„Összefoglaló feleleventéshez, nem kizárólagos tanulási forrás!”

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

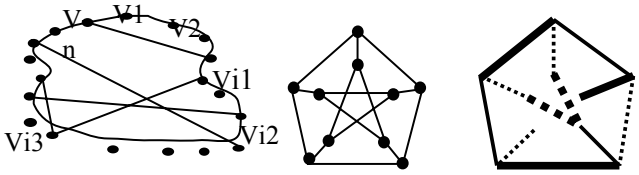
Szükséges feltétel Hamilton-kör létezésére:

Ha a G gráfban létezik k olyan pont, amelyeket elhagyva a gráf több mint k komponensre esik, akkor nem létezik a gráfban Hamilton-kör.

Szükséges feltétel Hamilton-út létezésére:

Ha létezik k olyan pont, amelyeket elhagyva a gráf több mint k+1 komponensre esik, akkor nem létezik a gráfban Hamilton-út sem.

Bizonyítása: Indirekt módon tegyük fel, hogy van a gráfban Hamilton-kör, legyen ez (v_1, v_2, ... v_n) és legyen v_{i1}, v_{i2}, ... , v_{ik} az a k pont, amelyet elhagyva a gráf több mint k komponensre esik. Az elhagyott pontok közötti “ívek” összefüggő komponenseket alkotnak. Pl. a (v_{i1+1}, v_{i1+2}, ... , v_{i2-1}) ív is összefüggő, hiszen két szomszédos pontja között az eredeti Hamilton-kör egy éle fut. Mivel éppen k ilyen ív van, nem lehet több komponens k-nál. (Kevesebb lehet, hiszen különböző ívek között futhatnak élek.) Hamilton-útra hasonlóan bizonyítható.



Szükséges tétel nem elégséges!

Legyen G a Petersen-gráf. Teljesíti a szükséges feltételt: ha elhagyunk n=k+b pontot, (k a külső, b a belső körből) akkor a külső kör legfeljebb k, a belső kör legfeljebb b ívdarabra bomlik. Azaz a G legfeljebb k+b=n komponensre eshet. Ennek ellenére G-ben nincs Hamilton-kör. Ha lenne, az 10 élet jelentene, minden pontba 2 él futna be. “Színezzük ki” a H-kör éleit felváltva vastag és vékony vonalra. Ekkor minden pontból pontosan egy kiinduló él nincs még kiszínezve: fessük vékony szaggatott vonalra. Tehát ha van H-kör, akkor az élek színezhetők 3 színnel, hogy minden pontba 3 különböző színű él fut be. A külső ötszög öt élét lényegileg egyféleképpen lehet 3-színezni (eltekintve a színek permutációjától), 2 vastag, 2 vékony, 1 vékony szaggatott. Ez meghatározza az összekötő élek színét. Viszont ekkor a két vastag szaggatottal jelölt élnek vastagnak kéne lennie, ami ellentmondás.

Dirac és Ore tétele, ezeknek egymáshoz való viszonya

Dirac-tétel: Ha egy n pontú G gráfban minden pont foka legalább n/2, akkor a gráfban létezik Hamilton-kör.

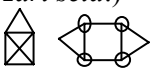
Ore-tétel: Ha az n pontú G gráfban minden olyan x, y $\in$ V(G) pontpára, amelyre $\{x,y\} \notin E(G)$, teljesül az is, hogy $d(x) + d(y) \geq n$, akkor a gráfban van Hamilton-kör. (Ore a szomszédos pontpárok fokszámainak összegéről nem mond semmit!)
Ore-tétel másképpen kimondva: Ha minden u, v pontra igaz, hogy $(u,v) \in E(G)$ VAGY $d(u) + d(v) \geq n \Rightarrow \exists$ Hamilton-kör.

Ore-tételből következik a Dirac-tétel
Biz.: Ha Dirac feltétele teljesül, azaz ha minden pont foka legalább n/2, akkor teljesül Ore feltétele, mivel bármely x, y pontpárra $d(x) + d(y) \geq n$.

2. Euler-körök és -utak, ezek létezésének szükséges és elégséges feltétele

Euler kör:

G gráfban Euler-útnak nevezünk egy olyan összefüggő élsorozatot, ami pontosan egyszer tartalmazza a G összes élét. Ha az élsorozat zárt, akkor Euler-kört kapunk. (az Euler-út nem igazi út a gráfban, mert egy pontot többször is tartalmazhat, hivatalosan *sétának* nevezhetjük, ugyanígy az Euler-kör *zárt séta*.)



Euler kör létezésének szükséges feltétele: Egy összefüggő G gráfban akkor és csak akkor van Euler-kör, ha G minden pontjának fokszáma páros.

Bizonyítás: Szükséges feltétel: triviális (Ha végigmegyünk az Euler-körön minden csúcsba „egyszer bemegyünk, egyszer kijövünk").

Elégséges: G pontszámára való indukcióval. A háromszög a legkisebb pontszámú ilyen gráf, erre igaz. Tegyük fel, hogy minden G-nél kisebb pontszámú gráfra igaz az állítás.

Létezik zárt élsorozat: Induljunk el a gráf egy tetszőleges pontjából, és haladjunk az élek mentén úgy, hogy egy élen kétszer nem megyünk át. Ha olyan pontba érünk, amelyből nem vezet ki olyan él, amelyen még nem haladtunk át, akkor ez csak a kiindulópont lehet, mivel minden pont foka páros. Válaszzuk ki a zárt élsorozatok közül a maximálisat, nevezzük E-nek, ez Euler-kör. Indirekt tegyük fel, hogy E nem egy Euler-köre G-nek. Vizsgáljuk a G' gráfot, amelyet úgy kapunk, hogy a G gráfból elhagyjuk az E-ben szereplő éleket. Ha E nem Euler kör, akkor G' nem csak izolált pontokból áll, hanem vannak benne komponensek, ráadásul ezekben minden fokszám páros (zárt sétát hagytunk el), tehát az indukciós feltevés alapján ezekben biztosan van Euler kör. Ekkor viszont E nem a maximális zárt élsorozat volt: E és a komponens közös pontjából elindulva végigjárhatjuk a komponenst, majd E-t. Vagyis E valóban Euler-kör.

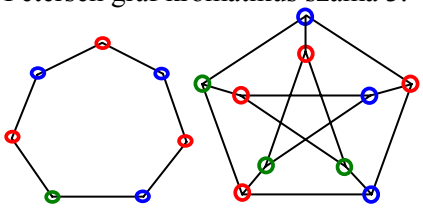
Euler-út létezésének tétele: Egy összefüggő G gráfban akkor és csak akkor van Euler-út, ha a páratlan fokú pontok száma 0 vagy 2.

Bizonyítás: Szükségesség: az előző tételhez hasonlóan bebizonyítható. Elégségesség: 0 páratlan fokú pont: az előző tétel. 2 páratlan fokú pont: kössük össze ezeket egy újabb e éllel. A keletkező G' gráfban minden pont foka páros lesz, így az előző tétel értelmében van benne Euler-kör, ami a definíció szerint tartalmazza az *e* élet is. Hagyjuk el ebből az Euler-körből az e élet, így egy Euler-utat kaptunk G-ben.

3. Gráfok színezése, $\chi(G)$ fogalma, viszonya $\omega(G)$-hez, $\Delta(G)$-hez, Brooks tétele (bizonyítás nélkül) Mycielski konstrukciója.

Egy G hurokmentes gráf **k színnel kiszínezhető**, hogy ha minden csúcsot ki lehet színezni k szín felhasználásával úgy, hogy bármely két szomszédos csúcs színe különböző legyen. G **kromatikus száma** $\chi(G) = k$, ha G k színnel kiszínezhető, de k-1 színnel nem. Egy ilyen színezésnél az azonos színű pontok halmazát **színosztálynak** nevezzük. Hurokél nem lehet, párhuzamos él nem számít, csak egyszerű gráfokat tekintünk. (Végtelen gráfra is értelmes a definíció, k lehet végtelen számosság.)

Példa: K_n kromatikus száma n. Általában $\chi(G) \leq V(G)$. Egy páratlan kör kromatikus száma 3. A Petersen gráf kromatikus száma 3.

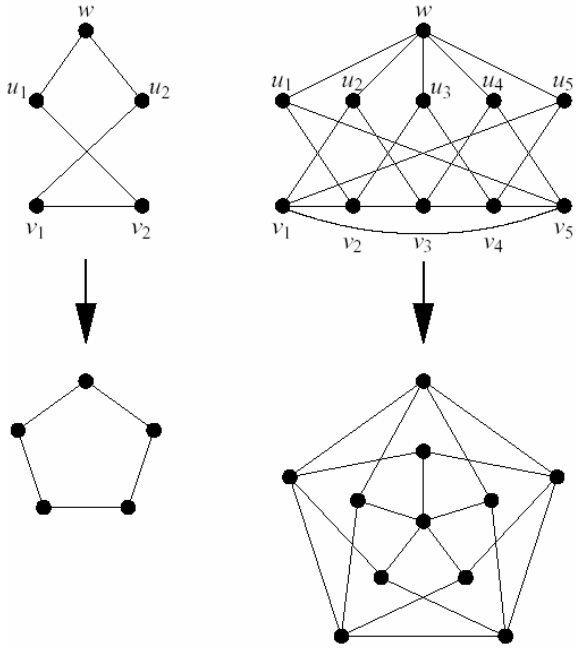


Tétel: Egy legalább egy élet tartalmazó G gráf akkor és csak akkor páros, ha $\chi(G) = 2$.
Bizonyítás: Ha nincs él, akkor $\chi(G) = 1$. Egyébként a két fogalom definíciója lényegében megegyezik: a csúcsokat két halmazra osztjuk, és a halmazokon belül nem futhat él.

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

Alsó becslés a kromatikus számra: Minden G gráfra $\chi(G) \geq \omega(G)$.
Bizonyítás: Értelemszerű, mert a teljes részgráf minden csúcsa különböző színű kell, hogy legyen.

Mycielski konstrukciója: Minden $k \geq 2$ egész számra van olyan G_k gráf, hogy $\omega(G_k) = 2$ és $\chi(G_k) = k$. (azaz az alsó becslésünk nem túl erős ;-P)
Bizonyítás: Teljes indukció: k=2 esetére jó példa a következő gráf: egy él, és két végpontja.
Ha találtunk megfelelő G_k-t, abból a következő módszerrel állíthatunk elő G_{k+1}-et:
G_k pontjai legyenek $v_1..v_n$. A gráfhoz vegyük hozzá $u_1..u_n$ pontokat, és w pontot. w pontot kössük össze az összes u_i ponttal, $\forall$i-re u_i pontot kössük össze v_i szomszédjaival.



(k=3 eredménye az 5 pontú kör, k=4 eredménye a Grötzsch gráf)

Azt kell belátnunk, hogy a művelet során nem keletkezett háromszög, és a kromatikus szám nőtt.

Az u jelű pontok között nem fut él, tehát nem lehet olyan háromszög, melynek mindhárom csúcsa u jelű. w csak u jelű pontokkal van összekötve, tehát az sem lehet háromszög része. u_i, v_j, v_k csúcsok nem

alkothatnak háromszöget, mert ez azt jelentené, hogy v_j és v_k szomszédosak v_i-vel, viszont az volt az indukciós feltevés, hogy $v_1..v_n$ nem tartalmaz háromszöget.

Ha $v_1..v_n$ k színnel színezhető, akkor $u_1..u_n$ színezéséhez is kell k szín. Tegyük fel indirekt, hogy $u_1..u_n$ színezéséhez elég k-nál kevesebb szín: ekkor minden i-re v_i-t színezzünk u_i színére. Mivel i-re v_i és u_i szomszédai azonosak, továbbra is különböző lesz minden szomszédos csúcs színe – $v_1..v_n$ színezéséhez sem volt szükség k színre – ellentmondás.

Ha viszont $u_1..u_n$ színezéséhez k szín kell, w-t k+1 színűre kell színezni. Tehát az átalakítás során a gráf kromatikus száma nőtt.

Felső becslés a kromatikus számra: $\chi(G) \leq \Delta + 1$, ahol Δ a maximális fokszám.

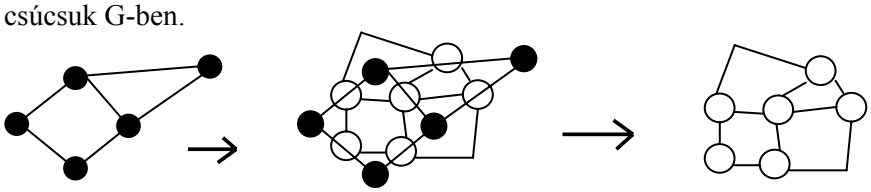
Bizonyítás: A mohó színezés legfeljebb $\Delta + 1$ színnel be tudja színezni a gráfot. Mohó színezéskor tetszőleges sorrendben végigjárjuk a csúcsokat, és a legkisebb sorszámú megengedett színnel színezünk (megengedett: még egyik szomszédját sem színeztük ezzel a színnel). Mivel a legnagyobb fokszám Δ, $\Delta+1$ szín közül egy mindig megengedett lesz.

Teljes gráfok és páratlan hosszú körök esetén valóban szükség van $\Delta+1$ színre, minden egyéb esetben Δ is elég, ezt mondja ki a Brooks tétel.

Brooks-tétel: Ha G egyszerű, összefüggő gráf, nem teljes gráf vagy páratlan hosszúságú kör, akkor $\chi(G) \leq \Delta$, azaz a kromatikus szám nem nagyobb, mint a maximális fokszám.

4. Síkgráfok színezése, ötszíntétel. Élkromatikus szám. Vizing-tétel (bizonyonyítás nélkül)

A G = (V,E) gráf **élgráfja** az L(G) gráf, melyre V(L(G)) = E és $\{e_1,e_2\} \in E(L(G)) \Leftrightarrow e_1 \cap e_2 \neq 0$.
Azaz minden G-beli él egy pont L(G)-ben, és akkor fut él két pont között, ha a megfelelő éleknek van közös csúcsuk G-ben.



Egy G gráf élei k színnel kiszínezhetők, hogyha minden élet ki lehet színezni k szín felhasználásával úgy, hogy bármely két szomszédos él színe különböző legyen. **G élkromatikus száma χ_e(G)** = k, ha G élei k színnel kiszínezhetők, de k-1-el már nem. Az élkromatikus szám az élgráf kromatikus száma.

Vizing-tétel: Ha G egyszerű gráf, akkor $\chi_e(G) \leq \Delta + 1$.

5-szín tétel: Ha G síkbarajzolható gráf, akkor $\chi(G) \leq 5$. (itt csúcsok színezéséről van szó!)

Bizonyítás: Feltehető, hogy G egyszerű, mert a párhuzamos élek nem befolyásolják a színezést, a hurokéleket pedig kizártuk. Teljes indukcióval bizonyítjuk. 2 pontú gráfra triviálisan igaz az állítás.

Lássuk be, ha minden n-1 csúcsú gráfra igaz az állítás, akkor n csúcsúra is igaz.

Minden síkbarajzolható gráfban van olyan v pont, melynek fokszáma legfeljebb 5.

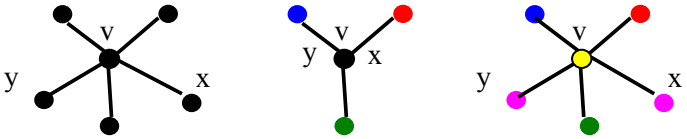
(Ha G egyszerű, pontjainak száma n>2, akkor éleinek száma $e \leq 3n-6$. Ha minden pont foka legalább hat, akkor az élek száma legalább 6n/2 volna, ami ellentmondás.)

v-t elhagyva a gráf 5 színnel színezhető az indukciós feltevés miatt, tehát csak azt kell bizonyítani, hogy v megfelelően színezhető.

Ha v foka legfeljebb 4, akkor a (max.) négy szomszédjától eltérő 5. színnel színezzük ki.

Ha v fokszáma 5, és minden szomszédja között fut él, akkor a gráfban K_6 részgráf szerepel, ami ellentmond G síkba-rajzolhatóságának.

Ha v fokszáma 5 és x, y szomszédjai között nem fut él, akkor G színezhető öt színnel: v,x,y pontokat húzzuk össze egy ponttá [v,x,y] – az így keletkezett G' gráf (az indukciós feltevés miatt) színezhető 5 színnel. G pontjait színezzük ki G' megfelelő pontjainak színére; x és y is megkaphatja a G'-beli [v,x,y] színét, mivel nincsenek összekötve. Ekkor v szomszédjai 4 féle színűek, tehát v színezéséhez elég egy 5. szín.



4-szín tétel: Ha G síkbarajzolható gráf, akkor $\chi(G) \leq 4$. (ennek bizonyítása jóval bonyolultabb.)

5. Perfekt gráfok: erős perfekt gráf tétel, Lovász tétele, intervallumgráfok perfektsége

Erős perfekt gráf tétel

G akkor és csak akkor perfekt, ha G és komplementere nem tartalmaz feszített részgráfként legalább 5 hosszú páratlan kört. (Berge megsejtése 1960-ban. 2002-ben bizonyították)

Szükségesség bizonyítása: Páratlan hosszú kör, az nem perfekt, ha tartalmazna ilyet, akkor biztos, hogy nem lenne perfekt. Be kell látni, hogy egy páratlan hosszú kör komplementere sem perfekt. Belátható, hogy egy ilyen komplementernél ω(G) legalább k. k+1-es klikk pedig biztos, hogy nincs benne, mert ha lenne, az azt jelentené, hogy van legalább 2 csúcs, akik a körben szomszédosak voltak, és most is azok.

Tehát ω(G)=k.

Ha elkezdjük színezgetni a gráfot, egyértelmű, hogy egy színt többször is fel tudunk használni, ugyanis egy tetszőleges csúcs a mellette levő kettővel nem szomszédos. Mind3at azonban nem lehet ugyanazzal a színnel színezni, mert a két szélső szomszédos lesz...húú ehhez lehet kéne egy ábra:) rajzolj kör alakzatban pontokat, csak ne a körívet huzd be hanem a komplementer éleit...talán igy érthetőbb:)

Tehát minden színt legfeljebb kétszer használhatunk fel.

k-színnel színezhető? k szín --> 2k csúcs, de 2k+1 van -->nem

k+1 színnel? k+1 szín --> 2k+2 csúcs, tehát igen.

Ez pedig ellentmondás, mert ω(G) nem egyenlő a kromatikus számmal.

Lovász-tétel: Egy gráf akkor és csak akkor perfekt, ha a komplementere perfekt.

Tétel: Minden véges összehasonlítási gráf perfekt. Az összehasonítási gráf komplementere intervallumgráf.

Tétel: Minden intervallumgráf perfekt.

Szemléletesen: A csúcsok focimeccsek, a színek a pályák. Két csúcs akkor van összekötve, ha időbeni átfedés van. Ha van ω párhuzamos meccs, akkor $\chi \geq \omega$ pályára van szükség. Ha χ pálya nem elég, az azt jelenti, hogy volt olyan időpont, amikor $\omega \geq \chi$ meccs zajlott. Tehát $\chi = \omega$.

Bizonyítás: Mivel egy intervallumgráf feszített részgráfja is intervallumgráf, ezért elég belátni, hogy a klikkszámuk megegyezik a kromatikus számukkal.

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

6. Aciklikus irányított gráfok, PERT módszer

Irányított gráf: az élek irányítva vannak, minden él két végpontja közül pontosan az egyik kiemelt, ebbe mutat az él. **Aciklikus irányított gráf:** nincs benne irányított kör. (Nem létezik olyan v pont, amelyből kilépve az élek mentén visszajuthatunk v-be.)

Ha egy összehasonlítási gráfot irányítottan tekintünk, akkor abban nincs irányított kör. Megfordítva, ha egy irányított körmentes gráfba behúzzuk a tranzitivtásból adódó éleket (képezzük a tranzitív lezártját), akkor összehasonlítási gráfot kapunk.

Forrás: olyan csúcs, amelybe nem megy be él.
Nyelő: olyan csúcs, amelyből nem megy ki él.

Tétel: Akkor és csak akkor aciklikus, ha nem tartalmaz irányított kört

Aciklikus=>Emeletekre bontható: Lemma: Ha nincs benne irányított kör, akkor van benne nyelő (ugyebár elindulsz tetszőleges pontból, és addig mész amíg el nem akadsz -> véges lépésben elakadsz, mert nincs kör, vagyis ott van egy nyelő). Ha van benne nyelő akkor azt levágod és ezt ismételgetve az egész gráfot emeletekre tudod bontani, tehát emeletekre bontható volt.
Emeletekre bontható=>Aciklikus: minden csúcsból csak jobbra vezet él, tehát nem lehet benne kör.

Pert módszer (Program evaluation and review technique):

Az emeletekre bontás fontos alkalmazása az úgynevezett PERT–módszer. Az elnevezés az angol „Program Evaluation and Review Technique” rövidítéséből származik.

Tegyük fel, hogy egy összetett feladatot több alvállalkozóval kell elvégeztetni. Az egyes részfeladatok nem végezhetőek el egymástól függetlenül: pl. egy házépítés során a kőművesmunkák nyilván megelőzik a festési munkákat.

Modell: G gráf élsulyokkal. $V(G)$ =részfeladatok, $(x; y)$ 2 $E(G)$ l súllyal: y részfeladat nem kezdhető el korábban, mint az x kezdése után l idővel. $l = 0$ is lehetséges.

Megkeressük, hogy egy gráffal leírt feladat (ebben a gráfban nincsenek irányított körök) milyen gyorsan oldható meg.

1. Szintezés: emeletekre bontás a nyelőtől indulva. Először a nyelő(k) jobbszélső halmazba, ennek elhagyása után keletkező nyelő(ke)t a jobbról második halmazba és így tovább. (**jobbról balra!**)
2. Ezek után **balról jobbra**, szintenként, meghatározhatjuk minden tevékenység elkezdésének lehetséges legkorábbi időpontját. A bal szélső tevékenység(ek) azonnal (0. időpontban) megkezdhető(ek). Egy y-hoz x_1; x_2;…tevékenységek, melyekre $(x_i; y)$ 2 E(G), legkorábban a t_1; t_2;… időpontban kezdhetőek el, akkor y legkorábban $\max(t_1 + l(x_1; y); t_2+l(x_2; y);…)$ időpontban kezdhető.
3. Kritikus út meghatározása: Megjelöljük (nyelő(k)ből visszafelé) azokat az $(x_i; y)$ éleket, melyeken a maximumok felvétetnek. A G gráf kritikus élei, van legalább egy irányított út a forrásból a nyelőbe csupa kritikus élen. Ezek a kritikus utak: a leghosszabb utak a forrásból a nyelőbe.

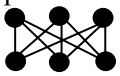
Az ilyen kritikus utakon lévő pontoknak megfelelő részfeladatok bármelyikének késedelmes elvégzése az egész összetett feladat befejezését késleltetné (innét a kritikus út elnevezés). Ha viszont egy pont nincs kritikus úton, akkor a megfelelő feladat késedelmes elvégzése bizonyos határon belül még elfogadható.

A leghosszabb út meghatározása általában nem végezhető el polinom időben. Ebben a speciális esetben azért tudtunk gyors algoritmust adni, mert G-ben nincsenek irányított körök.

7. Páros gráfok. Párosítás és teljes párosítás fogalma, König tétele, Hall tétele, Frobenius tétele. Magyar módszer.

Páros gráfok: Egy G gráfot páros gráfnak nevezünk, ha a G pontjainak V(G) halmaza két részre, egy A és B halmazra osztható úgy, hogy G minden élének egyik végpontja A-ban, másik végpontja B-ben van.

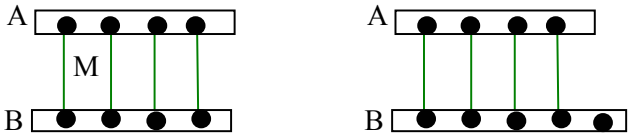
Jele: G = (A,B). A $K_{a,b}$-vel jelölt teljes páros gráfban minden A-beli pont össze van kötve minden B-beli ponttal.



Tétel: Egy G gráf akkor és csak akkor páros gráf, ha minden G-ben lévő kör páros hosszúságú.
Bizonyítás: Ha egy gráf komponensei egyenként páros gráfok, akkor a gráf is páros. Tehát elég összefüggő gráfokra bizonyítani. Ha G páros gráf, és C egy kör G-ben, akkor C pontjai felváltva vannak A-ban és B-ben. Így ez a kör triviálisan páros.

Ha G minden köre páros, akkor a következő módszerrel megadhatjuk A és B halmazt: Válasszunk egy tetszőleges v ∈ V(G) pontot. Ez legyen A első pontja. v szomszédjait tegyük B-be. Ezek után a B-beli pontok szomszédait tegyük A-ba, majd az A-belik szomszédait B-be. Ha az eljárás során két A-beli, vagy két B-beli pontot kell összekötnünk, az ellentmond annak, hogy csak páros körök vannak.

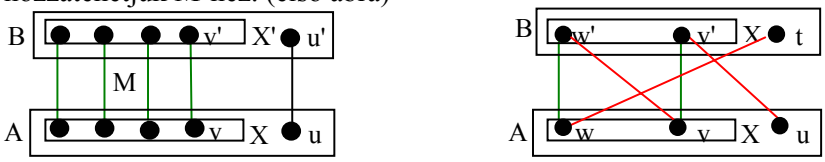
Párosításnak nevezünk egy élhalmazt, ha semelyik két élnek nincs közös pontja. Az ilyen éleket független éleknek is nevezzük (első ábra, a párosítást M-nek jelöljük). A párosítás az élek végpontjait **fedi le**. Egy párosítást **teljes párosítás**nak nevezünk, ha a gráf minden pontját lefedi (mindenkinek van párja), **részlegesnek**, ha csak részüket. **A-t lefedő** párosítás: minden $a \in$ A-nak van párja (második ábra). A párosítás **maximális**, ha az élek száma maximális.



Hall-feltétel: Egy G = (A,B) páros gráfban akkor és csak akkor van A-t lefedő párosítás, ha minden $X \subseteq A$ részhalmazra $|N(X)| \geq |X|$, ahol N(X)-el jelöljük egy X ponthalmaz szomszédainak halmazát.
Bizonyítás:

Szükségesség: Ha van A-t lefedő párosítás, akkor teljesül a feltétel, hiszen ekkor a párosítás élei minden ponthoz egyértelműen hozzárendelnek egy B-beli pontot.

Elégségesség: Tegyük fel, hogy teljesül a Hall feltétel, és lássuk be, hogy ekkor van A-t lefedő párosítás. Legyen M egy tetszőleges, $X \subseteq$ A-t lefedő párosítás. Ennek élszámát fogjuk növelni, és belátjuk, hogy ha |M| már nem növelhető tovább, akkor vagy lefedtük A-t, vagy mégsem teljesül a Hall feltétel.
Minden v ∈ X pont M-beli párját jelöljük v'-vel, X' pedig legyen a B-beli, M által lefedett pontok halmaza.
Legyen u ∈ A-X (azaz még nincs párja)! Ha u-nak van szomszédja a B-X'-ben: u', akkor ezt az új élet hozzátehetjük M-hez. (első ábra)



Alternáló útnak nevezzük egy olyan (páros hosszú) utat, aminek minden második éle M-beli, a többi pedig nem (\/\/\, ahol / mindig M-beli). Ha az út két végpontja u és t (t ∈ B-X') ($^{t}\backslash_{v}/^{v'}\backslash_{v}/^{v'}\backslash_{u}$) akkor |M| nő, ha az eredeti M-beli élek (/) helyett a többi élet (\) vesszük be M-be – az ilyen utat javító útnak nevezzük.
Tegyük fel indirekt, hogy u ∈ A-X nem vehető be M párosításba az előző két módszer egyikével sem.
u X'-beli (csak ilyen lehet, különben működne az első módszer) szomszédjait jelöljük T'-vel. T' X-beli párjait jelöljük T-vel. Ha |N(T)| > |T'|, akkor létezik javító út (*), ha nem, akkor $|N(T)| \leq |T'| < |T+u|$, azaz nem teljesül a Hall feltétel.

* Tfh: |N(T)| > |T'|, ekkor van olyan {x,y} él, hogy x ∈ T és y ∉ T'. Legyen P egy alternáló út u-ból x'-be. P

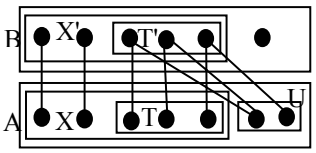
nem mehet át x-en, mert {x',x} nem lehet az alternáló út szélén, ugyanis a párosítás része. Ekkor viszont P folytatható {x',x} és {x,y} élekkel.

Frobenius-tétel: Egy G = (A,B) páros gráfban akkor és csak akkor van teljes párosítás, ha |A| = |B| és |N(X)| ≥ |X| minden X ⊆ A-ra.

Bizonyítás: a két feltétel szükségessége nyilvánvaló. Ha viszont teljesül a második feltétel, akkor a Hall-feltétel miatt van A-t lefedő párosítás. De mivel |A| = |B|, ez lefedi B-t is, tehát a tétel igaz.

König-tétel: Ha G = (A,B) páros gráf: $\nu(G) = \tau(G)$ és (ha nincs G-ben izolált pont) $\alpha(G) = \rho(G)$

Bizonyítás: Először $\nu(G) = \tau(G)$-t bizonyítjuk. Elég $\tau(G) \leq \nu(G)$-t belátni, mert $\tau(G) \geq \nu(G)$ (Ez utóbbi a 8. tételben van benne!).
Legyen M egy olyan párosítás, ami nem növelhető javító úttal. Legyen U = A – X, legyen T' azon B-beli pontok halmaza, amelyek elérhetőek U-ból alternáló úttal. Álljon T a T'-beli pontok párjaiból, T ⊆ X.



T' ∪ (X-T) halmaznak épp |M| pontja van. Ezek minden élet lefognak, hiszen N(T ∪ U) = T'. (Hall-tétel bizonyításához hasonlóan) Ezért: $\tau(G) \leq |M| \leq \nu(G)$, s ebből már következik az állítás.
És ebből következik az is, hogy $\alpha(G) = \rho(G)$ (Gallai két tétele miatt: $\nu(G) + \rho(G) = \tau(G) + \alpha(G)$)

Magyar módszer: könyv 59. oldal

8. Párosítások tetszőleges gráfban, Tutte tétele. Gallai tételei.

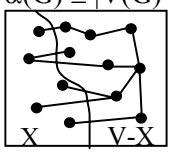
Gallai-azonosságok:
$\nu(G)$: független élek száma (maximális párosítás)
$\rho(G)$: Lefogó élek minimális száma (összes pontot lefedik)
$\alpha(G)$: Független pontok maximális száma (semelyik más ponttal nincs összekötve)
$\tau(G)$: Lefogó pontok minimális száma (összes élt lefogja)

	pontok		élek	
max független	α		ν	
	+	$\tau \geq \nu$; $\rho \geq \alpha$	+	
min lefogó	τ		ρ	
	$=\|V(G)\|$ *Gallai 1.*		$=\|V(G)\|$ *Gallai 2.*	

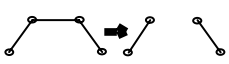
Tétel: $\nu(G) \leq \tau(G)$ minden G gráfra.
Bizonyítás: A maximális méretű független élhalmaz éleinek lefogásához már $\nu(G)$ pontra van szükség, ezért $\tau(G) \geq \nu(G)$.
Tétel: $\alpha(G) \leq \rho(G)$ minden G gráfra.
Bizonyítás: A maximális méretű független ponthalmaz pontjainak lefogásához már $\alpha(G)$ élre van szükség, ezért $\rho(G) \geq \alpha(G)$.

Tutte tétele: Egy tetszőleges gráfban van van teljes párosítás <=> minden x<=V(G) részhalmazra teljesül, hogy ha X-et elhagyjuk a gráfban maradt páratlan komponensek száma <= |X| (ptl komponens: ptl számú csúcsot tartalmazó komponens, továbbiakban Cp).
Csak =>-t az irányt kell bebizonyítani.
Van egy téglalap alakú X halmaz középen, 3-4 krumpli felette a Cp-k ábrázolására, és van 3-4 krumpli alatta a páros komponenseknek.
Meg kell nézni, hogy hol mehet és hol nem mehet él. Két páros között nem mehet, mert akkor egybe tettük volna őket, két páratlan között szintén nem, mert akkor egybetéve őket ráadásul páros komponensünk lenne, egy páratlan és egy páros között szintén nem mehet, mert akkor is egybe tettük volna őket csak a páratlan oldalon.
Szal ahol mehet él, az a párosokból az X-be és Cp-kből az X-be. A különbség a páros és Cp-k között az az, hogy a páros komponensek nem is érdekelnek minket, és hogy a Cp-kből egy párosításbeli él is biztosan megy az X-be, mehet több párosítatlan él is, de azaz egy biztos hogy megy, mert egy páratlan komponensben nem tudunk teljes párosítást csinálni, azt meg az előbb leírtam, hogy Cp-kből csak az X-be mehetnek élek.

1. Gallai-tétel: $\tau(G) + \alpha(G) = |V(G)|$ minden hurokmentes G gráfra.
Bizonyítás: Egy X halmaz pontjai akkor és csak akkor függetlenek, ha a V(G) – X halmaz lefogó ponthalmaz. Hiszen ha X nem lenne független, akkor lenne két összekötött pontja, így V(G) – X nem fogná le azt az élet. $\Rightarrow \tau(G) \leq |V(G) - X|$ minden X független ponthalmazra. $\Rightarrow \tau(G) + \alpha(G) \leq |V(G)|$. Hasonlóan $\alpha(G) \geq |V(G) - Y|$ minden Y lefogó ponthalmazra. $\Rightarrow \tau(G) + \alpha(G) \geq |V(G)|$.



2. Gallai-tétel: $\nu(G) + \rho(G) = V(G)$ minden G gráfra, amelyben nincs izolált pont.
Bizonyítás: Egy $\nu(G)$ elemű X független élhalmaz lefog $2\nu(G)$ számú különböző pontot. A többi pont (mivel nincs köztük izolált) lefogható $V(G) - 2\nu(G)$ éllel. $\Rightarrow \nu(G) + V(G) - 2\nu(G) = V(G) - \nu(G) \geq \rho(G)$.
Tehát $V(G) \geq \rho(G) + \nu(G)$.
Ha Y egy minimális lefogó élhalmaz, akkor Y néhány (mondjuk k darab) diszjunkt csillagból áll, ugyanis ha Y tartalmazna kört, akkor annak bármely élét, ha pedig 3 hosszú utat, akkor annak középső élét el lehetne hagyni, mert a többi él még mindig lefogná az összes pontot. A k csillagnak V(G) – k ága van, így $\rho(G) = V(G) - k$. Vegyünk ki minden csillagból egy élet, a kapott élhalmaz független. Tehát $\nu(G) \geq k = V(G) - \rho(G)$.
$\rho(G) + \nu(G) \geq V(G)$.



9. Hálózati folyamok. Ford-Fulkerson tétel, Edmonds-Karp tétel (bizonyítás nélkül). Egészértékűségi lemma. A folyamprobléma általánosítása.

Legyen G egy irányított gráf, c függvény minden élhez egy nemnegatív valós számot rendel, amit az él kapacitásának nevezünk. Jelöljünk ki továbbá s,t pontokat G-ben, melyeket termelőnek illetve fogyasztónak hívunk. Ekkor a (G, s, t, c) négyest **hálózatnak** hívjuk.

f függvény rendeljen a hálózat minden éléhez egy nemnegatív valós számot. *f* megengedett, ha minden e élre f(e)≤c(e), és minden $v \neq s,t$ pontra $\sum_{\text{befutó élek}} f(e) = \sum_{\text{kifutó élek}} f(e)$ (csomóponti törvény). A megengedett függvényeket **folyamoknak** nevezzük. $\sum_{\text{s-bőkifutó élek}} f(e) = \sum_{\text{t-be befutó élek}} f(e) = \text{a folyam értéke}$

Egy élet **telítettnek** nevezünk egy folyamban, ha f(e)=c(e), és **telítetlennek**, ha f(e)<c(e).
s-t vágás élek (minimális elemszámú) halmaza, melyeket elhagyva G két komponensre esik szét, és *s* és *t* külön komponensbe kerül. A vágás értéke a *t*-t tartalmazó komponens felé mutató élek összkapacitása.

Javító út
Legyen a gráfban $s=v_0, v_1 \ldots v_{k-1}, v_k=t$ egy út, aminek most nem kell feltétlenül az irányítás szerint haladnia. Minden t felé mutató élen x-szel növeljük az átfolyó mennyiséget, a visszafelé mutató éleken pedig ugyanennyivel csökkentsük. x megengedett maximuma ott van, ahol az egyik t felé mutató él telített, vagy az egyik s felé mutató el 0 értékű lesz. Az út minden egyes pontjába befolyó és onnan kifolyó mennyiség egyensúlyban marad, és betartottuk a kapacitáskorlátozást, tehát ez az út megengedett. A t pontba folyó mennyiséget figyelve viszont láthatjuk, hogy a folyam értéke x-szel nőtt.

Tétel: Egy folyam értéke akkor és csak akkor maximális, ha nincs javító út *s*-ből a *t*-be.
Biz.: Legyen P egy javító út. Ekkor P minden t-be mutató élére a $c(e_i)$-$f(e_i)$, az s-be mutatókra pedig az $f(e_i)$ érték szigorúan pozitív. Legyen ezeknek a minimuma *d*. Az első típusú élekre növeljük $f(e_i)$-t *d*-vel, a második típusúaknál pedig csökkentsük $f(e_i)$-t *d*-vel. Ekkor a módosított folyam is megengedett marad, értéke viszont d-vel nőtt.
Tegyük most fel, hogy nincs javító út *s*-ből *t*-be. Lehetnek azonban olyan pontok a gráfban, amelyek elérhetők *s*-ből javító úton (tehát most nem követeljük meg, hogy a javító út elérjen *t*-ig, azaz $v_k=t$ legyen). Legyen az ilyen pontok halmaza $X \subset V(G)$. Ekkor sem az X, sem a V(G)-X nem üres, hiszen $s \in X, t \in V(G) - X$. Tekintsünk egy olyan *e* élet, ami egy X-beli *x* pontból egy nem X-beli *y* pontba mutat. Ekkor f(*e*)=c(*e*), hiszen ellenkező esetben az *s*-ből *x*-be vezető javító út *e*-vel meghosszabbítva egy *s*-ből *y*-ba mutató javító utat szolgáltatna. Ugyanígy egy olyan élre, ami egy nem X-beliből egy X-beli pontba mutat, teljesül, hogy f(*e*)=0. Tehát az X és V(G)-X között futó élek mind telítettek, és a visszafelé mutató éleket nem használjuk, tehát ezen a vágáson nem folyhat át több víz. Vagyis f maximális folyam. És ha létezik f maximális folyam, akkor van ilyen értékű vágás is.

Ford-Fulkerson tétele:
Egy (G, s, t, c) hálózatban a maximális folyamérték egyenlő a minimális vágás értékével.
Bizonyítás: A maximális folyam nyílván nem lehet nagyobb a minimális vágásnál, hiszen ha a vágásban minden előremutató él telített, a visszafelé mutatókon pedig 0 a folyam értéke, akkor ezen a vágáson nem folyhat át több víz. Ugyanakkor a maximális folyam értékével van egyező értékű vágás a hálózatban, lásd a fenti tételt.

Maximális folyam keresése algoritmikusan:
Vegyünk egy kiindulási folyamot (ha nincs ilyenünk, akkor az azonosan nulla folyam használható), keressünk egy javító utat, és e mentén növeljük a folyam értékét.
Hogyan keressük a javító utat, illetve honnan tudjuk, hogy nincs javító út?
Adott G gráfhoz definiálunk egy G_f irányított gráfot, úgy, hogy G minden pontjának megfeleltetünk G_f beli pontot ($V(G_f)=V(G)$). G_f –ben akkor megy él x-ből y pontba, ha G-ben ment olyan folyam x-ből y-ba, ami nem volt maximális ($(x,y) \in E(G)$ és f(x,y)<c(x,y)), vagy ha G-ben ment y-ból x-be nem nulla értékű folyam ($(y,x) \in E(G)$ és f(y,x)>0). Ha a G_f –ben van egy irányított út s-ből a t-be, akkor az ezeknek megfelelő élek G-ben egy javító utat adnak erre a folyamra nézve. (ez azért van, mert a javító útban ugye növelhető „jó” irányú éleknek, és csökkenthető „rossz” irányú éleknek kell lennie, jó-az út, amit vizsgálunk, abban előre felé mutat, a rossz meg hátra felé, tehát az úton a kiindulópont felé)

Megjegyzés: Irányított utat a G –ben BFS (szélességi bejárás) algoritmussal is kereshetünk.

Edmonds-Karp tétel:
Ha mindig a legrövidebb (értsd legkevesebb élből álló) javító utak egyikén javítunk, akkor polinom sok lépésben eljutunk a maximális folyamig. (nem bizonyítjuk) (BFS hál'istennek pont ezt találja meg)

Egészértékűségi Lemma:
Ha a kapacitások egész számok, akkor a maximális folyam értéke is egész szám, és található olyan maximális folyam, amely minden élhez egész számot rendel. Ez az algoritmusból következik.

10. Menger tételei, többszörös összefüggőség, többszörös élösszefüggőség. Dirac tétele (biz. nélkül)

Egy utat lefog egy él, ha az él elhagyásával az út megszakad.

Menger I tétele:
G irányított gráf s és t csúcsa közötti élidegen (azaz ugyanaz az él nem szerepelhet több útban) irányított útjainak max száma egyenlő az összes irányított s->t utat lefogó élek minimális számával.
Bizonyítás: Ha létezik G-ben k darab élfüggetlen irányított s-t út, akkor az s-t utakat lefogó minimális élek száma triviálisan legalább k. Most nézzük ezt az egyenlőtlenséget fordított irányban: lássuk be, hogy ha az s-t utakat lefogó élek minimális száma k, akkor van k élidegen út. Rendeljünk minden élhez 1 kapacitást! Az így kapott hálózatban a minimális vágás értéke k, mivel ennyi él kellett az utak lefogásához. Ekkor azonban a Ford-Fulkerson tétel értelmében a maximális folyam is k értékű. Az egészértékűségi lemma szerint van olyan maximális folyam, amelyben minden él értéke egész, azaz 0 vagy 1. Ezért minden csúcsba pontosan annyi él fut be, mint ahány kiindul belőle; azaz s-ből 1-es élek mentén haladva mindig eljutunk t-be. Elhagyjuk egy ilyen út összes élét, ekkor a folyamérték eggyel csökken, ám az előző tulajdonság nem sérül. Ezt addig folytatjuk, amíg a folyamérték 0-ra csökken: ezzel k darab élfüggetlen utat jelöltünk ki.

Menger II tétele:
G irányított gráf s-t pontjai közötti pontidegen utak max száma egyenlő az összes s->t irányított utat lefogó pontok minimális számával (kivéve az s és t pontokat).
Bizonyítás: Ugyanúgy, mint legutóbb, az most is evidens, hogy ha létezik k db pontidegen út, akkor azok lefogásához legalább k db lefogó pont szükséges. Most lássuk be azt, hogy pont k darabra van szükség. A problémát vezessük vissza az első tételre! Készítsünk egy G' gráfot! Minden pontot húzzunk szét két ponttá: v pont helyett vegyük fel v' és v" pontokat. A befutó élek v'-be fussanak, a kifutók v"-ből induljanak ki, és fusson él v'-ből v"-be. Ha a G gráfban egy minimális ponthalmaz lefogja az irányított s-t utakat, akkor a lefogó pontoknak megfelelő v'-v" élek G'-ben lefogják az irányított s-t utakat. Kevesebb él nem elég a lefogáshoz, ugyanis ha a lefogó élek között lennének (a", b') típusú élek, akkor ezeket helyettesíthetjük (b', b")-vel, ha $b' \neq t$, illetve (a', a")-val, ha b'=t. Így pedig a G-ben egy kisebb lefogó ponthalmazt nyernénk. Vagyis a G-beli lefogó pontok és a G'-beli lefogó élek minimális száma egyenlő.
Megjegyzés: G-beli pontdiszjunkt utaknak G'-beli éldiszjunkt utak felelnek meg, és fordítva.

Menger III tétele:
G irányítatlan gráf s-t pontjai közötti élidegen utak max száma egyenlő az összes s-t utat lefogó irányítatlan élek minimális számával.
Bizonyítás: Visszavezetjük a problémát az irányított gráfos problémára. Készítsünk egy G' gráfot úgy, hogy minden élet két, egy oda és egy vissza mutató irányított éllel helyettesítünk. Az nyilvánvaló, hogy k darab diszjunkt utat nem lehet lefogni k-nál kevesebb éllel, vagyis a maximum nem nagyobb a minimumnál. Tegyük fel, hogy G-ben „k" a diszjunkt utakat lefogó élek minimális száma. G'-ben ennél kevesebb él nem foghatja le az utakat, mert akkor G-ben is le tudná fogni kevesebb él az s-t utakat.
Minden G-beli s-t útnak megfelel egy G'-beli út. Viszont G'-beli két éldiszjunkt útnak megfelelő G-beli utak nem feltétlenül élidegenek. Legyen például az egyik út: f-g_1-h, a másik pedig j-g_2-l, ahol g_1 és g_2 G-ben egy él, itt viszont két egymással ellentétes irányú él. Ekkor kihagyjuk ezt az élet mindkét útból, még pedig úgy, hogy kapunk f-l, és j-h utakat, amik már G-ben tényleg élfüggetlenek lesznek. Így csökkentjük az utakban szereplő élek számát, és véges sok lépés után eljutunk abba az állapotba, amikor már nem fog ilyen helyzet előállni. Ekkor viszont a diszjunkt utak száma G-ben és G'-ben meg fog egyezni. Így visszavezettük a feladatot egy korábbi problémára, hiszen G'-ben már bizonyítottuk, hogy a minimum nem nagyobb a maximumnál, G-ben pedig a lefogó élek száma nem lehet nagyobb, mint G'-ben.

Menger IV tétele:
Egy G irányítatlan gráf s-t közötti irányítatlan pontidegen utak maximális száma megegyezik az összes irányítatlan s-t utat lefogó pontok minimális számával.
Bizonyítás: Ezt az előző tételre vezetjük vissza, csak az irányított élek helyett mindkét irányba húzunk egy irányított élet.

Többszörös összefüggőségek:
Definíció: Egy G gráfot k-szorosan összefüggőnek nevezünk, ha legalább k+1 pontja van, és akárhogy hagyunk el belőle k-nál kevesebb pontot, a maradék gráf összefüggő marad. Jelölése: K(G):= max k, amire G k-szorosan összefüggő

A gráf k-szorosan élösszefüggő, ha akárhogy hagyunk el belőle k-nál kevesebb élet, összefüggő gráfot kapunk. Jelölése: $\lambda(G)$:= max k, amire G k-szorosan élösszefüggő

Megjegyzés: a (pont)összefüggőség erősebb (kisebb), mint az élösszefüggőség.

Állítás: $K(G) \leq \lambda(G) \leq \delta(G)$, ahol $\delta(G)$=minimális fokszám a gráfban

Bizonyítás: Minimális fokú ponthoz csatlakozó éleket elhagyva szétesik a gráf. És ha létezik k db él, amiket elhagyva szétesik a gráf, akkor létezik k db csúcs is így, például úgy, hogy ezen élek egy-egy csúcsát elhagyjuk. Itt baj lehet, ha egy komponenst effektíve megszüntetünk pontjainak elhagyásával, és így csak egy komponens marad. Hogy ezt el lehet kerülni, azt nem bizonyítjuk.

Tétel:
A G gráf akkor és csak akkor k-szorosan pontösszefüggő, ha legalább k+1 pontja van, és bármely két pontja között létezik k pontidegen út. Hasonlóan G akkor és csak akkor k-szorosan élösszefüggő, ha bármely két pontja között létezik k élidegen út.
Bizonyítás: Először a második részt bizonyítjuk. Ha G k-szorosan élösszefüggő, akkor az u-v utakat lefogó élek minimális száma nyilván k. Így Menger tétele értelmében az élidegen u-v utak maximális száma legalább k. Ennek a megfordítása is következik a Menger tételből.
(Tehát ha elhagyunk k-1 élet, akkor még nem szabad a gráfnak szétesnie, tehát kell, hogy legyen benne legalább k élfüggetlen útnak, mert ha kevesebb lenne, és sorban mindegyik élfüggetlen útból elveszünk egy élet, akkor szétesne a gráf, megszűnne u és v között az „összeköttetés")
Ha G k-szorosan pontöszefüggő, akkor k-nál kevesebb pontot elhagyva még összefüggőnek kell maradnia. Tehát bármely két u-v pontot választva legalább k darab u-tól és v-től különböző pontra van szükség, hogy lefogjuk az összes u és v közötti utat (ha ennél kevesebb elég lenne, ezeket elvéve nem maradna több út u és v között, tehát nem lenne k-szorosan pontösszefüggő). Így Menger negyedik tétele értelmében létezik u és v között k pontidegen út.
Ha G bármely két pontja között létezik k pontidegen út, akkor ezeket nyílván nem lehet k-nál kevesebb ponttal lefogni, tehát a k-szoros összefüggőség következik.

Menger tétele az összefüggőségre:
A legalább 3 pontú G gráf akkor és csak akkor 2-szeresen összefüggő, ha tetszőleges két pontján át vezet kör. Igaz az is, hogy akkor és csak akkor 2-szeresen összefüggő, ha bármely két élén át vezet kör.
Bizonyítás: Az első állítás triviálisan igaz, hiszen két pontidegen u-v út egy kört ad, amely átmegy u-n és v-n. A második állítás pedig az elsőből következik. Tehát lássuk be, hogy ha G 2-szeresen összefüggő, akkor az e, f éleken keresztül van kör. Vegyünk fel két pontot úgy, hogy ezekkel osszuk két részre az e illetve az f éleket. Az így kapott gráf is 2-szeresen összefüggő marad (pontösszefüggő). Az első állítás szerint ezen a két ponton át megy kör , és ez a kör az eredeti gráfban átmegy e és f éleken. Tehát a gráf akkor és csak akkor lesz 2-szeresen összefüggő, ha bármely két élén keresztül megy kör.

Dirac tétele:
Ha G k-szorosan összefüggő, akkor bármely k csúcsán keresztül megy kör. (nem bizonyítottuk)

11. Gráfok és mátrixok. Szomszédossági mátrix (hatványaik jelentése, reguláris esetén egy sajátértéke). Illeszkedési mátrix, annak rangja (csak a kisebb vagy egyenlő bizonyításával).

Gráfok tárolása:

1. Szomszédossági mátrix: olyan mátrix, amiben a sorok és az oszlopok is a gráf pontjait fogják jelenteni, az érték az oszlopfejléc pontból a sorfejléc pontba mutató élek száma (0, 1…), irányítatlan esetben elég csak az átló feletti értékeket tárolni. Az átló ennek megfelelően a hurokélek számát jelöli.
   Tul.: -pazarló tárolás, ha sok a nulla, azaz kevés az él
   -előnye az, hogy gyorsan megmondható, hogy megy-e él két pont között
   -v^2 helyet foglal el, ahol v az élek száma
   -v idő felsorolni a szomszédokat
2. Illeszkedési mátrix: A sorok a gráf pontjai, az oszlopok a gráf éleit jelölik. Az érték 1, ha a pont az él végpontja, -1, ha a kezdőpontja, egyébként 0. *ve* helyet foglal. (nagyon lassú)

Könyv: 31.-34. oldal

12. Oszthatóság, felbonthatatlan és prímtulajdonságú számok, ezek kapcsolata, számelmélet alaptétele. Osztók száma és összege. Nevezetes tételek prímszámokról. Dirichlet tétele. Kongruencia fogalma, alapműveletek kongruenciákkal.

a **osztója** *b*-nek, ha létezik olyan *k*, hogy *b=ka* , jelölése: *a|b*.
Prímtulajdonság: p (≠-1,0,1) **prím**, ha $p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$ (ez megengedő VAGY)
p (≠-1,0,1) **fölbonthatatlan**, ha $p = ab \Rightarrow p = \pm a$ vagy $p = \pm b$, azaz vagy a, vagy b az egységelem, ÉS nem teljesülhet közöttük (kizáró VAGY).
A fenti definíciók tetszőleges gyűrűn értelmezhetőek, mi a természetes (nem negatív egész) számok körében foglalkozunk velük.
A természetes számok körében a fölbonthatatlanok megegyeznek a prímekkel. Tehát p prím, ha csak 1 és p osztja. Ilyenkor nincs valódi osztója.

Kapcsolatukra vonatkozó tétel: p akkor és csak akkor prím, ha felbonthatatlan.
Bizonyítás (csak egyik irány): p prím := ab => be kell látnunk, hogy a vagy b egység. Mivel p = ab, ezért p | ab => p | a VAGY p | b (mivel p prím), tehát:
– ha p | a => ab | a => b | 1 => b egység
– ha p | b => ab | b => a | 1 => a egység

Számelmélet alaptétele: Minden pozitív egész n szám egyértelműen bontható fel prímek szorzatára: $n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_k}^{\alpha_k}$, ($\alpha_i > 0$ az egyértelműség miatt), ez a szám **kanonikus** alakja.

Legyen $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\ldots{p_k}^{\alpha_k} = \prod_{i=1}^{k} {p_i}^{\alpha_i}$, az osztók alakja: ${p_1}^{\beta_1}{p_2}^{\beta_2}\ldots{p_k}^{\beta_k}$, ahol a p_i számok ugyanazokat a prímszámokat jelölik, és $0 \le \beta_i \le \alpha_i$. Ekkor:

n osztóinak száma: $d(n) = \prod_{i=1}^{k} (\alpha_i + 1)$, ugyanis $\beta_i \quad \alpha_i + 1$ féle értéket vehet fel.

n osztóinak összege: $\sigma(n) = \prod_{i=1}^{k} \left(1 + p_i + p_i^2 + \ldots + p_i^{\alpha_i + 1}\right) = \prod_{i=1}^{k} \left(\frac{p_i^{\alpha_i + 1} - 1}{p_i - 1} \right)$, a visszaellenőrzéshez gondolatban bontsuk fel az első képletben a zárójeleket, minden tagot minden taggal szorozva épp az összes lehetséges osztó összege jön ki.

az n-nél kisebb, **n-hez relatív prímek száma**: $\varphi(n) = \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$, szita módszerrel, lásd köv tétel.

Nevezetes tételek prímszámokról:
$x \ge 2$ valós számra π(*x*) jelöli az *x*-nél nem nagyobb prímek számát

Tétel: Végtelen sok prímszám van.
Biz.: Tegyük fel, hogy csak véges sok van, ezeket fel lehet sorolni: p_1, p_2, p_3….p_n
Ekkor: egyik prímszám sem lehet osztója a $(p_1p_2p_3\ldots p_n)+1$ számnak (1 maradékot ad), tehát a jobb oldalon álló szám is prím, ami ellentmond a kezdeti állításnak

Csebisev tétele: $\forall n : \exists prím\ n$ és $2n$ között

Ikerprímsejtés: végtelen olyan prím pár létezik, ahol a két prím különbsége 2 (pl: 11, 13).

Bármely N-re van N db szomszédos összetett szám: nézd (N+1)! + 2.... (N+1)! +n + 1-et, ez N darab szám és sorra oszthatóak 2...N+1-el, tehát összetettek.

Π(n) 1-től n-ig a prímszámok száma: $\lim_{n\to\infty} \frac{\pi(x)}{\frac{n}{\ln n}} = 1$, tehát Π(n) = n/(ln n).

Chan(1966):
$\forall n = 2k \quad n>2 \quad n=p_1+p_2p_3$, ahol p_1, p_2, p_3 prímszámok

Euler tétele:
$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+...+\frac{1}{p_i}+...=\sum_{i=1}^{\infty}\frac{1}{p_i}\to\infty$$

Dirichlet tétele: a, b számpár, (a , b) =1 => végtelen a*m+b alakú prím van, magyarul bármely szám bármely maradákosztálya végtelen sok prímet tartalmaz, ha a modulus relatív prím a maradékkal, azaz (m,b)=1.

Definíció: Az *a* és *b* számok relatív prímek , ha (*a*,*b*)=1

Kongruencia fogalma:
a kongruens *b*-vel modulo *c*, ha *a* és *b* *c*-vel vett maradéka ugyanaz. Jelölése $a \equiv b(\mathrm{mod}\, c)$
a≡b(mod c) ⇔ c|(a-b)

13. Lineáris kongruencia megoldása, Wilson tétel

Lineáris kongruencia (mint feladat megoldása):
Feladtat: Oldjuk meg: $ax \equiv b(\mathrm{mod}\, c)$
Állítás: $ax \equiv b(\mathrm{mod}\, c)$ megoldhatóságához szükséges: $(a,c)|b$, és ilyenkor a megoldások száma $d=(a,c)$ darab maradékosztály mod c.
Bizonyítás: Ha x_0 megoldás, akkor $c \mid ax_0 - b \Rightarrow \exists y_0$, amire $ax_0 - cy_0 = b \Rightarrow (a,c) \mid ax_0 - cy_0 \Rightarrow (a,c) \mid b$
Vagyis: ha $(a,c) \nmid b \Rightarrow$ nincs megoldás.

ha $(a,c) = d \mid b \Rightarrow \frac{a}{d}x \equiv \frac{b}{d}\left(\mathrm{mod}\, c\right)$, ahol (mivel d volt a legnagyobb osztó) $\left(\frac{a}{d},\frac{c}{d}\right) = 1$, tehát relatív prímek. Ha a teljes $\mathrm{mod}\frac{c}{d}$ maradékrendszer minden elemét megszorozzuk egy $\frac{c}{d}$-hez relatív prím $\frac{a}{d}$ számmal, akkor is teljes maradékrendszert kapunk. Tehát csak pontosan egy $\frac{c}{d}$ maradékosztály elemeire teljesül a kongruencia. Ha $x \equiv x_0\left(\mathrm{mod}\frac{c}{d}\right)$ megoldása, akkor $x_0, x_0 + \frac{c}{d}, x_0 + 2\frac{c}{d}, \ldots x_0 + (d-1)\frac{c}{d}$, számok által meghatározott d darab maradékrendszer lesz a megoldása az eredeti kongruenciának.

Megoldás keresése:
Ha c kanonikus alakja, és így $\varphi(m)$ ismert, akkor feltéve, hogy $(a,c)=1$, $a^{\varphi(c)} \equiv 1(\mathrm{mod}\, c)$-t felhasználva, a megoldás: $x \equiv ba^{\varphi(c)-1}(\mathrm{mod}\, c)$, hiszen a kongruencia mindkét oldalát a-val szorozva $ax \equiv ba^{\varphi(c)} \equiv b(\mathrm{mod}\, c)$ adódik.

Wilson tétel:
$(n-1)! \equiv$ -1 (mod n), ha n prím
0 (mod n), ha n összetett szám
2 (mod n), ha n=4

Bizonyítás:

1. Ha n összetett szám: n=ab, a,b<n. Ha $a \neq b \Rightarrow a \mid (n-1)!$ és $b \mid (n-1)!$ miatt $ab \mid (n-1)!$ Ilyen felbontás összetett n esetén csak akkor nincs, ha $n=p^2$, ahol p prím.
   Ekkor viszont: $p \mid (n-1)!$ és $2p \mid (n-1)!$, ha $2p<n$. Ebből következik, hogy a szorzatukra is igaz lesz: $2p^2 \mid (n-1)!$ Ha viszont $2p \neq n \Rightarrow n = p^2$, tehát $2p \geq n \Rightarrow n = 4$ (egy ilyen szám van csak, az n=4).
2. Ha n=4, akkor $(n-1)! = 3 \cdot 2 = 6 \equiv 2\left(\mathrm{mod}\, 4\right)$

Ha n prím: $(n-1)! = (p-1)! = (p-1)(p-2)...2 \cdot 1$. Láttuk, hogy $ax \equiv 1(\mathrm{mod}\, c)$ mindig megoldható, ha $(a,c)=1$: $a \in \{1,2,...,p-1\}$ esetén $\exists x \in \{1,2,...,p-1\}$, amire $ax \equiv 1(\mathrm{mod}\, p)$. Tehát a (p-1)! szorzást páronként végezhetjük el, ahol egy pár szorzata 1 mod p. Kik lesznek pár nélkül, kiket mondhatunk pár nélkülinek? Nyílván azokat, akik saját maguk párjai. Ezek: $a^2 \equiv 1(\mathrm{mod}\, p) \Rightarrow a^2 - 1 \equiv 0(\mathrm{mod}\, p)$, tehát $p \mid a^2 - 1 \Leftrightarrow p \mid (a-1)(a+1) \Rightarrow p \mid a-1$ vagy $p \mid a+1$. Akkor viszont: $a \equiv 1(\mathrm{mod}\, p)$, vagy $a \equiv -1(\mathrm{mod}\, p)$. Nincs párja a szorzatban ezek szerint a p+1-nek, és a p-1-nek, az összes többi szorzótényező (pár) 1-et ad. Így végül: $(p-1)! \equiv 1...1...1...1 \cdot 1 \cdot (p-1) \equiv -1(\mathrm{mod}\, p)$ (a sok egyes a párokból jött ki, az utolsó 1-es a (p+1)-ből, (p-1) pedig kongruens -1-gyel modulo p).

14. Euklédeszi algoritmus. Kétismeretlenes, lineáris diofantikus egyenlet megoldása (konkrét példán, ill. eukl alg-al is). Két kongruenciából álló kongruenciarendszer megoldása (konkrét példán).

Euklideszi algoritmus:
Keressük a és b számnak a legnagyobb közös osztóját (legyen $a>b$).
$a=h_1b+m_1$ (h_1 egész szám, $m_1<b$)
$b=h_2m_1+m_2$ (h_2 egész szám, $m_2<m_1$)
$m_1=h_3m_2+m_3$ (h_3 egész szám, $m_3<m_2$)
…
$m_{k-1}=h_{k+1}+m_{k+1}$
$m_k=h_{k+2}m_{k+1}+0$
Ekkor: lnko(a,b)= m_{k+1}
Mert m_{k+1} közös osztó: $m_{k+1} \mid m_k \Rightarrow m_{k+1} \mid m_{k-1} \ldots \; m_{k+1} \mid b$, $m_{k+1} \mid a$, és a legnagyobb is, mert minden közös osztó minden m-et oszt, így az m_{k+1} –et is, viszont az m-ek közül csak m_{k+1} osztója a-nak és b-nek is, tehát ezért lesz a legnagyobb közös osztó.

Könyv: 113.-114. oldal és környéke.

15. tétel: Euler féle φ-függvény, teljes és redukált maradékrendszer, Euler-Fermat tétel, kis Fermat-téttel

Def.: Az *a* és *b* számok relatív prímek , ha (*a*,*b*)=1

Kongruencia fogalma:
a kongruens *b*-vel modulo *c*, ha *a* és *b* *c*-vel vett maradéka ugyanaz. Jelölése $a \equiv b(\mathrm{mod}\, c)$
$a \equiv b(\mathrm{mod}\ c) \Leftrightarrow c|(a-b)$

Teljes és redukált maradékrendszer:
A kongruencia segítségével maradékosztályokba soroljuk az egész számokat. Ugyanabba a maradékosztályba azok a számok fognak tartozni, amik *m*-mel osztva ugyanazt a maradékot adják.

Teljes maradékrendszer:
$\{a_1 a_2 ... a_k\}$ teljes maradékrendszert alkot mod *m*, ha minden mod *m* maradékosztályt pontosan egy a_i képvisel, tehát teljesül:

1. $k=m$
2. $i \neq j \Rightarrow a_i \not\equiv a_j (\mathrm{mod}\, m)$

Ha a mod *m* maradékosztályok mindegyikéből kiválasztunk egy-egy elemet, akkor az így keletkező számhalmazt mod *m* teljes maradékrendszernek nevezzük

Redukált maradékrendszer:
$\{b_1, b_2 ... b_k\}$ redukált maradékrendszer, ha $\forall i$ esetén (b_i, *m*)=1, és az összes ilyen maradékosztályt képviseli pont egy b_i
azaz: 1. $k=\varphi(m)$ Def.: $\varphi(m)$- az *m*-nél kisebb, *m*-hez relatív prím pozitív egészek száma

2. $i \neq j \Rightarrow b_i \not\equiv b_j (\mathrm{mod}\, m)$
3. $\forall i \rightarrow (b_1, m) = 1$

A mod *m* maradékosztályok közül azokból, amelyek minden eleme relatív prím *m*-hez, kiveszünk egy-egy elemet, az így keletkező számhalmazt mod *m* redukált maradékrendszereknek nevezzük

Tétel:
Ha *m* és *a* két relatív prím pozitív egész szám, akkor :
ha $\{a_1, a_2 ... a_m\}$ teljes maradékrendszer *m*-hez, $\{b_1, b_2 ... b_{\varphi(m)}\}$ redukált maradékrendszer *m*-hez, akkor $\{aa_1, aa_2 ... aa_m\}$ is teljes maradékrendszer lesz *m*-hez, és $\{ab_1, ab_2 ... ab_{\varphi(m)}\}$ is redukált maradékrendszer marad *m*-hez.
Bizonyítás teljes maradékrendszerre:

1. $|\{aa_1, aa_2 ... aa_m\}| = m$
2. $aa_i \equiv aa_j (\mathrm{mod}\, m) \Rightarrow m \mid a(a_i - a_j) \xrightarrow{(a,m)=1} m \mid (a_i - a_j)$, akkor $a_i \equiv a_j (\mathrm{mod}\, m) \Rightarrow i = j$, mivel maradékrendszerből indultunk ki

Bizonyítás redukált maradékrendszerre:

1. $|\{ab_1, ab_2 ... ab_{\varphi(m)}\}| = \varphi(m)$
2. $ab_i \equiv ab_j (\mathrm{mod}\, m) \Rightarrow m \mid a(b_i - b_j) \xrightarrow{(a,m)=1} m \mid (b_i - b_j)$, akkor $b_i \equiv b_j (\mathrm{mod}\, m) \Rightarrow i = j$, mivel redukált maradékrendszerből indultunk ki
3. mivel (*a*, *m*)=1, és (b_i, *m*)=1, ezért (ab_i, *m*)=1 is teljesül

φ-függvény, tulajdonságai:
Def.: $\varphi(m)$ az m-nél kisebb, m-hez relatív prím pozitív egészek száma
Neve: Euler féle φ-függvény

Kiszámítása:
Ha $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, akkor $\varphi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$

Ha $n=p$ (prímszám), akkor $\varphi(m)=p-1$
Ha $n=p^{\alpha}$, akkor $\varphi(m)=p^{\alpha}-p^{\alpha-1}$
Biz.: Szita módszer:

$\varphi(n)=n-\left(\frac{n}{p_1}+\frac{n}{p_2}+\frac{n}{p_3}+\ldots+\frac{n}{p_k}\right)$ ekkor kivontuk azokat a számokat n-ből, amik oszthatók voltak a prímtényezőivel, de bizonyos számokat, amik két prímtényezővel voltak oszthatóak, azokat 2-szer vontuk ki, így azokat újra hozzá kell adni az eredményhez:

$\varphi(n)=n-\left(\frac{n}{p_1}+\frac{n}{p_2}+\frac{n}{p_3}+\ldots+\frac{n}{p_k}\right)+\left(\frac{n}{p_1p_2}+\frac{n}{p_1p_3}+\ldots+\frac{n}{p_{k-1}p_k}\right)$ ekkor viszont megint hozzáadtuk kétszer azokat a számokat, amik 3 prímtényezővel oszthatóak, tehát azokat újra ki kell vonni…. Végül:

$\varphi(n)=n-\left(\frac{n}{p_1}+\frac{n}{p_2}+\frac{n}{p_3}+\ldots+\frac{n}{p_k}\right)+\left(\frac{n}{p_1p_2}+\frac{n}{p_1p_3}+\ldots+\frac{n}{p_{k-1}p_k}\right)+\ldots+(-1)^k\left(\frac{n}{p_1\cdots p_k}\right)$

Tehát:

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

Tétel:
Ha $(m,n)=1$, akkor $\varphi(m*n)=\varphi(m)\varphi(n)$ (formulából következik)

Euler-Fermat tétel:
Ha $(a,m)=1$, akkor $a^{\varphi(m)}\equiv 1(\mathrm{mod}\,m)$

Biz.: Legyen $\{c_1,c_2\ldots c_{\varphi(m)}\}$ egy mod m redukált maradékrendszer. Az előbb láttuk, hogy akkor $\{ac_1,ac_2\ldots ac_{\varphi(m)}\}$ számhalmaz is egy mod m redukált maradékrendszer lesz, tehát az ac_1, ac_2, $ac_3\ldots ac_{\varphi(m)}$ szorzatok valamilyen sorrendben kongruensek a c_1, $c_2,\ldots,c_{\varphi(m)}$ számokkal. Így:

$\prod_{i=1}^{\varphi(m)}(ac_i)=\prod_{i=1}^{\varphi(m)}c_i(\mathrm{mod}\,m)$ teljesül, és kiemelhetünk, ekkor:

$a^{\varphi(m)}\prod_{i=1}^{\varphi(m)}c_i=\prod_{i=1}^{\varphi(m)}c_i(\mathrm{mod}\,m)$, ezt átrendezzük: $\left(a^{\varphi(m)}-1\right)\prod_{i=1}^{\varphi(m)}c_i=0\left(\mathrm{mod}\,m\right)$, viszont mivel c_i–k relatív prímek voltak m-hez, ezért csak az $\left(a^{\varphi(m)}-1\right)$ lehet osztható m-mel, akkor pedig: $a^{\varphi(m)}\equiv 1(\mathrm{mod}\,m)$

(kis) Fermat tétel:
Tetszőleges p prímszámra, és tetszőleges a egész számra $a^p\equiv a(\mathrm{mod}\,p)$.

Biz.: Ha $p|a$, akkor $a^p\equiv a\equiv 0\left(\mathrm{mod}\,p\right)$

Ha p nem osztja a-t, akkor az Euler-Fermat tételből:
$a^{\varphi(m)}\equiv 1(\mathrm{mod}\,m)\Rightarrow a^{p-1}\equiv 1\left(\mathrm{mod}\,p\right)\Rightarrow a^p\equiv a\left(\mathrm{mod}\,p\right)$

Fermat-sejtés, Wiles tétel:
Ha $n\geq 3$, akkor $\nexists x,y,z$ egész, amire $x^n+y^n=z^n$.

16. Számelmélet és algoritmusok (alapműveletekm hatványozás az egészek körében és mod m). Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosítás.

Egy aritmetikai művelet bonyolultságán azt értjük, hogy hogyan függ az input hosszától a végrehajtáshoz szükséges idő (az elemi lépések száma). A függvényben nem vesszük figyelembe a konstans különbséget és a konstans szorzót. Például két szám összeadásánál (az általános iskolai algoritmusban) a műveletek száma egyenesen arányos a nagyobbik szám számjegyeinek számával.

Ha az input n szám, és k számrendszerben ábrázoljuk, a számjegyeinek száma, tehát az input hossza $\log_k n$. Mivel más alapú logaritmusra téréskor egy konstanssal szorzunk, az algoritmus bonyolultsága nem függ attól, hogy milyen számrendszerben dolgozunk.

Polinom idejű algoritmusról beszélünk, ha a bonyolultság felülről becsülhető az inputhossz egy polinomjával. Az ilyen algoritmusokat tartjuk elfogadható sebességűeknek. (Pl. 100 méretű inputnál a polinom idő kivárható, az exponenciálishoz viszont kevés egy emberélet.)

Alapműveletek:

Az általános iskolai összeadás és kivonás a számjegyek számával egyenesen arányos, azaz lineáris időben megoldható.

Az ái szorzás ideje számjegyek számával négyzetesen arányos, mivel mindegyik számjegyet mindegyikkel szorozzuk. (van gyorsabb algoritmus is).

Az ái osztás nem igazi algoritmus, mert mindig meg kell sejteni a következő számjegyet – ám ez helyettesíthető az összes számjegy kipróbálásával, így tehát erre is van polinomiális algoritmus.

Legnagyobb közös osztó:

Két szám törzstényezős alakjából (kanonikus alak) gyorsan ki lehet számolni a legnagyobb közös osztót. Ám a prímtényezőkre bontás nem polinomidejű.

Az Euklideszi algoritmussal legnagyobb közös osztót ki lehet számítani polinomidőben. a>b esetén a-t maradékosan osztjuk b-vel, majd b-t osztjuk a maradékkal, majd a maradékot a következő maradékkal.

$a = h_1 b + m_1$
$b = h_2 m_1 + m_2$
$m_1 = h_3 m_2 + m_3$
…

Ezt addig folytatjuk, míg az osztásnak nincs maradéka:

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

Ekkor m_{n-1} osztója m_{n-2}-nek, az egyenleteket alulról fölfelé végignézve láthatjuk, hogy m_{n-1} végül osztója a-nak és b-nek. a és b tetszőleges közös osztója osztja m_1-et is, felülről lefelé haladva láthatjuk, hogy osztja m_{n-1}-et is, tehát ez a legnagyobb közös osztó.

A mod osztás polinomidejű. Ha az egyenletek száma az input hosszának ($\log a$) polimomfüggvénye, akkor az Euklideszi algoritmus is polinomidejű.

Az egyenletekben láthatjuk, hogy $m_{i+2} < m_i/2$, ebből következik, hogy az egyenletek számát $\log a$-val becsülhetjük.

Hatványozás:

A hatványozás nem polinomidejű, mert már az eredmény kiírása sem az (exponenciális).

Az $a^n \pmod m$ hatványozás elvégezhető polinomidőben. Az eredmény 0 és m-1 közé esik, azaz a kiírás ideje konstanssal becsülhető. n kettes számrendszerbeli alakja kiszámítható $\log_2 n$ darab mod osztással. $a^i \pmod m$-ből $a^{2i} \pmod m$ egy szorzással és egy mod osztással kiszámítható. A megfelelő a^{2^x} számok összeszorzása, tehát kitevőbeli ugyancsak polinomidőben megvalósítható.

Prímtesztelés:

Legegyszerűbb módszer, hogy 1-től $\sqrt{n}$-ig minden számra kipróbáljuk, hogy osztó-e. A számításigény nem becsülhető felül $\log n$ polinomfüggvényével.

Eratoszthenész szita-algoritmusával megkaphatjuk az első n prímszámot:

A számokat felírjuk sorban 2-től n-ig. A sorban első szám prímszám, ennek többszöröseit kivesszük a sorból, majd elhagyjuk a prímszámot is. A maradék sor első eleme ugyancsak prímszám, hiszen nem volt nála kisebb prímszám osztója. A módszert addig folyatjuk, amíg el nem fogy a lista.

Ha a szita módszert használjuk n szám prímtesztelésére, a számításigény az input hosszának exponenciális függvénye.

Ezek a módszerek nemcsak azt mondják meg, hogy a szám prím-e, hanem megmondják egy osztóját is, ha összetett.
A következő módszer véletlenszerűen választott próbákkal vizsgálja, hogy a szám prím-e. Ha összetettnek találja a számot, az biztos. Ha nem talál az összetettségre bizonyítékot, akkor csak nagyon nagy az esély arra, hogy prímszám. Az algoritmus polinom idejű, de nem adja meg eredményül egy osztóját a számnak.

Euler-Fermat tétel $t^{\varphi(n)} \equiv 1 \pmod n$, ha n és t relatív prímek. Ha n prím akkor $t^{n-1} \equiv 1 \pmod n$ $t<n$ esetén. Tehát ha $t^{n-1} \equiv 1 \pmod n$ nem igaz tetszőleges $1<t<n$ esetén, akkor biztos, hogy n összetett szám. Ilyenkor a kongruenciát nem kielégítő t-t n árulójának nevezzük. Ha az összefüggés igaz, akkor nem tudtunk meg semmit n összetettségéről; az ilyen t-t n cinkosának nevezzük.
Ha egy számnak van árulója, akkor legalább annyi árulója van, mint cinkosa.
cinkos*cinkos = cinkos // $t_1^{n-1} \equiv 1 \pmod n$; $t_2^{n-1} \equiv 1 \pmod n$; $t_1^{n-1} t_2^{n-1} \equiv 1 \pmod n$
cinkos*áruló = áruló // $t_1^{n-1} \equiv 1 \pmod n$; $t_2^{n-1} \equiv k \pmod n$; $t_1^{n-1} t_2^{n-1} \equiv k \pmod n$

Ha $c_1, c_2, \dots c_n$ a cinkosok sorozata, és *a* áruló, akkor $c_1a, c_2a, \dots c_na$ különböző árulók (a és n rel prímek), tehát legalább annyi áruló van, mint cinkos. Carmichael számnak nevezzük azokat a számokat, melyeknek egy árulója sincs (ezekkel egyelőre ne foglalkozzunk).
Egy véletlenszerűen választott t szám esetén legalább ½ az esély arra hogy árulót találjunk. 100 tesztelés esetén 2^{-100} az esély arra, hogy egy összetett számról ne bizonyosodjon be, hogy nem prím, ami elfogadható.

Tehát az algoritmus: (1) Választunk egy $1<t<n$ számot. (2) Megkeressük n és t lnko-ját, ha nem 1, találtunk egy osztót n-hez (n összetett). (3) Kiszámítjuk t^{n-1} (mod n)-t, ha nem 1, n összetett. Ezt a három lépést q-szor ismételjük. Ha nem bizonyosodott be, hogy n összetett, $1-2^{-q}$ az esély arra, hogy prím.
Az algoritmus q darab lnko keresésből és mod n hatványozásból áll, tehát polinomidejű.
A Carmichael-féle számok leleplezésére a következőképpen módosítjuk a (3) lépést (Rabin-Miller teszt):
n páratlan, ezért $m^{n-1}-1=\left(m^{\frac{n-1}{2}}+1\right)\left(m^{\frac{n-1}{2}}-1\right)$; ha $n-1 = 2^t q$, és q páratlan.

Az $m^{n-1}-1=\left(m^{\frac{n-1}{2}}+1\right)\left(m^{\frac{n-1}{4}}+1\right)\dots\left(m^{\frac{n-1}{2^t}}+1\right)\left(m^{\frac{n-1}{2^t}}-1\right)$ szorzat t+1 tényezőjére kell belátni, hogy egyikük sem osztható n-nel. (Ha n prím, akkor feltétlenül osztja az egyik tényezőt, viszont ha csak Carmichael-szám, akkor igazolható, hogy van olyan m árulója, amelyre n nem osztja egyiket se, csak a szorzatukat, és így minden második m is biztosan Rabin-Miller áruló lesz.)

Így az algoritmusban nem egy, hanem t+1 oszthatóságot kell megvizsgálni, de $t=\log\frac{n-1}{q}<\log n$ miatt ez csak a szükséges időt felülről becslő polinom fokszámát növeli eggyel, az algoritmus továbbra is polinomidejű.

Nyilvános kulcsú titkosírások, bizonyítás információközlés nélkül.

Az alapötlet:

Veszek két nagyon nagy prímszámot, és azokat összeszorzom. Az eredményt nevezzük el lakatnak. Nevezzük el kulcsnak a két osztót. Bárki könnyen leellenőrizheti, hogy a kulcsom valóban nyitja a lakatot (persze innentől neki is lesz kulcsa). Egy másik ember lakatját felbontani két prímszám szorzatára elvileg lehetséges, gyakorlatilag évmilliókba telhet.

Titkosított adatcsere:

A titkosított adatcsere úgy folyhat két fél között, hogy megegyeznek egy kódoló (C) és egy dekódoló (D) függvényben, melyre a következő igaz: D(C(x))=x.

x a közlendő információ, és C(x) „megy át a dróton”. Egy harmadik személy, ha nem ismeri a D függvényt, nem fogja megtudni x-et C(x)-ből.

(Legegyszerűbb példa: a két fél megegyezik egy k számban, majd C és D is a k-val való bitenkénti XOR művelet. Hibái, hogy k-ban előre meg kell egyezni, és D ismeretében C is megtudható)

A nyilvános kulcsú titkosítás lényege, hogy olyan D és C párost kell találni, hogy D ismeretében ne lehessen kitalálni C-t, és fordítva.

Ekkor mindenki közzéteheti a saját C függvényét, D mégis titok marad. Ha valaki ennek a félnek üzenetet akar küldeni, azt elkódolja a nyilvános C-vel, és biztos lehet benne, hogy csak a címzett tudja elolvasni, mert csak ő ismeri a D függvényt, amivel az üzenet dekódolható.
Ha C(D(x))=D(C(x)), akkor a rendszert használhatjuk úgy, hogy a feladót is biztonsággal azonosítsuk:

A küldő az üzenetet előbb elkódolja a saját D függvényével, majd a fogadó C függvényével. A fogadó megkapja az üzenetet, amit csak ő tud visszafejteni, először a saját D függvényét, majd a küldő C függvényét alkalmazva. Ilyenkor biztos lehet, hogy a feltüntetett küldő a valódi küldő, mert ismerte a feltüntetett küldő D függvényét.

RSA titkosítás:

Veszek két nagy prímszámot: p, q.
n:=pq; m:=φ(n)=(p-1)(q-1).
Keresek egy $1 \le e \le m$ számot, melyre lnko(e,m)=1.
d legyen az ed=1 (mod m) kongruencia megoldása.
Ekkor $C(x):=x^e \pmod n$; $D(x):=x^d \pmod n$.
$C(D(x)) = D(C(x)) = x^{ed} = x^{mh+1}=(x^{\varphi(n)})^h x=x \pmod n$
Tehát a C és D függvények jók adatok kódolására/dekódolására.

Ha közzéteszem e-t és n-t, bárki végre tudja hajtani C-t. D végrehajtásához viszont d ismerete is kellene. d előállításához n prímtényezői kellenek, amit én tudok, mások pedig gyakorlatban nem tudják kiszámolni. Tehát a módszer jó nyilvános kulcsú titkosításra.

A függvények csak akkor adnak egyértelmű eredményt, ha x és n relatív prímek. Ezért az elkódolandó x-et ki kell egészíteni néhány megfelelően megválasztott számjeggyel, amit a dekódolás után eldobnak.

A gyakorlati megvalósítás központjai hitelesítő szervezetek, akiknél nyilvános kulcsot lehet regisztrálni. Ezekben a szervezetekben mindegyik félnek meg kell bíznia. Ők tárolják el mindenki személyes C-jét, és ezt bárki megkérdezheti tőlük, mint egy telefonkönyvből.

Az RSA titkosítást nagyon hosszú idő feltörni (56 bitest egy szuperszámítógép 2 év alatt tört meg – 1024 bites az elterjedt), ám maga a kommunikáció is számításigényes. Tehát ahol nem végzetesen fontos a biztonság, RSA adatfolyammal csak egy titkos kulcsot beszélnek meg, és azzal a titkosítással folyik az igazi kommunikáció.

Hitelesítés az RSA kulcsok alapján

(Ezt a módszert senki nem használja, csak szemléltetés.) Hogy tudja egy bank eldönteni, hogy én vagyok-e a bankszámla tulajdonosa? Megkérdezheti a bankszámla tulajdonosának a C függvényét. Majd kitalál egy tetszőleges x számot. Elküldi nekem C(x)-et. Ha ebből elő tudom állítani x-et, akkor tudom a tulajdonos D függvényét – ami elég bizonyíték.

A probléma van: ha a bank ügyes, rá tud venni arra, hogy egy üzenetet, ami nekem szólt, dekódoltasson velem.

Zero knowledge proof

Gyártok egy nagy gráfot (G), melyben van Hamilton kör. Ezt leadom a postafiók kezelőjének, (vagy akár nyilvánossá is tehetem) de azt, hogy hol van a Hamilton kör, csak én tudom. A kezelő a következő hitelesítés után nyithatja ki a postafiókot:

Előállítom G egy izomorfját (G1), és ezt mutatom be bizonyítéknak. A kezelő ekkor rákérdez a következő két kérdés egyikére:

- Mi a megfeleltetés G és G1 között?
- Hol van Hamilton kör G1-ben?

Egy H kör vagy egy izomorfia leellenőrzése gyorsan elvégezhető, viszont H kört vagy izomorfiát keresni belátható időn belül gyakorlatilag lehetetlen.
A kezelő csak mindkét kérdés egyidejű megválaszolása esetén tudná meg, hogy hol van H kör G-ben.

Egy csaló G ismeretében képes előállítani olyan G1 gráfot, hogy vagy az egyik, vagy a másik kérdésre tudjon helyesen válaszolni, de egyszerre mindkettőre nem (mivel a H kört csak én ismerem). Ha a kezelő a hitelesítést 100-szor végzi el a postafiók tényleges kinyitása előtt(100 különböző Gi gráfot hozok), a csalónak csak 2^{-100} esélye van arra, hogy ne bukjon le, ami gyakorlatilag 0.

Mivel a csalónak van esélye arra, hogy hitelesítse magát a H kör ismerete nélkül, a postafiók kezelője könnyen tud sikeres hitelesítési folyamatot szimulálni és rögzíteni, anélkül, hogy ismerné a H kört.

Tehát a hitelesítést a gyakorlatban nem lehet becsapni, viszont egy rögzített hitelesítés nem bizonyítja azt, hogy az valóban megtörtént.

G méretét ügyesen kell megválasztani, hogy gyakorlatilag ne lehessen benne találni H kört (ne legyen benne túl sok), és gyakorlatilag ne lehessen megtalálni a megfeleltetést G és G1 között (ha a második kérdéssel tesztelt a postafiók kezelője).

17. Művelet fogalma, félcsoport, csoport, Abel-csopot. Példák: csoportok számokon, mátrixokon, rajzok szimmetriacsoportja, diédercsoport, szimmetrikus csoport.

Művelet:
f, n-változós függvény n-változós művelet H halmazon, ha H halmaz bármely n darab eleméhez H halmaz egy elemét rendeli. (tehát H zárt f-re nézve)
Egy H halmazon értelmezett 2-változós művelet (jelöljük *-gal) kommutatív, ha $\forall a,b \in H : a*b = b*a$, és asszociatív, ha $\forall a,b,c \in H : (a*b)*c = a*(b*c)$.

Félcsoport:
S halmaz és a rajta értelmezett * (kétváltozós) művelet párost félcsoportnak nevezünk, ha * asszociatív. Ha * kommutatív is, akkor kommutatív, vagy Abel-féle félcsoportnak nevezzük.

Egységelem, inverz:
Ha $\exists e : e*a = a*e = a, \forall a \in H$, akkor e-t egységelemnek, H-t egységelemes félcsoportnak nevezzük.

Az egységelem egyértelmű: tfh: e' és e" is egységelem. Ekkor e'=e'e"=e".

a elem balinverze a^{-1}, ha $a*a^{-1}=e$. (Itt a -1 kitevő csak szimbólum.)

Az inverz egyértelmű: legyen a' és a" is a inverze. Ekkor a'=ea'=(a"a)a'=a"(aa')=a"e=a"

Csoport:
{G, *} csoport, ha * asszociatív (kétváltozós művelet G-n), létezik egységelem, és mindegyik elem inverze is G eleme. Ha * kommutatív is, akkor Abel-féle csoportról beszélünk.
{G, *} csoportot szokták egyszerűen G-vel is jelölni. G csoport rendjén G halmaz elemszámát értjük, jelölése |G|.

Abel-csoport:
Könyv 126.o., 138. o.

Példák:
Félcsoportok: {pozitív számok, +}; {nxn mátrixok, szorzás}; {egész számok, szorzás}…
Csoportok: {nxn invertálható mátrixok, szorzás}, szimmetrikus csoport, diédercsoport…
Ábel csoportok: {egész számok, +}, {rac. számok, szorzás}…

Diédercsoport
n. diédercsoport (D_n): {az n csúcsú szabályos sokszög egybevágósági transzformációi, a transzformációk egymás után végrehajtása (kompozíciója)}. A csoport rendje 2n: n darab tengelyes tükrözés, és n darab elforgatás. Az egységelem a 0-val való elforgatás. A csoport nem kommutatív.

Szimmetrikus csoport, Cayley tétel:
n. szimmetrikus csoport (S_n): {n elem összes permutációja, a permutációk egymás után végrehajtása (kompozíciója)}. A csoport rendje n!, a csoport nem kommutatív.

Pl kompozícióra: $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

(első oszlop: 1->1->2; második oszlop: 2->3->3; harmadik oszlop: 3->2->1)
Cayley tétel: Minden csoport izomorf egy permutációcsoporttal (S_n egy részcsoportjával)

18. Elem rendje, ciklikus csoport. Részcsoportok. Csoportok izomorfiája, Cayley tétele (bizonyítás nélkül).

Elem renje:

Ciklikus csoport

Az egy elem által generált (lásd következő tétel) csoportokat nevezzük ciklikus csoportnak.

a generátuma: <a> az *e, a, a*a, a*a*a* ... és a^{-1}, $a^{-1}*a^{-1}$, ... elemek összessége. Itt is használhatjuk az a^n rövidítést. Az asszociativitás miatt $a^{n+k}=a^n a^k$, és és $(a^n)^k=a^{nk}$, ahol n és k pozitív egész számok. Az asszociativitás miatt $(a^{-1})^n(a)^n=e$, tehát ha $(a^{-1})^n:=a^{-n}$ jelölést használjuk, a hatványazonosságok igazak maradnak negatív kitevők esetén is. ($a^0=e$)

Tehát *a* hatványainak összessége <a>.

Ha létezik olyan $m\neq n$, melyre $a^n=a^m$, akkor $a^{m-n}=e$. *a* rendje a legkisebb ilyen (m-n) szám (pozitív). Ha nem létezik ilyen szám, *a* rendje végtelen.

<a> rendje megegyezik *a* rendjével.

Jelöljük C_n-nel a következő csoportot: {moduló n maradékosztályok, mod n összeadás}. Az egységelem a 0, és 1 generálja a csoportot.

Minden n-ed rendű ciklikus csoport izomorf C_n-nel, ugyanis a^n-hez n-t rendelve művelettartó, bijektív leképezést kapunk. A végtelen rangú ciklikus csoportok izomorfja az {egész számok, összeadás}, ugyanilyen összerendeléssel.

Ezekből következik, hogy minden azonos rangú ciklikus csoport izomorf.

Ciklikus csoport részcsoportja is ciklikus.

Részcsoportok:

Legyen G csoport. $H \subseteq G$ részhalmazt részcsoportnak nevezünk, ha H is csoport ugyanarra a műveletre. Jele: $H \leq G$.

Példa: {egészek, +}≤{racionális, +}≤{valósak, +}; {forgatások, kompozíció}≤D_n

Minden csoport **triviális részcsoportja** önmaga és az egységelem önmagában. A többi részcsoportot (ha van ilyen) **valódi részcsoportnak** nevezzük.

Egy részhalmaz akkor részcsoport, ha benne van az egységelem, minden elemének az inverze és zárt a műveletre ($a,b \in H \Rightarrow a*b \in H$)

Részcsoportok metszete is részcsoport.

Legyen $K \subseteq G$. K által **generált részcsoport** (jele: <K>) az a legszűkebb részcsoport, amely K-t tartalmazza. (Ez a K-t tartalmazó részcsoportok metszete.)

Az egy elem által generált csoportot **ciklikus csoportnak** nevezzük.

Cayley tétel: Minden csoport izomorf egy permutációcsoporttal (S_n egy részcsoportjával)

Izomorfia:

Két csoport izomorf egymással, ha létezik köztük kölcsönösen egyértelmű, művelettartó leképezés. $\{G_1,*\} \cong \{G_2,\bullet\}$ ha $\exists \phi : G_1 \to G_2$ bijekció, melyre $\forall g,h \in G_1 : \phi(g) \bullet \phi(h) = \phi(g*h)$

19. Mellékosztály, Lagrange tétel, elem- és csoport rendjének kapcsolata. Normálosztó, faktorcsoport.

Mellékosztályok:

Legyen K, M részhalmazok G-ben. Ekkor $KM = \{km \mid k \in K, m \in M\}$. (művelet neve: komplexusszorzás)

Legyen $H \leq G$ részcsoport, $g \in G$. Ekkor Hg szorzat H g szerinti jobboldali mellékosztálya, g a mellékosztály reprezentánsa.

$g \in Hg$, mivel $e \in H$

Hg mellékosztály minden eleme reprezentálja Hg mellékosztályt.

Legyen $a \in Hg$, így $\exists h_a \in H : a = h_a g$. Ekkor $\forall h \in H : ha = h(h_a g) = (hh_a)g$, tehát $Ha \subseteq Hg$. Viszont $a = h_a g \Rightarrow h_a^{-1} a = h_a^{-1} h_a g = eg = g \Rightarrow hg = hh_a^{-1} a$, tehát $Hg \subseteq Ha$.

Az előző két állításból következik, hogy két mellékosztály vagy egybeesik, vagy diszjunkt (nincs egyetlen közös eleme sem).

Hg mellékosztály elemszáma megegyezik H elemszámával (ha az véges), mivel

$h_1 g = h_2 g \Leftrightarrow h_1 g g^{-1} = h_2 g g^{-1} \Leftrightarrow h_1 = h_2$

Lagrange tétel:

G véges, H ≤ G, ekkor H rendje osztja G rendjét.

G minden eleme, mely nem eleme H-nak reprezentál egy mellékosztályt. Ezek a mellékosztályok vagy egybeesnek, vagy diszjunktak, és felpartícionálják az egész G-t. Elemszámuk |H|, ezért |G| csak |H| egész számú többszöröse lehet. |G|/|H| számot H indexének nevezzük, és |G:H|-val jelöljük.

Rendek:

Egy elem rendje megegyezik az általa generált részcsoport rendjével, ezért egy elem rendje is osztja a csoport rendjét.

Ha egy csoport rendje prímszám, akkor csak triviális részcsoportjai lehetnek. Ekkor az egységelemen kívül minden elem rendje megegyezik a csoport rendjével. Egy elem generálja a csoportot, tehát ciklikus.

Normálosztó:

Legyen *G* csoport, $N \leq G$. *N* normálosztó *G*-ben ($N \lhd G$), ha *N* jobb és bal oldali mellékosztályai megegyeznek.

($\forall h \in G : hN = Nh$, ám $hn_1 = n_1 h$ <u>nem</u> feltétlenül igaz)

$N \lhd G \Leftrightarrow \forall g \in G : Ng = gN \Leftrightarrow g^{-1}Ng = Ng^{-1}g = Ne = N$

$\Rightarrow \forall n \in N : g^{-1}ng \in N$

$\forall n \in N : g^{-1}ng \in N \Rightarrow \underbrace{g^{-1}Ng \subseteq N \quad gg^{-1}Ngg^{-1} \subseteq gNg^{-1} \Rightarrow N \subseteq gNg^{-1}}_{\Rightarrow g^{-1}Ng = N \Rightarrow N \lhd G}$

Faktorcsoport:

G csoport N normálosztója szerinti faktorcsoportja: {N mellékosztályai, részhalmaz szorzás}, a jele G/N.

$g^{-1}Ng=N$; $NN=N$ ezért $NgNh=Ngg^{-1}Ngh=Ngh$.

N az egységelem: $N(Ng)=(Ng)N=Ng$. Az inverz: $Ng^{-1}Ng=Ne=N$.

|G/N|=|G:N| (a faktorcsoport rendje megegyezik N indexével, ezért |G| osztója)

Abel csoport minden faktorcsoportja kommutatív (Nxy=Nyx). Ciklikus csoport minden faktorcsoportja ciklikus (G=<a> => G/N=<Na>).

20. Gyűrű és test fogalma, példák (Z, Q, R, C, n×n-es mátrixok, polinomok, kvaterniók, Q(√2), p elemű test).

{R, +,*} **gyűrű**, ha + és * az R halmazon értelmezett műveletek, melyekre
a+b=b+a; (a+b)+c=a+(b+c); létezik nullelem, (0): a+0=0+a=a; létezik ellentett (-a): a+(-a)=0;
(a*b)*c=a*(b*c); (a+b)*c=a*c+b*c; c*(a+b)=c*a+c*b;
Ha a szorzás is kommutatív, **kommutatív gyűrűről** beszélünk.
Ha van a szorzásra nézve egységelem (1), **egységelemes gyűrűről** beszélünk.
Az axiómák következményei:

- A nullelem és egységelem egyértelmű.
- 0a=a0=0, mivel a0=a(0+0)=a0+a0 |+(-a0) => 0=a0
- (-a)b=-ab, mivel ab+(-a)b=(a+(-a))b=0b=0
- (-a)(-b)=ab, mivel (-a)(-b)=-a(-b)=--ab=ab

Pl.: Az egész számok a szokásos összeadással és szorzással kommutatív, egységelemes gyűrűt alkotnak (jele: Z). A polinomok gyűrűt alkotnak a polinom-összeadásra és szorzásra nézve. Az adott intervallumon értelmezett és folytonos függvények gyűrűt alkotnak a szorzásra és összeadásra nézve. A mod n maradékosztályok gyűrűt alkotnak (Z_n) a mod n összeadásra és mod n szorzásra, a nullelem 0, az egységelem 1.

Ha $a,b \in R$, $a\neq 0$, $b\neq 0$ és $ab=0$, akkor a baloldali, b jobboldali **nullosztó**. (Pl. a moduló 6 maradékosztályok gyűrűjében 2*3=0)

Nullosztómentes a gyűrű, ha nincs benne nullosztó.
A nullosztómentes kommutatív gyűrűket **integritási tartománynak** nevezzük.

Legyen R gyűrű. $R' \subseteq R$ részhalmaz R **részgyűrűje** ($R' \leq R$), ha gyűrű ugyanazokra a műveletekre nézve. R és {0} **triviális részgyűrűk**, a többit (ha van ilyen) **valódi részgyűrűnek** nevezzük.
R' részgyűrű voltának bizonyításához elég belátni, hogy zárt a műveletekre, tartalmazza a nullelemet, és minden elemnek szerepel az inverze is.

R egységelemes gyűrű **ferdetest**, ha a szorzásra nézve is van inverz (0-t kivéve); **test**, ha ferdetest, és a szorzás is kommutatív.

Minden ferdetest nullosztómentes, hiszen ab=0, a≠0 $\Rightarrow$ $a^{-1}ab= a^{-1}0$ $\Rightarrow$ b=0

Minden véges integritási tartomány test. Ehhez meg kell mutatnunk az egységelem, és az inverz létezését. Legyenek a gyűrű elemei a_1(=0), a_2, … a_n. Legyen $a \in R, a \neq 0$, tekintsük az aa_1, aa_2, … aa_n elemeket. $aa_i=aa_j$ esetén $a(a_i-a_j)=0$, a nullosztómentesség miatt $a_i=a_j$, tehát az aa_i elemek mind különbözőek. Mivel n elem van, felsoroltuk az összes elemet, tehát ae=a-t is. e egységelem, mert
$\forall b \in R : ae = a \Rightarrow bae = ba \xrightarrow{kommutatív} abe = ab$
$\Rightarrow a(be-b) = 0 \xrightarrow{nullosztómentes, a\neq 0} be - b = 0 \Rightarrow b = be$
aa_i elemek között szerepelnie kellett e-nek is, tehát a-nak van inverze.

Pl.: A racionális, valós, komplex számok testet alkotnak a szokásos műveletekre nézve. A Z_n (maradékos)gyűrűk testek, ha n prím. Testet alkotnak a $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ alakú mátrixok a mátrixműveletekre.

Kvaterniók ferdeteste

Kvaterniónak nevezzük az $a+bi+cj+dk$ alakú számokat, ahol a,b,c,d valós számok, $i^2=j^2=k^2=(-1)$; ij=k; jk=i; ki=j; a valóssal való szorzás kommutatív, ám ji=(-k)=(-ij); kj=(-i)=(-jk); ik=(-j)=(-ki)!
Ezek alapján az összeadás és szorzás a komplex számok mintájára folyik.
Konjugált: $\overline{a+bi+cj+dk} = a-bi-cj-dk$.
Norma (hossz): $\left|a+bi+cj+dk\right|^2 = \left(a+bi+cj+dk\right)\left(\overline{a+bi+cj+dk}\right) = a^2+b^2+c^2+d^2$

Reciprok: $\overline{k}/|k|^2$, mert $k \neq 0 : k \cdot \overline{k}/|k|^2 = 1$

Tehát ferdetest. ij≠ji, tehát nem test.
x^2+1 polinomnak végtelen sok megoldása van: az összes bi+cj+dk alakú kvaternió, ahol $b^2+c^2+d^2=1$.
$(\alpha+\beta)^2 \neq \alpha^2+2\alpha\beta+\beta^2$
$\alpha^2+1 \neq (\alpha-i)(\alpha+i)$

Egy, a valós számokat tartalmazó ferdetest mindig izomorf a valós számok, a komplex számok vagy a kvaterniók egyikével (Frobenius).

Könyv 142.-158. o.

Impresszum

I. rész:
A tételsort Molnár Andi (molandi_1@yahoo.de), Vörös András (vorike@hotmail.com) és Szabó Marcell (szabom@jedlik.hu) állította össze.
Köszönet Bergmann Gábornak (maffley.check@aramszu.net) a korrektúráért.
A doksi tartalmáért semmi felelősséget nem vállalunk ;-P

2004. június 3.

II. rész:
A tételsort az idei év tételjegyzékéhez átdolgozta és kiegészítette: Kozma János (kj556@hszk.bme.hu), aki ezúton mond köszönetet a fenti 3 embernek az alapanyagért.
Valamint a tartalomért felelőséget továbbra sem vállalunk, sem azért, hogy néhol csak utalás van a könyvbeli oldal/fejezetszámra. :]

2005. június 14.