műv.: $x \to -x$ (ellentettképzés), x' (deriválás), stb.) egy tetszőleges $f: H^n \to H$ leképezést értünk, azaz minden, H elemeiből képzett, rendezett n-eshez (pl. $(h_1, h_2, \dots, h_n)$-hez) H -nak egy bizonyos elemét (itt $f(h_1, h_2, \dots, h_n)$-t) rendeljük.
A **művelet ne vezessen ki adott struktúrából**!

Def.: A H halmazon értelmezett, 2-változós $*$ művelet:
- **kommutatív** (felcserélhető), ha $a * b = b * a$ teljesül $\forall\, a, b \in H$ elemekre
- **asszociatív** (átzárójelezhető), ha $(a * b) * c = a * (b * c)$ teljesül $\forall\, a, b, c \in H$–ra
- $S =<$ H,$*>$ 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 $n \times n$-es mátrixok a szorzással félcsoportot alkotnak: mátrixok szorzása asszociatív, de nem kommutatív)
- A pozitív számokon értelmezett hatványozás nem asszociatív és nem kommutatív (hisz $2^{(2^3)} = 256 \neq 64 = (2^2)^3$, ill. $2^3 = 8 \neq 9 = 3^2$),
- a polinomok kompozíciója (egymásba helyettesítése) asszociatív, de nem kommutatív (hisz $[(p \circ q) \circ r](x) = p\left(q\left(r(x)\right)\right) = [p \circ (q \circ r)](x)$, de $(p \circ q)(x) = p\big(q(x)\big) \neq q\big(p(x)\big) = (q \circ p)(x)$ általában).

Def.: ($*$ műv., H alaphalmaz), $e \in H$ **egységelem**, ha $\forall\, a \in H$ elemére $e * a = a * e = a$ (helybenhagyja az elemet).
Összeadás esetén az egységelemet nullelemnek vagy nullának nevezzük, és 0-val jelöljük.

Állítás: az egységelem egyértelmű (ha van)

biz.: tfh. e, f különböző egységelemek: $f \underbrace{=}_{\text{mert } e \text{ egységelem}} e * f \underbrace{=}_{\text{mert } f \text{ egységelem}} e$ ↯

Def.: az $a \in H$ **inverz**e $b \in H$, ha $a * b = b * a = e$, ahol e az egységelem.
Jele: $b = a^{-1}$. Tehát $a * a^{-1} = e$.

Csoport, Abel-csoport

Def.: $(G,*)$ **csoport**, ha $*$ *művelet* G-n **és**:
- $*$ **asszociatív** (értelmezve van G-n egy asszoc. művelet, $(a * b) * c = a * (b * c)\ \forall\, a, b, c \in H$ elemre; tehát *félcsoport*)
- $\exists$ **egységelem**
- $\forall$ elemnek $\exists$ **inverz**e a * műveletre.

Állítás: egy csoportban a^{-1} egyértelmű (ha van)

biz.: tfh. b, c az a két különböző inverze:

$$a \begin{matrix} \to & b \\ \to & c \end{matrix} \Big\} \text{inverzek}, \qquad c = \overbrace{(b * a)}^{c} * c = b * \overbrace{(a * c)}^{c} = b \quad \text{↯}$$

másképp: $a_b^{-1} = a_b^{-1} * e = a_b^{-1} * \left(a * a_j^{-1}\right) = (a_b^{-1} * a) * a_j^{-1} = a_j^{-1}$

Def.: ha $(G,*)$ csoport és $*$ kommutatív, akkor $(G,*)$ **Abel-csoport**

Csoportok számokon:

- **egész számok** $(\mathbb{Z}, +)$: Abel-csoportot alkotnak az egész számok az összeadásra nézve: komm., asszoc.: $(1 + 2) + 3 = 1 + (2 + 3)$, egységelem: $0 + 1 = 1 + 0 = 1$, inv.: $-1 + 1 = 1 + (-1) = 0$,
- **rac. sz.** $(\mathbb{Q}, +)$: Abel-csoport,
- **valós sz.** $(\mathbb{R}, +)$: Abel-csoport: egységelem a 0, inverz az ellentett (-x), asszoc. komm.,
- **komplex sz.**[4] $(\mathbb{C}, +)$: Abel-csoport: egységelem a 0, inverz az ellentett (-x), assz. $((z_1 + z_2) + z_3 = z_1 + (z_2 + z_3))$, komm. $(z_1 + z_2 = z_2 + z_1)$
- De pl. **term. számok** $(\mathbb{N}, +)$ **NEM** csoport, mert a pozitív tagoknak $\nexists$ inverze!
- **valós számok a szorzásra nézve** $(\mathbb{R}, \bullet)$ **NEM** csoport, mert 0-nak $\nexists$ inverze!
- Viszont **kivéve a 0-t** már csoportok lesznek a következők:

$(\mathbb{R}\backslash\{0\}, \bullet)$ - nemnulla valósak, a szorzásra nézve Abel-csoportot alkotnak: komm., asszoc., egységelem az 1, inverz a reciprok $\left(\frac{1}{x}\right)$.
$(\mathbb{Q}\backslash\{0\}, \bullet)$, $(\mathbb{C}\backslash\{0\}, \bullet)$

Csoportok mátrixokon:

Adott: $H \coloneqq \{n \times n\text{-es}, \ det \neq 0 \text{ mx.-ok}\}$, a művelet legyen a **mátrixszorzás**. Csoportot alkot? Vizsgáljuk meg:

1. **zártság**: $\det(A \cdot B) = \underbrace{\det A}_{\neq 0} \cdot \underbrace{\det B}_{\neq 0}$ a determinánsok szorzástétele miatt ✓
2. **asszociativitás** (átzárójelezhetőség) $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ ✓(Az $n \times n$-es mátrixok a szorzással félcsoportot alkotnak: mátrixok szorzása asszociatív, de *nem kommutatív*!)
3. **egységelem**:=egységmátrix $\coloneqq \begin{pmatrix} \overbrace{\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 \end{matrix}}^{n} \end{pmatrix} \} n$ ✓
4. **inverz**:=inverzmátrix $\coloneqq A \to A^{-1}$: ez is H-beli, és biztosan $\exists\, A^{-1}$, mert $\det A \neq 0$ (invertálás csak a nem nulla determinánsú mátrixokra értelmezett) ✓

$\Longrightarrow$ IGEN, $(\{n \times n\text{-es}, det \neq 0 \text{ mx-ok}\}, \text{ mátrixszorzás})$ csoport ✓

Rajzok/alakzatok szimmetriacsoportja:[5]

a sík azon egybevágósági transzformációi, amelyek ezt az alakzatot önmagába viszik, és a **művelet** ezen transzformációk egymás utáni elvégzése.

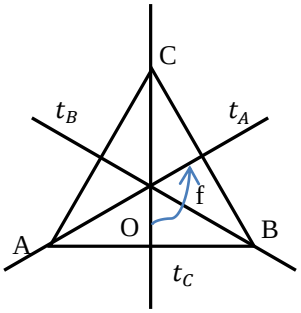
Most tekintsük egy rajznak, pl. egy szabályos háromszögnek a szimmetriáit/egybevágódási transzformációit!
$H = \{I, f_{120}, f_{240}, t_A, t_B, t_C\}$ (3 forgatás, 3 tükrözés (a feleződőlegesekre); I az identitás, vagyis helybenhagyás, 0 fokkal való forgatás)
A háromszög szimmetriája a sík egy olyan egybevágósági transzformációja, ami a háromszöget önmagába képzi.
Legyen $H \coloneqq \{R \text{ rajznak a szimmetriái}\}$, a művelet pedig a **függvénykompozíció**!
A függvénykompozícióról $((f \circ g)(x) = f(g(x)), f \circ g$ az f és g kompozíciója vagy szorzata, jele néha $f(g))$ tudjuk, hogy rendelkezik az **asszociativitás** (átzárójelezhetőség) tulajdonsággal:
f, g, h: $H \to H$ függvények: $(f \circ g) \circ h = f \circ (g \circ h)$

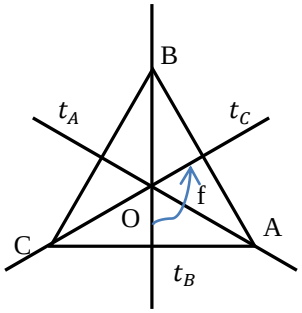
$$id = \begin{bmatrix} A & B & C \\ A & B & C \end{bmatrix}, \quad f = \begin{bmatrix} A & B & C \\ B & C & A \end{bmatrix}, \quad f^2 = \begin{bmatrix} A & B & C \\ C & A & B \end{bmatrix}$$

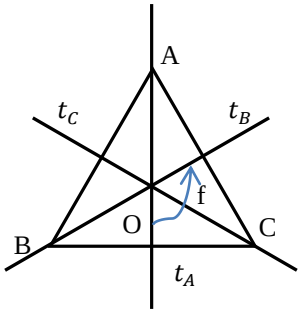
$$t_A = \begin{bmatrix} A & B & C \\ A & C & B \end{bmatrix}, \quad t_B = \begin{bmatrix} A & B & C \\ C & B & A \end{bmatrix}, \quad t_C = \begin{bmatrix} A & B & C \\ B & A & C \end{bmatrix}$$

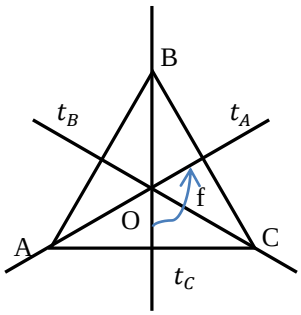
[4] emlékeztető: http://www.math.bme.hu/~szilagyi/01_komplex.pdf [komplex számok $(z = a + bi)$ összeadása a vektorösszeadás szabályai szerint történik (eltolás; $(a + bi) + (c + di) = (a + c) + (b + d)i$); szorzás: $(a + bi)(c + di) = ac + bci + adi + bdi^2 = (ac - bd) + (bc + ad)i$; egyébként komplex szám inverze: $z^{-1} = \frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{a-bi}{a^2+b^2}$ stb.]

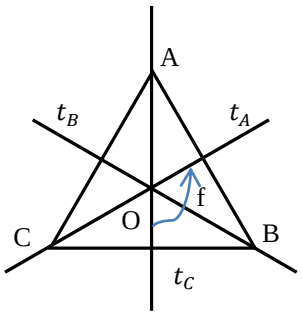
[5] http://www.cs.elte.hu/~ewkiss/bboard/07t.mat/Alg2_art_12.pdf

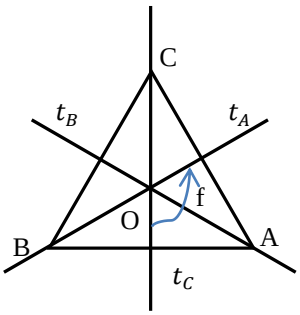
$\boldsymbol{f_0}$: 

, $\boldsymbol{f_{120}}$: 

, $\boldsymbol{f_{240}}$: 

$\boldsymbol{t_A}$: 

, $\boldsymbol{t_B}$: 

, $\boldsymbol{t_C}$: 

f az O körüli 120°-os forgatás, $f^2 = f \circ f$ a +240°-os forgatás

t_A a BC felezőmerőlegesére tükrözés

$ft_A = t_C$, mivel A→A→B; B→C→A; C→B→C

$t_c t_A = f$, forgatás a tengelyek szögének 2x-esével, A→A→B; B→C→C; C→B→A

egységelem/identitás: $f^3 = id$ (360°-kal forgatás), $t^2 = id$,

inverz (első transzformáció hatását „visszacsinálja”): $tft = f^{-1} (= f^2)$ $(f(x) = y \Leftrightarrow h(y) = x)$

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

D_3	id	f	f^2	t_A	t_B	t_C
id	id	f	f^2	t_A	t_B	t_C
f	f	f^2	id	t_C	t_A	t_B
f^2	f^2	id	f	t_B	t_C	t_A
t_A	t_A	t_B	t_C	id	f	f^2
t_B	t_B	t_C	t_A	f^2	id	f
t_C	t_C	t_A	t_B	f	f^2	id

Tehát a csoport elemei: $[id, f, f^2, t, tf, tf^2]$, ahol $t = t_A$, $tf = t_B$, $tf^2 = t_C$.
$f^3 = id$, $t^2 = id$, $tft = f^{-1} (= f^2)$. (inverz: $ff^{-1} = ff^2 = f^3 = id$)
Példa: $t_B t_C = (tf)(tf^2) = (tft)f^2 = f^{-1}f^2 = f$

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

biz.:
- a függvénykompozíció **asszociatív** ✓
- **egységelem** := identitás ($id(x) = x$, 0 fokkal forgatás, helybenhagyás) ✓
- **inverz**:= inverzfüggvény ($h = f^{-1}$, azt jelenti, hogy $f(x) = y \Leftrightarrow h(y) = x$) ✓

Diédercsoport

Def.: **diédercsoport**nak nevezzük az n-oldalú szabályos sokszög szimmetriacsoportját (szabályos n-szög egybevágóságai). Jele: D_n

$D_n = \{I = f_0, f_\alpha, f_{2\alpha}, f_{3\alpha}, \dots, f_{(n-1)\alpha}, t_1, t_2, \dots, t_n\}$, és $\alpha = \frac{360°}{n}$

$|D_n| = 2n$ (a szabályos n-szögnek 2n szimmetriája van – csoport rendje $2n$, ugyanis van n darab tengelyes tükrözés és a helybenhagyással együtt n darab forgatás)

Az előzőekben említett háromszöges példa a D_3-nak felel meg.

$f^n = 1, t^2 = 1, tf^i t = f^{-i}$

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

Elem rendje (ez véges csoportban véges)

Def.: G csoport rendje = az elemszámával, ezért jele: $|G|$, pl.: $|S_{10}| = 10!$ (első 10 szám permutációja), $|D_{10}| = 20$ $(2 \cdot 10)$

Def.: $(G,*)$ csoport, $g \in G$
$g^n := \underbrace{g * g * g * \dots * g}_{n\ db}$
Példa: $(\mathbb{Z},+)$-nál $3^5 = 3+3+3+3+3 = 15$
$D_3 - nál\ f_{120}^2 = f_{240},\ f_{120}^3 = I,\ t_1^2 = I$

Tétel: G véges, $g \in G \Rightarrow \exists n \geq 1$, hogy $g^n = e$

biz.: Soroljuk fel g hatványait: $g^1, g^2, \dots, g^k, \dots, g^l, \dots$ Mivel G véges $\Rightarrow \exists\ 1 \leq k < l$, hogy $g^l = g^k$.
Szorozzuk ezt be g^{-1}-gyel jobbról: $\overbrace{g \cdot g \cdot \dots \cdot g}^{l} \cdot g^{-1} (= (l-1) \cdot e) = \overbrace{g \cdot g \cdot \dots \cdot g}^{k} \cdot g^{-1} \Rightarrow g^{l-1} = g^{k-1}$. Ezt a g^{-1}-es szorzást hajtsuk végre annyiszor, hogy végül $g^{l-k} = e$ egyenlőséget kapjunk, ekkor $n := l-k$. ✓

Def.: $g \in G$, a g rendje k, ha k a legkisebb olyan kitevő, hogy $g^k = e$ $(1 \leq k)$, jele: $\sigma(g) = k$ (elemet k-szor összeszorozva önmagával egységelemhez jutunk)
$\underbrace{g^1, g^2, \dots, g^{k-1}, \underbrace{g^k}_{=e}}_{különböző k}, g^1, g^2, \dots$ 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 n szám, amelyre $g^n = e$. Ha ugyanis $\exists$ ilyen n, akkor $g^{-1} = g^{n-1}$, és a $g, g^2, g^3, \dots, g^n$ elemek különbözőek (hiszen ha $g^i = g^j$, akkor $g^{i-j} = e$), ezért <g> n-elemű. Ha $\nexists$ ilyen n, akkor a $g, g^2, g^3, \dots, g^n$ elemek mind különbözőek, <g> végtelen.
Ha $< G, \cdot >$ ciklikus csoport, melyet $g \in G$ generál, akkor G $\forall$ eleme előáll $g^i (= g \cdot g \cdot \dots \cdot g$ [i-szer] alakban), ahol $i \in \mathbb{Z}$. 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 $|G| = |H| = n$ G és H ciklikus csoportra $\Rightarrow G \cong H$.[6]

Pl.: D_3-nál $\sigma(f_{120}) = 3$ (360°-os forgatás), $\sigma(t_1) = 2$ (2x-es tükrözés)
$(\{\pm 1, \pm i\}, 0)$-nál $\sigma(i) = 4,\ \sigma(-1) = 2$

Ciklikus csoport

Def.: G **ciklikus csoport**, ha $\exists\ g \in G$ generátorelem, hogy g-ből G $\forall$ eleme kifejezhető a művelet és az inverzképzés segítségével, jele: C_n.
Másként: az olyan csoportot, melyet valamely eleme generál, ciklikus csoportnak nevezzük.

Állítás: G véges, G ciklikus $\Leftrightarrow \exists\ g \in G$, amire $\sigma(g) = |G|$.

biz.:
$\Leftarrow$: G tartalmazza g-t és annak hatványait, g kül. hatványainak száma $\sigma(g)$, ami egyenlő $|G|$-kel, tehát g generálni tudja G $\forall$ elemét $\Rightarrow G$ ciklikus ✓
$\Rightarrow$:Mivel G ciklikus, $\exists$ egy g generátoreleme, amivel elő lehet állítani G $\forall$ elemét $\Rightarrow \sigma(g) = |G|$ ✓

Pl.: $(\{\pm 1, \pm i\}, \bullet)$ ciklikus, $(\mathbb{Z},+)$ ciklikus.

Állítás: G ciklikus → G Abel

biz.: $a \cdot b = b \cdot a$
$g^i \cdot g^j = g^j \cdot g^i \Rightarrow g^{i+j} = g^{j+i}$ ✓

Állítás: minden párosrendű csoport ciklikus.

biz.: Legyen $|G| = p$ prím. A Lagrange-tétel miatt $\forall e \neq g \in G$-re $\sigma(g) | p \implies \overbrace{\sigma(g) = 1}^{\text{az egységelemeit kizártuk}}\ vagy\ p = |G|$ ✓

[6] Fleiner, 36. o.

Részcsoport. Csoportok izomorfiája

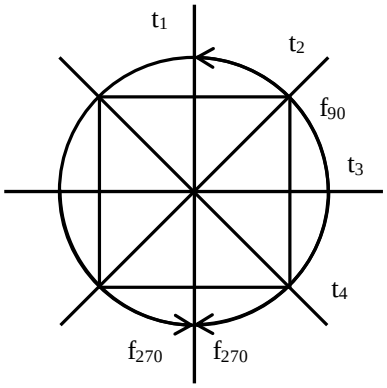
Def.: $(G,*)$ **izomorf** $(H,\circ)$-rel (H, körrel) [jele: $\cong$], ha $\exists\, f: G \to H$ kölcsönösen egyértelmű függvény úgy, hogy:
$\forall\, a,b,c \in G$-re $a * b = c \iff f(a) \circ f(b) = f(c)$, másképpen: $\forall\, a,b \in G$-re $f(a * b) = f(a) \circ f(b)$.
Vagy: G és H csoport **izomorf**, ha van köztük műveletartó bijekció, azaz létezik egy $\varphi: G \to H$ bijekció, melyre tetszőleges $g, g' \in G$ esetén $\varphi(g \cdot g') = \varphi(g) \cdot \varphi(g')$ áll. (a baloldali szorzás a G, a jobboldali pedig H művelete)

Pl.: G: $(\mathbb{R}^+, \bullet)$, H: $(\mathbb{R}, +)$
$f: \mathbb{R}^+ \to \mathbb{R}$
$f(a \cdot b) = f(a) + f(b)$ } vegyük észre, hogy f a logaritmusfüggvény!
$f = \log a,\ 0 < a \neq 1$

Def.: $(G, \bullet)$ csoport, $H \subseteq G$, H **részcsoportja** G-nek, ha H is csoport a G $\bullet$ csoportműveletére nézve. Jele: $H \leq G$.
Tetszőleges G csoport részcsoportjainak metszete is G részcsoportja.

Tétel: $(G, \bullet)$ csoport, $0 \neq H \subseteq G$
H részcsoport $\Leftrightarrow \begin{matrix}(i)\ a,b \in H \implies a \cdot b \in H \\ (ii)\ a \in H \implies a^{-1} \in H\end{matrix}$

biz.:
$\Rightarrow$: a szükségesség nyilvánvaló
$\Leftarrow$: H-ra $\bullet$ művelet:
➡asszociatív (mert G-ben is az) ✓
➡$g \in H \implies g^{-1} \in H \implies \overbrace{g \cdot g^{-1}}^{e} \in H$ egységelem ✓
➡(ii) miatt $\forall\, g \in H$-nak inverze is H-ban van ✓



Pl.: D_4
$D_4 = \{I, f_{90}, f_{180}, f_{270}, t_1, t_2, t_3, t_4\}$ $|D_4| = 8$
$H_1 := \{I, f_{90}, f_{180}, f_{270}\}$ $|H_1| = 4$ $H_1 \leq G$
$H_2 := \{I, t_1\}$ $|H_2| = 2$ $H_2 \leq G$
$H_3 := \{I\}$ $|H_3| = 1$ $H_3 \leq G$

Állítás: ciklikus csoport részcsoportja ciklikus.

biz.: G ciklikus csoport generátoreleme legyen g, és legyen $H \leq G$ valódi részcsoport. Tekintsük a minimális $0 < k$-t, melyre $g^k \in H$. A cél belátni, hogy g^k generálja H-t.
Tfh. a g^k $g^l \in H$-t nem generálja, vagyis $k \nmid l$.
Legyen $l = ak + r \implies r$ *maradék* $(1 \leq r \leq k)$. Mivel $g^k, g^l \in H$: $g^l \cdot ((g^k)^{-1})^a = g^r \in H$ ↯

Állítás: azonos rendű ciklikus csoportok izomorfak

biz.: $|G| = |H| = n$. Legyen g, h a G, H generátoreleme, ekkor $g^n, h^n := h^i$ izomorfizmus. ✓

Tétel: (**Cayley**) G véges csoport $\implies \exists\, n$, hogy S_n valamelyik H részcsoportjára $\overbrace{G \cong H}^{G\ izomorf\ H-val}$.

Szimmetrikus csoport

Def.: Az $f: \{1,2,\dots,n\} \to \{1,2,\dots,n\}$ kölcsönösen egyértelmű függvényt **permutáció**nak nevezzük.
A halmaz permutációján annak önmagára vett bijektív leképezését értjük. A a legtöbb vizsgálatban véges, így permutáción A elemeinek egy meghatározott átrendezéseit vagy sorbarendezését értjük. (Ha pl. A egy csomag kártya, akkor a kártyák megkeverésével A egy permutációját állítjuk elő. VAGY: ha A elemei egy futóversseny résztvevői, akkor a verseny minden lehetséges végeredménye A egy permutációját képviseli.)
n-elemű A-halmaz elemei: első n pozitív egész szám A-nak egy permutációja: zárójelben, egymás alá írva, sorbarendezve felsoroljuk az értelmezési tartományát és értékkészletét.
Pl. 1.: $f(1) = 5, f(2) = 2, f(3) = 1, f(4) = 3, f(5) = 4$. Permutáció rövidebben:
$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 2 & 1 & 3 & 4\end{pmatrix}$ → természetes sorrend
→képelemek
még rövidebben: $(5,2,1,3,4)$ (Descartes-féle alak)
Permutációk száma: $P_n = n!$
Mivel az 1 képe n különböző érték lehet, ezek mindegyikére $(n-1)$ különböző értéket választhatunk a 2 képéül a fennmaradó számokból, ezek mellé a párok mellé $(n-2)$-féleképpen választhatjuk a 3 képét, stb. Az n db szám képeként tehát $n(n-1)(n-2),\dots,1 = n!$-féleképpen választhatjuk meg a rendezett értékeket.

Pl. 2.:
$\begin{matrix}1&2&3&4&5\\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\ 3&5&2&1&4\end{matrix}$ szokásos jelölés: $\begin{pmatrix}1&2&3&4&5\\3&5&2&1&4\end{pmatrix}$

Def.: S_n **szimmetrikus csoport**: $\{1,2,\dots,n\}$ halmaz permutációi alkotta csoport a függvénykompozíció műveletre nézve.
elemei: $\{1,2,\dots,n\}$ permutációi, *művelet*: kompozíció; $|S_n| = n!$

Permutációk szorzása: megfelelő leképezések egymás utáni végrehajtása.
Az n elem feletti permutációk csoportja az n elemű szimmetrikus csoport, S_n. 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 $n!$ elemű szimmetrikus csoport valamelyik részcsoportjával, lásd Cayley-tétel (Cayley-tétel: ∀ véges csoport izomorf egy alkalmas permutációcsoporttal (S_n 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.)
$|S_n| = n!$,
$S_1 = \left\{\begin{pmatrix}1\\1\end{pmatrix}\right\}, S_2 = \left\{\begin{pmatrix}1&2\\1&2\end{pmatrix}, \begin{pmatrix}1&2\\2&1\end{pmatrix}\right\}$
$S_3 = \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}$
Fontos (lásd Fleiner-jegyzet): egy $\pi \circ \sigma$ permutáció kiszámításakor először alkalmazzuk a σ permutációt, és aztán a π-t.
Pl. 1.
$\pi = \begin{pmatrix}1&2&3&4&5\\2&4&3&1&5\end{pmatrix}$
$\sigma = \begin{pmatrix}1&2&3&4&5\\3&2&1&5&4\end{pmatrix}$
$\pi \circ \sigma = \begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix}$ adódik.
Így: $\sigma\pi$ szorzat $(x(\sigma\pi) = (x\sigma)\pi)$:
$1(\sigma\pi) = (1\sigma)\pi = 3\pi = 3$
$2(\sigma\pi) = (2\sigma)\pi = 2\pi = 4$
$3(\sigma\pi) = (3\sigma)\pi = 1\pi = 2$
$4(\sigma\pi) = (4\sigma)\pi = 5\pi = 5$
$5(\sigma\pi) = (5\sigma)\pi = 4\pi = 1$

Pl. 2.[7]:
$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} := \alpha \circ \beta = ?$
először alkalmazzuk a β permutációt, és aztán az α-t.
Tudjuk, hogy ∀ x elemre $x(\alpha\beta) = (x\alpha)\beta$ (ez a leképezés szorzás-definíciója). Tehát
$1(\alpha\beta) = (1\alpha)\beta = 2\beta = 3,$
$2(\alpha\beta) = (2\alpha)\beta = 1\beta = 2$
$3(\alpha\beta) = (3\alpha)\beta = 3\beta = 1$
$\beta \circ \alpha = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$
Másik oldalról megvizsgálva:
Tudjuk, hogy ∀ x elemre $\beta\alpha$ szorzat $x(\beta\alpha) = (x\beta)\alpha$ (ez a leképezés szorzás-definíciója). Tehát:
$1(\beta\alpha) = (1\beta)\alpha = 2\alpha = 1$
$2(\beta\alpha) = (2\beta)\alpha = 3\alpha = 3$
$3(\beta\alpha) = (3\beta)\alpha = 1\alpha = 2$
$\alpha \circ \beta = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$
$\alpha\beta \neq \beta\alpha$, tehát a permutációk szorzata NEM kommutatív.

$\beta^{-1} = ?$ Mivel $\beta = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \{(1,2),(2,3),(3,1)\}$, ezért $\beta^{-1} = \{(2,1),(3,2),(1,3)\} = \{(1,3),(2,1),(3,2)\} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$
β és β^{-1} szorzata az identikus leképezés:
$\beta\beta^{-1} = \beta^{-1}\beta = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

Pl. 3.:

[7] forrás: http://www.math.u-szeged.hu/~katai/disz3ea/permutaciok.pdf

$\begin{pmatrix}1&2&3&4&5&6\\6&3&4&1&2&5\end{pmatrix}\circ\begin{pmatrix}1&2&3&4&5&6\\2&1&4&3&6&5\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\3&6&1&4&5&2\end{pmatrix}$, jobbról balra szorozva $(f(g(x))$, először g, majd f)

$\begin{pmatrix}1&2&3&4&5&6\\5&4&3&2&1&6\end{pmatrix}$, balról jobbra szorozva $(f(g(x))$, először f, majd g)

Pl. 3.:

$\begin{pmatrix}1&2&3&4&5\\3&5&2&1&4\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4&5\\5&4&1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\4&1&3&5&2\end{pmatrix}$ ($\begin{matrix}4\\5\end{matrix}$ pl. így áll elő: $4\to2\to5$)

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: $(S_n,\circ)$ csoport.

biz.:

- a függvénykompozíció **asszociatív** ✓
- **egységelem** := identitás $\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}$ ✓ (az identikus (mindent helybenhagyó leképezés) egy permutáció, és ezzel akár jobbról, akár balról komponálunk, egységként viselkedk)
- **inverz** := inverzfüggvény (f^{-1}), $\pi\circ\pi^{-1}=\pi^{-1}\circ\pi=id$,

pl.: $\pi=\begin{pmatrix}1&2&3&4&5\\3&5&2&1&4\end{pmatrix}$; $\pi^{-1}=\begin{pmatrix}1&2&3&4&5\\3&5&2&1&4\end{pmatrix}^{-1}=\{(1,3),(2,5),(3,2),(4,1),(5,4)\}^{-1}=$

$\{(3,1),(5,2),(2,3),(1,4),(4,5)\}=\{(1,4),(2,3),(3,1),(4,5),(5,2)\}=\begin{pmatrix}1&2&3&4&5\\4&3&1&5&2\end{pmatrix}$

$\pi\circ\pi^{-1}=\begin{pmatrix}1&2&3&4&5\\3&5&2&1&4\end{pmatrix}\circ\begin{pmatrix}1&2&3&4&5\\4&3&1&5&2\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}$

$\pi^{-1}\circ\pi=\begin{pmatrix}1&2&3&4&5\\4&3&1&5&2\end{pmatrix}\circ\begin{pmatrix}1&2&3&4&5\\3&5&2&1&4\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}$ ✓

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

Mellékosztály fogalma, példák

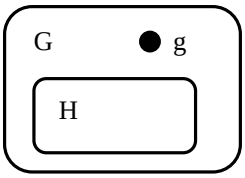
Def.: $(G,*)$ csoport, $g \in G, H \leq G$

A $\{g * h \mid h \in H\}$ halmaz a H részcsoport g szerinti bal oldali **mellékosztálya**, jele: gH

$H = \{e, h_1, h_2, \dots\}$

$g * H = \{g * h | h \in H\} = \{g, gh_1, gh_2, \dots\} \subseteq G$

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.



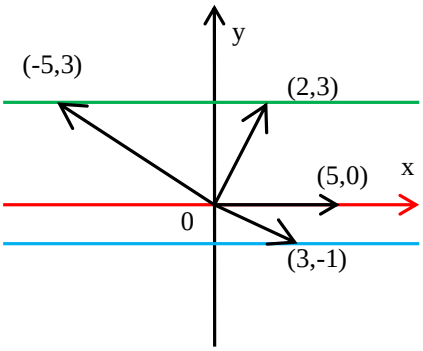
Pl.: $G \coloneqq \{síkvektorok, +\}$, $H = \{\text{x-tengely vektorai}\}$

$g = (2,3) \rightarrow (2,3) + H$

$g = (3,-1) \rightarrow (3,-1) + H$

$g = (-5,3) \rightarrow (-5,3) + H$

$g = (5,0) \rightarrow (5,0) + H$



Pl. 2.: $H = (n\mathbb{Z}, +) \leq (\mathbb{Z}, +) = G$, ahol $n\mathbb{Z} \coloneqq \{nz : z \in \mathbb{Z}\}$ az n többszöröseit jelöli. Egy adott $k \in \mathbb{Z}$ esetén a G csoport k szerinti baloldali mellékosztálya a $k + n\mathbb{Z}$ halmaz lesz, vagyis mindazon egészek, amelyek k-val kongruensek modulo n.

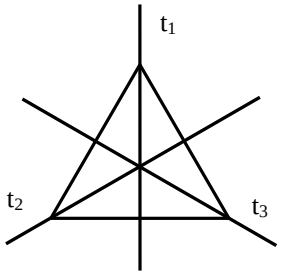
Pl.: $G = D_3$, $H = \{I, f_{120}, f_{240}\}$

$g = t_1$

$gH = \{t_1 I, t_1 f_{120}, t_1 f_{240}\} = \{t_1, t_2, t_3\}$

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

$t_2 H = \{t_2, t_3, t_1\}$



Tulajdonságok:

1.) $g \in gH$

biz.: mivel $e \in H \implies g = g \cdot e \in H$ ✓

2.) $g_1 H \cap g_2 H \neq 0 \implies g_1 H = g_2 H$

biz.:

$a \in g_1 H \cap g_2 H, b \in g_1 H$; cél: $b \in g_2 H$

$a = g_1 h_1 = g_2 h_2$, $h_1, h_2 \in H$ $\quad / h_1^{-1} jobbról$

$g_1 \underbrace{h_1 h_1^{-1}}_{e} = g_2 h_2 h_1^{-1} \implies g_1 = g_2 h_2 h_1^{-1}$

$b \in g_1 H \implies b = g_1 h_3$, $h_3 \in H$ $\quad b = g_2 \underbrace{h_2 h_1^{-1} h_3}_{\coloneqq h_4 \in H}$ ✓

3.) H véges $\implies |H| = |gH|$

biz.: $H = \{h_1, h_2, \dots, h_k\}$

$gH = \{gh_1, gh_2, \dots, gh_k\}$

ha $gh_i = gh_j$ $/ \cdot g^{-1}$ balról

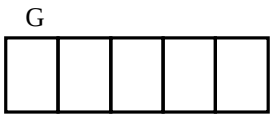
$h_i = h_j$ ✓

Mivel a H és g*H között létesíthető kölcsönösen egyértelmű hozzárendelés ($H \rightarrow g * H, x \rightarrow g * x$ egyértelmű hozzárendelés (függvény)), a két halmaz számossága egyenlő: $|g * H| = |H|$

Lagrange tétele, elemrend és csoport rendjének kapcsolata

Tétel: (**Lagrange**) Ha G véges csoport, akkor $\forall H \leq G$-re $|H| \mid |G|$, azaz H rendje osztója G rendjének minden H részcsoportra.

Elem és csoport rendjének kapcsolata: speciálisan, G bármely g elemének rendje $[o(g)]$ (amely gyakorlatilag a g által generált részcsoport elemszáma) osztja G rendjét, azaz $o(g) \mid |G| \; \forall g \in G$-re.



H szerinti mellékosztályok, számuk: i

$|G| = |H| \cdot i \implies |H| \mid |G|$ ✓ (a tartalmazó csoport rendje megegyezik a részcsoport rendjének és indexének szorzatával.)

Szövegesen:

Az előző megfigyelés szerint a G csoport néhány H szerinti (jobb oldali) mellékosztály uniója, és minden mellékosztály $|H|$ elemet tartalmaz. ✓

A tétel második felének bizonyítása:

Ha G csoportnak g egy eleme, akkor álljon H a g hatványaiból: $H = \left\{ \underbrace{g^1, g^2, \dots, g^{k-1}, e}_{k \; db \; különböző \; elem} \right\}$

Állítás: H részcsoport.

biz.:

(i) $g^i, g^j \in H \quad (g^i \cdot g^j = g^{i+j})$

ha $i + j < k$, akkor $g^{i+j} \in H$

ha $k < i + j$, akkor $g^{i+j} = g^{i+j-k} \cdot \underbrace{g^k}_{e} = g^{i+j-k} \in H$ ✓

(ii) $\underbrace{g^i \cdot g^{k-i}}_{g^k} = e \implies g^{k-i} = (g^i)^{-1}$ ✓

17.) Gyűrű, ferdetest és test fogalma. Nullosztómentes gyűrű, test nullosztómentessége. Példák:$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $n \times n$-es mátrixok, polinomok, $\mathbb{Z}_n$ (ez milyen n-re test), kvaterniók, $\mathbb{Q}(\sqrt{2})$.

Gyűrű, ferdetest és test fogalma

Eddig egyműveletes stuktúrákkal foglalkoztunk. Ha azonban a $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 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: $(R, \{+, \bullet\})$[8]).
A két művelet **disztributív** (kb. szétválasztható) ha $\forall a, b, c \in R$-re: $a(b+c) = ab + ac$ és $(a+b)c = ac + bc$.

(1) $a + b = b + a$ $(\forall\, a, b \in R)$ (**kommutatív**)	(I) $a \cdot b = b \cdot a$ (**kommutatív**)
(2) $(a + b) + c = a + (b + c)$ (**asszociatív** → félcsoport)	(II) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (**asszociatív**)
(3) $\exists\, 0 \in R$, amire $a + 0 = a$ $(\forall\, a \in R)$ (**nullelem** (összeadás egységeleme vagy additív semleges elem))	(III) $\exists\, 1 \in R, amire\ a \cdot 1 = 1 \cdot a = a$ $(\forall\, a \in R)$ (**egységelem** vagy multiplikatív semleges elem)
(4) $\forall\, a \in R$-re $\exists\, (-\boldsymbol{a}) \in R$; $a + (-a) = 0$ (additív **inverz** vagy ellentett**)**	(IV) $\forall\, a \neq 0 \in R\ \ \exists\, a^{-1} \in R$; $a \cdot a^{-1} = a^{-1} \cdot a = 1$ (multiplikatív **inverz** vagy reciprok (0-hoz nincs))
(5) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$; $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ (a • művelet **disztributív** a + műveletre nézve)	

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

Kommutatív gyűrű: (1-5)+(I-II)
gyűrű ÉS még $(R, \bullet)$ kommutatív is

Ferdetest: (1-5)+(II-IV)
A T gyűrű ferdetest, ha $(T\backslash\{0\}, \bullet)$ 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:$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $n \times n$-es mátrixok, polinomok

- **végtelen test**: $(\mathbb{R}, \{+, \bullet\})$, $(\mathbb{C}, \{+, \bullet\})$, $(\mathbb{Q}, \{+, \bullet\})$ (komm. gyűrű, és minden nemnulla számnak van reciproka, így a szorzás is csoport a nemnulla számokon)
- $(\mathbb{Z}, \{+, \bullet\})$ NEM test, mert ∄ inverze ∀ elemnek, hanem csak kommutatív gyűrű.
- $(\mathbb{N}, \{+, \bullet\})$ NEM gyűrű, mert nem csoport az összeadásra, nincs inverze.
- gyűrűk még: tetszőleges $n \in$ N szám többszörösei ($n\mathbb{Z}$);
- **véges test**: modulo p maradékosztályok $\{+, \bullet\}$, ahol p prím $\mathbb{Z}_p$; ($\mathbb{Z}_p$ kommutatív gyűrű; F_p-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 ($(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 (mod\ m)$) adódik), azt pedig elemi számelmélettel meg lehet mutatni). Ha m nem prím (összetett), akkor $\mathbb{Z}_n$-ben (modulo n maradékosztályok $\{+, \bullet\}$) van nullosztó, tehát $\mathbb{Z}_n$ 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 n-hez.)
- **végtelen gyűrű**: ($n \times n$-es mátrixok $\mathbb{R}$ felett, $\{+, \bullet\}$) (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 ✓

[8] • a szorzást (·) jelöli (hogy nyomtatásnál jobban látsszon)

(3) nullelem legyen a nullmátrix: $0 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$ ✓	(III) egységelem legyen az egységmátrix: $E = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ ✓
(4) additív inverz: $A \to -A$ ✓	~~(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 ($\mathbb{Z}$[x],$\mathbb{R}$[x]) kommutatív gyűrűt alkotnak a szokásos p.összeadásra, szorzásra nézve. Testet azért nem alkothatnak, mert pl. az x polinomnak az $\frac{1}{x}$ felelne meg multiplikatív inverznek, de az $\frac{1}{x}$ sem polinom!

- a valós polinomok hányadosteste test:
  $\mathbb{R}(x) := \left\{\frac{p}{q} : p, q \in \mathbb{R}[x], q \not\equiv 0\right\}$, a műveletek:
  $\frac{p}{q} + \frac{r}{s} = \frac{ps+qr}{qs}$, ill. $\frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$.

Nullosztómentes gyűrű, test nullosztómentessége

Def.: R gyűrűben az $a \neq 0$ elem **nullosztó**, ha ∃ olyan $0 \neq b \in R$, amelyre $ab = 0$.

Def.: R gyűrű **nullosztómentes**, ha R-ben ∄ nullosztó, azaz
ha $\forall a, b \in R$-re az $a \cdot b = 0$ csak akkor teljesül, ha $a = 0\ vagy\ b = 0$.
Pl.: $(\mathbb{Z}, \{+, \bullet\})$

Tétel: ∀ test nullosztómentes.

biz.: $a \cdot b = 0$

➡ha $a = 0$ ✓

➡ha $a \neq 0$: $a \cdot b = 0$ $/\cdot a^{-1}$ balról

$\underbrace{a^{-1} \cdot a}_{1} \cdot b = \underbrace{a^{-1} \cdot 0}_{0} \implies b = 0$ ✓

Def.: A **kommutatív nullosztómentes gyűrű** neve **integritási tartomány**. (Pl. $n\mathbb{Z}$ komm. és nullosztómentes. De $\mathbb{R}^{n\times n}$ mátrixgyűrűben A nullosztó, ha ∃ olyan B mátrix, amelyre $AB = 0$ (ha $Ax = 0$ egyenletnek van nemtriviális megoldása).)

Pl.: az egész számok, a páros számok gyűrűje integritási tartomány.
$\mathbb{Z}_6$ NEM integritási tartomány, mert pl. $2 \cdot 3 = 0$ és $2 \neq 0 \neq 3$, tehát a 2 ill. a 3 nullosztók.

$\mathbb{Z}_n$ (ez milyen n-re test)

Def.: $\mathbb{Z}_n$-nel jelöljük és **modulo n maradékosztályok gyűrűjének** nevezzük a
$\mathbb{Z}_n = \{0, 1, 2, \ldots, (n-1)\}$ halmazt a modulo összeadásra, ill. szorzásra nézve:
$a \oplus b := a + b\ (mod\ n)$
$a \odot b := a \cdot b\ (mod\ n)$

Pl.: $\mathbb{Z}_{10}$-nél:
$7 \oplus 8 = (7+8)\ mod\ 10 = 15\ mod\ 10 = 5$
$7 \odot 8 = (7 \cdot 8)\ mod\ 10 = 56\ mod\ 10 = 6$
$2 \odot 5 = 0$, de a 2 és az 5 sem 0 $\implies \mathbb{Z}_{10}$ nem nullosztómentes $\implies$ **nem test**.

Tétel: $\mathbb{Z}_n$ test $\Leftrightarrow$ n prím

biz.:
$\implies$: tfh. n összetett: ekkor szorzattá alakítható az előző példához hasonlóan, vagyis $\mathbb{Z}_n$ nem nullosztómentes $\implies$ $\mathbb{Z}_n$ nem test!
↯
$\Longleftarrow$: $n = p$ prím:

(1), (2), (3), (4) ✓ (komm.,assz.,nullelem,additív inverz)

(I) ✓ (komm.)

(II) ✓ (assz.)

(III) ✓ (egységelem)

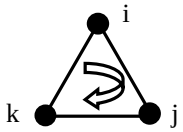
(IV): egyedül ez nem triviális (mult. inverz):

$a \neq 0,\ a^{-1} \coloneqq x,\ a \odot x = 1 \Leftrightarrow \underbrace{ax \equiv 1\ (p)}_{\text{megoldható} \Leftrightarrow \underbrace{(a,p)}_{=1,\text{mert p prím}}} \quad |1$

(v) ✓ (disztr.)

Kvaterniók

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \subseteq ?$ → a válasz: **kvaterniók**. A kvaterniók a komplex számok négy dimenzióra történő nem kommutatív kiterjesztései. A Q kvaterniócsoport elemei $1, -1, i, -i, j, -j, k, -k$.



Def.: $\mathbb{K} \coloneqq \{a + bi + cj + dk :\ a, b, c, d \in \mathbb{R}\}$

$i^2 = j^2 = k^2 = -1$

$ij = k,\ jk = i,\ ki = j,$

de $ji = -k, kj = -i, ik = -j$ → 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 $(0 + 0i + 0j + 0k)$, additív inverz ($a + bi + cj + dk$ ellentettje $-a - bi - cj - dk$)) ✓

~~(I)~~ (szorzás nem komm.) ($ij = k,\ jk = i,\ ki = j$, DE $ji = -k, kj = -i, ik = -j$)✖

(II) (szorzás asszociatív) ✓

(III) (van egységelem): $1 = 1 + 0i + 0j + 0k$ ✓

(IV) (multiplikatív inverz): ha $x \neq 0$ akkor

$$x^{-1} \coloneqq \frac{1}{x} = \frac{1}{a + bi + cj + dk} \underset{\substack{x \text{ konjugáltjával bővítünk:} \\ \bar{x} = a - bi - cj - dk}}{=} \frac{1}{(a + bi + cj + dk)} \cdot \frac{(a - bi - cj - dk)}{(a - bi - cj - dk)} = \frac{a - bi - cj - dk}{\underbrace{a^2 + b^2 + c^2 + d^2}_{\text{a nevező most már valós } \checkmark}}$$

(5) (szorzás disztr. az összea. műv.-re) ✓

$\mathbb{Q}(\sqrt{2})$, azaz $\{a + b\sqrt{2} :\ a, b \in \mathbb{Q}\}$ is test (a racionális számok kibővítve $\sqrt{2}$-vel)

$$\mathbb{Q} \subseteq \underbrace{\mathbb{Q}(\sqrt{2})}_{\{a+b\sqrt{2} :\ a,b \in \mathbb{Q}\}} \subseteq \mathbb{R}$$

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:

$$(a + b\sqrt{2})^{-1} \coloneqq \frac{1}{(a + b\sqrt{2})} \underset{\text{gyöktelenítés}}{=} \frac{1}{(a + b\sqrt{2})} \cdot \frac{(a - b\sqrt{2})}{(a - b\sqrt{2})} = \underbrace{\frac{a}{(a^2 - 2b^2)}}_{\in \mathbb{Q}\ \checkmark} - \underbrace{\frac{b}{(a^2 - 2b^2)}}_{\in \mathbb{Q}\ \checkmark} \cdot \sqrt{2}$$