Bevezetés a Számításelméletbe II. vizsgatételek
(2007/2008. második félév)

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.

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

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).

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.

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

6. Páros gráf fogalma, karakterizációja. Párosítások páros gráfban, a javítóutas módszer. Kőnig, Hall és Frobenius tételei.

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.

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).

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

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

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

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

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

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

(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

H-kör: Egy G gráfban Hamilton-körnek nevezünk egy H-kört, ha G minden pontját (pontosan egyszer) tartalmazza

(2.)

Egy utat H-útnak nevezünk, ha G minden pontját pontosan egyszer tartalmazza.

(3.)

Ha a G gráfban létezik k darab olyan pont, amelyeket elhagyva a gráf több mint k komponensre esik szét, akkor nem létezik G-ben Hamilton kör. Ha létezik k darab olyan pont melyeket elhagyva G több mint k+1 komponensre esik szét, akkor nem létezik G-ben Hamilton út. SZÜKSÉGES FELTÉTEL

(4.)

Vesszük azt a k darab csúcsot melyek elhagyásával G több mint k komponensre esik szét. Az elhagyott pontok közötti részen az esetek Hamilton kör élei futnak így ezek már nem összefüggőek. Ilyen „mellől" k darabot kapunk. Vagyis G nem eshet szét k-nál több komponensre

Ha G Hamilton-gráf, akkor minden pontjának fokszáma legalább 2.

ELÉGSÉGES FELTÉTELEK

DIRAC: Ha az n-pontú ($n \geq 3$), egyszerű G gráf minden pontjának foka legalább $\frac{n}{2}$ akkor G-nek van H-köre.

ORE → DIRAC

ORE: Ha az n-pontú ($n \geq 3$), egyszerű G gráf olyan, hogy $uv \notin E(G)$ esetén $d(u) + d(v) \geq n$ (azaz összetételben csúcsok fokszámösszege legalább n) akkor G-ben ∃ H-kör

Egy G gráf Euler körének nevezünk egy zárt élsorozatot, ha az élsorozat pontosan egyszer tartalmazza G összes élét. Ha az élsorozat nem feltétlenül zárt akkor Euler-utat kapunk.

(1.) Egy G gráfban akkor van E-kör, ha G minden pontjának fokszáma páros és G ö.f.

(2.) → Ha az E-kör vonalán körüljárjuk a gráfot, akkor minden pontba ha bemegyünk akkor ki is megyünk belőle egy másik még nem járt élen. Öf volt különben nem lehetett volna benne E-kör

(3.) Ha a véges G gráfnak létezik E-köre, akkor G minden csúcsának páros a fokszáma. Ha G-ben létezik E-út akkor G-nek 0 v. 2 pl fokú csúcsa van.
G-nek pontosan akkor van E-körsétája, ha G minden csúcsa páros fokú
G-nek pontosan akkor van E-sétája, ha G-nek 0 v. 2 páratlan fokú csúcsa van.

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

---

D: A G gráf, k színnel színezhető, ha G minden csúcsa kiszínezhető k adott szín valamelyikére úgy, hogy G bármely élének két végpontja különböző színű legyen.

D: A G gráf kromatikus száma $\chi(G)=k$, ha G kiszínezhető k színnel de $k-1$ színnel még nem. Egy ilyen színezésnél az azonos színt kapott pontok halmazát színosztálynak nevezzük.

D: G gráf klikkje a G teljes részgráfja. A gráf $\omega(G)$-vel jelölt klikkszáma G legnagyobb klikkjének pontszáma, azaz a legnagyobb olyan k szám, melyre létezik G-ben k páronként összekötött csúcs, de $k+1$ már nem létezik.

T: Minden irányítatlan véges G gráfra $\omega(G) \le \chi(G) \le \Delta(G)+1$ valamint $\chi(G) \ge \frac{n}{\alpha(G)}$ teljesül, ahol n a G csúcsainak számát jelenti.

B: G pontjainak kiszínezésével a maximális klikk pontjait is kiszínezzük, mégpedig különböző színekkel, ~~ahol n a G csúcsainak számát jelenti~~. Ebből világos az első egyenlőtlenség.

Másrészt az ún. mohó színezés mutatja, hogy bármely G gráf $(\Delta(G)+1)$ színezhető. Színezzük ki G pontjait $v_1, v_2, \dots, v_n$ sorrendben úgy, hogy az i-edik lépésben v_i-t olyan színre színezzük, ami nem szerepel v_i kiszínezett szomszédain. Mivel v_i-nek legfeljebb $\Delta(G)$ kiszínezett szomszédja lehet és mindegyik szomszéd legfeljebb egy-egy színt zár ki, v_i színezése elvégezhető a rendelkezésre álló színek valamelyikével. v_n kiszínezése után G egy $(\Delta(G)+1)$ színezését kapjuk, ami a második egyenlőtlenséget igazolja.

A tétel második része azért igaz, mert ha G-t kiszínezzük $\chi(G)$ színnel akkor minden egyes színosztály legfeljebb $\alpha(G)$ méretű, kis független pontokból áll. Ezek szerint G csúcsait $\chi(G)$ darab legfeljebb $\alpha(G)$ méretű halmaz uniójára bontottuk, ahonnan $n \le \chi(G) \cdot \alpha(G)$ és innen az állítás közvetlenül adódik.

Brooks tétele: Legyen G véges egyszerű, irányítatlan gráf. Ha G nem teljes gráf és nem páratlan kör akkor $\chi(G) \le \Delta(G)$

Mycielski konstrukció: Tetszőleges $k \ge 2$ pozitív egészhez létezik olyan G gráf melyre $\chi(G)=k$ és $\omega(G)=2$

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

Síkbarajzolható gráfok kromatikus száma:

T: 5-szín tétel: Ha G sr. gráf, akkor $\chi(G) \leq 5$ TK 84. oldal.

B: A gráf pontszámára vonatkozó indukcióval bizonyítunk. Mivel a párhuzamos élek nem befolyásolják a színezést, feltehetjük, hogy a gráf egyszerű. 2 pontú gráfra nyilván igaz az állítás. G éleinek száma legfeljebb $3n-6$ ahol $n = |V(G)|$. Így biztosan van egy olyan x pont amelynek foka legfeljebb 5, hiszen ha minden pont foka legalább 6, akkor az élek száma legalább $\frac{1}{2} 6n$ volna ami ellentmondás. Ha x foka legfeljebb 4, akkor az indukciós feltevés miatt x-et elhagyva kiszínezhető a gráf 5 színnel, majd x-et a 4 szomszédjától eltérő 5. színnel színezzük ki.
Tegyük most fel, hogy $d(x) = 5$. Ha x-nek bármely két szomszédja között van él, akkor a gráfban egy K_5 részgráf szerepel, ami ellentmond G síkbarajzolhatóságának. Tehát x két szomszédját, y és z nem összekötve. Húzzuk össze egy ponttá az x, y és z pontokat. Az így kapott G' gráf az indukciós feltevés miatt kiszínezhető 5 színnel. Az ennek megfelelő színezés G-ben nem jó csupán x, y, z eggyéválnak. G-ben x-nek három szomszédja van y-on és z-n kívül. Ezek legfeljebb három színt foglalnak le és tovább két szomszédja, y és z egyszínű. Marad tehát az 5. szín amellyel kiszínezhetjük x-et. Tehát G kiszínezhető 5 színnel.

T: 4-szín tétel: Ha G s.r. gráf, akkor $\chi(G) \leq 4$

$\chi(G) = \omega(G)$

D: A G véges gráf perfekt, ha G minden feszített G' részgráfjára $\chi(G') = \omega(G')$ teljesül

T: Minden páros gráf perfekt

T: Minden ps gráf komplementere ps, tehát perfekt gráf

T: Minden ps gráf élgráfja perfekt

T: Minden ps gráf élgráfjának a komplementere perfekt.

D: G intervallumgráf, csúcsai I_1, I_2 valós intervallumok és akkor van összekötve, ha a két intervallum metszi egymást.

T: Minden intervallumgráf perfekt.

Lovász tétel: A G gráf perfekt $\Leftrightarrow$ G minden G' feszített részgráfjára $\alpha(G') \cdot \omega(G') \geq |V(G')|$

Gyenge perfekt gráf tétel: Ha G perfekt, akkor és csak akkor $\bar{G}$ is perfekt.

Erős perfekt gráf tétel: G perfekt $\Leftrightarrow$ G-nek nincs feszített részgráfja ami ≥ 5 hosszú ptl kör vagy ilyenek komplementere

Egy G véges gráf pontosan akkor perfekt, ha sem G, sem $\bar{G}$ nem tartalmaz legalább 5 hosszú, páratlan kört.

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

D: A G gráf k-élszínezhető, ha G élei k színnel színezhetők úgy, hogy szomszédos élek különböző színt kapnak. A G gráf élkromatikus száma $\chi'(G) = \chi(G) = k$, ha G k-élszínezhető de G nem $(k-1)$ színezhető

A: Tetszőleges G gráfra $\chi'(G) \geq \Delta(G)$ áll.

B: Az egy csúcsból induló élek egymástól különböző színt kapnak és ez speciálisan a maximális fokszámú csúcsból induló élekre is igaz. Formálisan: $\chi'(G) = \chi(L(G)) \geq \omega(L(G)) \geq \Delta(G)$

Vizing tétele: Ha G véges egyszerű gráf akkor $\chi'(G) \leq \Delta(G) + 1$

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

D: Hálózatnak nevezünk egy olyan (G, s, t, c) négyest, amelyben G egy irányított gráf amiben s és t különböző csúcsai, továbbá G minden e élét jellemzi egy nemnegatív c(e) szám, az él ún. kapacitása

D: A (G, s, t, c) hálózatban folyamnak mondunk egy olyan f függvényt, mely G minden élhez egy számot rendel úgy, hogy

-1) $0 \le f(e) \le c(e)$ teljesül G minden élére, továbbá

-2) $\sum\{f(uv) : u \in V(G)\} = \sum\{f(vu) : u \in V(G)\}$ áll G minden s-től és t-től különböző v csúcsára.

Az első kapacitás-feltétel azt fejezi ki, hogy a folyam minden élen legfeljebb kapacitásnyi lehet, a második ún. Kirchoff-szabály azt mondja ki, hogy minden s-től és t-től különböző v csúcsba a belépő folyam összmennyisége azonos a kilépő összmennyiséggel, tehát folyamnál tehát egyetlen csúcsban sem keletkezik vagy tűnik el folyadék. A név eredete is utal, hogy a hálózati folyam fogalma az elektromos hálózatok elméletében is hasonló szerepet kap.

Legyen G egy irányított gráf. Rendeljünk minden élhez c(e) nemnegatív valós számot, amit az él kapacitásának nevezünk. Jelöljünk ki továbbá két s, t pontot G-ben melyeket termelőnek illetve nyelőnek hívunk.)

Egy élet telítettnek hívunk egy folyamban, ha $f(e) = c(e)$
és telítetlnek ha $f(e) < c(e)$

D: Az f folyam m_f folyam nagysága az a nettó folyammennyiség, ami s-ből kifolyik:

$$m_f := \sum\{f(sv) : v \in V(G)\} - \sum\{f(vs) : v \in V(G)\}$$

Rendszerint nincs az arra, hogy s-be folyam érkezzen, hiszen annak nincs többet alatta kijuttatni, de általában nem zárhatjuk ki ezt a lehetőséget sem. Az s-t elhagyó összfolyammennyiség kiszámításához tehát le kell vonni azt ami s-be érkezik.

D: Legyen X a G csúcsainak egy s-t tartalmazó, de t-től diszjunkt részhalmaza. Az X és $V(G) \setminus X$ között futó élek halmazát a hálózat egy s-t-vágásának nevezzük. Az X által meghatározott st-vágás kapacitása az X-ből $V \setminus X$-be futó élek kapacitásösszege azaz $\sum\{c(xy) : x \in X \not\ni y \in V(G)\}$

Ford Fulkerson: maximális folyamérték = minimális s-t vágás
Ha (G, s, t, c) egy véges hálózat, akkor létezik egy f folyam és egy $s \in X \subseteq V(G) \setminus \{t\}$ részhalmaz úgy hogy az m_f folyamnagyság azonos az X által definiált st-vágás kapacitásával

Edmonds Karp tétel: Ha a (G, s, t, c) hálózatban a maximális folyamot a javítóutas algoritmussal keressük és mindig egy lépésben élből álló javító út mentén növelünk akkor a maximális folyam meghatározásához szükséges lépésszám felülről becsülhető |V(G)| polinomjával.

Egészértékűségi lemma: Ha a hálózatban minden kapacitás egész, akkor létezik olyan max folyam ami minden élen egész értéket vesz fel.

B) Az állítás nyilvánvaló, hiszen a kiindulásnál azonosan 0 folyam rendelkezik a kívánt tulajdonságokkal, majd az algoritmus során minden lépésben a folyamértékek minden élen csak egész számmal változhatnak.

Folyamprobléma általánosítása

- Nem egy forrás/nyelő van — Felveszünk egy super forrást/nyelőt és ebbe belekötjük az összes forrást/nyelőt. Ezzel nem változik a kapacitása.
- Pontkapacitás — pontból csinálunk egy élet. A pontba bemenő élek az új élbe belemennek, amik kifelé mutatók élek, arról az élből vezetnek ki. Az eredeti pont kapacitása lesz az új él kapacitása
- Oda-vissza élek / irányítatlan élek. Az irányítatlan él helyett berakunk egy oda és egy vissza élet, ezeknek a kapacitása megegyezik az eredeti irányítatlan élével

5) Menger tételei. Többszörös összefüggőség és élösszefüggőség. Dirac tétele (bizonyítással)

D) A G irányított vagy irányítatlan gráf u pontjából v pontjába futó P és Q utjait élidegennek vagy élidegen utaknak (pontidegennek vagy pontidegen utaknak) nevezzük, ha $E(P) \cap E(Q) = \emptyset$ (ill. $V(P) \cap V(Q) = \{u, v\}$)

D) Azt mondjuk, hogy a G (irányított vagy irányítatlan) gráf U ponthalmaza (ill. F élhalmaza) lefog minden u-v utat, ha a $G-U$ (ill $G-F$) gráfban nem létezik u-ból v-be (irányított) út.

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

B) Ha létezik G-ben k darab ilyen irányított s-t út, akkor az s-t utakat lefogó élek száma nyilvánvalóan legalább k. Tehát $\max\{\} \leq \min\{\}$. Most lássuk a fordítottját. Tegyük fel, hogy az s-t utakat lefogó élek minimális száma ℓ. 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 látjuk már, hogy van olyan maximális folyam, melyben minden élen a folyam értéke 0 vagy 1. Lássuk be, hogy G-ben van k élidegen irányított s-t út. Egy ilyen út mindenképpen van, hiszen különben nem lehetne k a folyam értéke. Az ebben az utban 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 k élidegen irányított s-t utat kapunk.

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

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

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

D) Az irányítatlan G gráfot k-szorosan (pont)összefüggőnek nevezzük, ha G-nek legalább $(k+1)$ pontja van, és G öf marad, bárhogyan is hagyunk el belőle legfeljebb $k-1$ pontot. A maximális k-t, amire G k-öf marad $\kappa(G)$ jelöli

D) A G irányítatlan gráfot k-szorosan élösszefüggőnek nevezzük, ha G öf marad bárhogyan is hagyunk el belőle legfeljebb $k-1$ élt. A maximális k-t amire G k-élöf $\lambda(G)$ jelöli

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

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

Ⓓ 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. Ennek jelölése: $G=(A,B)$. 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

Ⓣ Egy G gráf akkor páros gráf, ha minden G-ben levő kör páros hosszúságú

Ⓓ Párosításnak, vagy élfüggetlen élhalmaznak nevezünk egy M élhalmazt, ha semelyik két élének 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.

Ha van egy olyan P út, ami egy $A-X$-beli pontból indul egy $B-X$-beli pontban végződik és minden második éle M-beli, de a többi nem M-beli, akkor növelhetjük a párosítást, 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

Hall tétel: A $G=(A,B;E)$ páros gráfban akkor van A-t lefedő párosítás, ha minden $X_0 \subseteq A$ részhalmazra $|N(X_0)| \geq |X_0|$

Ⓑ A szükségesség nyilvánvaló: ha létezik A-t fedő 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.
Az elégségességhez tegyük fel, hogy $|X| \leq |N(X)|$ minden $X \subseteq A$-ra. Azt kell igazolnunk, hogy $\nu(G) \geq |A|$. Legyen U minimális (azaz $\tau(G)$ méretű) lefogó ponthalmaz, és legyen $U_A := U \cap A$, $U_B := U \setminus B$. Mivel U lefogja az $X := A \setminus U_A$-ból induló éleket, ezért $N(X) \subseteq U_B$ tehát $|N(X)| \leq |U_B|$. A König tétel illetve a Hall feltétel miatt:
$\nu(G) = \tau(G) = |U| = |U_A| + |U_B| \geq |U_A| + |N(X)| \geq |U_A| + |X| = A$

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

Ⓑ 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.

$\alpha(G)$ = független pontok max száma
$\nu(G)$ = független élek max száma
$\tau(G)$ = lefogó pontok minimális száma
$\varrho(G)$ = lefogó élek minimális száma

König tétel: Ha $G=(A,B)$ páros gráf, akkor $\nu(G) = \tau(G)$.
Ha nincs G-ben izolált pont akkor $\alpha(G) = \varrho(G)$

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

Tutte tétel: Egy G gráfban akkor és csak akkor létezik teljes párosítás, ha minden $X \subseteq V(G)$-re $q(G-X) \leq |X|$, azaz akárhogy hagyunk el a gráfból néhány pontot a maradékban a páratlan komponensek száma ennél több nem lehet.

alfa: $\alpha(G)$: fleny pontok max száma — tau: $\tau(G)$: lefogó pontok minimális száma
nű: $\nu(G)$: fleny élek max száma — ró: $\rho(G)$: lefogó élek minimális száma

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

(B) Egy X halmaz pontjai akkor és csak akkor flenek, 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 hurokból különböző élet, akkor X-ben ennek az élnek mindkét végpontja szerepel. Tehát $\tau(G) \leq |V(G)-X|$ teljesül minden X fleny ponthalmazra. Ebből pedig következik, hogy $\tau(G) + \alpha(G) \leq |V(G)|$. Hasonlóan $\alpha(G) \geq |V(G)-Y|$ minden Y lefogó ponthalmazra, amiből $\tau(G) + \alpha(G) \geq |V(G)|$ következik

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

Nincs teljes párosítás:
- ha ptl sok csúcs van
- ha 2 ptl komponense van a gráfnak
- ha el tudunk úgy hagyni k csúcsot, hogy k-nál több ptl komponens keletkezik.

Páros gráfban $\alpha(G) = \rho(G)$ ha nincs izolált pont
$\nu(G) = \tau(G)$

(D) Egy n pontú gráf mátrixszal való reprezentálásának egyik legtermészetesebb módja ha definiálunk egy $n \times n$-es $A(G) = (a_{ij})$ mátrixot 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 gráfokkal is megadhatunk ilyen módon, csak ott a_{ij} az i-edik pontból a j-edik pontba vezető élek száma. Ezt az $A(G)$ mátrixot a G gráf szomszédossági mátrixának nevezzük.

(T) Nyilvánvaló, hogy a szomszédossági 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 pontot, vagy akár élen többször átmenő sorozatokat is

D Legyen az n-pontú G gráfnak e éle és definiáljuk az $n \times n$-es $B(G) = (b_{ij})$ mátrix elemei úgy, hogy:

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

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, csak ott a j-edik él mindkét végpontjának megfelelő mátrixelem 1. Ezt a $B(G)$ mátrixot a G gráf <u>illeszkedési mátrixának</u> nevezzük.

T Az n pontú, c darab öf komponensből álló, hurokélmentes irányított G gráf illeszkedési mátrixának rangja $n - c$.

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

Def: Az a, b egész számokról azt mondjuk, hogy a b-t osztja, illetve b az a többszöröse (jelölése $a|b$) ha $b = aq$, valamely q egész számra. Világos, hogy $n \neq 0$ esetén $1 | 1$ és $n | n$, ezek az n triviális osztói. Az n-nek osztóit, amelyek nem triviálisak, valódi osztóinak nevezzük.

D) A $p \in \mathbb{Z}$ szám felbonthatatlan, ha $|p| \neq 1$ és p-t csak triviális módon tudjuk egészek szorzataként előállítani, azaz $p = ab$ ($a, b \in \mathbb{Z}$) esetén $|a| = 1$ vagy $|b| = 1$. Ugyanezt úgy is mondhatjuk, hogy p akkor felbonthatatlan, ha p-nek csak triviális osztói vannak, és $p \neq 1$ illetve $p \neq -1$.

D) 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 előjelekben különbözhetnek.

D) A $p \in \mathbb{Z}$ szám prím, ha tetszőleges $a, b \in \mathbb{Z}$-re teljesül, hogy $p | ab \Rightarrow p | a$ vagy $p | b$. Szavakban: egy szám akkor prím, ha csak úgy tud osztani egy szorzatot, ha a szorzat valamelyik tényezőjét osztja. A számelmélet alaptételének fontos következménye a prím és a felbonthatatlan ugyanazokat a számokat jelenti:

Tétel: 1) Ha a p egész szám prím, akkor p felbonthatatlan.
2) Ha a p egész szám felbonthatatlan akkor p prím.

D) Legyen $a, b \in \mathbb{Z}$ olyan, hogy $a \neq 0$ vagy $b \neq 0$ teljesül. Az a és b számok (a,b)-vel jelölt legnagyobb közös osztója a legnagyobb olyan szám, mely osztója a-nak és b-nek is. Az a, b számokat relatív prímeknek mondjuk ha $(a,b) = 1$ (közös prímtényezőik a legkisebb hatványon)

D) Legkisebb közös többszörös: (összes prímtényező a legnagyobb hatványon)

Euklidészi algoritmus: Input a, b egészek (mondjuk $b \leq a$). Output (a,b)
Legyen $a_0 := a$, $a_1 := b$. Ha már meghatároztuk az $a_0 \geq a_1 \geq \ldots \geq a_i$ számokat, akkor legyen $a_{i-1} = q_i a_i + a_{i+1}$ azaz osszuk el maradékosan a_{i-1}-t a_i-vel és legyen a_{i+1} a maradék, amire tehát $0 \leq a_{i+1} < a_i$ teljesül. Az eljárás akkor ér véget ha $a_{k+1} = 0$. Ekkor az algoritmus válasza $(a,b) = a_k$

Osztók száma: $d(n) = \prod (a_i + 1)$

Osztók összege: $\sigma(n) = \prod \frac{p_i^{a_i+1} - 1}{p_i - 1}$

(T) A prímszámok száma végtelen

(B) Elegendő azt megmutatni, hogy minden $2 \leq n \in \mathbb{N}$-re létezik n-nél nagyobb prímszám. Mivel $n!$ az $1, 2, \ldots, n$ számok mindegyikével osztható ezért $N := n! + 1$ az $1, 2, \ldots, n$ 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.

(T) Tetszőleges hosszú sorozat képezhető szomszédos összetett számokból azaz bármely $n \in \mathbb{N}$-re létezik olyan N, melyre az $N+1, N+2, \ldots N+n$ számok mindegyike összetett.

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

Dirichlet tétel: Ha a és d relatív prímek, akkor az $a, a+d, a+2d, \ldots$ számtani sorban végtelen sok prím fordul elő.

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

(D) $a, b, m \in \mathbb{Z}$, $0 < m$ esetén azt mondjuk, hogy a a kongruens b modulo m (jelölése $a \equiv b \pmod m$), ha $m \mid a-b$

Tulajdonságok
- reflexív $a \equiv a \pmod m$
- szimmetrikus $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$
- tranzitív $a \equiv b \pmod m$ és $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$
- m szerinti ekvivalencia osztály – maradék
- $a \equiv b \pmod m \Rightarrow a+c \equiv b+c \pmod m$
- $a \equiv b \pmod m \Rightarrow a-c \equiv b-c \pmod m$
- $a \equiv b \pmod m \Rightarrow a \cdot c \equiv b \cdot c \pmod m$
- $a \equiv b \pmod m \Rightarrow a \cdot c \equiv b \cdot c \pmod{mc}$ $\quad c \neq 0$

(PÉ) $2 \equiv 17 \pmod 5$ A 2-vel kongruens számok modulo 5 a $2, 7, 12, 17, 22, \dots$ ill. $-3, -8, -13, -18, \dots$

Tetszőleges $m \geq 2$ egész esetén az egész számok halmaza m diszjunkt osztály uniójára bontható fel, mégpedig úgy, hogy $0 \leq i \leq m-1$ esetén az i-edik osztályban az $k \cdot m + i$ alakú számok vannak, ahol k végigfut az egészeken. (Más szóval, az i-edik osztályba az m-mel osztva i maradékot adó számok tartoznak.) Ezeket az osztályokat az m szerinti (vagy másképpen modulo m) maradékosztályoknak nevezzük.

A maradékosztályok jelentősége az, hogy ha két szám azonos maradékosztályba esik (modulo m) akkor kongruensek egymással modulo m, ha pedig különböző maradékosztályokból valók akkor nem kongruensek.

(A) 1) Ha $a \equiv b \pmod m$ és $c \equiv d \pmod m$ akkor $a+c \equiv b+d \pmod m$ és $ac \equiv bd \pmod m$, azaz két kongruencia összeadható és összeszorozható

2) Ha $d \mid a$ és $d \mid b$ és $a \equiv b \pmod m$, akkor $\frac{a}{d} \equiv \frac{b}{d} \left(\frac{m}{(m,d)}\right)$, azaz kongruencia osztásakor nemcsak a kongruencia két oldalát osztjuk, hanem a modulust is (az osztó és a modulus LNKO-val)

(B) 1) Tudjuk, hogy $m \mid a-b$ és $m \mid c-d$. Ezért $m \mid a-b+c-d = a+c-(b+d)$, azaz $a+c \equiv b+d \pmod m$. Az is igaz, hogy $m \mid c(a-b) + b(c-d) = ac - bd$ azaz $ac \equiv bd \pmod m$

2) Legyen $a = a'd$, $b = b'd$, $D = (m,d)$, $d = d'D$ és $m = m'D$. Ekkor az $a \equiv b \pmod m$ kongruencia $a'd'D \equiv b'd'D \pmod{m'D}$ alakot ölt, ami definíció szerint azt jelenti, hogy $m'D \mid a'd'D - (a'-b')d'D$, azaz $m' \mid (a'-b')d'$ adódik. Mivel D az m és d legnagyobb közös osztója, ezért az $m' = \frac{m}{D}$ és a $d' = \frac{d}{D}$ számoknak már nem lehet közös prímosztójuk. Tehát $m' \mid a'-b'$ is igaz, ami éppen azt jelenti, hogy $a' \equiv b' \pmod{m'}$ azaz $\frac{a}{d} \equiv \frac{b}{d} \left(\frac{m}{(m,d)}\right)$

Kör: 1) Az $a \equiv b \pmod m$ kongruencia pontosan akkor teljesül, ha $a+\varepsilon \equiv b+\varepsilon \pmod m$

2) Ha d relatív prím az m-hez, akkor az $a \equiv b \pmod m$ kongruencia ekvivalens a $ad \equiv bd \pmod m$ kongruenciával, tehát kongruencia mindkét oldalát csak akkor ekvivalens átalakítás, ha a modulushoz relatív prím számmal szorzunk.

3) Az $d > 0$ rögzített egész, akkor az $a \equiv b \pmod m$ kongruencia ekvivalens a $ad \equiv bd \pmod{md}$ kongruenciával.

Műveletek: $a+c \equiv b+d \pmod m$ $\quad ac \equiv bd \pmod m$

$a-c \equiv b-d \pmod m$ $\quad a^2 \equiv b^2 \pmod m$

① Lineáris kongruencián egy $ax \equiv b \ (m)$ kongruenciát értünk, ahol a és b adott egészek, m pedig adott pozitív egész. (Az $m=1$ esetet nem túl izgalmas, általában $m \geq 2$-vel fogunk foglalkozni.) A lineáris kongruencia megoldása azt jelenti, hogy meghatározzuk mindazon egészeket, melyeket x helyébe írva a kongruencia igaz lesz.

Ⓣ Az $ax \equiv b \ (m)$ kongruencia $a \neq 0$ esetén pontosan akkor oldható meg, ha $(a,m) \mid b$
A kongruencia megoldáshalmaza (a,m) darab maradékosztály modulo m

Euklideszi algoritmus:
2 szám LNKO kiszámítására használjuk.
- ha az egyik szám osztja a másikat pl $x \mid y$ akkor $(x,y) = x$
- ha nem osztják egymást és mondjuk x a nagyobbik, akkor el maradékosan y-nal $x = y \cdot q + r$, ahol $0 < r < y$. Ekkor $(x,y) = (y,r)$, így a problémát kisebb számokra vezettük le (kisebb nem LNKO meghatározásáig)
- addig hajtjuk ezt végre amíg 0-t nem kapunk maradéknak. Az LNKO a 0 előtti maradék

Pl $a, b \in \mathbb{Z} \quad b \neq 0$

$a = b q_1 + r_1 \quad 0 \leq r_1 \leq |b|$
$b = r_1 q_2 + r_2 \quad 0 \leq r_2 \leq r_1$
$r_1 = r_2 q_3 + r_3 \quad 0 \leq r_3 \leq r_2$

360 és 225 LNKO-ja
$360 = 1 \cdot 225 + 135$
$225 = 1 \cdot 135 + 90$
$135 = 1 \cdot 90 + (45)$
$90 = 2 \cdot 45 + 0$

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

(D) Legyen $m>1$ 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 $RC\geq$ 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 $\varphi(m)$-mel jelöljük

$\varphi(m)$: 1 és m közé eső m-hez relatív prím számok száma.

$\varphi(p) = p-1$ (mivel prím)

$\varphi(m) = m \cdot \prod \left(1-\frac{1}{p_i}\right)$ pl $\varphi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40$

Euler-Fermat: Ha $m>1$ tetszőleges egész szám és a tetszőleges olyan szám amelyre $d(a,m)=1$ akkor $a^{\varphi(m)} \equiv 1 \ (m)$

(B) Legyen $\{c_1, c_2, \dots c_{\varphi(m)}\}$ egy mod m redukált maradékrendszer. A $\{ac_1, ac_2, \dots, ac_{\varphi(m)}\}$ számhalmaz is egy mod m redukált maradékrendszer lesz, mivel csak egy a számmal szorzat meg, tehát az $ac_1, ac_i, \dots ac_{\varphi(m)}$ sorozatok valamilyen sorrendben kongruensek a $c_1, c_2, \dots c_{\varphi(m)}$ számokkal (sőbm)

$3 \cdot 1 = 3$
$3 \cdot 2 = 6 \equiv 1$ (1)
$3 \cdot 3 = 9 \equiv 4$ (2)
$3 \cdot 4 = 12 \equiv 2$ (3)

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

Mivel a c_i számok m-hez relatív prímek voltak, ezért egyszerűsíthető $a^{\varphi(m)}-1$ onnantól m-mel

Kis Fermat: Tetszőleges p prímszámra és tetszőleges a egész számra

$a^p \equiv a \ (p)$

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

---

(D) 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.

(D) Egy H halmazon értelmezett 2-változós műveletet (jelöljük *-gal) kommutatívnak nevezünk, ha tetszőleges $a,b \in H$ esetén $a*b = b*a$; asszociatívnak nevezünk, ha tetszőleges $a,b,c \in H$ esetén $(a*b)*c = a*(b*c)$

pl: a valós számokon értelmezett + művelet asszociatív és kommutatív

(D) A S halmazt a rajta értelmezett * művelettel félcsoportnak nevezzük, ha * asszociatív. Ha * kommutatív is, akkor kommutatív (vagy Abel-féle) félcsoportról beszélünk.

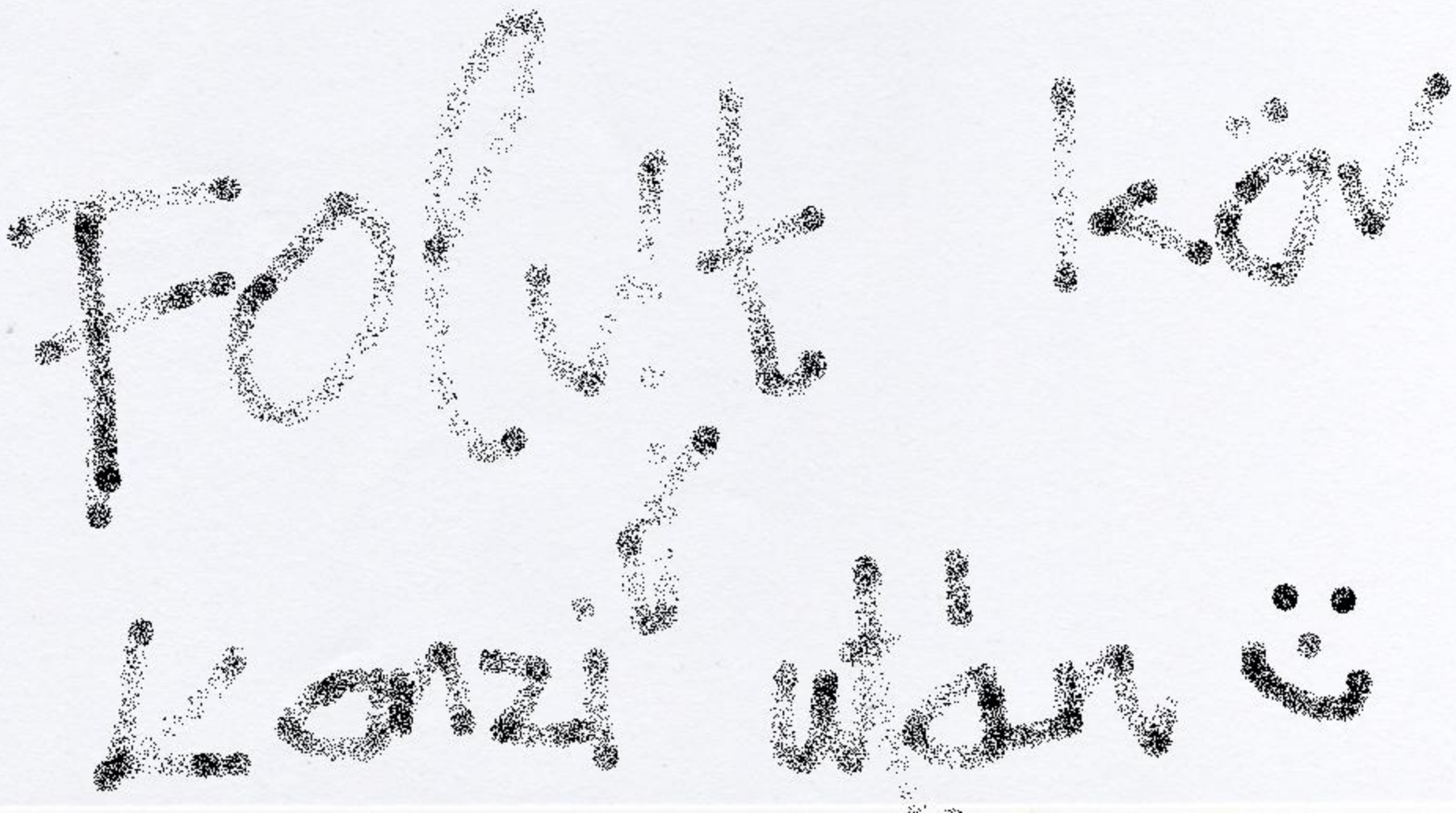
pl: - A pozitív számok az összeadásra nézve félcsoportot alkotnak
- Az nxn-es mátrixok a szorzással félcsoportot alkotnak

(D) Ha az S félcsoportban van olyan e elem, amelyre igaz az hogy $e*a = a*e = a$ minden $a \in S$ esetén, akkor e-t egységelemnek hívjuk.

(D) Egy G halmazt a $\cdot$ művelettel csoportnak nevezünk, ha
a) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ minden $a,b,c \in G$ esetén $\Leftarrow$ asszoc
b) $\exists e \in G$, amelyre $a \cdot e = e \cdot a = a$ $\forall a \in G$-re $\Leftarrow \exists$ egységelem
c) $\forall a \in G$-re $\exists a' \in G$ úgy, hogy $a \cdot a' = a' \cdot a = e$ $\Leftarrow \exists$ inverz

A csoportművelettől nem követeljük meg a kommutatívitási szabály teljesülését, ha ez teljesül, kommutatív (Abel-féle) csoportról beszélünk

pl: - 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
- A pozitív valós és a pozitív racionális számok Abel-csoportot alkotnak a szorzásra nézve.
- Az nxn-es invertálható mátrixok csoportot alkotnak a szorzásra nézve.



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

(D) Elem rendje: Az a legkisebb ($k \geq 1$) k szám, amelyet ha k-ra emelünk az egységelemet kapjuk.

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

- pl: - n elem permutációinak részcsoportját alkotják a páros permutációk.
  - a háromszög egybevágóságainak részcsoportját alkotják a forgatások.

(D) 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 K-t tartalmazó részcsoportok metszete.

(A) Egy elem rendje megegyezik az általa generált részcsoport rendjével

(D) Az egy elem által generált csoportokat ciklikus csoportnak nevezzük és C_n-nel jelöljük

Köv: Minden $n > 0$ egész számra van n elemű csoport

pl

- Minden páros rendű csoport ciklikus
- A G csoport g elemének rendje a g által generált részcsoport elemszáma
- (A) • Ciklikus csoport minden részcsoportja ciklikus

(A) Azonos rendű ciklikus csoportok izomorfak.

(D) A G_1, G_2 csoportokat izomorfnak nevezzük, ha van közöttük egy kölcsönösen egyértelmű művelettartó leképezés arról 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 $G_1 \simeq_\phi G_2$ vagy egyszerűen $G_1 \simeq G_2$

pl: $(\mathbb{R}^+, \cdot) \simeq (\mathbb{R}, +)$, ahol a ϕ izomorfizmus minden pozitív valós számhoz hozzárendeli a logaritmusát, azaz $\phi(a) = \log a$. A bijektivitás a logaritmus függvény monotonitásából adódik, a műveletlartás pedig a $\log(ab) = \log a + \log b$ összefüggés eredménye

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

(A) 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;

Lagrange tétel: Legyen G véges, $H \leq G$. Ekkor H rendje osztja G rendjét.

(R) Osztályozzuk G-t a H szerinti jobboldali mellékosztályai szerint. $G = \bigcup Hg$. Jelölje k H mellékosztályainak számát. Mivel minden elem pontosan egy mellékosztályban szerepel, ezért $|G| = |\bigcup Hg|$ miatt $|G| = \sum |Hg| = k|H|$. A $k = |G|/|H|$ számot H G-beli indexének nevezzük és $|G:H|$-val jelöljük.

Mivel egy elem rendje megegyezik az általa generált részcsport rendjével:

Köv: 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 azaz:

Köv: Minden prímrendű csoport ciklikus.

(D) Az S_n szimmetrikus csoport $\{1, 2, \ldots, n\}$ halmaz permutációi alkotta a függvénykompozíció műveletre nézve.

Cayley tétel: Minden G véges csoport izomorf egy alkalmas permutációcsoporttal.

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

D) A $\langle R, \{+, \cdot\}\rangle$ algebrai struktúra **gyűrű**, ha $\langle R, + \rangle$ Abel csoport, $\langle R, \cdot \rangle$ félcsoport továbbá teljesülnek a disztributív azonosságok: $a(b+c) = ab+ac$ ill. $(a+b)c = ac+bc$ ($\forall a,b,c \in R$). Ha röviden csak R gyűrűt mondunk akkor konvenció szerint R két művelete $+$ és $\cdot$ a fentiek szerint.

Az R gyűrű kommutatív, ha a szorzás kommutatív. Az R gyűrű összeadásánál egységelemét **nullelemnek** nevezzük és 0-val jelöljük. Az R gyűrűben az $a \in R$ elem inverzét az összeadásra $-a$ jelöli. Az R gyűrű **egységelemes**, ha a szorzásműveletnek van egysége, melyet (ha van) 1 jelöl.

Pl: - $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ gyűrű. $\mathbb{N}$ nem gyűrű, mert nem csoport az összeadásra (nincs inverz)
- A mod m maradékosztályok
- Az $n \times n$-es mátrixok is gyűrűt alkotnak

D) Az R gyűrűben a $a \neq 0$ elem **nullosztó**, ha létezik olyan $0 \neq b \in R$, melyre $ab = 0$. Az R gyűrű **nullosztómentes**, ha R-ben nincs nullosztó. Az R gyűrű **integritási tartomány**, ha kommutatív és nullosztómentes.

Pl: - Az egész számok, a páros számok gyűrűje integritási tartomány
- $\mathbb{Z}_6$-ban $2 \cdot 3 = 0$, ezért 2 ill. a 3 nullosztó

D) Az R gyűrű **részgyűrűje** az $\langle R, \{+, \cdot\}\rangle$ olyan részstruktúrája, mely gyűrű (csupán a műveletekre való zártságot és az ellentettek meglétét (valójában a kivonásra való zártságot) kell ellenőrizni)

Pl: - az egész számokat részgyűrűjét alkotják az m-mel osztható egész számok.

D) A T gyűrű **ferdetest**, ha $\langle T \setminus \{0\}, \cdot \rangle$ csoport. Ha a szorzás kommutatív akkor T **test**

Pl: - $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ testek
- valós polinomok hányadosteste: $R(x) := \left\{ \frac{p}{q} : p, q \in \mathbb{R}[x], q \neq 0 \right\}$

D) Egy algoritmust **polinomiálisnak** nevezünk, ha lépésszáma a bemenet méretének polinomjánál felülről becsülhető.

Szám hossza: $\log n$

Két számnál: $\log n + \log m$

Összeadás: Helyiértékenként 2 művelet $(a_n + b_n)\, c_{n-1}$

felső korlát a lépésszámra $\leq 2 \cdot \max(\log n, \log m) < 2 \cdot (\log n + \log m) \Rightarrow$ polinomiális

Kivonás: ua. mint az összeadás

Szorzás: $\log n$ db összeadás, egyes tagokat $2 \cdot \log m$ lépésben lehet

Tehát az összlépésszám: $2(\log n)(\log m) \leq (\log n + \log m)^2 \Rightarrow$ polinomiális

Hatványozás: n^m a szám hossza: $\log n^m = m \log n \Rightarrow$ NEM polinomiális függvény az eredmény kiírása is exponenciális

modulo m hatványozás: $n^k \pmod m$ megvalósítása polinomiális

Pl $3^{59} \bmod 17$

Max $\log_2 59$-nyi lépés volt

$59 = 111011_{(2)}$

$59 = 32 + 16 + 8 + 2 + 1$

$3^{59} = 3^{32} \cdot 3^{16} \cdot 3^8 \cdot 3^2 \cdot 3^1$

$3^8 \equiv 16^2 \equiv -1$

$3^{16} \equiv 1$

$3^{32} \equiv 1$

$3^1 \equiv 3$

$3^2 \equiv 9$

$3^4 \equiv 81 \equiv 13$

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

Az exponenciális
A teszt alapja az Euler-Fermat tétel:
ha n prím, $t^{n-1} \equiv 1 \ (n)$ minden $(t,n)=1$ esetén $\Rightarrow$ csak összetett számnál lehet kivétel
↳ Ha $\exists$ t amire $(t,n)=1$ és $t^{n-1} \not\equiv 1 \ (n)$ akkor n összetett → t n **áralója**
↳ Ha található olyan t-t, amire $0<t<n$ $(t,n) \neq 1$ azaz megtudjuk n egy valódi osztóját $\Rightarrow$ t n **lelepleződ**
(a lelepleződ egyben $t^{n-1} \not\equiv 1 \ (n)$, de nem áraló!)
↳ Ha egy t $0<t<n$ számra $t^{n-1} \equiv 1 \ (n)$, akkor t n **tanúsága**

(T) Ha $1 \leq c_1 < c_2 < \dots < c_e < n$ az n szám osztásai és az n egy áralója, akkor $ac_1, ac_2, \dots ac_e$ az n szám páronként (modulo n) különböző maradéki

(B) Ha $ac_i \equiv ac_j \ (n)$, akkor $(a,n)=1$ miatt $c_i \equiv c_j \ (n)$, azaz $c_i = c_j$, tehát az $ac_1, ac_2 \dots ac_e$ számok valóban különböző maradékosztályokból valók.
Mivel $c_i^{n-1} \equiv 1 \ (n)$ és $a^{n-1} \not\equiv 1 \ (n)$ ezért $(ac_i)^{n-1} = a^{n-1} \cdot c_i^{n-1} \equiv a^{n-1} \not\equiv 1 \ (n)$)
tehát a fenti számok csak úgy az áralók.

Fermat-teszt: $0<t<n$ véletlen szám. Ha $t^{n-1} \not\equiv 1 \ (n) \Rightarrow$ n nem prím, ha $\equiv 1 \rightarrow$ úgy tűnik, hogy prím.
Ha n-nek van áralója, akkor annak a valószínűsége, hogy összetett számot prímnek mond $\leq \frac{1}{2}$ így sok Fermat-teszt után szinte biztosak lehetünk az eredményben és ez **polinomiális**

Carmichael számok: álprímek, ezek okozzák a Fermat teszt bizonytalanságát.
a legkisebb az 561

(D) **Egyirányú fv**: $f: \{1,2,\dots n\} \rightarrow \{1,2,\dots n\}$ bijekció ahol f polinomiális időben számítható, f viszont f ismeretében reménytelen
↑ visszaszámítása
pl: telefonkönyvnél NÉV → TELszám

(D) **kiskapus egyirányú fv**: f^{-1} kiszámítására is létezik hatékony eljárás, de ezen f ismeretében reménytelen.

(D) **Nyilvános kulcsú titkosítás**: üzenetek 1 és $|\Sigma|^t$ közti számok, f: kiskapus egyirányú fv ahol $n \geq |\Sigma|^t$ f-et megadjuk ezzel NYILVÁNOS KULCS
Címzett pedig ismeri f^{-1}-et lehető titkos kulcsot, ami alapján azt hatékonyan tudja módosítani
Lehallgató f-et és f^{-1}-et ismeri $\Rightarrow$ csak M „ismeretében" tudja M-et kitalálni
nem kell külön üzenni

$A \longrightarrow B : f^{-1}$

$\xleftarrow{f} \quad \xrightarrow{f(M)} \quad f^{-1}(f(M)) = M$ ✓

(11) Digitális aláírás

f_A, f_B kölcsönös egyértelmű f-ek

B biztos afelől, hogy ezt A küldte, mert f_A^{-1}-et csak A ismeri

Ez f_A^{-1} felfedezése nélkül bizonyítható: a címzett tudja bizonyítani

(B felfedi $f_A^{-1}(M)$-et és M-et $\rightarrow f_A(f_A^{-1}(M)) = M$)

~~$M = f_B(M_{igaz})$~~, ekkor bárki láthatja, hogy M_{igaz} titkosított változata M.

A: f_A^{-1} ⟶ B: f_B^{-1}

$$f_A\left(f_B^{-1}\left(f_B\left(f_A^{-1}(M)\right)\right)\right) = M$$

RSA kódolás:

$n = p \cdot q$, $m = \varphi(n) = (p-1)(q-1)$. Csak n nem titkos

Választunk egy e számot, melyre: $(e,m) = 1$

Áll: $e \cdot d = 1 \pmod m$ d-re megoldható: hiszen $(e,m) \mid 1 \rightarrow n$ és e nyilvános

B, a címzett ekkor meg is semmisítheti p, q, m-et mert elég neki d (a titkos kulcs n, d)

$f(M) = M^e \pmod n$

Áll: $f^{-1}(M^e) = (M^e)^d \pmod n$

EFtétel $\equiv 1$ ha $(M,n) = 1$

(B) $(M^e)^d \equiv M^{ed} \underset{\text{miatt}}{\overset{e \cdot d \equiv 1}{=\!=\!=}} M^{k \cdot m + 1} \equiv (M^m)^k = (M^{\varphi(n)})^k \cdot M \equiv M \pmod n$

Jó mert n, e-ből d meghatározása hasonlóan nehéz mint n prímfelbontása, ha e-t jól választjuk. Ezt pedig reménytelen, ha p, q prímek elég nagyok (200 jegyűek)

p és q választása: véletlenszerűen kell, hogy titkos legyen