Def.: Egy G gráfban **Hamilton-körnek** nevezünk egy H kört, ha G minden pontját pontosan egyszer tartalmazza. Egy utat pedig **Hamilton-útnak** nevezünk, ha G minden pontját pontosan egyszer tartalmazza.

Tétel: (1). Ha G-ben $\exists$ Hamilton-kör és $X \subseteq V(G)$ tetsz. $\Rightarrow$
~~$\Rightarrow G-X$ összefüggő komponens~~
$\Rightarrow G-X$ összefüggő komponenseinek száma $\leq |X|$

(2). Ha G-ben $\exists$ Hamilton-út és $X \subseteq V(G)$ tetsz. $\Rightarrow$
$\Rightarrow G-X$ öf. komp. száma $\leq |X|+1$

Biz.: (1)

(2) hasonlóan

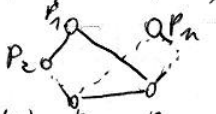
Tétel: **Ore:** Ha G egy n-pontú egyszerű gráf és $\forall x,y \in V(G)$-re, ha $d(x)+d(y) < n$, akkor $\{x,y\} \in E(G) \Rightarrow \exists G$-ben H-kör.

Biz.: Indirekt: Ha G egy ellenpélda és tesszünk egy élt:

(1) ellenpélda marad:

(2) lesz benne H-kör, mivel az Ore-feltételt nem lehet él berajzolásával elrontani: $(\{x,y\} \notin E(G) \Rightarrow d(x)+d(y) \geq n$; $\forall x,y \in V(G)$-re)

$\Rightarrow$ Egy olyat kell egy G_0 nagy ellenpéldához.



Ha $\{P_1 ; P_{i+1}\} \in E(G_0) \Rightarrow P_i, P_n \notin E(G_0)$ (Lesz benne H-kör)

Ekkor $d(P_n) \leq n-1$

$d(P_n) \leq n-1-d(P_1)$

$d(P_1)+d(P_n) < n \Rightarrow \{P_1 ; P_n\} \in E$ ↯

Tétel: **Dirac:** Ha G egy n-pontú egyszerű gráf és $\forall x \in V(G)$-re $d(x) \geq \frac{n}{2} \Rightarrow$

$\Rightarrow \exists G$-ben H-kör.

Biz.: Ore-tételből.

Tétel: **Hall:** ∃ egy páros gráfban ∀F-beli pontot lefedő párosítás ⇔
⇔ ∀ X ⊆ F-re $|N(X)| \geq |X|$

Biz.: ⇒ triv.

⇐

Def.: Egy bookult M párosításra vonatkozóan u egy alternáló út, ha ∀ második élem $\notin M$.

Def.: Egy M párosításra vonatkozóan u egy javító út, ha alternáló és az első és utolsó éle $\notin M$.

Áll.: ∃ javító út M-re vonatkozóan ⇔ M nem volt maximum

Biz.: ⇒: $M' \leftarrow (M - \{u_2, u_4 \dots\}) \cup \{u_1, u_3, \dots\}$ így nagyobb

Indirekt. Tfh.: ∃ párosítás, nem javítható tovább, de F-ben vannak lefedetlen pontok

~~F1: nincs lefedve~~ *F-beli állva*

Áll.: $N(F_1 \cup F_2) = L_2$

Biz.: F_1: L_1-ből nincs ismerős

F_2: L_1-ből nem elérhető

L_2-gal nem lehet összekötve

$X = F_1 \cup F_2$ választással $|N(X)| < |X|$ ↯

Tétel: **Frobenius:** G páros gráfban ∃ teljes párosítás ⇔ (1) $|F| = |L|$

(2) ∀ X ⊆ F-re $|N(X)| \geq |X|$

Magyar módszer: Algoritmus

- független élek felvétele, amíg lehet
- javítás javító úttal
- nincs több javító út → STOP

Tétel: A magyar módszer max párosítást talál

Biz.: alp: M párosítás, $|M| = k$

cél: k pontú lefogó ponthalmaz ⇒ $|M| \leq k$ } kész

Áll.: *F-beli állva* $(F_1 \cup F_2)$ és $(L_1 \cup L_2)$ közötti nincs él.

Biz.: F_1-L_1: összekötésük

F_1-L_2: ✓

F_2-L_1: javító út

F_2-L_2: ✓

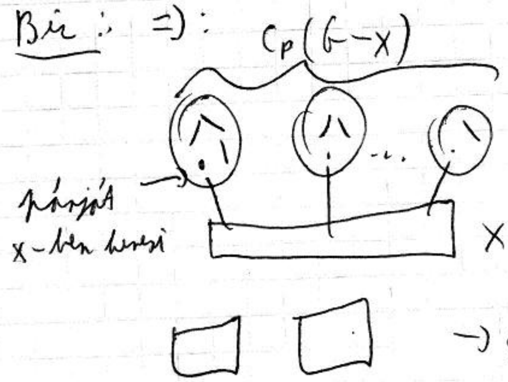
(1)

$X = L_2 \cup F_2$ lef. ponthalmaz, $|X| = k$

Def/Jelölés: $c_p(H)$: ptlan pontszámú összefüggő komponensek száma.

Tétel: Tutte: Egy G gráfban $\exists$ teljes párosítás $\Leftrightarrow \forall X \subseteq V(G)$-re $c_p(G-X) \le |X|$

Biz.: $\Rightarrow$):



$\rightarrow$ ptl. komp.

$\Rightarrow |X| \ge c_p(G-X)$

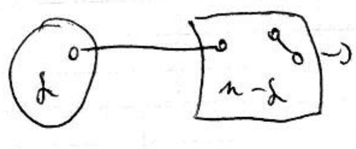
$\rightarrow$ ps. komponensek.

nem futhat: O–O
□–□
O–□

Tétel: Gallai: (1) $\alpha(G)+\tau(G)=n$ (nincs hurokél)

(2) $\nu(G)+\rho(G)=n$ (nincs izo. pont)

Biz.: (1) α pontot kiválasztok:

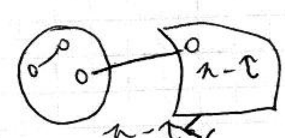


$n-\alpha$: lefogó ponthalmaz

$n-\alpha \ge \tau$

$\alpha+\tau \le n$

τ pontot



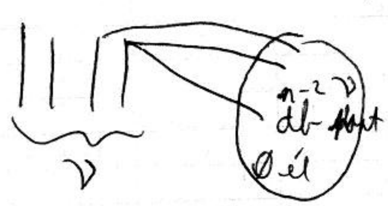
$n-\tau \le \alpha$

$\alpha+\tau \ge n$

$\alpha+\tau=n$

(2) ($\nu+\rho=n$)

i) $\nu+(n-2\nu) = n-\nu \ge \rho$

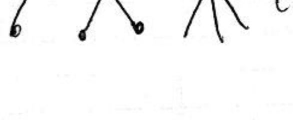


ii) H: részgráfja G-nek, lefog minden pontot,

$|E(H)| = \rho(G)$

$\rightarrow$ H körmentes (= erdő)

$\rightarrow$ nincs benne ≥ 3 hosszú út

H:  (csillag) $e(H)=n-k=\rho$

$k=n-\rho \le \nu$

i + ii $\Rightarrow \rho+\nu=n$

Def.: Legyen G egy irányítatlan gráf. Rendeljünk minden éléhez egy $c(e)$ nemnegatív valós számot, amit az él **kapacitásának** nevezünk. Jelöljünk ki továbbá két s,t pontot G-ben, melyeket **termelőnek** ill. **fogyasztónak** hívunk. Ekkor a (G,s,t,c) négyest **hálózatnak** hívjuk.
Hálózat: $(\vec{G},s,t,c)$; $s,t \in V(G)$; $c: E(G) \to \mathbb{R}^+$

Def.: Legyen $f(e)$ az a mennyiség, ami az e élen folyik át. Ez az f fv. **megengedett fv.**, ha $f(e) \le c(e)$ minden élre és $m(v) = \sum\{f(e) \mid e$ végpontja $v\} - \sum\{f(e) \mid e$ kezdőpontja $v\} = 0$ minden $v \in V(G)$-re, kivéve s és t pontokat. Egy megengedett fv-t **folyamnak** hívjuk. $m(t) = -m(s)$. Ezt a közös értéket a **folyam értékének** nevezzük és m_f-el jelöljük. Egy él **telített** hívjuk, ha $f(e) = c(e)$; **telítetlen**, ha $f(e) < c(e)$.
Folyam: olyan $f: E(G) \to \mathbb{R}^+$, melyre (1) $\forall e$-re $f(e) \le c(e)$

(2) $\sum_{e=(\vec{x},\cdot)} f(e) - \sum_{e=(\cdot,\vec{x})} f(e) = \begin{cases} 0, \text{ha } x \in V(G)-\{s,t\} \\ m(f), \text{ha } x = s \\ -m(f), \text{ha } x = t \end{cases}$

Def.: (G,s,t,c) és $f \to M_f$ **segédgráf**: $V(M_f) = V(G)$ és $(\vec{x,y}) \in E(M_f)$ ha vagy $(\vec{x,y}) \in E(G)$ és $f(x,y) < c(x,y)$; (① **első típusú él**)
vagy $(\vec{y,x}) \in E(G)$ és $f(x,y) > 0$. (② **második típusú él**)

Tétel: $\exists$ irányított út s-ből t-be a M_f-ben $\Leftrightarrow$ f nem valt max.

Biz.: $\Rightarrow$ legyen egy irányított út:

$$\delta_1 = \min_{e \in U \text{ és } ①} [c(e) - f(e)] > 0$$
$$\delta_2 = \min_{e \in U \text{ és } ②} [f(e)] > 0$$
$$\delta = \min[\delta_1, \delta_2] > 0$$

$$f(e) \leftarrow \begin{cases} f(e)+\delta & \text{ha } e \in U \text{ és } ① \\ f(e)-\delta & \text{ha } e \in U \text{ és } ② \\ f(e) & \text{különben} \end{cases}$$

$\Rightarrow m(f_{új}) = m_f + \delta$ ✓

Def.: $X \cap Y = \emptyset$; $X \cup Y = V(G)$; $s \in X$, $t \in Y$ $\to$ **s-t vágat**

$\forall f$-re és $\forall Q$-ra:

$$\sum_{\substack{e=(x,y) \\ x \in X \\ y \in Y}} f(e) - \sum_{\substack{e=(x,y) \\ x \in Y \\ y \in X}} f(e) = m(f) \le \sum c(e) - \sum 0 = \underbrace{c(Q)}_{\text{vágat kapacitása}}$$

Tétel: Ford-Fulkerson: $\max_{\forall f} m(f) = \min_{\forall Q} c(Q)$

Biz.: Indirekt: f_0 nem max, de $\nexists$ irányított út H_{f_0}-ban s-ből t-be.

Segédgráf: 

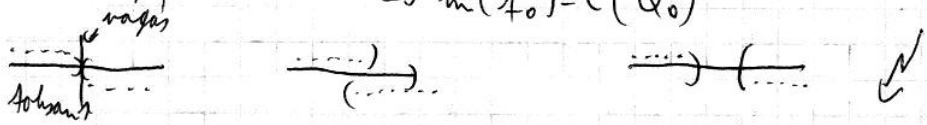
Legyen X a H_{f_0}-ban s-ből elérhető pontok halmaza

$Y = V(G) - X$

Q_0: telített

$f = 0$

$\hookrightarrow m(f_0) = c(Q_0)$

Vagy: 

Tétel: Edmonds-Karp: Ha a javítási eljárás során $\forall$ lépésben egy min. élszámú $s \to t$ irányított út mentén javítunk, akkor az össz. lépésszám $\leq c \cdot n^5$

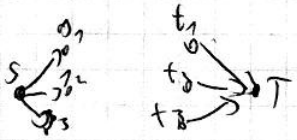
Tétel: Egészértékűségi lemma: (G, s, t, c) és $\forall e$ élre $c(e)$ egész szám:

(1) max: $m(f)$ is egész

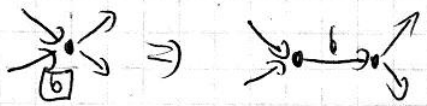
(2) Ez a max. olyan folyammal is elérhető, melyben $\forall$ élen $f(e)$ egész

A folyamprobléma általánosítása:

- Több termelő / több fogyasztó: szupertermelő / szuperfogyasztó.



- Pontkapacitás ($E(v)$ is):

$\forall v$-re $-\sum k_i = 0$ és $\sum f(u,v) \leq E(v)$ 

- Több termék szállítása egyidejűleg $\Rightarrow$ nem visszavezethető

Tételek: Menger:

① $\vec{G}$-ben s-ből t-be vezető éldiszjunkt irányított utak max száma = az s-ből t-be vezető összes irányított utat lefogó élek min. száma $\exists = k$.

Biz.: $\leq$: triv. ✓ egyenlőség: $(\vec{G}, s, t) \to (\vec{G}, s, t, c)$ $\forall$ élre $c(e) = 1 \Rightarrow$

$\to \max\limits_{\forall f} m(f) \underset{(F-F)}{=} \min\limits_{\forall Q} c(Q) = k$ ~~$\Rightarrow$~~ egészértékűségi lemma

$\to \exists f$ folyam, melynek értéke k és $\forall$ élen $f(e) \in \{0,1\}$. Ekkor $\exists k$ élidegen irányított s-t út, hiszen egy ilyen út mindenképp van; Az út éleinek kapacitását változtassuk 0-ra. Így a folyam értéke $\geq k-1$...

② $(s,t) \notin E(\vec{G})$; $\vec{G}$-ben s-ből t-be vezető pontdiszjunkt irányított utak max száma = az s-ből t-be vezető összes irányított utat lefogó pontok min száma $\exists k$

Biz.: $\leq$ triv ✓ =: megduplázási trükk:

k db $\vec{G}$ → pontdiszjunkt $\exists k$ db pontdiszjunkt ir. út

$\downarrow$ $\uparrow$

k db $\vec{G}$ → éldiszjunkt $\to \exists k$ db éldiszjunkt ir. út

③ G-ben s és t között haladó éldiszjunkt utak max száma = az s és t között vezető összes utat lefogó élek min. száma $\exists k$

Biz.: $\leq$ triv ✓; =: G o—o $\exists k$ db út

$\downarrow$ $\uparrow$

$\vec{G}$ → $\exists k$ db ir. út

Probléma: duplán használt élek kiküszöbölése helyettesítéssel

④ $\{s,t\} \notin E(G)$; G-ben s és t között haladó pontdiszjunkt utak max száma = az s és t között vezető összes utat lefogó pontok min száma.

Biz.: Előző tételre...

Def: $G(V,E)$ gráf k-szorosan él-öf, ha $\forall X \subseteq E, |X| < k \Rightarrow G - X$ még öf

⑤ G-ben $\exists k$ db éldiszjunkt út bármely 2 pont között $\Leftrightarrow$ G k-él-öf

~~⇐~~ Biz.: ③-ból

⑥ G-ben $\exists k$ db <u>pontdisjunkt út</u> bármely 2 pont között $\Leftrightarrow$ G k-pontöf.

<u>Def.:</u> $G(V,E), |M| > k$ gráf <u>k-szorosan pont-öf.</u>, ha $\forall X \subseteq V, |X| < k \Rightarrow G-X$ még öf.

<u>Bic.:</u> ...

<u>Dirac-tétel</u>: Ha $k \geq 2$ és G k-szorosan pont öf. $\Rightarrow$ tetsz. $x_1, \dots x_k \in V(G)$-hez $\exists K$ hív, hog $x_1, \dots x_k \in V(K)$

Def.: $T_k(n)$ az n csúcsú k osztályú **Turán-gráf** az alábbi:

- $\forall$ osztály mérete $\left\lfloor \frac{n}{k} \right\rfloor$ vagy $\left\lceil \frac{n}{k} \right\rceil$
- él pontosan akkor fut két csúcs között, ha azok különböző osztályban vannak.

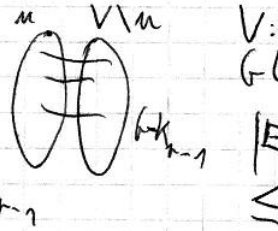
Áll.: hány éle lehet egy n csúcsú (egyszerű) gráfnak, ha nem tartalmaz K_r részgráfot?

Tétel: Turán: ha G olyan n csúcsú egyszerű gráf, ami nem tartalmaz $K_r - t$, akkor $|E(G)| \leq |E(T_{r-1}(n))|$. továbbá: = csak akkor, ha $G \cong T_{r-1}(n)$.

Biz.: teljes indukció n-re.

$n = 1, 2, \dots (r-1)$-re nyilvánvaló. Tekintsük a G K_r-mentes n csúcsú gráfot, és tfh. $(k-1)$-ig már igazoltuk az állítást. Feltehetjük azt is, hogy $n \geq r$.

Tfh. G tartalmaz: nyilván élhez hozzávéve hozzávéve $K_r \Rightarrow K_{r-1} \subseteq G$



$V := V(G)$

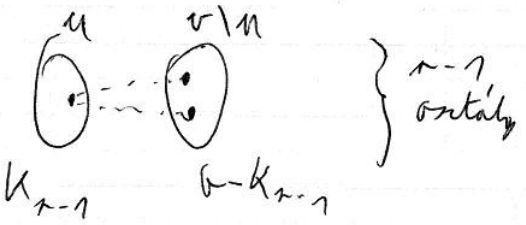
$G[u] \cong K_{r-1}$ (u-t tartalmazó részgráf) $u, r \setminus u$ közötti futó élek száma

$$|E(G)| = |E(G[u])| + |E(G[r \setminus u])| + |E(G[u, r \setminus u])| \leq$$

$$\leq \binom{r-1}{2} + |E(T_{r-1}(n-r+1))| + (n-r+1)(r-2) = |E(T_{r-1}(n))| \quad \forall$$

↑ ind. feltevésből ↑ K_r mentességből

Egyenlőség esete: 3 betűs tag mindegyikénél egyenlőségnek kell állnia. Ha egyenlőség áll, akkor tehát: $G[r \setminus u] \cong T_r(n-r+1)$ ind. feltevés szerint, továbbá $r \setminus u$ minden pontjából pontosan $r-2$ él kell jusson u-ba. Ez K_r keletkezése nélkül csak úgy lehet, ha u $\forall$ pontja pontosan egy-egy (és másik) $T_r(n-r+1)$-beli osztály csúcsaival van összekötve



Ez nem lehet

Def.: $n \in \mathbb{N}$ **felbonthatatlan**, ha $a > 1$ és n nem bontható fel két nála kisebb egész szám szorzatára.

Def.: $n \in \mathbb{N}$ **prímtulajdonságú**, ha $n \mid ab \Rightarrow n \mid a$ vagy $n \mid b$

Oszthatóság: $k \mid m$ jelentése: m osztható k-val, tehát $\exists l \in \mathbb{N} : m = k \cdot l$

Kapcsolat: Ált. struktúrákban a kettő nem egyenlő sosem, de a poz. egészek körében igen $\Rightarrow$ **prímek**

Állítás: Ha p prím $\Rightarrow p$ felbonthatatlan.

Biz.: Ha $n = ab$ akkor $p \mid ab$, és mivel p prím, ezért $p \mid a$ vagy $p \mid b$. Tudjuk, hogy $p \geq a$ és $p \geq b$. Ha $a \leq p \mid a$, akkor $a = p$, egyébként $b \leq p \mid b$, így $b = p$. Tehát p felbonthatatlan.

Tétel: Számelmélet alaptétele: $\forall n \in \mathbb{N}$ a tényezők sorrendjétől eltekintve egyértelműen felbontható prímszámok szorzatára.

Biz.: Ha n prím, akkor $n = p$, ez egyértelmű. Ha nem prím, akkor szorzattá bontjuk, amíg lehet, végül $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ alakú felbontást kapunk ($\alpha_i > 0$). Ha létezne 2 különböző felbontás: $n = p_1^{\alpha_1} \dots p_m^{\alpha_m} = q_1^{\beta_1} \dots q_m^{\beta_m}$ különböző: $\exists i : p_i \neq q_j$ semelyen j-re, vagy legalábbis más hatványon szerepel, akkor a kisebbel leosztom, a fenti áll elő. Prímtul. miatt: előbbi p_i osztója vmely q_j-nek, noha q_j felbonthatatlan $\lightning$.

Áll.: $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ felbontású szám **osztóinak a száma**: $(\alpha_1+1) \dots (\alpha_m+1)$

Biz.: n osztói a $p_1^{\beta_1} \dots p_m^{\beta_m}$ alakú számok, ahol $\forall i$-re $0 \leq \beta_i \leq \alpha_i$.

Ilyen ennyi: $\prod_{i=1}^{m} (\alpha_i + 1)$ féle van

Áll.: Előbbi n **osztóinak az összege**: $\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \dots \cdot \frac{p_m^{\alpha_m+1} - 1}{p_m - 1}$

Biz.: Az osztók összege így írható:

$(1 + p_1 + p_1^2 + \dots p_1^{\alpha_1})(1 + p_2 + \dots p_2^{\alpha_2}) \dots (1 + p_m + \dots + p_m^{\alpha_m})$

Tétel: prímek száma végtelen.

Biz.: Indirekt. Tfh.: véges sok van: $p_1, \dots p_k$. Ekkor az $n = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$ szám nem osztható egyik p_i-vel sem $\Rightarrow$ vagy ő prím, vagy van a felsoroltaktól különböző osztója is.

Áll.: $\forall k \in \mathbb{N}$-re $\exists$ k egymásutáni szám, melyek közül $\geq k$ összetett szám van.

Biz.: $(k+1)! + i$ osztható i-vel $\forall 2 \leq i \leq (k+1)$-re, vagyis ez k db egymást követő összetett szám.

Tétel: Nagy prímszámtétel: Legyen $\pi(n)$ az n-nél kisebb prímek száma.

Ekkor $\lim\limits_{n \to \infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$

Tétel: Dirichlet: Ha a és b relatív prímek, akkor végtelen sok $a \cdot k + b$ alakú prím van.

KONGRUENCIÁK:

Def.: $a \equiv b \pmod m$: kongruens, ha a és b m-mel osztva ugyanazt a maradékot adják $\overset{D_1}{\Leftrightarrow} \overset{D_2}{\Leftrightarrow} a \equiv b \,(m) \Leftrightarrow m \mid a-b$

$D_1 \Rightarrow D_2$: $a = r_1 \cdot m + k$, $b = r_2 \cdot m + k$, $0 \leq k \leq m-1 \Rightarrow a - b = (r_1 - r_2)\, m + 0 \Rightarrow m \mid a-b$

Tétel: $\left.\begin{matrix} a \equiv b\,(m) \\ c \equiv d\,(m) \end{matrix}\right\} \Rightarrow$ (1) $a \pm c \equiv b \pm d\,(m)$

(2) $a\,c \equiv b\,d\,(m)$

(3) $a^k \equiv b^k\,(m)$ $(k \geq 1$ egész$)$

Biz.: (2) $\left.\begin{matrix} m \mid a-b \\ m \mid c-d \end{matrix}\right\} \overset{c}{\Rightarrow} m \mid ac - bc \left.\right\} \overset{+}{\Rightarrow} m \mid ac - bd$
$\Rightarrow b$ $m \mid bc - bd$

(1) $\left.\begin{matrix} m \mid a-b \\ m \mid c-d \end{matrix}\right\} \overset{+}{\Rightarrow} m \mid a+c-(b+d) \Leftrightarrow a + c \equiv b + d\,(m)$

(3) (2)-ből lép: k $\left\{\begin{matrix} a \equiv b\,(m) \\ a \equiv b\,(m) \end{matrix}\right.$ (2) $\Rightarrow a^k \equiv b^k\,(m)$

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

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

$m \mid ac - bc \Leftrightarrow \underset{\downarrow}{m} \mid \underset{\downarrow}{c}(a-b) \Leftrightarrow m' \mid c'(a-b) \Leftrightarrow m' \mid a-b \Rightarrow a \equiv b\,(\underset{\downarrow}{m'})$
$md \quad cd$ $\frac{m}{(m,c)}$

LINEÁRIS KONGRUENCIÁK

$ax \equiv b \ (m)$ adott: a, b, m $\quad x = ?$

Tétel: $ax \equiv b \ (m)$ megoldható $\Leftrightarrow (a,m) \mid b$, és ha megoldható $\Rightarrow$ m - ok száma : (a,m)

Biz.: $\Rightarrow$: $d = (a,m) \quad d \mid m \mid ax - b \Big\} d \mid b = (a,m)$

$\Leftarrow$: I. speciális eset: $d = (a,m) = 1$ hiányos maradékrendszer: $x = 0, 1, \dots m-1$

áll: $0 \le i, j \le m-1$, $i \neq j$ $\Big\} a_i \not\equiv a_j \ (m)$

biz.: indirekt: $a_i \equiv a_j \ (m) \ / : a$

$i \equiv j \ (m) \Rightarrow i = j$!

van m. és 1 db van.

II. $(a,m) = d$ tetsz. $\frac{a}{d} = a'$, $\frac{m}{d} = m'$, $\frac{b}{d} = b' \Rightarrow (a', m') = 1$

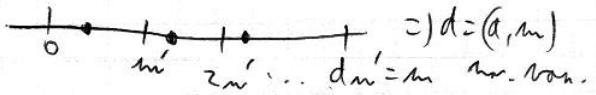
$$\begin{cases} ax \equiv b \ (m) \\ m \cdot t = ax - b \end{cases}$$

$$m' d t = a' d x - b' d \ / : d$$

$$\begin{cases} m' t = a' x - b' \\ a' x \equiv b' \ (m') \end{cases}$$

$(a', m') = 1 \Rightarrow$ 1. eset $\Rightarrow \exists$ 1 mo. !

1 db van mod m!



2 ismeretl. lin. diofantikus egyenlet:

$ax + by = c$ $\quad$ adott: a, b, c

x, y ?

$by = c - ax$

$b \mid c - ax$

$ax \equiv c \ (b)$

megoldható $\Leftrightarrow (a,b) \mid c$

Def: A G gráf **Euler-körének** nevezünk egy zárt élsorozatot, ha az élsorozat pontosan egyszer tartalmazza G összes élét. Ha az élsorozat nyílt, akkor **Euler-utat** kapunk.

Tétel: Egy öf. G gráfban $\exists$ E-kör ($\Leftrightarrow$) G $\forall$ pontjának foka páros.

Biz: $\Rightarrow$ ✓

$\Leftarrow$ G pontszámára teljes indukcióval ($n \geq 2$ triv)

- Legyen $n = 1$-re igaz. Tfh. $\forall k < n$-re igaz, ekkor $k = n$-re is igaz.
- Legyen P egy pont a gráfban. P-ből tegyünk lépést úgy, hogy minden élt pontosan használunk. Ekkor P-be kell visszaérnünk, mert $\forall$ pont foka páros.
- Legyen S a legtöbb élű olyan zárt séta, mely P-ből indul és $\forall$ élt max. egyszer használ fel.
  - Ha $E(S) = E(G) \Rightarrow$ kész ✓
  - Ha $\neq \Rightarrow$ tekintsük a $H = G - E(S)$ gráfot. (P pont izolált)
    Legyen H_1 H-nak egy öf., élekből tartalmazó komponense.
    H_1-ben $\forall$ pont foka páros: tetsz. $x \in V(H_1)$-re $d_{H_1}(x) = \underbrace{d_G(x)}_{\text{páros}} - \underbrace{d_S(x)}_{\text{páros}}$
    $|V(H_1)| < |V(G)| = n$ (legalább $P \notin V(H_1)$)
    - H_1-ben $\exists$ E-kör (ind. feltevés miatt)
    - Legyen $Q \in V(H_1)$ tetsz., tekintsük az eredeti G gráfban a P-ből Q-ba vezető vmelyik u utat!
      u: $P - P_1 - P_2 - \dots - P_i \in V(H_1) - \dots Q$
      S: $P \dots \overset{\curvearrowright}{P_1} \dots P$
      - Bejárom a H_1-beli, majd az eredeti S-beli E-kört P_i-ből. Így egy az S elszámánál nagyobb élszámú ~~zárt~~ zárt élsorozatot találtunk, ami ellentmond a feltevésünknek. Vagyis S E-kör.

Tétel: Wilson: p prím $(p-1)! \equiv -1 \ (p)$

Biz.: $p=11$ $\quad 10! = 1 \cdot \underbrace{2 \cdot 6}_{\equiv 1} \cdot \underbrace{3 \cdot 4}_{\equiv 1} \cdot \underbrace{5 \cdot 9}_{\equiv 1} \cdot \underbrace{7 \cdot 8}_{\equiv 1} \cdot \underbrace{10}_{\equiv -1} \equiv -1 \ (11)$

Ötlet: $1, \dots, p-1$

$a \to b$ úgy, hogy $a \cdot b \equiv 1 \ (p)$

b nem más, mint $ax \equiv 1 \ (p)$

megoldható: $\underbrace{(a,p)}_{1} | 1$ ✓

Előfordulhat-e: $a \to a \ (=) \ a^2 \equiv 1 \ (p)$

$p | a^2-1 = (a+1)(a-1) \Rightarrow p \mid \underbrace{a+1}_{a=p-1}$ vagy $\underbrace{p \mid a-1}_{a=1}$ } 2 db 1-re zérói ben önmaga párja

↳ $(p-1)! = 1 \underbrace{(p-1)}_{\equiv -1} \cdot \underbrace{a \cdot a'}_{\equiv 1} \cdot \underbrace{b \cdot b'}_{\equiv 1} \dots \equiv -1$

Euklidészi algoritmus: Legyen $a, b \in \mathbb{N}$, $b > a$. Definiáljuk az $a_0 := a, a_1, a_2 \dots$ ill. $b_0 = b, b_1 \dots$ számokat úgy, hogy $b_i = q_i \cdot a_i + a_{i+1}$, ill. $b_{i+1} := a_i$ legyen, ahol q_i-t úgy választjuk, hogy $0 \leq a_{i+1} < a_i$ teljesüljön. Az eljárás akkor ér véget, ha $a_{k+1} = 0$.

A fentiek szerint $(a,b) = (a_0, b_0) = \dots = (a_{k+1}, b_{k+1}) = (0, b_{k+1}) = b_{k+1} = a_k$ adódik a legnagyobb közös osztóra. Az eljárás azért ér véget, mert az (a_i) sorozat nemnegatív egészekből áll és csökken, tehát a legkisebb (a_0) felső becslés.

Pl.:

a	b	r
360	225 · 1	+ 135
225	135 · 1	+ 90
135	90 · 1	+ 45
90	45 · 2	+ 0

$\Rightarrow (360, 225) = 45$

Kétismeretlenes, lineáris diofantikus egyenlet megoldása:

$ax + by = c$ adott: a, b, c megoldható $\Leftrightarrow (a,b) \mid c$

$x, y \in \mathbb{Z}$

$by = c - ax$

$b \mid c - ax$

$ax \equiv c \pmod b$

Kongruenciarendszerek:

Pl.: $2x \equiv 5 \pmod 7$ és $3x \equiv 4 \pmod 8$

$x \equiv 6 \pmod 7$

$x = 7k + 6$

$21k + 18 \equiv 4 \pmod 8$

$5k \equiv 2 \pmod 8$ ell!

$k \equiv 2 \pmod 8 \Rightarrow k = 8l + 2$

$x = 56l + 20$

Menete: - megoldom mind2t!

- 1-ből kifejezem x-et és beírom 2-ba
- megoldom a 2-at.

Maradékosztályok: $\{km \mid k=0,\pm1,\dots\}$, $\{km+1 \mid k=0,\pm1\dots\}$, $\vdots$, $\{km+(m-1) \mid k=0,\pm1\dots\}$

Ha két szám ugyanabba a mod m maradékosztályba tartozik, akkor vagy mindkettő relatív prím m-hez, vagy egyik sem

$\varphi(m)$ = m-hez relatív prím mod m maradékosztályok száma

Tételek:

- ~~$\varphi(m)$~~ $m = p$ (prím) $\Rightarrow \varphi(p) = p-1$
- $\varphi(p^2) = p^2 - p$ Biz.: $0, 1, \dots (p-1)p, 1\dots 2p, \dots (p^2-1)$
- $\varphi(p^k) = p^k - p^{k-1}$
- $\varphi(p \cdot q) = pq - q - p + 1 = (p-1)(q-1) = \varphi(p)\cdot\varphi(q)$ $(p \neq q$ két prím)
- Ha $(a,b)=1 \Rightarrow \varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$
- Ha $n = \prod_{i=1}^{k} p_i^{\alpha_i} \Rightarrow \varphi(n) = \varphi\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = \prod_{i=1}^{k} p_i^{\alpha_i} - p_i^{\alpha_i - 1} = n \cdot \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$

Def: Ha a mod m maradékosztályok mindegyikéből kiválasztunk egy elemet, a keletkező számhalmazt mod m teljes maradékrendszernek nevezzük

Def: Ha az m-hez relatív prím mod m maradékosztályok mindegyikéből kiválasztunk egy elemet, a keletkező számhalmazt mod m redukált maradékrendszernek nevezzük

Tétel: $\{x_1, x_2, \dots x_t\}$ egy TMR mod m $\Leftrightarrow$ (1) $\forall i \neq j$-re $x_i \not\equiv x_j \pmod m$
(2) $t = m$

Tétel: $\{x_1, x_2, \dots x_t\}$ egy RMR mod m $\Leftrightarrow$ (1) $\forall i \neq j$-re $x_i \not\equiv x_j \pmod m$
(2) $t = \varphi(m)$
(3) $\forall i$-re $(x_i, m) = 1$

Tétel: Legyen $(a,m)=1$. Ha egy mod m TMR vagy RMR $\forall$ elemét megszorozzuk a-val ugyanúgy TMR-t vagy RMR-t kapunk.

Biz.: - elemszám nem változik – $x \not\equiv y \pmod m$ és $(a,m)=1$, akkor $ax \not\equiv ay \pmod m$:
ha $ax - ay = a(x-y)$ osztható lenne m-mel, akkor $(a,m) \neq 1$ vagy $x \not\equiv y \pmod m$ nem teljesülne.
- RMR esetén: m-hez relatív prím a és x_i számok szorzatánál sem lehet m-el közös prímosztója.

Tétel: Euler-Fermat: Ha $m>1$ tetsz. egész szám és a tetsz. olyan szám, melyre $d(a,m)=1$, akkor $a^{\varphi(m)} \equiv 1 \pmod m$

Biz.: Legyen $\{x_1, x_2, \dots, x_{\varphi(m)}\}$ egy RMR mod m.

Az $\{a x_1, \dots a x_{\varphi(m)}\}$ számhalmaz is egy mod m RMR, tehát az $ax_1, ax_2, \dots a x_{\varphi(m)}$ számoktól valamilyen sorrendben lényegesen az $x_1, x_2 \dots x_{\varphi(m)}$ számokkal.

így: $\prod_{i=1}^{\varphi(m)} (a x_i) \equiv \prod_{i=1}^{\varphi(m)} (x_i) \pmod m$

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

Mivel $d(x_i, m)=1$, ezért $a^{\varphi(m)}-1$ osztható m-mel.

Tétel: „kis" Fermat tétel: Tetsz. p prímre és tetsz. a egészre:

$a^p \equiv a \pmod p$

Biz.: Ha a osztható p-vel $\Rightarrow a \equiv a^p \equiv 0 \pmod p$

Ha nem $\Rightarrow d(a,p)=1$, tehát $a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod p$ /·a

Milyen jó az algoritmus? Ha felülről becsülhető az input hosszának polinomjával

	egység	mod m
összeadás	lin.	pol
kivonás	lin.	pol
szorzás	pol.	pol
osztás	pol.	pol* (szám m)
hatványozás	exp.	pol

a: input
$n \approx \log a$: input hossza
„jó": lépésszáma $\leq P(n)$

$a+b$
$n \approx \log a + \log b$

$a! = 2^a = b$
lépésszám $\geq \ldots + \log b > a \approx c^n$

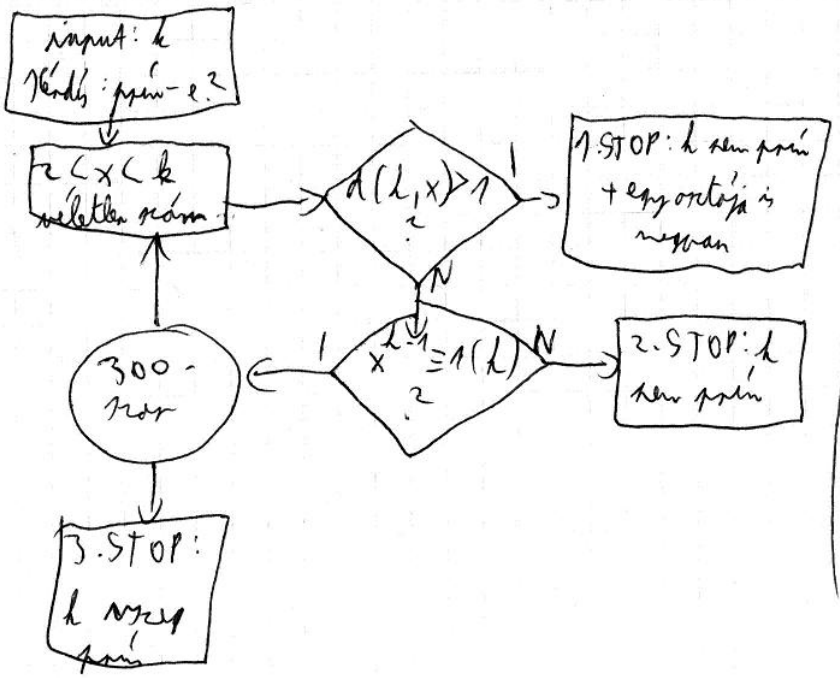
Pl.: $3^{100} \equiv ? \pmod 7$

$\Rightarrow 3^2 \equiv 2 \pmod 7$
$3^4 \equiv 4 \pmod 7$
$3^8 \equiv 2 \pmod 7$
$3^{16} \equiv 4 \pmod 7$
$3^{32} \equiv 2 \pmod 7$
$3^{64} \equiv 4 \pmod 7$
$3^{100} = 3^{64+32+4} \equiv 4 \cdot 2 \cdot 4 \equiv 4 \pmod 7$

$100 = 1100100_2$

$3^a \equiv ?$: log. négyzetreemelés } $\log a$-val arányos
1-esek száma: WCS

Prímtesztelés: Fell.: $\varepsilon - F$: Ha k prím és $(k,x) = 1 \Rightarrow x^{k-1} \equiv 1 \pmod k$



Valószínűség: $\leq \frac{1}{2^{300}}$

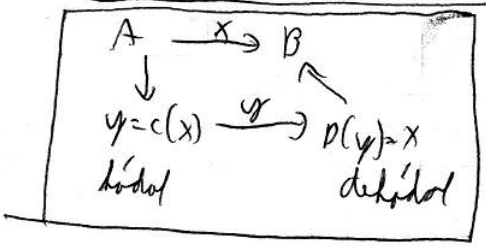
Tetsz. x-re, melyre $(x,k) = 1$:
- <u>osztó</u>, ha $x^{k-1} \equiv 1 \pmod k$
- <u>árnyló</u>, ha $x^{k-1} \not\equiv 1 \pmod k$

Összes osztó: $c_1, \ldots c_l$ / $\cdot a$.

$a_0 c_1, \ldots a_0 c_l$
tört árnyló
⇓
legalább annyi árnyló, mint osztó

Carmichael szám: spec. összetett számok, az algoritmus prímnek mondaná, mert nincs árnyója; minden hozzá relatív szám osztója

Nyilvános kulcsú titkosítások:



RSA

Nyilvános	Titkos
n_B	p_B, q_B
a_B	m_B
$y = C_B(x)$	b_B
	$x = D_B(y)$

B választ: p, q (prímek)

$n := p \cdot q$

$\varphi(n) = (p-1)(q-1) = m$

választ: $1 \le a \le m$; $(a, m) = 1$

$ax \equiv 1 \pmod m$

megoldás: b

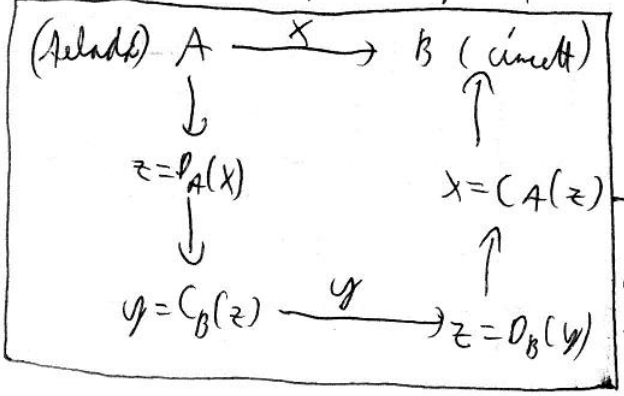
Kódolás: $c: y \equiv x^a \pmod n$ – ez nyilvános

x: az üzenet

$D: y^b \equiv x^{ab} \equiv x^{tm+1} = (x^m)^t \cdot x \equiv x \pmod n$

$x^{\varphi(n)} \equiv 1 \pmod n$

– Címzett: tényleg az igazi feladó küldte?



A rendel B-től. B leszállítja, A nem fizet B → bíróság.

Bíró ezeket kapja:

$\left.\begin{matrix} x \\ y \\ z \end{matrix}\right\}$ $C_A(z) \stackrel{?}{=} x$, $C_B(z) \stackrel{?}{=} y$

Tényleg x és y?

↑ nyilvános kulcsok + z (B szolgáltatja)

CSOPORTELMÉLET

Def: Legyen H tetsz. halmaz, jelölje $H \times H$ a H-beli elemekből képezett rendezett párok (Descartes-szorzat) halmazát. Az $f: H \times H \to H$ minden ilyen értelmezett fv-t 2-változós **műveletnek** nevezünk.

Def: Egy H halmazon értelmezett 2-változós műveletet $(*)$ **kommutatívnak** nevezünk, ha $\forall a,b \in H$-esetén $a*b = b*a$;
asszociatívnak, ha $\forall a,b,c \in H$ esetén $(a*b)*c = a*(b*c)$

Egy $*$ műveletbe $n \in H$ egy **neutrális elem**, ha $\forall a \in H$-ra $a*n = n*a = a$

Legyen $*$ olyan művelet, melyhez $\exists n \in H$ neutrális elem. Ekkor $*$ egy **invertálható művelet**, ha $\forall a \in H$-ra $\exists b \in H$, hogy $a*b = b*a = n$

Def: A H halmazt a rajta értelmezett $*$ művelettel **félcsoportnak** nevezzük, ha $*$ asszociatív. Ha $*$ kommutatív is, akkor kommut. (v. Abel-féle) félcsoportról beszélünk.

Def: Egy H halmazt a $*$ művelettel **csoportnak** nevezünk, ha:
- $*$ asszociatív
- $\exists$ neutrális elem
- $*$ invertálható

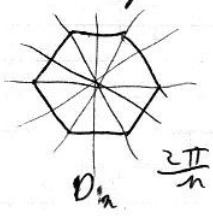
Pl:

H:	$*$:
egészek	$+ \Rightarrow$ Abel-csoport
pozitív egészek	$+ \Rightarrow$ kommut. félcsoport
≥ 0 egészek	$+ \Rightarrow$ kommut. félcsoport, $\exists$ neutrális elem
> 0 valósak	$\cdot \Rightarrow$ Abel-csoport
≥ 1	$\cdot \Rightarrow$ kommut. félcsoport
≥ 1	$\cdot \Rightarrow$ kommut. félcsoport, $\exists$ neutrális elem.
$\{0, \dots (m-1)\}$	$(+ \bmod m) \Rightarrow$ Abel csoport
$\{0, \dots (m-1)\}$	$(\cdot \bmod m) \Rightarrow$ kommut. félcsoport, $\exists$ neutrális elem.

Def: Legyen adva a síkon egy rajz ($\subset \mathbb{R}^2$). Legyen H a síknak azon egybevágósági transzformációinak a halmaza, melyek ezt a rajzot önmagába viszik. Ezen a halmazon legyen $*$ az a művelet, hogy az ilyen transzformációkat egymás után végezzük. Ekkor $(H, *)$ csoport. $(H, *)$ neve: a rajz **szimmetriacsoportja**: $S(R)$

Diéder csoport:

Sokszög



$|D_n| = 2n$

$\{ 2, 4, 4^2, \dots 4^{n-1}, t_1, \dots t_n \}$

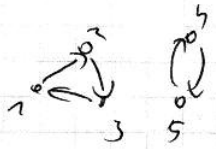
Szimmetrikus csoport:

Def.: permutáció: véges, halmaz bijektív önmagára.
↳ $n!$ féle permutáció

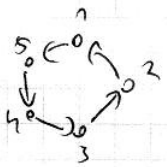
Def.: szimmetrikus csoport (S_n): elemei az n elemű halmaz permutációi, művelet: az egymás után végzés; $|S_n| = n!$

Pl.: $n = 5 - re$

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \quad (123)(45)$$



$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} \quad (15432)$$



$$\pi_1 * \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix} \quad (1)(2)(35)(4)$$

$$\pi_2 * \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix} \quad (14)(2)(3)(5)$$

$o = 2$

Inverz:

$$\pi_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \quad (132)(45)$$

$o = 6$

$$\pi_2^{-1} = (12345) \quad o = 5$$

o = a ciklushosszak legkisebb közös többszöröse

Def.: $(G,*)$ egy tetszőleges csoport, $x \in G$; tekintsük a g elem által generált részcsoportot:

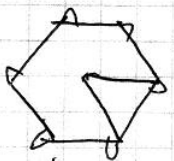
→ 1. $\{g, g*g=g^2, \dots, g^k=e, g^{k+1}=g, \dots$ VAGY

→ 2. $\{g, g^2, g^3, \dots$ $\forall$ eleme különböző lesz

- $o(x) = ac$ x elem rendje, a legkisebb olyan pozitív egész k szám, melyre $x^k = e$ véges; ha nincs ilyen k, akkor végtelen rendű elem.
- Véges csoport rendje a csoport elemszáma: $|G|$

~~Tételek~~:

Ciklikus csoport:



„Füles" sokszög

$|C_n| = n$

Def: Ha $\exists x$ eleme, hogy $\{x, x^2, \dots (x^{-1}), (x^{-1})^2, \dots, e\}$

- Ha egy ciklikus csoport véges rendű, akkor $\exists y$ eleme is, hogy $\{e, y, y^2, \dots\}$, ilyenkor $o(y) = |G|$

Tétel: Ha $|G|$ = prímszám $\Rightarrow G$ ciklikus csoport

Def.: Legyen $(G,*)$ csoport. Egy $X \subseteq G$ részhalmazt részcsoportnak nevezünk, ha X is csoport ugyanarra a műveletre nézve. Jele: $X \leq G$

Def: izomorfia: $(G_1,*_1) \cong (G_2,*_2)$, ha $\exists f: G_1 \overset{1:1}{\leftrightarrow} G_2$, hogy $a *_1 b = c \Rightarrow f(a) *_2 f(b) = f(c)$.

Tétel: Cayley: Minden véges csoport előáll alkalmas szimmetrikus csoport valamely részcsoportjaként.

Tétel: Legyen H a G-nek egy valódi részcsoportja, legyen $h \in H$, $a \notin H \Rightarrow$
$\Rightarrow h * a \notin H$

Biz.: indirekt: $h * a = h' \in H$ lenne, akkor
$a = h^{-1} * h' \in H$ ↯ (felt. h.: $a \notin H$)

Def: $H \subset G$ részcsop., $a \notin H$, $H * a = \{h * a \mid h \in H\}$: a H-hoz tartozó jobboldali
mellékosztály.

Tétel: ($b \notin (H \cup (H * a)) \Rightarrow$ $H * b$)
Nemcsak $H \cap (H * a) = \emptyset$
és $H \cap (H * b) = \emptyset$
hanem $(H * a) \cap (H * b) = \emptyset$ is

Biz.: indirekt: $\exists t . t \in (H * a) \cap (H * b)$
$t = h_1 * a = h_2 * b$
$(h_2^{-1}) * (h_1 * a) = b$
$(\underbrace{h_2^{-1} * h_1}_{= h_3 \in H}) * a = b$
$\hookrightarrow b \in H * a$ ↯

Tétel: Ha G véges $\Rightarrow H$ és jobboldali mellékosztályai lefedik őt $\Rightarrow$
$\Rightarrow |H|$ osztója $|G|$-nek.

Következmény: Ha G véges és $x \in G$ tetsz. $\Rightarrow o(x)$ osztója $|G|$-nek

Állít: 1, csoport kommut. $\Rightarrow \forall a, b$-re $a * b = b * a$)
$\Rightarrow a * H = H * a$ (darabonként ugyanabban a sorrendben)
2, nem kommut. $\Rightarrow$ -általában $\forall a$-ra $a * H = H * a$ (más sorrend)
- Nem.

Tételek: - Véges csoportban $\forall$ elem rendje véges ($x, x^2, x^3 = e, x^4 = x \ldots$) (ismétlődés)
- (Lagrange): Legyen G véges, $H \leq G$. Ekkor H rendje osztja G rendjét.
- $\forall$ véges rendű csoportban $\forall$ elem rendje osztója a csoport rendjének.

Tétel: Egy öf. G gráfban $\exists$ E-út $\Leftrightarrow$ G $\forall$ pontjának foka páros, $\vee$ kivételével.

Biz.: $\Rightarrow$ V

$\Leftarrow$ Tfh.: öf., $\forall x \neq a,b$-re $d(x)$ páros

$G' = G + \{a,b\}$ öf., $\forall$ pont foka páros $\Rightarrow$ $\exists$ benne K E-köre.

$K - \{a,b\}$ lesz E-út G-ben.

Def.: egy részcsoportot **normálosztónak** (normális részcsoport) hívunk, ha $\forall a$-ra $a*H=H*a$.

- Kommut. csoportban $\forall$ részcsoport normálosztó.
- Ha G tetsz. és $|H|=\frac{1}{2}|G| \Rightarrow H$ normálosztó

Def.: $H \leq G$, H normálosztó esetén definiálható egy új $\oplus$ műveletet a H szerinti mellékosztályok halmazán:

$(H*a)\oplus(H*b)=H*(a*b)$

Ekkor a mellékosztályok csoportot alkotnak a $\oplus$ műveletre.

Ezt a csoportot a G csoport H normálosztója szerinti **faktorcsoportjának** nevezik és G/H-val jelölik.

Tétel: $a' \in H*a$, $b' \in H*b \Rightarrow a'*b' \in H*(a*b)$

Biz.: $a'=h_1*a \quad b'=h_2*b$

$a'*b'=(h_1*a)*(h_2*b)=h_1*(a*h_2)*b=\ldots$

H normálosztó: $\left.\begin{array}{l} a*h_2 \in a*H \\ a*h_2 \in H*a \end{array}\right\} \exists h_3$, hogy $a*h_2=h_3*a$

$\ldots=h_1*(h_3*a)*b=(h_1*h_3)*(a*b)$ ✓

Def.: $(H,+,\cdot)$ **gyűrű**, ha: (1) $(H,+)$ kommutatív csoport

(2) $(H,\cdot)$ félcsoport

(3) Disztributivitás: $\forall a,b,c\in H$-ra $(a+b)c = ac+bc$ és $a(b+c)=ab+ac$

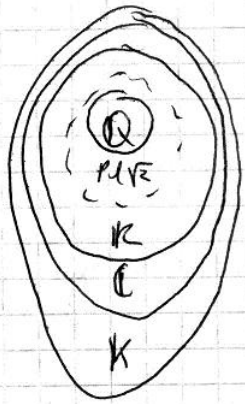
Egy gyűrű **kommutatív**, ha a szorzás is kommutatív

Egy gyűrű **egységelemes**, ha a szorzásnak is van egységeleme

Egy gyűrű **nullosztómentes**, ha $\underbrace{a}_{\text{egyik nem nulla}}\cdot\underbrace{b}_{\text{másik nem nulla}} = 0 \Rightarrow a=0$ vagy $b=0$ vagy mindkettő

Egy gyűrű **test**, ha $(H-\{0\},\cdot)$ csoport (0: összeadás 0-eleme)

Kommutatív test: test $\Leftrightarrow$ a $\cdot$ műv. kommutatív



Pl.:

H	gyűrű	komm.	egységelem	nullosztómentes	test
Egész számok	+	+	+	+	−
Racionális	+	+	+	+	+
Valós	+	+	+	+	+
Komplex	+	+	+	+	+
$n\times n$ mátrix	+	−	+	−	−
$f(x)=\sum_{i=0}^{n} a_i x^i,\ a_i\in\mathbb{R}$	+	+	+	+	−

$\mathbb{K}$: nem komm. ; kvaterniók teste

$\mathbb{K}=\{a+bi+cj+dk \mid a,b,c,d\in\mathbb{R}\}$

$i^2=j^2=k^2=-1$

$ij=k \quad jk=i \quad ki=j$

$ji=-k \quad kj=-i \quad ik=-j$

Tétel: Frobenius: – $\mathbb{C}$ és $\mathbb{K}$ közötti nincs újabb test

– $\mathbb{C}$-n kívül nem létezik bővebb komm. test

– $\mathbb{K}$-n kívül sem nincs bővebb test

Köztes testek: $\exists T$ test, hogy $\mathbb{Q} \subsetneq T \subsetneq \mathbb{R}$

Pl.: $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$ ez test: $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}$$

Áll.: $\sqrt{3}\notin\mathbb{Q}[\sqrt{2}]$

Biz.: indirekt: $\sqrt{3}=a+b\sqrt{2}$

$3=a^2+2b^2+2ab\sqrt{2} \to \sqrt{2}=\frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$ ↯

$Q[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Q\} \sim 2D$

$Q[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in Q\} \sim 3D$ → Térbővítés: bővebb test az alatta lévő test fölötti lin. vektortér

ebből szorzás kivezet

$x \cdot \sqrt{2} \in$

<u>Tétel</u>: Megadom adott: $c_0 + c_1x + c_2x^2 + \dots c_kx^k = 0$ (rac. együtthatók)
Ha ennek „t" a gyöke, akkor $Q[t] = \{a_0 + a_1t + a_2t^2 + \dots \mid a_0 \dots \in Q\}$.
Ebben a testben az egyenlet megoldható lesz.
$\dim \leq k$

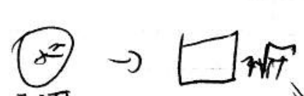
\$: körzővel és vonalzóval megszerkeszthető távolságok halmaza, ez is közbülső test: $Q \subseteq \$ \subseteq \mathbb{R}$

+, − osztás, szorzás

Rajzolható:

<u>Tétel</u>: <u>Galois</u>: $x \in \$ \Leftrightarrow \dim \dots = 2^{?}$

nincs benne: − kör negyszögesítése:



↘ nincs benne

− kockakettőzés: $2a^3 \to \sqrt[3]{2}\, a$ dim 3 és nem 2

− szögharmadolás: $\sin 3\alpha = \dots \sin\alpha + \dots \sin^3\alpha$

3-adfokú egyenlet

Def.: G k színnel színezhető, ha csúcsai úgy színezhetők k színnel, hogy a szomszédos csúcsok különböző színűek.

Def.: kromatikus szám: $\chi(G)=k$, ha $\exists$ k színnel színezés, de ~~$k-1$-nel~~.

Def.: klikk: G egy teljes részgráfja, klikkszám: a G gráfban található legnagyobb teljes részgráf pontjainak a száma. jel: $\omega(G)$

Tétel: - $\forall G$ gráfra $\chi(G) \geq \omega(G)$

- $\chi(G)=1 \Leftrightarrow E(G)=\emptyset$ és $V(G)\neq\emptyset$

~~- $\chi(G)=2 \Leftrightarrow$ G páros gráf~~

Def.: Egy G gráfot páros gráfnak nevezünk, ha G pontjait $V(G)$ halmaza két nem (A, B halmaz) osztható úgy, hogy G minden élének egyik végpontja A-ban, másik B-ben van.

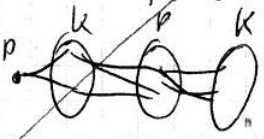
Jelölése: $G=(A,B)$.

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.

Tétel: G páros $\Leftrightarrow$ $\forall$ körének hossza páros.

Biz.: $\Rightarrow$: Ha G páros, és $\exists$ egy kör G-ben, akkor $\exists$ pontjai felváltva vannak P-ben és K-ban. $\Rightarrow$ egy $|V(C)|$ páros

$\Leftarrow$: ($\nexists$ G öf., lehet komponensenként)



G $\forall$ köre páros hosszú: megoldottjuk P-t és K-t

Ez jó elosztás, mert ha pl P-ben lenne szomszédos pont, akkor a gráfban lenne nem kétl. kör. ☺

Tétel: $\exists G_2, G_3, \ldots$ gráfsorozat, melynek $\forall$ tagjára teljesül, hogy $\omega(G_k)=2$ és $\chi(G_k)=k$ ($k \geq 2$ egész)

Mycielski - konstrukció: $G \rightarrow M(G)$

$\omega(M(G)) = \omega(G)$

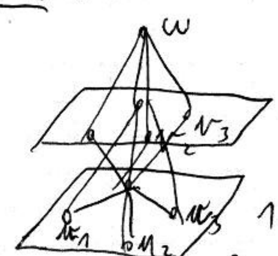
$\chi(M(G)) = \chi(G)+1$

$G_2 =$ o—o

$G_3 = M(G_2)$

$G_4 = M(G_3) \ldots$

Biz.: G_2: o—o Tfh. G_k, ebből konstruáljuk G_{k+1}-et.

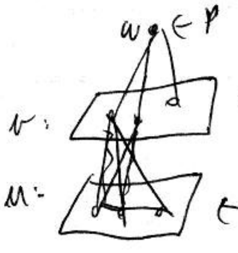


3. em Új élek: $\forall v_i$-t kössük össze u_i $\forall$ szomszédjával

2. em w-t kössük össze $\forall v_i$-vel

1. em

- $\omega(M(G)) \stackrel{?}{=} \omega(G)$: kell: ha G_k-ban nem volt Δ, akkor G_{k+1}-ben sincs.
  - G_k-ban nincs.
  - egyik csúcs $w \Rightarrow$ másik kettő v_i és v_j, de ezek nem szomsz.
  - v_i a Δ egyik csúcsa $\Rightarrow u_x$ és u_y. De akkor u_i, u_x, u_y Δ ↯
- $\chi(M(G)) \leq \chi(G)+1$: u_i-ket mint G_k-ban k színnel.
  $\forall v_i$-t ugyanolyanra, mint u_i-t, w-t $(k+1)$-el.
- Indirekt tfh. $\chi(M(G)) = \chi(G)$ (ennél kisebb nem lehet, mert részgráfként tartalmazza G_k-t)



$w \in P$

v: $\leftarrow$ itt $\nexists P$

u: $\leftarrow$ itt $\exists P$? $\rightarrow$ a: Ha nincs, akkor a 1 színnel kisebb lenne.

b: u-ban lévő P-ket átfestem a párja színére $\Rightarrow$ nem romlik el $\Rightarrow$ nem lenne P u_i-kben ↯

Def: $\Delta(G) = \max(d(v))$; $v \in V(G)$; $\delta(G) = \min(d(v))$

Tétel: $\forall G$ gráfban $\chi(G) \leq \Delta(G)+1$

Biz.: Mohó algoritmus: gráf pontjait számozzuk $\Rightarrow$ legkisebb sorszámú olyan színt kapja, amilyen szomszédja még nincs. Ekkor max Δ színt használtunk, és a soron következő elem megkapja a $\Delta + 1$-et.

Tétel: Brooks: Ha G egyszerű ösf. (G nem teljes és nem ptl. kör) $\Rightarrow \chi(G) \leq \Delta(G)$

Tétel: ∀ egyszerű, síkbarajzolható gráfra $\chi \le 4$. (4-szín tétel)

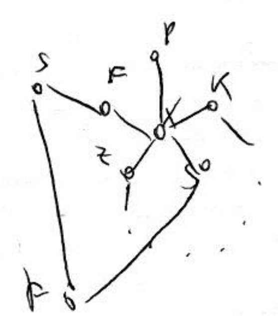
Biz.: 5-szín tétel:

Indirekt: Legyen G_0 egy minimális ellenpélda, tehát G_0 egyszerű, síkbarajzolható, $\chi(G_0) \ge 6$, $\forall x$-re $\chi(G_0 - x) \le 5$

- kell: $\delta(G_0) \le 5$. biz.: indirekt. ∀ pont foka $\ge 6 \Rightarrow \sum d = 2e \ge 6p$

$e \le 3p-6 \longleftrightarrow e \ge 3p$

- Ha $\delta(G_0) \le 4 \Rightarrow$ ↯, ugyanis: legyen $d(x) \le 4$, x-et elhagyva $G_0 - x$ kiszínezhető 5 színnel
- Ha $\delta(G_0) = 5 \Rightarrow$ ↯, ugyanis



F-nek kell legyen S szomszédja

S-nek kell legyen F szomszédja ...

F−S, K−Z: 2 lánc

Mivel G_0 síkbarajzolt, ezért a 2 lánc csak közös ponton keresztezheti egymást, a színezés miatt ez nem lehet ↯

$\Rightarrow$ ↯

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

G élkromatikus száma $\chi_e(G) = k$, ha G élei k színnel színezhetők, de k−1 színnel nem.

Tétel: $\Delta(G) \le \chi_e(G)$ triv.

Tétel: Vizing: $\Delta(G) \le \chi_e(G) \le \Delta(G)+1$ ∀G egyszerű gráfra

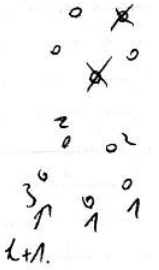
Def.: Egy G gráf **perfekt**, ha $\chi(F) = \omega(F)$ és G minden G' feszített részgráfjára is teljesül, hogy $\chi(G') = \omega(G')$

Áll.: C_{2k+1} $(k>1)$ nem perfekt: triv.

Áll.: $\overline{C_{2k+1}}$ $(k>1)$ nem perfekt.

Biz.: $\omega(\overline{C_{2k+1}}) = k$

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



Tétel: **erős perfekt gráf tétel:** G perfekt $(\Leftrightarrow)$ Abban C_{2k+1} $\overline{C_{2k+1}}$ feszített részgráként

Tétel: **Lovász:** G perfekt $(\Leftrightarrow)$ $\overline{G}$ perfekt (gyengén perf. gráf tétel)

Def.: Legyenek $I_1 = [a_1, b_1]$, $I_2 = [a_2, b_2]$, ... korlátos, zárt intervallumok és minden a_i, b_i legyen páronként különböző 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 $I_i \cap I_j \neq \emptyset$. Az így előálló gráfokat **intervallumgráfoknak** nevezzük.

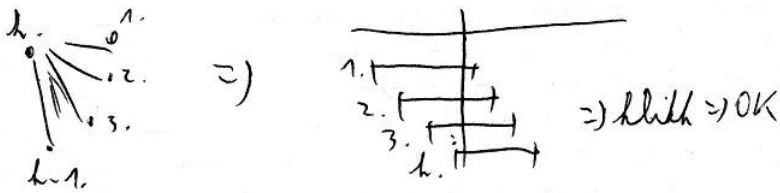
Tétel: $\forall$ intervallumgráf perfekt.

Biz.: algoritmus: $I_1 \ldots I_n \rightarrow$ bal végpont szerinti növő sorrend

$\rightarrow$ mohó színezés

Tfh.: k színt használ $\Rightarrow$ Cél: k színűre kellett találni

I_j először kapta a k. színt



Def.: $\vec{G}(V,E)$ **irányított gráf** $:\Leftrightarrow (\vec{x,y}) \in E$

- irányított út, irányított kör, erősen öf. gráf: $\forall$ pontból $\forall$ pontba el lehet jutni ir. körön
- $d_{ki}(v)$: ki-fok; $d_{be}(v)$: be-fok; $\sum_{v\in V} d_{ki}(V) = \sum_{v\in V} d_{be}(V) = |E|$
- $d_{ki}(V)=0$ nyelő; $d_{be}(V)=0$ forrás

Tétel: Ha $\vec{G}$ emeletekre bontható $\Leftrightarrow$ nem tart. ir. kört.

Biz.: $\Rightarrow$ V

$\Leftarrow$: van benne nyelő $\Rightarrow$ utolsó emelet, törlöm

PERT módszer:

Algoritmus:

- emeletekre bontás ($\emptyset$ ir. kör)
- ütemezés: $\max(t_1 + l(x_1,y), t_2 + l(x_2,y), \dots$
- kritikus élek (min 1 db.

$\chi(G) = 2 (\Leftarrow)$ G páros gráf

Def.: Egy G gráfot **páros gráfnak** nevezünk, ha G pontjainak $V(G)$ halmaza két részre, A és B halmazra, osztható úgy, hogy G minden élének egyik végpontja A-ban, másik B-ben legyen. Jelölése: $G = (A, B)$

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

Tétel: G páros $(\Leftrightarrow)$ $\forall$ körének hossza páros

Biz.: $\Rightarrow$ Ha G páros, és C egy kör G-ben, akkor C pontjai felváltva vannak A-ban és K-ban, így $|V(C)|$ = páros

$\Leftarrow$: (öt, mert lehet komponensenként is)

$\forall$ köre páros hosszú, ezért vegyük P és K-t. Ez jó elosztás, mert ha P-ben lenne 2 szomszédos pont, akkor lenne köre pl. K-ban

Def.: **párosítás:** diszjunkt (független) élek halmaza

Teljes ~: olyan párosítás, amely $\forall$ pontot lefed.

Max. ~: - maximum: lehető legnagyobb: !!

- maximal: tovább nem bővíthető: ⚠

Sper: páros gráfban: házasság probléma

Jelölések:
- τ: lefogó pontok ~~min~~ száma
- α: független pontok max száma
- ρ: lefogó élek min száma
- ν: független élek max száma

Tétel: Kőnig: Ha G páros $\Rightarrow$ $\nu(G) = \tau(G)$ és $\alpha(G) = \rho(G)$

(G-ben nincs izolált pont)

Biz.: $F_3 \cup L_2$ lefogó halmaz, ugyanis

L_c: párban, elérhető alt. úton

L_1: F_1-hez nem elérhető

$N(F_1 \cup F_2) = L_2 \Rightarrow$ $\forall$ él legalább 1-hez van fogva ✓

$\tau(G) \leq |F_3 \cup L_c| = |F_3| + |L_c| = |F_3 \# F_2| = |M| \leq \chi(G) \leq \tau(G)$ ✓

diszjunkt párban

$\alpha + \tau = n$

$\rho + \nu = n$ $\Rightarrow$ $\alpha = \rho$