Hamilton-kör (-út): olyan kör (út) ami a gráf $\forall$ csúcsát tartalmazza.

Szükséges feltétel: Ha G-ben $\exists$ H-kör (-út) $\Rightarrow$ akárhogy k csúcsot törölve G'-nek legfeljebb k ($k+1$) komponense van

Biz: Ha G = H-kör (-út) $\not\supset$ azaz $\forall$ élet is tartalmaz $\Rightarrow$ egyértelmű, ha további élek is vannak $\Rightarrow$ pontok törlésével a komponensek száma csak csökkenhet.

Elégséges feltételek:

Dirac-tétel: Ha G n csúcsú ($n \geq 3$), egyszerű és $\forall v$-re $d(v) \geq \frac{n}{2}$ $\Rightarrow$ $\exists$ H-kör

$\Leftarrow$

Ore-tétel: — " — és $\forall u, v$ nem szomszédos csúcsokra

$d(u)+d(v) \geq n \Rightarrow \exists$ H-kör

$\Leftarrow$

Indirekt Biz: G-re teljesül $d(u)+d(v) \geq n$, de $\not\exists$ H-kör, G a legtöbb ~~élű~~ ilyen gráf $\Rightarrow$

~~+~~ + él behúzása nem rontja el $\rightarrow$, de egy élet behúzva már $\exists$ H-kör $\Rightarrow$

$\Rightarrow \exists$ H-út $u \to v$: $u = x_1, x_2, \dots, x_n = v$

$K = \{x_i : x_i$ szomszédos v-vel$\}$ $|K| = d(v)$

$P = \{x_{i+1} : x_i$ — " — u-val$\}$ $|P| = d(u)$

~~a másikban~~ $v \notin K, v \notin P \Rightarrow d(u)+d(v) \leq n-1$ ↯

Euler-út (kör): (zárt) élsorozat ami a gráf $\forall$ élét pontosan egyszer tartalmazza.

$\exists$ feltétele: Ha G összefüggő és (legfeljebb 2 kivétellel) $\forall$ pont foka páros $\Leftrightarrow \exists$ E-kör(-út)

Biz: $\Leftarrow$: az élsorozat éleit a bejárás irányítsa az egy csúcsba be- és ki menő élek száma egyenlő (kivéve esetleg az első és utolsó csúcsot szerint) $\Rightarrow d(v) = k+k = 2k \Rightarrow$ biztosan páros

$\Rightarrow$ E-kör: tetszőleges $v \in V(G)$ -ből élismétlés nélküli élsorozatot (p) rajzolunk amíg elakad.

$\forall$ pont foka páros $\Rightarrow$ v-ben akad el és minden élét felhasználta, $\forall$ csúcsból páros számú élet használt.

$\Downarrow$

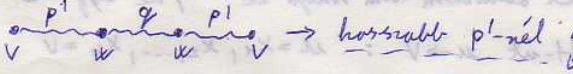
p' erek körül a leghosszabb.

p' E-kör, mert ha nem az lenne:

$G' = G - p'$ élei : G'-ben is $\forall$ fokszám páros ($ps = ps - ps$)

w: csúcs, melynek van és p'-beli éle is

q: w-ből indulló élismétlés nélküli w-ben elakadó élsorozat.



→ hosszabb p'-nél ↯

$\Rightarrow$ E-út: - ha $\forall$ fok ps $\Rightarrow$ E-kör, ez egyben E-út is.

- ha van 2db páratlan fokú pont (u, v) G-ben

G'-ben : összekötjük őket $\Rightarrow$ E-kör, amiz a + élet elhagyva G-ben $\exists$ E-út

G gráf k színnel színezhető, ha csúcsai k színnel megszínezhetők úgy, hogy a szomszédos csúcsok különböző színűek legyenek.

G kromatikus száma k $(\chi(G)=k)$, ha k színnel színezhető, de $k-1$-gyel nem.

G max klikkmérete k $(\omega(G)=k)$, ha $\exists$ k db csúcs, hogy közülük bármely 2 szomszédos, de $k+1$ nem.

$\Delta(G)$ = a legnagyobb fokszám G-ben

Tétel: $\omega(G) \leq \chi(G)$ $\forall$ gráfra

Biz: $\omega(G)=k$ -hoz kell k db szín.

Mohó színezés: csúcsok: $v_1, \dots, v_n$ színek: ①, ②, ...

v_i színe: a legkisebb sorszámú olyan szín, amilyen színű szomszédja még nincs.

Tétel: $\chi(G) \leq \Delta(G)+1$

Biz: a mohó színezés $\leq \Delta(G)+1$ színt használ

a $d(v)=\Delta(G)$ csúcs szomszédainak kell $\Delta(G)$, neki meg a $+1$ szín

Brooks-tétel: G egyszerű, öt, $G \neq K_n$, $G \neq C_{2k+1} \Rightarrow \chi(G) \leq \Delta(G)$

($\Delta = n-1$, $\chi = n$)

Mycielski-konstrukció: $\forall$ $3 \leq k \in \mathbb{N}$ -hez $\exists$ G_k amire $\omega(G_k)=2$, $\chi(G_k)=k$

Biz: G_k-ból létrehozunk egy H-t úgy hogy $\omega(H)=2$, $\chi(H)=k+1$

$V(G)=\{v_1, \dots, v_n\}$

$V(H)=V(G) \cup \{v_1', \dots, v_n'\} \cup \{w\}$

Ha v_i össze van kötve v_j-vel akkor v_i'-t is összekötjük v_j-vel és w-t összekötjük mindegyik v_i'-vel.

$\omega(H)=2 \Rightarrow \nexists \Delta \Leftarrow$ G-ben nem volt sehol nincs és v_i'-t v_i nincs összekötve

$\chi(H)=k+1 \Rightarrow$ v_i'-k színezhetőek v_i-k színeivel, w-hez kell $+1$ szín

és k db színnel nem színezhető $\Rightarrow$ G $k-1$ színnel lenne színezhető ↯

Tehát létrehoztunk egy G_k-hoz egy G_{k+1}-t és ez tetszőlegesen folytatható.

5-szín tétel: G egyszerű, síkba rajzolható $\Rightarrow \chi(G) \leq 5$

Biz:

$\exists$ v csúcs: $d(v) \leq 5$, mert ha $\forall\, d(v) \geq 6$ lenne $\Rightarrow$ nem teljesülne $e \leq 3n-6$

$e = \frac{\sum d(v)}{2}$

teljes indukció: tegyük fel, hogy igaz n csúcsú és kisebb G-re

$\Downarrow$

igaz $n+1$ csúcsúra is

v: $d(v) \leq 5$

ha $d(v) \leq 4$
v-nek jut az 5 színből
v-t törölve 5 színnel színezhető

ha $d(v) = 5$
szomszédai közt kell lennie 2 nem szomszédosnak
(különben K_6 lenne $\lightning$)
ez a 2 színezhető ugyan azzal $\Rightarrow$ elég ide is 5 szín.

G élkromatikus száma k ($\chi_e(G) = k$), ha élei k színnel színezhetők úgy, hogy 1 csúcsra illeszkedő élek különböző színűek, de $k-1$-gyel nem.

Tétel: $\Delta(G) \leq \chi_e(G)$

Biz: a $d(v) = \Delta(G)$ csúcsból induló éleknek kell $\Delta(G)$ db szín

Vizing-tétel: G egyszerű $\Rightarrow \chi_e(G) \leq \Delta(G) + 1$

G perfekt, ha $\chi(G) = \omega(G)$ és ez igaz $\forall$ feszített részgráfjára is.

Erős perfekt gráf tétel: G perfekt $\Leftrightarrow$ nincs benne C_{2k+1} vagy $\overline{C_{2k+1}}$ $(k \geq 2)$ feszített részgráfként

Biz $\Rightarrow$:

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

$\omega(\overline{C_{2k+1}}) = 2$, $\chi(\overline{C_{2k+1}}) = 3$

$\omega(G) = k$, $\chi(G) \geq k+1$

Lovász-tétel: G perfekt $\Leftrightarrow$ $\overline{G}$ perfekt

Biz: ha G-ben nincs C_{2k+1} vagy $\overline{C_{2k+1}}$, $k \geq 2$, akkor $\overline{G}$-ben sincs.

Intervallum-gráf: $V(G) = \{$a számegyenes korlátos és zárt intervallumai$\}$

$E(G) = \{\{I_i, I_j\}: i \neq j$ és [illegible] metszik egymást$\}$

Tétel: $\forall$ intervallum gráf perfekt

Biz:
- int. gráf $\forall$ feszített részgráfja is int. gráf
- ha $\omega(G) = k$, akkor a mohó színezés az intervallumok baloldali végpontja szerinti növekvő sorrendben k színnel jó színezést ad.
- ha $k+1$ szín kellene I_j-nél $\Rightarrow$ előtte k [illegible] színű intervallum metszette egymást és I_j-t, azaz $\omega(G)$ is $= k+1$

Irányított gráf: $\vec{G}$

$\vec{G}$ emeletekre bontható, ha $V(\vec{G})$ felvágható diszjunkt részekre $(V_1, \dots, V_k)$ úgy, hogy él csak kisebb sorszámú részből a nagyobb sorszámúba megy, fordítva nem.

Irányított kör: 

Tétel: $\vec{G}$ emeletekre bontható $\Leftrightarrow \nexists$ benne $\vec{C}$ (azaz aciklikus)

Biz: $\Rightarrow$: él csak előre megy

$\Leftarrow$: $\vec{G}$-beli nyelők lesznek az utolsó emelet, őket törölve $\vec{G}'$-beli nyelők lesznek az utolsó előtti emelet, stb.

Lemma: $\vec{G}$ aciklikus $\Rightarrow \exists$ benne nyelő és forrás

Biz: tetszőleges csúcsból irányított élsorozaton haladva elakadunk, mert nincs kör és véges sok csúcs van, ahol elakadtunk az nyelő

ugyanez visszafelé és megtaláljuk a forrásokat.

PERT-módszer

$V(\vec{G})$ = részfeladatok

$E(\vec{G})$ = precedenciák: az él elejénél levő feladatnak előbb kell végrehajtódnia, mint a végénél levőnek

él súlya ($\xrightarrow{5}$): az idő aminek el kell telnie az korábbi feladat elkezdésétől a későbbi elkezdéséig.

cél: ütemezés: kezdési idők és kritikus részfeladatok meghatározása

I. emeletekre bontás

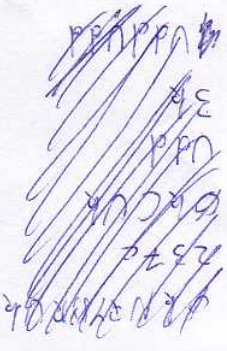
II. kezdési idők meghatározása: $y_1 \xrightarrow{t_1} y_3 = MAX(y_1+t_1; y_2+t_2)$, $y_2 \xrightarrow{t_2} y_3$

az első részfeladatra $y_0 = \emptyset$

III. kritikus részfeladatok meghatározása: amelynek a csúszása a teljes folyamat befejeződésének csúszását jelentené

az utolsó részfeladattól visszafele ellenőrizzük,

az első és az utolsó (ha 1-1 van belőlük) mindig kritikus



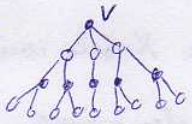
G **páros gráf**, ha $V(G)$ 2 diszjunkt részre vágható úgy, hogy $\forall$ él a két rész között fut

$G(A,B,E)$ (azaz $\chi(G) \leq 2$)

Tétel: G páros $\Leftrightarrow \nexists$ benne C_{2k+1} ($\Rightarrow \forall$ fa páros)

Biz: $\Rightarrow$ csak C_{2k} lehet benne, különben részcsaptelen belül futna él, C_{2k+1} nem színezhető 2 színnel (vagy semmilyen)

$\Leftarrow$ öl. részben tetszőleges v csúcs:



ha azonos színű csúcsok szomszédosak volnának $\Rightarrow$ legkörelebbi ősükön keresztül lenne ppáratlan kör $\lightning$

$M \subseteq E(G)$ **párosítás** (= független élhalmaz), ha semelyik 2 benne levő élnek nincs közös végpontja

(TP) **teljes párosítás**, ha $\forall$ csúcsra illeszkedik M-beli él.

$\nu(G)$ = maximális párosítás éleinek száma (= független élek max száma)

$X \subseteq V(G)$ **lefogó ponthalmaz**, ha $\forall$ él tartalmaz X-beli csúcsot

$\tau(G)$ = minimális lefogó ponthalmaz elemszáma

Tétel: $\nu(G) \leq \tau(G)$

Biz: $\forall X$ lefog minden élet, így M-t is, de minden X-beli pont max. 1 M-beli élet foghat le.

Párosítás páros gráfokban (magyar módszer)

I. független élek felvétele amíg lehet

II. javító út keresése és annak mentén a párosítás növelése amíg lehet.

Alternáló út: $G(A,B,E)$, M párosítás, párosítatlan A-beli csúcsból indul, $\forall$ második éle M-beli

Javító út: alternáló út, ami párosítatlan B-beli csúcsban ér véget.

Tétel: Ha $\nexists$ javító út $\Rightarrow M$ max. párosítás

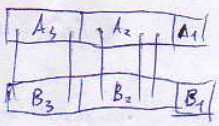
Biz: az algoritmus k élű M-t adott, k pontú X-t keresünk $\Rightarrow k \leq \nu(G) \leq \tau(G) \leq k \Rightarrow k = \nu(G)$

A_1, B_1 : párosítatlanok

A_2 : B_1-ből alternáló úton el lehet jutni, $A_2 \cap A_1 = \emptyset$, mert $\nexists$ jav. út.

B_2 : A_2 párjai M- szerint

A_3, B_3 : maradék



$B_1 \cup B_2$ -ből nem vezet él $A_1 \cup A_3$ -ba, mert A_1-B_1 1 élű jav. út lenne, A_3-B_1 1 élű alt. út lenne,
A_1-B_2 + A_2-B_1 — " — , $B_2 \subseteq A_3 \Rightarrow$ nem A_3-ban kellene lennie.

König-tétel: G páros $\Rightarrow \nu(G) = \tau(G)$ **biz:** magyar módszer; k élű $\overset{M}{\prec}_X \Rightarrow k \leq \nu(G) \leq \tau(G) \leq k \Rightarrow \nu(G) = \tau(G)$

Hall-tétel: $G(A,B,E)$ páros, $\exists$ A-t lefedő párosítás $\Leftrightarrow \forall Y \subseteq A$-ra $|Y| \leq |N(Y)|$ ($N(Y) = Y$ szomszédai (B-ben))

Biz: $\Rightarrow$ mivel $\forall$ A-belinek van párja ezért bármely Y szomszédainak száma legalább $|Y|$

$\Leftarrow$ magyar módszer $\rightarrow M$, ha M lefedi A-t akkor OK, ha nem $\Rightarrow$ láttuk, hogy $\nexists$ $(A_1 \cup A_2)$-$(B_1 \cup B_2)$ él, azaz $N(A_1 \cup A_2) = B_2 \Rightarrow |A_2| = |B_2| \Rightarrow |A_1 \cup A_2| > |B_2| \Rightarrow Y = A_1 \cup A_2$ sérti a Hall-feltételt $\Rightarrow \lightning$

Frobenius-tétel: $G(A,B,E)$, $\exists$ TP $\Leftrightarrow |A| = |B|$ és $\forall Y \subseteq A$-ra $|Y| \leq |N(Y)|$

Biz $\Leftarrow$ Hall-tétel $\Rightarrow \exists$ A-t lefedő párosítás és $|A| = |B| \Rightarrow$ TP

$\Rightarrow$ TP $\forall$ csúcsot tartalmaz, de 2 éle közöset nem $\Rightarrow |A| = |B|$ kell, A-t fedi $\Rightarrow$ Hall-tétel $\Rightarrow |Y| \leq |N(Y)|$

Tutte-tétel: G-ben $\exists$ teljes párosítás $\iff$ $\forall X \subseteq V(G)$-re $c_p(G-X) \leq |X|$

G-ből X csúcsait elhagyva G' páratlan pontú komponenseinek száma

Biz $\Rightarrow$: páratlan pontú komponensen belül nem lehet TP, azaz $|X| \geq c_p(G-X)$ kell, hogy ha visszarakjuk őket akkor a visszakerülő élek TP-sá egészíthessék ki a reménylegesetet.

$X \subseteq V(G)$ **független ponthalmaz**, ha X-beli csúcsok nem szomszédosak

$\alpha(G)$ = max. független ponthalmaz elemszáma

$X \subseteq E(G)$ **lefogó élhalmaz**, ha $\forall$ csúcsra illeszkedik X-beli él

$\varrho(G)$ = min. lefogó élhalmaz elemszáma

	független max	lefogó min
élek	ν	ϱ
pontok	α	τ

$\alpha(G) \leq \varrho(G)$

$\nu(G) \leq \tau(G)$

Gallai-tételek: G tetszőleges, n csúcsú

- hurokél mentes $\Rightarrow \alpha(G) + \tau(G) = n$
- izolált pont mentes $\Rightarrow \nu(G) + \varrho(G) = n$

Köv: G páros $\Rightarrow \nu = \tau$, $\alpha = \varrho$

Biz I: $X \subseteq V(G)$ fü. $\iff V(G) \setminus X$ lefogó

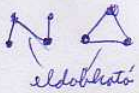
$\hookrightarrow |X| = \alpha(G)$ (fü.), $|V(G) \setminus X| = n - \alpha(G)$ (lefogó) $\Rightarrow \tau(G) \leq n - \alpha(G)$

$\hookrightarrow |Y| = \tau(G)$ (lefogó), $|V(G) \setminus Y| = n - \tau(G)$ (fü.) $\Rightarrow \alpha(G) \geq n - \tau(G)$

Biz II: max párosítás $\Rightarrow \nu(G)$, ez azonosít $2 \cdot \nu$ db csúcsot, maradék csúcsok száma: $n - 2\nu$

lefogó élhalmazba kellenek a fü. élek + a maradék csúcsokra illeszkedő 1-1 él, azaz

$\nu(G) + (n - 2 \cdot \nu(G)) = n - \nu(G) \geq \varrho(G)$

min. lefogó élhalmazban nem lehet :  $\Rightarrow Y = \{k$ db diszjunkt csillag$\}$

mivel a csillagok csúcs-száma = élek száma + 1, ezért

$|Y| = \varrho(G) = n - k$ és $\nu(G) \geq k \Rightarrow n - \nu(G) \leq \varrho(G)$

$\varrho(G) + \nu(G) = n$

Hálózat: $(\vec{G}, s, t, c)$, $s, t \in V(\vec{G})$, $c: E(\vec{G}) \to \mathbb{R}^+$ — 1(1) → (1) kapacitás, 1 aktuális érték

Folyam: $f: E(\vec{G}) \to \mathbb{R}^+$ amire $\forall \to 0 \le f(e) \le c(e)$ $\forall$ élre
$\to \forall$ (nem s,t) csúcsra a befutó élek Σértéke = a kifutó élek Σértékével

Folyam-értéke: m_f = s-ből kijövő Σ érték = t-be menő Σ érték

st-vágás (C): X és $V(G)\setminus X$ közt menő élek, ha $X \subseteq V(\vec{G})$, $s \in X$, $t \notin X$
értéke: $c(C) = \sum c(e^*)$, e^* az X-ből $V(G)\setminus X$-be menő él

Állítás: $m_f \le c(C)$

Maximális folyam meghatározása

I kiindulás tetszőleges folyamból (pl.: $f \equiv 0$)

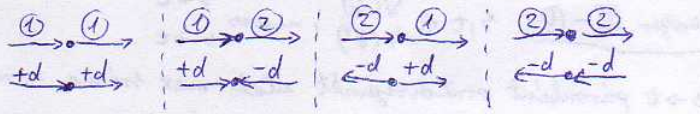
II javítás amíg m_f nő

H_f segédgráf: $V(H_f) = V(\vec{G})$, ha $f(\vec{xy}) < c(\vec{xy}) \Rightarrow \vec{xy} \in H_f$ $\quad c'(\vec{xy}) = c(\vec{xy}) - f(\vec{xy})$ ①
ha $f(\vec{xy}) > 0 \Rightarrow \vec{yx} \in H_f$ $\quad c'(\vec{xy}) = f(\vec{xy})$ ②

Javító-út: H_f-ben irányított út s-ből t-be

Javítás: a jav. úton annyit viszünk amennyit lehet, majd az eredeti $\vec{G}$-ben ez az értéket hozzáadjuk a régi $f(e)$-hez ha normál, levonjuk ha fordított irányú e-n vittük

Állítás: javítás után f folyam marad **Biz**: H_f / $\vec{G}$



Tétel: $\nexists$ jav. út H_f-ben $\Rightarrow f$ maximális folyam

Biz: $c(C) = m_f$ vágás mutatása
$X = \{$csúcsok ahova s-ből vezet irányított út H_f-ben$\} \Rightarrow s \in X$, $t \notin X$ mert már nincs jav. út
$\forall$ X-ből kijövő élre $f(e) = c(e)$ különben $X \xrightarrow{e} V(\vec{G})\setminus X$ $e \in H_f$ ↯
$\forall$ X-be bemenő élre $f(e) = 0$
Ekkor X és $V(G)\setminus X$ közt futó élek alkotta vágásra igaz $c(C) = m_f$

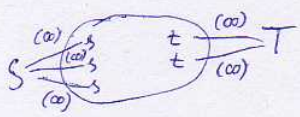
Ford-Fulkerson-tétel: $\exists \max m_f = \min c(C)$ **Biz**: ←

Edmonds-Karp-tétel: Ha H_f-ben mindig a legrövidebb javító utat választjuk, akkor az algoritmus véges sok lépés után leáll, a lépésszám felülről becsülhető $|V(G)|$ polinomjával

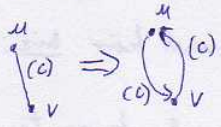
Egészértékűségi lemma: Ha $\forall c(e) \in \mathbb{Z} \Rightarrow \exists f$ maximális folyam, hogy $\forall f(e) \in \mathbb{Z}$
Biz: a jav. utas algoritmus nem lép ki $\mathbb{N}$-ből

A folyamprobléma általánosításai

több forrás / cél



irányítatlan él



kapacitással rendelkező pont

$Y \subseteq E(\vec{G})$ *lefogja* az $s \to t$ utakat, ha $\forall$ $s \to t$ út tartalmaz Y-beli élt.

Menger I: $s \to t$ páronként éldiszjunkt irányított utak max. száma $= \min |Y|$ $\quad s,t \in V(\vec{G})$

Biz: Y definíciójából következik, hogy a .... — " — $\leq \min |Y|$

tegyük fel, hogy $\forall c(e) = 1$, $\max m_f = \min c(C) = k$ $\Longrightarrow$ van $\emptyset$ vagy 1 értékű folyam is a Egész lemma k értékűek közt.

Egy $s \to t$ út $\forall$ élének értékét $1 \to \emptyset$ $\Rightarrow$ $k-1$ értékű folyam
" " — $\Rightarrow$ $k-2$ — " — } k db éldiszjunkt út

A k értékű vágás $X \to V(\vec{G}) \setminus X$ élei pedig lefogják az $s \to t$ utakat, ez k db él

Menger II: ugyanaz mint az I csak $s,t \in V(G)$

Biz: az éleket átrajzoljuk  $\Rightarrow$  és alkalmazzuk az I bizonyítást

az  eseteket feloldva $\Rightarrow$ 

az irányított utak "ősei" adnak k db irányítatlan páronként éldiszjunkt utat
a $\vec{G}$-beli lefogó élek ősei pedig lefogják a G-beli $s \to t$ utakat $\Rightarrow k$ db él

$X \subseteq V(G)$ *lefogja* az $s \to t$ utakat, ha $\forall$ $s \to t$ út tartalmaz X-beli pontot

Menger III–IV: $s,t \in \begin{matrix} V(G) \\ V(\vec{G}) \end{matrix}$, nincs $\begin{matrix} s-t \\ s \to t \end{matrix}$

$s \to t$ páronként pontdiszjunkt utak max száma $= \min |X|$ (s-t és t-t nem számolva!)

Biz: a pontokat szétbontjuk élekké és I. biz. / a lefogó éleket a pontokból lett élekből kell választani
irányítatlan esetben II. biz.

G k-szorosan *élösszefüggő*, ha bárhogyan $k-1$ élet elhagyva öf. marad.

G k-szorosan (pont)*összefüggő*, ha — " — pontot — " — és legalább $k+1$ pontja van.

k él/pont öf $\Rightarrow$ $k-1$ él/pont öf

Menger V–VI: G k-$\begin{matrix} \text{élöf} \\ \text{pontöf} \end{matrix}$ $\Longleftrightarrow$ bármely 2 pont közt $\exists$ k db páronként $\begin{matrix} \text{éldiszjunkt} \\ \text{pontdiszjunkt} \end{matrix}$ út

Biz: $\Leftarrow$ $k-1$ élet/pontot elhagyva $\exists$ $s \to t$ út tetszőleges s,t-re, mert volt k db él/pontdiszjunkt és $k-1$ él/pont csak $k-1$ utat ronthat el

$\Rightarrow$ ha s,t nem szomszédosak: $\exists$ közöttük k db él, ha nem lenne $\Rightarrow$ k-nál kevesebb éllel is lehetne bontani az utakat $\Rightarrow$ $k-1$ élet törölve nem $\exists$-ne s-t út

ha s,t szomszédosak: st élet töröljük, kell még $k-1$ s-t út, $k-2$-vel lehet bontani

Állítás: k-öf $\Rightarrow$ k-élöf *biz:* Menger V–VI.
$\not\Leftarrow$

Állítás: G 2-öf $\Longleftrightarrow$ bármely 2 ponton át vezet kör *biz:* Menger VI

Dirac-tétel: G k-öf és $k \geq 2$ $\Rightarrow$ bármely k ponton át vezet kör

$G(V,E)$ szomszédossági mátrixa $A(G)$ $n \times n$-es mátrix, ahol $|V|=n$, a_{ij} = i és j élek száma

Tétel: $A^k(G)$-ben a_{ij} = i és j pontok közt vezető k hosszú élsorozatok száma

$A^2(G)$-ben a_{ij} = — " — 2 hosszú utak száma $\Rightarrow a_{ii} = d(i)$

$A^3(G)$-ben $\sum_{i=1}^{n} a_{ii} = 6 \cdot (\triangle\text{-ek száma})$

Ha G k-reguláris $(\Rightarrow \forall d(v)=k) \Rightarrow k$ az $A(G)$ sajátértéke $\Rightarrow$

$\vec{G}(V,E)$ illeszkedési mátrixa $B(\vec{G})$ $n \times e$-es mátrix, ahol $|V|=n$, $|E|=e$, $a_{ij} = \begin{cases} 1, & i \text{ pont a } j \text{ él kezdőpontja} \\ -1, & i \text{ pont a } j \text{ él végpontja} \\ \emptyset, & \text{egyébként} \end{cases}$

$(B(G)$ esetében $a_{ij} \begin{cases} 1 & \text{ha } i \text{ és egyik végpont} \\ \emptyset & \text{ha nem} \end{cases})$

$r(B(\vec{G})) = n - (\text{öf. komponensek száma})$

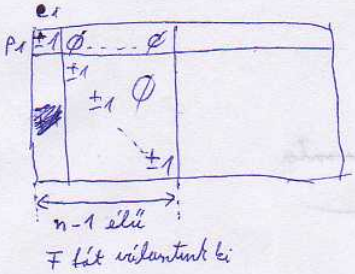
$K_1: n_1, e_1$

$K_2: n_2, e_2$

Tétel: $\vec{G}$ öf $\Rightarrow r(B(\vec{G})) = n-1$

Biz: $r \le n-1 \Rightarrow$ a sorok lineárisan összefüggőek

$r \ge n-1 \Rightarrow \exists (n-1)\times(n-1)$-es rész mx aminek determinánsa nem $\emptyset$



$d(P_1)=1$ $\mp$-ben és e_1 az egyetlen hozzá illeszkedő él

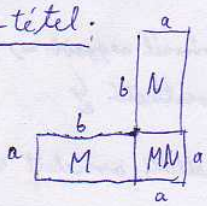
$d(P_2)=1$ $(\mp - P_1)$-ben és e_2 — " — —

$\triangle$ mx $\Rightarrow \det = a_{11} \cdot \ldots \cdot a_{nn} \neq \emptyset$

Tétel: $X \subseteq E(\vec{G})$, $|X|=n-1$ és X fa $\Leftrightarrow$ az X oszlopok lineárisan függetlenek.

Redukált illeszkedési mátrix: $B_0(\vec{G})$, az eredetiből 1 sort elhagyva kapjuk

Binet-Cauchy-tétel:



$\det(MN) = \sum \det M' \cdot \det N'$ $\binom{b}{a}$ tételjpp

M', N'-t az eredetiekből sor/oszlop elhagyással kapjuk, hogy axa-sak legyenek

$$\det\left(\underbrace{B_0(\vec{G}) \cdot B_0^T(\vec{G})}_{c_{ij}}\right) = a^{\text{feszítő fák száma}}$$

$c_{ij} = \begin{cases} -(ij \text{ közt vezető élek száma}) & i \neq j \\ d(i) & i = j \end{cases}$

$a|b$ ha $\exists c \in \mathbb{Z} : a \cdot c = b$

p felbonthatatlan; ha $p = a \cdot b \Rightarrow |a| = 1$ vagy $|b| = 1$

p prímszám, ha $p|a \cdot b \Rightarrow p|a$ vagy $p|b$, $\forall a,b$-re

} $|p| \neq 1$

Tétel: p prím $\Leftrightarrow$ p felbonthatatlan

Biz $\Rightarrow$: p prím, $p = ab \Rightarrow p|a \cdot b \Rightarrow$
- $p|a$ és $a|p \Rightarrow |a| = |p| \Rightarrow b = \pm 1$
- vagy
- $p|b$ és $b|p \Rightarrow |b| = |p| \Rightarrow a = \pm 1$

Számelmélet alaptétele: $\forall n$ $(|n| \geq 2)$ egyértelműen felbontható felbonthatatlanok szorzatára, ha a szorzat tagjainak sorrendjétől és előjelétől eltekintünk.

Biz: ha n
- felbonthatatlan ✓
- ~~nem~~ felbontható $\Rightarrow n = a \cdot b$
  - a, b felbonthatatlan ✓
  - $n = a_1 \cdot a_2 \cdot b$ ...

egyértelműség: $n = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l$

$\Rightarrow p_1 | \prod q_i$ és p_1 prím $\Rightarrow p_1|q_1$ v. $p_1|q_2$ v. ... $p_1|q_l$

pl.: $p_1|q_1 \Rightarrow q_1 = p_1 \cdot c$ és q_1 felbonthatatlan $\Rightarrow |p_1| = \pm 1$ ↯ mert prím

vagy

$p_2 \cdot \ldots \cdot p_k = \pm q_2 \cdot \ldots \cdot q_l \Leftarrow q_1 = \pm p_1 \Leftarrow |c| = \pm 1$ ✓

Prímtényezős felbontás (kanonikus alak): $n = \pm \prod_{i=1}^{k} p_i^{\alpha_i}$

Lnko(a,b): a közös prímtényezők kisebbik hatványukon vett szorzata

Lkkt$[a,b]$: az összes — " — nagyobbik — " —

a és b relatív prímek ha $(a,b) = 1$

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

⊕ osztók összege: $\sigma(n) = \prod_{1}^{k} (1 + p_i + p_i^2 + \ldots + p_i^{\alpha_i}) = \prod_{1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$

Tétel: ∞ sok prímszám van

Indirekt biz: $p_1, \ldots, p_n$ az összes prím, $A = p_1 \cdot \ldots \cdot p_n + 1 \Rightarrow A$ nem prím, mert $\forall$ prímnél nagyobb $\Rightarrow \exists$ prímosztója, DE A $p_1, \ldots, p_n$-nel osztva 1 maradékot ad $\Rightarrow$ egyikkel sem osztható ↯

Tétel: $\forall N$-hez $\exists p, q$ szomszédos prímek: $|p - q| \geq N$, azaz $\exists N$db egymás melletti összetett szám.

Biz:
- $2 | (N+1)! + 2$
- $3 | (N+1)! + 3$
- ⋮
- $(N+1) | (N+1)! + (N+1)$

} Ndb összetett

Vagy prímszámtétel: 1-től n-ig a prímek száma $= \pi(n)$, $\lim_{n \to \infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$, azaz $\pi(n)$ aszimptotikusan $\widetilde{=}$ $\frac{n}{\ln n}$

Dirichlet-tétel: ha $(a,b) = 1 \Rightarrow \infty$ sok $ak + b$ alakú prím van

$a \equiv b \ (m)$ ha a és b m-mel osztva ugyanazt a maradékot adja; $a \equiv b (m) \Leftrightarrow m | a - b$

Tétel:
- $a \equiv b (m)$
- $c \equiv d (m)$

} $\Rightarrow$
- $a \pm c \equiv b \pm d \ (m)$
- $ac \equiv bd \ (m)$
- $a^k \equiv b^k \ (m)$
- $ac \equiv bc \ (m)$

Tétel: $ac \equiv bc (m) \Leftrightarrow a \equiv b \ \left(\frac{m}{(m,c)}\right)$

Lineáris kongruencia: $a \cdot X \equiv b \ (m)$, $x = ?$

Tétel: $ax \equiv b \ (m)$ megoldható $\Leftrightarrow (a, m) \mid b$

Biz: $\Rightarrow$: $d = (a, m)$, x_0 mo. $\Rightarrow$ $d \mid m \mid ax_0 - b$, $d \mid a$, $d \mid ax_0$ $\Rightarrow$ $dc = ax_0 - b = d \cdot a' x_0 - b$

$a' = \frac{a}{d}$ $m' = \frac{m}{d}$

$b = d(a'x_0 - c) \Rightarrow d \mid b$

$\Leftarrow$: Ha $(a, m) = 1$

$0 \leq i, j \leq m-1$, $i \neq j$ $\Rightarrow a i \not\equiv a j \ (m)$, egyébként $i = j$

lehetséges: $a \cdot 0$, $a \cdot 1$, ... , $a(m-1)$

$\exists$ 1 db x amire $ax \equiv b \ (m)$

Ha $(a, m) = d \geq 2$, $b' = \frac{b}{d}$

$ax \equiv b \ (m)$

$a'dx \equiv b'd \ (m'd)$ $\quad (m, d) = d$ ment $d \mid m$

$a'x \equiv b' \ (m')$ $\quad$ első eset miatt $\exists$ mo.

$(a', m') = 1$

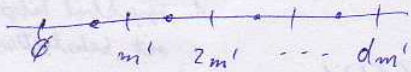
Tétel: $(a, m) \mid b \Rightarrow ax \equiv b \ (m)$ -nek (a, m) db megoldása van (mod m)

Biz: $(a, m) = 1$ -re láttuk, hogy 1 db mo. van

$(a, m) = d \geq 2$ -re

$ax \equiv b \ (m)$

$a'x \equiv b' \ (m')$ $\rightarrow$ 1 db mo. van. (m')



d db intervallum $\Rightarrow$ $d = (a, m)$ db mo. van (m)

Wilson-tétel: p prímszám $\Rightarrow (p-1)! \equiv -1 \ (p)$

Biz: $(p-1)! = \underbrace{a_1 \cdot b_1}_{1} \cdot \underbrace{a_2 \cdot b_2}_{1} \cdot \ldots \cdot \underbrace{1}_{1} \cdot \underbrace{(p-1)}_{-1} \ (\text{mod } p)$

$1 \leq a \leq p-1$, $ax \equiv 1 \ (p)$ megoldható, ment p prím $\Rightarrow (a, p) = 1 \mid 1$

Ha a-nak önmaga a párja $\Rightarrow a^2 \equiv 1 \ (p) \Rightarrow p \mid a^2 - 1 = (a+1)(a-1) \Rightarrow$

- $p \mid a-1 \Rightarrow a \equiv 1 \ (p)$ $a = 1$
- vagy
- $p \mid a+1 \Rightarrow a \equiv -1 \ (p)$ $a = p-1$

Euklideszi algoritmus: input: a, b output: (a,b) $a > b$

a-t osztjuk b-vel maradékosan : $a = h_1 \cdot b + m_1$
majd b-t a maradékkal : $b = h_2 \cdot m_1 + m_2$
így tovább, mindig az osztót a maradékkal: $m_i = h_{i+2} \cdot m_{i+1} + m_{i+2}$

$$m_k = h_{k+2} \cdot m_{k+1} + \emptyset$$
$$m_{k+1} = (a,b)$$

$a \equiv b\,(m)$ megoldása $\Leftrightarrow (a,m) \mid b \Rightarrow d = \frac{b}{(a,m)} \in \mathbb{Z}$

$m \mid b - ax$
$my = b - ax$
$my + ax = b$

Euklideszi alg. a, m-re $\Longrightarrow$ $(a,m) = a\alpha + m\beta \;/\cdot d$

$b = a(\underbrace{\alpha d}_{\text{jó } x \text{ mo.}}) + m(\beta d)$

2 ismeretlenes, lineáris diofantikus egyenlet: $ax + by = c$ $\quad x, y = ? \in \mathbb{Z}$

$by = c - ax$
$b \mid c - ax$
$ax \equiv c\,(b) \Rightarrow$ ebből x, ezt visszahelyettesítve meg van y

pl: $3x + 7y = 13$
$7y = 13 - 3x$
$3x \equiv 13\,(7)$
$3x \equiv 6\,(7)$ $\quad (3,7) = 1$
$x \equiv 2\,(7) \Rightarrow x = 2 - 7t$
$y = 1 + 3t$

Kongruencia-rendszer

pl: $x \equiv 3\,(7)$, $x \equiv -1\,(8)$ $\rightarrow x = 7k + 3 \quad k \in \mathbb{Z}$

$7k + 3 \equiv -1\,(8)$
$7k \equiv -4\,(8)$
$-k \equiv -4\,(8)$
$k \equiv 4\,(8)$
$k = 8l + 4$
$l \in \mathbb{Z}$

$x = 7(8l + 4) + 3 = 56l + 31$
$56l = x - 31$
$x \equiv 31\,(56)$

1. egyikből kifejezem x-t és ezt behelyettesítem a másikba
2. megoldom a másik kongruenciát, a végén kifejezem az ismeretlent és visszahelyettesítem az első kifejezésbe
3. megkapom $x \equiv ?\,(\text{mod } m_1 \cdot m_2)$

Euler-Fermat-tétel: $(a,m)=1 \Rightarrow a^{\varphi(m)} \equiv 1 \ (m)$

$\varphi(m) = 1$ és m közti m-hez relatív prímek száma

p prím $\Rightarrow \varphi(p) = p-1$ mert ~~egy~~ prímhez csak önmaga nem rel. prím.

$\varphi(p^d) = p^d - p^{d-1}$ mert csak akkor nem rel. prímek ha p-vel oszthatók

Tétel: $(a,b)=1 \Rightarrow \varphi(ab) = \varphi(a)\cdot\varphi(b)$

Állítás: $a \equiv b \ (m) \Rightarrow (a,m) = (b,m)$

Biz: $d=(a,m)$ $\left.\begin{matrix} d|a \\ d|m \end{matrix}\right\} \Leftrightarrow d|a+k\cdot m = b$

Redukált Maradék Rendszer mod m (RMR): $\{c_1, \dots, c_{\varphi(m)}\}$ $(c_i,m)=1$ és $c_i \not\equiv c_j (m)$ ha $i \neq j$

Állítás: $\left.\begin{matrix} c_1, \dots, c_k \ RMR(m) \\ (a,m)=1 \end{matrix}\right\} ac_1, \dots, ac_k$ is $RMR(m)$

Biz: db szám ua., $ac_i \equiv ac_j \ (m) \ / : a \ (a,m)=1$

$c_i \equiv c_j \ (m)$

csak ha $i=j$ ✓

E-T biz: $c_1, \dots, c_k$ tetsz. $RMR(m)$, $\varphi(m)=k$

$ac_1, \dots, ac_k$ is — " — mert $(a,m)=1$

$ac_1 \cdot \dots \cdot ac_k \equiv c_1 \cdot \dots \cdot c_k \ (m)$

$a^{\varphi(m)} \cdot c_1 \cdot \dots \cdot c_k \equiv c_1 \cdot \dots \cdot c_k \ (m) \ / : c_1, c_2, \dots, c_k \quad (c_i,m)=1$

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

kis-Fermat-tétel: $\left.\begin{matrix} p \text{ prím} \\ a \text{ tetsz.} \end{matrix}\right\} \Rightarrow a^p \equiv a \ (p)$

Biz: E-F-tétel $(a,p)=1 \Rightarrow p \nmid a \Rightarrow a^{p-1} \equiv 1 \ (p) \ / \cdot a$

$\varphi(p) = p-1$

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

$p|a \Rightarrow a^p \equiv 0 \ (p)$

$a \equiv 0 \ (p)$

polinomiális / exponenciális algoritmus $\Rightarrow$ gyors / lassú $\left(\begin{matrix} \sum^{k} \cdot n \\ x^n \end{matrix}\right.$ akol n a bemenet hossza, a bitlépés pedig a lépésszám. felső becslése $\left.\right)$

szám hossza 2-es szám rsz.-ben $\log_2 n$, 16-osban $\log_{16} n$

$\mathbb{Z}$	lépésszám felső becslés	típus
$+$	$2(\log a + \log b)$	lineáris (azaz polinomiális
$-$	— " —	— " —
$\cdot$	$(\log a + \log b)^2$	polinomiális
$/$	— " —	— " —
a^b	$\log a \cdot 2^{\log b}$	exponenciális

$a \# b \equiv ? (m)$	
$+$	polinomiális
$-$	
$\cdot$	
$/$	
a^b	

A hatványozásra a kongruencia periódikus

Pl: $3^{100} \equiv ? (7)$ $\quad 3^{100} = 3^{64} \cdot 3^{32} \cdot 3^4 \equiv 4 \cdot 2 \cdot 4 \equiv 4 (7)$

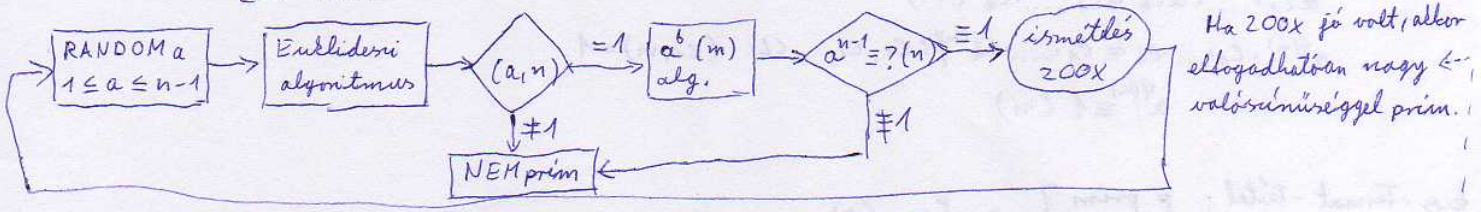
$3^2 \equiv 2 (7)$
$3^4 \equiv 4 (7)$
$3^8 \equiv 2 (7)$
$3^{16} \equiv 4 (7)$
$3^{32} \equiv 2 (7)$
$3^{64} \equiv 4 (7)$

Euklideszi algoritmus lépésszáma $\leq 2 \log a$ (a a bemenetek közül a nagyobbik)

Prímtesztelés (Fermat-teszt)

Ha n prím $(a,n) = 1 \Rightarrow a^{n-1} \equiv 1 (n)$ $\forall a$-ra! ha $1 \leq a \leq n-1$

E-F-tétel



Ha 200x jó volt, akkor elfogadhatóan nagy valószínűséggel prím.

a tanúja n-nek ha $a^{n-1} \not\equiv 1 (n)$ } $(a,n) = 1$
a cinkosa n-nek ha $a^{n-1} \equiv 1 (n)$ }

Tétel: Ha n-nek $\exists$ tanúja $\Rightarrow$ RMR (n) legalább fele tanú

Biz: a tanú $c_1, \dots, c_k$ cinkosok, $a \cdot c_i$ is tanú, de $a c_i \not\equiv a c_j (n)$ ha $i \neq j \Rightarrow$ tanúk száma $\geq$ cinkosok száma

Köv: Ha $\exists$ tanú $\Rightarrow$ a Fermat-tesz legfeljebb $\left(\frac{1}{2}\right)^{200}$ valószínűséggel téved

Carmichael-szám (álprím): összetett, de nincs tanúja RMR(n)-ben, azaz $\forall a$-ra $(a,n) = 1 \Rightarrow a^{n-1} \equiv 1 (n)$

pl.: 561

Titkosítás

Prím-generálás: RANDOM 200 jegyű szám $\rightarrow$ prím tesztelés $\Rightarrow$ néhány 100 próbálkozás után jó lesz

A prímtényezős felbontásra nem ismert hatékony algoritmus!

karakterek, adatok $\rightarrow 1, \dots, N$ közti számok, kódolás: $X \xrightarrow{C} C(x)$, dekódolás: $D(C(X)) = X$

RSA: $N = p \cdot q$: p | q 150-200 jegyű prímek, C : $(c, \varphi(N)) = 1$

nyilvános: N, c
titkos: p, q, d

kódolás: $X \longrightarrow X^c (N)$

dekódolás: $(X^c)^d \equiv X (N)$ $\forall X$-re ; $c \cdot d \equiv 1 (\varphi(N))$ megoldható d-re ; p és q ismerete nélkül $\varphi(N)$ nem írható fel

$\Downarrow$ $\Uparrow$

más nem tud dekódolni

kicsi az esély $X = p$ vagy $X = q$ -ra $\Rightarrow (X,N) = 1 \Rightarrow X^{k \cdot \varphi(N)+1} \equiv X (N)$

Digitális aláírás: $A \longrightarrow B$ $\quad A: X \rightarrow D_A(C_B(X)) = y$ $\quad B: y \rightarrow D_B(C_A(y)) = X$

C_A (D_A) $\quad C_B$ (D_B) $\quad$ A titkosította B tudja olvasni

Művelet: $\perp : H^2 \to H$ fv., ahol $H^2 \neq H$ elemeiből készíthető rendezett párok halmaza

kommutatív: $ab = ba$ $\quad \forall a,b,c \in H$-ra

asszociatív: $(ab)c = a(bc)$

Félcsoport: $(S, *)$ ha $*$ művelet asszociatív S halmazon

$e \in H$ egységelem, ha $\forall a \in H$-ra $e * a = a * e = a$; ~~csak kétoldalit~~, mert ha e, f egység $\Rightarrow f = e \cdot f = e$

$a^{-1} \in H$ inverze a-nak, ha $a * a^{-1} = a^{-1} * a = e$; egyértelmű, ha $\exists$, mert ha b, c inverz $\Rightarrow c = \underbrace{(b*a)}_{e} * c = b * \underbrace{(a*c)}_{e} = b$

Csoport: $(G, *)$, ha $*$ asszociatív művelet G halmazon és $\exists$ egységelem és $\exists \forall$ elemnek inverze.

Abel-csoport: $(G, *)$, ha csoport és $*$ kommutatív G-n

Szimmetria-csoport: $(H, \circ)$: H = egy rajzot önmagába vivő műveletek (Identitás, forgatások, tükrözések)

$\circ$ = kompozíció = ~~műveletek~~ függvények egymás után alkalmazása : $(f \circ g) \circ h = f \circ (g \circ h)$

csoport, mert $\circ$ asszociatív, egységelem: I, inverz: ugyanaz a művelet visszafele $(t_i^{-1} = t_i)$

Diéder-csoport: D_n = n oldalú szabályos sokszög szimmetria-csoportja $\quad |D_n| = 2n$

Szimmetrikus csoport: elemei: $\{1, \dots, n\}$ permutációi, művelet: kompozíció (DE balról jobbra haladunk)

$|S_n| = n!$

csoport, mert a művelet asszociatív (DE nem kommutatív)

egységelem: $\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$

inverz: ugyanaz visszafelé

Példák

Abel-csoport: $(\mathbb{Z}, +)$: kommutatív, asszociatív, egység: $\emptyset$, inverz: $-X$

$(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{\emptyset\}, \cdot)$, $(\mathbb{R}^{n \times k}, +)$, $(\{1, -1, i, -i\}, \cdot)$

Diéder-csoport: $\triangle \Rightarrow H = \{I, t_{120}, t_{240}, t_1, t_2, t_3\}$

~~Szimmetrikus csoport~~

Szimmetrikus-csoport: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$

Csoport rendje $|G|$ = az elemszámával

$g^n = \underbrace{g * \dots * g}_{n}$, $g^1 = g$

Tétel: G véges $\Rightarrow \exists n \geq 1 : g^n = e$

Biz: $g^1, \dots, g^k, \dots, g^l, \dots$ közt ismétlődésnek kell lennie a végesség miatt

$\Rightarrow \exists\ 1 \leq k < l : g^l = g^k \mid \cdot g^{-1}$

$g^{l-1} = g^{k-1} \mid \cdot g^{-1}$

$\vdots$

$g^{l-k} = e \Rightarrow n = l - k$

Elem rendje: $o(g) =$ a legkisebb olyan k amire $g^k = e$ $(k \geq 1)$

G **ciklikus csoport**, ha $\exists g \in G$ **generátor elem**, hogy G $\forall$ eleme kifejezhető g-ből a művelettel és az inverzképzéssel

pl.: $(\mathbb{Z}, +)$

Tétel: Ha G véges és ciklikus $\Leftrightarrow \exists g \in G : o(g) = |G|$

Biz: $\Leftarrow$ $G = \{g$ hatványai$\}$, g hatványainak száma $o(g)$

$\Rightarrow$ — " — , $o(g) = k \Rightarrow g^k = e$

Tétel: G ciklikus $\Rightarrow$ G Abel $\quad$ **Biz:** $g^{i+j} = g^{i+j} \Rightarrow g^i g^j = g^j \cdot g^i$

$\not\Leftarrow$

Tétel: $|G| =$ prím $\Rightarrow G$ ciklikus **Biz:** $o(g) \mid p$ (Lagrange-tétel) $\rightarrow o(g) = 1 \Rightarrow g = e$; $\rightarrow o(g) = p = |G|$

$(G, *)$ **izomorf** $(H, \circ)$ **-rel**, ha $\exists f : G \to H$ kölcsönösen egyértelmű fv.: $f(a * b) = f(a) \circ f(b)$

$G \cong H$

a ciklikus csoportok, ha elemszámuk egyenlő $\Rightarrow$ izomorfak

$H \leq G$ **részcsoportja** G-nek, ha H is csoport G műveletével

$H \leq G$

Tétel: $\emptyset \neq H \subseteq G$, $(G, \circ)$, H részcsoport $\Leftrightarrow$ zárt a műveletre és inverz képzésre $(a, b \in H \Rightarrow ab \in H, a^{-1} \in H)$

Biz: $\Rightarrow$ def.

$\Leftarrow$ asszociativitás nem romlik el kevesebb elem miatt

egységelem eleme H-nak, mert g, g^{-1} és $g \cdot g^{-1}$ eleme

a $\cdot$ művelet, inverz léte az alapállítás.

Cayley-tétel Ha G véges csoport $\Rightarrow \exists n : S_n$ szimmetrikus csoport valamely H részcsoportjára $G \cong H$

$g \cdot H$ a $H \leq G$ g elem szerinti baloldali **mellékosztálya** : $gH = \{g \cdot h : h \in H\}$ Pl: $G = D_3$

$H \cdot g$ jobboldali $Hg = \{h \cdot g : h \in H\}$ $H = \{I, t_{120}, t_{240}\}$

$t_1 H = t_2 H = \{t_1, t_2, t_3\}$

$t_{120} H = H$

Mellékosztály tulajdonságai

1, $g \in gH$ biz: $e \in H \Rightarrow \underbrace{g \cdot e}_{g} \in gH$

2, Ha $g_1 H \cap g_2 H \neq \emptyset \Rightarrow g_1 H = g_2 H$ biz: $a \in g_1 H \cap g_2 H \Rightarrow a = g_1 h_1 = g_2 h_2 \mid \cdot h_1^{-1} \in$

$\Downarrow \; g_1 = g_2 h_2 h_1^{-1}$

$b \in g_1 H \Rightarrow b = g_1 h_4 = g_2 \underbrace{h_2 h_1^{-1} h_4}_{h_3 \in H \text{ mert } H \text{ részcsop}} \Rightarrow b \in g_2 H$-nak is

3, $|H| = |gH|$ (ha H véges) biz: H elemszáma a véges. szorzástól nem változik és 2 gH-beli elem csak akkor $=$ ha már H-ban is azok voltak

Lagrange-tétel: $H \leq G$ véges $\Rightarrow |H| \mid |G|$

Biz:

$\Rightarrow n$ db különböző mellékosztály $\Rightarrow |G| = |H| \cdot n \Rightarrow |H| \mid |G|$

Köv: $o(g) \mid |G|$

Biz: $\exists H \leq G : |H| = o(g) = k$

↳ zárt a műveletre: $g^i, g^j \in H$, $g^i \cdot g^j = g^{i+j}$

ha $i+j \leq k \Rightarrow g^{i+j} \in H$

ha $i+j > k \Rightarrow g^{i+j} = g^{i+j-k} \cdot \underbrace{g^k}_{e} = g^{i+j-k} \leq k$

↳ zárt az inverzre: $e = g^k \in H \Rightarrow g^k = g^i \cdot g^{k-i} = e \Rightarrow g^{k-i} = (g^i)^{-1} \in H$

$\emptyset = R$ halmazon műveletek: $+, \cdot$

1, $a+b = b+a$ kommutativitás
2, $(a+b)+c = a+(b+c)$ asszociativitás
3, $\exists \emptyset \in R : a+\emptyset = a$ egységelem
4, $\exists -a \in R : a+(-a) = \emptyset$ inverz.

disztributivitás

5, $a(b+c) = ab+ac$
$(b+c)a = ba+ca$

① $ab = ba$
② $(ab)c = a(bc)$
③ $\exists 1 \in R : a \cdot 1 = 1a = a$
④ $\forall \emptyset \neq a \in R \ \exists a^{-1}: aa^{-1} = a^{-1}a = 1$

$(R, +, \cdot)$
gyűrű
kommutatív gyűrű
ferde test
test

Tétel: $\forall$ gyűrűben $\forall a$-ra $a \cdot \emptyset = \emptyset$ **Biz:** $a(\emptyset+\emptyset) = a\cdot\emptyset$
$a\cdot\emptyset + a\emptyset = a\emptyset \ / + (-a\emptyset)$
$a\emptyset = \emptyset$

R nullosztómentes gyűrű, ha $\forall a,b \in R$-re ha $ab = \emptyset \Rightarrow a = \emptyset$ vagy $b = \emptyset$ pl.: $\mathbb{Z}, \mathbb{Z}[x]$

Tétel: $\forall$ test nullosztómentes **Biz:** $ab = \emptyset$ és $a \neq \emptyset \Rightarrow \underbrace{a^{-1}a}_{1} b = \underbrace{a^{-1}\emptyset}_{\emptyset} \Rightarrow b = \emptyset$

Testek: $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Q}(\sqrt{2})$
Gyűrűk: $\mathbb{Z}$ (kommutatív egységelemes), $\mathbb{R}^{n\times n}$ (egységelemes), $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$
↳ egész együtthatós polinómok $\{a_0 + a_1x + a_2x^2 + \dots + a_nx^n : a_i \in \mathbb{Z}\}$

$\Rightarrow \mathbb{Z}_n = \{\emptyset, 1, \dots, n-1\}$ $a \oplus b = a+b \pmod n$, $a \odot b = a\cdot b \pmod n$

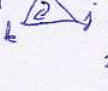
Ferdetest: $\mathbb{K}$

Tétel: $\mathbb{Z}_n$ gyűrű $\forall n \geq 1$-re **Biz:** $(-a) = n-a$, $(-\emptyset) = \emptyset$, $\underbrace{(a \odot b)}_{x} \odot c = y$ $ab \equiv x \ (n)$, $abc \equiv xc \ (n) \equiv y$, ...

Tétel: n prím $\Leftrightarrow$ $\mathbb{Z}_n$ test **Biz:** $\Leftarrow$ ha n nem lenne prím $\Rightarrow n = ab$, $a \odot b = \emptyset \Rightarrow$ nem nullosztómentes $\Rightarrow$ nem test

$\Rightarrow$ tudjuk: n prím, $\mathbb{Z}_n$ gyűrű, kommutatív, és $\exists 1 \in \mathbb{Z}_n$
kell még: ④ $a = \emptyset$ $a \odot a^{-1} = 1$
$a \cdot a^{-1} \equiv 1 \ (p) \Rightarrow \exists$ mo. a^{-1}-re $\Leftrightarrow \underbrace{(a,p)}_{\text{1 mert } p \text{ prím és } a \leq p-1} \mid 1$

Kvaterniók: $\mathbb{K} = \{a+bi+cj+dk : a,b,c,d \in \mathbb{R}\}$, $i^2 = j^2 = k^2 = -1$



$ij = k$; $ji = -k$
$ki = j$; $ik = -j$
$jk = i$; $kj = -i$

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$
rac. irrac + rac = valós