A Számítástudomány Alapjai

Kidolgozott tételsor

Eke Máté
eke.mate@outlook.com

Tartalom

1. Leszámlálási alapfogalmak: permutációk, variációk és kombinációk (ismétlés nélkül és ismétléssel); binomiális együtthatók közti egyszerű összefüggések, a binomiális tétel, skatulya elv, szita formula

	Permutáció	Variáció	Kombináció
ismétlés nélkül	n!	$\frac{n!}{(n-k)!}$	$\binom{n}{k}$
ismétléssel	$\frac{n!}{(k_1! * k_2! * \dots * k_n!)}$	n^k	$\binom{n+k-1}{k}$

Permutáció: n elem sorba rendezése ismétléssel vagy ismétlés nélkül.
Ismétlés nélküli példa: 5 ember hány féleképpen állhat sorba
Ismétléses példa: Ha egy héten egy tanórából több is van, akkor a lehetséges heti órarendek száma

Variáció: n elemből k kiválasztása és a k elem sorba rendezése ismétléssel vagy ismétlés nélkül.
Ismétlés nélküli példa: n versenyzőből, hány féle lehet az első k
Ismétléses példa: versenynapon n versenyző, k résztáv, hány féle lehet a résztáv győztesek sorrendje

Kombináció: n elemből k elem kiválasztása úgy, hogy nem számít a sorrend.
Ismétlés nélküli példa: Lottó.
Ismétléses példa: Cukrászdában n féle sütemény van, mindegyikből végtelen áll rendelkezésre, és ezekből akarunk k darabot kiválasztani.

$$\binom{n}{k} := \frac{n!}{(n-k)! * k!}$$

$$\binom{n}{k} = 0 \; ha \; n < k \; vagy \; k < 0$$

Binomiális tétel: $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

Bizonyítás: *A zárójelet felbontva minden kifejtési tag $a^k b^{n-k}$ alakú lesz. Minden $a^k b^{n-k}$ annyiszor fog előfordulni, ahányféleképp k-t ki lehet választani n-ből ->* $\binom{n}{k}$.

Következmény: $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$

Binomiális együtthatók közötti összefüggések:

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

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

Skatulya elv:

Ha f: H -> K és |K|<|H|, akkor létezik H-nak két olyan különböző *h* és *h'* eleme, amikre teljesül *f(h) = f(h')*

Példa: 10 gyufa szétosztása 9 dobozba.

Szita-formula:

$$|UA_i| = \sum A_i - \sum A_i \cap A_j + \sum A_i \cap A_j \cap A_k - . + . - \cdots$$

Az unió elemszámát úgy kapjuk, hogy A_i halmazok elemszámainak összegéből levonjuk a páronkénti metszetek elemszámait, aztán hozzáadjuk a hármas metszetek elemszámait stb.
Példa: 1 és 1000 között hány olyan szám van, ami 30-hoz nem relatív prím? Mivel akkor nem relatív prím egy szám 30-hoz, ha 2, 3 vagy 5 osztója, így ezeknek a halmazából áll össze.

2. Alapvető adatstruktúrák: tömb, láncolt lista, bináris fa. Lineáris és bináris keresés, ezek lépésszáma, minimumkeresés, beszúrási feladat, rendezési feladat. Buborék-, kiválasztásos, beszúrásos, összefésüléses és gyorsrendezés, alsó korlát, lépésszám becslések.

Tömb: Összefüggő memóriaterületen találhatóak az elemek, egymás utáni memóriacímeken, indexeléssel érhetőek el. *Műveletek:* OLVAS[n], ÍR[n].

Láncolt lista: A láncolt lista elemei cellák, és minden cella egy adatmezőből és egy mutatóból áll, ahol a mutató a lista következő cellájára mutat.
Kétszeresen láncolt lista: Itt még egy mutató van, a második az aktuális cellát megelőző cellára mutat.
Műveletek: ELSŐ ELEM, AKTUÁLIS ELEM, KÖVETKEZŐ ELEM, (kétszeresen láncolt esetén ELŐZŐ ELEM), BESZÚRÁS, TÖRLÉS.

Bináris fa: Minden cella legfeljebb két mutatót tárol, ahol az egyik a bal-, a másik a jobb fiúra mutat. Megkötés, hogy legyen egy gyökérelem, és a mutatók definiálta gráf irányított, körmentes legyen.
Műveletek: GYÖKÉR, AKTUÁLIS ELEM, BALFIÚ, JOBBFIÚ, APA, BALRÉSZFA, JOBBRÉSZFA.

Tömb és láncolt lista előnyei/hátrányai (lépésszámok):

	Tömb	Láncolt lista
Előnyök	Gyors hozzáférés (1)	Gyors törlés (1)/beszúrás (3)
Hátrányok	Lassú törlés/beszúrás (~n)	Lassú hozzáférés (~n)

Lineáris keresés: végigmegy az első elemtől, amíg meg nem találjuk a keresett elemet, vagy el nem fogynak az adatok. Rendezetlen esetben, vagy pl. növekvő sorrendbe rendezett láncolt listánál alkalmazzuk. Lépésszáma n-nel arányos.

Bináris keresés: rendezett esetben. Kiolvas egy elemet a tömbből, három eset lehetséges: megtalálta, nagyobb/kisebb a kereset elemnél. Ha nagyobb/ kisebb akkor a tömbnek már csak az aktuális elemet megelőző/követő részét kell nézni. Lépésszáma $\lfloor log_2(n+1) \rfloor + 1$-nek legfeljebb konstans szorosa.

Minimumkeresés: rendezetlenül adottak számok, és ezek közül kell megtalálni a minimálist. Az algoritmus kiválaszt egy $a_i és\ a_j$ számot, és ezeket összehasonlítja. Legfeljebb n-1 összehasonlítás szükséges.

Beszúrás:
Tömb: lassú, az összes elemet át kell mozgatni.
Láncolt lista: gyors. Új cellát kell létrehozni, a megelőző elem mutatóját erre a cellára kell állítani, az új celláét pedig a következőre.

Buborék rendezés: input egy rendezetlen, n elemű T tömb, output T elemeit tartalmazó rendezett tömb. Minden fázisban összehasonlítja T[i]-t és T[i+1]-et, és ha T[i]>T[i+1], akkor felcseréli őket. Legfeljebb n-1 összehasonlítás, és legfeljebb n-1 csere történik, ezért lépésszáma n^2 konstans szorosával felülről becsülhető.

Kiválasztásos rendezés: adott egy A[1..n] tömb, a rendezés sorra megy A[1..n], A[2..n],..,A[n-1..n] tömbökön, és az adott tömb legkisebb elemét felcseréli a tömb első elemével. A lépésszám legfeljebb $c * n^2$.

Beszúrásos rendezés: a rendezendő rekordokat egyenként szúrjuk be egy már rendezett tömbbe. A lépésszám legfeljebb $c * n^2$.

Összefésüléses rendezés: a rendezetlen tömböt szétbontja, és ezeken a részeken hajtja végre az összefésülést, amíg ismét egy – már rendezett – tömböt nem kap. Összefésülés: tegyük fel, hogy van két, n/2 elemű listánk, amik külön-külön már rendezve vannak. Először megnézzük, hogy a két lista első elemei közül melyik a kisebb, a kisebbet kiválasztjuk – ezt egy új n elemű tömb első helyére írjuk. Az új listáknál (maradék elemekből) is ugyan ezt tesszük. Ha az egyik lista elfogy, akkor a maradékot csak sorrendbe le kell írni. Rekurzív algoritmus. Legfeljebb $n * log_2 n$ összehasonlítást igényel.

Gyors rendezés: készítünk egy P(s) partíciót, választunk egy véletlen s elemet (az első elem is megfelelő), készítünk három tömböt, az elsőbe s-nél kisebb elemek, a másodikba s-el megegyezőek, a harmadikba s-nél nagyobb elemek kerülnek. A maximális lépésszám $c * n^2$, de a várható csak $n * log_2 n$.

Alsó korlát: minden összehasonlításon alapuló rendezés n elem esetén legalább $n * log_2 n$ összehasonlítást igényel.
Bizonyítás: *n elem esetén n! féle sorrend van, és ebből csak 1 megfelelő. Ha összehasonlítok két elemet, az 2 részre osztja a sorrendeket, tehát a sorrendek felét kizárja. Ha tehát k-szor hasonlítok össze, akkor* $\binom{n}{2^k}$*sorrend jöhet még szóba. Akkor tudom biztosan a jó sorrendet, ha* $\binom{n}{2^k} < 1$*, vagyis* $n! \leq 2^k$*. Két oldal logaritmusát véve* $log_2 n! \leq k$*. Mivel* $log_2 n! \approx n * log_2 n$*, így állításunkat igazoltuk.*

Lépésszám becslések:

	Buborék	Kiválasztásos	Beszúrásos	Összefésüléses	Gyors
Max. összehasonlítás	n^2	n^2	$log_2 n$	$n * log_2 n$	n^2
Átl. összehasonlítás	n^2	n^2	$log_2 n$	$n * log_2 n$	$n * log_2 n$
Max. mozgatás	n^2	n	n		
Átl. mozgatás	n^2	n	n		

3. Ládarendezés, bináris keresőfák. Keresés, beszúrás, törlés, minimumkiválasztás, pre-, in- és posztorder bináris keresőfában, rendezés bináris keresőfával. Kupac, kupacos rendezés.

Ládarendezés: $a_1 \dots a_n$, elem esetén, ha az elemek mindegyik 1 és m közötti egész, és m<n, de legalábbis nem sokkal nagyobb, akkor használható a ládarendezés. Létrehozunk egy m méretű T tömböt, és minden i elemet T[i]-be rakunk. Ez után végigolvasva a ládákat és ezt egy n méretű tömbbe írva rendezett tömböt kapunk. Lépésszáma felülről becsülhető n+m konstans szorosával.

Bináris keresőfa: a keresőfa x csúcsának bal részfájában tárolt egyetlen elem sem nagyobb x-nél, és a jobb részfában tárolt egyetlen elem sem kisebb, mint x.

Műveletek bináris keresőfákkal:
Keresés: s-t összehasonlítjuk a gyökérrel, és ha nem egyezik, akkor tudjuk, hogy a bal vagy a jobb fiúnál folytassuk a keresést. Legrosszabb esetben a fa mélységével arányos a lépésszám.

Beszúrás: kereséssel indul, és ha s nincs a keresőfában, akkor az alá a levél alá szúrjuk be, értelemszerűen bal- vagy jobbfiúként, ahol véget ért a keresés. Szintén a fa mélységével arányos.

Törlés: 3 eset:
1.: Nincs gyereke -> simán kitöröljük
2.: Egy gyereke van -> kitörüljük, majd a gyerek új szülője az lesz amiről kitöröltük az elemet.
3. Két gyereke van -> megkeressük a legközelebbi rákövetkezőjét, kivágjuk, és az elem helyére rakjuk.

Minimum/maximum kiválasztás: a gyökérből addig megyünk balra/jobbra, amíg van ott rekord.

Bejárások:
Inorder: balrészfa-gyökér-jobbrészfa, keresőfánál ez az elemek növekvő sorrendjét adja.

Preorder: gyökér-balrészfa-jobbrészfa

Postorder: balrészfa-jobbrészfa-gyökér, a fa törlése.

Rendezés bináris keresőfával: faépítés, majd inorder bejárás az elemek növekvő sorrendjét adja.

Kupac: teljes bináris fára (úgy kapható meg egy *l* szintes, $2^{l+1} - 1$ elemet tároló fából, hogy annak valamelyik levelétől jobbra álló minden levelét töröljük) törekszünk. Teljes bináris fa akkor kupac, ha egyetlen rekord sem nagyobb a fiaiban tárolt rekordok egyikénél sem.

Kupac építés: Apák és fiaik elemeinek cseréjével elérjük, hogy egyre nagyobb és nagyobb részfákban teljesüljön a kupac tulajdonság. A csak levélből álló részfára természetesen egyből teljesül a kupac-tulajdonság. Ezért a tömb utolsó elemétől az első irányába haladva a következőket hajtjuk végre: ha A[j] > min(A[2j],A[2j + 1]), akkor apa és a kisebbik értékű fia elemei helyet cserélnek, majd rekurzívan hívjuk meg a KUPAC eljárást a szóban forgó fiúra. A haladási irány miatt eredetileg a fiúkra teljesült a kupac tulajdonság. Ez a cserével esetleg felborult, ezért ezt az adott fiúnál újra meg kell vizsgálni.

Beszúrás: az új elemet beszúrjuk a soron következő helyre, majd „felszivárogtatjuk”.

MINTÖR: Kitörlöm a legkisebb elemet (a gyökeret), majd beírom a helyére az utolsót. Sérült a kupac-tulajdonság, tehát ezt az elemet mindig ki kell cserélni a fiai közül a kisebbel, amíg helyre nem áll.

Kupacos rendezés: Tömbből kupacot építünk (legfeljebb $c * n$ lépés), majd n-szer végrehajtjuk MINTÖR műveletet ($c * log_2$), így legfeljebb $n * log_2 n$ konstans szorosa a rendezés.

4. Gráfelméleti alapfogalmak: pont, él, fokszám, szomszédossági mátrix, éllista. Egyszerű gráf, részgráf, feszített részgráf, izomorfia, élsorozat, séta, út, kör, összefüggő gráf, komponens. Gráfok fokszám-összege, fák egyszerűbb tulajdonságai.

Definíció: G=(V,E) G gráf V(G) jelöli a G pontjainak, E(G) pedig G éleinek a halmazát.

Hurokél: a kiindulási és a végcsúcs azonos.

Párhuzamos él: a két él ugyan azt a két csúcsot köti össze.

Fokszám: G gráf v csúcsának fokszáma – d(v) – a G v végpontú éleinek száma (hurokél kétszer számít).
ΔG a G maximális fokszáma.
Gráf **k-reguláris** ha minden $v \epsilon V(G)$-re d(v)=k

Ha G véges, akkor $\sum_{v \epsilon V(G)} d(v) = 2 * |E(G)|$, azaz **a fokszámok összege az élek számának kétszerese**.
Bizonyítás: *Kezdetben legyen $|E(G)| = 0$, egy élt behúzva az általa összekötött csúcsok fokszámát növelem eggyel, tehát $|E(G)| = 1$ és $\sum_{v \epsilon V(G)} d(v) = 2$ (hurokélre is igaz, hiszen ott kettővel növeli a csúcs fokszámát) és így tovább.*

Szomszédossági mátrix: V(G) x V(G) méretű mátrix, aminek (u,v) pozícióján az u és v pontok között futó élek száma áll.

Egyszerű gráf: G egyszerű ha (1) nem üres, (2) E(G) elemei V(G) valamilyen két elemű részhalmazai. Egyszerű, ha nem engedünk meg hurok- és párhuzamos éleket.

K_n n pontú teljes gráf. Minden pont minden ponttal szomszédos.
C_n n pontú kör. Minden pont pontosan két másik ponttal szomszédos.
P_n n pontú út. A végpontok kivételével minden pont pontosan két másik ponttal szomszédos.

Feszített részgráf: H a G feszített részgráfja, ha H csúcstörléssel kapható G-ből.

Részgráf: H a G részgráfja, ha H él-, és csúcstörléssel kapható G-ből.

Izomorfia: két gráf izomorf, ha csúcsaik között létezik olyan kölcsönösen egyértelmű megfeleltetés, amelyre minden él helyesen van megfeleltetve.

Élsorozat: csúcsok és élek felváltva követik egymást, csúccsal kezdve.

Séta: olyan élsorozat, aminek minden éle különböző.

Út: olyan séta, aminek minden pontja különböző

Kör: olyan út, aminek a kezdő és a végpontja azonos.

Összefüggő gráf: ha bármely két pontja között vezet élsorozat = vezet séta = vezet út.

Komponens: $K \subseteq V(G)$, ha bármely $u, v \epsilon K$ között vezet út, de $u \epsilon K$ és $v \epsilon (V(G) \backslash K)$ között nem. Bármely gráf egyértelműen felbontható komponensek uniójára.

Izolált pont: d(v)=0. Az izolált pont önmagában egy komponens.

G gráf **erdő**, ha körmentes.
G gráf **fa**, ha körmentes és összefüggő. Egy erdő minden komponense fa.

Tétel: Ha G n pontú körmentes gráf, G pontosan akkor összefüggő, ha **|E(G)|=n-1.**
Bizonyítás: *építsünk egy F fát n pontú üres gráfból. Húzzuk be úgy az éleket, hogy ne alkossanak kört! Az éleket behúzva mindig eggyel csökken a komponensek száma, |E(G)| pedig egyel nő. Ha végül F összefüggő, akkor n-ről 1-re csökken a komponensek száma, és pont n-1 élt húztunk be.*

Ha G egy n pontú és k komponensű erdő, akkor |E(G)| = n-k.

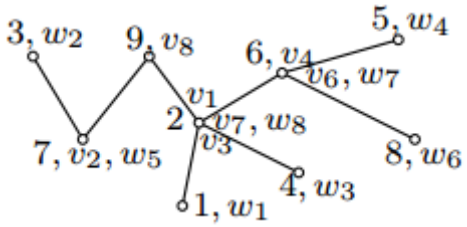
Levél: v levél, ha F fa része és d(v)=1.

Tétel: minden fának van legalább két elsőfokú csúcsa.

5. Cayley tétele fák számáról, Prüfer kód. Minimális költségű feszítőfa, Kruskal algoritmus, normál fák.

Cayley-tétel: n címkézett ponton pontosan n^{n-2} féle fa adható meg
Bizonyítás: *Számozzuk meg a fa csúcsait 1-től n-ig. Kezdjük el sorban letépkedni a leveleket, és írjuk fel annak a csúcsnak a számát, amiről letéptük, az utolsót már nem írjuk fel, hiszen ez úgyis n. Az így kapott n-2 hosszú csúcssorozat a* ***Prüfer-kód****. A Prüfer-kód egyértelműen meghatároz egy fát, mivel ennek ismeretében felrajzolhatjuk azt. Minden ismétléses variáció előáll Prüfer-kódként, így Cayley tétele igaz*.

Pl.:



Levéltörlési sorrend: 1; 3; 4; 5; 7; 8; 6;
Prüfer kód:(2; 7; 2; 6; 9; 6; 2)

Megfigyelés: Prüfer kódban minden csúcs a fokszám-összegénél eggyel kevesebbszer szerepel.
Bizonyítás: *Ha nem a legnagyobb, akkor róla minden levelet letépünk egészen addig, amíg valamely szomszédja nagyobb nem lesz. Ha a legnagyobb, akkor az utolsó helyre kerülne saját maga, de az már nem szerepel a Prüfer kódban.*

Költségfüggvény: $k: E \rightarrow R_+$ minden élhez egy költséget rendel.

Minimális költségű feszítőfa: olyan $F \in E$ élhalmaz, amire (V,F) fa, és k(F) minimális.

Kruskal algoritmus:
Input: G=(V,E) gráf, és $k: E \rightarrow R_+$ költségfüggvény.
Output: minimális költségű feszítőfa.
Működés: minden lépésben megépítjük a legolcsóbb élt, ami nem hoz létre kört. Mohó algoritmus, mert csak azzal törődik, ami éppen a legalacsonyabb költségű.
Optimum bizonyítása: tegyük fel, hogy az algoritmus helytelen, ekkor létezik egy f él, amit e helyére bevéve olcsóbb feszítőfát kapunk. Ekkor azonban f költsége kisebb, mint e költsége, így f-et az algoritmussal korábban már ellenőriztük, tehát ellentmondásra jutottunk, azaz a feszítőfa minimális költségű.

Normál fák: áramköröket, mint gráfokat modellezzük, ahol csúcsok ekvipotenciális területek, élek áramköri elemek. A hálózat megoldásának szükséges feltételei vannak:
- Feszültségforrásokból nem létezhet kör.
- Áramforrások elhagyása után a gráf összefüggő kell maradjon.
G gráf F feszítőfáját normális fának nevezzük, ha F tartalmaz minden feszültségforrást, de nem tartalmaz egy áramforrást sem, valamint a lehető legtöbb kondenzátort, és legkevesebb tekercset tartalmazza.

Feszítőfa megtalálásához az éleket súlyozzuk, és Kruskal-algoritmust használjuk:
Feszültségforrások: 1; Kapacitások: 2; Ellenállások: 3; Induktivitások: 4; Áramforrások: 5.

Ha létezik normális fa, a Kruskal-algoritmus ilyet ad.

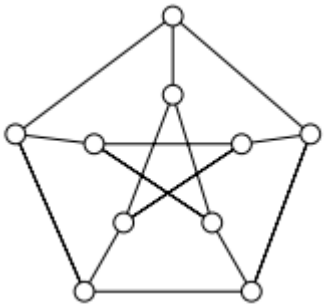
6. Euler-séta és körséta, létezésének szükséges és elégséges feltétele. Hamilton-kör és út, szükséges, illetve elégséges feltételek Hamilton-kör létezésére, Dirac és Ore tételei.

Euler-(kör)séta: olyan (kör)séta, ami G minden élét pontosan egyszer tartalmazza.

Megfigyelés: Ha G véges gráfnak létezik Euler-körsétája, akkor minden csúcs foka páros. Ha létezik Euler-sétája, akkor pontosan 0 vagy 2 páratlan fokszámú csúcsa van.
***Bizonyítás**: a séta éleit irányítva minden csúcs befoka azonos lesz a kifokával, kivéve esetleg az első és az utolsó csúcsot. d(v)=befok+kifok, tehát ha ezek megegyeznek, akkor d(v) páros.*

Tétel: G véges, összefüggő gráfnak pontosan akkor van Euler-körsétája, ha minden csúcs foka páros, Euler-sétája pedig, ha 0 vagy 2 páratlan fokú csúcsa van.
***Bizonyítás**: szükségessége következik az első megfigyelésből.*
1. Elégségesség |E(G)| szerinti indukcióval: 0-ra nyilvánvalóan igaz. TFH m-nél kisebb élszámra már bizonyítottuk, legyen az élek száma m. G-ben létezik C kör, mert minden fokszáma legalább kettő. Ha elindulunk egy pontból, akkor előbb-utóbb visszaérünk egy már érintett v-be, mert nem akadhatunk el. G'=G-C, C éleinek törlésével. G' minden komponense véges, összefüggő, m-nél kevesebb élt tartalmaz, és minden fokszáma páros, tehát az indukciós feltevés miatt minden komponensének létezik Euler-körsétája. A G gráf C Euler-körsétáját úgy kapjuk, hogy elindulunk v pontból C élein, és amikor egy nemtriviális komponensbe érkezünk, akkor annak Euler-körsétáján haladunk tovább, majd ha ezzel végeztünk, akkor C-n haladunk tovább. A kapott élsorozat nyilván G Euler-körsétája lesz.*
2. A páratlan fokú csúcsok közé húzzuk be e élt – így 1. már teljesül. Feltehetjük, hogy e* az Euler körséta utolsó éle, így ezt elhagyva Euler-sétát kapunk.*

Hamilton-kör: olyan kör, ami G minden pontját pontosan egyszer tartalmazza.
Hamilton-út: olyan út, ami G minden pontját pontosan egyszer tartalmazza.



Petersen-gráf

Tétel: Ha G véges gráfban létezik Hamilton-kör (vagy út), akkor G-ből k tetszőleges pontot törölve, a keletkező gráfnak legfeljebb k (vagy k+1) komponense van. Nem elégséges a létezéshez – Pl. Petersen Gráf.
***Bizonyítás:** ha G gráf maga egy Hamilton-kör/út, akkor triviális. Ha további élei is vannak, akkor pedig csak csökkenhet a komponensek száma.*

Dirac tétel: ha $n \geq 3$ pontú, egyszerű G gráf minden csúcsának fokszáma legalább $\frac{n}{2}$, akkor G-nek van Hamilton-köre.

Ore tétel: ha $n \geq 3$ pontú, G egyszerű gráf bármely két, nem szomszédos u,v pontjára igaz, hogy $d(u) + d(v) \geq n$, akkor G-nek van Hamilton-köre.
***Bizonyítás:** Tegyük fel, hogy teljesül az Ore feltétel. Húzzunk be annyi új élt (Ore nem sérül), amíg a következő él Hamilton-kört nem eredményezne. Ekkor G-ben van Hamilton út. Ekkor létezik két olyan nem szomszédos pont, amelyre d(v)< n-1- d(u), mivel ha u előtti pontokkal v szomszédos volna, akkor Hamilton-kör lenne. Ez azonban ellentmondás.*

Dirac tétel következik Ore tételből.

7. Legrövidebb utat kereső algoritmusok (BFS, Dijkstra, Ford, Floyd). Legszélesebb utak irányított és irányítatlan gráfban.

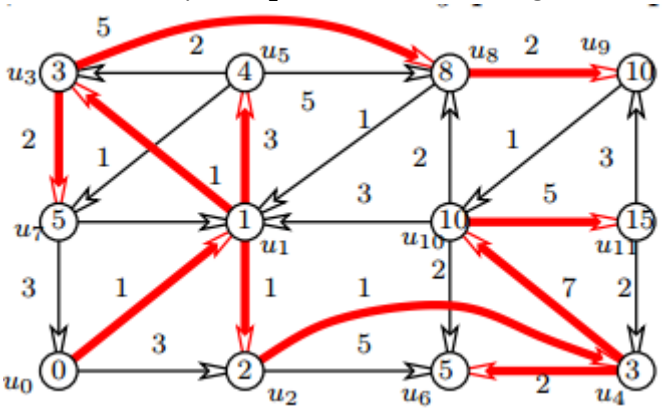
BFS: szélességi bejárás. Soron következő csúcsot mindig a legkorábban meglátogatottból látogatja meg. Az így kapott szélességi fa, a legrövidebb utak fája.

Tétel: a BFS által kapott szélességi fában u-ból v-be irányított út vezet, akkor ez az út egyben az (egyik) legrövidebb u,v út is.
Bizonyítás: *a szélességi fa minden éle mentén egy egységnyit távolodunk a gyökértől, mert először* v_0 *–t járjuk be, után a* V_1*-et alkotó szomszédokat, és így tovább.*

Tétel: a szélességi bejárás $c * (n + m)$-el becsülhető, ahol n és m a gráf csúcsai, ill. élei.
Bizonyítás: *a BFS minden lépése egy csúcshoz vagy egy élhez köthető,* v_i*-hez kötjük azt a lépést, amikor először meglátogatjuk a csúcsot, illetve azt, amikor észrevesszük, hogy már nem vezet bejáratlan pontba él.* $e = v_i v_j$*-hez kötjük azt a lépést, amikor megvizsgáljuk, hogy* v_j*-t már meglátogattuk-e. Látható, hogy minden csúcshoz, ill. élhez legfeljebb két lépést kötöttünk.*

Definíció: G=(E,V) gráf, $l: E \to R$ egy **hosszfüggvény**, ami minden élhez egy hosszt rendel.
A hosszfüggvény konzervatív, ha nincs negatív köre.

Dijkstra algoritmus:
Input: G=(V,E) gráf, és $l: E \to R_+$ nem negatív hosszfüggvény.
Output: a dist(u,-) hosszfüggvény, azaz G minden v csúcsára meghatározunk egy legrövidebb u,v utat.
Működés: kezdetben $d(u_0) := 0, ill.\ d(v) := \infty$. Először elvégezzük a javítást u_0-ból induló élekre, utána továbblépünk u_1-be a minimumot meghatározó élen…



Lépésszám: minden él mentén legfeljebb egyszer javítunk, a másik lépés az aktuális csúcs kiválasztása, ami minimum kiválasztás, legfeljebb n elem közül. Tehát legfeljebb $c * n^2$.

Ford algoritmus:
Input: G=(V,E) gráf, $l: E \to R$ konzervatív hosszfüggvény, és $u \in V$ pont.
Output: a dist(u,-) hosszfüggvény, azaz G minden v csúcsára dist(u,v).
Működés: kezdetben $d(u_0) := 0, ill.\ d(v) := \infty$. Az algoritmus fázisokból áll, és minden fázisban megpróbálunk sorra $e_1, e_2 \ldots$ éleken javítani. Ha egy fázisban nem sikerült javítani, akkor az algoritmus véget ér.
Lépésszám: mivel egy útnak legfeljebb n-1 éle lehet, ezért legkésőbb az (n-1). lépésre az algoritmus végez. Mivel minden fázisban körülbelül élszámnyi lépést végez, így a lépésszám $m * m$-el becsülhető.

Floyd algoritmus:
Input: G=(V,E) irányított gráf, $l: E \to R$ konzervatív hosszfüggvény

Output: dist(u, v) minden u, v-re.
Működés: Az algoritmus szomszédossági mátrixhoz hasonló táblázat segítségével működik, ahol a táblázat cellái a sorhoz és oszlophoz tartozó pontok távolságát tartalmazzák. $v_1, v_2 \dots v_n$ a G csúcsai. $d^k(i,j)$ a v_i-ből v_j-be vezető legrövidebb út hossza, úgy, hogy csúcsai a $v_i, v_j, v_1, v_2 \dots v_n$ halmazból kerülnek ki. Világos, hogy $d^0(i,j) = l(i,j)$. Mivel $d^{(k+1)}(i,j)$ vagy nem használja v_k pontot, vagy felbontható $v_i v_k$ *és* $v_k v_j$ utakra ezért $d^{(k+1)}(i,j)$=$min\{d^k(i,j), d^k(i,k+1) + d^k(k+1,j)\}$ tehát d^kismeretében $d^{(k+1)}$ könnyen számolható. Tehát $dist(v_i, v_j) = d^n(i,j)$, és ezt a függvényt $c * n^3$ lépésből ki tudjuk számolni.

Legszélesebb utak:

Szélességfüggvény: $w: E \to R_+$ az egyes élek „szélességét" leíró függvény. Ha P G útja, akkor P szélességét a „legkeskenyebb" útja határozza meg.

Mohó algoritmus a legszélesebb utak keresésére:
Megépítjük a legszélesebb utat, ami nem hoz létre kört. Ekkor egy legszélesebb utakat tartalmazó feszítőfát kapunk.
Az algoritmus helyességének bizonyítása:
Tegyük fel, hogy létezik szélesebb út u-v között. Hagyjuk el a legkeskenyebb e élt, ekkor a keletkező két komponens közt létezik szélesebb f él, de ezt az algoritmussal korábban már ellenőriztük. Ellentmondásra jutottunk.

Általánosított Dijkstra algoritmus:
Definiálhatunk egy konzisztens, monoton „jóság" fogalmat.
Input: G=(V,E) gráf, egy $u = u_0$ kezdőpont, és egy monoton, konzisztens „jóság" szerinti rendezés G útjain.
Output: u gyökerű, u-ból kifele irányított F részfa, amiben u-ból G minden csúcsa elérhető, ráadásul a „legjobb" G-beli uv úton.
Működés: Általános lépés, a legjobb tulajdonságú úttal elérhető pontot mindig a kész halmazhoz csatoljuk, majd ezen csúcs mentén javítunk.

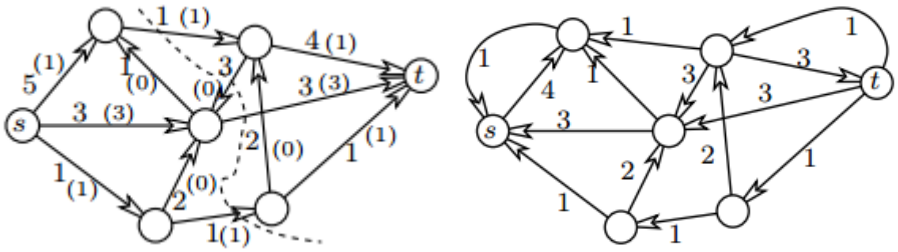
8. Hálózati folyamok: hálózat, folyam, folyamnagyság (folyamérték), st-vágás, vágás kapacitása. Ford-Fulkerson tétel, javító utas algoritmus. Egészértékűségi lemma, Edmonds-Karp tétel (biz. nélkül).

Hálózat: (G,s,t,c), ahol G irányított gráf, s,t G csúcsai, és G minden élét jellemzi c(e) nem negatív szám – az él kapacitása.
Példa: egy csővezeték, ahol s-ből t-be szállítjuk a folyadékot

Folyam: olyan f függvény (G,s,t,c) hálózatban, ami G minden éléhez egy számot rendel, úgy hogy:
- a folyam minden élen legfeljebb kapacitásnyi lehet (kapacitás feltétel)
- minden s-től és t-től különböző pontra igaz, hogy a befolyó folyam összmennyisége azonos a kifolyóéval (Kirchhoff-szabály).
Folyamnagyság: az f folyam m_f nagysága az a nettó folyammennyiség, ami s-ből kifolyik.

st-vágás: X a G csúcsainak s-t tartalmazó, de t-től diszjunkt részhalmaza. Az X és V(G)\X között futó éleinek egy halmazát a hálózat egy st-vágásának nevezzük.
Az X által meghatározott st-vágás kapacitása az X-ből V(G)\X-be futó élek kapacitásösszege.

Ford-Fulkerson tétel: Ha (G,s,t,c) egy véges hálózat, akkor létezik egy f folyam, és egy $s \in X \subseteq \mathrm{V(G)}\backslash\{t\}$ részhalmaz úgy, hogy az m_f folyamnagyság azonos az X által definiált st-vágás kapacitásával.
Bizonyítás: *javító utas algoritmussal. G_f segédgráfot hozunk létre, irányítsuk úgy G éleit, hogy ahol még növelhető a folyamnagyság, ott előreél, ahol pedig a folyam csökkenthető, ott visszaélek szerepelnek. A G_f segédgráfon definiáljuk a c(u,v)=c(u,v)-f(u,v) ha uv előreél, c(u,v)=f(v,u) ha uv visszaél, kapacitásokat. Az algoritmus addig fut, amíg van s-t út. Ha talál ilyen utat, akkor az út előre élein növeljük a folyamot, az út visszaéleinek megfordítottjain pedig csökkentjük. Ez alapján látszik, hogy ha nincs már s-t út, akkor maximális folyamot találtunk.*
Megkeressük azokat a pontokat, amik s-ből elérhetőek, ők alkotják az X halmazt. Ehhez a halmazhoz tartozó vágás minimális vágás lesz.



Hálózati folyam. A zárójelekben az f folyam által felvett értékek állnak. A folyamérték 1+3+1=5. A szaggatott vonal 5 értékű st-vágás. A másik ábra a segédgráf - már nem tartalmaz javító utat

Egészértékűségi lemma: ha a hálózatban minden kapacitás egész szám, akkor létezik olyan maximális folyam, ami a gráf minden élén egész értéket vesz fel. Az ilyen folyamot egész folyamnak nevezzük.

Edmonds-Karp tétel: ha a hálózatban a maximális folyamot javító utas algoritmussal keressük, és mindig egy legkevesebb élből álló út mentén növelünk, akkor a folyamat lépésszáma felülről becsülhető n^3-al.

9. Többtermelős, többfogyasztós hálózatok, csúcskapacitások és irányítatlan élek kezelése. Él- és pont-idegen utak. Menger négy tétele, gráfok többszörös összefüggősége, kapcsolata a Menger tételekkel.

Folyamproblémák általánosítása:
Irányítatlan élek: minden él helyett vegyünk be egy-egy oda-vissza irányított élt.
Csúcskapacitások: minden csúcsot daraboljunk ketté, őket a csúcs kapacitásának megfelelő él kösse össze, egyik csúcsba csak befolyó élek érkezzenek, másik csúcsból csak kifolyó élek induljanak.
Több termelő, több fogyasztó: vegyünk fel egy virtuális termelőt/fogyasztót, és az összes termelőt/fogyasztót kössük össze a virtuális megfelelőjükkel végtelen kapacitású élekkel.

P és Q u és v közt futó utak, akkor:
Éldiszjunkt(él-idegen): P és Q út nem tartalmaz közös élt. $E(P) \cap E(Q) = \emptyset$. Éldiszjunkt utak maximális száma: $\lambda(u, v)$.
Pontdiszjunkt(pont-idegen): P és Q pontnak csak a kezdő és végpontja közös. $V(P) \cap V(Q) = \{u, v\}$. Pontdiszjunkt utak maximális száma: $\kappa(u, v)$.

G gráf U ponthalmaza (ill. F élhalmaza) **lefog** minden u,v utat, ha a G-U (ill. G-F) nem tartalmaz u-ból v-be vezető utat.

Menger tételei:
1. Ha u és v G irányított gráf különböző csúcsai, akkor az él-idegen uv utak maximális száma ($\lambda_G(u, v)$) azonos az uv utakat lefogó élek minimális számával.
2. Ha u és v G irányított gráf különböző, nem szomszédos csúcsai, akkor a pont-idegen uv utak maximális száma ($\kappa_G(u, v)$) azonos az uv utakat lefogó, u-tól és v-től különböző pontok minimális számával.
3. Ha u és v G irányítatlan gráf különböző csúcsai, akkor az él-idegen uv utak maximális száma ($\lambda_G(u, v)$) azonos az uv utakat lefogó élek minimális számával.
4. Ha u és v G irányítatlan gráf különböző, nem szomszédos csúcsai, akkor a pont-idegen uv utak maximális száma ($\kappa_G(u, v)$) azonos az uv utakat lefogó, u-tól és v-től különböző pontok minimális számával.

Bizonyítás:
1. *(G; u; v; 1) hálózat. Ebben a hálózatban minden uv egészfolyam 0-t vagy 1-et rendel minden élhez. f egy maximális folyam, X pedig egy olyan ponthalmaz, ami minimális uv vágást határoz meg. Mivel minden kapacitás egész, így az egészértékűségi-lemma miatt f egész folyam, és nagysága k. Mivel max folyam = min vágás, így X vágás kapacitása is k. Ez által az X csúcsaiból pontoson k él lép ki (mivel minden élen 0 vagy 1 folyik). k élt elhagyva nem tudunk X-ből V\X-be eljutni, tehát ez a k él minden uv utat lefog -> a lefogó élek minimális száma k.*
Most mutassuk meg azt, hogy van k éldiszjunkt út. Legyen E' azoknak az éleknek a száma, amiken 1 egységnyi folyam folyik. Kirchhoff szabálya miatt minden u-tól és v-től különböző pontra igaz, hogy ugyanannyi E'-beli él lép be, mint amennyi ki. Tekintsük G=(V,E*) gráfot, ahol E*-ot úgy kapjuk, hogy E'-höz hozzáveszünk még k párhuzamos vu élt. Így G*-ban minden csúcsnak megegyezik a befoka és kifoka. Legyen K a G* azon irányítatlan értelemben vett komponense, ami tartalmazza az u csúcsot. Mivel minden pont foka páros, így K-nak létezik Euler körsétája. Ha ebből elhagyjuk az utólag bevett k vu élt, akkor a körséta k éldiszjunkt irányított uv sétára esik szét. Minden ilyen uv sétából kiválasztható egy uv-út.*
2. *Csúcsokat vágjuk szét a fentebb ismertetett módon, és használjuk az első tétel bizonyítását.*
3-4. *Hasonlóan 1-es és 2-es bizonyításához, csak itt az irányítatlan élek helyett párhuzamos oda-vissza éleket kell felvenni.*

k-szorosan (pont)összefüggő egy irányítatlan gráf, ha k+1 csúcsa van, és bárhogy hagyunk el belőle k-1 csúcsot, összefüggő marad. Maximális: $\kappa(G)$
k-szorosan élösszefüggő egy irányítatlan gráf, ha összefüggő marad, bárhogy is hagyunk el belőle k-1 élt. Maximális: $\lambda(G)$

Tétel: Egy egyszerű, irányítatlan G gráf pontosan akkor k-összefüggő, ha G-nek legalább k+1 pontja van, és G bármely két különböző pontja között létezik k pontidegen út.
G pontosan akkor k-élösszefüggő, ha G bármely két, különböző pontja között vezet k élidegen út.
Bizonyítás:
Éldiszjunkt változat: Ha G k-élösszefüggő, akkor semelyik két pont közti utakat nem fogja le k-nál kevesebb él (azokat elhagyva ugyanis G szétesne), ezért Menger 3. tétele szerint tetszőleges két pont között létezik k élidegen út.
Pontdiszjunkt változat: indirekt: G k-összefüggő, és u-ból v-be legfeljebb k-1 pontdiszjunkt út található. Ha u és v nem szomszédosak, akkor Menger 4. tétele miatt az uv-utak lefoghatóak k-1 ponttal. Ezek elhagyásával G szétesne, de ez ellentmond G k-szoros összefüggőségének.

Menger tétel: ha G legalább 3 pontú gráf, akkor az alábbi állítások ekvivalensek:
1. G 2-összefüggő
2. G bármely 2 pontján át vezet kör
3. Ha nincs izolált pontja, akkor bármely 2 élén át vezet kör.
Bizonyítás:
1->2: Ha G 2-összefüggő, akkor bármely u,v pontja között van két pontidegen út, amelyek együtt kört alkotnak.
2->1: A kör tekinthető két pontidegen út uniójának, tehát G 2-összefüggő.
3->2: Ha u-n és v-n keresztül akarunk kört találni, akkor elegendő egy u-ra és v-re illeszkedő körön keresztül kört találni, ami 3. feltétel szerint létezik.
1->3: G úgy is 2-összefüggő marad, ha két élét felosztjuk egy-egy ponttal. 2. miatt létezik a felosztó pontokon keresztül kör, ami épp a felosztott éleken keresztüli kör.

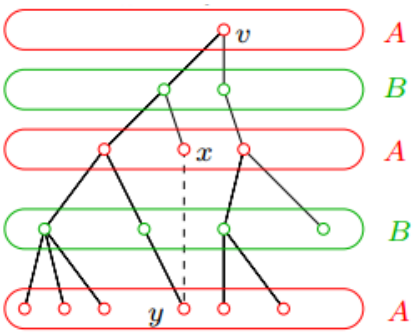
Dirac tétele: Ha G k-összefüggő, és $k \geq 2$, akkor G bármely k pontján keresztül található kör G-ben.

10. Páros gráfok, ekvivalens definíció. Párosítások, Hall, Frobenius és Kőnig tételei, alternáló utas algoritmus maximális párosítás keresésére. Lefogó és független csúcsok, ill. élek, Gallai két tétele. Tutte tétele párosításokról (csak a triviális irányban bizonyítva).

Páros gráfok: G csúcsai két diszjunkt halmazra bonthatóak, úgy hogy minden él a halmazok között fut.
Ekvivalens definíció: G akkor páros, ha $\chi(G) \leq 2$, azaz G két színnel színezhető.

Megfigyelések:
1: Páros hosszú kör páros, mert felváltva ki lehet színezni a pontjait.
2: Páratlan kör nem páros, mert mire körbeérünk, két azonos színű pont lesz egymás mellett.
3: Ha egy gráf páros, akkor a részgráfja is páros.
4. Páros gráf nem tartalmazhat páratlan kört.

Tétel: G véges gráf pontosan akkor páros, ha nem tartalmaz páratlan kört.



Bizonyítás: *szükségesség adódik az előző megfigyelésből. Elégségesség: tegyük fel, hogy G nem tartalmaz páratlan kört. Mivel élek csak a komponenseken belül futnak, elegendő egy komponensen belül találni 2-színezést, azaz feltehető, hogy G összefüggő. F a G feszítőfája, és u az F gyökere. A a v-től páros távolságra, B pedig a páratlan távolságra lévő csúcsok halmaza. Világos, hogy F minden éle A és B között fut. Ha futna G-nek xy éle, mondjuk A halmazon belül, akkor létezne G-ben páratlan hosszú körséta.*
Következmény: Mivel a fában nincs kör, így minden fa páros.

Definíció: a G=(V,E) gráf éleinek M részhalmaza független, más szóval M (részleges) **párosítás**, ha az M-beli élek végpontjai különbözőek. M **teljes párosítás**, ha G minden csúcsát fedi.

Definíció: a G=(V,E) gráf $X \subseteq V$ ponthalmaz szomszédjainak számát N(X) jelöli.

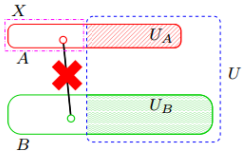
Definíció: adott G gráf esetén $\nu(G)$ jelöli a maximális független élhalmaz méretét, azaz G maximális párosításának elemszámát.
Definíció: adott G pontjainak U halmaza lefogó ponthalmaz, ha G minden élének van U-beli végpontja. Minimális lefogó ponthalmaz: $\tau(G)$.

Állítás: ha G véges gráf, akkor $\nu(G) \leq \tau(G)$.

Kőnig tétele: ha G=(A,B,E) véges, páros gráf akkor $\nu(G) = \tau(G)$.
Bizonyítás: *Menger tételével. G irányítatlan gráf, felveszünk hozzá s,t pontokat. s és A, valamint t és B minden pontja közé vezessünk élt. Világos, hogy ha létezik G-ben k független él, akkor ezek segítségével találunk k pontdiszjunkt st-utat a G' gráfban. Ha ismerünk k pontdiszjunkt st-utat, akkor az ezek által használt G-beli élek függetlenek – a független élek száma megegyezik az st-utak maximális számával -> ($\nu(G) = \kappa_G(s,t)$). Menger 4 miatt a pont-idegen st utak maximális száma ($\kappa_G(s,t)$) megegyezik az st-utakat lefogó, s-től és t-től különböző pontok minimális számával. U részhalmaz pont akkor fogja le G összes élét, ha lefog minden st-utat -> $\tau(G) = \kappa_G(s,t)$.*
Tehát: $\tau(G) = \kappa_G(s,t) = \nu(G)$.

Hall tétele: a G=(A,B,E) véges, páros gráfnak pontosan akkor létezik A-t fedő párosítása, ha $|X| \leq |N(X)|$ minden $X \subseteq A$-ra.

Biz.: *a szükségesség nyilvánvaló. Elégségesség: Tegyük fel, hogy ha* $|X| \leq |N(X)|$ *minden* $X \subseteq A$*-ra.*

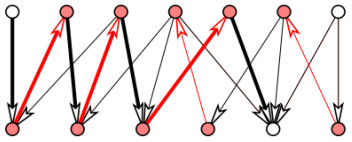


Így azt kell bizonyítanunk, hogy $\nu(G) \geq |A|$*. Legyen U minimális lefogó ponthalmaz,* $U_A = U \cap A$ *és* $U_B = U \cap B$*. Mivel U lefogja az* $X := A \backslash U_A$*-ból induló éleket, ezért* $N(X) \subseteq U_B$*, tehát* $|N(X)| \leq |U_B|$*. Hall és Kőnig miatt:*

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

Frobenius tétele: a G=(A,B,E) véges, páros gráfnak pontosan akkor létezik teljes párosítása, ha |A|=|B|, és $|X| \leq |N(X)|$ minden $X \subseteq A$-ra.
Bizonyítás: *triviálisan következik Hall tételéből.*

Alternáló utas algoritmus maximális párosítás keresésére: kiindulunk az üres párosításból, és azt javítgatjuk. Ha már találtunk M párosítást, akkor tekintjük az ahhoz tartozó segédgráfot, azaz M éleit B-ből A-ba irányítjuk, G egyéb éleit fordítva. Ha ebben a segédgráfban létezik út egy fedetlen A-ból,



eddig fedetlen B-be, akkor az ú.n. alternáló úton az eddigi párosítás éleket elhagyva, és az út párosításon kívüli éleit bevéve egy eggyel nagyobb méretű párosítást kapunk. Ha nincs ilyen út, akkor M maximális párosítás.

Definíció: G gráf pontjainak U részhalmaza <u>független ponthalmaz</u>, ha U nem feszít élt. A maximális független ponthalmaz elemszáma $\alpha(G)$.
Definíció: G gráf éleinek F részhalmaza <u>lefogó élhalmaz</u>, ha G minden pontjából indul F-beli él. Minimális lefogó élhalmaz elemszáma $\rho(G)$.

	élhalmaz	ponthalmaz
maximális független	$\nu(G)$	$\alpha(G)$
minimális lefogó	$\rho(G)$	$\tau(G)$

Megfigyelés: tetszőleges, véges G gráfra $\alpha(G) \leq \rho(G)$.

Gallai tétele:
1. ha G-ben nincs hurokél, akkor $\tau(G) + \alpha(G) = n$
2. ha G-nek nincs izolált pontja: $\nu(G) + \rho(G) = n$
Bizonyítás:
1. $U \subseteq V(G)$ *pontosan akkor lefogó ponthalmaz, ha V(G)\U független részhalmaz.*
2. *Mivel G-nek létezik* $\nu(G)$ *diszjunkt éle, ezek* $2\nu(G)$ *pontot fognak le. A maradék pontok mindegyike lefogható egy új éllel, hiszen nincs izolált pont ->* $\nu(G) + n - 2\nu(G) = n - \nu(G)$ *éllel minden pont lefogható. Innen* $\rho(G) \leq n - \nu(G)$*, ebből pedig:* $\nu(G) + \rho(G) \leq n$*.*
Ha F minimális méretű lefogó élhalmaz, akkor F körmentes, és nem tartalmaz 3 hosszú utat sem -> F diszjunkt csillagok uniója. Ha a minimális lefogó élhalmazban k csillag van, akkor n-k élt tartalmaz, és tartalmaz k diszjunkt élt, tehát $\nu(G) \geq k$*.* $\nu(G) + \rho(G) \geq n - k + k = n$ *-> a másik egyenlőtlenséget is figyelembe véve következik a tétel.*

Kőnig tétele: ha G véges, páros gráfnak nincs izolált pontja, akkor $\alpha(G) = \rho(G)$.
Bizonyítás: *páros gráfnak nem lehet hurokéle, így következik Kőnig előző, és Gallai két tételéből:*
$\alpha(G) = |V(G)| - \tau(G) = |V(G)| - \nu(G) = \rho(G)$

Definíció: $C_p(G)$ a G páratlan méretű komponenseinek száma

Tutte tétele: a véges G gráfnak pontosan akkor van teljes párosítása, ha tetszőleges $X \subseteq \mathrm{V(G)}$-re $C_p(G - X) \leq |X|$

11. Pont- és élszínezés, kromatikus szám, klikkszám, alsó és felső korlátok a kromatikus és élkromatikus számra, Brooks tétel (biz. nélkül), Vizing tétel (biz. nélkül).

k-színezhető egy G gráf, ha minden csúcs kiszínezhető k adott szín valamelyikére, úgy hogy minden szomszédos csúcs különböző színű.
Kromatikus szám χ(G)=k, ha G k-színezhető, de nem (k-1)-színezhető.

Megfigyelések:
1. Ha G tartalmaz hurokélt, akkor nem színezhető
2. G gráf színosztályának (adott színezéshez tartozó) csúcsai között nem fut él.

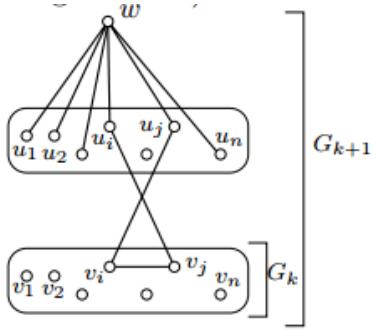
Klikk: a G teljes részgráfja. $\omega(G)$ **klikkszám** a G legnagyobb klikkjének pontszáma, azaz $\omega(G) = k$, ha G-ben van k méretű, de nincs k+1 méretű klikk.

Állítás: minden irányítatlan G véges gráfra igaz, hogy $\omega(G) \leq \chi(\mathrm{G}) \leq \Delta(\mathrm{G}) + 1$, valamint $\chi(\mathrm{G})\alpha(G) \geq n$, ahol n a G pontjainak száma.
Bizonyítás: *első egyenlőtlenség: G pontjainak kiszínezésével a klikk pontjait is kiszínezzük*
második egyenlőtlenség: Mohó színezés. Minden csúcs kapja azt a legkisebb színt, amit a szomszédjai nem használnak, így nem kaphat nagyobb színt, mint a szomszédjai számánál egyel nagyobb szám.

Megfigyelés: $\chi(\mathrm{G}) = \Delta(\mathrm{G}) + 1$, ha $G = K_n$ vagy $G = C_{2n+1}$

Brooks tétele: G véges, egyszerű, összefüggő. Ha G nem teljes, és nem páratlan kör, akkor $\chi(\mathrm{G}) \leq \Delta(\mathrm{G})$

Tétel: tetszőleges $k \geq 2$ pozitív egészhez létezik olyan G gráf, amelyre $\chi(\mathrm{G}) = k$ és $\omega(G) = 2$.
Bizonyítás: Mycielski konstrukció.
Megadunk egy megfelelő G_k gráfot, és k paraméter szerinti indukcióval bizonyítunk. k=2-re az állítás nyilván helyes. TFH, hogy k-ra már sikerült megfelelőG_k gráfot létrehoznunk. $V(G_k) = \{v_1 v_2 \dots v_n\}$. Most hozzuk létre G_{k+1}-et, úgy hogy $V(G_k) = \{v_1 v_2 \dots v_n\} \cup \{u_1 u_2 \dots u_n\} \cup \{w\}$, ahol u_i és w az eddigiektől, és egymástól független csúcsok. Kössük össze w-t minden u_i-vel, valamintG_k-beli él (önmagán kívül) két másikért legyen felelős. Mivel az u_i pontok függetlenek, és w-ből nem fut él v_i-be, ezért G_{k+1}-ben minden háromszög legalább két G_k-beli pontot tartalmaz – ennek nyilván nem lehet w a harmadik pontja. Az indukciós feltevés miatt ez nem lehet G_k-beli pont sem. Ha mondjuk u_l lenne ez a pont, akkor G_{k+1}-ben lenne háromszög, ami megint csak ellent mond az indukciós feltevésnek.



Azt kell még bebizonyítani, hogy G_{k+1} k+1 kromatikus. Világos, hogy $\chi(G) \leq (k+1)$. Indirekt belátható az is, hogy nem színezhető k színnel.

k-élszínezhető egy G gráf, ha minden él kiszínezhető k adott szín valamelyikére, úgy hogy minden szomszédos él különböző színű.
Élkromatikus szám $\chi'(\mathrm{G}) = k$, ha G k-élszínezhető, de nem (k-1)-élszínezhető.

Állítás: tetszőleges G gráfra $\chi'(\mathrm{G}) \geq \Delta(\mathrm{G})$.
Bizonyítás: *Az egy csúcsból induló élek mind más színt kapnak, ez a legnagyobb fokszámúra is igaz.*

Vizing tétele: Ha G véges, egyszerű gráf, akkor $\chi'(\mathrm{G}) \leq \Delta(\mathrm{G}) + 1$.

Shannon tétele: Ha G véges, akkor $\chi'(\mathrm{G}) \leq \frac{3}{2}\Delta(\mathrm{G})$.

12. Síkbarajzolhatóság, gömbre rajzolhatóság. Az Euler-féle poliéder tétel és következményei: egyszerű, síkbarajzolható gráfok élszáma és minimális fokszáma. Kuratowski gráfok, Kuratowski tétele (csak könnyű irányban biz.), Fáry-Wagner tétel (biz. nélkül).

Definíció: G=(V,E) gráf **síkbarajzolható**, ha van G-nek olyan diagramja, amin élek csak végpontban metszik egymást.
G síkbarajzolható, ha létezik síkbarajzolása.

Tétel: G gráf pontosan akkor síkbarajzolható, ha gömbrerajzolható.
Bizonyítás: *sztereografikus projekcióval.*

Tétel: tetszőleges konvex poliéder élhálója síkbarajzolható.
Bizonyítás: *vetítsük az élhálót egy belső P pontból P középpontú gömbre, így az élháló gömbrerajzolható -> síkbarajzolható.*

Tétel: G síkbarajzolt gráf, akkor $n + t = e + k + 1$, ahol n a pontok, t a tartományok, e az élek, k pedig a komponensek száma.
Euler formula: G síkbarajzolt, összefüggő gráf, akkor $n + t = e + 2$.
Bizonyítás: *élszám szerinti teljes indukcióval.*

Következmények:
1. Ha G síkbarajzolható, akkor bármely síkbarajzolásának ugyanannyi tartománya van
2. Ha G egyszerű, legalább 3 pontú, síkbarajzolható, akkor $e \leq 3n - 6$
3. Sem K_5 sem $K_{3,3}$ nem síkbarajzolható
Bizonyítás:
2. *Húzzunk be annyi új élt, amennyit csak tudunk a síkbarajzolhatóság megtartásával. Legyen e' az élek t' a tartományok száma az így létrejött gráfban. Minden tartományt három él, és minden él 2 tartományt határol* $2e' = 3t' = 3(e' + 2 - n) = 3e' + 6 - 3n \rightarrow\ 3n - 6 = e' \geq e$.
3. K_5*: n=5, e=10,* $10 \geq 3 * 5 - 6$ *ellentmondás* $e \leq 3n - 6$
$K_{3,3}$*: n=6, e=9, ->t=5. Mivel körmentes, minden tartományt legalább 4 él határol ->* $20 = 4t \leq 2e = 18$.

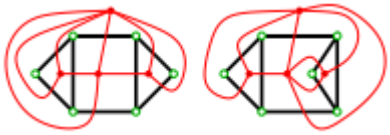
Topologikusan izmorf: H és G gráf, ha G megkapható H-ból ezt a két lépést ismételve:
1. egy élt kettéosztunk egy ponttal
2. törlünk egy pontot, és egy éllel összekötjük a két szomszédját.
Topologikus izomorfia nem befolyásolja a síkbarajzolhatóságot.

Kuratowski tétele: G gráf pontosan akkor síkbarajzolható, ha nem tartalmaz K_5-el, vagy $K_{3,3}$-al topologikusan izomorf részgráfot.
Bizonyítás: *csak a szükségességet bizonyítjuk. Ha G síkbarajzolható, akkor minden H részgráfja is síkbarajzolható. Ha H topologikusan izomorf K-val, akkor K is síkbarajzolható. Így K=*K_5*, vagy K=*$K_{3,3}$ *nem lehetséges.*

Fáry-Wagner tétel: H G egyszerű és síkbarajzolható, akkor G síkbarajzolható úgy is, hogy minden él egyenes szakaszként van lerajzolva.

13. Dualitás, tulajdonságai. Elvágó él, soros élek, vágás. Gyenge izomorfia, absztrakt dualitás, Whitney három tétele (biz. nélkül), síkgráfok kromatikus száma, ötszíntétel.

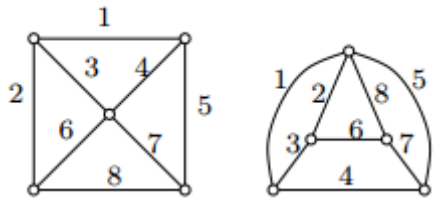
G*=(V*,E*) G gráf **duálisa**, ha V* G tartományainak felel meg, $E^* = \{e^* : e \in E\}$, ahol e* az e-t határoló tartományokat összekötő él. G* függ G adott síkbarajzolásától is.



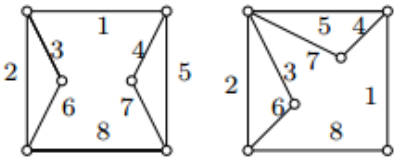
Definíció: $Q \subseteq E(G)$ élhalmaz **vágás**, ha Q-t elhagyva G több komponensre esik szét, és Q egy legszűkebb ilyen halmaz, azaz Q semelyik valódi részhalmazára ez nem teljesül. Az e él **elvágó él**, ha $\{e\}$ vágás. G gráf e és e' élei **soros élek**, ha $\{e, e'\}$ vágás.

Tétel: G=(V,E) síkbarajzolható
1. Ha G* a G duálisa, akkor G* síkbarajzolható, és összefüggő
2. f(e):=e egy f: E(G)->E*(G) természetes bijekciót definiál.
3. Ha e a G hurokéle (elvágó éle) ↔ f(e) a G* elvágó éle (hurokéle)
4. e,e' G soros (párhuzamos) élei ↔ f(e),f(e') a G* párhuzamos (soros) élei
5. Ha G összefüggő, akkor G=(G*)*, és ekkor G pontja bijektíven G* lapjainak felelnek meg
6. C a G köre (vágása) ↔ f(C) a G* vágása (köre)

Absztrakt duális: G a H absztrakt duálisa, ha létezik egy $\varphi: E(G) \to E(H)$ úgy, hogy
1. C a G köre ↔ $\varphi(C)$ a H vágása
2. Q a G vágása ↔ $\varphi(Q)$ a H köre

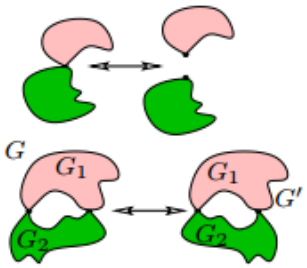


Gyengén izomorf két gráf, ha létezik egy $\varphi: E(G) \to E(H)$ úgy, hogy C pontosan akkor köre G gráfnak, ha $\varphi(C)$ H köre.



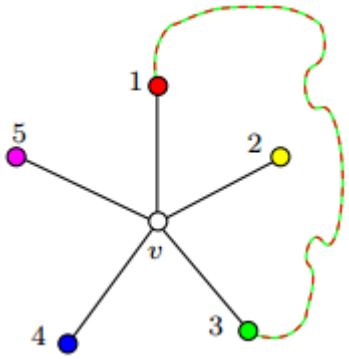
Whitney I.: G gráfnak pontosan akkor létezik absztrakt duálisa, ha G síkbarajzolható.
Whitney II.: Ha G síkbarajzolható, továbbá G és H gyengén izomorf akkor
1. H is síkbarajzolható
2. G* és H* is gyengén izomorf
3. G és (G*)* gyengén izomorf

Whitney III.: Ha G és H gyengén izomorf, akkor H előállítható G-ből az alábbi 3 művelettel:
1. egy elvágó pont mentén ketté daraboljuk a gráfot, vagy egy izolált pontot adunk hozzá
2. két külön pontot elvágó pontként egyesítünk
3. két elvágó pont mentén a gráfot szétszedhetjük, és a pontokat fordított sorrendben köthetjük össze



4-szín tétel: Minden egyszerű, síkbarajzolható gráf 4-színezhető.
Bizonyítás: *számítógéppel*

5-szín tétel: Minden egyszerű, síkbarajzolható gráf 5-színezhető. $\chi(G) \leq 5$
Bizonyítás: *legfeljebb 3 pontú gráfokra a tétel triviálisan igaz. Nagyobbakra pontszám szerinti indukció: tfh. legfeljebb (n-1) pontú gráfokra a tétel igaz. Legyen G egy n>3 pontú egyszerű, síkbarajzolható gráf. Ekkor tudjuk, hogy* $e \leq 3n - 6$*, tehát G pontjainak fokszámösszege legfeljebb 6n-12 -> G-nak van legfeljebb 5-ödfokú v csúcsa. Mivel G-v is egyszerű és síkbarajzolható, ezért az indukciós feltevés miatt 5-színezhető. Tehát ha v szomszédjai legfeljebb 4 színt kapnak, akkor v kaphatja az ötödiket. Ez nem működik, ha d(v)=5. Ekkor G-v-ben nézzük a v 1-es és 3-as színű szomszédjai által feszített* $G_{1,3}$ *részgráfot. Ha v 1-es és 3-as színezésű szomszédjai* $G_{1,3}$ *különböző komponenseibe esnek, akkor pl. 1-es szomszéd komponensében felcserélve az 1-es és 3-as színezéseket, v-nek nem lesz 1-es színű szomszédja -> v 1-es színűre színezhető. Ellenkező esetben van v 1-es és 3-as színű szomszédjai között olyan út, ami csak 1-es és 3-as színeket használ. A síkbarajzoltság miatt ekkor v 2-es és 4-es színű szomszédjai között nincs olyan út, ami csak 2-es és 4-es csúcsokat használna, tehát* $G_{2,4}$*-ben ezek a csúcsok különböző komponensekbe kerülnek.*



14. Mélységi keresés és alkalmazásai (élek osztályozása, irányított kör létezésének eldöntése), alapkörrendszer. Aciklikus irányított gráfok jellemzése, topologikus sorrend, Pert-módszer, kritikus utak és tevékenységek.

Mélységi bejárás (DFS): olyan bejárás, ahol egy v_0 gyökércsúcsból indulunk, és mindig a legutóbb elért v_i csúcsból egy még bejáratlan v_{i+1} csúcsba igyekszünk egy gráfél mentén. Ha ez nem sikerül, akkor visszalépünk egy v_j csúcsba, ahonnan v_i-t elértük, és innen próbálunk bejáratlan csúcsba lépni. Ha visszajutunk v_0-ba, és nem tudunk tovább menni, de még nem jártunk be minden csúcsot, akkor új gyökérpontot választunk.
A mélységi bejárás bejárási fáját **mélységi fának** nevezzük.
A mélységi számozás a mélységi bejárás elérési sorrendje.
Faél, vagy előreél: az az uv él, ahol v mélységi száma nagyobb, mint u-é. v az u közvetlen leszármazottja.
Visszaél ha u mélységi száma nagyobb, mint v-é, és u a v leszármazottja.
Keresztél, ha u mélységi száma nagyobb, mint v-é, és u és v nem leszármazottai egymásnak.

Aciklikus egy G irányított gráf, ha nem tartalmaz (irányított) kört.

Tétel: Ha G irányított gráf, akkor az alábbi négy állítás ekvivalens:
1. G aciklikus
2. G egyetlen mélységi bejárásában sincs visszaél
3. G valamely mélységi bejárásában nincs visszaél
4. G csúcsai sorba rendezhetőek úgy, hogy G minden éle egy sorrendben későbbi csúcsba mutat – ez a sorrend a **topologikus sorrend.**
Bizonyítás:
1->2 *ha találnánk a mélységi bejárásban uv visszaélt, akkor létezne vu út csupa faélekből, ehhez hozzáadva egy uv visszaélt kört kapnánk.*
2->3 *triviális.*
3->4 *Tekintsük azt a mélységi bejárást, amiben nincs visszaél. Ennek során minden v csúcs esetén pontosan egyszer történt meg, hogy éppen v-ből próbáltunk bejáratlan csúcsot találni, de ilyen nem volt. E mélységi bejáráshoz tartozik tehát egy* ***befejezési sorrend*** *is, ami a csúcsokat olyan sorrendben sorolja fel, ahogyan a fenti szituáció előadódott. Ebből látszik, hogy ha uv faél, visszaél, vagy keresztél, akkor v megelőzi u-t a befejezési sorrendben. Ezért ha nincs visszaél, akkor a befejezési számozás pont olyan sorrendet ad, amilyet kerestünk.*
4->1 *Ha lenne irányított kör, akkor az feltétlenül tartalmazna olyan élt, ami egy a sorrendben későbbi csúcsból mutat egy korábbiba.*

Tétel: ha G gráfnak n csúcsa, és e éle van, akkor a mélységi bejárás lépésszáma felülről becsülhető $c * (n + e)$-vel.
Bizonyítás: *BFS hasonló bizonyításának értelemszerű módosítása.*

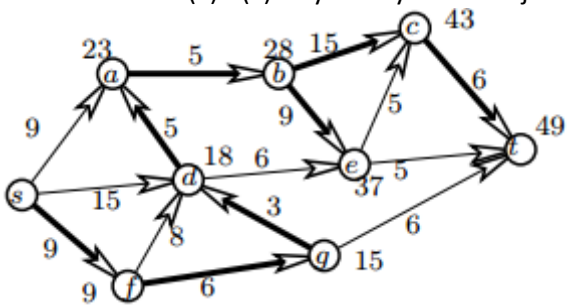
Definíció: Ha F a G feszítőfája, akkor minden $e \epsilon E(G)$ élhez, ami nincs benne a feszítőfában, tartozik egy **alapkör**, ez pedig az $F \cup e$ egyetlen köre.

Definíció: Ha F a G irányítatlan gráf feszítőfája, akkor F-hez tartozik egy **fundamentális körrendszer**: a G-F éleihez tartozó alapkörök.

Definíció: Ha F a G irányítatlan gráf feszítőfája, akkor F minden éle meghatározza a G csúcsainak egy két részre osztását. Ezen felosztások alkotják a **fundamentális vágásrendszert**.

Pert-módszer: a probléma lényege egy F feladat optimális ütemezése. A szabályok mindegyike olyan alakú, hogy egy v tevékenységet nem kezdhetünk meg hamarabb u tevékenység után c(uv) időnél. Definiálható F-hez egy P(F) irányított gráf, aminek a csúcsai a tevékenységek. Minden szabálynak megfelel P(F) egy súlyozott, irányított éle. P(F) aciklikus. F feladat k ütemezése abból áll, hogy F minden tevékenységéhez úgy jelölünk ki egy-egy kezdési időpontot, hogy minden vonatkozó szabályt betartunk. Tehát minden v tevékenységhez úgy jelölünk ki egy k(v) kezdési időpontot, hogy minden uv élre teljesüljön $k(v) \geq k(u) + c(uv)$. Az F feladat k ütemezés szerinti elvégzéséhez szükséges idő k(t). Optimális esetben k(t) minimális. Az F feladat h(F) hossza, az F végrehajtásához szükséges idő, azaz h(F)=k(t), ha k(t) minimális. Egy u tevékenységet **kritikus tevékenységnek** nevezünk, ha u kezdési időpontja nem függ az optimális ütemezéstől. Pert célja egy optimális ütemezés kiszámítása, és a kritikus tevékenységek meghatározása.

Tétel: a fentiek szerint megadott F feladat hossza megegyezik a P(F) gráfban az irányított st-utak maximumával.
Egy u tevékenység pontosan akkor kritikus, ha létezik u-n keresztül irányított, h(F) súlyú st-út.
Kritikus útnak a P(F) h(F) súlyú irányított st-útját nevezzük.



15. Algoritmusok bonyolultsága, döntési problémák. P, NP, co-NP bonyolultsági osztályok fogalma, feltételezett viszonyuk, polinomiális visszavezethetőség, NP-teljesség, Cook-Levin tétel (biz. nélkül), nevezetes NP-teljes problémák: SAT, HAM, 3-SZÍN, k-SZÍN, MAXFTN, MAXKLIKK, HAMÚT.

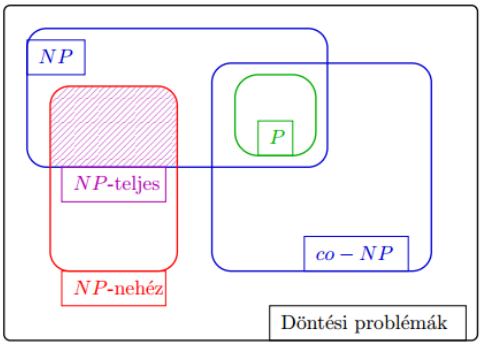
$\boldsymbol{f_A(n)}$ az A algoritmus **legnagyobb lépésszáma** n hosszúságú input esetén.

Egy algoritmus **polinomiális**, ha lépésszáma felülről becsülhető a bemenet méretének polinomjával.
Egy algoritmus **exponenciális**, ha a futásideje exponenciális függvénye lehet a bemenet hosszának.
Pl. összeadás, szorzás polinomiális, hatványozás exponenciális.

Döntési probléma: adott bemenetre igen vagy nem választ ad.
Pl.: prímtesztelés, bemenete egy szám, kimenete pedig egy bit, ami 1 ha prím, 0 ha nem.

P: a polinom időben eldönthető döntési problémák osztálya
Pl.: Van-e Euler kör a gráfban. Bemenet egy n pontú, m élű gráf (bemenet mérete n+4m). Azt ellenőrizzük, hogy összefüggő-e a gráf, valamint, hogy minden pont foka páros-e. Ezeket meg lehet tenni polinomiális algoritmusokkal. Létezik tehát $c * (n + m)$ hosszú algoritmus a probléma eldöntésére.
További példák: gráf összefüggősége (BFS-el), k-méretű párosítás létezése, k nagyságú folyam létezése (max. folyam kereséssel), PERT elvégezhető-e k idő alatt (optimális ütemezés keresése), síkbarajzolható-e a gráf.
NP: az olyan π döntési problémák osztálya, melyekre létezik p_πk - polinom minden egyes olyan b bemenetre, amire igen a válasz, hogy ez legfeljebb $p_\pi(|b|)$ lépésben bebizonyítható.
Pl.: Hamilton-teszt esetén a bizonyíték a Hamilton-kör leírása volt, ugyanis ennek ismeretében $c * n$ lépésben bizonyítható, hogy igen a válasz.
co-NP: az olyan π döntési problémák osztálya, melyekre létezik p_πk - polinom minden egyes olyan b bemenetre, amire nem a válasz, hogy ez legfeljebb $p_\pi(|b|)$ lépésben bebizonyítható.

Megfigyelés: ha $\pi \in P$ akkor $\pi \in NP$ és $\pi \in co - NP$ egyaránt igaz. Azaz $\pi \in NP \cap co - NP$.
Sejtés: ha $\pi \in NP \cap co - NP$ akkor $\pi \in P$ is igaz.



Visszavezethetőség: Van két döntési probléma, π és π' és π-re létezik egy A algoritmusunk. Elképzelhető, hogy π'-re tudunk olyan A' algoritmust konstruálni, ami felhasználja az A algoritmust, azaz A' felírja A egy bemenetét, és meghívja A-t. Ha a meghívást egy lépésnek számítva A' polinomiális, akkor π' (polinomiálisan) visszavezethető π-re.
Megfigyelés: ha π'' polinomiálisan visszavezethető π'-re, és π' pedig π-re, akkor π'' is polinomiálisan visszavezethető π-re.
Bizonyítás: *tudjuk, hogy π'-re létezik A' algoritmus, ami meghív egy π-hez tartozó A algoritmust, és ezen kívül polinomiális lépést végez. Világos, hogy A' meghívásán kívüli lépések száma legfeljebb polinomja |b''|-nek. Ezért A' hívásakor konstruált |b'| bemenet szintén polinomja lesz |b''|-nek.*

Azokat a lépéseket, amik nem A hívásából adódnak, szintén be kell számítanunk. Ezen lépések száma |b'| polinomja. |b'| polinomja azonban |b''|-nek is polinomja.

Állítás: ha $\pi \in P$ és π' polinomiálisan visszavezethető π-re akkor $\pi' \in P$.
Bizonyítás: *π'-t polinomiálasn visszavezetve π-re, és ezt megoldva, a lépések száma továbbra is polinomiális marad.*

NP-nehéz: π probléma NP-nehéz, ha bármely NP beli π' probléma polinomiálisan visszavezethető π-re.
NP-teljes: π probléma NP-teljes, ha π NP-nehéz, és $\pi \in NP$.

Sejtés: $P \neq NP$

Cook-Levin: a SAT probléma NP-teljes.
Következtetés: ha sikerül egy NP-beli problémára visszavezetni SAT-ot (vagy egy már korábban SAT segítségével NP-teljesnek nyilvánított problémát), akkor az adott probléma is NP-teljes. Tehát ha bármely NP-teljes problémára sikerülni polinomiális megoldást találnunk, akkor az összes NP-beli probléma megoldhatóvá válna polinom időben – nem túl valószínű ☺.

HAM probléma: inputja egy gráf, és a válasz igen, ha létezik Hamilton-út a gráfban. Korábban már példaként megmutattuk, hogy **NP-beli**. **NP-teljes**, mert 3-SAT probléma polinomiálisan visszavezethető rá.

3-SZÍN probléma: bemenete egy G gráf, és a válasz igen, ha G 3-színezhető. **NP-beli**, mert az igen válasz polinom időben bebizonyítható: egyszerűen megadjuk G egy 3-színezését. **NP-teljes**: 3-SAT probléma visszavezethető rá.

k-SZÍN probléma: bemenete egy G gráf, és a válasz igen, ha G k-színezhető. Ha k>3, akkor **NP-beli**, mert az igen válasz polinom időben bebizonyítható: egyszerűen megadjuk G egy k-színezését. **NP-teljes**: 3-SZÍN probléma visszavezethető rá.
Bizonyítás: *legyen G 3-SZÍN probléma bemenete. Vegyünk k-3 új pontot G-hez, és kössük össze azokat G minden pontjával és egymással. Ezáltal kapjuk G' gráfot. Ha G 3 színezhető, akkor G' k-színezhető, mert G' új pontjai kaphatnak új színeket. Ha pedig G' k-színezhető, akkor az új pontok páronként különböző színt kapnak, és ezek G-re használt színektől is különbözőek. Mivel G' konstrukciója, G ismeretében polinomiálisan megtehető, így 3-SZÍN probléma polinomiálisan visszavezethető k-SZÍN problémára.*

MAXFTN probléma: bemenete egy G gráf, és k szám, és a válasz annak függvénye, hogy G-ben van-e k független csúcs. A probléma **NP-beli** – ha mutatunk k független csúcsot, akkor polinom időben bebizonyítható, hogy igen a válasz. **NP-teljes**, mert 3-SZÍN probléma visszavezethető rá.

MAXKLIKK probléma: bemenete egy G gráf, és k szám, és a válasz annak függvénye, hogy G-ben van-e k méretű klikk. A probléma **NP-beli** – egy k méretű klikk megadása után polinom időben bizonyítható, hogy az adott pontok G-ben klikket alkotnak. **NP-teljes**, mert MAXFTN probléma visszavezethető rá.

HAMÚT probléma: bemenete G gráf, és a válasz megmondja, hogy van-e G-ben Hamilton-út. **NP-beli**, mivel ha adott egy Hamilton-út, akkor arról polinom időben bebizonyítható, hogy valóban Hamilton-utat adtunk-e meg. **NP-teljes**, mert HAM probléma polinomiális időben visszavezethető rá.

16. Oszthatóság, legnagyobb közös osztó, legkisebb közös többszörös, euklideszi algoritmus, prímek és felbonthatatlan számok, a számelmélet alaptétele, osztók száma, nevezetes tételek prímszámokról: prímek száma, prímek közti hézag mérete és a prímszámtétel (biz. nélkül).

Definíció: a és b számokról azt mondjuk, hogy a osztja b-t, vagy b az a többszöröse (a|b), ha b=aq valamely q egész számra.
Triviális osztó: $n \neq 0$, esetén $\pm 1, \pm n$|n az n triviális osztói.
Valódi osztó: az n nemtriviális osztói.

Maradékos osztás: b szám felírható úgy, hogy $b = a * \left\lfloor \frac{b}{a} \right\rfloor + m, 0 \leq \frac{b}{a} - \left\lfloor \frac{b}{a} \right\rfloor < 1, és\ 0 \leq m < b$ maradék adódik.
Pl.: 111 9-es osztási maradéka 3.

Felbonthatatlan szám: $p \in Z$ szám felbonthatatlan, ha csak triviális osztói vannak, és $|p| \neq 1$.
Pl.: 2, 11

Állítás: bármely z szám előáll felbonthatatlan számok szorzataként, ha |z|>1.
Bizonyítás: *|z| szerinti teljes indukció. |z|=2 felbonthatatlan, és egytényezős szorzatként megfelel önmaga. TFH. k-ig már bizonyítottuk. Legyen |z|=k+1, ha z felbonthatatlan, akkor önmaga megfelel, ha nem felbonthatatlan z felbomlik z=ab alakra, ahol* $1 < |a| \leq k$ *és* $1 < |b| \leq k$*. Az indukciós feltevés miatt az állítás igaz a-ra és b-re, ezért szorzatukra is igaz.*

A számelmélet alaptétele: ha egy z egész számra |z|>1, akkor z előáll felbonthatatlan egész számok szorzataként, és az ilyen előállítások csak a tényezők sorrendjében és előjeleiben különböznek.
Pl.: $-24 = 2 * 3 * (-2) * 2 = (-3) * (-2) * (-2) * 2$

Kanonikus alak: $1 < n \in N$ szám kanonikus alakja $n = p_1^{\alpha_1} * p_2^{\alpha_2} * \ldots * p_n^{\alpha_n}$, ahol a p-k különböző (pozitív) felbonthatatlanok, α-k pedig pozitív egészek.

Prím: egy $p \in Z$ szám akkor prím, ha |p|>1, és csak úgy tud osztani egy szorzatot, ha a szorzat valamelyik tényezőjét osztja – p|ab akkor p|a, vagy p|b.
Számelmélet alaptételének következménye: a prím és a felbonthatatlan ugyanazokat számokat jelöli.

Állítás: egy d szám pontosan akkor osztója az $n \in N$ számnak, ha d kanonikus alakjában pontosan ugyan azok a számok szerepelnek, mint n kanonikus alakjában, és minden ilyen prím kitevője d-ben legfeljebb akkora, mint n-ben.

Következmény: legyen $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ az n kanonikus alakja. Az n pozitív osztóinak száma $d(n) = \prod_{i=1}^{k} (\alpha_i + 1)$.

Legyen $a, b \in Z$ olyan, hogy $a \neq 0$ és $b \neq 0$, és $a = p_1^{\alpha_1} * p_2^{\alpha_2} * \ldots * p_n^{\alpha_n}$ és $b = p_1^{\beta_1} * p_2^{\beta_2} * p_n^{\beta_1}$

Legnagyobb közös osztó: (a,b) az a legnagyobb szám, ami a-nak és b-nek is osztója.
$(a, b) = p_1^{\min(\alpha_1, \beta_1)} * p_2^{\min(\alpha_2, \beta_2)} * p_n^{\min(\alpha_n, \beta_1)}$ – azaz a közös prímek, a legkisebb hatványon.

Relatív prím: a és b relatív prímek, ha (a,b)=1

Legkisebb közös többszörös: [a,b] az a legkisebb $n \in N$ szám, amire a|n és b|n.
$[a, b] = p_1^{\max(\alpha_1, \beta_1)} * p_2^{\max(\alpha_2, \beta_2)} * \ldots * p_n^{\max(\alpha_n, \beta_1)}$ – azaz az összes prím. a legnagyobb hatványon.

Euklideszi algoritmus:
Input: a és b egészek (mondjuk $b \leq a$)
Output: (a,b)
Működés: Legyen $a_0 \coloneqq a$, $a_1 \coloneqq b$. Ha már meghatároztuk $a_0 \geq a_1 \geq \cdots \geq a_i$ számokat, akkor legyen $a_{i-1} = q_i a_i + a_{i+1}$, azaz osszuk el maradékosan a_{i-1}-t a_i-vel, és legyen a_{i+1} a maradék. Az eljárás addig megy, amíg $a_{i+1} \neq 0$, ekkor$(\mathrm{a}, \mathrm{b}) = a_k$.

Tétel: a prímszámok száma végtelen.
Bizonyítás: *Mivel n! az 1,2…n számok mindegyikével osztható, így N:=n!+1 relatív prím ezen számok mindegyikéhez, így N nem osztható az n-nél kisebb prímek egyikével sem.*

Tétel: Tetszőlegesen hosszú sorozat képezhető szomszédos összetett számokból, azaz bármely $n \in \mathbb{N}$-re létezik olyan N, amire az N+1, N+2,…,N+n számok mindegyike összetett.
Bizonyítás: *legyen* $N \coloneqq (n+1)! + 1$*, ekkor tetszőleges* $2 \leq k \leq n+1$ *esetén k|(n+1)!+k=N+(k-1), tehát a számok mindegyike összetett.*

Csebisev tétel: Tetszőleges n pozitív egészre létezik p prím, $n < p \leq 2n$.

Dirichlet tétel: Ha a és d relatív prím, az a, a+d, a+2d,… számtani sorozatban végtelen sok prím fordul elő.

Nagy prímszámtétel:

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$$

ahol $\pi(x)$ az x-nél nem nagyobb prímek számát jelöli.

Definíció: a és b ikerprímek, ha prímek, és különbségük 2.

17. Kongruencia fogalma, műveletek kongruenciákkal. Teljes és redukált maradékrendszer, az Euler féle φ-függvény, Euler-Fermat tétel és kis Fermat tétel. Lineáris kongruenciák megoldhatósága és megoldása. Lineáris diofantikus egyenletek megoldása.

Definíció: a, b, m $\in \mathbb{Z}$, 0<m esetén azt mondjuk, hogy a kongruens b modulo m, ha m|a-b
Jelölése: $a \equiv b(mod\ m) \rightarrow a \equiv b(m)$
Pl.: $12 \equiv -3(5)$

Megfigyelés: Az egész számok halmaza modulo m maradékosztályokra partícionálható.
Pl.: mod 5 3-as maradékosztályában vannak a 3, 8, 13, 18 … és-2, -7, -12 …

Két kongruencia **összeadható**, és **összeszorozható**: $a \equiv b(m)$ és $c \equiv d(m)$, akkor $a + c \equiv b + d(m)$, és $ac \equiv bd(m)$.
Ha d|a és d|b, akkor $\frac{a}{d} \equiv \frac{b}{d}(\frac{m}{(m,d)})$, azaz kongruencia osztásakor a modulust is osztjuk, az osztó és a modulus legnagyobb közös osztójával.

Következmények:
1. $a \equiv b(m)$ pontosan akkor teljesül, ha $a + k \equiv b + k(m)$
2. ha d relatív prím az m-hez, akkor $a \equiv b(m)$ kongruencia ekvivalens az $ad \equiv bd(m)$ kongruenciával, tehát kongruencia szorzása csak akkor ekvivalens átalakítás, ha a modulushoz relatív prím számmal szorzunk
3. Ha d>0 rögzített egész, akkor $a \equiv b(m)$ ekvivalens $ad \equiv bd(md)$

Megfigyelés: ha $a \equiv b(m)$, akkor (a,m)=(b,m)
Bizonyítás: *tudjuk, hogy m|a-b, b=a+km valamely k egészre.*
(a,m)=(a+m,m)=(a+2m,m)…=(a+km,m)=(b,m)

TMR: rögzített m>1 esetén az m elemű, $T = \{a_1, a_2, \dots, a_m\}$ halmazt modulo m teljes maradékrendszerének nevezzük, ha minden m szerinti maradékosztályból pontosan egy elemet tartalmaz.
RMR: $R \subset \mathbb{Z}$ halmaz redukált maradékrendszer modulo m, ha minden m-hez relatív prím m szerinti maradékosztályból pontosan egy elemet tartalmaz mérete: $\varphi(m)$
Pl.: TMR modulo m $T = \{0,1,2, \dots, m-1\}$

Euler féle φ-függvény: egy adott egész számhoz a nála kisebb relatív prím pozitív egész számok számát adja meg – RMR mérete.

Megfigyelés: $\varphi(m)$ megegyezik az 1 és m közé eső m-hez relatív prím számok számával.
p prímre $\varphi(p) = p - 1$
p prímre $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$
Ha (a,b)=1, akkor $\varphi(a * b) = \varphi(a) * \varphi(b)$

Euler-Fermat tétel: Ha (a,m)=1, akkor $a^{\varphi(m)} \equiv 1(m)$
Bizonyítás: $R = \{r_1, r_2, \dots, r_{\varphi(m)}\}$ *RMR modulo m.* $aR = \{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$ *is RMR modulo m. Mivel a kongruenciák szorozhatóak* $\prod_i r_i = \prod_i ar_i(m) \rightarrow \prod_i r_i = a^{\varphi(m)} \prod_i r_i(m)$*, mivel* $(m, \prod_i r_i) = 1$*, a modulus változtatása nélkül tudunk osztani:* $a^{\varphi(m)} \equiv 1(m)$

kis Fermat tétel: ha p prím, akkor bármely egészre $a^p \equiv a(p)$.

Lineáris kongruencia: $ax \equiv b(m)$, ahol a és b adott egészek, m pedig adott pozitív egész.

Tétel: $ax \equiv b(m)$ lineáris kongruencia pontosan akkor oldható meg, ha (a,m)|b. A kongruencia megoldáshalmaza (a,m) darab modulo m maradékosztály.

Lehetséges megoldási módok:
1. Euklideszi algoritmust felhasználva
2: ha a modulus elég kicsit, akkor TMR minden elemét behelyettesítve, pontosan azok a maradékosztályok alkotják a megoldáshalmazt, amelyeknek reprezentánsait behelyettesítve teljesül a kongruencia
3: ha ismert m kanonikus alakja, akkor $\varphi(m)$-et kiszámítva, az Euler-Fermat tételt kihasználva tudjuk megoldani a kongruenciát, a leosztás után, amikor is már (a,m)=1 teljesül. Így beszorozhatjuk mindkét oldalt $a^{\varphi(m)-1}$, m-hez relatív prím számmal. $a^{\varphi(m)-1}ax \equiv a^{\varphi(m)-1}b(m)$, azaz megkapjuk a lineáris kongruencia egyértelmű megoldását.
4. az a együttható abszolút értékét csökkentjük egészen 1-ig ekvivalens átalakításokkal.
a, a-t, vagy b-t, vele kongruens számmal helyettesítünk
b, Ha (a,b)>1, akkor osztunk, szükség esetén a modolust is
c, a modulushoz relatív prímmel szorzunk – és a modulushoz nem nyúlunk.

Diofantoszi egyenlet: ax+by=c ahol a, b, c adott egészek, x, y ismeretlen egészek.
Diofantoszi egyenlet megoldható kongruenciák használatával
Pl.:
$7x + 5y = 29$
$7x \equiv 29(5)$ $7 \equiv 2(5)$ miatt:
$2x \equiv 29(5)$ $29 \equiv 4(5)$ miatt:
$2x \equiv 4(5)$ (2,4)=2 miatt:
$x \equiv 2(5)$
Ekkor x=5k+2
visszahelyettesítve: $y = \frac{29-7*(5k+2)}{5} = \frac{15-35k}{5} \rightarrow y = 3 - 7k$

18. 2-változós művelet, félcsoport, csoport, példák számokon és nem számokon. Csoport rendje, csoportok izomorfiája, részcsoport, generált részcsoport, elem rendje, ciklikus csoport, diédercsoport, Lagrange tétele (biz. nélkül).

Definíció: A H halmazon értelmezett n-változós műveleten egy tetszőleges $f: H^n \to H$ leképezést értünk, azaz minden, H elemeiből képzett rendezett n-eshez H-nak egy bizonyos elemét rendeljük. Pl. itt $(h_1, h_2, \dots, h_n) - hez\ f(h_1, h_2, \dots, h_n)$.
Kétváltozós példa: valós számokon összeadás, szorzás, kivonás.

Cayley táblával is meg lehet adni egy műveletet, ami a szorzótábla általánosítása.
Pl.: ha az alaphalmaz $\{a, b, c, d, e\}$

$\star$	a	b	c	d	e
a	c	c	d	a	b
b	b	a	a	c	e
c	b	d	d	d	d
d	e	e	e	e	c
e	d	e	c	b	a

az adott Cayley tábla szerint pl. $a \star c = d$ és $c \star a = b$

Asszociativitás (átzárójelezhetőség): H halmazon értelmezett 2 változós $\star$ művelet asszociatív, ha tetszőleges $x, y, z \in H$ elemekre teljesül $x \star (y \star z) = (x \star y) \star z$.
Kommutativitás (felcserélhetőség): ha $x \star y = y \star x$
Pl.: 1. valós számokon + művelet asszociatív és kommutatív
2. pozitív számokon a hatványozás nem kommutatív, és nem asszociatív
3. $\mathbb{R} \to \mathbb{R}$ függvények kompozíciója asszociatív, de nem kommutatív
4. valós számokon a számtani közép kommutatív, de nem asszociatív

Félcsoport: $\langle H, \star \rangle$ félcsoport, ha $\star$ a H-n asszociatív
Abel félcsoport: $\langle H, \star \rangle$ Abel félcsoport, ha $\star$ a H-n asszociatív és kommutatív.
Példa: n x n-es mátrixok szorzása félcsoport, n x n-es szimmetrikus mátrixok szorzása e félcsoport Abel részfélcsoportja.

Egységelem: Legyen $\star$ kétváltozós művelet H-n. e a H egységeleme, ha $e \in H$ és $e \star h = h \star e = h$, a H tetszőleges elemére.
Megfigyelés: ha létezik $\langle H, \star \rangle$ algebrai struktúrán egységelem, akkor pontosan egy egységelem létezik.
Bizonyítás: *legyen e és e' egységelem, ekkor* $e = e \star e' = e' \star e = e'$

Inverz: ha $\langle H, \star \rangle$ struktúrán $e \in H$ egységelem, és $h \star h' = h' \star h = e$, akkor h' a h inverze a $\star$ műveletre (fordítva is igaz).
Példa: valós számokon az összeadás egységeleme a 0, és x inverze –x. A szorzás egységelem az 1, és $x \neq 0$ inverze az $\frac{1}{x}$.

Csoport: $\langle G, \star \rangle$ struktúra csoport, ha:
1. félcsoport
2. a $\star$ műveletnek létezik egységeleme
3. minden $g \in G$ elemnek létezik inverze a $\star$ műveletre.
Abel csoport, ha csoport, és csoportművelete kommutatív.

Pl.: $\langle \mathbb{R}, + \rangle, \langle \mathbb{Z}, + \rangle, \langle \mathbb{R} \backslash \{0\}, * \rangle, \langle \mathbb{R}^{n\,x\,k}, + \rangle$, Abel csoportok, ahol $\mathbb{R}^{n\,x\,k}$ $n\,x\,k$ méretű, valós mátrixok halmazát jelöli.
$\mathbb{Z}_n$ halmazon a modulo n szorzás asszociatív, ráadásul az 1 maradékosztály egységelem, de pl. 0 maradékosztálynak nincs inverze, így ez csak egységelemes félcsoport.

A G **csoport rendje** |G|.

Megfigyelés: Ha G csoport, akkor G minden elemének egyértelmű inverze van.
Bizonyítás: *Ha x és y a g inverzei, és e az egységelem, akkor* $x = xe = x(gy) = (xg)y = ey = y$

Definíció:
1. $\langle G, \star \rangle$ és $\langle H, * \rangle$ csoport izomorf, ha létezik $\varphi: G \to H$ művelettartó bijekció, amire $g, g' \in G$ esetén $\varphi(g \star g') = \varphi(g) * \varphi(g')$.
2. A G csoport H részhalmaza a G részcsoportja, ha ($H \leq G$), ha H maga is csoport G műveleteire.

Definíció: Tetszőleges $K \subseteq G$ által **generált $\langle K \rangle$ csoport** a G csoport, K-t tartalmazó részcsoportjainak metszete.

Megfigyelés: Ha G csoport, akkor tetszőleges $K \subset G$ $\langle K \rangle$ a G részcsoportja.

Ciklikus csoport: Az olyan csoportot, amelyet valamely elem generál ciklikus csoportnak szoktuk nevezni.
Elem rendje: a G csoport g elemének rendje a g által generált $\langle g \rangle$ részcsoport elemszáma
Vagy: g elem rendje az a legkisebb szám n, amire $g^n = e$, ha nem létezik ilyen n, akkor végtelen.

Diédercsoport: D_n diédercsoport, X a sík egy szabályos, n oldalú sokszöge, D_n csoport elemei a az X egybevágóságai (azaz a sík mindazon egybevágóságai, amik X sokszöget fixen hagyják), a csoportművelet pedig az egybevágóságok egymás utáni elvégzése.
A diédercsoportnak 2n eleme van.
Pl.: egybevágóság a szimmetria-tengelyre való tükrözés

Definíció: a G csoport H és K részcsoportjainak komplexusszorzatán
$HK := \{hk : h \in H, k \in K\} \subseteq G$ halmazt értjük. Ha $H \leq G$ és $g \in G$, akkor gH (Hg) komplexusszorzat H részcsoport **baloldali (jobboldali) mellékosztálya.** Ha $a \in gH$ ($a \in Hg$), akkor a-t az adott mellékosztály **reprezentáns**ának nevezzük.

Megfigyelés: Legyen $H \leq G \ni g, g'$. Ekkor
1. $g \in Hg$
2. $g' \in Hg \to Hg = Hg'$
3. $Hg = Hg'$ vagy $Hg \cap Hg' = \emptyset$
4. $|H| = |Hg|$

Lagrange tétel: ha $H \leq G$, akkor $|H| \mid |G|$.

Következmény: ha G csoport, akkor bármely $g \in G$ elemének rendje, az egész csoport rendjét osztja.

Következmény: Bármely prím rendű csoport ciklikus csoport.

19. Gyűrűk. 0, 1, ellentett fogalma, 0-val szorzás gyűrűben. Kommutatív, egységelemes gyűrű. Példák gyűrűkre számokon és polinomokkal. Ferdetest, test fogalma, példák.

A $\langle R, \{+,*\}\rangle$ **gyűrű**, ha $\langle R, +\rangle$ Abel csoport és $\langle R,*\rangle$ félcsoport, továbbá teljesülnek a disztributív tulajdonságok - $a(b+c) = ab + ac$, ill $(a+b)c = ac + bc$.
R gyűrű kommutatív, ha a szorzás kommutatív. R gyűrű összeadásának egységelemét nullelemnek nevezzük és 0-val jelöljük. Az R gyűrűben az $a \in R$ elem inverzét az összeadásra –a jelöli. A R gyűrű egységelemes, ha a szorzásnak van egységeleme, amit (ha van) 1 jelöl.

Megfigyelés: ha R gyűrű, és $a, b \in R$, akkor 0a=a0=0 ill. (-a)b=-ab=a(-b)

Példák: 1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ gyűrűk. $\mathbb{N}$ nem gyűrű, mert nem csoport az összeadásra (nincs inverz elem).
2. Egy tetszőleges $n \in N$ szám többszörösei ($n\mathbb{Z}$) is gyűrű.
3. n x n-es mátrixok (racionális, valós vagy komplex) szintén
4. egész együtthatós polinomok is.

Definíció: R gyűrűben az $a \neq 0$ **elem nullosztó**, ha $0 \neq b \in R$, amire ab=0.
R gyűrű **nullosztómentes**, ha nincs benne nullosztó.
R gyűrű **integritási tartomány**, ha kommutatív és nullosztómentes.
Pl.: $n\mathbb{Z}$ nullosztómentes, és kommutatív, ezért integritási tartomány.
$\mathbb{Z}_n$ nem nullosztó mentes, ha n összetett, mert $ab \equiv 0(mod\ n)$ lehetséges. Ha prím, akkor nullosztó mentes, és így integritási tartomány.

Definíció: az R gyűrű részgyűrűje az $\langle R, \{+,*\}\rangle$ olyan résztstruktúrája, ami gyűrű.

Ferdetest: T gyűrű ferdetest, ha $\langle T\backslash\{0\},*\rangle$ csoport.
Test: test, ha ferdetest és a szorzás kommutatív.
Pl.: 1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ testek.
2. Ha p prím, akkor $\mathbb{Z}_p$ test, jelölése $\mathbb{F}_p$.
3. A valós polinomok hányadosteste a következő. $\mathbb{R}(x) \coloneqq \left\{\frac{p}{q} : p, q \in \mathbb{R}[x], q \not\equiv 0\right\}$. A műveletek $\frac{p}{q} + \frac{r}{s} \coloneqq \frac{ps+qr}{qs}$, ill. $\frac{p}{q} * \frac{r}{s} = \frac{pr}{qs}$.

Tétel: minden véges integritási tartomány test.

Definíció: A T test prímtest, ha nincs valódi részteste.
Állítás: $\mathbb{Q}$ *és* $\mathbb{F}_p$(ha p prím) prímtest, és más prímtest nincs.

20. Számelméleti algoritmusok: alapműveletek, (modulo m) hatványozás és az euklideszi algoritmus. Prímtesztelés. Nyilvános kulcsú titkosírások, digitális aláírás. Az RSA titkosítási módszer.

$\boldsymbol{f_A(n)}$ az A algoritmus **legnagyobb lépésszáma** n hosszúságú input esetén.

Egy algoritmus **polinomiális**, ha lépésszáma felülről becsülhető a bemenet méretének polinomjával. Egy algoritmus **exponenciális**, ha a futásideje exponenciális függvénye lehet a bemenet hosszának.

- **Összeadás:** a műveletigény minden helyiértéknél legfeljebb 2, hisz két számot adunk össze az adott helyiértéken, plusz még egy esetleges maradékot az előző helyiértékről. A lépésszámra felső korlát tehát a $2 * \max(\log n, \log m) < 2 * (\log n + \log\ m)$, ami lineáris, vagyis polinomiális. A kivonásra hasonló igaz.

- **Szorzás:** a szokásos írásbeli szorzás működik, és megvalósítható log n db. összeadással, ahol minden összeadandó az m egyjegyű számmal összeszorzott többszöröse. Egy egyjegyű számmal m-et 2 log m db lépésben össze lehet szorozni, ugyanis minden jegyet szorozni kell, és az esetleges maradékot a szorzathoz kell adni. Tehát az össz lépésszám $2(\log n)(\log m) < (\log n + \log m)^2$, vagyis a szorzás polinomiális. Az írásbeli osztás is polinom időben elvégezhető.

- **Hatványozás**: az n^m szám számjegyeinek a száma $k * 2^l$, ahol k és l az n ill. m jegyeinek a száma kettes számrendszerben. Mivel itt a bemenet mérete k+l, ezért a végeredményt még leírni sem tudjuk a bemenet hosszával, tehát a hatványozásra nincs polinomiális algoritmus, tehát exponenciális.

- **Hatványozás modulo m:** az input n, k és m és a cél $n^k(mod\ m)$ meghatározása.
  Legyen $k = \sum_i k_i 2^i$ azaz $k = \cdots k_2 k_1 k_0$ kettes számrendszerbeli alak. Sorra kiszámoljuk a 0 és n – 1 közé eső $n_0, n_1, n_2, \ldots$ számokat, ahol $n_0 \equiv n(m)$, $n_1 \equiv n^2(m), \ldots, n_i \equiv n^{2^i}(m)$. Az n_{i+1}-et az $n_{i+1} \equiv n_i^2(m)$ alapján egy szorzással, és egy maradékos osztással kaphatjuk, ráadásul n_i mérete mindig legfeljebb log m lesz. Tehát egy n_i kiszámítása mindig legfeljebb egy log m méretű szám négyzetre emelését, és egy legfeljebb 2 log m méretű eredmény maradékos osztását igényli. A szükséges n_i-k kiszámításához mindezt log k-szor kell megtenni. Az n^k meghatározását pedig $n^k = \prod_{i=0}^{\infty} n^{k_i 2^i} \equiv \prod_{i=0}^{\infty} {n_i}^{k_i}(m)$ alapján további, legfeljebb log k darab, legfeljebb log m méretű szám szorzásával, és legfeljebb log k darab, legfeljebb 2 log m méretű szám maradékos osztásával kapjuk. Ebből látszik, hogy a modulo m hatványozás polinomiális.

- **Euklideszi algoritmus:** Az euklideszi algoritmus egy lépésében adott $a_i \leq a_{i+1}$ esetén kell egy maradékos osztást elvégezni, és meghatározni azt a $0 \leq a_{i+2} \leq a_{i+1}$-et, melyre $a_i = q_{i+1} * a_{i+1} + a_{i+2}$ áll. Az a_i mérete legfeljebb akkora, mint a_0 és a_1 mérete közül a nagyobbik, tehát az euklideszi algoritmus mindegyik lépése polinomiális időt igényel. A nagy észrevétel, hogy $a_{i+2} \leq \frac{a_i}{2}$, ezért a fentieket legfeljebb $\log a_0$-szor kell elvégezni, amitől az eljárás polinomiális marad.

Euler-Fermat tétel alapján: Ha n prím, akkor $k^{n-1} \equiv 1(n)$ bármely k esetén.
n szám árulója az a k, amire (k,n)=1 és $k^{n-1} \not\equiv 1(n)$, ha van áruló, akkor a számok legalább fele áruló.
leleplező az a k, amire $(k, n) \neq 1$. Nyilván ezekre is igaz, hogy $k^{n-1} \not\equiv 1(n)$
cinkos, ha n összetett, és $k^{n-1} \equiv 1(n)$.

Prímtesztelés: Fermat-teszt – nagy pontossággal (de nem tökéletes bizonyossággal) határozza meg egy számról, hogy prím-e.
Véletlenül választunk egy $0 < k < n$ számot, ha $k^{n-1} \not\equiv 1(n)$, akkor kész vagyunk, n összetett, ha $k^{n-1} \equiv 1(n)$, akkor valószínűsítjük, hogy k prím. A teszt hibázhat, de csak az lehet a hibája, hogy egy összetett számot prímnek mond, fordítva soha. Valamint ha létezik áruló, akkor a hiba lehetősége legfeljebb $\frac{1}{2}$. Ha tehát m-szer választunk, akkor a hiba lehetősége legfeljebb $\frac{1}{2^m}$. Többször megismételt Fermat teszt polinomiális számú, polinom időben elvégezhető lépést használt.

Léteznek olyan számok, ú.n. álprímek, vagy **Charmichael számok**, amelyeknek csak cinkosai és leleplezői (elenyésző számban) vannak. Ezeket a Fermat-teszt majdnem biztosan prímnek találja.

Egyirányú függvény: egyirányú függvénynek nevezünk egy $f: \{1,2,\dots,n\} \to \{1,2,\dots,n\}$ függvényt, mely hatékonyan számolható, de f^{-1} kiszámítása pusztán f ismeretében reménytelen. Elképzelhető, hogy f^{-1} kiszámítására is létezik hatékony eljárás (persze nem pusztán f ismeretében), ezeket hívjuk **kiskapus egyirányú függvényeknek**. Ezekre épül a nyilvános kulcsú titkosírás.

Nyilvános kulcsú titkosírás: rögzítünk egy Σ-val jelölt ABC-t: ennek a jeleivel írjuk le az üzenetet. A kódolandó M üzenetről feltehető, hogy t betűből áll, tehát $M \in \Sigma^t$, hiszen a hosszabb üzeneteket t hosszúságú blokkokra vághatjuk. Feltehetjük, hogy Σ^t szavai 1 és $|\Sigma|^t$ közötti természetes számoknak felelnek meg. A nyilvános kulcsú titkosírási rendszert egy olyan kiskapus egyirányú $f: \{1,2,\dots,n\} \to \{1,2,\dots,n\}$ függvény írja le, melyre $n \geq |\Sigma|^t$. Ezt a leképezést egy nyilvános kulcs segítségével megadjuk, és bárki számára hozzáférhetővé tesszük. Feltételezzük, hogy az A-nak nevezett címzett képes f^{-1} hatékony számítására, mert rendelkezik az azt leíró titkos kulccsal. Ha tehát akarunk A-nak küldeni egy titkosított M üzenetet, akkor elküldjük neki $M' = f(M)$-et, ő pedig hatékonyan ki tudja számítani $f^{-1}(M) = M$-et. Aki lehallgatná ezt az üzenetet, f ismeretében csak arra képes, hogyha sejti, hogy mi az üzenet, akkor ellenőrizni tudja, hogy valóban az-e.
Digitális aláírás: segítségével bizonyítható, hogy az üzenet kitől érkezett. TFH minden szereplőnek van kiskapus egyirányú függvénye, A-é f_A, B-é pedig f_B. Ha B alá akarja írni az A-nak küldött M üzenetet, akkor A-nak az $M' = f_B^{-1}(M)$-et küldi el, ezt A vissza tudja fejteni a nyilvános f_B segítségével: $f_B(M') = f_B(f_B^{-1}(M)) = M$. Ez alapján bizonyítható, hogy az üzenet B-től érkezet, anélkül, hogy B-nek fel kéne fednie a titkos kulcsát.

RSA titkosítási módszer: először választunk két kellően nagy prímszámot, p-t és q-t, elég nagyot ahhoz, hogy $n \coloneqq pq$ ne legyen faktorizálható, valamint $n \geq |\Sigma|^t$ teljesül.
Legyen $m \coloneqq \varphi(n) = (p-1) * (q-1)$, és válasszunk egy $1 \leq e \leq n$ számot úgy, hogy (e,n)=1.
Legyen $f(M) \coloneqq M^e (mod\ n)$. n és e lesz a nyilvános kulcs, ezt közhírré lehet tenni.
p, q és n számok titokban maradnak! A kapott üzenet megfejtéséhez szükség van f^{-1} hatékony számítására. d-re meg kell oldani $ed \equiv 1(m)$ kongruenciát, amit (e,m)=1 miatt hatékonyan és egyértelműen meg lehet tenni. A d meghatározásával megkaptuk az (n,d) titkos kulcsot. Ha kapunk egy $M' = f(M)$ kódolt üzenetet, akkor az inverz leképezés: $f^{-1}(M') = M'^d (mod\ n)$.