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

Euler-kör/út: olyan zárt/nem feltétlenül zárt élsorozat, amely a gráf minden **élét** pontosan egyszer tartalmazza

Hamilton-kör/út: olyan kör/út, amely a gráf minden **pontját** pontosan egyszer tartalmazza.

Szükséges és elégséges feltételek Euler-kör, ill. –út esetén:

Tétel: Összefüggő G gráfban van Euler-kör ⇔ G minden pontjának fokszáma páros.

Biz:
⇨
belátni: ha van benne Euler-kör, akkor minden pont foka páros. Ez világos, hiszen ha az Euler-kör mentén járjuk be a gráfot, akkor minden pontba ugyanannyiszor „mentünk be", mint ahányszor „kimentünk", és ezek száma azonos, összegük pedig a pont fokszáma, ez pedig biztosan páros.
⇦
indukcióval: tegyük fel, hogy minden $k<n$-re igaz, és G egy n pontú gráf. Járjuk be a gráfot úgy, hogy egy élen csak egyszer megyünk át. Ha olyan pontba érünk, ahonnan kifelé már nem vezet „érintetlen" él, akkor az csak a kiindulópontunk lehet, hiszen minden pont foka páros. Ez így egy zárt élsorozat. Legyen H egy olyan zárt élsorozata G-nek, amelyben az előforduló élek száma maximális. Mivel a kiindulópontunkból nem tudtunk továbbmenni, az ebből a pontból kiinduló összes és H-beli. Indirekt tegyük fel, hogy H nem Euler-kör. Nézzük meg G'-t, amit úgy kapunk, hogy G-ből elhagyjuk a H-ban szereplő éleket. G' nem feltétlenül összefüggő, viszont n-nél kevesebb pontja van, hisz a kiindulópont nincs benne. Az indukció miatt minden komponensében van Euler-kör. Mivel G összefüggő, G' valamelyik komponensének van olyan pontja, ami H-ban szerepel. Nevezzük az ebben a komponensben található Euler-kört H'-nek. Tehát, ha elindulunk az előbb talált közös pontból, és először bejárjuk H-t, majd H'-t, akkor egy H élszámánál nagyobb élszámú zárt élsorozatot találunk, ami ellentmond az indukciónak, tehát H Euler-kör.

Tétel: Összefüggő G gráfban van Euler-út ⇔ G-ben a páratlan fokú pontok száma 0, vagy 2.

Biz:
⇨
Az előző tétel bizonyításához hasonlóan belátható, hogy ha G-ben van E-út, akkor a két végpont kivételével minden pont foka páros.

⇦
Felhasználjuk az előző tételt. Ha 0 páratlan fokú pont van, akkor készen vagyunk. Ha 2, akkor ezeket kössük össze egy új e éllel, így minden pont foka páros lesz, tehát G-ben van Euler-kör. Hagyjuk el ebből e-t, így egy Euler-utat kapunk G-ben.

Szükséges feltételek Hamilton-kör, és Hamilton-út létezésére:

Tétel: Ha a G gráfban van k olyan pont, amelyeket elhagyva a gráf több mint k komponensre esik szét, akkor nem létezik a gráfban Hamilton-kör. Ha van k olyan pont, amelyeket elhagyva a gráf több mint $k+1$ komponensre esik szét, akkor nem létezik a gráfban Hamilton út.

Biz:
Tegyük fel, hogy a gráfban van H-kör. Ez k pont elhagyásával éppen k komponensre esik szét, majdhogynem triviális. H-út esetén k pont elhagyása $k+1$ komponenst von maga után.

Tétel (Ore): Ha az n pontú G gráfban minden $x, y \in V(G)$ pontpárra, amelyre $\{x, y\} \notin E(G)$ teljesül az is, hogy $d(x) + d(y) \geq n$, akkor a gráfban van Hamilton-kör.

Biz:
Indirekt módszer. Legyen egy gráfunk, amire a feltétel igaz, de nincs benne Hamilton-kör. Addig vegyünk hozzá éleket, amíg a következő él hozzáadásával már lenne benne Hamilton-kör. Legyen ez a gráf G'. A feltétel továbbra is teljesül. Biztosan van két olyan pont is, hogy $\{x, y\} \notin E(G')$. Ekkor a $G' + \{x, y\}$ van egy Hamilton-kör, tehát G'-ben van Hamilton-út, ez legyen $P = (z_1, z_2, \dots, z_n)$, ahol $z_1 = x$, és $z_n = y$. Ha x szomszédos a P út egyik z_k pontjával, akkor y nem lehet összekötve z_{k-1}-el, mert $(z_1, \dots, z_{k-1}, z_n, z_{n-1}, \dots, z_k, z_1)$ egy Hamilton-kör. Így y nem lehet összekötve $d(x)$ darab ponttal, ezért

$$d(y) \leq n - 1 - d(x)$$

ami viszont ellentmondás, mert $\{x, y\} \notin E(G)$.

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

Biz:
Ez az Ore-tételből következik, hiszen ha minden pont foka legalább $n/2$, akkor teljesül, hogy $d(x) + d(y) \geq n$.

2) Gráfok színezése, kromatikus szám. A kromatikus szám becslései a klikkszám, a maximális fokszám, és a független pontok száma segítségével. Brooks tétele (biz. nélkül). Mycielski konstrukciója.

Színezhetőség: egy G hurokmentes gráf k színnel színezhető, hogyha minden csúcsot ki lehet színezni k szín felhasználásával úgy, hogy bármely két szomszédos pont színe különböző.

Kromatikus szám: $\chi(G) = k$, ha G k színnel színezhető, de k-1 színnel nem.

Színosztály: azonos színű pontok halmaza

Klikk: G egy teljes részgráfját klikknek nevezzük. A G-ben található maximális méretű klikk pontszáma $\omega(G)$, ez a gráf **klikkszáma**.

Tétel: Egy legalább egy élet tartalmazó G gráf páros $\Leftrightarrow \chi(G) = 2$.

Biz:
egyik oldal egyik szín, másik oldal másik szín, egy élnek két végpontja van, tehát szomszédosak, így nem lehetnek azonos színűek, tehát az állítás teljesül.

Alsó becslés a klikkszámmal:
Tétel: Minden G gráfra $\chi(G) \geq \omega(G)$.

Biz:
világos, hiszen egy klikkben minden pont szomszédos minden ponttal, így csak különböző színűek lehetnek, tehát az egész gráfban is legalább ennyi színt felhasználunk.

Tétel (Mycielski konstrukciója): Minden $k \geq 2$ egész számra van olyan G_k gráf, hogy s $\omega(G_k) = 2$, és $\chi(G_k) = k$.

Biz:
Tegyük fel, hogy van már egy G_k gráfunk, amely kielégíti a feltételt. Ebből készítsük el G_{k+1}-et: legyenek G_k pontjai $v_1, v_2, \dots, v_n$. Vegyünk fel $n+1$ új pontot: $u_1, u_2, \dots, u_n$, és w. Kössünk össze minden u_i-t v_i minden G_k-beli szomszédjával, de magával v_i-vel ne. Végül w-t kössük össze minden u_i-val, de v_i-vel ne. Belátjuk, hogy az így kapott G_{k+1} kielégíti a feltételeket.
Ha G_k-ban nem volt háromszög, akkor G_{k+1}-ben sincs, azaz $\omega(G_{k+1}) = 2$. Indirekt tegyük fel, hogy mégis van háromszög G_{k+1}-ben. Ennek nyilván nem lehet mindhárom csúcsa G_k-ban, hiszen ekkor G_k-ban lenne a háromszög, ami ellentmond a feltevésünknek. Ha w a háromszög egyik csúcsa, akkor a másik kettő csak u_i és u_j lehet, ezek viszont nem szomszédosak. Végül, ha u_i a háromszög egyik csúcsa, akkor a másik kettő csak v_x és v_y lehet, ekkor azonban (mivel u_i és v_i szomszédjai azonosak) v_i, v_x és v_y is háromszöget alkotnának G_k-ban, ami megintcsak ellentmondás.
Az is nyilvánvaló, hogy $\chi(G_{k+1}) \leq k + 1$, hiszen a v_i pontok G_k egy jó színezése szerint k színnel színezhetők, ezután minden u_i megkapja v_i színét, végül w a $k+1$-edik színt. Így G_{k+1}-et jól kiszíneztük $k+1$ színnel.

Felső becslés a maximális fokszámmal:
Tétel: $\chi(G) \leq \Delta + 1$.

Biz:
mohó színezéssel. Kezdjük el tetszőleges sorrendben színezni a pontokat. Amikor egy újabb pontot színeznénk, akkor annak legfeljebb Δ szomszédja van kiszínezve, így a $\Delta + 1$-edik színt felhasználhatjuk a pont színezésére.

Tétel (Brooks): Ha G egyszerű, nem reguláris, összefüggő gráf, nem teljes gráf, és nem egy páratlan hosszú kör, akkor $\chi(G) \leq \Delta$, a kromatikus szám nem nagyobb, mint a maximális fokszám.
Biz: nem kell.

Alsó becslés a független pontok maximális számával:
Tétel: $\chi(G) \geq \frac{n}{\alpha(G)}$, ahol n a pontok száma, $\alpha(G)$ pedig a független pontok maximális száma.

Biz:
Ha G-t kiszínezzük $\chi(G)$ színnel, akkor minden egyes színosztály legfeljebb $\alpha(G)$méretű, hiszen független pontokból áll. Ezek szerint G csúcsait $\chi(G)$ darab, legfeljebb $\alpha(G)$méretű halmaz uniójára bontottuk, ahonnan $n \leq \chi(G) \cdot \alpha(G)$, és innen az állítás közvetlenül adódik.

3) Síkbarajzolható gráfok kromatikus száma. Perfekt gráfok, Lovász gyenge perfekt gráf tétele (biz. nélkül), erős perfekt gráf tétel (biz. nélkül), intervallumgráfok perfektsége. Élkromatikus szám viszonya a maximális fokszámhoz, Vizing tétel (biz. nélkül).

Tétel (4 szín): Minden egyszerű, síkbarajzolható gráf 4-színezhető.
Biz: nem kell.

Tétel (5 szín): Minden egyszerű, síkbarajzolható gráf 5-színezhető, azaz $\chi(G) \leq 5$.

Biz:
Legfeljebb 3-pontú gráfokra a tétel triviálisan igaz. Nagyobb gráfokra indukcióval: tegyük fel, hogy a legfeljebb *n-1* pontú gráfokra a tétel igaz. Legyen *G* egy *n* pontú (*n>3)*, egyszerű, síkbarajzolható gráf. Tudjuk, hogy *G* élszáma legfeljebb *3n-6*, azaz *G* pontjainak fokszámösszege legfeljebb *6n-12*. Van tehát *G*-nek egy legfeljebb 5-ödfokú *x* csúcsa (ez a Recski-féle bsz könyv 2.5.4. tételéből következik).
Ha *d(x)=4*, akkor az indukció miatt *v*-t elhagyva kiszínezzük a gráfot 5 színnel, végül *x* a 4 szomszédjától eltérő ötödik színt kapja.
Tegyük fel, hogy *d(x)=5*. Ha *v*-nek bármely két szomszédja között van él, akkor a gráfban egy K_6 részgráf szerepel, ami ellentmond *G* síkbarajzolhatóságának. Tehát *x* két szomszédja, *y* és *z* nincs összekötve. Húzzuk össze egy ponttá *x, y, z*-t. Az így kapott *G'* gráf az indukció miatt színezhető 5 színnel. Az ennek megfelelő színezés az eredeti *G* gráfban nem jó, hiszen *x,y,z* egyszínűek. *G*-ben *x*-nek három szomszédja van *y*-on és *z*-n kívül. Ezek legfeljebb három színt foglalnak le, és a további két szomszéd, *y,* és *z* egyszínű, marad tehát az ötödik szín, amellyel kiszínezhetjük *x*-et. Tehát *G* kiszínezhető 5 színnel.
(először kitaláltuk, hogy x szomszédai hogyan lehetnek összekötve, ezután ebből következtettünk a színezésre).

Perfekt gráf: Egy G gráf perfekt, ha $\chi(G) = \omega(G)$, és G minden G' feszített részgráfjára is teljesül, hogy $\chi(G') = \omega(G')$.

Tétel: Minden páros gráf perfekt.

Biz:
Páros gráf minden részgráfja is páros, ezért elég belátni, hogy minden *G=(A,B)* páros gráfra $\chi(G) = \omega(G)$. Ez viszont nyilván igaz, hiszen a legalább egy élet tartalmazó gráfokra $\omega(G) = 2$ (mert páros gráfban nincs háromszög), másrészt, ha A pontjait egy színnel, B pontjait egy másik színnel színezzük, akkor G egy 2-színezését kapjuk. Az egy élet sem tartalmazó páros gráfokra pedig $\chi(G) = 1 = \omega(G)$.

Tétel (Lovász): Egy gráf perfekt ⇔ a komplementere perfekt.
Biz: nem kell.

Tétel (Erős perfekt gráf tétel): Egy G gráf perfekt ⇔ sem *G*, sem $\bar{G}$ nem tartalmaz feszített részgráfként legalább 5 hosszú páratlan kört.
Biz: nem kell.

Intervallumgráf: Legyenek $I_1 = [a_1,b_1]$, $I_2 = [a_2,b_2]$, … korlátos zárt intervallumok, és minden a_i, b_i legyen pozitív egész. Legyenek p_1, p_2, … egy G gráf pontjai, és $\{p_i, p_j\}$ akkor és csak akkor legyen él G-ben, ha $Ii \cap Ij \neq 0$. Az így előálló gráfot **intervallumgráfnak** hívjuk.

Tétel: Minden intervallumgráf perfekt.

Biz:
Az intervallumgráfok feszített részgráfjai is intervallumgráfok, így elég belátni, hogy az intervallumgráfok kromatikus száma megegyezik a klikkszámukkal.
Tegyük fel, hogy $\omega(G) = k$. Mivel $\chi(G) \geq \omega(G)$, elég belátni, hogy $\chi(G) \leq k$. Kezdjük el színezni az intervallumokat balról jobbra úgy, hogy mindig azt az intervallumot színezzük, amelyiknek a kezdőpontja legbalrább van. Ha egy intervallumot a $k+1$-edik színnel színezünk, az azt jelenti, hogy ennek az intervallumnak a bal vége benn a van már k intervallumban, amelyeket kiszíneztünk az $1,2,\ldots,k$ színekkel. Így van $k+1$ intervallum, amelyek közül bármely kettő metszi egymást, azaz van az intervallumgráfban egy $k+1$ méretű klikk, ez viszont ellentmond a feltevésünknek.

Él-színezhetőség: Egy G gráf élei k színnel színezhetők, hogyha minden élet ki lehet színezni k szín felhasználásával úgy, hogy bármely két szomszédos él színe különböző.

Élkromatikus szám: $\chi_e(G) = k$, ha G élei k színnel kiszínezhetőek, de $k-1$-el nem.

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

Megjegyzés: $\chi_e(G) = \chi(L(G))$. Az élkromatikus szám nem lehet kisebb a maximális fokszámnál, hiszen az egy pontra illeszkedő éleket mind különböző színekre kell színezni.

Tétel (Vizing): Ha G egyszerű gráf, akkor $\chi_e(G) \leq \Delta + 1$.
Biz: nem kell.

4) Hálózat, hálózati folyam és *(s,t)*-vágás fogalma, folyam nagysága, *(s,t)*-vágás kapacitása. Ford-Fulkerson tétel, Edmonds-Karp tétel (biz. nélkül), egészértékűségi lemma. A folyamprobléma általánosításai.

Hálózat: Legyen G egy irányított gráf. Rendeljünk minden éléhez egy $c(e)$ nemnegatív valós számot, amit az él **kapacitásának** nevezünk. Jelöljünk ki továbbá két s,t pontot G-ben, melyeket **termelőnek,** illetve **fogyasztónak** hívunk. Ekkor, a $(G;s;t;c)$ négyest **hálózatnak** nevezzük.

Folyam: Legyen $f(e)$ olyan függvény, amely minden e élhez egy valós számot rendel. Ez az f függvény **megengedett függvény,** ha $f(e) \leq c(e)$ minden élre, és

$$m(v) = \sum\{f(e)|e\ végpontja\ v\} - \sum\{f(e)|e\ kezdőpontja\ v\} = 0,$$

minden $v \in V(G)$-re, kivéve az s és t pontokat. Egy megengedett függvényt **folyamnak** hívunk. Könnyen belátható, hogy $m(t) = -m(s)$. Ezt a közös értéket a **folyam értékének** nevezzük, és m_f-el jelöljük. Egy él **telített**, ha $f(e) = c(e)$, és **telítetlen,** ha $f(e) < c(e)$.
(emberi nyelven: minden élen legfeljebb kapacitásnyi terhelés lehet, és a csomópontba bemenő érték megegyezik a kimenő értékkel).

Vágás: Legyen $s \in X \subseteq V(G) - \{t\}$, így nyilvánvaló, hogy sem X, sem $V(G) - X$ nem üres halmaz. Azoknak az éleknek a C halmazát, amelyeknek egyik végpontja X-beli, másik $V(G) - X$-beli, a hálózati folyam egy ***(s,t)-vágásának*** nevezzük. A **vágás értéke** $c(C)$ azon éleken lévő kapacitások összege, amelyek egy X-beli pontból egy $V(G) - X$-beli pontba mutatnak. Ezeket előremutató éleknek nevezzük. tehát a vágás értékében nem játszanak szerepet a visszafelé mutató élek, vagyis azok, amelyek egy X-beli pontba mutatnak.

Tétel (Ford-Fulkerson): A maximális folyam értéke egyenlő a minimális vágás értékével:

$$\max\{m_f | f\ egy\ folyam\ s - ből\ t - be\} = \min\{c(C)|C\ vágás\}.$$

Biz:
A maximális folyam nyilván nem lehet nagyobb a minimális vágásnál, hiszen ha minden előremutató él telített, a visszafelé mutatókon pedig 0 a folyam értéke, akkor ezen a vágáson nem mehet át több egység. Az előző tételben pedig láttuk, hogy ha létezik egy f maximális folyam, akkor van ilyen értékű vágás. Azt, hogy maximális folyam mindig létezik, azt a javítóút kereső algoritmussal bizonyíthatjuk.
Javítóút keresés: Az irányított G gráfon adott f folyamhoz definiálunk egy H irányított gráfot: legyen $V(H)=V(G)$, és H-ban fusson egy irányított él x-ből y-ba, ha vagy
(1) $(x,y) \in E(G)$, és $f(x,y) < c(x,y)$, (azaz van még szabad kapacitás), vagy
(2) $(y,x) \in E(G)$, és $f(y,x) > 0$. (azaz az élen nemnulla érték folyik).
Könnyen látható, hogy ha H-ban van egy irányított út s-ből t-be, akkor az ennek az útnak megfelelő élek G-ben éppen egy javító utat adnak az f folyamra nézve. Ha pedig van javító út G-ben, akkor lesz irányított út s-ből t-be.

Tétel (Edmonds-Karp): Ha mindig a legrövidebb javító utat vesszük, akkor a maximális folyam meghatározásához szükséges lépések száma felülről becsülhető a pontok számának polinomjával.
Biz: nem kell.

Tétel (egészértékűségi lemma): Ha a kapacitások egész számok, akkor a maximális folyam értéke egész szám, és ez olyan f függvénnyel is megvalósítható, amely minden élen egész értéket vesz fel.

Biz:
Nyilvánvaló, hiszen az azonosan 0 (kiindulási) folyam rendelkezik a kívánt tulajdonsággal, és az algoritmus során a folyamértékek minden élen csak egész számmal változhattak.

5) Menger tételei. Többszörös összefüggőség, és élösszefüggőség. Dirac tétele (biz. nélkül).

Menger tételei:
Tétel (Menger 1): Ha G egy irányított gráf, $s, t \in V(G)$, akkor az s-ből t-be vezető páronként éldiszjunkt irányított utak maximális száma megegyezik az összes irányított s-t utat lefogó élek minimális számával.

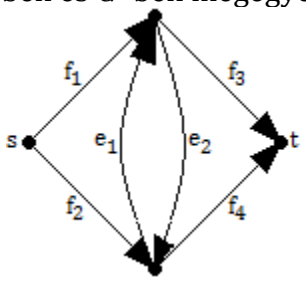
Biz:
Ha létezik G-ben k darab ilyen irányított s-t út, akkor az s-t utakat lefogó élek száma legalább k. Tehát $\max\{\} \leq \min\{\}$. Most lássuk a fordított egyenlőtlenséget. Tegyük fel, hogy az s-t utakat lefogó élek minimális száma k. Legyen minden él kapacitása 1. Az így kapott hálózatban a minimális vágás értéke tehát legalább k. Ekkor a Ford-Fulkerson tétel miatt a maximális folyam is legalább k értékű. Azt is láttuk már, hogy van olyan maximális folyam, melyben minden élen a folyamérték 0 vagy 1. Lássuk be, hogy G-ben van k éldiszjunkt irányított s-t út. Egy ilyen út mindenképpen van, különben nem lehetne k a folyam értéke. Az ebben a folyamban szereplő élek kapacitását változtassuk 0-ra. Így a folyam értéke legalább $k-1$ lesz. Ekkor viszont ismét kell lennie s-t útnak, és ennek nyilván nincs közös éle az előbbi úttal. A gondolatmenetet folytatva éppen k éldiszjunkt irányított s-t utat kapunk.

Tétel (Menger 2): Ha G egy irányított gráf, $s, t \in V(G)$, két nemszomszédos pont, akkor az s-ből t-be vezető, végpontoktól eltekintve pontdiszjunkt irányított utak maximális száma megegyezik az összes irányított s-t utat s és t felhasználása nélkül lefogó pontok minimális számával.

Biz:
Készítsünk egy új G' gráfot úgy, hogy minden pontot húzzunk szét két ponttá. 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 lehet elég a lefogáshoz, mert ha a lefogó élek között lennének (a'',b') típusú élek, akkor ezeket helyettesíthetjük (b',b'')-vel, ha $b' \neq t$, illetve (a',a'')-vel, ha $b'=t$. Így pedig G-ben egy kisebb lefogó ponthalmazt nyernénk. Vagyis a G-beli lefogó pontok és a G'-beli lefogó élek minimális száma egyenlő. Az is könnyen látható, hogy G-beli pontdiszjunkt utaknak G'-ben éldiszjunkt utak felelnek meg, és fordítva, G'-beli éldiszjunktaknak G-ben pontdiszjunktak. Így Menger 1 bizonyítja állításunkat.

Tétel (Menger 3): Ha G egy irányítatlan gráf, $s,t \in V(G)$, akkor az s-ből t-be vezető éldiszjunkt irányítatlan utak maximális száma megegyezik az összes irányítatlan s-t utat lefogó élek minimális számával.

Biz:
A probléma visszavezethető a hasonló, de irányított gráfos esetre: legyen G' olyan gráf, ahol minden irányítatlan él helyére egy oda és egy visszamutató irányított élt rajzolunk. Az visszavezetés nélkül is látszik, hogy k darab diszjunkt utat nem lehet k-nál kevesebb éllel lefogni, vagyis a maximum nem nagyobb a minimumnál. Tegyük fel, hogy G-ben k a diszjunkt utakat lefogó élek minimális száma. Ha G'-ben ennél kevesebb él lefogná az irányított utakat, akkor az ezeknek az éleknek G-ben megfelelő élek lefognák az utakat G-ben, ami ellentmondás.
Világos, hogy egy G-beli s-t útnak G'-ben megfelel egy irányított s-t út. Azonban két éldiszjunkt irányított s-t útnak megfelelő utak G-ben nem feltétlenül éldiszjunktak. Előfordulhat, hogy az egyik irányított út (ld. ábra) tartalmazza az f_1,e_2,f_3 utat, a másik pedig az f_2,e_1,f_4 utat, ahol az f_i szimbólumok nem csak irányított éleket, hanem irányított részutakat is jelölhetnek. Ezek ugyan éldiszjunktak, de a G-ben nekik megfelelő utaknak van közös éle. Ezt a két diszjunkt utat helyettesítsük az f_1, f_3 *és* f_2, f_4 utakkal. Az ezeknek G-ben megfelelő utak már diszjunktak. Evvel a helyettesítéssel csökken az utakban szereplő élek száma, tehát véges lépés után már nem fog ilyen helyzet előállni. Ebből tehát látszik, hogy a diszjunkt utak maximális száma G-ben és G'-ben megegyezik.



Így visszavezettük a feladatot a korábbi problémára, hiszen G'-ben már bizonyítottuk, hogy a minimum nm nagyobb a maximumnál, G-ben pedig a lefogó élek száma nem lehet nagyobb, mint G'-ben.

Tétel (Menger 4): Ha G egy irányítatlan gráf, $s,t \in V(G)$ két nemszomszédos pont, akkor az s-ből t-be vezető pontdiszjunkt irányítatlan utak maximális száma megegyezik az összes irányítatlan s-t utat s és t felhasználása nélkül lefogó pontok minimális számával.

Biz:
Az irányítatlan élek helyére behúzzuk az oda és visszamutatókat, onnantól pedig Menger 3.

Összefüggőség: 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. A gráf **k-szorosan élösszefüggő**, ha akárhogy hagyunk el belőle k-nál kevesebb élet, összefüggő gráfot kapunk.

Tétel: A G gráf k-szorosan összefüggő, ⇔ legalább $k+1$ pontja van, és bármely két pontja között létezik k pontdiszjunkt út. Hasonlóan G k-szorosan élösszefüggő ⇔ bármely két pontja között létezik k éldiszjunkt út.

Biz:
Először az élösszefüggőséget bizonyítjuk. Ha G k-szorosan élösszefüggő, akkor az u-v utakat lefogó élek minimális száma legalább k. Így Menger 3 miatt az éldiszjunkt utak minimális száma legalább k. Ennek a résznek a megfordítása is következik Menger 3-ból.
Ha G k-szorosan összefüggő, akkor bármely két $u, v \in V(G)$ pontot választva legalább k darab, u-tól és v-től különböző pontra van szükség ahhoz, hogy lefogjuk az összes u és v közötti utat (az esetleges $\{u, v\}$ él most nem játszik). Így a Menger 4 miatt létezik k darab pontdiszjunkt út u és v között.
Ha G bármely két pontja között létezik k pontdiszjunkt út, akkor nyilván nem lehet ezeket k-nál kevesebb ponttal lefogni, tehát a k-szoros összefüggőség következik.

Tétel (Menger 5): A legalább 3 pontú G gráf 2-szeresen összefüggő ⇔ tetszőleges két pontján, vagy élén át vezet kör.

Biz:
Az első rész triviális, hiszen két pontdiszjunkt u-v út együtt egy kört ad, amely átmegy u-n és v-n. A második rész pedig ebből következik. 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 f élet. Az így kapott gráf is 2-szeresen összefüggő. Az első állítás szerint ezen a két ponton át megy kör, és ez a kör az eredeti gráfban átmegy e-n és f-en. A megfordítás pedig nyilvánvaló.

Tétel (Dirac): Ha $k \geq 2$ és a G gráf k-szorosan összefüggő, akkor bármely $x_1, x_2, \ldots, x_k$ pontján át vezet kör.
Biz: nem kell.

6) Páros gráf fogalma, karakterizációja. Párosítások páros gráfban, a javító utas módszer. König, Hall és Frobenius tételei.

Páros gráf: 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 pontja A-ban, másik pontja B-ben van. Jelölés: $G=(A,B)$. A $K_{A,B}$-vel jelölt **teljes páros gráf** olyan $G=(A,B)$ páros gráf, ahol $|A| = a$ és $|B|=b$, és amelyben minden A-beli pont össze van kötve minden B-beli ponttal.

Tétel: Egy G gráf páros gráf ⇔ minden G-ben lévő kör páros hosszúságú.

Biz:
Ha G páros gráf, és C egy kör G-ben, akkor C pontjai felváltva vannak A-ban és B-ben, így $|V(C)|$ nyilván páros. Ha G minden köre páros hosszú, akkor megadhatjuk az A és B halmazt. Válasszunk ki egy tetszőleges $v \in V(G)$pontot. Legyen ez A első pontja. Most v minden szomszédját helyezzük B-be, majd minden B-ben lévő pont szomszédját A-ba. Ezután minden, eddig nem szerepelt A-beli pont szomszédját B-be, és így tovább, egészen addig, amíg a pontok el nem fogynak. Ez biztosan jó elosztás, hiszen ha most két A-beli pont össze lenne kötve, akkor lennie kéne a gráfban egy páratlan hosszú körnek, ami ellentmondás. Ha a gráf nem összefüggő, akkor az eljárást komponensenként csináljuk.

Párosítás: Párosításnak, vagy részleges párosításnak nevezünk egy M élhalmazt, ha semelyik két élnek nincs közös pontja. Az ilyen éleket **független éleknek** is nevezzük. A részleges párosítás **lefedi** éleinek végpontjait. Egy párosítást **teljes párosításnak** nevezünk, ha a gráf minden pontját lefedi.

$N(X)$-szel jelöljük egy $X \subseteq V(G)$ ponthalmaz szomszédjainak halmazát, vagyis $N(X)$ azon y pontok halmaza, amelyekhez van olyan él, melynek egyik végpontja y, a másik pedig egy X-beli pont.

α(G): független pontok maximális száma
ν(G): független élek maximális száma
τ(G): lefogó pontok minimális száma
ρ(G): lefogó élek minimális száma

Tétel: $\nu(G) \leq \tau(G)$, minden G gráfra.

Biz:
Legyen M egy maximális méretű független élhalmaz. Mivel pusztán M éleinek lefogásához már $\nu(G)=|M|$ pontra van szükség, ezért $\tau(G) \geq |M|$.

Tétel: $\alpha(G) \leq \rho(G)$, minden G gráfra.
Biz: nem kell.

Javító utas módszer: Legyen $G=(A,B)$ $X \subset A$, , és $N(X) \subset B$ (szokásos jelölésekkel). Legyen továbbá egy M párosításunk, amely lefedi az $X \subset A$halmazt, de van olyan $u \in A - X$ pont, amit nem. Ha van olyan P út, ami egy A-X-beli pontból indul, egy B-$N(X)$-beli pontban végződik, és minden második éle M-beli, de a többi nem M-beli, akkor növelhetjük a párosítást. Ekkor ugyanis a P út első és utolsó éle nem M-beli, tehát eggyel több nem M-beli él szerepel benne, mint az M-beliek száma. Az ilyen P utakat **javító útnak** nevezzük. Ha tehát $M' = \big(M - (M \cap P)\big) \cup (P - M)$, vagyis ha M-ből elhagyjuk a P-ben szereplő éleket, és hozzávesszük a többi O-beli élet, akkor az így kapott M' párosítás élszáma eggyel nő.

Tétel (König): Ha *G=(A,B)* páros gráf, akkor $\nu(G) = \tau(G)$. Ha nincs *G*-ben izolált pont, akkor $\alpha(G) = \rho(G)$ is teljesül.

Biz:
Készítsük el a *G'* gráfot az alábbi módon: irányítsuk *G* minden élét *A*-ból *B*-be, vegyünk fel egy új *s* és *t* pontot, vezessünk *s*-ből élt *A* minden pontjába, és vezessünk *B* minden pontjából élt *t*-be. Az élek kapacitásai: *c(s-A)=c(B-t)=1*, és *c(A-B)=* ∞ (pontosabban $|A|+1$). Tekintsük a *(G',s, t, c)* hálózatot, ahol *c* az imént definiált kapacitást jelenti.
Ha *G*-ben van egy *k* méretű párosítás, akkor létezik ebben a hálózatban *k* nagyságú egészfolyam: a párosításéleknek megfelelő éleken, az ezen élek *A*-beli végpontjaihoz vezető *s*-ből induló éleken, valamint a párosításélek *B*-beli végpontjaiból *t*-be vezető éleken legyen a folyam által felvett érték 1, minden egyéb élen 0. Az is könnyen látható, hogy a hálózatban minden egészfolyam úgy áll elő, hogy néhány, *A*-ból *B*-be vezető független élen a folyam 1 értéket vesz fel, ezeket az éleket *s*-ből tápláljuk, a kifolyó folyamot pedig *t*-be engedjük. A hálózatban tehát a maximális egészfolyam értéke $\nu(G)$, és az egészértékűségi lemma miatt a maximális folyamérték is ugyanennyi.
A Ford-Fulkerson tétel szerint létezik tehát egy $\nu(G)$ kapacitású vágás. Ha ezt a vágást az *s*-t tartalmazó *X* halmaz definiálja, akkor $X \cap A$-ból nem futhat *G'*-nek éle $B \backslash X$-be, hisz akkor a vágás kapacitása ∞ volna (pontosabban $|A|+1$, de már az is több mint $\nu(G)$, hisz *A* egy lefogó halmaz, ahonnan $\nu(G) \leq |A|$). Ez azt jelenti, hogy $(A \backslash X) \cup (B \cap X)$ egy lefogó ponthalmaz, tehát $|A \backslash X| + |B \cap X| \geq \tau(G)$. A hálózat konstrukciójából adódóan az *X* által definiált vágás kapacitása $\nu(G) = |A \backslash X| + |B \cap X| \geq \tau(G)$. Azt pedig már bizonyítottuk, hogy $\nu(G) \leq \tau(G)$, ahonnan $\nu(G) = \tau(G)$ adódik.

Tétel (Hall): Egy *G=(A, B)* páros gráfban van *A*-t lefedő párosítás ⇔ minden $X_0 \subseteq A$ részhalmazra $|N(X_0)| \geq |X_0|$ (Ezt a feltételt **Hall-feltételnek** nevezzük.)
Biz:
⇨
Nyilvánvaló, hiszen ha létezik *A*-t lefedő párosítás, akkor minden *A*-beli pontnak különböző párja van, tehát tetszőleges $X \subseteq A$ esetén az *X*-beli elemek *B*-beli párjai az *N(X)* egy $|X|$ méretű részhalmazát alkotják.
⇦
Tegyük fel, hogy $|X| \leq |N(X)|$ minden $X \subseteq A$-ra. Azt kell igazolni, hogy $\nu(G) \geq |A|$. Legyen *U* minimális ($\tau(G)$ méretű) lefogó ponthalmaz, és legyen $U_A := U \cap A$, $U_B := U \cap B$. Mivel *U* lefogja az $X := A \backslash U_A$-ból induló éleket, ezért $N(X) \subseteq U_B$, tehát $|N(X)| \leq |U_B|$. A König-tétel, illetve a Hall feltétel miatt:
$\nu(G) = \tau(G) = |U| = |U_A| + |U_B| \geq |U_A| + |N(X)| \geq |U_A| + |X| = |A|$.

Tétel (Frobenius): Egy *G=(A, B)* páros gráfban van teljes párosítás ⇔ $|A| = |B|$, és $|N(X)| \geq |X|$ minden $X \subseteq A$-ra.

Biz:
A két feltétel szükségessége nyilvánvaló. Ha viszont teljesül a második feltétel, akkor a Hall-tétel miatt van *A*-t lefedő párosítás. Mivel azonban $|A|=|B|$, ez lefedi *B*-t is.

7) Párosítások tetszőleges gráfban, Tutte tétele (csak a könnyű irány bizonyításával). Gallai tételei. Gráfok és mátrixok: szomszédsági mátrix és hatványainak jelentése, illeszkedési mátrix és rangja.

α(G): független pontok maximális száma
ν(G): független élek maximális száma
τ(G): lefogó pontok minimális száma
ρ(G): lefogó élek minimális száma

Tétel (Gallai 1): $\tau(G)+\alpha(G)=|V(G)|$ minden hurokmentes G gráfra.

Biz:
Egy X halmaz pontjai akkor és csak akkor függetlenek, ha a $V(G)$-X halmaz lefogó ponthalmaz. Hiszen ha X nem független, akkor van két összekötött pont, és így $V(G)$-X nem fogja le ezt az élet. Fordítva, ha $V(G)$-X nem fog le egy huroktól különböző élet, akkor X-ben ennek az élnek mindkét végpontja szerepel. Tehát $\tau(G) \leq |V(G)\text{- X}|$ minden X független ponthalmazra. Ebből pedig következik, hogy $\tau(G)+\alpha(G)\leq|V(G)|$. Hasonlóan $\alpha(G)\geq|V(G)\text{-}Y|$ minden Y lefogó ponthalmazra, amiből $\tau(G)+\alpha(G)\geq|V(G)|$ következik.

Tétel (Gallai 2): $\nu(G) + \rho(G) = |V(G)|$ minden G gráfra, amelyben nincs izolált pont.

Biz:
Egy $\nu(G)$ elemű X független élhalmaz lefog $2\nu(G)$ különböző pontot. A többi pont (mivel nincs köztük izolált) nyilván lefogható $|V(G)| - 2\nu(G)$ éllel, így$|V(G)| - \nu(G) \geq \rho(G)$. Másrészt, ha Y egy minimális lefogó élhalmaz, akkor Y néhány (mondjuk k darab) diszjunkt csillag egyesítése. Ha ugyanis Y tartalmazna kört, akkor annak bármely élét, ha pedig 3 hosszú utat, akkor annak középső élét el lehetne hagyni Y-ból, mert a többi él még mindig lefogná az összes pontot. Így $\rho(G) = |V(G)| - k$, (hiszen k komponensű erdőről van szó). Ha minden csillagból kiválasztunk egy élet, az így kapott élhalmaz nyilván független, tehát $\nu(G) \geq k = |V(G)| - \rho(G)$.

Tétel (Tutte): Egy G gráfban létezik teljes párosítás $\Leftrightarrow$ minden $X \subseteq V(G)$ esetén $c_p(G - X) \leq |X|$, azaz akárhogy hagyunk el a gráfból néhány pontot, a maradékban a páratlan hosszú komponensek száma ennél több nem lehet.

Biz:
$\Rightarrow$ Ha G-ben van teljes párosítás, akkor nyilvánvalóan teljesül a feltétel. Hiszen ha elhagyjuk a gráfból X-et, akkor a páratlan komponensek mindegyikéből az eredeti gráfban indul ki legalább egy párosításbeli él, és ezek az élek csak egy-egy (különböző) X-beli pontba mehetnek. Tehát $c_p(G - X) \leq |X|$.

$\Leftarrow$ nem kell.

Szomszédsági mátrix: legyen $A(G)=(a_{ij})$ $n\times n$-es mátrix az alábbi módon:

$$a_{ij}=\begin{cases}0, \text{ ha az } i\text{-edik és } j\text{-edik pont nem szomszédos}\\ k, \text{ ha az } i\text{-edik és } j\text{-edik pont között } k \text{ darab párhuzamos él halad}\\ l, \text{ ha } i=j, \text{ és az } i\text{-edik ponthoz } l \text{ darab hurokél illeszkedik.}\end{cases}$$

Irányított gráfok esetén a_{ij} az i-edik pontból a j-edik pontba vezető élek száma.

Tétel: A szomszédsági mátrix t-edik hatványa olyan $A^t=(m_{ij}^{(t)})$ mátrix, melynek $(m_{ij}^{(t)})$ eleme az i-ből j-be vezető t hosszúságú élsorozatok száma. Ezen élsorozatok között nem csak az utakat számoljuk, hanem az azonos ponton, vagy akár élen, többször átmenő sorozatokat is.

Biz:

Először lássuk be a tételt t=2-re. Az A^2 mátrix egy $(m_{ij}^{(2)})$ elemét az A mátrix i-edik sorának és j-edik oszlopának skalárszorzataként kapjuk meg. Ebben a skalárszorzatban a k-adik összeadandó a gráf v_i-ből v_k-ba vezető, és v_k-ból v_j-be vezető élei számának szorzata. Így a skalárszorzat ezeknek az összegzése minden k-ra, beleértve, hogy lehet $k=i$, vagy $k=j$ is. Ilyenkor számljuk a hurokéleket is. Tehát $(m_{ij}^{(2)})$ a v_i és v_j közötti 2 hosszú élsorozatok száma.

t>2-re teljes indukcióval bizonyítunk, felhasználva a fenti gondolatmenetet. Tegyük fel, hogy t-1-re már bizonyítottuk az állítást. A definíció szerint $A^t=A^{t-1}\times A$. Az A^t mátrix egy $(m_{ij}^{(t)})$ elemét ezért az A^{t-1} mátrix i-edik sorának, és az A mátrix j-edik oszlopának skalárszorzataként kapjuk meg. Ebben a skalárszorzatban a k-adik összeadandó a gráf v_i-ből v_k-ba vezető t-1 hosszú élsorozatai számának, és v_k-ból v_j-be vezető élek számának szorzata. Így a skalárszorzat ezeknek az összegzése minden k-ra, tehát $(m_{ij}^{(t)})$ a v_i és v_j közötti t élből álló élsorozatok száma.

Illeszkedési mátrix: legyen G n pontú, e élt tartalmazó gráf, melyhez tartozzék $B(G)=(b_{ij})$ $n\times e$-es mátrix az alábbi módon:

$$b_{ij}=\begin{cases}0, \text{ ha a } j\text{-edik él nem illeszkedik az } i\text{-edik ponthoz}\\ 1, \text{ ha a } j\text{-edik élnek az i-edik pont a kezdőpontja}\\ -1, \text{ ha a } j\text{-edik élnek az i-edik pont a végpontja}\end{cases}$$

Legyen –megállapodás szerint- $b_{ij}=1$ akkor is, ha a j-edik él az i-edik ponthoz illeszkedő hurokél. Irányítatlan esetben is ez a definíció, csk ott a j-edik él mindkét végpontjának megfelelő mátrixelem 1.

Tétel: Az n pontú c darab összefüggő komponensből álló, hurokélmentes irányított G gráf illeszkedési mátrixának rangja n-c.

Biz:

Ha $c>1$, akkor komponensenként sorolva fel a pontokat és éleket, $B(G)$ blokkdiagonális szerkezetű lesz. Elég tehát egy p pontú összefüggő komponensre belátni, hogy a neki megfelelő blokk rangja p-1. Mivel a blokk sorainak száma p, és az összes sor összege a (0,0,…,0) vektor (hiszen minden élnek megfelelő oszlopban egy +1, egy -1, és p-2 darab zérus található), nyilvánvaló, hogy a rang legfeljebb p-1 lehet (itt használtuk fel a hurokélmentességet).

Legyen F egy p pontú, p-1 élű feszítőfa ebben a komponensben. Legyen v_1 egy elsőfokú pont F-ben, és e_1 a hozzá illeszkedő él. Legyen v_2 egy elsőfokú pont (F-$\{v_1\}$)-ben, és e_2 a hozzá illeszkedő él, stb. Ha a blokk sorait $v_1, v_2,\ldots$ sorrendben soroljuk fel, oszlopait pedig e_1, e_2 felsorolásával kezdjük, akkor egy $p\times(p-1)$ méretű részmátrixot kapunk, amelyből az utolsó sor elhagyásával olyan mátrixot kapunk, melynek diagonális elemei ±1 értékűek, és az átló felett csupa zérus áll. Mivel így találtunk p-1 független oszlopot, a rang pontosan p-1.

8) Oszthatóság, felbonthatatlanok, a számelmélet alaptétele. Legnagyobb közös osztó, legkisebb közös többszörös, osztók száma. Euklideszi algoritmus. Nevezetes tételek prímszámokról: prímek száma, hézag a szomszédos prímek között, Csebisev-tétel (biz. nélkül), Dirichlet tétele (biz. nélkül).

Oszthatóság: Legyenek $a, b \in \mathbb{Z}$. Azt mondjuk, hogy b **osztható** a-val, vagy a **osztója** b-nek, (a **osztja** b-t), ha van olyan $q \in \mathbb{Z}$, amelyre $b = aq$. Jelölés: $a \mid b$.

Triviális osztó: n egész szám triviális osztói: ± 1, $\pm$n.
Valódi osztó: a nem triviális osztók.

Felbonthatatlanság: A $p \in \mathbb{Z}$ szám **felbonthatatlan**, ha |p|≠1 és p-t csak triviális módon tudjuk egészek szorzataként előállítani, azaz p=ab ($a, b \in \mathbb{Z}$) esetén |a|=1, vagy |b|=1. Másképp fogalmazva p akkor felbonthatatlan, ha p-nek csak triviális osztói vannak, és p≠1, ill. p≠-1. (Baromira nem összekeverendő a prímszámok definíciójával!).

A számelmélet alaptétele: Ha egy z egész számra $|z| > 1$, akkor z előáll felbonthatatlan számok szorzataként, és a z ilyen előállításai csak a tényezők sorrendjében és előjeleiben különböznek.

Biz:
Segédtétel: Bármely z egész szám előáll felbonthatatlan számok szorzataként, ha $|z| > 1$.

Ezt a tételt teljes indukcióval bizonyítjuk. Világos, hogy |z|=2 esetén z felbonthatatlan, és mint egytényezős szorzat megfelel. Tegyük fel, hogy k-ig már bizonyítottunk, azaz minden olyan számra igaz a tétel, aminek az abszolút értéke legfeljebb k. Legyen |z| = k+1. Ha z felbonthatatlan, akkor z megfelel, mint egytényezős szorzat. Ha z nem felbonthatatlan, akkor z nemtriviális módon felbomlik z=ab alakban, ahol 1<|a|≤k és 1<|b|≤k. Az indukciós feltevés értelmében a és b is előáll felbonthatatlan számok szorzataként, ezért ez a szorzatukra, z-re is igaz.

Eszerint a vizsgált számok előállnak felbonthatatlanok szorzataként. Mivel egy szám pontosan akkor felbonthatatlan, ha az ellentettje is felbonthatatlan, elegendő a pozitív egészeket vizsgálni. A felbontás egyértelműségéhez tehát csak azt kell igazolni, hogy ha $z = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l$ két előállítás, amelyekre $p_1 \le p_2 \le \cdots \le p_k$ és $q_1 \le q_2 \le \cdots \le q_l$ teljesül, akkor $k = l$, és a $p_i = q_i$ minden i-re. Ezt is z szerinti teljes indukcióval bizonyítjuk. Ha $z = 2$, akkor z felbonthatatlan, nincs mit igazolni. Tegyük fel tehát, hogy a z-nél kisebb számokra már megmutattuk a felbontás egyértelműségét. Tekintsük a fenti, $z = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l$ felbontásokat. Az általánosságot az sem korlátozza, ha kikötjük, hogy $p_i \le q_i$.

1. eset: $p_1 = q_1$. Ekkor $\frac{z}{p_1} = p_2 \cdot p_3 \cdot \ldots \cdot p_k = q_2 \cdot q_3 \cdot \ldots \cdot q_l$. Mivel $\frac{z}{p_1} < z$, az indukciós állítás szerint k=l és $p_2 = q_2$, $p_3 = q_3$, … $p_k = q_k$. Így $p_1 = q_1$ miatt z- re is igaz az indukciós állítás.
2. eset: $p_1 < q_1$. Ekkor $z = p_1 \cdot p_2 \cdot \ldots \cdot p_k = (q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_l + p_1 \cdot q_2 \cdot \ldots \cdot q_l$, tehát $p_1(p_2 \cdot p_3 \cdot \ldots \cdot p_k - q_2 \cdot q_3 \cdot \ldots \cdot q_l) = (q_1 - p_1) \cdot q_2 \cdot q_3 \ldots \cdot q_l =: z'$.

Világos, hogy $z'<z$, ezért z'-re tudjuk, hogy igaz a számelmélet alaptétele. Az előző két felírás alapján elkészíthetjük a z' felbonthatatlanok szorzataként történő kétféle felírását, mégpedig úgy, hogy a baloldalon a $(p_2 \cdot p_3 \cdot \ldots \cdot p_k - q_2 \cdot q_3 \cdot \ldots \cdot q_l)$, a jobb oldalon pedig a $(q_1 - p_1)$ tényezőt helyettesítjük egy-egy felbonthatatlanok szorzataként történő előállításukkal. E két felírásból a baloldalon p_1 lesz az egyik tényező, így az indukciós feltevés szerint p_1-nek szerepelnie kell a jobb oldalon is. Mivel p_1 mindegyik q_i-nél kisebb, ezért p_1–nek a $(q_1 - p_1)$ felbontásban kell szerepelnie. Ekkor azonban $p_1 \mid (q_1 - p_1)$, ezért $p_1 \mid q_1$, és ez $1 < p_1 < q_1$ miatt ellentmond q_1 felbonthatatlanságának. Az ellentmondás mutatja, hogy a 2. eset nem valósulhat meg, és ezzel az indukciós bizonyítást befejeztük.

Prímszám: A p 0-tól, 1-től, és -1-től különböző egész számot **prímszámnak** nevezzük, ha $a, b \in \mathbb{Z}$, $p \mid ab$ esetén $p \mid a$, vagy $p \mid b$. Azaz p prím, ha csak úgy tud osztani egy szorzatot, ha a szorzat valamelyik tényezőjét osztja.

Biz: csak akkor kell, ha nagyon brillírozni akarsz. Én nem akarok.

Legyen n kanonikus alakja: $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.

Osztók száma: $d(n) = \prod_{i=1}^{k}(\alpha_i + 1)$

Biz:
Bármely d|n osztó kanonikus alakja olyan, hogy azt alkalmas prímekkel megszorozva n kanonikus alakját kapjuk, azaz $d = \prod_{i=1}^{k} p_i^{\beta_i}$, ahol $0 < \beta_i < \alpha_i$ teljesül minden i-re. Világos, hogy minden osztóhoz tartozik egy $(\beta_1, \dots, \beta_k)$ kitevősorozat, és különböző kitevősorozatok (a prímfelbontás egyértelműsége miatt) különböző osztókhoz tartoznak. (A d=1 osztóhoz pl. a csupa-0 sorozat tartozik). Vagyis a pozitív osztók száma azonos a lehetséges $(\beta_1, \dots, \beta_k)$ sorozatok számával, ahonnan a fenti képlet adódik, hiszen minden β_i érték a többi kitevőtől függetlenül $\alpha_i + 1$ érték valamelyikét veszi fel.

Osztók összege: $\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1}-1}{p-1}$.

LNKO: $a, b \in \mathbb{Z}$, (a, b) a legnagyobb olyan szám, amely osztója a-nak és b-nek is.
A kanonikus alakokban szereplő közös prímeket kell a kisebb hatványon összeszorozni.
LKKT: az a legkisebb $n \in \mathbb{N}$ szám, amelyre $a|n$ és $b|n$ áll.
A kanonikus alakokban szereplő összes prímet kell a nagyobb hatványon összeszorozni.

Euklideszi algoritmus:
Input: $a, b \in \mathbb{Z}$. Output: (a, b).
Osszuk el a-t b-vel, majd b-t a maradékkal, majd a maradékot az új maradékkal, és így tovább, mindig az osztót a maradékkal. Ekkor egy

$a = bq_1 + r_1 \qquad 0 \le r_1 < |b|$
$b = r_1 q_2 + r_2 \qquad 0 \le r_2 < r_1$
$r_1 = r_2 q_3 + r_3 \qquad 0 \le r_3 < r_2$
… …

alakú sorozatot kapunk, ahol $0 \le \cdots < r_3 < r_2 < r_1 < |b|$. Így az r_n sorozat nyilván véges, és valamely $N \in \mathbb{N} - re\ r_N = 0$. Tehát
$r_{N-2} = r_{N-1} q_{N-1} + r_N$, és $r_N = 0$.
Jelöljük n-el az utolsó nem nulla maradék indexét, $n = N - 1$. Állítás: $r_n = (a, b)$.
A legnagyobb közös osztó osztja a-t és b-t is, tehát r_1 kreálásának módja miatt azt is. Mivel b-t és r_1-et is osztja, hasonlóan r_2-t is kell neki. Általánosan, ha r_i-t és r_{i+1}-et osztja, akkor r_{i+2}-t is. Következésképpen $(a, b)|r_n$. Visszafelé haladva pedig tudjuk, hogy $r_n|r_{n-1}$. Ekkor azonban $r_n|r_{n-2}$, és így tovább, általánosan, ha $r_n|r_i$, és $r_n|r_{i-1}$, akkor $r_n|r_{i-2}$. Így visszafelé elértük, hogy $r_n|(a, b)$. Ez viszont, mivel $(a, b)|r_n$, csak úgy lehet, ha $r_n = (a, b)$. Az algoritmus tehát jó.

Tétel: A prímszámok száma végtelen.

Biz:
Elegendő azt megmutatni, hogy minden $2 \le n \in \mathbb{N}$ -re létezik n-nél nagyobb prímszám. Mivel $n!$ az *1,2…n* számok mindegyikével osztható, ezért $N := n! + 1$ az 1,2,…n számok mindegyikéhez relatív prím, tehát N nem osztható egyetlen n-nél kisebb prímmel sem. Vagyis N kanonikus alakjában kizárólag n-nél nagyobb prímek fordulnak elő.

Tétel: Létezik bármilyen sok, egymást követő összetett szám.

Biz:
Legyen $N := (n+1)! + 1$. Ekkor tetszőleges $2 \leq k \leq n+1$ esetén
$k|(n+1)! + k = N + (k-1)$, tehát $N+1, N+2, \ldots, N+n$ számok mindegyike összetett.

Tétel (Csebisev): Tetszőleges n pozitív egészre létezik p prím, melyre$n < p \leq 2n$
Biz: nem kell.

Tétel (Dirichlet): Ha a és d relatív prím, akkor az $a, a+d, a+2d, \ldots$ számtani sorban végtelen sok prím fordul elő.
Biz: nem kell.

Tétel (prímtulajdonság): Ha p prím, és osztója egy ab szorzatnak, akkor p osztója a-nak, vagy b-nek, vagy mindkettőnek.
Biz: nem kell.

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

Kongruencia: $a, b, m \in \mathbb{Z}, 0 < m$ esetén azt mondjuk, hogy a **kongruens** b modulo m, ha $m|a-b$. Jelölés: $a \equiv b\ (m)$. Azaz, két szám kongruens, ha egy tetszőleges számmal elosztva őket, ugyanazt a maradékot adják.

Tétel:
ha $a \equiv b$, $és\ c \equiv d\ (m)$, akkor $a \pm c \equiv b \pm d$, $ac \equiv bd$, $és\ a^k \equiv b^k (m), k \geq 1 \in \mathbb{Z}$.

Biz:

1) a fenti feltételekből következik, hogy $m|a-b, és\ m|c-d$, innen következik, hogy $m|(a-b)+(c-d) = (a+c)-(b+d)$ ami éppen az állítás.
2) $m|a-b \rightarrow m|ac-bc$. Emellett $m|c-d \rightarrow m|bc-bd$. Innen következik, hogy $m\ |ac-bc+bc-bd = ac-bd$, ami éppen az állítás.

Tétel:
$ac \equiv bc\ (m) \Leftrightarrow$a $\equiv b\ (\frac{m}{(m,c)})$.
Biz:
$(m, c) \coloneqq d$.

$\frac{m}{d} = m'; \frac{c}{d} = c' \Rightarrow (m', c') = 1$.

$ac \equiv bc\ (m) \Leftrightarrow m|ac-bc \Leftrightarrow m \cdot k|c(a-b) \overset{:(m,c)}{\Longleftrightarrow} m' \cdot k|c'(a-b) \Leftrightarrow m'|c'(a-b) \overset{:c'}{\Leftrightarrow} m'|a-b,$
ez pedig éppen az állítás.

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

Tétel: Az $ax \equiv b\ (m)$ kongruencia megoldható $\Leftrightarrow$ $(a, m)|b$. Ekkor pontosan (a, m) darab megoldás lesz.

Biz:
Ha a kongruencia megoldható, akkor $m|ax-b$, így b szükségképp osztható a és m valamennyi közös osztójával. Megfordítva, ha b osztható (a, m)-el, akkor fentebbi, osztásos tételből következik, hogy
1). $\frac{a}{(a,m)} x \equiv \frac{b}{(a,m)}\ (\frac{m}{(a,m)})$,
ahol $\frac{a}{(a,m)}$ és $\frac{m}{(a,m)}$már relatív prímek. Ha tehát a mod $\frac{m}{(a,m)}$ teljes maradékrendszer minden elemét végigszorozzuk a modulushoz relatív prím $\frac{a}{(a,m)}$-el, akkor a redukált maradékrendszerekre vonatkozó tétel (ld. 10. tétel) szerint ismét teljes maradékrendszerhez jutunk, vagyis pontosan egy mod$\frac{m}{(a,m)}$ elemeire teljesül 1).
Végül, ha $x \equiv x_0\ (\frac{m}{(a,m)})$ megoldása 1)-nek, akkor nyilván az
$x_0, x_0 + \left(\frac{m}{(a,m)}\right), x_0 + 2\left(\frac{m}{(a,m)}\right), \dots, x_0 + ((a,m)-1)(\frac{m}{(a,m)})$ számok által meghatározott (a, m) darab mod m maradékosztály lesz a kongruencia megoldása.

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

Maradékosztály: az *i*-edik maradékosztályba azok a számok esnek, amelyek *m*-el osztva *i* maradékot adnak, azaz ezek a számok előállnak $k \cdot m + i$ alakban.

Maradékrendszer: Rögzített $m > 1$ egész esetén az m elemű $T = \{a_1, a_2, \dots, a_m\}$ halmazt **modulo m teljes maradékrendszernek** nevezzük, ha T minden m szerinti maradékosztályból pontosan egy elemet tartalmaz. Az $R \subset \mathbb{Z}$ halmaz pedig **redukált maradékrendszer modulo m**, ha R minden olyan modulo m maradékosztályból, mely elemei relatív prímek m-hez, pontosan egy elemet tartalmaz. A modulo m redukált maradékrendszer méretét, azaz azoknak az m szerinti maradékosztályoknak a számát, amik m-hez relatív prím számot tartalmaznak, $\varphi(m)$-el jelöljük.

Redukált maradékrendszerre: $\{c_1, c_2, \dots, c_k\}$

1) $k = \varphi(m)$
2) bármely $i \neq j$ indexpárra $c_i \not\equiv c_j (m)$
3) bármely i indexre $(c_i, m) = 1$.

***φ(n)*:** az n-nél kisebb, n-hez relatív prímek száma.
Kiszámítása:
ha $n = \prod p_i^{\alpha_i}$, akkor $\varphi(n) = n \cdot \prod(1 - \frac{1}{p_i}) = \prod(p_i^{\alpha_i} - p_i^{\alpha_i - 1})$.

Tétel: Legyen $(a, m) = 1$. Ha egy mod m teljes vagy redukált maradékrendszer minden elemét a-val megszorozzuk, ismét egy mod m teljes ill. redukált maradékrendszert kapunk.

Biz:
A maradékrendszer elemeinek számát az a-val való szorzás nyilván nem befolyásolja. Belátjuk, hogy ha $x \not\equiv y\ (m)$, és $(a, m) = 1$, akkor $ax \not\equiv ay\ (m)$. Csakugyan, ha $ax - ay = a(x - y)$osztható lenne m-el, akkor a prímtulajdonság (ld. 8. tétel vége) miatt m minden prímosztója vagy a-nak, vagy $(x - y)$-nak osztója lenne, tehát vagy $(a, m) = 1$, vagy $x \not\equiv y\ (m)$ nem teljesülne. Végül redukált maradékrendszer esetén a redukált maradékrendszer 3)-as tulajdonsága is teljesül: az m-hez relatív prím a és c_i számok szorzatának sem lehet m-el közös prímosztója.

Tétel (Euler-Fermat): Ha $m > 1$ tetszőleges egész szám és a tetszőleges olyan szám, melyre $(a, m) = 1$, akkor

$$a^{\varphi(m)} \equiv 1\ (m).$$

Biz:
Legyen $\{c_1, c_2, \dots, c_{\varphi(m)}\}$ egy mod m redukált maradékrendszer. Az előző tétel szerint az $\{ac_1, ac_2, \dots, ac_{\varphi(m)}\}$ számhalmaz is egy mod m redukált maradékrendszer lesz, tehát az $\{ac_1, ac_2, \dots, ac_{\varphi(m)}\}$ szorzatok valamilyen sorrendben kongruensek a $\{c_1, c_2, \dots, c_{\varphi(m)}\}$ számokkal. Így

$$\prod_{i=1}^{\varphi(m)} (ac_i) \equiv \prod_{i=1}^{\varphi(m)} (c_i)$$

teljesül, vagyis

$$\left(a^{\varphi(m)} - 1\right) \prod_{i=1}^{\varphi(m)} (c_i) \equiv 0 (m)$$

Mivel a c_i számok m-hez relatív prímek voltak, szükségképp $a^{\varphi(m)} - 1$ osztható m-mel.

Tétel (kis Fermat): Tetszőleges p prímszámra, és tetszőleges a egész számra $a^p \equiv a\ (p)$.

Biz:
Ha a osztható p-vel, akkor $a \equiv a^p \equiv 0\ (p)$. Ha nem, akkor $(a, p) = 1$, tehát $a^{\varphi(p)} \equiv a^{p-1} \equiv 1\ (p)$. A kongruencia mindkét oldalát a-val szorozva kapjuk az állítást.

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

Művelet: Legyen H tetszőleges halmaz, jelölje H^n a H halmaz elemeiből képzett n hosszú sorozatokat. Az $f: H^n \to H$ mindenütt értelmezett függvényt n-változós **műveletnek** nevezzük.

Definíció: Egy H halmazon értelmezett 2-változós művelet (jelöljük $*$-al) **kommutatív**, ha tetszőleges $a, b \in H$ esetén $a * b = b * a$, és **asszociatív**, ha tetszőleges $a, b, c \in H$ esetén $(a * b) * c = a * (b * c)$.

Definíció: Az S halmazt a rajta értelmezett $*$ művelettel **félcsoportnak** nevezzük, ha $*$ asszociatív. Ha $*$ kommutatív is, akkor kommutatív, vagy Abel-féle félcsoportról beszélünk.
Pl.: pozitív számok az összeadásra nézve, az $n \times n$-es mátrixok a szorzásra nézve, és a pozitív valós számok a szorzásra nézve félcsoportot alkotnak.

Definíció: Egy G halmazt a $*$ művelettel **csoportnak** nevezünk, ha

a) $(a * b) * c = a * (b * c)$
b) $\exists\, e \in G$, amelyre $a * e = e * a = a$ $\forall a \in G$-re
c) $\forall a \in G$-re $\exists\, a' \in G$ úgy, hogy $a * a' = a' * a = e$.

vagyis, ha a művelet asszociatív, létezik egységelem, és létezik inverz.
Ha a művelet kommutatív is, akkor **Abel-csoportról** beszélünk.

Csoport **rendje** alatt a csoport elemszámát értjük.

Példák:

1. Az egész, a racionális és a valós számok Abel-csoportot alkotnak az összeadásra nézve $((\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +))$, a természetes számok $(\mathbb{N})$ viszont nem.
2. A pozitív valós és a pozitív racionális számok Abel-csoportot alkotnak a szorzásra nézve ($(\mathbb{R}^+, \cdot)(\mathbb{Q}^+, \cdot)$).
3. Az $n \times n$-es invertálható mátrixok csoportot alkotnak a szorzásra nézve.
4. A szabályos n-szög egybevágóságai csoportot alkotnak, ahol a művelet az egymás után való elvégzés. Megjegyezzük, hogy itt a csoport egységeleme a helybenhagyás, a csoport rendje 2n, ugyanis van n darab tengelyes tükrözés, és a helybenhagyással együtt n forgatás. A csoportot D_n-el jelöljük, és **diédercsoportnak** nevezzük.

Kommutatív véges:

Kommutatív végtelen:

Nem kommutatív véges:

Nem kommutatív végtelen:

12) Elem rendje, részcsoport, generált részcsoport, ciklikus csoport. Mellékosztályok, Lagrange tétele, következménye az elemek rendjére vonatkozóan. A szimmetrikus csoport. Csoportok izomorfiája, Cayley tétele.

Szimmetrikus csoport: n elem permutációi (önmagára való bijektív leképezései) csoportot alkotnak a kompozícióra. A csoportot n-ed fokú **szimmetrikus csoportnak** nevezzük, S_n-el jelöljük, rendje $n!$. Egy H halmaz összes permutációjának csoportját S_H-val jelöljük.

Izomorfia: A G_1, G_2 csoportokat **izomorfaknak** nevezzük, ha van köztük egy kölcsönösen egyértelmű művelettartó leképzés, azaz van olyan $\Phi: G_1 \to G_2$ leképezés, amely bijektív és tetszőleges $g, h \in G_1$ esetén $\Phi(g)\Phi(h) = \Phi(gh)$ teljesül.
Jelölése: $G_1 \simeq G_2$.

Homomorfia: Legyenek G_1, G_2 csoportok. A$\Phi: G_1 \to G_2$ leképezést **homomorfizmusnak** nevezzük, ha Φ értelmezve van G_1, minden elemén és tetszőleges $a, b \in G_1$ esetén $\Phi(ab) = \Phi(a)\Phi(b)$ teljesül.

Példa: $(\mathbb{R}^+, \cdot) \simeq (\mathbb{R}^+, +)$, ahol a Φ izomorfizmus minden pozitív valós számhoz hozzárendeli a logaritmusát, azaz $\Phi(a) = log\ a$. A bijektivitás a logaritmus függvény monotonitásából adódik, a művelettartás pedig a $log(ab) = log\ a + log\ b$ összefüggés következménye.

Részcsoport: Legyen G csoport. Egy $H \subseteq G$ részhalmazt **részcsoportnak** nevezünk, ha H is csoport ugyanarra a műveletre nézve. Jelölése: $H \leq G$.

Példa: minden csoportnak részcsoportja maga a csoport, és az egységelemet tartalmazó egyelemű halmaz. Ezeket a részcsoportokat **triviális részcsoportoknak,** az ezektől különböző részcsoportokat **valódi részcsoportoknak** nevezzük.
A háromszög egybevágóságainak (D_3) részcsoportját alkotják a forgatások.

Generált részcsoport: Legyen $K \subseteq G$. K által **generált részcsoportnak** nevezzük és $\langle K \rangle$-val jelöljük a K-t tartalmazó legszűkebb részcsoportot. Ez nem más, mint a K-t tartalmazó részcsoportok metszete.
Pl.: legyen $a \in G$. Ekkor $\langle a \rangle$nyilván tartalmazza aa-t, aaa-t, stb. Az a elem n-szer önmagával vett szorzatát a^n-el jelöljük. Ekkor a hatványozás azonosságai teljesülnek, azaz
$a^{n+k} = a^n a^k$, és $(a^n)^k = a^{nk}$, tetszőleges n, k pozitív egészekre. $\langle a \rangle$ továbbá tartalmazza a^{-1}-et is, valamint ennek hatványait. Tekintsük az $(a^{-1})^n a^n$ szorzatot. Kiírva tényezőnként, azt kapjuk, hogy a szorzat értéke e, a csoport egységeleme, tehát $(a^{-1})^n = (a^n)^{-1}$. Jelöljük ezt az elemet a^{-n}-el. A hatványozás tulajdonságai ezek alapján kiterjeszthetőek negatív hatványokra is:
$a^{k+l} = a^k a^l$, és $(a^k)^l = a^{kl}$ tetszőleges $k, l \in \mathbb{Z}$ esetén. Ezek szerint $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$, azaz egy elem által generált részcsoport az elem (negatív és pozitív kitevős) hatványaiból áll.
Különböztessünk meg két esetet:

1. a összes hatványa különböző.
2. vannak olyan k, l egész számok, hogy $a^k = a^l$. Ekkor $a^{k-l} = 1$, azaz van a-nak olyan hatványa, amely az egységelem. Legyen n a legkisebb ilyen szám.

Rend: Ezt a legkisebb ilyen számot a **rendjének** nevezzük, és o(a) („ordó a") –val jelöljük. Ha nincs ilyen szám, akkor végtelen rendű csoportról beszélünk.

Állítás: egy elem rendje megegyezik az általa generált részcsoport rendjével.

Ciklikus csoport: Az egy elem által generált csoportokat **ciklikus csoportnak** nevezzük, és C_n-el jelöljük.

Mellékosztály: Legyenek *K, M* részhalmazok *G*-ben. A *KM* szorzaton a $KM = \{km | k \in K, m \in M\}$ halmazt értjük. Legyen $H \leq G$ részcsoport, $g \in G$. A *Hg (gH)* szorzatot a H *g* szerinti jobboldali (baloldali) **mellékosztályának,** g-t pedig a mellékosztály **reprezentánsának** nevezzük.

(bocs, de az alábbi szösszenet a Lagrange-tételhez kell…)
Állítás: Legyen $H \leq G$, Ekkor

(1) $g \in Hg$
(2) a Hg mellékosztály minden eleme reprezentálja a Hg mellékosztályt
(3) két különböző jobboldali mellékosztály vagy egybeesik, vagy diszjunktak
(4) ha H véges, akkor bármely mellékosztály elemszáma megegyezik H rendjével.

Biz:

(1) $1 \in H$, így $g = 1g \in Hg$
(2) Legyen $h \in Hg$. Ekkor van olyan $h_1 \in H$, hogy $h = h_1 g$. A tetszőleges $x \in H$-ra érvényes $xh = (xh_1)g$ összefüggés igazolja, hogy $Hh \subseteq Hg$, és $xg = xh_1^{-1}h$ pedig azt, hogy $Hg \subseteq Hh$.
(3) (1)-ből és (2)-ből következik.
(4) A $h_1 g = h_2 g$ egyenlőséget g^{-1}-zel jobbról szorozva kapjuk, hogy $h_1 \neq h_2$ esetén $h_1 g$ és $h_2 g$ különböznek.

Tétel (Lagrange): Legyen G véges, $H \leq G$. Ekkor H rendje osztja G rendjét.

Biz:
Osztályozzuk G-t a H szerinti jobboldali mellékosztályok szerint: $G = \cup Hg$. Jelölje k H mellékosztályainak számát. Mivel minden elem pontosan egy mellékosztályban szerepel, ezért $|G| = |\cup Hg|$ miatt $|G| = \sum |Hg| = k|H|$. A $k = |G| \backslash |H|$ számot H G-beli **indexének** nevezzük, és $|G:H|$-val jelöljük. $|G:H||H| = |G|$.

Következmény: Mivel egy elem rendje megegyezik az általa generált részcsoport rendjével, egy elem rendje osztja a csoport rendjét.

Legyen $|G| = p, p$ prím. ekkor egy egységelemtől különböző csoportelem által generált ciklikus csoport rendje csak p lehet.
Következmény: Minden prímrendű csoport ciklikus.

Tétel (Cayley): Minden csoport izomorf egy permutációcsoporttal.

Biz:
Megmutatjuk, hogy G izomorf S_G egy részcsoportjával, ami azt jelenti, hogy izomorf $S_{|G|}$ egy részcsoportjával is. Tekintsük a $\Phi: G \to S_G$, $h \to \binom{g}{gh}$ megfeleltetést, azaz minden $h \in G$-hez rendeljük hozzá G elemeinek azt a permutációját, amely bármely g-hez annak h-szorosát, gh—t rendeli. Φ valóban a csoportelemek egy permutációja, ehhez azt kell megmutatni, hogy a különböző csoportelemekhez különböző csoportelemeket rendel. Nyilvánvaló, hogy $g_1 h = g_2 h$ esetén $g_1 = g_2$. Ez a megfeleltetés injektív, hiszen minden permutáció mást rendel a csoport egységeleméhez. A leképezés művelettartó, mert

$$\Phi(h_1)\Phi(h_2) = \binom{g}{gh_1}\binom{g}{gh_2} = \binom{g}{gh_1h_2} = \Phi(h_1h_2)$$

Ezzel az állítást igazoltuk.

13) Gyűrű és test fogalma, véges és végtelen példák. Számelmélet és algoritmusok: összeadás, szorzás, maradékos osztás, hatványozás lépésszáma. Modulo *m* hatványozás polinomiális időben.

Gyűrű: Az R halmaz a $+$ és $\cdot$ műveletekkel **gyűrű**, ha
(1) $a+b=b+a, \forall a,b \in R$ esetén;
(2) $(a+b)+c=a+(b+c), \forall a,b,c \in R$ esetén;
(3) van olyan R-beli elem (jelöljük 0-val), hogy $a+0=0+a=a, \forall a \in R$ esetén;
(4) $\forall a \in G$-re $\exists a' \in G$ úgy, hogy $a+a'=0$ (ahol 0 a (3)-ban szereplő elem);
(5) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a,b,c \in R$ esetén;
(6) $(a+b) \cdot c = a \cdot c + b \cdot c \quad \forall a,b,c \in R$ esetén;
(7) $c \cdot (a+b) = c \cdot a + c \cdot b \quad \forall a,b,c \in R$ esetén;

Az első négy axióma mondja ki, hogy R Abel-csoport az összeadásra nézve, az ötödik pedig, hogy félcsoport a szorzásra nézve. A hatodik, illetve hetedik axiómákat a jobboldali illetve baloldali **disztributív** törvényeknek nevezzük. Ha a szorzás is kommutatív, **kommutatív gyűrűről**, ha van a szorzásra nézve egységelem, **egységelemes gyűrűről** beszélünk. A harmadik axiómában említett elem a **nullelem.** A negyedik axiómában említett a'-t a **ellentetjének** hívjuk, és $-a$-val jelöljük. Az $a-b=a+(-b)$ művelet a **kivonás**.
A fenti axiómák következményei:
(1) a nullelem és az ellentett egyértelmű;
(2) $0a=a0=0$;
(3) $(-a)b=-ab$;
(4) $(-a)(-b)=ab$.

Példák:
1. Az egész számok kommutatív, egységelemes gyűrűt alkotnak a szokásos összeadásra és szorzásra ($\mathbb{Z}$).
2. Az m-mel osztható egész számok kommutatív gyűrűt alkotnak a szokásos műveletekre.
3. A racionális, a valós, a komplex számokt kommutatív, egységelemes gyűrűt alkotnak a szokásos műveletekre.

Test: Egy R egységelemes gyűrűt **ferdetestnek** hívunk, ha a szorzásra nézve is van inverz, azaz $\forall 0 \neq a \in R$-hez $\exists a' \in R$, hogy $aa'=1$. Egy ferdetestet **testnek** hívunk, ha a szorzás kommutatív.

Példák:
1. A racionális, a valós illetve a komplex számok ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) testet alkotnak a szokásos műveletekre.
2. Az $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ alakú valós mátrixok testet alkotnak a mátrixműveletekre.

Definíció: Egy algoritmust **polinomiálisnak** nevezünk, ha lépésszáma a bemenet méretének polinomjával felülről becsülhető. Persze a bemenet mérete függ a számrendszer megválasztásától, általában decimális, bináris, vagy hexadecimális számrendszereket alkalmazunk. Egy n és egy m szám együttes mérete $\log n + \log m$ lesz, a kéréds tehát, hogy ennek a számnak milyen függvénye egy-egy művelet lépésszáma.

Összeadás: A közismert „írásbeli összeadás” minden számrendszerre jól működik. A műveletigény minden helyiértéknél legfeljebb 2, hisz két számot adunk össze az adott helyiértéken, néha az esetleges maradékot az előző helyiértékből. A lépésszám felső korlátja tehát a $2 \cdot \max(\log n, \log m) < 2 \cdot (\log n + \log m)$, ami lineáris, vagy polinomiális. A kivonásra ugyanez igaz.

Szorzás: a szokásos írásbeli szorzás működik, és megvalósítható $\log n$ darab összeadással, ahol minden összeadandó az m egy egyjegyű számmal összeszorzott többszöröse. Egy egyjegyű számmal m-t $2 \log m$lépésben össze lehet szorozni, hisz minden jegyet szorzunk, és az estleges előző helyiértékes maradékot hozzáadjuk. Tehát az összlépésszám $2(\log n)(\log m) \leq (\log n + \log m)^2$, vagyis a szorzás polinomiális. Az írásbeli osztás is polinom időben elvégezhető, de a soron következő hányados becslésénél kicsit tökölni kell.

Hatványozás: az n^mszám hossza kb $m \log n$, ami nem polinomiális függvénye $(\log n + \log m)$-nek. Mivel az algoritmus egy lépésben legfeljebb egy (pontosabban konstans számú) jegyét tudja kiírni az eredménynek, már az eredmény megadása is exponenciálisan sok időt igényel, azaz általában nem lehet polinomiális algoritmussal hatványozni.

Hatványozás mod m: Az input n, k és m, a cél pedig $n^k(m)$ meghatározása.
Legyen $k = \sum_i k_i 2^i$, azaz $k = \underline{\ldots k_2 k_1 k_0}_2$ a kettes számrendszerbeli alak. Sorra kiszámoljuk az $n_0, n_1, n_2, \ldots$ 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}-t 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 legfeljebb egy $\log m$ méretű szám négyzetre emelését, és a 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 $n^k = \prod_{i=1}^{\infty} n^{k_i 2^i} \equiv \prod_{i=1}^{\infty} n^{k_i}(m)$ alapján további, legfeljebb $\log k$darab, legfeljebb $\log m$ méretű szám szorzásával, és $\log k$ darab, legfeljebb $2 \log m$ méretű szám maradékos osztásával kapjuk. A mod m hatványozás tehát összességében is polinomiális.

Bónusz:
Euklideszi algoritmus: Az euklideszi algoritmus egy lépésében adott $r_{i+1} \leq r_i$ esetén kell egy maradékos osztást végezni, és meghatározni azt a $0 \leq r_{i+2} < r_{i+1}$-t, melyre $r_i = q_{i+1} \cdot r_{i+1} + r_{i+2}$ áll. Az r_i mérete legfeljebb akkora, mint r_0 és $r_1$mérete közül a nagyobbik, tehát minden lépés polinomiális időt igényel. A trükk, hogy $r_{i+2} \leq \frac{r_i}{2}$, ezért a fentieket legfeljebb $\log r_0$-szor kell elvégezni, amitől az eljárás polinomiális marad.

14) Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosírás és digitális aláírás fogalma, megvalósításuk RSA-kódolás segítségével.

Prímtesztelés: ami matematikailag korrekt, az ennek megfelelően bazinehéz, úgyhogy felejtsük is el. Van egy másik algoritmus helyette, amivel annyi a probléma, hogy mivel véletlen választást is megenged, az eljárás nem lesz tévedhetetlen (de, ez elhanyagolható). Szóval, ezen eljárás alapja az Euler-Fermat tétel (ld. 10. tétel). Eszerint, ha egy n szám prím, akkor $k^{n-1} \equiv 1(n)$, minden $(k,n) = 1$ esetén. Ha tehát $(k,n) = 1$és $k^{n-1} \not\equiv 1(n)$, akkor bizonyosan tudjuk, hogy n összetett, annak ellenére, hogy egyik osztóját sem ismerjük . Az ilyen k számot az n szám **árulójának** nevezzük, hiszen ezzel megtudtuk, hogy n nem prím. Egy másik lehetőség meggyőződni n összetettségéről, hogy találunk egy olyan $0 < k < n$ számot, amire $(k,n) \neq 1$. Ekkor az euklideszi algoritmus az n egy valódi oszóját is megtalálja, ezért k még további információt ad n ről. Az ilyen k számok az n **leleplezői.** Mint ahogyan az árulókra, úgy a leleplezőkre is igaz, hogy $k^{n-1} \not\equiv 1(n)$,hiszen k^{n-1} nem relatív prím n-hez, ha k sem volt az, tehát nem lehet a redukált maradékrendszer eleme sem. Viszont, olyan is lehet, hogy n összetett, és egy $0 < k < n$ számra $k^{n-1} \equiv 1(n)$ áll. Ekkor k az n szám **cinkosa**, hisz nem árulja el, hogy n összetett. Igaz viszont, hogy ha van áruló, akkor az $1,2,\dots,n-1$ számok között legalább annyi áruló van, mint cinkos (és akkor a leleplezőkről még nem is beszéltünk).

Lehetséges prímtesztelési módszer: véletlenül választunk egy $0 < k < n$ számot. Ha k árulója, vagy leleplezője n-nek, azaz $k^{n-1} \not\equiv 1(n)$, akkor kész vagyunk, n összetett. Ha k cinkos, akkor n-ről azt valószínűsítjük, hogy prím. Ezen alapszik a **Fermat-teszt.**

Fermat-teszt:
Input: $n \in \mathbb{N}$. Output: döntés, hogy n prím-e.
begin
Legyen $0 < k < n$ véletlen szám
if $k^{n-1} \not\equiv 1(n)$ *then STOP:* n nem prím.
else STOP: úgy tűnik, n prím.
end if
end
(ezen eljárás nagy hibája, hogy csak akkor működik, ha n-nek létezik árulója).

Carmichael számok: olyan számok, amiknek csak cinkosai, és leleplezői vannak (utóbbiak elenyésző számban). Azaz, olyan kitevőkről beszélünk, melyek minden, hozzájuk relatív prím, de egyébként tetszőleges alaphoz álprímek (olyan$n$-ek, amelyekre $(k,n) = 1$, és $k^{n-1} \not\equiv 1(n)$ igaz, és mégsem prímek).