

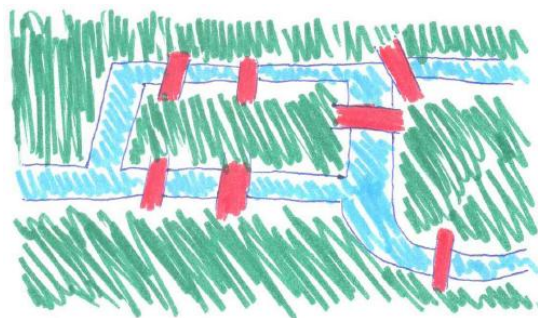
A jegyzet anyaga kb. 96%-ban **Vőneki Balázs** kézzel írt jegyzetéből származik, a tételek alapos kidolgozásáért őt illeti köszönet!
 Az én munkám az anyag begépelésére, formázására irányult elsősorban.
 Itt megtalálható a kézi jegyzet, ami alapján dolgoztam: https://wiki.sch.bme.hu/pub/Infoalap/BsZ2/bsz2_20082009tavasz_tetelkidolgozas.pdf.

Tartalomjegyzék

1.) Euler-körök és -utak, ezek létezésének szükséges és elégséges feltétele. Hamilton-körök és -utak. Szükséges feltétel Hamilton-kör létezésére és példa arra, hogy a feltétel nem elégséges. Elégséges feltételek: Dirac és Ore tétele.	1
2.) Páros gráf fogalma, karakterizációja. Párosítások páros gráfban, alternáló út és javítóút fogalma, Hall és Frobenius tételei.	3
3.) König tétele. Párosítások tetszőleges gráfban, Tutte tétele (csak a könnyű irány [szükségesség] bizonyításával). Gallai tételei.	6
4.) Gráfok színezése, kromatikus szám. A kromatikus szám becslései a klikkszám és maximális fokszám segítségével. Brooks tétele (biz. nélkül). Mycielski konstrukciója.	8
5.) Síkbarajzolható gráfok kromatikus száma. Élgráf fogalma, élkromatikus szám, viszonya a maximális fokszámhoz, Vizing-tétel (biz. nélkül). Perfekt gráfok. Páros gráf és komplementere perfektsége.	10
6.) Hálózat, hálózati folyam és s, t -vágás fogalma, folyam értéke, s, t -vágás kapacitása. Ford-Fulkerson tétel, Edmonds-Karp tétel (biz. nélkül), egészértékűségi lemma. A folyamprobléma általánosításai.	14
7.) Menger tételei (4). Többszörös összefüggőség és élösszefüggőség (jellemzésük pont-, ill. éldiszjunkt utak segítségével). Dirac tétele (biz. nélkül).	17
8. Oszthatóság, prímekek, prímekek száma, hézag mérete szomszédos prímekek között, a számelmélet alaptétele (biz. nélkül). Legnagyobb közös osztó, legkisebb közös többszörös, osztók száma. Euklideszi algoritmus.	19
9.) Kongruencia fogalma, alpműveletek kongruenciákkal. Lineáris kongruenciák megoldása euklideszi algoritmussal, a megoldhatóság feltétele, megoldások száma.	21
10.) Teljes és redukált maradékrendszer fogalma, ϕ -függvény, kiszámítása. Euler-Fermat-tétel, kis Fermat-tétel.	23
11.) Művelet fogalma, félcsoport, csoport, Abel-csoport. Csoportok számokon, mátrixokon, diédercsoport. Példák véges és végtelen, kommutatív és nem kommutatív csoportra mind a négy lehetséges variációban.	24
12.) Elem rendje, részcs csoport, egy elem generált részcs csoport, ciklikus csoport. Mellékosztályok, Lagrange tétele, következménye az elemek rendjére vonatkozóan. A szimmetrikus csoport. Csoportok izomorfiaja, Cayley tétele (biz. nélkül).	26
13.) Gyűrű, ferdetest és test fogalma. Példa véges és végtelen testre, ill. véges és végtelen gyűrűre, ami nem ferdetest. Számelmélet és algoritmusok: összeadás, szorzás, maradékos osztás, hatványozás lépésszáma. <i>Modulo m</i> hatványozás polinomiális időben.	29
14.) Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosítás és digitális aláírás fogalma, megvalósításuk az RSA-kód segítségével.	32
xxx?. Gráfok és mátrixok. Szomszédossági mátrix (hatványainak jelentése, reguláris gráf esetén egy sajátértéke). Illeszkedési mátrix, annak rangja.	34

1.) Euler-körök és -utak, ezek létezésének szükséges és elégséges feltétele. Hamilton-körök és -utak. Szükséges feltétel Hamilton-kör létezésére és példa arra, hogy a feltétel nem elégséges. Elégséges feltételek: Dirac és Ore tétele.

Euler-körök és -utak, ezek létezésének szükséges és elégséges feltétele. Königsbergi hidak problémája

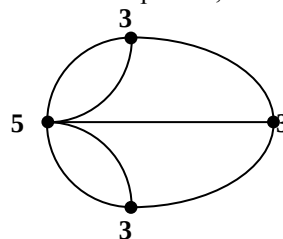


Königsbergi hidak problémája:

← 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 egy olyan zárt élsorozat, ami a gráf $\forall$ élét pontosan egyszer tartalmazza. Ha az élsorozat nem feltétlenül zárt, akkor Euler-utat 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 -ben $\exists$ E-kör $\Rightarrow \forall$ pont foka páros.
- 2.) Ha G -ben $\exists$ 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: (Euler) G összefüggő véges gráf

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

Bizonyítás:

A szükségességet előbb bebizonyítottuk.

Elégségség

- 1.) Legyen $v \in V(G)$ a gráf tetszőleges pontja, P pedig egy v -ből induló élismtélés 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

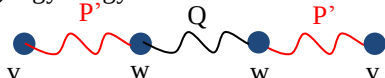
Legyen P' az ilyen séták közül a leghosszabb.

Állítás: P' E-kör

Bizonyítás:

(indirekt) H : G -ből elhagyjuk a P' -beli éleket. Tudjuk, hogy H -ban $\forall$ fokszám páros ($\text{páros} - \text{páros} = \text{páros}$) 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 élismtélésmentes w -ben elakadó séta.



Ez hosszabb P' -nél: **ELLENTMONDÁS.** ✗

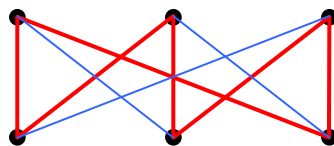
- 2.) Ha $\forall$ fokszám páros $\Rightarrow$ OK (Euler-kör)

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 gráfban elhagyjuk uv -t, akkor lesz E-út.

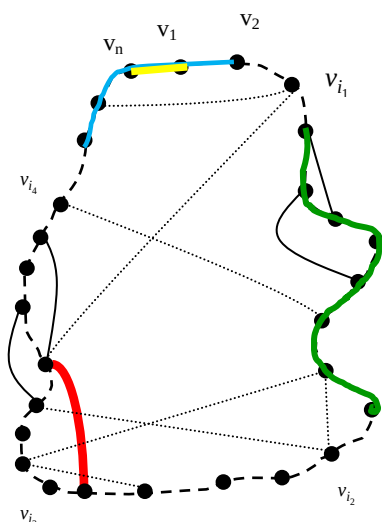
Hamilton-körök és -utak. Szükséges feltétel Hamilton-kör/út létezésére. Elégséges feltételek: Dirac és Ore tétele.

Def.: Hamilton-kör/út a gráf olyan köre/útja, ami a gráf minden csúcsát (egyszer) tartalmazza. (egyszer: egy körben/útban szereplő minden csúcs különböző.)

Pl.: a $K_{3,3}$ -ban egy H-kör:

**Szükséges feltételek:**

- 1.) Ha $\exists$ **H-kör** $\Rightarrow$ G -ből akárhogy k csúcsot törölve maradék **legfeljebb** k komponensre esik szét.
- 2.) Ha $\exists$ **H-út** $\Rightarrow$ G -ből akárhogy k csúcsot törölve maradék **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**.)

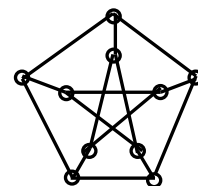
Bizonyítás: H-út

A bizonyítás nagyon hasonló az előzőhöz. Pl. hagyjuk el a gráfból a $V_n V_1$ élet, hogy csak H-utunk legyen! Amíg az előző példában a pontok elhagyása után a $V_{i_4+1}, \dots, V_n, V_1, V_2$ ív összefüggő volt, itt már nem, mert $V_n V_1 \notin E(G)$, tehát legfeljebb $k + 1$ komponens keletkezhetett. ✓

Példa arra, hogy a feltétel nem elégséges:

A **Petersen-gráfnak nincs H-köre, noha teljesíti a feltételt**. Ha volna H.-köre, akkor 3 színnel színezhettünk 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.) 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**

Tétel: (Ore) Ha az n -pontú ($n \geq 3$), egyszerű gráfban $\forall$ nem szomszédos x, y pontpárra $d(x) + d(y) \geq n \Rightarrow \exists$ **H-kör**.

Bizonyítás:

Indirekt. Tfh.: a két feltétel teljesülése ellenére $\nexists$ **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 $\exists$ **H-kör** $\Rightarrow G'$ -ben $\exists$ **H-út**.

Legyen ez $P = (\underbrace{Z_1, \dots, Z_2}_{=x}, \dots, \underbrace{Z_n}_{=y})$. Ha x szomszédos Z_k -val $\Rightarrow y$ 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 $\frac{n}{2} \Rightarrow \exists$ **H-kör**.

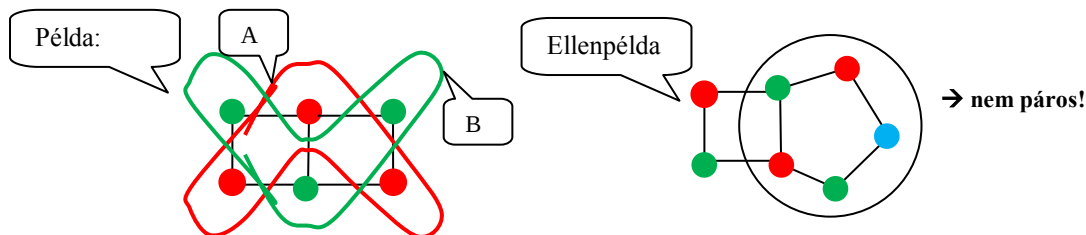
Bizonyítás: Teljesül az Ore-feltétel: $\forall x, y$ pontpárra $d(x) + d(y) \geq n$

2.) Páros gráf fogalma, karakterizációja. Párosítások páros gráfban, alternáló út és javítóút fogalma, Hall és Frobenius tételei.

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 $\forall$ éle A -beli csúcsot köt össze B -belivel.

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



Tétel: G páros $\Leftrightarrow$ nincs benne páratlan hosszú kör.

Bizonyítás:

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

$\Leftarrow$: Ha G $\forall$ köre páros hosszú, akkor megadhatjuk az A , és B halmazt. Válasszunk egy tetszőleges $v \in V(G)$ pontot.

Legyen ez A első pontja, majd v $\forall$ szomszédját tegyük B -be, majd $\forall$ eddig B -ben lévő pont $\forall$ szomszédját tegyük A -ba stb. Ezt addig végezzük, amíg $\forall$ pontot el nem helyeztünk.

Ez biztosan jó elosztás, hiszen, ha lenne pl. A -ban két szomszédos pont, akkor lenne páratlan kör is.

→ **ELLENTMONDÁS.**

Ha a gráf nem összefüggő, akkor az eljárást *komponensenként* hajtjuk végre.

Def.:

Párosításnak nevezünk egy M élhalmazt, ha semelyik két élnek nincs közös pontja. Az ilyen éleket **független élek**nek is nevezzük.

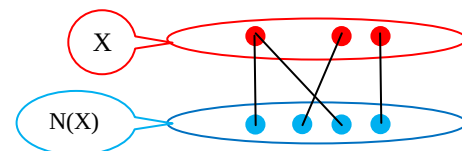
Teljes párosítás: olyan párosítás, ami a gráf $\forall$ pontját lefedi.

Def.: Egy G gráfban $N(x)$ jelöli az $x \subseteq V$ pontthalmaz szomszédainak halmazát.

$\nu(G)$: független élék maximális száma.

$x \subseteq \nu(G)$ lefoglaló pontthalmaz, ha G $\forall$ élének legalább egyik végpontját tartalmazza.

$\tau(G)$: lefoglaló pontok minimális száma.

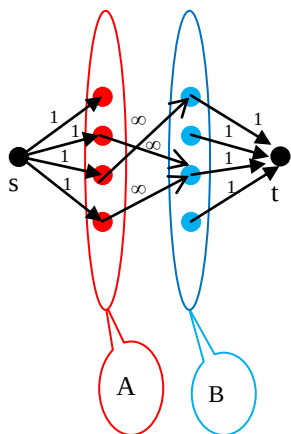


Tétel: (Kőnig) Ha $G = (A, B; E)$ véges páros gráf $\Rightarrow \nu(G) = \tau(G)$ (Ha nincs G -ben izolált pont, akkor $\alpha(G) = \rho(G)$ is teljesül.)

Bizonyítás:

Állítás: 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 lefoglaló pontthalmaz, akkor lefoglalja M $\forall$ élt is, de V $\forall$ pontja max. egy párosításélt fog le. $\Rightarrow |M| = \nu(G) \leq \tau(G) = |V|$

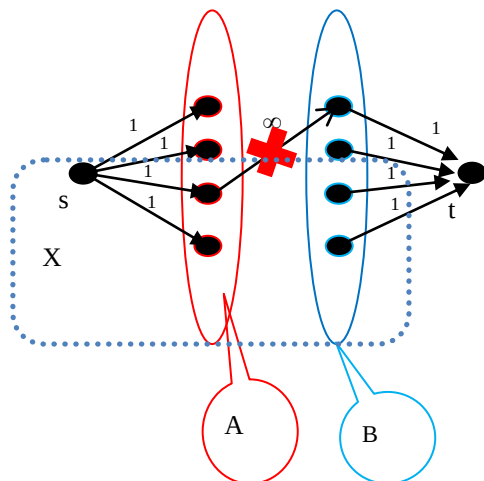
Készítsük el G' -t az alábbiak szerint. Irányítsunk G $\forall$ élt A -ból B -be, vegyünk fel egy-egy élt B $\forall$ pontjából t -be.

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

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

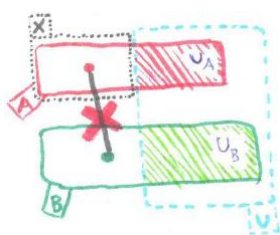
$$\tau(G) \leq |A \setminus X| + |B \cap X| = \nu(G)$$

Tehát: $\nu(G) \leq \tau(G) \wedge \tau(G) \leq \nu(G) \Rightarrow \nu(G) = \tau(G) \checkmark$



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

Bizonyítás:



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

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

Mivel U lefoglalja az $X := A \setminus U_A$ -ból induló éleket $\Rightarrow N(x) \subseteq U_B$, azaz $|N(x)| \leq |U_B|$. Felhasználva a König-tételt adódik:

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

Tétel: (Frobenius) $G = (A, B; E)$ véges páros gráf, $\exists$ teljes párosítás $\Leftrightarrow |A| = |B|$ és $\forall X \subseteq A$ -ra $|X| \leq |N(x)|$

Bizonyítás:

$\Rightarrow$: Triviális.

$\Leftarrow$: teljesül a Hall-feltétel $\Rightarrow \exists F$ -et fedő párosítás, de $|A| = |B| \Rightarrow$ ez TP

Def.: $G(A, B; E)$ páros gráf, M párosítás.

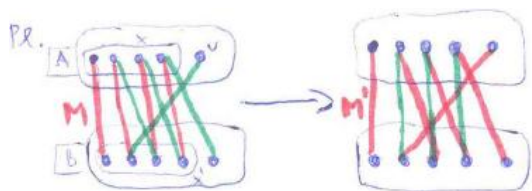
Alternáló út: párosítatlan A -beliből indul és $\forall$ második éle M -beli.

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

Magyar módszer: (Hatékony algoritmus max. élszám párosítás megtalálására.)

I. független élek feltétele, amíg lehet.

II. javító út 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 $\forall$ szomszédja X' -ben van és van egy P -vel jelölt javító út, ami tehát $A - X$ -beliből indul, $B - X'$ -beli pontban végződik és $\forall$ 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 $\Rightarrow$ STOP

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

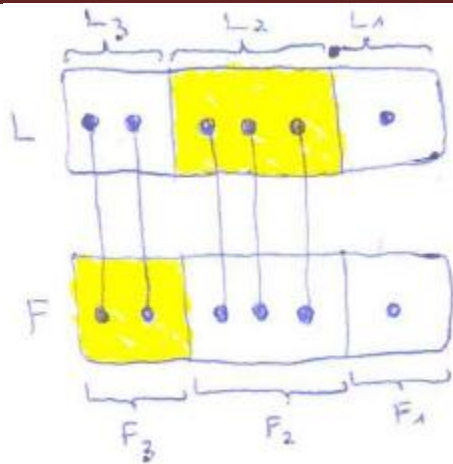
Bizonyítás:

Tfh. az algoritmus k élű párosítást adott. Cél: k pontú lefoglaló ponthalmazt találni! Ha találunk, akkor teljesül ez: $k \leq \nu(G) \leq \tau(G) \leq k \Rightarrow k = \nu(G)$

F_1 : párosítatlan F -beliek, L_1 : párosítatlan L -beliek,

L_2 : azon L -beliek, amikhez F_1 -ből alternáló úton el lehet jutni (ekkor $L_1 \cap L_2 = \emptyset$, mert $\nexists$ javító út),

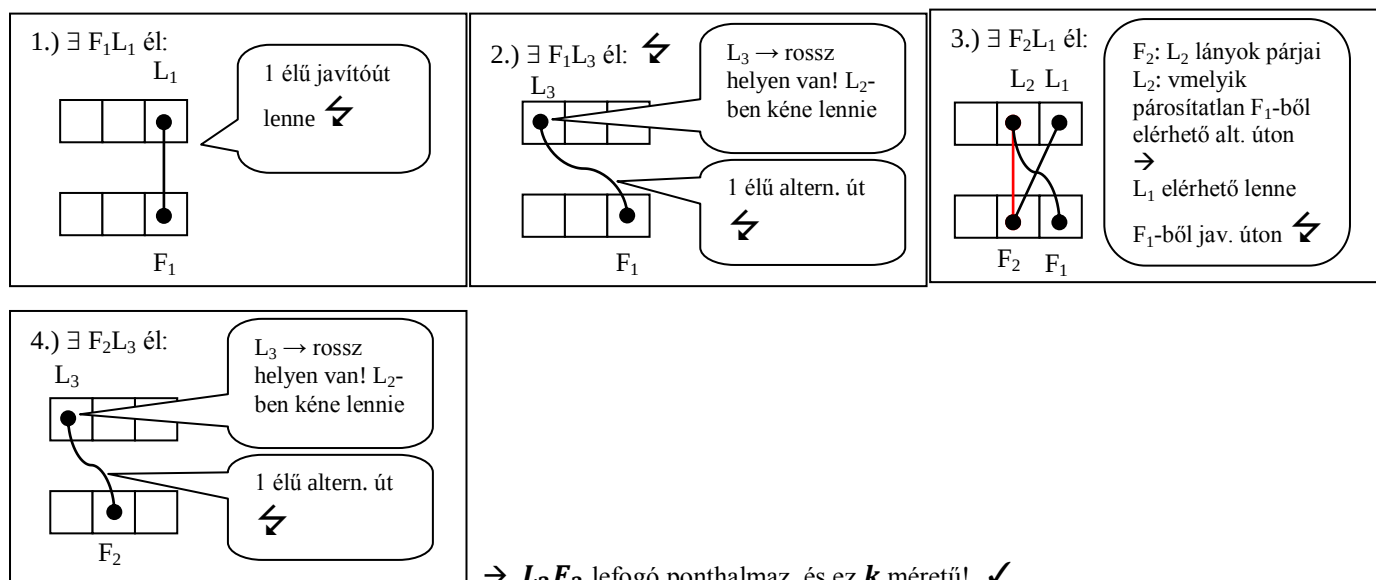
F_2 : L_2 -beliek párjai M szerint; $L_3 F_3$: maradék $L \setminus F$ -beliek



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

Bizonyítás: (indirekt)

Tegyük fel, hogy...



Még egy kérdés.

Hogyan keressünk javítóutat?

Induljunk ki egy A -beli, M által le nem fedett u pontból és mintha szélességi keresést végeznénk, menjünk el ennek összes szomszédjába, amiket $b_1, \dots, b_d$ jelöljön.

Ezek nyilván mind B -beli pontok és mindet lefedi M . Miután M lefedi a $b_1, \dots, b_d$ pontokat, jelölje $a_1, \dots, a_d$ ezek M által meghatározott pontját.

Most $\forall a_1, \dots, a_d$ pontból kiinduló, nem M -beli élen elérhető pontjába menjünk el.

Látható, hogy ezek éppen azok a pontok, amelyekbe vezet u -ból 3 élből álló alternáló út. Lényegében BFS-t alkalmazunk.

3.) Kőnig tétele. Párosítások tetszőleges gráfban, Tutte tétele (csak a könnyű irány [szükségesség] bizonyításával). Gallai tételei.

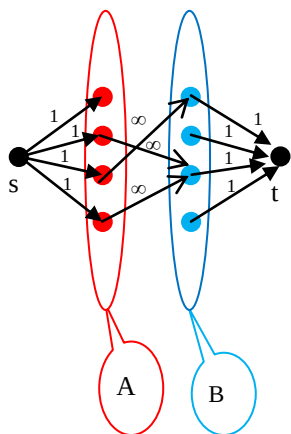
ld. még előző tételt!!

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

Bizonyítás:

Állítás: 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 lefoglaló pontthalmaz, akkor lefoglalja M $\forall$ élét is, de V $\forall$ pontja max. egy párosításélt fog le. $\Rightarrow |M| = \nu(G) \leq \tau(G) = |V|$

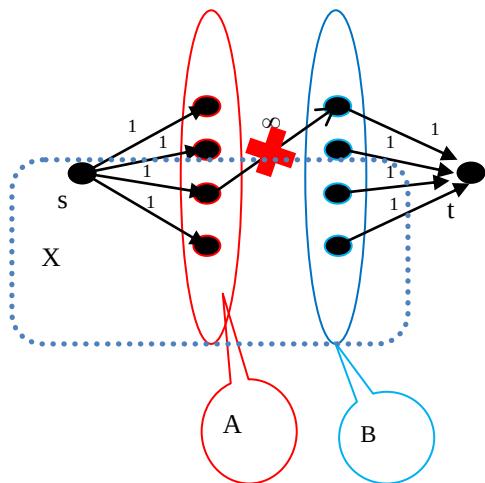
Készítsük el G' -t az alábbiak szerint. Irányítsunk G $\forall$ élét A -ból B -be, vegyünk fel egy-egy élt B $\forall$ pontjából t -be.

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

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

$$\tau(G) \leq |A \setminus X| + |B \cap X| = \nu(G)$$

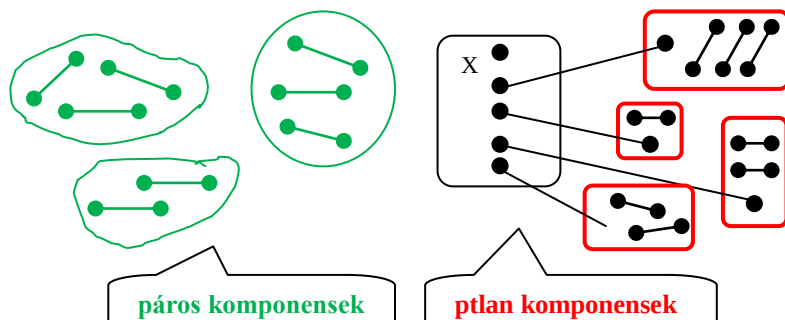
Tehát: $\nu(G) \leq \tau(G) \wedge \tau(G) \leq \nu(G) \Rightarrow \nu(G) = \tau(G) \checkmark$



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

Tétel: (Tutte) G -ben $\exists TP \Leftrightarrow \forall X \subseteq V(G) - re C_p(G - X) \leq |X|$ ($G - X$: G -ből X -beli csúcsok elhagyása)

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 $C_p(G - X) \leq |X|$. $\checkmark$

Def.:

$\nu(G)$: **független élek max. száma** G -ben.

Független élhalmaz: olyan élhalmaz, hogy semelyik két élének nincs közös pontja.

(Diszjunkt.)

$X \subseteq V(G)$ **lefogó pontthalmaz**, ha $G \setminus X$ éle tartalmaz X -beli csúcsot ($G \setminus X$ élének min. 1 pontját tart.)

$\tau(G)$: **lefogó pontok min. száma**.

$X \subseteq V(G)$ **független pontthalmaz**, ha az X -beli csúcsok nem szomszédok (nincs benne 2 szomsz. pont)

$\alpha(G)$: **független pontok max. száma**.

$Y \subseteq E(G)$ **lefogó élhalmaz**, ha $G \setminus Y$ pontjára illeszkedik Y -beli él ($\forall$ pontot lefog)

$\rho(G)$: **lefogó élek min. száma**.

	ftlen ~ max.	lef. ~ min.
élek	ν	ρ
pontok	α	τ

Tétel: $\nu(G) < \tau(G) \quad \forall G$ gráfra.

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: $\alpha(G) < \rho(G) \quad \forall G$ gráfra. (biz. mint előző)

Tétel: (Gallai) G tetszőleges, n csúcsú

1.) $\alpha(G) + \tau(G) = n$, ha G hurokélmentes

2.) $\nu(G) + \rho(G) = n$, ha G -ben $\nexists$ izolált pont.

Bizonyítás:

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

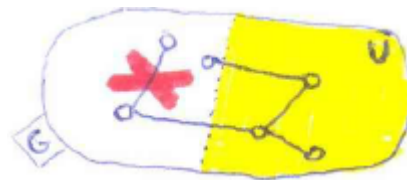
2.) G -nek $\exists \nu(G)$ diszjunkt éle, ezek két $\nu(G)$ pontot fognak le. A maradék $n - 2 \cdot \nu(G)$ db $\nu(G)$ pont mindegyike lefogható egy-egy új éllel (mert nincs izolált pont) $\Rightarrow \nu(G) + n - 2 \cdot \nu(G) = n - \nu(G)$ éllel $\forall$ pont lefogható $\Rightarrow \rho(G) \leq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

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 $\forall$ pont foka 1.) Ha a min. lefedő élhalmazban k csillag van, akkor a halmaz $n - k$ élel tartalmaz, hiszen k komponensű erdőből van szó: $\rho(G) = n - k$.

Másrészt a halmaz tartalmaz k diszjunkt élt: $k \leq \nu(G)$.

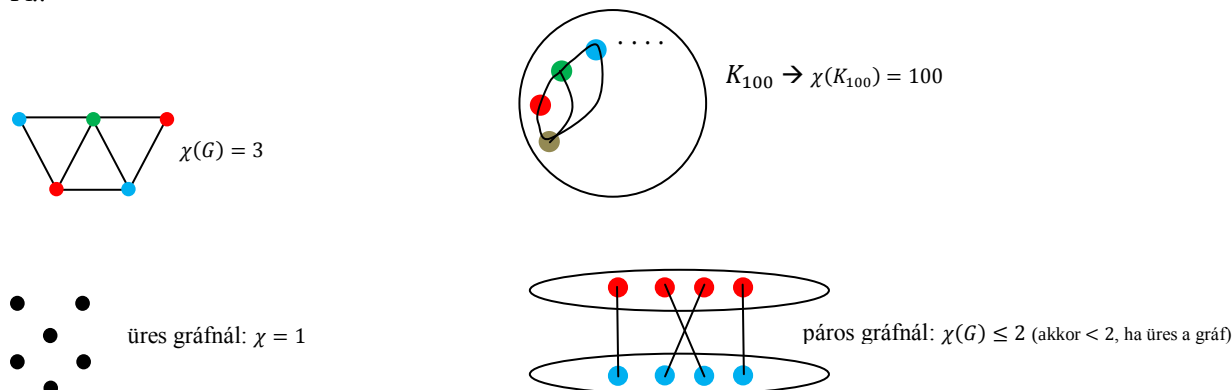
Ehhez hozzáadjuk az előző egyenlőséget $n - k + k \leq \nu(G) + \rho(G)$. Tehát $n \leq \nu(G) + \rho(G) \leq n$



4.) Gráfok színezése, kromatikus szám. A kromatikus szám becslései a klikkszám és maximális foksám segítségével. Brooks tétele (biz. nélkül). Mycielski konstrukciója.

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.:



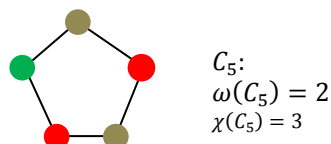
Def.: G maximális klikkmérete k , ha G -ben van k db csúcs, hogy közülük bármely kettő szomszédos, de $k + 1$ nem.

Jele: $\omega(G) = k$ (G egy teljes részgráfját klikknek nevezzük.)

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

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

Példa:



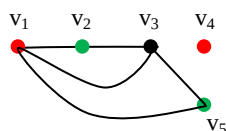
Mohó színezés: csúcsokat jelöljük $v_1, v_2, \dots, v_n$ -nel

a színeknek adjunk számokat: ① ② ③ ...

$v_1 \rightarrow \textcircled{1}$

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

Pl.:



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

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.

Tétel: (Brooks) Ha G egyszerű összefüggő gráf, nem K_n , nem $C_{2k+1} \Rightarrow \chi(G) \leq \Delta$

Tétel: (Mycielski konstrukciója) $\forall 2 \leq k$ egésze $\exists G_k$ gráf, hogy $\omega(G_k) = 2$ és $\chi(G_k) = k$

Bizonyítás:

G_2 -nek megfelel: $\bullet - \bullet$.

Tegyük fel, hogy már G_k -t megalkottuk, készítünk ebből G_{k+1} -et! G_k pontjai: $a_1, a_2, \dots, a_n$. Vegyünk fel $n + 1$ új pontot: $b_1, b_2, \dots, b_n, c$ -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: $\omega(G_k + 1) = 2$

Bizonyítás: (indirekt)

Tegyük fel, hogy $\exists G_{k+1}$ -ben háromszög (Δ). Ennek nem lehet mind a 3 csúcsa 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 a_x és a_y lehet.

Mivel b_i szomszédjai megegyeznek a_i szomszédjaival, ekkor nemcsak $b_i a_x a_y$, hanem $a_i a_x a_y$ is Δ lenne.

→ ELLENTMONDÁS.

Állítás: $\chi(G_{k+1}) \leq k + 1$

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

Állítás: $\chi(G_{k+1}) \neq k$

Bizonyítás: (indirekt)

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

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

Megadunk egy f' színezést az a_i pontok által feszített részgráfban (ami 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 G_k -nak, ami *ellentmondás*, mert $\chi(G_k) = k$.

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 $f'(a_i) = f'(a_j)$!

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

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

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

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

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

→ Ellentmondás ⇐

$$\Rightarrow \Rightarrow \chi(G_k) = k$$

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

→ → ELLENTMONDÁS ⇐

5.) Síkbarajzolható gráfok kromatikus száma. Élgráf fogalma, élkromatikus szám, viszonya a maximális fokszámmal, Vizing-tétel (biz. nélkül). Perfekt gráfok. Páros gráf és komplementere perfektsége.

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 síkba rajzolható gráf, akkor $\chi(G) \leq 5$

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 G egy $3 \leq n$ pontú egyszerű síkba rajzolható gráf. Ha $\forall$ pont foka legalább 6 lenne, akkor ez teljesülne rá:

$$3n - 6 \geq e = \frac{\sum d(v)}{2} \geq \frac{6n}{2} = 3n \quad \Leftarrow \text{ELLENTMONDÁS} \Rightarrow \exists G\text{-nek legfeljebb 5-ödfokú csúcsa. Jelöljük } x\text{-szel.}$$

Ha $G - x$ is egyszerű síkba rajzolható gráf, az indukciós feltevés miatt 5-színezhető.

Ha 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 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 G' gráf – az indukciós feltétel miatt – 5-színezhető.

Az ennek megfelelő színezés G -ben nem jó, mert x, y, z egyszínűek. 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 $\Rightarrow \chi(G) \leq 4$

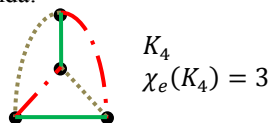
Ezt a tételt Appel és Haken bizonyította be először 1977-ben. Itt alkalmaztak először bizonyításhoz számítógépes módszereket.

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

Def.: A G gráf **k -élszínezhető**, ha G élei k színnel színezhetőek úgy, hogy szomszédos élek különböző színt kapnak. A G gráf élkromatikus száma $\chi'(G) = \chi_e(G) = \chi(L(G)) \leq k$, ha G k -élszínezhető, de G nem $(k - 1)$ -élszínezhető (ha G élei k színnel színezhetőek, de $k - 1$ -gyel nem).

Megj.: G k -élszínezhető $\Leftrightarrow L(G)$ k -színezhető, továbbá $\chi'(G) = \chi(L(G))$.

Példa:

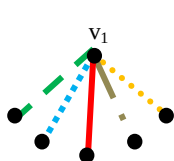


Állítás: tetsz. G gráfra $\omega(L(G)) \geq \Delta(G)$, továbbá, ha $\Delta(G) \geq 3$, akkor $\omega(L(G)) \geq \Delta(G)$.

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: $\chi_e(G) \geq \Delta(G)$ tetszőleges G gráfra.

Biz.: az egy csúcsból induló élek egymástól különböző színt kapnak, és ez speciálisan a max. foksámú csúcsból induló élekre is igaz. Formálisan: $\chi'(G) = \chi(L(G)) \geq \omega(L(G)) \geq \Delta(G)$.



Tekintsük a gráf egy max. fokú csúcsát! (v_1)

Ennek Δ db szomszédja van. Az ezekhez húzott élek különböző színt kell, hogy kapjanak.

Kőnig tétel: Ha $G = (A, B; E)$ páros gráf, akkor $\chi_e(G) = \Delta(G)$.

Biz.: az előző állítás miatt elegendő azt igazolni, hogy $\chi'(G) \leq \Delta(G)$, azaz csupán egy $\Delta(G)$ -élszínezést kell mutatni.

$\exists$ olyan H ps. gráf, melynek G részgráfja, és H minden csúcsának foka $\Delta(G)$. (Ilyen H -t pl. úgy kaphatunk, hogy G mellé felvesszük még G -nek egy $G' = (A', B'; E')$ másolatát, H színesztályai $A \cup B'$ és $B \cup A'$ lesznek, és $\forall v$ csúcs és annak v'

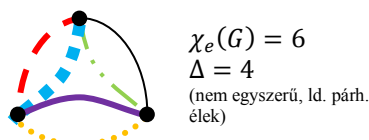
másolata közé behúzzunk további $\Delta(G) - d(v)$ párhuzamos élt.) Ha sikerül a $\Delta(G)$ -reguláris H gráf éleit $\Delta(G)$ színnel kiszínezni, akkor egyúttal a G részgráf éleinek is megkapjuk egy ugyanennyi színnel való színezését.

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 $(\Delta(G) - 1)$ -reguláris páros gráfot alkotnak, abban is találunk egy teljes psítást, ez a második színt kapja, stb.

Miért $\exists$ 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 $\exists$ teljes psítás, és pontosan ezt kellett bizonyítanunk.

Tétel: (Vizing) Ha G egyszerű $\Rightarrow \chi_e(G) \leq \Delta + 1$

Ellenpélda:



Perfekt gráfok

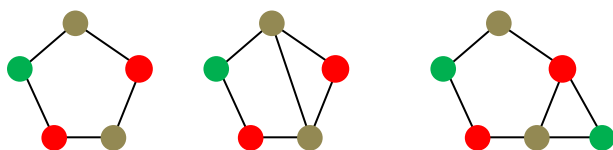
Egy gráf kromatikus száma és klikkszám között általában nem tételeztünk fel egyenlőséget. Mégis igen sok példa van arra, amikor ez a két paraméter egyenlő (pl. páros gráfok). Felmerül a kérdés: érdemes-e közelebbről is megvizsgálni ezeket a gráfokat.

A válasz igen, ha még kikötjük, hogy ne csak magára a gráfra, hanem $\forall$ feszített részgráfjára is igaz legyen. Enélkül ugyanis tetszőleges gráfot kiegészíthetnénk egy elegendően nagy klikk hozzá vételével.

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

Megjegyzés: Ez a halmaz tartalmazza magát G -t is!

Példák:



C_5 :

$$\chi(C_5) = 3$$

$$\omega(C_5) = 2$$

nem perfekt ✗

$$\omega(C_5) = 3$$

$$\chi(C_5) = 3$$

+ $\forall$ fesz. részgráfjára

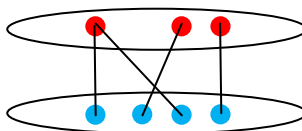
$$\chi' = \omega'$$

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. $\rightarrow$ ezek **perfektek** ✓

Páros gráf élgráfjának és ennek komplementerének perfektsége. Intervallumgráfok perfektsége, perfekt gráf tétel ([Lovász-tétel] biz. nélkül), erős perfekt gráf tétel (biz. nélkül).

Tétel: Ha G komplementere páros gráf, akkor G perfekt.

Biz.: Ha G páros gráf komplementere, akkor $G \forall$ feszített részgráfja is páros gráf komplementere, ezért elegendő azt bizonyítani, hogy $\chi(G) = \omega(G)$, ha G komplementere páros. König 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 $\nu(\overline{G})$

éleiből álló, M maximális psítást, és $\forall$ csúcsot kül. színnel színezzünk, kivéve, hogy $M \forall$ élének végpontjai azonos színt kapnak. Ezáltal a felhasznált színekben az n -hez képest $\nu(\overline{G})$ megtakarítást érünk el.

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 $L(G) \forall$ klikkje G egy csúcsból induló élének felel meg, így $\omega(L(G)) = \Delta(G)$. König páros gráfok élszínezéséről szóló tételének felhasználásával $\omega(L(G)) = \Delta(G) = \chi'(G) = \chi(L(G))$ következik. ■

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 $\chi(\overline{L(G)}) \leq \omega(\overline{L(G)})$ tetszőleges G gráfra (a másik irányú egyenlőtlenség triviális).

A König-tétel alapján $\omega(\overline{L(G)}) = \alpha(L(G)) = \nu(G) = \tau(G)$, ezért elegendő $\tau(G)$ színnel kiszínezni $\overline{L(G)}$ -t. Legyen $U \subset V(G)$ egy $\tau(G)$ pontból álló lefoglaló ponthalmaz, és válasszunk $G \forall$ éléhez e -nek egy U -beli végpontját. Ha $\forall$ élt a kiválasztott végpontnak megfelelően színezzünk, 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.

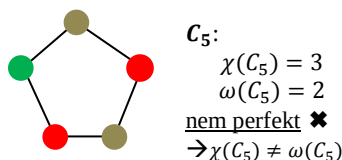
Tétel: (Erős perfekt gráf tétel) G perfekt $\Leftrightarrow$ sem G , sem $\overline{G}$ nem feszít (nem tart. fesz. részgr.-ként) min. 5-hosszú páratlan kört.

Bizonyítás: (szükségesség)

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

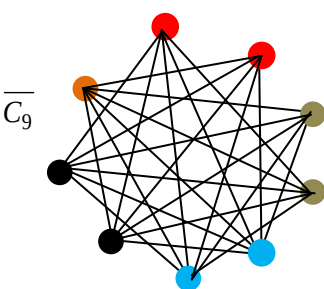
Állítás: $(2 \leq k) C_{2k+1}$ nem perfekt.

Bizonyítás:



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

Bizonyítás:



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. $\Rightarrow \omega(\overline{C_{2k+1}}) = k$
 Mivel $\forall$ színt legfeljebb kétszer használhatjuk $\Rightarrow k$ színnel csak $2k$ csúcs lefesthető $\Rightarrow \chi(\overline{C_{2k+1}}) \geq k+1$. Ebből és az előbbiből következik, hogy **nem perfekt**.
 (Valójában $k+1$ szín elég is, tehát $\chi(\overline{C_{2k+1}}) = k+1$)

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 G perfekt $\Rightarrow \overline{G}$ perfekt irányt, akkor $H := \overline{\overline{G}}$ jelöléssel a $\overline{G}$ perfekt $\Rightarrow G$ perfekt átírható H perfekt $\Rightarrow \overline{H}$ alakra. ($H = \overline{\overline{G}}$, illetve $\overline{\overline{H}} = \overline{\overline{\overline{G}}} = G$)

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



Def.: $I_1, I_2, \dots, I_k$ a számegyenes korlátos és zárt intervalluma.

$$v(G) := \{I_1, I_2, \dots, I_k\}$$

I_i szomszédos I_j -vel $\Leftrightarrow$ ezek metszők ($i \neq j$)

} G intervallumgráf

Tétel: $\forall$ intervallumgráf perfekt.

Bizonyítás:

Mivel az intervallumgráfok feszített részgráfjai is intervallumgráfok, elég azt belátni, hogy $\chi = \omega$.

Legyen $\omega(G) = k$, mivel $\omega(G) \leq \chi(G)$, ezért elég azt belátni, hogy $\chi(G) \leq k$.

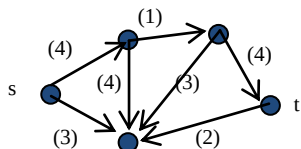
Kezdjük el színezni az intervallumokat balról jobbra! A még színezetlen intervallumok közül mindig azt színezzük ki, amelyiknek baloldali végpontja a legbalrább van. Ha egy intervallumot $k + 1$ -edik színnel kellene színezni, akkor ez azt jelenti, hogy ennek az intervallumnak a bal vége benne van már k intervallumban, amik már elhasználták az $1, 2, \dots, k$ színt. Így van $k + 1$ intervallum, amelyek közül bármely kettő metszi egymást. $\Rightarrow \exists G$ -ben $k + 1$ méretű klikk.

ELLENTMONDÁS ✂

6.) Hálózat, hálózati folyam és (s, t) -vágás fogalma, folyam értéke, (s, t) -vágás kapacitása. Ford-Fulkerson tétel, Edmonds-Karp tétel (biz. nélkül), egészértékűség lemmája. A folyamprobléma általánosításai.

Def.: Hálózatnak 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.
Röviden: ha $\vec{G}$ irányított gráf, $s, t \in v(\vec{G})$, $c: E(\vec{G}) \rightarrow \mathbb{R}^+$

Példa:

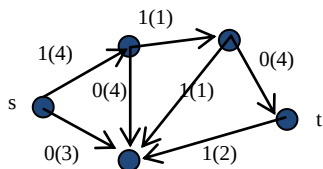


Def.: f folyam egy $f: E \rightarrow \mathbb{R}^+$ fv. (olyan fv., amely az élekhez valós számokat rendel), amire teljesül:

- 1.) $\forall e \in E(\vec{G}) - re \quad 0 \leq f(e) \leq c(e)$
- 2.) $\forall v \in V(\vec{G}), v \neq s, t - re \quad \sum_{e \rightarrow v} f(e) = \sum_{e \leftarrow v} f(e)$

$$\sum_{e \rightarrow s} f(e) = \sum_{e \leftarrow t} f(e)$$

Példa: fvérték(kapacitás) alakban:



Def.: f folyam értéke:

$$m_f = \sum_{e \rightarrow s} f(e) - \sum_{e \leftarrow s} f(e) = \sum_{e \rightarrow t} f(e) - \sum_{e \leftarrow t} f(e)$$

A folyam értékének meghatározására az s , ill. t -n kívül:

$x \in v(\vec{G}), s \in X \not\equiv t$,

$$m_f = \sum_{e \rightarrow x} f(e) - \sum_{e \leftarrow x} f(e) \text{ vagy } m_f := \sum \{f(sv)\} - \sum \{f(vs)\}, v \in V(G)$$

Def.: $X \subseteq v(\vec{G}), s \in X \not\equiv t$

X és $V(\vec{G}) \setminus X$ között futó élek halmazát a hálózat egy **st -vágásának** nevezzük,

jele: C , értéke:

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

st -vágás kapacitása az X -ből és $V \setminus X$ -be futó élek kapacitásösszege, azaz $\sum \{c(xv): x \in X \not\equiv v \in V(G)\}$

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

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

Algoritmus:

- I. Kiindulunk egy tetszőleges folyamból (Pl.: $f \equiv 0$)
- II. Javítás $\Rightarrow m_f$ nő
- III. Ha nincs több javítás $\Rightarrow$ STOP

A javítást egy ún. **segédgráffal** tudjuk elvégezni.

Def.: a $(\vec{G}, s, t, c)$ hálózat f folyamához tartozó $\vec{H}_f$ segédgráf: $V(\vec{H}_f) = V(\vec{G})$

$$1.) \left. \begin{array}{l} \overrightarrow{xy} \in E(\vec{G}) \\ f(\overrightarrow{xy}) < c(\overrightarrow{xy}) \end{array} \right\} \Rightarrow \overrightarrow{xy} \in \vec{H}_f \quad 2.) \left. \begin{array}{l} \overrightarrow{xy} \in E(\vec{G}) \\ 0 < f(\overrightarrow{xy}) \end{array} \right\} \Rightarrow \overrightarrow{yx} \in \vec{H}_f$$

Javitóút: $\vec{H}_f$ -ben irányított út s -ből t -be.

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

$$d := \min(\{c(e) - f(e) : e \in P, \quad e(1) - es\} \cup \{f(e) : e \in P, \quad e(2) - es\})$$

$$f(e) = \begin{cases} f(e) + d, & \text{ha } e \in P, \quad e(1) - es \\ f(e) - d, & \text{ha } e \in P, \quad e(2) - es \\ f(e), & \text{ha } e \notin P \end{cases}$$

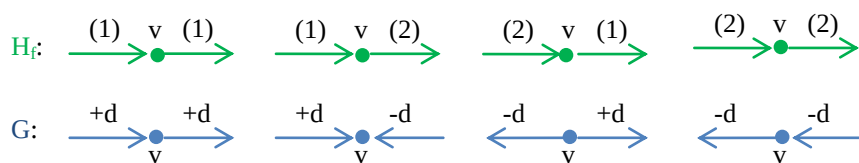
Fontos kiegészítés az „algorithmus” III. pontjához:

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

Állítás: a segédgráf javítás után f folyam marad.

Bizonyítás:

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



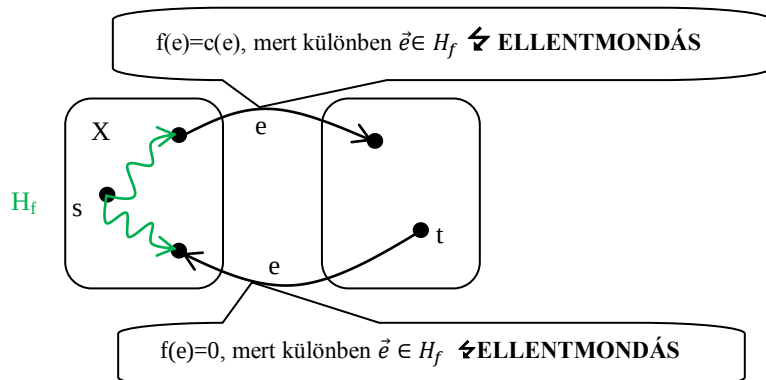
Tétel: Ha nincs javítóút H_f -ben $\Leftrightarrow f$ maximális folyam

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 $\Rightarrow s \in X \nrightarrow t$



A fentiekből következik:

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

Tétel: (Ford-Fulkerson)

$$\max_{f \text{ folyam}} m_f = \min_{c \text{ vágás}} c(C), \text{ vagyis a maximális folyam értéke egyenlő a minimális vágás értékével. (MF = MC)}$$

Bizonyítás:

A maximális folyam nyilván nem lehet nagyobb a minimális vágásnál, hiszen ha $\forall$ 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. ✓

Tétel: (Edmonds-Karp)

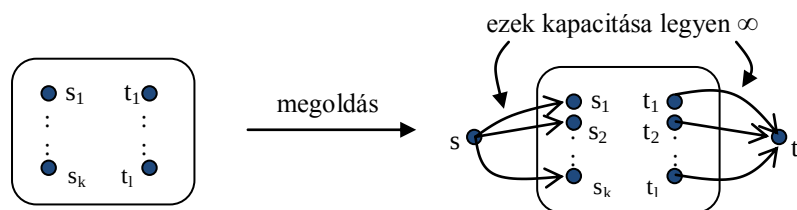
Ha H_f -ben mindig a legrövidebb utat választjuk, akkor az algoritmus véges sok lépésben leáll és polinomiális lépésszámú.

Egészértékűség lemmája: Ha $\forall e \text{ élre } c(e) \text{ egész} \Rightarrow \exists \text{ olyan } f \text{ max. folyam, amire } \forall e \text{ élre } f(e) \text{ egész.}$

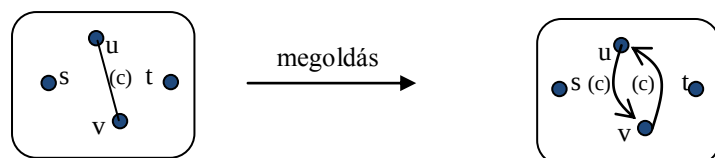
Bizonyítás: Az algoritmus nem lép ki $\mathbb{N}$ -ből (csupa 0-ból indítva).

A folyamprobléma általánosítása:

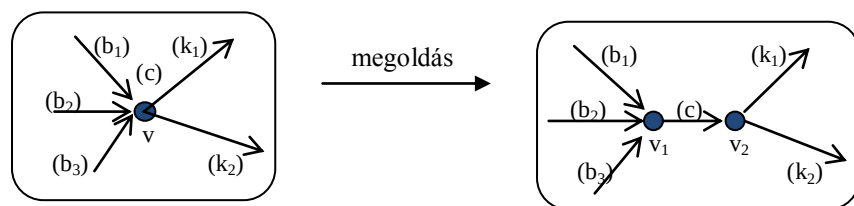
1.) több termelő/fogyasztó



2.) irányítatlan élek



3.) kapacitással rendelkező csúcsok



7.) Menger tételei (4). Többszörös összefüggőség és élösszefüggőség (jellemzésük pont-, ill. éldisjunkt utak segítségével). Dirac tétele (biz. nélkül).

Def.: a G gráf u pontjából v pontjába futó P és Q útjait éldisjunkt taknak/pontdisjunkt taknak nevezzük, ha

$$E(P) \cap E(Q) = \emptyset \quad / \quad V(P) \cap V(Q) = \{u, v\}$$

Def.: G gráf U élhalmaza/ponthalmaza lefog $\forall uv$ utat, ha $G - U$ -ban $\nexists u$ -ból v -be út.

Tétel: (Menger I.)

Az s -ből t -be menő, páronként éldisjunkt irányított 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 $\max\{ \} \leq \min\{ \}$.

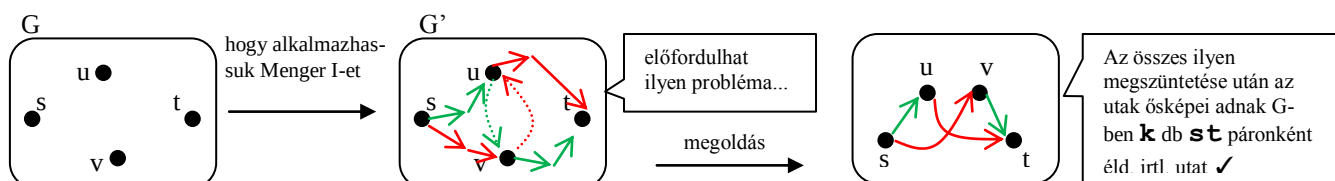
Tfh. k az st utakat lefogó élek minimális száma. Legyen $\forall$ él kapacitása 1. Az így kapott hálózatban a minimális vágás értéke legalább k . Ekkor a Ford-Fulkerson tétel értelmében a maximális folyam is k értékű.

Van olyan maximális folyam, melyben $\forall$ élen a folyamérték 0 vagy 1 (egészértékűségi lemma miatt). Lássuk be, hogy G -ben $\exists k$ éldisjunkt 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 éldisjunkt irányított utat kapunk.

Tétel: (Menger II.)

G irányítatlan gráf, $s, t \in V(G)$.

Az s -ből t -be menő páronként éldisjunkt irányítatlan utak maximális száma = az st -utakat lefogó élek minimális számával.



Bizonyítás:

Készítsük el a G' -t G -ből úgy, hogy $G \forall$ élt irányítjuk oda és vissza.

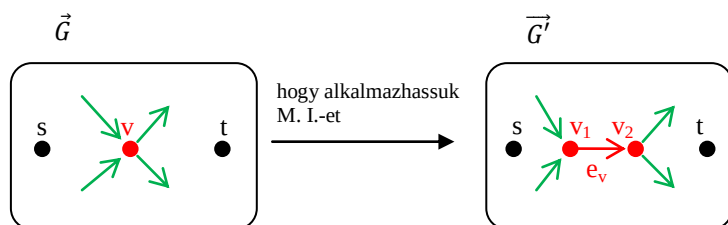
Ha G' -ben van k db él, melyek lefogják k db st irányított éldisjunkt utat $\Rightarrow$ ezek ősei lefogják az st utakat G -ben.

Tétel: (Menger III./IV.)

G irányított/irányítatlan gráf, $s, t \in V(G)$. Az st páronként pontdisjunkt irányított/irányítatlan utak maximális száma = az st utakat (s és t nem szomszédos csúcsok használata nélkül) lefogó pontok minimális számával.

Bizonyítás:

M.III.:

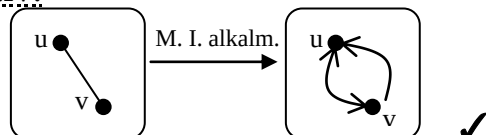


Ha G' -ben van k éldisjunkt st út $\Rightarrow G$ -ben van k db pontdisjunkt út.

Probléma: ha G' -ben van k db él, melyek lefogják az st utakat, akkor ezek G -ben pontok vagy élek?

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

M.IV.:



Def:

G k -szorosan élösszefüggő, ha bárhogyan legfeljebb $k - 1$ élt elhagyva összefüggő marad.

G k -szorosan pontösszefüggő, ha bárhogyan legfeljebb $k - 1$ pontját elhagyva összefüggő marad és legalább $k + 1$ pontja van.

k élösszefüggő $\Rightarrow k - 1$ élösszefüggő és

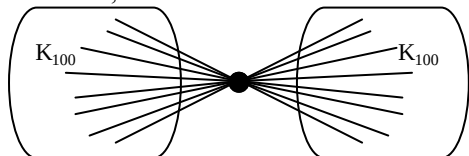
k (pont)összefüggő $\Rightarrow k - 1$ összefüggő.

(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-élőf.:



Tétel: (Menger V., VI.)

M. V.: G k -élösszefüggő $\Leftrightarrow$ Bármely 2 pont között $\exists k$ db páronként éldisjunkt út.

M. VI.: G k -összefüggő $\Leftrightarrow$ Bármely 2 pont között $\exists k$ db páronként pontdiszjunkt út és $k + 1$ pontja van.

Bizonyítás:

$\Leftarrow$: (**M. V.**, **M. VI.**): $k - 1$ él/pont elhagyásakor tetszőleges s -ből t -be van út, mert volt k db éldisjunkt/pontdiszjunkt út, $k - 1$ törlése csak $k - 1$ -et ronthatott el.

$\Rightarrow$: (**M. V.**): Tfh. s, t között nincs k db éldisjunkt 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!

$\rightarrow$ ELLENTMONDÁS $\Leftarrow$

$\Rightarrow$: (**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.

$\rightarrow$ ELLENTMONDÁS $\Leftarrow$

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 szétesen. 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.

8. Oszthatóság, prímek, prímek száma, hézag mérete szomszédos prímek között, a számelmélet alaptétele (biz. nélkül). Legnagyobb közös osztó, legkisebb közös többszörös, osztók száma. Euklideszi algoritmus.

Oszthatóság, felbonthatatlan és prím tulajdonságú számok, ezek kapcsolata (bizonyítás csak az egyik irányban), a számelmélet alaptétele. Osztók száma és összege. Nevezetes tételek prímszámokról: prímek száma, hézag a szomszédos prímek között, $\pi(n)$ nagyságrendje (biz. nélkül), prímek számtani sorozatokban (Dirichlet tétele) (biz. nélkül).

Def.: a osztója b -nek, ha $\exists c \in \mathbb{Z}$, hogy $a \cdot c = b$. Jele: $a|b$.

p felbonthatatlan ($|p| \neq 1$), ha $p = a \cdot b \rightarrow |a| = 1$ vagy $|b| = 1$, $a, b \in \mathbb{Z}$

p prímszám ($|p| \neq 1$), ha $p|a \cdot b \rightarrow p|a$ vagy $p|b$

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:

$\Rightarrow$: 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 $b|p \Rightarrow |b| = |p| \Rightarrow |a| = 1$ ✓

$\Leftarrow$: nem kell vizsgán

Tétel: (számelmélet alaptétele) Minden n ($2 \leq n$) a sorrendtől és előjelektől eltekintve egyértelműen felbontható felbonthatatlanok sorozatára.

Másképp: 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)

felbonthatatlan ✓

$\therefore$
 n

$n = a \cdot b$

a, b felbonthatatlan ✓

$\therefore$
 $\therefore$

$n = a_1 \cdot a_2 \cdot b$

$\therefore$
 $\therefore$

$a_1 \cdot a_2 \cdot b$ felbonthatatlan ✓

...

(egyértelműség)

Tfh. n két különböző módon felbontható:

$n = p_1 \cdot p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_l$

p_1 prím; $p_1|q_1 \cdot q_2 \cdot \dots \cdot q_l \Rightarrow p_1|q_1$ vagy $p_1|q_2$ vagy ... vagy $p_1|q_l$

Pl.: $p_1|q_1$, de q_1 felbonthatatlan, $q_1 = p_1 \cdot c \Rightarrow |p_1| = 1$, de $|p_1|$ prím, nem lehet 1! ✗

vagy

$|c| = 1 \Rightarrow$ ez azt jelenti, hogy $|p_1| = |q_1|$

$\rightarrow$ visszaveztük a problémát egy egyszerűbb esetre:

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

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

Következmény: prímtenyezős felbontás / **kanonikus alak:** $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \dots \cdot p_k^{\alpha_k} = \prod_{i=1}^k p_i^{\alpha_i}$

kan. alakban $p_1 \cdot p_2 \cdot \dots \cdot p_k$ kül. pozitív felbonthatatlanok, $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{Z}^+$; ált. $p_1 < p_2 < \dots < p_k$

Figyeljük meg, hogy jöllehet ∞ sok prímszám van, csak véges sok kitevő lesz pozitív, tehát csak véges sok 1-től különböző szám szorzatát képezzük.

Osztók száma: jele: $d(n)$

pl.: $n = 2^3 \cdot 3^2 \cdot 7^4$

$\begin{matrix} & 0 & 1 \\ 0 & & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 3 \end{matrix}$

$d|n$, ha $d = 2^3 \cdot 3^2 \cdot 7^4$, $d(2^3 \cdot 3^2 \cdot 7^4) = (3+1)(2+1)(4+1)$

általános: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$, $d(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \dots \cdot (\alpha_k + 1) = \prod_{i=1}^k (\alpha_i + 1)$

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

pl.: $n = 36 = 2^2 \cdot 3^2$, $\sigma(36) = (1 + 2 + 2^2)(1 + 3 + 3^2) = 91$

általánosan: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$,

$$\sigma(n) = (1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1}) \cdot (1 + p_2 + p_2^2 + \dots + p_2^{\alpha_2}) \cdot \dots \cdot (1 + p_k + p_k^2 + \dots + p_k^{\alpha_k}) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \dots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$$

$$= \prod_{i=1}^k \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

Tétel: ∞ sok prímszám $\exists$.

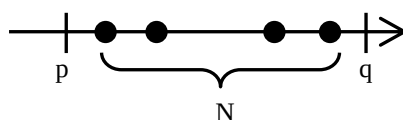
Biz.: (indirekt) tfh. véges sok van: $p_1, p_2, \dots, p_n$. $A := p_1 \cdot p_2 \cdot \dots \cdot p_n + 1 \rightarrow$ nagyobb $\rightarrow A$ -nak van prímosztója, de $A \neq p_1 \cdot p_2 \cdot \dots \cdot p_n$ -nel osztva 1 maradékot ad. $\Leftarrow$

Másképp: elegendő megmutatni, hogy $\forall 2 \leq n \in \mathbb{N}$ -re $\exists n$ -nél nagyobb prím. Mivel $n!$ az $1, 2, \dots, n$ számok mindegyikével osztható $\rightarrow N := n! + 1$ az $1, 2, \dots, n$ számok mindegyikéhez relatív prím, tehát N nem osztható egyetlen n -nél kisebb prímmel sem. N kan. alakjában csak n -nél nagyobb prímek fordulnak elő.

Tétel: $\forall N$ -re $\exists p, q$ szomszédos prímek, amelyekre $N \leq |p - q|$.

Tetsz. hosszú sorozat képezhető szomszédos összetett számokból $\rightarrow$ bármely $n \in \mathbb{N}$ -re $\exists$ olyan N , melyre az $N + 1, N + 2, \dots, N + n$ számok mindegyike összetett.

Biz.: azaz: $\exists N$ db szomszédos összetett szám



$$\left. \begin{array}{l} 2|(N+1)!+2 \\ 3|(N+1)!+3 \\ \vdots \\ N+1|(N+1)!+N+1 \end{array} \right\} N \text{ db, mindegyik összetett } \checkmark$$

Legyen $N := (n + 1)! + 1$. $\rightarrow$ tetsz. $2 \leq k \leq n + 1$ esetén $k|(n + 1)! + k = N + (k - 1) \rightarrow N + 1, N + 2, \dots, N + n$ számok mindegyike összetett.

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

Tétel: („nagy prímszámtétel”) $\Pi(n) \approx \frac{n}{\ln n}$; $\approx$: aszimptotikus egyenlőség, jelentése: $\lim_{n \rightarrow \infty} \frac{\Pi(n)}{\frac{n}{\ln n}} = 1$

Tétel: (Dirichlet) ha $(a, b) = 1 \rightarrow \infty$ 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 $(0, 0) = \text{nem értelmezett}$.

(rel. 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.: $[-5, -17] = 85$, $[-9, 0] = 0$, $[0, 0] = 0$.

Euklideszi algoritmus (ennek alkalmazása lineáris kongruenciák megoldására is). Kétismeretlenes, lineáris diofantikus egyenlet megoldása (konkrét példán). Két kongruenciából álló kongruenciarendszer megoldása (konkrét példán).

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 $a_0 \geq a_1 \geq \dots \geq a_i$ 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 $(a, b) = a_k$

Pl.: $(360, 225) = ?$

$$360 = 1 \cdot 225 + 135$$

$$225 = 1 \cdot 135 + 90$$

$$135 = 1 \cdot 90 + 45$$

$$90 = 2 \cdot 45 + 0$$

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.

$$(a, b) = (a_0, a_1) = \left(\underbrace{a_0 - q_1 a_1}_{a_2}, a_1 \right) = (a_1, a_2) = \left(\underbrace{a_1 - q_2 a_2}_{a_3}, a_2 \right) = (a_2, a_3) = \dots = \left(a_k, \underbrace{a_{k+1}}_0 \right) = a_k \checkmark$$

9.) Kongruencia fogalma, alpműveletek kongruenciákkal. Lineáris kongruenciák megoldása euklideszi algoritmussal, a megoldhatóság feltétele, megoldások száma.

Kongruencia

Def1.: $a \equiv b \pmod{m}$ [a kongruens b-vel modulo m]; ha a és b m-mel osztva ugyanazt a maradékot adja

Def2.: $a \equiv b \pmod{m} \Leftrightarrow m \mid a - b$

Pl.: $17 \equiv 52 \equiv -4 \pmod{7}$

Tétel:

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

Biz.:

$$(1) \left. \begin{array}{l} m \mid a - b \\ m \mid c - d \end{array} \right\} \Rightarrow m \mid (a + c) - (b + d) \Rightarrow a + c \equiv b + d \pmod{m} \quad \checkmark$$

$$(2) \left. \begin{array}{l} m \mid a - b \xrightarrow{\cdot c} m \mid ac - bc \\ m \mid c - d \xrightarrow{\cdot b} m \mid bc - bd \end{array} \right\} \oplus \Rightarrow m \mid ac - bd \Rightarrow ac \equiv bd \pmod{m} \quad \checkmark \quad \text{Speciális esete: } \left. \begin{array}{l} a \equiv b \pmod{m} \\ c \equiv c \pmod{m} \end{array} \right\} \Rightarrow ac \equiv bc \pmod{m} \quad \checkmark$$

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

Tétel:

$$\text{ha } c \mid a \text{ és } c \mid b \text{ és } ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{(m,c)}}$$

$$m := m' \cdot (m, c), \quad c := c' \cdot (m, c) \Rightarrow (m', c') = 1$$

$$m \mid ac - bc \Leftrightarrow m \mid c(a - b) \Leftrightarrow m' \mid c'(a - b) \Leftrightarrow m' \mid a - b \quad \checkmark$$

Def.: lineáris kongruencia: $ax \equiv b \pmod{m}$, adottak: $a, b, m \in \mathbb{Z}$; kérdés: $x = ?$

Pl.: $6x \equiv 7 \pmod{15}$,

$$3 \mid 15 \mid \underbrace{6}_{3 \mid 6} x - \underbrace{7}_{3 \nmid 7} \Rightarrow \nexists \text{ megoldása!}$$

Tétel: Az $ax \equiv b \pmod{m}$, $a \neq 0$ lin. kongruencia megoldható $\Leftrightarrow (a, m) \mid b$

A kongruencia megoldáshalmaza (a, m) darab maradékosztály modulo m.

biz.: Legyen $d := (a, m)$, $a = a'd$, $m = m'd$, $b = b'd$

Ha $ax \equiv b \pmod{m}$, megoldható $\Rightarrow d \mid m \mid ax - b$ és $d \mid a \mid ax$ miatt $d \mid ax - (ax - b) = b \quad \checkmark$

Elégségesség bizonyítása: tñh. $d \mid b$. A kongruenciát d-vel végigosztva $a'x \equiv b' \pmod{m'}$ 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 $p \mid ka' + lm' = 1$ állna $\Rightarrow (k, m') = 1$.

$$a'x \equiv b' \pmod{m'} \xLeftrightarrow{(k, m')=1} ka'x \equiv kb' \pmod{m'} \Leftrightarrow \left. \begin{array}{l} (1 - lm')x \equiv kb' \pmod{m'} \\ lm'x \equiv 0 \pmod{m'} \end{array} \right\} \oplus \Rightarrow x \equiv kb' \pmod{m'}$$

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:

$$x \equiv kb' + dm' \pmod{m}, \quad d = 0, 1, \dots, (d - 1)$$

Lineáris kongruenciák megoldása euklideszi algoritmussal, a megoldhatóság feltétele, megoldások száma

Példa: lin. kongr. megoldása eukl. alg. segítségével:

$$59x \equiv 1 \pmod{101}, \quad x = ?$$

Először meghatározzuk LNKO-t:

$$(101, 59) = ?$$

$$101 = 1 \cdot 59 + 42$$

$$59 = 1 \cdot 42 + 17$$

$$42 = 2 \cdot 17 + 8$$

$$17 = 2 \cdot 8 + 1$$

$$8 = 8 \cdot \frac{1}{1} + 0$$

$$\frac{1}{1} \checkmark$$

$$\exists 1 \text{ mo.}$$

Ezután az egyenletekből kifejezzük a maradékokat:

$$\begin{aligned}
42 &= 101 - 1 \cdot 59 \equiv (-1) \cdot 59 \pmod{101} \\
17 &= 59 - 42 \equiv 59 - 1 \cdot 59 = 2 \cdot 59 \pmod{101} \\
8 &= 42 - 2 \cdot 17 \equiv (-1) \cdot 59 - 2 \cdot 2 \cdot 59 = (-5) \cdot 59 \pmod{101} \\
1 &= 17 - 2 \cdot 8 \equiv 2 \cdot 59 - 2 \cdot (-5) \cdot 59 = 12 \cdot 59 \pmod{101} \rightarrow \\
1 &\equiv 12 \cdot 59 \pmod{101} \\
59x &\equiv 1 \equiv 12 \cdot 59 \pmod{101} \quad / : 59 \\
x &\equiv 12 \pmod{101} \blacksquare
\end{aligned}$$

Példa 2.: $62x \equiv 24 \pmod{36}$

$$\begin{aligned}
62x &\equiv 24 \pmod{36} \rightarrow 62 \equiv 26 \pmod{36} \\
26x &\equiv 24 \pmod{36} \rightarrow (26, 36) = 2, \text{ osztunk:} \\
13x &\equiv 12 \pmod{18} \rightarrow 13 \equiv -5 \pmod{18} \\
-5x &\equiv 12 \pmod{18} \rightarrow \cdot (-1) \\
5x &\equiv -12 \pmod{18}, \\
5x &\equiv 6 \pmod{18} \rightarrow \cdot 7 \text{ (7 rel. prím a 18-hoz!)} \\
35x &\equiv 42 \pmod{18}, \\
-x &\equiv 6 \pmod{18} \rightarrow \cdot (-1) \\
x &\equiv -6 \equiv 12 \pmod{18} \rightarrow 36 \text{ modulusra áttérünk} \\
x &\equiv 12 \pmod{36} \text{ VAGY } x \equiv 12 + 18 = 30 \pmod{36}. \blacksquare
\end{aligned}$$

Példa: kétismeretlenes, lineáris diofantikus egyenlet megoldása

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

$$by = c - ax$$

$b|c - ax \rightarrow ax \equiv c \pmod{b}$. Tehát visszavezettük a problémát egy lin. kongr. megoldására.

$$\begin{aligned}
59x + 101y &= 1 \\
101y &= 1 - 59x \\
101|1 - 59x &\Rightarrow 59x \equiv 1 \pmod{101}
\end{aligned}$$

Előzőleg láttuk, hogy ennek megoldása az $x \equiv 12 \pmod{101}$, tehát

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

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

Példa: Két kongruenciából álló kongruenciarendszer megoldása

$$\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv -1 \pmod{8} \end{cases} x = ?$$

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

$$\begin{aligned}
7k + 3 &\equiv -1 \pmod{8} \quad / -3 \\
7k &\equiv -4 \pmod{8} \quad / -8k \\
-k &\equiv -4 \pmod{8} \quad / \cdot (-1) \\
k &\equiv 4 \pmod{8} \Rightarrow k = 8l + 4 \text{ alakú } l \in \mathbb{Z} \Rightarrow \\
x = 7k + 3 &= 7(8l + 4) + 3 = 56l + 31 \text{ alakú} \Rightarrow \\
x &\equiv 31 \pmod{56}
\end{aligned}$$

--- (valszeg nem kell, de hátha mégis):

Tétel: (Wilson) Legyen $2 \leq k \in \mathbb{Z}$, ekkor:

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

biz.:

$$k = 4\text{-re nyilvánvaló: } 3! = 2 \cdot 3 = 6 \equiv 2 \pmod{4}$$

Ha $6 \leq k$ összetett, akkor vagy található két ilyen különböző $1 < a < b < k$ egész, melyekre $ab = k$, és akkor $1 \cdot 2 \cdot \dots \cdot (n-1) = abc \equiv 0 \pmod{k}$, 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 $ab \equiv 1 \pmod{p}$, hiszen az $ax \equiv 1 \pmod{p}$ kongruenciát pontosan egy $\text{mod } p$ maradékosztály oldja meg.

Látható, hogy ha a -hoz b , akkor b -hez a tartozik, tehát az $1, 2, \dots, p-1$ számok úgy rendezhetők párokba, hogy $\forall$ pár szorzata 1-et ad maradékosztály p -vel osztva. A párokba rendezés azért nem egészen pontos, mert bizonyos számok esetleg

önmagukkal állnak párban. Ezekre az a számokra $a^2 \equiv 1 \pmod{p}$ teljesül, azaz $p|a^2 - 1 \Leftrightarrow p|(a+1)(a-1) \xrightarrow{p \text{ prím}} p|a+1$ vagy $p|a-1 \Rightarrow$ az önmagukkal párban álló számok kizárólag az 1 és $(p-1)$ lesznek. Átrendezve a $(p-1)!$ -t, $\forall$ prím szorzata 1 lesz, és lesznek még a páratlanul maradt 1 és $(p-1) \Rightarrow (p-1)! \equiv 1 \cdot 1 \cdot \dots \cdot 1 \cdot (p-1) \equiv p-1 \equiv -1 \pmod{p} \blacksquare$.

10.) Teljes és redukált maradékrendszer fogalma, φ -függvény, kiszámítása. Euler-Fermat-tétel, kis Fermat-tétel.

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 $\forall$ szám relatív prím p prímmel

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

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

$$\begin{aligned} \text{Ha } n &= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k} \Rightarrow \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \dots \cdot \varphi(p_k^{\alpha_k}) = (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdot \dots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k-1}) = \\ &= \underbrace{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}}_n \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right) \end{aligned}$$

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

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

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

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

- (1) $k = \varphi(m)$
- (2) $1 \leq i, j \leq k \quad i \neq j \Rightarrow c_i \not\equiv c_j \pmod{m}$
- (3) $(c_i, m) = 1 \quad \forall i = 1 \dots k$

PL.: *RMR mod 10*: $\{1, 3, 7, 9\}$ vagy $\{37, 29, -59, 33\}$

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

PL.: $\{1, 3, 7, 9\}$ *RMR mod 10* $\because 7$, mert $(7, 10) = 1$

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

biz.:

- (1) a két halmaz elemszáma nyilván megegyezik ✓
- (2) ha $ac_i \equiv ac_j \pmod{m} \because (a, m) = 1$
 $c_i \equiv c_j \pmod{m}$ tudjuk, hogy $\{c_1, c_2, \dots, c_k\}$ *RMR mod 10* volt $\Rightarrow i = j$
- (3) tudjuk:
 $(a, m) = 1$
 $(c_i, m) = 1 \Rightarrow (ac_i, m) = 1$ ✓

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

Mivel $(a, m) = 1 \Rightarrow \{ac_1, ac_2, \dots, ac_k\}$ is *RMR mod m* $\Rightarrow$ tehát az $ac_1, ac_2, \dots, ac_k$ szorzatok valamilyen sorrendben kongruensek a $\{c_1, c_2, \dots, c_k\}$ számokkal $\Rightarrow (ac_1) \cdot (ac_2) \cdot \dots \cdot (ac_k) \equiv c_1 \cdot c_2 \cdot \dots \cdot c_k \pmod{m} \because c_1; \dots \because c_2, \dots, \because c_k$
 $a^{\varphi(m)} \equiv 1 \pmod{m}$ ✓

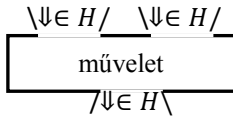
Tétel: („kis” Fermat tétel) p prím, a tetszőleges egész $\Rightarrow a^p \equiv a \pmod{p}$

Biz.: p prím

$$\varphi(p) = p - 1 \xrightarrow[\substack{\text{mert} \\ (a, p) = 1}]{E-F} a^{p-1} \equiv 1 \pmod{p} \xrightarrow{\cdot a} a^p \equiv a \pmod{p} \quad \checkmark$$

11.) Művelet fogalma, félcsoport, csoport, Abel-csoport. Csoportok számokon, mátrixokon, diédercsoport. Példák véges és végtelen, kommutatív és nem kommutatív csoportra mind a négy lehetséges variációban.

Def.: az $f: H^2 \rightarrow H$ függvényt műveletnek hívjuk, ahol $H \neq \emptyset$ alaphalmaz és H^2 a H -ből készíthető rendezett párok halmaza



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

Def.: * művelet:

- kommutatív, ha $a * b = b * a$
- asszociatív, ha $(a * b) * c = a * (b * c) \forall a, b, c \in H$ – ra
- S alaphalmaz, * asszociatív művelet S-ben $\Rightarrow (S, *)$ félcsoport

Def.: (* műv., H alaphalmaz), $e \in H$ egységelem, ha $\forall a \in H - ra \quad e * a = a * e = a$

Állítás: az egységelem egyértelmű (ha van)

biz.: tfh. e, f különböző egységelemek: $f = e * f = e$ (mert e, f egységelem) $\nleftrightarrow$

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

Def.: $(G, *)$ **csoport**, ha * művelet G-n és:

- * asszociatív
- $\exists$ egységelem
- $\forall$ elemnek $\exists$ inverze

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

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

$$\left. \begin{array}{l} a \rightarrow b \\ a \rightarrow c \end{array} \right\} \text{inverzek,} \quad c = \overbrace{(b * a)}^c * c = b * \overbrace{(a * c)}^c = b \quad \nleftrightarrow$$

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

Példák:

Csoportok számokon:

$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ csoport

De pl. $(\mathbb{N}, +)$ az NEM csoport, mert a pozitív tagoknak $\nexists$ inverze!

$(\mathbb{R}, \bullet)$ NEM csoport, mert 0-nak $\nexists$ inverze!

Vizsgálat kivéve a 0-t már csoportok lesznek a következők: $(\mathbb{R} \setminus \{0\}, \bullet), (\mathbb{Q} \setminus \{0\}, \bullet), (\mathbb{C} \setminus \{0\}, \bullet)$

Csoportok mátrixokon:

Adott: $H := \{n \times n\text{-es, } \det \neq 0 \text{ mx-ok}\}$, a művelet legyen a mátrixszorzás. Ez vajon csoportot alkot-e?

1. zártság:

$$\det(A \cdot B) = \underbrace{\det A}_{\neq 0} \cdot \underbrace{\det B}_{\neq 0} \text{ a determinánsok szorzástétele miatt } \checkmark$$

2. asszociativitás $\checkmark$

3. egységelem := *egységmátrix*:
$$\left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 \end{array} \right)_n \checkmark$$

4. inverz := *inverzmátrix* $A \rightarrow A^{-1}$: ez is H-beli, és biztosan $\exists A^{-1}$, mert $\det A \neq 0$ $\checkmark$

$\Rightarrow \Rightarrow \Rightarrow (\{n \times n\text{-es, } \det \neq 0 \text{ mx-ok}\}, \text{ mátrixszorzás}) \text{ csoport } \checkmark$

Rajzok szimmetriacsoportja:

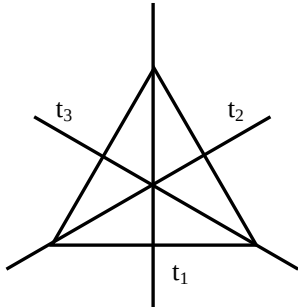
Most tekintsük egy rajznak, pl. egy szabályos háromszögnek a szimmetriáit/egybevágódási transzformációit!

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

Legyen $H := \{R \text{ rajznak a szimmetriái}\}$, a művelet pedig a függvénykompozíció!

A fv.komp.-ról tudjuk, hogy rendelkezik az asszociativitás tulajdonsággal:

$$f, g, h: H \rightarrow H \text{ függvények: } (f \circ g) \circ h = f \circ (g \circ h)$$



Állítás: az R szimmetriacsoport csoport.

biz.:

- a függvénykompozíció asszociatív ✓
- egységelem := identitás ✓
- inverz := inverzfüggvény (f^{-1}) ✓

Def. diédercsoportnak nevezzük az n -oldalú szabályos sokszög szimmetriacsoportját. Jele: D_n

$$D_n = \{I, f_\alpha, f_{2\alpha}, f_{3\alpha}, \dots, f_{(n-1)\alpha}, t_1, t_2, \dots, t_n\} \quad \alpha = \frac{360^\circ}{n}$$

$$|D_n| = 2n$$

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

Def.: Az $f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ kölcsönösen egyértelmű függvényt **permutációnak** nevezzük.

Pl.:

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 2 & 1 & 4 \end{array} \quad \text{szokásos jelölés: } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

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; $|S_n| = n!$

Pl.:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix} \quad \left(\begin{smallmatrix} 4 \\ 5 \end{smallmatrix} \text{ pl. így áll elő: } 4 \rightarrow 2 \rightarrow 5 \right)$$

Állítás: S_n csoport

biz.:

- a függvénykompozíció asszociatív ✓
- egységelem := identitás $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ ✓
- inverz := inverzfüggvény (f^{-1}), pl.: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$ ✓

12.) Elem rendje, részcsoporth, egy elem generált részcsoporth, ciklikus csoport. Mellékosztályok, Lagrange tétele, következménye az elemek rendjére vonatkozóan. A szimmetrikus csoport. Csoportok izomorfiaja, Cayley tétele (biz. nélkül).

Def.: G csoport rendje = az elemszámával, ezért jele: $|G|$, pl.: $|D_{10}| = 20$, $|S_{10}| = 10!$

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

$$g^n := \underbrace{g * g * g * \dots * g}_{n \text{ db}}$$

Példa: $(\mathbb{Z}, +)$ -nál $3^5 = 3 + 3 + 3 + 3 + 3 = 15$

$$D_3 \text{ -nál } f_{120}^2 = f_{240}, f_{120}^3 = I, t_1^2 = I$$

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: $\underbrace{g \cdot g \cdot \dots \cdot g}_l \cdot g^{-1} = (l-1) \cdot e = \underbrace{g \cdot g \cdot \dots \cdot g}_k \cdot g^{-1} \Rightarrow g^{l-1} = g^{k-1}$. 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: $\sigma(g) = k$

$g^1, g^2, \dots, g^{k-1}, \underbrace{g^k}_{=e}, g^1, g^2, \dots$ Ha nincs ilyen szám, végtelen rendű elemről beszélünk.

különbözők

Pl.: D_3 -nál $\sigma(f_{120}) = 3, \sigma(t_1) = 2$

$(\{\pm 1, \pm i\}, 0)$ -nál $\sigma(i) = 4, \sigma(-1) = 2$

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

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, D_3 nem ciklikus, $(\mathbb{Z}, +)$ ciklikus.

Állítás: G ciklikus $\Rightarrow G$ Ábel

biz.: $a \cdot b = b \cdot a$

$$g^i \cdot g^j = g^j \cdot g^i \Rightarrow g^{i+j} = g^{j+i} \quad \checkmark$$

Állítás: minden párosrendű csoport ciklikus.

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

Mellékosztály, Lagrange tétele, elemrend és csoport rendjének kapcsolata.

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

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

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

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

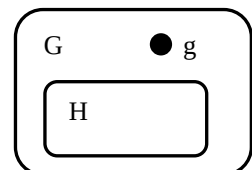
Pl.: $G := \{\text{síkvektorok}, +\}$, $H = \{x\text{-tengely vektorai}\}$

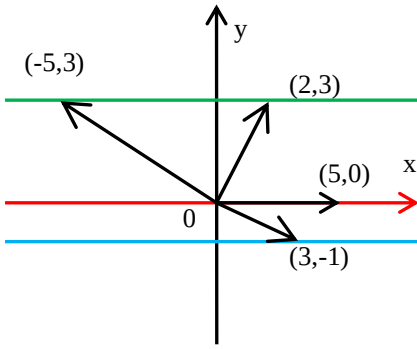
$$g = (2, 3) \rightarrow (2, 3) + H$$

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

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

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





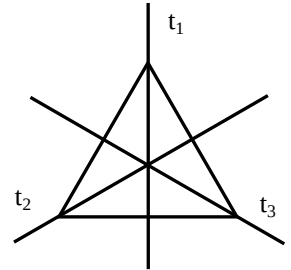
Pl.: $G = D_3$, $H = \{I, f_{120}, f_{240}\}$

$$g = t_1$$

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

(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 $e \in H \Rightarrow g = g \cdot e \in H$ ✓

2.) $g_1 H \cap g_2 H \neq \emptyset \Rightarrow g_1 H = g_2 H$

biz.:

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

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

$$g_1 \underbrace{h_1 h_1^{-1}}_e = g_2 h_2 h_1^{-1} \Rightarrow g_1 = g_2 h_2 h_1^{-1}$$

$$b \in g_1 H \Rightarrow b = g_1 h_3, \quad h_3 \in H \quad b = g_2 \underbrace{h_2 h_1^{-1} h_3}_{:= h_4 \in H} \quad \checkmark$$

3.) H véges $\Rightarrow |H| = |gH|$

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

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

$$\text{ha } gh_i = gh_j \quad \wedge \quad g^{-1} \text{ balról}$$

$$h_i = h_j \quad \checkmark$$

Tétel: (Lagrange) G véges, $H \leq G \Rightarrow |H| \mid |G|$. Speciálisan, G bármely g elemének rendje $[\sigma(g)]$ osztja G rendjét.

H szerinti mellékosztályok, számuk: i

$$|G| = |H| \cdot i \Rightarrow |H| \mid |G| \quad \checkmark$$

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 hatványaiából: $H = \{g^1, g^2, \dots, g^{k-1}, e\}$
 k db különböző elem

Állítás: H részcsoport.

biz.:

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

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

$$\text{ha } k < i + j, \text{ akkor } g^{i+j} = g^{i+j-k} \cdot \underbrace{g^k}_e = g^{i+j-k} \in H \quad \checkmark$$

(ii) $\underbrace{g^i \cdot g^{k-i}}_{g^k} = e \Rightarrow g^{k-i} = (g^i)^{-1} \quad \checkmark$

Def.: $(G, *)$ izomorf $(H, \circ)$ -rel $(H, \text{körrel})$ [jele: $\cong$], ha $\exists f: G \rightarrow H$ 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 $f(a * b) = f(a) \circ f(b)$.

Pl.: $G: (\mathbb{R}^+, \bullet)$, $H: (\mathbb{R}, +)$

$$f: \mathbb{R}^+ \rightarrow \mathbb{R}$$

$$f(a \cdot b) = f(a) + f(b) \} \text{ vegyük észre, hogy } f \text{ a logaritmusfüggvény!}$$

$$f = \log a, \quad 0 < a \neq 1$$

Def.: $(G, \bullet)$ csoport, $H \subseteq G$, H részcsoportha G -nek, ha G is csoport a $\bullet$ -ra nézve, jele: $H \leq G$

Tétel: $(G, \bullet)$ csoport, $0 \neq H \subseteq G$

$$H \text{ részcsoportha} \iff \begin{cases} (i) a, b \in H \implies a \cdot b \in H \\ (ii) a \in H \implies a^{-1} \in H \end{cases}$$

biz.:

$\implies$: 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 ✓

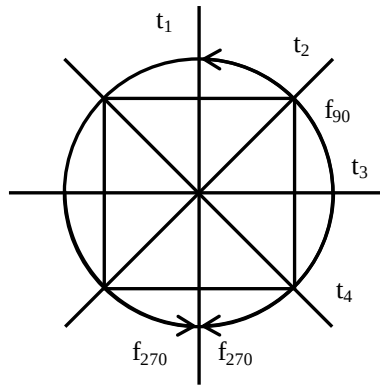
Pl.: D_4

$$D_4 = \{I, f_{90}, f_{180}, f_{270}, t_1, t_2, t_3, t_4\} \quad |D_4| = 8$$

$$H_1 := \{I, f_{90}, f_{180}, f_{270}\} \quad |H_1| = 4 \quad H_1 \leq G$$

$$H_2 := \{I, t_1\} \quad |H_2| = 2 \quad H_2 \leq G$$

$$H_3 := \{I\} \quad |H_3| = 1 \quad H_3 \leq G$$



Állítás: ciklikus csoport részcsoportha ciklikus.

biz.: G ciklikus csoport generátoreleme legyen g , és legyen $H \leq G$ valódi részcsoportha. Tekintsük a minimális $0 < k$ -t, melyre $g^k \in H$. A cél belátni, hogy g^k generálja H -t.

Tfh. a $g^k \cdot g^l \in H$ -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. ✓

G izomorf H -val

Tétel: (Cayley) G véges csoport $\implies \exists n$, hogy S_n valamelyik H részcsoportha $\overline{G} \cong H$.

Def.: S_n szimmetrikus csoport

elemei: $\{1, 2, \dots, n\}$ permutációi, művelet: kompozíció $|S_n| = n!$

Pl.:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix} \quad \left(\begin{smallmatrix} 4 \\ 5 \end{smallmatrix} \text{ pl. így áll elő: } 4 \rightarrow 2 \rightarrow 5 \right)$$

Állítás: S_n csoport

biz.:

- a függvénykompozíció asszociatív ✓

- egységelem := identitás $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ ✓

- inverz := inverzfüggvény (f^{-1}), pl.: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$ ✓

13.) Gyűrű, ferdetest és test fogalma. Példa véges és végtelen testre, ill. véges és végtelen gyűrűre, ami nem ferdetest. Számelmélet és algoritmusok: összeadás, szorzás, maradékos osztás, hatványozás lépésszáma. Modulo m hatványozás polinomiális időben.

Eddig egyműveletes struktúrákkal 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.: R tetszőleges halmaz ($\neq 0$), R -en két művelet: $+$, $\bullet$

(I) $a + b = b + a$ ($\forall a, b \in R$)	(I') $a \cdot b = b \cdot a$
(II) $(a + b) + c = a + (b + c)$	(II') $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
(III) $\exists 0 \in R$, amire $a + 0 = a$ ($\forall a \in R$)	(III') $\exists 1 \in R$, amire $a \cdot 1 = 1 \cdot a = a$ ($\forall a \in R$)
(IV) $\forall a \in R$ - re $\exists (-a) \in R$ additív inverz, hogy $a + (-a) = 0$	(IV') $\forall a \in R$ $\exists a^{-1} \in R$ multiplikatív inverz, amire $a \cdot a^{-1} = a^{-1} \cdot a = 1$
(V) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$	

Ha $(R, +, \bullet)$ -ra teljesülnek

- $\rightarrow$ akkor gyűrű (I-V)+(II')
- $+$ $\rightarrow$ akkor kommutatív gyűrű (I-V)+(I')
- $+$ $\rightarrow$ akkor ferdetest (I-V)+(III'-IV')
- $+$ $\rightarrow$ akkor (kommutatív) test (I-V)+(I', III'-IV')

Példák:

- $(\mathbb{R}, +, \bullet)$, $(\mathbb{C}, +, \bullet)$, $(\mathbb{Q}, +, \bullet)$ test
- $(\mathbb{Z}, +, \bullet)$ NEM test, mert $\nexists$ inverze $\forall$ elemnek, hanem csak kommutatív gyűrű.
- $(n \times n - \text{es mátrixok } \mathbb{R} \text{ felett}, +, \bullet)$ vizsgálata:

(i) mátrixok összeadása kommutatív ✓	(i') mátrixszorzás NEM kommutatív ✓
(ii) mátrixok összeadása asszociatív ✓	(ii') mátrixszorzás asszociatív ✓
(iii) nullelem legyen a nullmátrix: $0 = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$ ✓	(iii') egységelem legyen az egységmátrix: $E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$ ✓
(iv) additív inverz: $A \rightarrow -A$ ✓	(iv') a 0 determinánsú mátrixoknak $\nexists$ inverze!
(v) disztributivitás teljesül ✓	
	(i') és (iv') miatt ez csak gyűrű, egészen pontosan egységelemes gyűrű; egységelemes, mert a szorzásra nézve $\exists$ egységelem

- az egész vagy a valós együtthatós polinomok $(\mathbb{Z}[x], \mathbb{R}[x])$ kommutatív gyűrűt alkotnak a szokásos $+$ összeadásra, $\cdot$ 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:

$\mathbb{R}(x) := \left\{ \frac{p}{q} : p, q \in \mathbb{R}[x], q \neq 0 \right\}$, a műveletek:

$$\frac{p}{q} + \frac{r}{s} = \frac{ps+qr}{qs}, \text{ ill. } \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}.$$

Def.: R gyűrű nullosztómentes, ha $\forall a, b \in R$ esetén ha $a \cdot b = 0 \Rightarrow a = 0$ vagy $b = 0$.

Pl.: $(\mathbb{Z}, +, \cdot)$

Tétel: $\forall$ test nullosztómentes.

biz.: $a \cdot b = 0$

⇒ ha $a = 0$ ✓

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

$$\underbrace{a^{-1} \cdot a}_1 \cdot b = \underbrace{a^{-1} \cdot 0}_0 \Rightarrow b = 0 \quad \checkmark$$

Def.: A kommutatív nullosztómentes gyűrű neve **integritási tartomány**.

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.

Def.: $\mathbb{Z}_n$ -nel jelöljük és modulo n maradékosztályok gyűrűjének nevezzük a

$\mathbb{Z}_n = \{0, 1, 2, \dots, (n-1)\}$ halmazt a modulo összeadásra, ill. szorzásra nézve:

$$a \oplus b := a + b \pmod{n}$$

$$a \odot b := a \cdot b \pmod{n}$$

Pl.: $\mathbb{Z}_{10}$ -nél: $7 \oplus 8 = 5$, $7 \odot 8 = 6$

$2 \odot 5 = 0$, de a 2 és az 5 sem 0 $\Rightarrow \mathbb{Z}_{10}$ nem nullosztómentes $\Rightarrow$ nem test.

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

biz.:

⇒ tfh. n összetett: ekkor szorzattá alakítható az előző példához hasonlóan, vagyis $\mathbb{Z}_n$ nem nullosztómentes $\Rightarrow \mathbb{Z}_n$ nem test!

⇐

⇐: $n = p$ prím:

(i), (ii), (iii), (iv) ✓

(i') ✓

(ii') ✓

(iii') ✓

(iv'): egyedül ez nem triviális:

$$a \neq 0, \quad a^{-1} := x, \quad a \odot x = 1 \Leftrightarrow \begin{array}{l} ax \equiv 1 \pmod{p} \\ \text{megoldható} \Leftrightarrow \underbrace{(a,p)}_{=1, \text{mert } p \text{ prím}} \mid 1 \end{array}$$

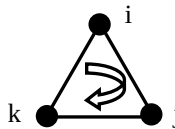
(v) ✓

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \subseteq ? \rightarrow$ a válasz: kvaterniók

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

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

$$ij = k, \quad jk = i, \quad ki = j, \quad (\text{de } ji = -k, \quad kj = -i, \quad ik = -j \rightarrow \text{tehát az már biztos, hogy NEM kommutatív})$$



A kvaterniók **ferdetestet alkotnak**, mert:

(i), ..., (iv) ✓

(i') nem komm.

(ii') ✓

(iii') ✓

(iv'): ha

$$x \neq 0, \quad x^{-1} := \frac{1}{x} = \frac{1}{a+bi+cj+dk} \stackrel{\substack{x \text{ konjugáltjával bővítünk:} \\ \tilde{x}=a-bi-cj-dk}}{=} \frac{a-bi-cj-dk}{(a+bi+cj+dk) \cdot (a-bi-cj-dk)} = \frac{a-bi-cj-dk}{\underbrace{a^2+b^2+c^2+d^2}_{a \text{ nevező most már valós } \checkmark}}$$

(v) ✓

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

Ez is testet alkot, mert:

könnyen látható, hogy ez is teljesíti az összes kritériumot, az egyedüli nemtriviális itt is az (iv') pont, vagyis a multiplikatív inverz:

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

Számelmélet és algoritmusok: összeadás, szorzás, maradékos osztás, hatványozás lépésszáma. Modulo m hatványozás polinomiális időben.

Egy **algoritmust** akkor tekintünk **jónak**, ha lépésszáma felülről becsülhető az input hosszának polinomjával.

Vizsgáljuk meg az **alapműveletek** lépésszámgigényét!

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).

Vizsgálat **hatványozás** nem végezhető el polinomrendben, hiszen pl. 2^x végeredményének pusztán 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** $+ \dots + \dots + \dots /$ is polinomiális!

Mi a helyzet a **mod m hatványozással**?

Az alábbi példa bemutatja, hogy a **mod m** hatványozás elvégezhető polinomidőben:

Példa: $3^{100} \equiv ? \pmod{7}$

$$3^1 \equiv 3 \pmod{7}$$

$$3^2 \equiv 9 \equiv 2 \pmod{7}$$

$$3^4 \equiv 2^2 = 4 \pmod{7}$$

$$3^8 \equiv 4^2 = 16 \equiv 2 \pmod{7}$$

$$3^{16} \equiv 2^2 = 4 \pmod{7}$$

$$3^{32} \equiv 4^2 = 16 \equiv 2 \pmod{7}$$

$$3^{64} \equiv 4 \pmod{7}$$

Most írjuk fel a 100-at binárisan: $100_{(10)} = 1100100_{(2)}$

$$\Rightarrow 3^{100} \equiv 3^{2^6} \cdot 3^{2^5} \cdot 3^{2^2} = 3^{64} \cdot 3^{32} \cdot 3^4 \pmod{7}$$

$$3^{100} \equiv 4 \cdot 2 \cdot 4 = 32 \equiv 4 \pmod{7}$$

...

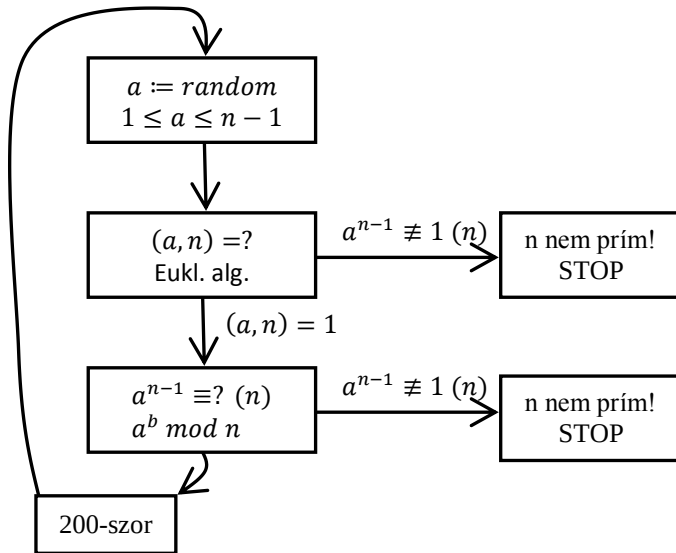
14.) Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosítás és digitális aláírás fogalma, megvalósításuk az RSA-kód segítségével.

Prímtesztelés:

Egy egyszerű módszer, hogy 1-től $\sqrt{n}$ -ig ellenőrizzük az oszthatóságot. Előnye, hogy ha egy szám összetettnek bizonyul, akkor ez magadja egy osztóját is, viszont exponenciális lépésszáma.

Létezik ennél gyorsabb algoritmus is:

Fermat-teszt: kérdés: n prím-e?



ha 200-szor $a^{n-1} \equiv 1 (n) \Rightarrow \text{STOP: „n valószínűleg prím”}$

a **tanúja/árulója** n -nek, ha $a^{n-1} \not\equiv 1 (n)$

a **cinkosa** n -nek, ha $a^{n-1} \equiv 1 (n)$

Tétel: ha n -nek $\exists$ tanúja $\Rightarrow \text{RMR mod } n$ legalább fele tanú! (RMR=redukált maradékrendszer)

Biz.: legyen „ a ” egy tanú, $c_1, \dots, c_k$ cinkosok

Állítás: $a \cdot c$: tanú

biz.: $(a \cdot c_i)^{n-1} \equiv \underbrace{a^{n-1}}_{\equiv 1} \cdot \underbrace{c_i^{n-1}}_{\equiv 1} (n) \Rightarrow (a \cdot c_i)^{n-1} \equiv 1 (n) \quad \checkmark$

Állítás: $a \cdot c_i \not\equiv a \cdot c_j (n)$, ha $c_i \not\equiv c_j (n)$

Biz.: ha $a \cdot c_i \equiv a \cdot c_j (n) \quad \wedge \quad a, \text{ mert } (a, n) = 1$

$c_i \equiv c_j (n) \quad \checkmark$

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

Def.: n **Carmichael-szám**, ha összetett, de $\nexists$ tanúja RMR-ben, azaz $\forall a (a, n) = 1$ -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 $\rightarrow$ prímtesztelés. Ha összetett, megnézzük $(n+1) - \text{et}$, $(n+2) - t, \dots$ A $\Pi(n) \approx \frac{n}{\ln n}$ függvény szerint rövid időn belül prímre fogunk találni. $\checkmark$

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: $D(c(x)) = x$

RSA-kód: $N := p \cdot q$, ahol p, q sokszámjegyű prímek

c választása úgy, hogy $\varphi(n) = (p-1)(q-1)$ -hez relatív prím legyen: $(c, \varphi(N)) = 1$

kódolás: $x \rightarrow x^c \bmod N$

nyilvános: N, c ;

titkos: $p, q, d, \varphi(N)$

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

Dekódolás: $y \rightarrow y^d \bmod N$

$$d \text{ jól van megválasztva} \Leftrightarrow x^{c \cdot d} = (x^c)^d \equiv x(N) \forall x - re$$

Segédétel: $(X, N) = 1 \Rightarrow x^{\varphi(N)} \equiv 1(N) \Rightarrow x^{k \cdot \varphi(N)} \equiv 1(N) \Rightarrow x^{k \cdot \varphi(N) + 1} \equiv x(N)$

cél: $c \cdot d = k \cdot \varphi(N) + 1$ valamely k -ra, azaz $c \cdot d \equiv 1 \pmod{\varphi(N)}$ lin. kongruencia $\rightarrow (c, \varphi(N)) = 1$ ✓

kongr. az euklideszi algoritmussal megoldható! $d \equiv _ \pmod{\varphi(N)}$

A d -t azért nem tudja bárki kiszámolni, mert nem tudja felírni a lin. kongruenciát, 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.

$A \rightarrow B$

$C_A \quad C_B$ } kódoló függvények nyilvánosak $\rightarrow x \rightarrow y := D_A(C_B(x))$

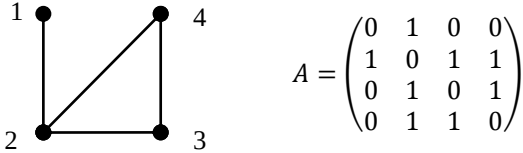
$D_A \quad D_B$ } dekódoló függvények titkosak $y \rightarrow x := D_B(C_A(y))$

xxx?. Gráfok és mátrixok. Szomszédossági mátrix (hatványainak jelentése, reguláris gráf esetén egy sajátértéke). Illeszkedési mátrix, annak rangja.

Def.: A $G = (V, E)$ irányított gráf szomszédossági mátrixa $A(G) = (a_{ij}) \in \mathbb{R}^{V \times V}$, ahol a_{ij} legyen az i -ből j -be futó élek száma.

Megjegyzés: G v_i pontjának ki/befoka a mátrix i . sorában/oszlopában lévő elemek összege. Ha G irányítatlan, akkor A szimmetrikus a főátlóra: $A = A^T$.

Példa:



Tétel: Ha $G = (V, E)$ irányított gráf, akkor az A_k mx. (i, j) pozíciójában álló $(A_k)_j^i$ eleme az i -ből j -be vezető k élű séták száma.

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:

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

Következmény:

- Ha G egyszerű, irányítatlan gráf $\Rightarrow (A^2)_v^v = d(v), \forall v \in V(G)$;
- A hurokélmentes gráfoknál A^3 főátlóbeli elemeinek összege a gráfban található 3-hosszú körök számának 6-szorosa.

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

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

Ekkor:

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

Ha G Δ -reguláris, akkor az egységvektor a Δ sajátértékhez tartozó sajátvektor, mert a fenti egyenlőségek egyenlőséggel teljesülnek. $\checkmark$

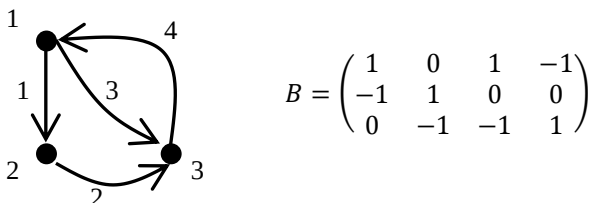
Def: A $G = (V, E)$ irányított gráf illeszkedési mátrixa $B(G) \in \mathbb{R}^{V \times E}$, amire:

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

ha G irányítatlan, akkor:

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

Példa:



Tétel: A G n pontú irányított hurokél mentes c komponensű gráfnál $r(B) = n - c$.

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 $\mathbf{0}$ -t adja, a rang $\leq p - 1$.

Legyen F egy p pontú, $p - 1$ élű feszítőfa ebben a komponensben.

Legyen v_1 egy elsőfokú pont F -ben és e_1 a hozzáilleszkedő él.

Legyen v_2 egy elsőfokú pont $F - \{v_1\}$ -ben és e_2 a hozzáilleszkedő él, stb.

Ha a blokk sorait $v_1, v_2, \dots$ sorrendben soroljuk fel, oszlopait $e_1, e_2, \dots$ 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 $\mathbf{0}$ -t adja.

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

(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-tételt**:

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

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.

$$\begin{array}{c} \begin{array}{cc} & \begin{array}{c} b \\ \boxed{N} \end{array} \\ \begin{array}{c} b \\ \boxed{M} \end{array} & \begin{array}{c} a \\ \boxed{MN} \end{array} \end{array} \end{array}$$

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

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

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

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

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

(utsó végösszeg): $\det(B_0 \cdot B_0^t) = n^{n-2} \rightarrow$ újabb bizonyítást kaptunk Cayley tételére ✓