Bevezetés a számításelméletbe 2.

Kidolgozott tételek szóbeli vizsgához
2012 tavasz

v.1.0.

Készítette:
Talapa Viktor

Tartalomjegyzék

Előszó

Ez a jegyzet a 2012 tavaszi félévi vizsgához készült és **CSAK a definíciókat és tételeket tartalmazza, bizonyításokat nem.** Ennek oka, hogy a VIK Wikin már nagyon sok tételkidolgozás található, amelyek teljesen lefedik az anyagot, viszont tudom (saját példából), hogy célszerű először a tételeket megtanulni, és csak utána foglalkozni a bizonyításokkal. Nem is beszélve azokról, akik eleve csak a tételeket akarják tudni, a bizonyításokat nem, számukra a többi jegyzet kifejezetten zavaró lehet, hiszen szelektálni kell lényeges és kevésbé lényeges információ között. Elsősorban nekik szól ez a jegyzet, de a többieknek is hasznos összefoglalóként szolgál. A tételeket a VIK Wikin található különböző jegyzetek, Fleiner Tamás letölthető jegyzete, Váry Anna Zsófia kézzel írott jegyzete illetve a Katona-Recski-Szabó: A számítástudomány alapjai című könyv alapján készítettem. Használjátok egészséggel. Amennyiben bármi (akár elvi, akár helyesírási) hibát észleltek, vagy esetleg egyéb észrevételetek van, a tv1113@hszk.bme.hu e-mail címen jelezzétek.

Üdvözlettel:

Talapa Viktor

Tételsor

1. Hamilton-körök és -utak. Szükséges feltétel Hamilton-kör/út létezésére. Elégséges feltételek: Dirac és Ore tétele. Euler-körök és –utak, ezek létezésének szükséges és elégséges feltétele.
2. Páros gráf fogalma, kapcsolat a páratlan körökkel. Párosítások páros gráfban, a javítóutak módszere, Hall és Frobenius tételei.
3. Kőnig tétele. Párosítások tetszőleges gráfban, Tutte tétele (csak a szükségesség bizonyításával), Gallai tételei.
4. Gráfok színezése. $\chi(G)$ fogalma és viszonya $\omega(G)$-hez, illetve $\Delta(G)$-hez. Brooks tétele (biz. nélkül). Mycielski konstrukciója. Síkbarajzolható gráfok kromatikus száma, ötszíntétel.
5. Élkromatikus szám: $\chi_e(G)$ viszonya $\Delta(G)$ -hez, Vizing-tétel (biz. nélkül), páros gráfok élkromatikus száma. Perfekt gráfok, erős perfekt gráf tétel (csak a szükségesség bizonyításával), Lovász tétele (biz. az erős perfekt gráf tételből). Intervallumgráfok perfektsége.
6. Hálózat, hálózati folyam és vágás fogalma, folyam értéke, vágás kapacitása. Algoritmus a maximális folyam és a minimális vágás megkeresésére, Ford-Fulkerson tétel, Edmonds-Karp tétel (biz. nélkül), egészértékűségi lemma. A folyamprobléma általánosításai.
7. Menger pontpárok közötti diszjunkt utakra vonatkozó tételei.
8. Többszörös összefüggőség és élösszefüggőség fogalma, Menger vonatkozó tételei. Gráfok szomszédossági mátrixa, a szomszédossági mátrix hatványainak jelentése.
9. Oszthatóság, felbonthatatlan és prímtulajdonságú számok, ezek kapcsolata (biz. csak az egyik irányban), a számelmélet alaptétele. Osztók száma és összege. Prímek száma, $\pi(n)$ nagyságrendje (biz. nélkül). Kongruencia fogalma, alapműveletek kongruenciákkal.
10. Lineáris kongruenciák: a megoldhatóság szükséges és elégséges feltétele, a megoldások száma. Euklideszi algoritmus, alkalmazása lineáris kongruenciák megoldására.
11. Euler-féle φ -függvény, redukált maradékrendszer, Euler-Fermat tétel, kis Fermat-tétel. Kétismeretlenes, lineáris diofantikus egyenlet megoldása (konkrét példán). Két kongruenciából álló kongruencia rendszer megoldása (konkrét példán).
12. Számelmélet és algoritmusok: alapműveletek, hatványozás az egészek körében és a $modulo\ m$. Prímtesztelés, carmichael számok. Nyilvános kódú titkosírás.
13. Művelet fogalma, csoport, Abel-csoport. Példák: csoportok számokon, mátrixokon, rajzok szimmetriacsoportja, diédercsoport. Példák véges és végtelen, kommutatív és nem kommutatív csoportra mind a négy lehetséges variációban.
14. Elem rendje (ez véges csoportban véges), ciklikus csoport. Részcsoport. Szimmetrikus csoport. Csoportok izomorfiája, Cayley tétele (biz. nélkül).
15. Mellékosztály fogalma, példák. Lagrange tétele, elemrend és csoport rendjének kapcsolata.
16. Gyűrű, ferdetest és test fogalma, példák. Nollosztómentes gyűrű, test nullosztómentessége. Példák: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $n \times n$-es mátrixok, polinomok, $\mathbb{Z}_n$ (ez milyen n-re test), $\mathbb{Q}(\sqrt{2})$.

1. tétel

Hamilton-kör és –út

Def.: Egy G tetszőleges gráfban egy olyan utat, mely G minden **pontját** pontosan egyszer tartalmazza, **Hamilton-út**nak nevezünk.

Def.: Egy G tetszőleges gráfban egy olyan kört, mely G minden **pontját** pontosan egyszer tartalmazza, **Hamilton-kör**nek nevezünk.

Megj.: Ha G-ben van Hamilton-kör, akkor van benne Hamilton-út is.

Szükséges feltétel Hamilton-kör és -út létezésére

Tétel: **Ha** egy G tetszőleges gráfban **létezik Hamilton-kör**, **akkor** G-ből bárhogyan k darab csúcsot elhagyva G **legfeljebb** k darab komponensre esik szét.

Tétel: **Ha** egy G tetszőleges gráfban **létezik Hamilton-út**, **akkor** G-ből bárhogyan k darab csúcsot elhagyva G **legfeljebb** $k+1$ darab komponensre esik szét.

Megj.: Példa arra, hogy a szükséges feltétel nem elégséges: Petersen-gráf.

Ore tétele

Tétel: Ha egy n csúcsú, **egyszerű** G gráf **bármely két, nem szomszédos** x, y csúcsára igaz az, hogy $d(x) + d(y) \geq n$, azaz ha x, y csúcsok **fokszámainak összege legalább** n, akkor a G-ben **van Hamilton-kör**.

Dirac tétele

Tétel: Egy n csúcsú, **egyszerű** G gráf **minden** x csúcsára igaz, hogy $d(x) \geq \frac{n}{2}$, azaz ha minden csúcs **foka legalább** $\frac{n}{2}$, akkor G-ben **van Hamilton-kör.**

Euler-kör és -út

Def.: Egy G tetszőleges gráfban egy olyan **élsorozatot**, mely G minden **élét** pontosan egyszer tartalmazza, **Euler-út**nak nevezünk.

Def.: Egy G tetszőleges gráfban egy olyan **zárt élsorozatot**, mely G minden **élét** pontosan egyszer tartalmazza, **Euler-kör**nek nevezünk.

Megj.: Ha G-ben van Euler-kör, akkor van benne Euler-út is.

Szükséges és elégséges feltétel Euler-kör és -út létezésére

Tétel: Egy G **összefüggő** gráfban **létezik Euler-kör**, ha G **minden** pontjának fokszáma páros.

Tétel: Egy G **összefüggő** gráfban **létezik Euler-út**, ha **0 vagy 2 kivétellel** G **minden** pontjának fokszáma páros.

2. tétel

Páros gráf

Def. Egy G gráf **páros**, ha G csúcsainak halmaza – $V(G)$ – felbontható A és B halmazokra úgy, hogy **G minden éle A-beli csúsot kössön össze B-belivel**.

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

Kapcsolat a páratlan körökkel

Tétel: Egy G gráf **akkor és csak akkor** páros, ha **nem tartalmaz páratlan kört**.

Párosítások páros gráfban

Def.: Egy **egyszerű** G gráfban egy M **élhalmazt** (részleges) **párosításnak** nevezünk, ha semelyik két élnek **nincs közös pontja**. Az ilyen éleket **független élek**nek is nevezzük.

Def.: Egy párosítás lefedi éleinek végpontjait. Ha az M párosítás **G minden pontját** lefedi, akkor M-et **teljes párosításnak** nevezzük.

A javító utak módszere

A módszer arra szolgál, hogy egy párosításról eldöntsük, hogy maximális-e, illetve ha nem, hogyan növeljük meg.

Legyen $G(A, B; E)$ egy adott páros gráf, melyben már meg van adva egy M párosítás. Rajzoljuk le a gráfot úgy, hogy M éleit folytonos, a gráf többi élét pedig szaggatott vonallal kötjük össze. Ha egy A-beli, az M párosítás által nem lefedett pontból elindulva, felváltva szaggatott illetve folytonos éleken át vezető úton el tudunk jutni egy B-beli, M által le nem fedett pontba, akkor találtunk javító utat, és a párosítás növelhető úgy, hogy az úton lévő szaggatott éleket folytonos, a folytonosakat pedig szaggatott élekre cseréljük. Így, mivel a javító út első és utolsó éle is szaggatott volt, növeltük a párosítást. Ha nem találunk javító utat, akkor a megadott párosítás maximális.

Hall tétele

Def.: Egy $X \in V(G)$ ponthalmaz **szomszédainak halmazát $N(X)$-el** jelöljük.

Megj.: $N(X)$ azon y pontok halmaza, amelyekhez van olyan él, melynek egyik végpontja y, a másik pedig egy X-beli pont.

Tétel: Egy $G(A, B; E)$ **páros** gráfban **akkor, és csak akkor** van A-t lefedő párosítás, ha **minden** $X \subseteq A$ részhalmazra $|N(X)| \geq |X|$ (ezt a feltételt **Hall-feltétel**nek nevezzük).

Frobenius tétele

Tétel: Egy $G(A, B; E)$ **páros** gráfban **akkor, és csak akkor** van teljes párosítás, ha $|A| = |B|$ és $|N(X)| \geq |X|$ minden $X \subseteq A$ részhalmazra.

3. tétel

Def.: Jelöljük $\nu(G)$-vel a G gráfban található **független élek maximális számá**t.

Def.: $X \subseteq V(G)$ egy **lefogó ponthalmaz**, ha G minden élének legalább egyik végpontját tartalmazza. A G-ben található **lefogó pontok minimális számá**t $\tau(G)$-vel jelöljük.

Def.: $Y \subseteq E(G)$ **lefogó élhalmaz**, ha G minden pontját lefogja. A G-ben található **lefogó élek minimális számá**t $\rho(G)$-vel jelöljük.

Def.: $X \subseteq V(G)$ **független ponthalmaz**, ha nincs benne két szomszédos pont. A **független pontok maximális számá**t $\alpha(G)$-vel jelöljük.

Kőnig tétele

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

Párosítás tetszőleges gráfban, Tutte tétele

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

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

Gallai tételei

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

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

4. tétel

Gráfok színezése

Def.: Egy G **hurokmentes** gráf k **színnel kiszínezhető**, ha minden csúcsot ki lehet színezni k darab szín felhasználásával úgy, hogy **bármely két szomszédos csúcs** színe különböző legyen.

$\chi(G)$ fogalma és viszonya $\omega(G)$-hez, illetve $\Delta(G)$-hez

Def.: G gráf **kromatikus száma** k, ha G k színnel kiszínezhető, de $k-1$ színnel nem.
Jele: $\chi(G) = k$.

Def.: G egy teljes részgráfját **klikk**nek nevezzük. A G-ben található **maximális klikk méretét**(, azaz a legnagyobb klikkben lévő pontok számát) a gráf **klikk-szám**ának nevezzük.
Jele: $\omega(G)$.

Tétel: Minden G gráfra $\omega(G) \leq \chi(G)$.

Def.: Egy G gráfban a **maximális fokszám** G összes csúcsainak fokszámai közül a legnagyobb.
Jele: $\Delta(G)$.

Tétel: Minden G gráfra $\chi(G) \leq \Delta(G) + 1$.

Brooks-tétel

Tétel: Minden olyan G gráfra, mely **nem teljes gráf** és **nem páratlan kör**, igaz az, hogy $\chi(G) \leq \Delta(G)$.

Mycielski tétele és konstrukciója

Def.: A Mycielski-konstrukció a $V(G) = \{v_1, \dots, v_n\}$ csúcshalmazú G gráfhoz egy olyan $M(G)$-vel jelölt gráfot rendel, mely tartalmazza G-t feszített részgráfként, továbbá $(n+1)$ csúcsot. Ezek úgy helyezkednek el, hogy $\forall v_i$ csúcsnak van egy u_i párja, melynek szomszédai megegyeznek v_i szomszédaival (, vagyis u_i azokkal a csúcsokkal van csak összekötve, amelyekkel v_i). Az $(n+1)$-edik csúcs pedig minden u_i csúccsal össze van kötve, de egyik v_i csúccsal sem.

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

Ötszín-tétel

Tétel: Minden G **síkbarajzolható** gráfra igaz, hogy $\chi(G) \leq 5$.

Négyszín-tétel

Tétel: Minden G **síkbarajzolható** gráfra igaz, hogy $\chi(G) \leq 4$.

5. tétel

Gráfok élszínezése

Def.: Egy G gráf élei k **színnel kiszínezhetők**, ha minden élet ki lehet színezni k darab szín felhasználásával úgy, hogy **bármely két szomszédos él** színe különböző legyen.

$\chi_e(G)$ fogalma és viszonya $\Delta(G)$-hez

Def.: G gráf **élkromatikus száma** k, ha G élei k színnel kiszínezhetők, de $k-1$ színnel nem.

Jele: $\chi_e(G) = k$.

Tétel: Minden G gráfra $\Delta(G) \leq \chi_e(G)$.

Vizing tétele

Tétel: Minden G **egyszerű** gráfra $\chi_e(G) \leq \Delta(G) + 1$.

Páros gráfok élkromatikus száma (Kőnig tétele)

Tétel: Ha G **páros** gráf, akkor $\chi_e(G) = \Delta(G)$.

Perfekt gráfok

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

Tétel: Minden **páros** gráf **perfekt**.

Erős perfekt gráf tétel

Tétel: Egy G gráf akkor és csak akkor perfekt, ha sem G, sem $\overline{G}$ nem tartalmaz feszített részgráfként páratlan kört.

Lovász tétele

Tétel: Egy G gráf akkor és csak akkor perfekt, ha $\overline{G}$ is perfekt.

Intervallumgráfok perfektsége

Def.: 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 $p_1, p_2, \ldots$ egy G gráf pontjai és $\{p_i, p_j\}$ akkor és csak akkor legyen él G-ben, ha $I_i \cap I_j \neq 0$. Az így előálló gráfokat **intervallumgráfoknak** nevezzük.

Tétel: Minden **intervallumgráf perfekt**.

6. tétel

Hálózat

Def.: Legyen $\vec{G}$ egy irányított gráf. Rendeljünk minden éléhez egy $c(e)$ nemnegatív valós számot, amit az él **kapacitásának** nevezünk. Jelöljünk ki továbbá két s, t pontot, melyeket **termelő**nek és **fogyasztó**nak hívunk. Ekkor a $(\vec{G}; s; t; c)$ négyest **hálózat**nak nevezzük.

Hálózati folyam

Def.: Legyen $f(e)$ az a mennyiség, ami az e élen folyik át. Ez az f függvény megengedett függvény, ha $f(e) \leq c(e)$ és legyen:
$m(v) = \sum\{f(e) \mid e \text{ végpontja } v\} - \sum\{f(e) \mid e \text{ kezdőpontja } v\} = 0$, azaz egy adott (s, t pontoktól különböző) $v \in V$ pontba ugyanakkora mennyiség folyik be, mint amennyi ki[1]. Ezt az f megengedett függvényt **folyam**nak hívjuk.

Folyam értéke

Def.: Előbbiből könnyen belátható, hogy $m(s) = -m(t)$. Ezt a közös értéket a **folyam értéké**nek nevezzük.

Jele: m_f

Megj.: Egy e élet egy folyamban **telített**nek hívunk, ha $f(e) = c(e)$, és **telítetlen**nek, ha $f(e) < c(e)$.

Vágás

Def.: Legyen $X \subseteq V(\vec{G})$, ahol $s \in X$ és $t \notin X$. Azoknak az éleknek C halmazát, amelyeknek egyik végpontja X-beli, a másik végpontja pedig $\{V(\vec{G}) - X\}$-beli, a hálózati folyam egy (s, t) **vágás**ának nevezzük.

Vágás kapacitása

Def.: A vágás kapacitása azon éleken lévő kapacitások összege, amelyek egy X-beli pontból egy $\{V(\vec{G}) - X\}$-beli pontba mutatnak. (Az ilyen éleket előremutató éleknek nevezzük, tehát a vágásba nem tartozhatnak bele visszafelé mutató élek, melyek X-beli pontba mutatnak.)

Jele: $c(C)$.

[1] Ezt nevezzük **Kirchoff-féle csomóponti törvény**nek, mely fizikai áramköröknél is előjön.

Algoritmus a max. folyam és min. vágás megkeresésére

0. lépés $f \equiv 0$ folyam.

1. lépés f' folyam felvétele f helyett, hogy $m_f, > m_f$ igaz legyen. Ezt addig ismételjük, ameddig tudjuk, azaz „szemre” megpróbálunk egy maximális folyamot meghatározni s-ből t-be.

2. lépés Felrajzolunk egy H_f segédgráfot a következő tulajdonságokkal:
($\vec{G}$ a gráfunk, $e \in E(\vec{G})$, $e' \in E(H_f)$, $u, v \in V(\vec{G})$)
   - $V(H_f) = V(\vec{G})$, azaz $H_f$csúcsai megegyeznek $\vec{G}$ csúcsaival.
   - Ha $e = \overrightarrow{uv}$ és $f(e) < c(e)$, akkor $e' := \overrightarrow{uv}$, azaz ha $\vec{G}$-ben az $\overrightarrow{uv}$ él értéke kevesebb, mint az él kapacitása, akkor H_f-ben is fusson él u-ból v-be.
   - Ha $e = \overrightarrow{uv}$ és $f(e) > 0$, akkor $e' := \overrightarrow{vu}$, azaz ha $\vec{G}$-ben az $\overrightarrow{uv}$ él értéke nagyobb, mint 0, akkor H_f-ben fusson „vissza él”, azaz v-ből u-ba.

3. lépés Amennyiben H_f-ben létezik irányított út s-ből t-be (ezt **javító út**nak hívjuk), akkor a folyam értéke növelhető. Megnézzük, hogy az eredeti $\vec{G}$ gráfban mennyi a minimális érték, amennyivel lehet növelni a javító út élein átmenő folyam étékét. („Előre él” esetén növelni, „vissza él” esetén csökkenteni kell az él értékét) Ezután meg is növeljük az adott éleken átmenő folyam értékét, majd visszatérünk a 2. lépéshez, és keresünk újabb javítóutat.

4. lépés Amennyiben nincs további javító út, megtaláltuk az s-ből t-be futó maximális folyamot. A minimális vágás pedig azon pontok halmaza, melyek az utolsó felrajzolt segédgráfon még elérhetőek s-ből.

Ford-Fulkerson-tétel

Tétel: A **maximális folyam értéke egyenlő a minimális vágás kapacitásával**,azaz $\max\{m_f \mid f \text{ egy folyam } s\text{-ből } t\text{-be}\} = \min\{c(C) \mid C \text{ vágás}\}$.

Edmond-Karp-tétel

Tétel: Ha mindig a legrövidebb javító utak egyikét választjuk, akkor az algoritmus véges sok lépés után leáll.

Egészértékűségi lemma

Lemma: Ha a kapacitások egész számok, akkor m_f értéke egész szám és ez megvalósítható olyan f folyammal, mely minden élen egész értéket vesz fel.

A folyamprobléma általánosításai

1. példa Mi van akkor, ha több termelő és/vagy több fogyasztó van?

Megoldás: Felveszünk egy „szupertermelőt”(S)/„szuperfogyasztót”(T), amelyeket összekötünk a termelőkkel/fogyasztókkal végtelen kapacitású éleken. Az így kapott gráfban keresünk maximális folyamot (S-ből T-be), majd ha megtaláltuk, letöröljük a két pontot.

2. példa Mi van akkor, ha a pontoknak is van kapacitása?

Megoldás: A probléma azt jelenti, hogy az adott pontba belépő élek kapacitásának összege nem lehet nagyobb a pont kapacitásánál. Ez is visszavezethető hagyományos hálózatra, ha a k kapacitással rendelkező v pontot két másik ponttal helyettesítjük, amiket egy k kapacitású él köt össze. A két új pontból az egyikbe futnak a v-be bejövő élek, a másikból futnak ki a v-ből kimenő élek.

3. példa Mi van akkor, ha vannak irányítatlan élek?

Megoldás: Az irányítatlan él helyett felveszünk két irányított élet azonos kapacitással, az egyik él az egyik, a másik a másik irányba mutat. Abban az esetben, ha a folyam meghatározásakor mindkét helyettesítő élen 0-nál nagyobb a folyamérték, a két él folyamértékét ki kell vonni egymásból, és az lesz az irányítatlan él értéke, míg az iránya a két helyettesítő élből a nagyobb folyamértékűnek az irányával egyezik meg.

7. tétel

Def.: A G irányított vagy irányítatlan gráf u pontjából v pontjába futó P és Q útjait **éldiszjunkt**aknak vagy **élidegen**nek nevezzük, ha $E(P) \cap E(Q) = \emptyset$.

Def.: A G irányított vagy irányítatlan gráf u pontjából v pontjába futó P és Q útjait **pontdiszjunkt**aknak vagy **pontidegen**nek nevezzük, ha $V(P) \cap V(Q) = \emptyset$.

Menger I. tétele

Tétel: Ha u és v a G irányított gráf különböző csúcsai, akkor az élidegen uv utak maximális száma azonos az uv utakat lefogó élek minimális számával.

Menger II. tétele

Tétel: Ha u és v a G irányított gráf különböző, nem szomszédos csúcsai, akkor a pontidegen uv utak maximális száma azonos az uv utakat lefogó, u-tól és v-től különböző csúcsok minimális számával.

Menger III. tétele

Tétel: Ha u és v a G irányítatlan gráf különböző csúcsai, akkor az élidegen uv utak maximális száma azonos az uv utakat lefogó élek minimális számával.

Menger IV. tétele

Tétel: Ha u és v a G irányítatlan gráf különböző, nem szomszédos csúcsai, akkor a pontidegen uv utak maximális száma azonos az uv utakat lefogó, u-tól és v-től különböző csúcsok minimális számával.

8. tétel

Többszörös összefüggőség és élösszefüggőség fogalma

Def.: Az irányítatlan G gráfot ***k*-szorosan (pont)összefüggőnek** nevezzük, ha G-nek minimum $(k+1)$ csúcsa van, és G-ből bárhogyan $(k-1)$ csúcsot elhagyva G továbbra is összefüggő lesz. A maximális k-t, amire G k-összefüggő $\kappa(G)$ jelöli.

Def.: Az irányítatlan G gráfot ***k*-szorosan élösszefüggőnek** nevezzük, ha G-ből bárhogyan $(k-1)$ csúcsot elhagyva G továbbra is összefüggő lesz. A maximális k-t, amire G k-élösszefüggő $\lambda(G)$ jelöli.

Menger V. tétele

Tétel: Egy G gráf akkor és csak akkor k-szorosan élösszefüggő, ha bármely két pont között létezik k db. éldiszjunkt út.

Menger VI. tétele

Tétel: Egy G gráf akkor és csak akkor k-szorosan (pont)összefüggő, ha bármely két pontja között létezik k db páronként pontdiszjunkt út.

Gráfok szomszédossági mátrixa

Def.: Legyen G n-csúcsú gráf, $V(G)=\{v_1, v_2, \dots, v_n\}$. Ekkor az $A(G)$ $n \times n$-es mátrix G **szomszédossági mátrixa**, ha minden $a_{i,j} \in A(G)$-re teljesül, hogy:

$$a_{i,j} = \begin{cases} 0, \text{ ha } v_i \text{ és } v_j \text{ nem szomszédos,} \\ k, \text{ ha } v_i \text{ és } v_j \text{ között } k \text{ db pontdiszjunkt él fut,} \\ l, \text{ ha } i=j \text{ és } l \text{ db hurokél illeszkedik rá.} \end{cases}$$

A szomszédossági mátrix hatványai

Tétel: Legyen G n-csúcsú gráf, $V(G)=\{v_1, v_2, \dots, v_n\}$ és A, B $n \times n$-es mátrixok. Ha $A=A(G)$ és $B=A^k$, akkor minden $b_{i,j} \in B$-re teljesül, hogy:
$b_{i,j} = G$-ben v_i-ből v_j-be vezető pontosan k hosszú élsorozatok száma.

9. tétel

Oszthatóság

Def.: Legyen $a, b \in \mathbb{Z}$. Azt mondjuk, hogy a **osztója** b-nek, ha létezik egy olyan $c \in \mathbb{Z}$, hogy $a \cdot c = b$.

Jele: $a|b$

Felbonthatatlan és prímszámok, valamint ezek kapcsolata

Def.: Egy $p \in \mathbb{Z}$ számra azt mondjuk, hogy **felbonthatatlan** ha $p \neq 0$ vagy ± 1 és $p = a \cdot b$ csak akkor lehetséges, ha $a = \pm 1$ vagy $b = \pm 1$.

Def.: Egy $p \in \mathbb{Z}$ számra azt mondjuk, hogy **prím**, ha $p \neq 0$ vagy ± 1 és $p|a \cdot b$ csak akkor lehetséges, ha $p|a$ vagy $p|b$.

Tétel: Egy $p \in \mathbb{Z}$ szám **akkor és csak akkor prím**, ha **felbonthatatlan** és fordítva.

A számelmélet alaptétele

Tétel: Minden $n \in \mathbb{Z} \mid n \neq 0$ vagy ± 1 számra igaz az, hogy n **felbontható felbonthatatlanok** (prímek) **szorzatára** és ez a felbontás sorrendtől és előjelektől függetlenül **egyértelmű**.

Osztók száma és összege

Def.: Egy $1 < n \in \mathbb{N}$ szám **kanonikus alak**ján egy olyan $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ előállítást értünk, amiben p_i-k különböző (pozitív) prímek, az α_i-k pedig pozitív egészek. (Az ilyen előállítást hívjuk **prímtényezős felbontás**nak.)

Def.: Legyen $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ egy $1 < n \in \mathbb{N}$ szám kanonikus alakja. Ekkor n (pozitív) **osztóinak száma**:

$$d(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1).$$

Def.: Legyen $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ egy $1 < n \in \mathbb{N}$ szám kanonikus alakja. Ekkor n (pozitív) **osztóinak összege:**

$$\sigma(n) = \left(1 + p_1^1 + p_1^2 + \ldots + p_1^{\alpha_1}\right) \cdot \left(1 + p_2^1 + p_2^2 + \ldots + p_2^{\alpha_2}\right) \cdot \ldots \cdot (1 + p_k^1 + p_k^2 + \ldots + p_k^{\alpha_k}).$$

Prímek száma

Tétel: A prímszámok száma végtelen.

$\pi(n)$ nagyságrendje

Def.: A prímszámok számát 1 és n között $\pi(n)$-nel jelöljük.

Tétel: $\pi(n) \approx \frac{n}{\ln n}$, illetve $\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$.

Kongruencia

Def.: Azt mondjuk, hogy a és b **kongruens** $modulo\ m$, ha $a, b, m \in \mathbb{Z}$ és mind a-t, mind b-t m-mel osztva azonos maradékot kapunk.
Másik megfogalmazásban a és b kongruens $modulo\ m$, ha m osztója $a - b$-nek $(m|a - b)$.

Jele: $a \equiv b\ (m)$

Def.: Az azonos maradékot adó egészeket külön osztályokba helyezhetjük. Az ilyen osztályokat **maradékosztály**oknak nevezzük.

Alapműveletek kongruenciákkal

Tétel:
$a, b, c, d, m \in \mathbb{Z}$
$a \equiv b\ (m)$
$c \equiv d\ (m)$
$\Leftrightarrow$
1. $a \pm c \equiv b \pm d\ (m)$
2. $a \cdot c \equiv b \cdot d\ (m)$
3. $a^k \equiv b^k\ (m)$

Tétel: $a \cdot c \equiv b \cdot c\ (m) \quad \Leftrightarrow \quad a \equiv b\ (m)$.

10.tétel

Lineáris kongruencia

Def.: Az $a \cdot x \equiv b\ (m)$ kongruenciát **lineáris kongruenciának** nevezzük, ha $a, b \in \mathbb{Z}$ és $m \in \mathbb{Z}^+$ ismertek, és keressük az $x \in \mathbb{Z}$ ismeretlent.

Megoldhatóság szükséges és elégséges feltétele, a megoldások száma

Def.: $a, b \in \mathbb{Z}$ esetén (a, b)-vel jelöljük a és b **legnagyobb közös osztó**ját, $[a, b]$-vel pedig a **legkisebb közös többszörös**ét.

Tétel: Az $a \cdot x \equiv b\ (m)$ akkor és csak akkor oldható meg, ha $(a, m)|b$, azaz a és m legnagyobb közös osztója osztója b-nek is. A megoldások száma az (a, m) darab maradékosztály $modulo\ m$.

Euklideszi algoritmus

Az algoritmus lényege, hogy **meghatározzuk két $a, b \in \mathbb{Z}$ szám legnagyobb közös osztóját**, azaz (a, b)-t. Első lépésként elosztjuk a-t maradékosan b-vel:
$a = k_1 \cdot b + m_1$
Ezután már (b, m_1)-t keressük:
$b = k_2 \cdot m_1 + m_2$
A további lépések képlete így néz ki:
$m_{i-2} = k_i \cdot m_{i-1} + m_i$
Az algoritmus addig megy, míg $m_i = 0$ lesz, ekkor megkapjuk, hogy $(a, b) = m_{i-1}$.

Példa: Legyen $a = 200, b = 72$, tehát $(200{,}72)$-t keressük:

$200 = 2 \cdot 72 + 56,$
$72 = 1 \cdot 56 + 16,$
$56 = 3 \cdot 16 + 8,$
$16 = 2 \cdot 8 + 0.$
Tehát $(200{,}72) = 8.$

Lineáris kongruencia megoldása Euklideszi algoritmussal

Adott egy $ax \equiv b\ (m)$ lineáris kongruencia. Először meg kell vizsgálni, hogy megoldható-e: az algoritmus segítségével kiszámoljuk (a, m)-t, és ha ez osztható b-vel, akkor van megoldás. Ezután az algoritmus során kapott maradékokat fordított sorrendben kifejezzük az egyenletekből, és így megkapjuk x-et. Konkrét példán bemutatva:

Példa: $59x \equiv 1\ (101), x = ?$

Először meghatározzuk $(59{,}101)$-t:

$101 = 1 \cdot 59 + \mathbf{42}$

$59 = 1 \cdot 42 + \mathbf{17}$

$42 = 2 \cdot 17 + \mathbf{8}$

$17 = 2 \cdot 8 + \mathbf{1}$

$8 = 8 \cdot 1 + 0 \implies (59{,}101) = 1;\ 1|1 \implies$ ∃megoldás, méghozzá 1.

Ezután az egyenletekből kifejezzük a maradékokat:

$42 = 101 - 1 \cdot 59 \equiv (-1) \cdot 59\ (101)$

$17 = 59 - 42 \equiv 59 - (-59) = 2 \cdot 59\ (101)$

$8 = 42 - 2 \cdot 17 \equiv (-1) \cdot 59 - 2 \cdot 2 \cdot 59 = (-5) \cdot 59\ (101)$

$1 = 17 - 2 \cdot 8 \equiv 2 \cdot 59 - 2 \cdot (-5) \cdot 59 = 12 \cdot 59\ (101)$, vagyis:

$1 \equiv 12 \cdot 59\ (101).$

$59x \equiv 1 \equiv 12 \cdot 59\ (101) \qquad / : 59$

$\underline{x \equiv 12\ (101).}$

11.tétel

Euler-féle φ-függvény

Def.: Az $a, b \in \mathbb{Z}$ számokat **relatív prím**nek nevezzük, ha $(a, b) = 1$.

Def.: Az n-hez **relatív prímek számát** 1 és n között $\varphi(n)$-nel jelöljük.

Tétel: Ha $(a, b) = 1$, akkor $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

$\varphi(n)$ meghatározása:

- ha $p \in \mathbb{Z}$ prímszám, akkor
  $\varphi(p) = p - 1$,
  $\varphi(p^\alpha) = p^\alpha - \frac{p^\alpha}{p} = p^\alpha - p^{\alpha-1}$.
- ha $n \in \mathbb{Z}$ tetszőleges egész szám, felírjuk kanonikus alakban:
  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$,
  Ekkor:
  $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}) =$
  $= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdot \ldots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$.

Példa: $\varphi(100) = ?$
$100 = 2^2 \cdot 5^2$, szóval
$\varphi(100) = \varphi(2^2) \cdot \varphi(5^2) = (2^2 - 2^1) \cdot (5^2 - 5^1) = 2 \cdot 20 = 40$.

Redukált maradékrendszer

Def.: Egy $R = \{c_1, c_2, \ldots, c_k\}$ halmaz **redukált maradékrendszer** $modulo\ m$, ha:

- $k = \varphi(m)$,
- $(c_i, m) = 1$ $\forall i$-re,
- $i \neq j \implies c_i \not\equiv c_j\ (m)$.

Állítás: Ha $c_1, c_2, \ldots, c_k$ redukált maradékrendszer $modulo\ m$ és $(a, m) = 1$, akkor $a \cdot c_1, a \cdot c_2, \ldots, a \cdot c_k$ is redukált maradékrendszer lesz $modulo\ m$.

Euler-Fermat-tétel

Tétel: Ha $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ és $(a, m) = 1$, akkor: $\boldsymbol{a^{\varphi(m)} \equiv 1\ (m)}$.

Kis Fermat-tétel

Tétel: Ha $p \in \mathbb{Z}^+$ prímszám, $a \in \mathbb{Z}$ és $(a, p) = 1$, akkor $\boldsymbol{a^p \equiv a\ (m)}$.

Két ismeretlenes, lineáris diofantikus egyenlet megoldása

Def.: Az olyan $ax + by = c$ alakú egyenletet, melyben $a, b, c \in \mathbb{Z}$ adott, $x, y \in \mathbb{Z}$ pedig ismeretlen**, kétismeretlenes, lineáris diofantikus egyenlet**nek nevezzük.

Megoldása: A cél lineáris kongruenciává alakítani az egyenletet:
$ax + by = c$ egyenletet átrendezzük:
$by = c - ax$, ez azzal ekvivalens, hogy
$b|c - ax$, tehát
$ax \equiv c\ (b)$ lineáris kongruenciát kapjuk, amit már csak meg kell oldani.

Példa:
$-3x + 13y = 36$
$13y \equiv 36\ (3)$
$y \equiv 36\ (3)$
$y \equiv 0\ (3)$, így: $y = 3t$
Most már csak x-et kell kiszámolni:
$-3x + 13 \cdot 3t = 36$
$-3x = 36 - 39t$
$x = 13t - 12$

Két kongruenciából álló kongruenciarendszer megoldása

Az egyik kongruenciát felírjuk olyan alakban, hogy behelyettesíthető legyen a másikba, kiszámoljuk így a másikat majd visszahelyettesítünk.

Példa:
$$\left.\begin{aligned} x &\equiv 3\ (7) \\ x &\equiv -1\ (8) \end{aligned}\right\} \quad x = ?$$
Az elsőből következik, hogy $x = 7k + 3$ alakú ($k \in \mathbb{Z}$), ezt kell behelyettesíteni a másodikba:
$7k + 3 \equiv -1\ (8) \quad /-3$
$7k \equiv -4\ (8) \quad /-8k$
$-k \equiv -4\ (8) \quad /\cdot(-1)$
$k \equiv 4\ (8) \Rightarrow k = 8l + 4$ alakú, ($l \in \mathbb{Z}$)
$x = 7k + 3 = 7(8l + 4) + 3 = 56l + 31$ alakú $\Rightarrow$
$x \equiv 31\ (56)$.

12.tétel

Számelmélet és algoritmusok

Tétel: Egy algoritmust akkor tekintünk jónak, ha **polinomrendű**, azaz ha a lépésszáma felülről becsülhető az input hosszának polinomjával. Az **exponenciális** lépésszámú algoritmus rossz.

Alapműveletek

Tétel: Az **összeadás** és a **kivonás** lépésszáma a számjegyek számával azonos, ezek tehát lineáris, azaz **polinomrendű** algoritmusok.

Tétel: A **szorzás** és az **osztás** is **polinomiális** (, de már nem lineáris).

Hatványozás az egész számok körében és a $modulo\ m$

Tétel: A **hatványozás nem polinomrendű** algoritmus, hanem **exponenciális**.

Tétel: Az **euklideszi algoritmus polinomrendű**, tehát hatékony.

Tétel: Ezekből következik, hogy a **maradékosztás** is **polinomiális**. (egy osztás, egy szorzás és egy kivonás).

Tétel: A $modulo\ m$ **összeadás, kivonás, szorzás, osztás is polinomiális**.

Tétel: **A $modulo\ m$ hatványozás is polinomrendű**.

Prímtesztelés

A feladat, hogy eldöntsük egy adott n számról, hogy prím-e. Az egyik módszer, hogy 1-től $\sqrt{n}$-ig ellenőrizzük az n-el való oszthatóságot. Előnye, hogy ha n összetettnek bizonyul, akkor ez megadja egy osztóját is, viszont exponenciális lépésszámú.

Sokkal hatékonyabb, polinomrendű algoritmus is létezik erre, a **Fermat-teszt**:

0. lépés: Feladat: egy adott n számról kell megállapítani, hogy prím-e.
1. lépés: Felveszük egy tetszőleges k számot, amire igaz, hogy $1 \leq k < n$.
2. lépés: Ha $k^{n-1} \not\equiv 1\ (n)$, akkor n nem prím.
Ha $k^{n-1} \equiv 1\ (n)$, akkor n valószínűleg prím.

A Fermat-teszt problémája, hogy hibázhat, azaz egy összetett számot is prímnek nézhet. Ennek kiküszöbölésére sokszor, sok k-ra kell végrehajtani a

tesztet. Ha a teszt kb. 200-szor lefutva is azt adja ki, hogy n prím, akkor nagy valószínűséggel igaza van.

Carmichael számok

Def.: Ha a prímtesztelés során n számról akarjuk eldönteni, hogy prím, és a Fermat-tesztet éppen egy $1 \leq k < n$ számon futtatjuk, akkor:

- ha $k^{n-1} \not\equiv 1\ (n)$, akkor azt mondjuk, hogy k **tanú**ja vagy **áruló**ja n-nek,
- ha $k^{n-1} \equiv 1\ (n)$, akkor azt mondjuk, hogy k **cinkos**a n-nek.

Tétel: Ha n-nek **létezik tanúja**, **akkor** a $modulo\ n$ redukált maradékrendszernek **legalább fele tanú**.

Tétel: Ha n-nek **létezik tanúja**, akkor a Fermat-teszt hibájának valószínűsége **legfeljebb** $\frac{1}{2}$.

Köv.: Ha n-nek létezik tanúja, és a Fermat-tesztet m-szer futtattuk le, akkor a Fermat-teszt hibájának valószínűsége legfeljebb $\frac{1}{2^m}$.

Def.: Ha n összetett szám, de $\forall a$: $(a, n) = 1$-re igaz, hogy $a^{n-1} \equiv 1\ (n)$, azaz ha nem létezik tanúja, csak cinkosa a redukált maradékrendszerben, akkor n-t **Carmichael-szám**nak nevezzük.

Nyilvános kulcsú titkosírás

Bármilyen üzenet átalakítható számjegyek szorzatává, feltehetjük tehát, hogy a titkosítandó üzenet sokszámjegyű számok szorzata. A rejtjelezés alapja, hogy legyen egy kódoló és dekódoló függvény: $x \to c(x),\ y \to D(y)$, amire teljesül a visszafejthetőség: $D\big(c(x)\big) = x$.

RSA-kódolás: Nyílt kulcsú titkosító algoritmus, mely napjaink egyik leggyakrabban használt titkosítási eljárása. Egy nyílt és egy titkos kulcs tartozik hozzá. A nyílt kulcs mindenki számára ismert, s ennek segítségével kódolhatják mások a nekünk szánt üzeneteiket. A nyílt kulccsal kódolt üzentet csak a titkos kulccsal tudjuk "megfejteni". Az RSA-eljárásban a következő módon generáljuk a kulcsokat és küldjük el az üzenetet:

0. lépés: p és q sokszámjegyű, véletlenszerű prímek felvétele.
1. lépés: $N := p \cdot q$ kiszámítása. (N lesz a nyílt és a titkos kulcs modulusa is),
2. lépés: $\varphi(N) = (p-1)(q-1)$ kiszámítása,
3. lépés: c szám választása úgy, hogy $1 < c < \varphi(N)$, illetve $\varphi(N)$-hez relatív prím legyen, azaz $\big(c, \varphi(N)\big) = 1$.
4. lépés: c-t nyilvánosságra hozzuk, ez lesz a nyilvános kulcs kitevője.

5. lépés: d szám választása úgy, hogy a $cd \equiv 1 \left(\varphi(N)\right)$ kongruencia teljesüljön, azaz $cd = 1 + k \cdot \varphi(N)$ minden k egészre.
d-t titokban tartjuk, ez lesz a tikos kulcs kitevője.

6. lépés: **A** el akar küldeni egy x üzenetet **B**-nek. Ehhez lekódolja azt **B** nyilvános kulcsával (c-vel): $e \coloneqq x^c \ mod \ N$, majd az e kódolt üzenetet elküldi.

7. lépés: **B** ezután a saját titkos kulcsát, d-t használva vissza tudja fejteni x-et c-ből a következő módon: $x = c^d \ mod \ N$.

(Wikipedia alapján)

Megj.: Azért működőképes, mert számok prímtényezős felbontására nem ismert hatékony algoritmus.

Az RSA-kódolás tehát használható arra a célra, hogy a címzett nyilvános kulcsával kódolt üzenetet csak a címzett olvashassa el (a titkos kulcsával). Viszont, mivel a kódoló/dekódoló függvények egymás inverzei, és így egy titkos kulccsal kódolt ellenőrzőösszeget fel lehet oldani a nyilvános kulccsal, az RSA tehát használható **digitális aláírás** előállításához is, azaz egy üzenetről ez alapján el tudjuk dönteni, hogy valóban attól jött, akitől várjuk.

13.tétel

Művelet fogalma

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

Csoport

Def.: H alaphalmazon a $*$ művelet:

- **kommutatív**, ha $a * b = b * a$, illetve
- **asszociatív**, ha $a * (b * c) = (a * b) * c \ \ \forall a, b, c \in H$-ra.

Def.: Ha a H alaphalmazon $*$ egy asszociatív művelet, akkor a $(H,*)$ párt **félcsoport**nak nevezzük.

Def.: Legyen $*$ művelet a H alaphalmazon. $e \in H$-t **egységelem**nek nevezzük, ha $\forall a \in H$-ra: $a * e = e * a = a$.

Def.: Legyen $*$ művelet a H alaphalmazon és $e \in H$ egységelem. Ekkor egy $a \in H$ **inverz**e $b \in H$, ha $a * b = b * a = e$. Jele: $a^{-1} = b$.

Def.: Ha a H alaphalmazon $*$ egy asszociatív művelet, létezik egységelem és minden elemnek van inverze, akkor a $(H,*)$ párt **csoport**nak nevezzük.

Abel-csoport

Def.: Ha $(H,*)$ félcsoport és $*$ kommutatív, akkor $(H,*)$ -t **Abel-félcsoport**nak nevezzük.

Def.: Ha $(H,*)$ csoport és $*$ kommutatív, akkor $(H,*)$-t **Abel-csoport**nak nevezzük.

Példák csoportokra

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ csoport,
- $(\mathbb{N}, +)$ viszont nem csoport, mert a pozitív tagoknak nincs inverze,
- $(\mathbb{Z},\cdot), (\mathbb{Q},\cdot), (\mathbb{R},\cdot), (\mathbb{C},\cdot)$ sem csoport, mivel a 0-nak nincs inverze, viszont
- $(\mathbb{Z}\backslash\{0\},\cdot), (\mathbb{Q}\backslash\{0\},\cdot), (\mathbb{R}\backslash\{0\},\cdot), (\mathbb{C}\backslash\{0\},\cdot)$ már csoport lesz.
- Ha $H \coloneqq \{n \times m$-es mátrixok$\}$, akkor $(H, +)$ csoport
- Ha $H \coloneqq \{n \times n$-es mátrixok, amelyekre $det \neq 0\}$ és $*$ a mátrixszorzás művelete, akkor $(H,*)$ csoport.

Rajzok szimmetriacsoportja

Def.: Legyen $H \coloneqq \{R$ rajznak – pl. szabályos háromszög – a szimmetriái/egybevágódási transzformációi$\}$, a $\circ$ művelet pedig a függvénykompozíció. Ekkor a $(H,\circ)$ párost **szimmetriacsoport**nak nevezzük.

Tétel: Az R szimmetriacsoport csoport.

Diédercsoport

Def.: Egy n-oldalú szabályos sokszög szimmetriacsoportját **diédercsoport**nak nevezzük.

Jele: D_n

Példák véges és végtelen, kommutatív és nem kommutatív csoportra

- **Végtelen, nem kommutatív** csoportot alkotnak például:
  $(\mathbb{R}^{n\times n}|\det \neq 0,\ \cdot)$,
- **Végtelen, kommutatív** (Abel-)csoportot alkotnak például:
  $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+),(\mathbb{R}^{n\times m},+)$,
  $(\mathbb{Z}\backslash\{0\},\cdot),(\mathbb{Q}\backslash\{0\},\cdot),(\mathbb{R}\backslash\{0\},\cdot),(\mathbb{C}\backslash\{0\},\cdot)$.
- **Véges, nem kommutatív** csoportot alkot például:
  $(\{E,A,A^{-1}|\ A\in\mathbb{R}^{n\times n},\det A\neq 0\},\ \cdot)$.
- **Véges, kommutatív** (Abel-)csoportot alkotnak például:
  $(\{0;a;\ -a\mid a\in\mathbb{R}\},+),\left(\left\{1;a;\ \frac{1}{a}|\ a\in\mathbb{R}\right\},\ \cdot\right)$.

14.tétel

Elem rendje

Def.: Egy G csoport elemeinek számát a **csoport rendjé**nek nevezzük, és $|G|$-vel jelöljük. Például: $|D_n| = 2n, |S_n| = n!$ *(Utóbbit lásd később!)*

Def.: Ha G csoport és $g \in G$, akkor:
$g^n = g * g * \ldots * g$ $(n\ db)$.

Példa: A $(\mathbb{Z}, +)$ csoport esetén $3^5 = 3 + 3 + 3 + 3 + 3 = 15$.

Tétel: Ha G **véges** csoport és $g \in G \Longrightarrow \exists n \geq 1$, hogy $g^n = e$.

Def.: Ha G csoport és $g \in G$, akkor a g **elem rendje** az a legkisebb olyan $k \geq 1$ kitevő, amire: $g^k = e$. (Ha nincs ilyen szám, akkor végtelen rendű elemről beszélünk.)

Jele: $\sigma(g) = k$.

Ciklikus csoport

Def.: Egy tetszőleges G csoportot **ciklikus csoport**nak nevezünk, ha $\exists g \in G$ ún. **generátorelem**, amiből G minden másik eleme kifejezhető G művelete és az inverzképzés segítségével.

Tétel: G véges, ciklikus csoport $\Leftrightarrow$ $\exists g \in G$, amire $\sigma(g) = |G|$.

Részcsoport

Def.: Ha $(G,*)$ csoport, $H \subseteq G$ és H is csoport a $*$ műveletre nézve, akkor azt mondjuk, hogy H **részcsoport**ja G-nek.

Példa: Ha $G \coloneqq \mathbb{R}$, $H \coloneqq \{0, a;\ -a \mid a \in \mathbb{R}\}$, akkor $H \leq G$, azaz H G részcsoportja a $+$ műveletre.

Szimmetrikus csoport

Def.: Az $f: \{1,2, \ldots, n\} \to \{1,2, \ldots, n\}$ kölcsönösen egyértelmű függvényt **permutáció**nak nevezzük.

Def.: Az $\{1,2, \ldots, n\}$ halmaz csoportot alkot a függvénykompozíció műveletére nézve, és ezt a csoportot **szimmetrikus csoport**nak nevezzük.

Jele: S_n.

Csoportok izomorfiája

Tétel: Azonos rendű ciklikus csoportok izomorfak.

Cayley tétele

Tétel: Ha G egy véges csoport, akkor $\exists n$, hogy $H \leq S_n$ és $H \cong G$, azaz S_n egy részcsoportja izomorf lesz G-vel.

15.tétel

Mellékosztály

Def: Legyen $(G,*)$ csoport, $g \in G, H \leq G$. Ekkor a $\{g * h \mid h \in H\}$ halmaz a H részcsoport g szerinti bal oldali **mellékosztály**a.

Jele: gH.

Példa: Legyen $G \coloneqq (\mathbb{R}^2, +), H \coloneqq \{(x,0)|x \in \mathbb{R}\}$ (x tengely vektorai).

- $g \coloneqq (2,3) \rightarrow gH = (2,3) + H = \{(x+2,3)|x \in \mathbb{R}\}$.
- $g \coloneqq (3,-1) \rightarrow gH = (3,-1) + H = \{(x+3,-1)|x \in \mathbb{R}\}$.
- $g \coloneqq (5,0) \rightarrow gH = (5,0) + H = \{(x+5,0)|x \in \mathbb{R}\}$.

Lagrange tétele

Tétel: Ha G véges csoport, akkor $\forall H \leq G$-re $|H| \mid |G|$, azaz H rendje osztója G rendjének minden H részcsoportra.

Elem és csoport rendjének kapcsolata

Tétel: G bármely g elemének rendje (amely gyakorlatilag g által generált részcsoport elemszáma) osztja G rendjét, azaz $\sigma(g) \mid |G| \; \forall g \in G$-re.

16.tétel

Def.: Legyen R egy tetszőleges halmaz, $+$ és $\cdot$ R-en értelmezett műveletek. A két művelet **disztributív**, ha $\forall a,b,c \in R$ -re: $a(b+c) = ab + ac$ és $(a+b)c = ac + bc$.

Gyűrű fogalma

Def.: Az $(R,+,\cdot)$ algebrai struktúrát **gyűrű**nek nevezzük, ha:

- $(R,+)$ **Abel-csoport**, azaz ha $+$ kommutatív, asszociatív, létezik egységelem és inverz,
- $(R,\cdot)$ **félcsoport**, azaz ha $\cdot$ asszociatív,
- $+$ és $\cdot$ **disztributív** műveletek R-en.

Def.: Ha $(R,+,\cdot)$ gyűrű, és $(R,\cdot)$ Abel-félcsoport, azaz ha a $\cdot$ művelet is kommutatív, akkor $(R,+,\cdot)$-t **kommutatív gyűrű**nek nevezzük.

Ferdetest fogalma

Def.: Ha $(R,+,\cdot)$ gyűrű, és $(R\backslash\{0\},\cdot)$ is csoport, azaz ha a $\cdot$ műveletnek is van egységeleme és inverze, akkor $(R,+,\cdot)$-t **ferdetest**nek nevezzük.

Test fogalma

Def.: Ha Ha $(R,+,\cdot)$ kommutatív gyűrű és ferdetest, akkor **test**nek nevezzük. Más megfogalmazásban$(R,+,\cdot)$ test, ha $(R,+)$ és $(R\backslash\{0\},\cdot)$ is Abel-csoport.

Összefoglaló táblázat

$(R,+,\cdot), a,b,c \in R$:

(1) $a+b=b+a$ (kommutatív)	(a) $a\cdot b = b\cdot a$ (kommutatív)
(2) $(a+b)+c = a+(b+c)$ (asszociatív)	(b) $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ (asszociatív)
(3) $\exists 0 \in R: a+0=0+a=a$ (nullelem)	(c) $\exists 1 \in R: a\cdot 1 = 1\cdot a = a$ (egységelem)
(4) $\forall a$-ra $\exists(-a) \in R: a+(-a)=0$ (additív inverz)	(d) $\forall a \neq 0$-ra $\exists(a^{-1}) \in R: a\cdot a^{-1}=1$ (multiplikatív inverz)
(5) $a(b+c) = ab+ac;\ (a+b)c = ac+bc$ (disztributív)	

Gyűrű: (1-5), (b),
Kommutatív gyűrű: (1-5), (a-b),
Ferdetest: (1-5), (b-d),
Test: (1-5), (a-d),

Nullosztómentesség

Def.: Egy $(R,+,\cdot)$ gyűrűben egy $a \neq 0$ **nullosztó**, ha $\exists b \neq 0$, hogy $a \cdot b = 0$ $(a, b \in R)$.

Def.: Az $(R,+,\cdot)$ gyűrű **nullosztómentes**, ha nem tartalmaz nullosztót, azaz ha $\forall a, b \in R$-re az $a \cdot b = 0$ csak akkor teljesül, ha $a = 0$ vagy $b = 0$.

Tétel: **Minden test nullosztómentes.**

Példák

- $(\mathbb{R},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{C},+,\cdot)$ test.
- $(\mathbb{Z},+,\cdot)$ nem test, mert nem létezik minden elemnek inverze – (c) sérül – így csak kommutatív gyűrű.
- $(\mathbb{R}^{n\times n},+,\cdot)$ nem test, mivel a nemnulla determinánsú mátrixoknak nincs inverze, és a mátrixszorzás nem kommutatív – (a) és (c) sérül –, így csak egységelemes gyűrű.
- $(\mathbb{R}[\mathrm{x}],+,\cdot)$ és $(\mathbb{Z}[\mathrm{x}],+,\cdot)$, azaz a valós és egész együtthatójú polinomok az összeadásra és a szorzásra nézve kommutatív gyűrűt alkotnak. Azért nem testet, mert nem létezik multiplikatív inverz – (c) sérül –, mert pl. egy $x \in \mathbb{R}[\mathrm{x}]$ polinom inverze $\frac{1}{x} \notin \mathbb{R}[\mathrm{x}]$ lenne.
- A valós polinomok hányadosteste test: $\mathbb{R}(\mathrm{x}) \coloneqq \left\{\frac{p}{q} : p, q \in \mathbb{R}[\mathrm{x}], \mathrm{q} \not\equiv 0\right\}$. A műveletek: $\frac{p}{q} + \frac{r}{s} = \frac{ps+qr}{qs}$, illetve $\frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$
- $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ halmaz esetén $(\mathbb{Q}\sqrt{2},+,\cdot)$ is test.

$\mathbb{Z}_n$ fogalma és ez milyen n-re test

Def.: Egy $Z = \{0, 1, \dots, n-1\}$ halmazt a $modulo\ n$ összeadásra ill. szorzásra nézve a ***modulo n* maradékosztályok gyűrűjé**nek nevezzük és $\mathbb{Z}_n$-el jelöljük.
$\mathbb{Z}_n = (Z,\oplus,\odot)$:
$a \oplus b = (a + b)\ mod\ n$
$a \odot b = (a \cdot b)\ mod\ n$

Példa: $\mathbb{Z}_{10}$ esetén:
$7 \oplus 8 = (7 + 8)\ mod\ 10 = 15\ mod\ 10 = 5$
$7 \odot 8 = (7 \cdot 8)\ mod\ 10 = 56\ mod\ 10 = 6$

Tétel: $\mathbb{Z}_n$ **akkor és csak akkor test**, ha n **prím**.