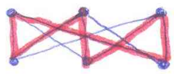
1. TÉTEL

Hamilton-körök és -utak. Szükséges feltétel Hamilton-kör/út létezésére. Elégséges feltételek: Dirac és Ore tétele.

DEF.: Hamilton-kör/út: a gráf olyan köre/útja, ami a gráf minden csúcsát (egyszer) tartalmazza.
ezt elég tömörségben megjegyezni, mivel egy körben/útban szereplő minden csúcs különböző

Példa: a $K_{3,3}$-ban egy H-kör:

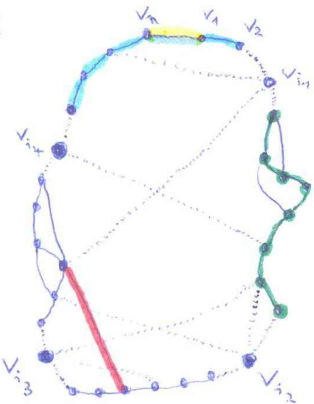


Szükséges feltételek:

(1) Ha ∃ H-kör ⇒ G-ből akárhogy k csúcsot törölve a maradék legfeljebb k komponensre esik szét

(2) Ha ∃ H-út ⇒ ——— " ——— $k+1$ — " —

biz.: H-kör:



A H-kör pontjai legyenek: $v_1, v_2, v_3, \dots, v_n$
és legyen $v_{i_1}, v_{i_2}, \dots, v_{i_k}$ az a k pont, amit elhagyunk.
Vegyük észre, hogy az elhagyott pontok közötti „ívek" biztosan összefüggő komponenseket alkotnak!
Pl.: $(v_{i_1+1}, v_{i_1+2}, \dots, v_{i_2-1})$ ív is összefüggő lesz, hiszen két szomszédos pontja között az eredeti H-kör egy éle fut.
Mivel éppen k ilyen ívet kapunk, nem lehet több komponens k-nál. ✓ (Kevesebb lehet, hiszen különböző ívek között futhatnak élek, pl. a piros él.)

H-út: a bizonyítás hasonló az előzőhöz. Pl. hagyjuk el a gráfból a $v_n v_1$ élet, hogy utunk H-utunk legyen. Amíg az előző példában a pontok elhagyása után a $v_{i_4+1}, \dots, v_n, v_1, v_2$ ív öf. volt, itt már nem, mert $v_n v_1 \notin E(G)$. Tehát legfeljebb $k+1$ komponens keletkezhetett. ✓

Elégséges feltételek:

TÉTEL: (Ore) Ha az n pontú gráfban ∀ nem szomszédos x, y pontpárra $d(x)+d(y) \geq n$ ⇒ ∃ H-kör

biz.: indirekt tfh.: a feltétel teljesülése ellenére ∄ H-kör a G gráfban.
A gráfhoz vegyünk hozzá éleket úgy, hogy továbbra se legyen benne H-kör. Ezt ismételjük addig, amíg lehet. Az így kapott gráfot jelöljük G'-vel, amire szintén teljesül a feltétel.
G'-ben biztosan van 2 nem szomszédos pont, legyen ez x, y. $G' + \{x, y\}$ gráfban ∃ H-kör ⇒ G'-ben ∃ H-út.
Legyen ez $P = (\overset{x}{z_1}, z_2, \dots, \overset{y}{z_n})$. Ha x szomszédos z_k-val ⇒ y nem szomsz. z_{k-1}-gyel, mert $(z_1, \dots, z_{k-1}, z_n, z_{n-1}, \dots, z_k, z_1)$ H-kör lenne, tehát $d(y) \leq n-1-d(x)$ ⇒ $d(x)+d(y) \ngeq n$ ↯

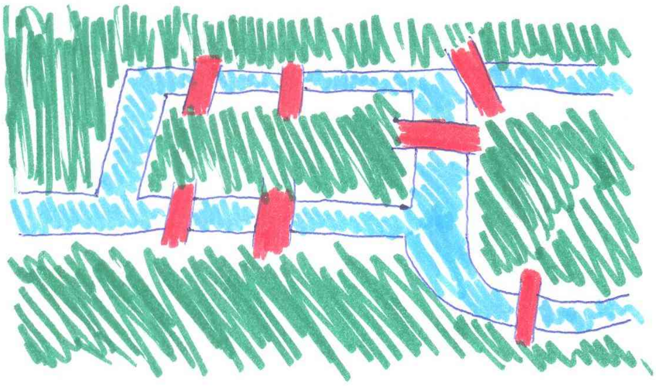
TÉTEL: (Dirac) Ha az n pontú gráfban ∀ pont foka legalább $\frac{n}{2}$ ⇒ ∃ H-kör

biz.: teljesül az Ore-feltétel: ∀ x, y pontpárra $d(x) + d(y) \geq n$. ✓

2. TÉTEL

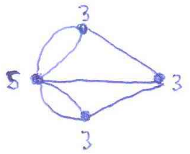
Euler-körök és -utak, ezek létezésének szükséges és elégséges feltétele.

Königsbergi hidak problémája



← Feladat: $\forall$ hídon pontosan egyszer átkelni

→ a feladat gráfelméletbeli megfelelője:



A folyók által határolt területeknek pontok, a hidaknak élek felelnek meg.

DEF.: G-ben Euler-kör egy olyan zárt élsorozat, ami a gráf $\forall$ élét pontosan egyszer tartalmazza.
Ha az élsorozat nem feltétlenül zárt, akkor Euler-utat kapunk.

Megjegyzés: $\forall$ Euler-kör egyben Euler-út is.
Az Euler-kör/út általában nem „rendes" kör/út a gráfban, mert egy ponton többször is áthalad.

TÉTEL: (szükségesség) (1) G-ben $\exists$ E-kör $\Longrightarrow$ $\forall$ pont foka páros

(2) G-ben $\exists$ E-út $\Longrightarrow$ G-nek 0 vagy 2 ptl. fokú csúcsa van

biz.: (1) Induljunk el a gráf egy tetszőleges pontjából, és járjuk körbe az E-kör mentén. Minden ponton pontosan annyiszor mentünk be, ahányszor kimentünk. A kimenések és bemenések számának összege a pont fokszáma, ami így biztosan páros.

(2) Az előzőhöz hasonlóan belátható, hogyha G-ben $\exists$ E-út, akkor az E-út két végpontjának kivételével $\forall$ pont foka páros.

TÉTEL: (Euler) G öf. véges gráf

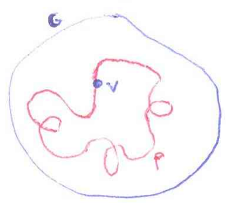
(1) G-ben $\exists$ E-kör $\Longleftrightarrow$ $\forall$ pont foka páros

(2) G-ben $\exists$ E-út $\Longleftrightarrow$ G-nek 0 vagy 2 ptl. fokú csúcsa van

biz.: A szükségességet az előbb bebizonyítottuk. ✓

Elégségesség:

(1) Legyen $v \in V(G)$ a gráf tetszőleges pontja, P pedig egy v-ből induló élismétlés nélküli séta, amíg elakad. Mivel $\forall$ pont foka ps $\Longrightarrow$
- P v-ben akad el
- v-nek $\forall$ élét használja
- $\forall$ csúcsból páros élet használ



Legyen P' az ilyen séták közül a leghosszabb.

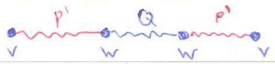
Állítás: P' E-kör

biz.: indirekt tfh.: nem az

H: G-ből elhagyjuk a P'-beli éleket; tudjuk, hogy H-ban is $\forall$ fokszám ps (ps − ps = ps)

w: legyen olyan csúcs, amire illeszkedik H-beli és P'-beli él is (megtaláljuk, mert a gráf öf.)

Q: legyen egy w-ből induló H-ban élismétlésmentes w-ben elakadó séta



} ez hosszabb P'-nél ↯

(2) Ha $\forall$ fokszám ps $\Longrightarrow$ OK ✓ (Euler-kör)

Ha van két ptl. fokú pont: u, v akkor húzzunk élet uv közé, így $\forall$. pont foka páros lesz, tehát lesz E-kör. Ha ebből a gráfból elhagyjuk uv-t, akkor lesz E-út. ✓

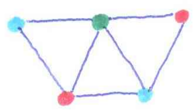
3. TÉTEL

Gráfok színezése. $\chi(G)$ fogalma és viszonya $\omega(G)$-hez, illetve $\Delta(G)$-hez. Brooks tétele (biz. nélkül), Mycielski konstrukciója.

DEF.: egy gráf <u>k színnel színezhető</u>, ha csúcsai k színnel színezhetők úgy, hogy a szomszédos csúcsok különböző színt kapnak.

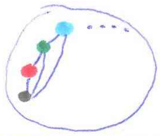
G <u>kromatikus száma</u> k, ha G k színnel színezhető, de $(k-1)$-gyel nem. Jele: $\chi(G) = k$

<u>Pl.:</u>

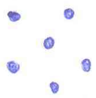


$\chi(G) = 3$

K_{100}

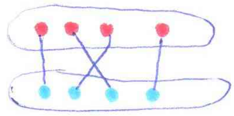


$\Rightarrow \chi(K_{100}) = 100$



üres gráfnál $\chi = 1$

páros gráfnál:



$\chi \leq 2$ (akkor < 2, ha üres a gráf)

DEF.: G <u>maximális klikkmérete</u> k, ha G-ben van k db csúcs, hogy közülük bármely 2 szomszédos, de $(k+1)$ nem. Jele: $\omega(G) = k$

/Az elnevezés onnan származik, hogy G egy teljes részgráfját <u>klikknek</u> nevezzük./

<u>Állítás:</u> $\omega(G) \leq \chi(G)$ $\forall G$ gráfban

<u>biz.:</u> ha $\omega(G) = k$, akkor ehhez a k csúcshoz kell k db szín

<u>Példa:</u>

C_5:

$\omega(C_5) = 2$

$\chi(C_5) = 3$

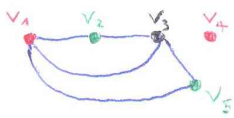
<u>Mohó színezés:</u> csúcsokat jelöljük $v_1, v_2, \dots, v_n$-nel

a színeknek adjunk számokat: ① ② ③ …

$v_1 \rightarrow$ ①

Ha már $v_1, \dots, v_i$ színezett $\rightarrow$ v_{i+1} színe legyen a legkisebb sorszámú olyan szín, amilyen szomszéd még nincs

<u>Pl.:</u>



<u>**TÉTEL:**</u> $\chi(G) \leq \Delta + 1$ (ahol Δ a G gráf max. fokszáma)

<u>biz.:</u> Ha a mohó színezéssel elkezdjük tetsz. sorrendben színezni a gráf pontjait, akkor nem kell $\Delta+1$-nél több színt felhasználnunk, mert amikor egy újabb pontot akarunk kiszínezni, akkor ennek legfeljebb Δ szomszédja van már kiszínezve, így a $\Delta+1$-ediket felhasználhatjuk.

<u>**TÉTEL:**</u> (Brooks) Ha G egyszerű öf. gráf, nem K_n, nem C_{2k+1} $\Longrightarrow$ $\chi(G) \leq \Delta$

<u>**TÉTEL:**</u> (Mycielski konstrukciója) $\forall$ $2 \leq k$ egészre $\exists$ G_k gráf, hogy $\omega(G_k) = 2$ és $\chi(G_k) = k$

<u>biz.:</u> G_2-nek megfelel: •—•. Tfh. már G_k-t megalkottuk, készítsük el ebből G_{k+1}-et!

G_k pontjai: $a_1, a_2, \dots, a_n$. Vegyünk fel $n+1$ új pontot: $b_1, \dots, b_n, c$-t a következőképp:

$\forall$ b_i-t kössük össze a_i G_k-beli szomszédjaival (de a_i-vel ne), c-t pedig $\forall$ b_i-vel.

<u>Áll.:</u> $\omega(G_{k+1}) = 2$

<u>biz.:</u> indirekt: tfh. $\exists$ G_{k+1}-ben háromszög. Ennek nem lehet mind3 csúcsa G_k-ban. Ha c a Δ egyik csúcsa, a másik kettő csak b_i és b_j lehet, de ezek nem szomszédosak. Ha b_i a Δ egyik csúcsa, akkor a másik két csúcs a_x és a_y lehet. Mivel b_i szomszédai megegyeznek a_i szomszédaival, akkor nem csak $b_i a_x a_y$, hanem $a_i a_x a_y$ is Δ lenne. $\downarrow$

<u>Áll.:</u> $\chi(G_{k+1}) \leq k+1$

<u>biz.:</u> Színezzük ki $\forall\, a_i$-t ugyanolyan színnel, mint G_k egy k színnel való színezésében, majd $\forall\, b_i$-t színezzük a_i színűre, c kapja a $k+1$-edik színt. ✓

<u>Áll.:</u> $\chi(G_{k+1}) \neq k$

<u>biz.:</u> indirekt tfh. $\chi(G_{k+1}) = k$ (ettől kisebb nem lehet, mert G_{k+1} részgráfként tartalmazza G_k-t és $\chi(G_k) = k$.)

Jelöljük x pont színét $f(x)$-szel. Legyen $f(c) = k \implies f(b_i) \in \{1, 2, \dots, k-1\}$

Megadunk egy f' színezést az a_i pontok által feszített részgráfon (ami G_k-val izomorf).

$$f'(a_i) = \begin{cases} f(b_i) & \text{ha } f(a_i) = k \\ f(a_i) & \text{egyébként} \end{cases}$$

Belátjuk, hogy f' egy $(k-1)$ színnel való jó színezése G_k-nak, ami ellentmondás, mert $\chi(G_k)=k$.

Az olyan élekkel nem lehet probléma, amiknek egyik végpontja sem volt k színű.

Tfh. $f(a_i)=k$ és a_i szomszédos egy olyan a_j-vel, hogy $f'(a_i) = f'(a_j)$.

$f(a_i) = k \implies f'(a_i) = f(b_i)$

Mivel az eredeti színezés jó volt: $f(a_j) \neq k \implies f'(a_j) = f(a_j)$

$$\Downarrow$$

$$f(b_i) = f'(a_i) = f'(a_j) = f(a_j)$$

$$\Downarrow$$

$$f(b_i) = f(a_j)$$

De $a_i a_j$ szomsz. G_k-ban $\implies$ $b_i a_j$ szomsz. G_{k+1}-ben $\rightarrow$ ↯

$$\Downarrow$$

$\chi(G_k) = k$ $\qquad$ f' egy $(k-1)$ színezése G_k-nak

$$\Downarrow$$

↯

4. TÉTEL

Síkbarajzolható gráfok kromatikus száma, ötszíntétel. Élkromatikus szám: $\chi_e(G)$ viszonya $\Delta(G)$-hez, Vizing-tétel (biz. nélkül).

Általában nem könnyű jó becslést adni egy gráf kromatikus számára. Ha viszont a gráf síkbarajzolható, akkor lényegesen könnyebb a helyzet.

TÉTEL: (5-szín tétel) Ha G síkbarajzolható gráf, akkor $\chi(G) \leq 5$

biz.: A párhuzamos élek nem befolyásolják a színezést, ezért feltehetjük, hogy a gráf egyszerű.
2 pontú gráfra nyilván igaz az állítás. Nagyobb gráfokra pontszám szerinti indukcióval bizonyítunk: tfh. a legfeljebb $(n-1)$-pontú gráfokra a tétel igaz. Legyen G egy $3 \leq n$-pontú egyszerű sr. gráf.
Ha $\forall$ pont foka legalább 6 volna, akkor ez lenne: $3n-6 \geq e = \frac{\sum d(v)}{2} \geq \frac{6n}{2} = 3n$ ↯ $\Rightarrow$

$\Rightarrow$ Van tehát G-nek legfeljebb 5-ödfokú csúcsa, jelöljük x-szel.

Mivel $G-x$ is egyszerű sr. gráf, az indukciós feltevés miatt 5-színezhető. Ha x szomszédai max 4 színt kapnak, akkor x megkaphatja az ötödik színt. Ez akkor nem működik, ha $d(x)=5$ és mind az 5 szomszéd külö. színű. Ha x-nek bármely két szomszédja között lenne él, akkor G-ben lenne K_6, ami ellentmond síkbarajzolhatóságának. Tehát x két szomszédja, y és z nincs összekötve. Húzzuk össze egy ponttá x, y, z pontokat, az így kapott G' gráf az ind. felt. miatt 5-színezhető. Az ennek megfelelő színezés G-ben nem jó, mert x, y, z egyszínűek. G-ben x-nek 3 szomszédja van y-on és z-n kívül, ezek max 3 színt foglalnak le, és további két szomszéd, y és z egyszínű (ez megtehető, mert nem szomszédosak). Tehát x-nek marad az ötödik szín. ✓

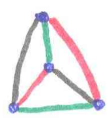
TÉTEL: (4-szín tétel) Ha G sr. gráf $\Rightarrow \chi(G) \leq 4$

Ezt a tételt Appel és Haken bizonyította be először 1977-ben. Ők alkalmaztak először bizonyításhoz számítógépes módszereket.

DEF.: egy gráf élei k színnel színezhetők, hogyha $\forall$ 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 $(k-1)$-gyel nem.

Megjegyzés: az élkromatikus szám megegyezik a gráf élgráfjának kromatikus számával.

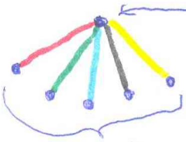
Példa:



$\chi_e(K_4) = 3$

Állítás: $\Delta \leq \chi_e(G)$ (ahol $\Delta = \max_{x \in V(G)} d(x)$)

biz.:



← tekintsük a gráf egy max. fokú csúcsát!

→ Ennek Δ db szomszédja van, az ezekhez húzott élek különböző színt kell, hogy kapjanak.

TÉTEL: (Vizing) Ha G egyszerű $\Rightarrow \chi_e(G) \leq \Delta + 1$

Ellenpélda:

$\chi_e = 6$

$\Delta = 4$

← a párhuzamos élek miatt a gráf nem egyszerű

5. TÉTEL

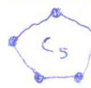
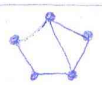
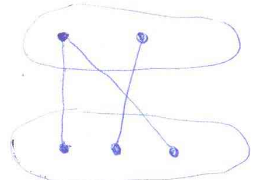
Perfekt gráfok: erős perfekt gráf tétel (csak a szükségesség bizonyításával), Lovász tétele (biz. az erős perfekt gráf tételből). Intervallumgráfok perfektsége.

Egy gráf kromatikus száma és klikkszáma között általában nem tételezhetünk fel egyenlőséget. Mégis igen sok példa van arra, amikor ez a két paraméter egyenlő (pl. páros gráfok). Felmerül a kérdés, hogy érdemes-e közelebbről is megvizsgálni ezeket a gráfokat. A válasz akkor igen, ha még kikötjük azt, hogy ne csak magára a gráfra, hanem ∀ feszített részgráfjára is igaz legyen. Enélkül ugyanis egy tetszőleges gráfot kiegészíthetnénk egy elegendően nagy klikk hozzáadásával.

DEF.: G perfekt, ha $\underbrace{G \text{ minden feszített } G' \text{ részgráfjára}}$ $\chi(G') = \omega(G')$

megjegyzés: ez a halmaz tartalmazza magát G-t is!

Példák:

			páros gráfok: 
$\chi=3$, $\omega=2$, nem perfekt	$\chi=3$, $\omega=3$ ⇒ de nem perfekt, mert tartalmazza fesz. részgráfként az előző C_5-t	$\chi=3$, $\omega=3$ + ∀ fesz. részgráfjára $\chi'=\omega'$ ⇒ perfekt ✓	ha van éle: $\chi=\omega=2$; ha nincs: $\chi=\omega=1$ ⇓ ps. gráfok részgráfja is ps. ⇒ ezek perfektek ✓

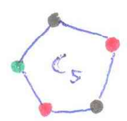
TÉTEL: (erős perfekt gráf tétel) G perfekt $\iff$ sem G, sem $\overline{G}$ nem feszít min. 5 hosszú ptl. kört

biz.: (szükségesség)

A tétel állítása átfogalmazható: G perfekt $\iff$ G nem tartalmaz feszített részgráfként C_{2k+1} vagy $\overline{C_{2k+1}}$-t $(2 \le k)$

Állítás: $(2 \le k)$ C_{2k+1} nem perfekt

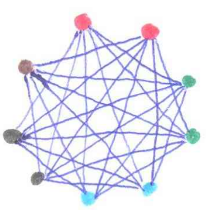
biz.:



$\left.\begin{array}{l}\omega=2\\ \chi=3\end{array}\right\} \Rightarrow \chi \ne \omega$

Állítás: $(2 \le k)$ $\overline{C_{2k+1}}$ nem perfekt

biz.:

$\overline{C_9} \rightarrow$ 

Ebben ∃ k csúcsból álló klikk (ha ∀ második pontot kiválasztjuk). De $k+1$ csúcs nincs, mert akkor az először és utoljára kiválasztott pont nem lenne szomszédos.

$\Downarrow$

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

Mivel ∀ színt legfeljebb 2 csúcshoz használhatjuk ⇒ k színnel csak $2k$ csúcs festhető ⇒ $\chi(\overline{C_{2k+1}}) \ge k+1$ ⟶ nem perfekt

(valójában $k+1$ szín elég is, tehát $\chi(\overline{C_{2k+1}}) = k$)

TÉTEL: (Lovász gyenge perfekt gráf tétele) G perfekt $\iff$ $\overline{G}$ perfekt

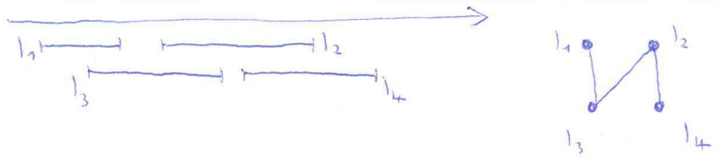
Megjegyzés: elég csak az egyik irányt bebizonyítani, mert „az állítás szimmetrikus". Ha már bebizonyítottuk a G p. ⇒ $\overline{G}$ p. irányt, akkor $H := \overline{G}$ jelöléssel a $\overline{G}$ p. ⇒ G p. átírható $\underbrace{H}_{\overline{G}}$ p. ⇒ $\underbrace{\overline{H}}_{\overline{\overline{G}} = G}$ p. alakra. ✓

biz.: (e.p.g.t. segítségével)

Ha G perfekt ⇒ G nem tartalmaz fesz. részgráfként C_{2k+1} vagy $\overline{C_{2k+1}}$-t

$\Downarrow$

$\overline{G}$ nem tartalmaz fesz. részgráfként $\overline{C_{2k+1}}$ vagy C_{2k+1}-t ⇒ $\overline{G}$ perfekt. ✓



<u>DEF.:</u> $I_1, I_2, \dots, I_k$ a számegyenes korl. és zárt intervallumai
$V(G) := \{I_1, I_2, \dots, I_k\}$
I_i szomszédos I_j-vel $\Longleftrightarrow$ ezek metszők (és $i \neq j$)
} G <u>intervallumgráf</u>

<u>TÉTEL:</u> $\forall$ intervallumgráf perfekt

<u>Biz.:</u> Mivel az int. gráfok feszített részgráfjai is int. gráfok, elég azt belátni, hogy $\chi = \omega$

Legyen $\omega(G) = k$, mivel $\omega(G) \leq \chi(G)$, ezért elég azt belátni, hogy $\chi(G) \leq k$.

Kezdjük el színezni az intervallumokat balról jobbra! A még színezetlen intervallumok közül mindig azt színezzük ki, amelyiknek baloldali végpontja a legbalrább van. Ha egy intervallumot $k+1$-edik színnel kellene színezni, akkor ez azt jelenti, hogy ennek az intervallumnak a bal vége benne van már k intervallumban, amik már elhasználták az $1, 2, \dots, k$ színt. Így van $k+1$ intervallum, melyek közül bármely 2 metszi egymást $\Longrightarrow$ $\exists$ G-ben $k+1$ méretű klikk. ↯

6. TÉTEL

Aciklikus irányított gráfok, PERT módszer.

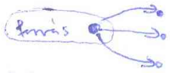
DEF.: $\vec{G} = (V, \vec{E})$ irányított gráf

ahol $\vec{E}$ az irányított élek végpontjai rendezett párjainak halmaza.

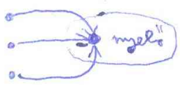
Az $e=(u,v)$ élről azt mondjuk, hogy u-ból v-be megy, v az u közvetlen leszármazottja/gyereke, u a v közvetlen őse/szülője.

DEF.: irányított kör: olyan kör, aminek élei azonos irányítottságúak. Pl.: 

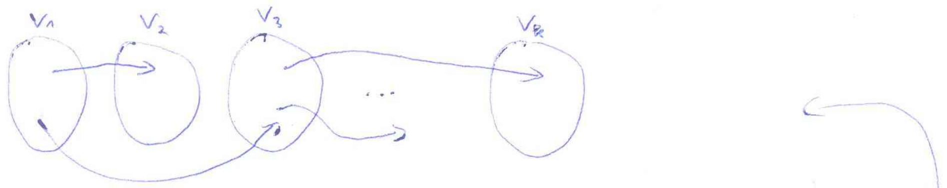
forrás: olyan pont, aminek nincs őse



nyelő: olyan pont, aminek nincs leszármazottja



DEF.: $\vec{G}$ emeletekre bontható, ha $V(\vec{G})$ felvágható $V_1, V_2, \dots, V_k$ diszjunkt részekre úgy, hogy bármely $\overset{x}{\bullet} \to \overset{y}{\bullet}$ $\vec{G}$-beli élre, ha $x \in V_i$ és $y \in V_j \implies i<j$



TÉTEL: $\vec{G}$ em. bontható $\iff$ nem tartalmaz kört (aciklikus)

biz.: szükségesség $\Longrightarrow$: Ha $\vec{G}$ tartalmazna kört, akkor az emeletekre bontott ábrázolásban kellene legyen balra mutató él. ↯

elégségesség $\Longleftarrow$: Lemma: $\vec{G}$ aciklikus $\implies$ van benne nyelő

biz.: $v \in V(\vec{G})$ tetsz., v-ből séta az élek mentén. Mivel aciklikus $\implies$ valahol a séta elakad (véges sok csúcs miatt)

↳ ez nyelő ✓

V_k legyen a $\vec{G}$-beli nyelők halmaza; V_k csúcsait töröljük!

V_{k-1} legyen a maradékban a nyelők halmaza; V_{k-1} csúcsait is töröljük!

⋮

↳ ez valóban egy megfelelő emeletekre bontás. ✓

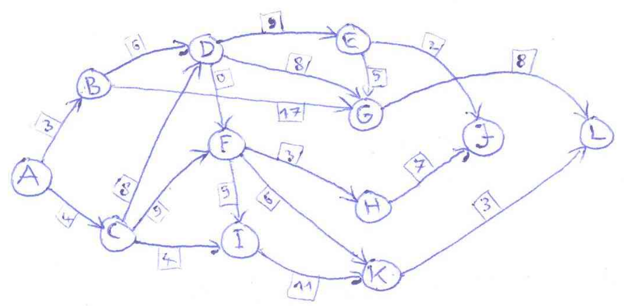
Az előzőleg látott emeletekre bontás fontos alkalmazása az ún. PERT-módszer (Program Evaluation and Review Technique).

Tfh. egy összetett feladatot több alvállalkozóval kell elvégeztetni. Az egyes részfeladatok nem végezhetők el egymástól függetlenül: pl. egy házépítés során a kőművesmunkák nyilván megelőzik a festési munkákat. A helyzetet egy G gráffal szemléltethetjük, melynek pontjai a részfeladatok, és egy l hosszúságú (x, y) irányított él azt jelenti, hogy az y feladatot az x kezdése után l idővel lehet legkorábban elkezdeni. Egy ilyen gráf nem tartalmazhat irányított kört!

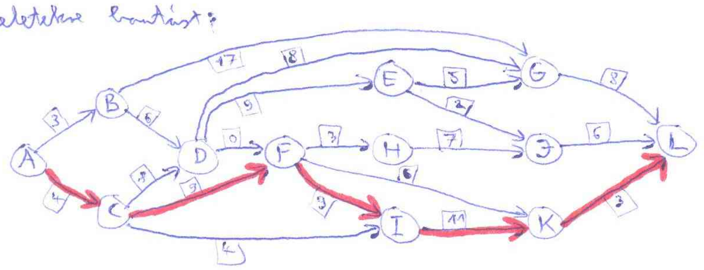
Az egyszerűség kedvéért feltesszük, hogy G egy forrást és egy nyelőt tartalmaz.

A PERT-módszer bemutatása egy konkrét példán:

adott egy gráf:



elvégezzük az emeletekre bontást:



A feladatok elkezdhetőségi idejének meghatározása stratégiailag:

- $A \to \underline{0}$
- $B \to \underline{3}$, $C \to \underline{4}$
- $D \to \max(3+6, \underline{4+8}) = 12$
- $F \to \max(\underline{9+4}, 12+0) = 13$
- $E \to \underline{12+9} = 21$, $H \to \underline{13+3} = 16$, $I \to \max(\underline{9+13}, 4+4) = 22$
- $G \to \max(17+3, 8+12, \underline{5+21}) = 26$, $J \to \max(\underline{21+2}, \underline{16+7}) = 23$, $K \to \max(13+6, \underline{22+11}) = 33$
- $L \to \max(26+8, 23+6, \underline{33+3}) = \underline{\underline{36}}$

Általánosan: a legelső tevékenység azonnal elkezdhető ($A \to \underline{0}$). Később egy J tevékenységhez tekintsük annak összes $x_1, x_2, \dots$ ősét, amik legkorábban $t_1, t_2, \dots$ időpontban kezdhetők el. Ekkor az J elkezdésére legkorábban $\max(t_1 + l(x_1, J), t_2 + l(x_2, J), \dots)$ időpontban kerülhet sor.

Végül érdemes megjelölni L-ből visszafelé azokat az éleket, melyeken a kulcs maximumok felvétetnek, ezek a gráf kritikus élei. Az ezek által meghatározott részgráf mindig tartalmaz legalább egy utat a kezdőből a végsőbe, az ilyet kritikus útnak nevezzük.

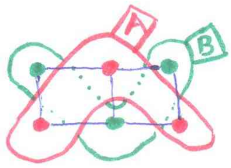
A kritikus utakon lévő pontok (nekik megfelelő részfeladatok) késése az egész projektet késlelteti. De ha egy pont nincs a kritikus úton, akkor megengedett valamekkora késés. Például a J-t legkorábban a 23. időegységben kezdhetjük el, és 7 egységnyi késedelem még nem baj, mert 23+7+6=36.

7. TÉTEL

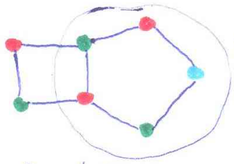
Páros gráfok. Párosítások páros gráfban, König tétele, Hall tétele, Frobenius tétele. Magyar módszer.

DEF.: G páros gráf, ha $V(G)$ felbontható két diszjunkt A és B részre úgy, hogy G $\forall$ éle A-beli csúcsot köt össze B-belivel. Jele: $G(A, B; E)$

Példa:



Ellenpélda:



$\Rightarrow$ nem páros!

TÉTEL: G páros $\Longleftrightarrow$ nincs benne ptl. hosszú kör

biz.: $\Rightarrow$: Ha G ps. gráf és C egy kör G-ben, akkor C pontjai felváltva vannak A-ban és B-ben.

$\Leftarrow$: Ha G $\forall$ köre ps. hosszú, akkor megadhatjuk az A és B halmazt: választunk egy tetsz. $v \in V(G)$ pontot, legyen ez A első pontja, majd v $\forall$ szomszédját tegyük B-be, majd $\forall$ addig B-ben levő pont $\forall$ szomszédját tegyük A-ba stb. Ezt addig végezzük, míg $\forall$ pontot el nem helyeztünk. Ez biztosan jó elosztás, hiszen ha lenne pl. A-ban két szomsz. pont, akkor lenne ptl. kör is. ↯

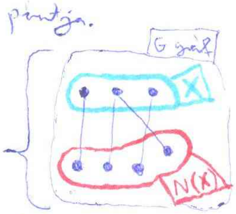
Ha a gráf nem öf., akkor az eljárást komponensenként hajtjuk végre.

DEF.: Párosításnak nevezünk egy M élhalmazt, ha semelyik két élnek nincs közös pontja.

Az ilyen éleket független éleknek is nevezzük.

Teljes párosítás: olyan párosítás, ami a gráf $\forall$ pontját lefedi.

DEF.: egy G gráfban $N(X)$ jelöli az $X \subseteq V$ ponthalmaz szomszédainak halmazát.



$\nu(G)$: független élek maximális száma.

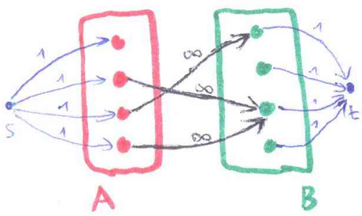
$X \subseteq V(G)$ lefogó ponthalmaz, ha G $\forall$ élének legalább egyik végpontját tartalmazza.

$\tau(G)$: lefogó pontok minimális száma.

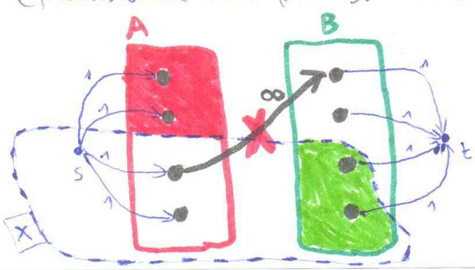
TÉTEL: (König) Ha $G = (A, B; E)$ véges ps. gráf $\Rightarrow \nu(G) = \tau(G)$

biz.: Állítás: G véges gráf $\Rightarrow \nu(G) \le \tau(G)$

biz.: Legyen M G-nek egy max. párosítása. Ha U egy min. méretű lefogó ponthalmaz, akkor lefogja M $\forall$ élét is, de U $\forall$ pontja max. egy párosításélt fog le $\Rightarrow |M| = \nu(G) \le \tau(G) = |U|$.



Készítsük el G'-t az alábbiak szerint. Irányítsuk G $\forall$ élét A-ból B-be, vegyünk fel egy új s és t pontot, vezessünk s-ből élt A $\forall$ pontjába, és vegyünk fel egy-egy élt B $\forall$ pontjából t-be. Adjunk $\forall$ élnek kapacitásokat: az s-ből induló, ill. t-be érkezők legyen 1, az A-ból B-be futóké pedig ∞ (pontosabban $|A|+1$). Tekintsük a (G', s, t, c) hálózatot, ahol c előbb definiált kapacitást jelenti. Ha G-ben $\exists$ k méretű párosítás $\Rightarrow \exists$ k nagyságú egészfolyam. Tehát a max. egészfolyam értéke $\nu(G)$, és az egészértékűségi lemma miatt a max. folyamérték is ugyanennyi. A Ford-Fulkerson tétel szerint $\exists$ $\nu(G)$ kapacitású vágás, definiálja ezt az s-t tartalmazó X. G'-nek nem futhat éle $X \cap A$-ból $B \setminus X$-be, mert akkor a vágás ∞ kapacitású volna (pontosabban min. $|A|+1$). Tehát $(A \setminus X) \cup (B \cap X)$ egy lefogó ponthalmaz: $\tau(G) \le \underbrace{|A \setminus X| + |B \cap X|}_{\nu(G)}$



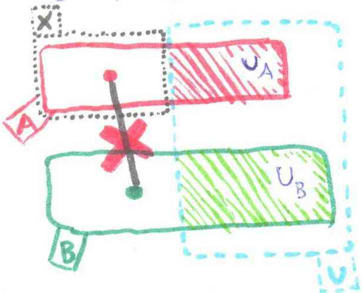
Tehát: $\nu(G) \le \tau(G)$
$\tau(G) \le \nu(G)$ $\Rightarrow \nu(G) = \tau(G)$

✓

TÉTEL: (Hall) $G=(A,B;E)$ véges ps. gráf, $\exists$ A-t fedő párosítás $\Longleftrightarrow$ $\underbrace{\forall X \subseteq A\text{-ra } |X| \leq |N(X)|}_{\text{Hall-feltétel}}$

biz.: $\Rightarrow$: A szükségesség nyilvánvaló: ha $\exists$ A-t fedő párosítás, akkor $\forall$ A-beli pontnak különböző párja van (tehát tetsz. $X \subseteq A$ esetén az X-beli elemek B-beli párjai az $N(X)$ egy $|X|$ méretű részhalmazát alkotják)

$\Leftarrow$: Tudjuk, hogy $\forall X \subseteq A$-ra $|X| \leq |N(X)|$. Azt kell igazolni, hogy $\nu(G) \geq |A|$. Legyen U minimális lefogó ponthalmaz, tehát $\tau(G)$ méretű, és $U_A := U \cap A$, $U_B := U \cap B$.



Mivel U lefogja az $X := A \setminus U_A$-ból induló éleket $\Rightarrow$ $N(X) \subseteq U_B$, azaz $|N(X)| \leq |U_B|$. Felhasználva a Kőnig-tételt adódik:

$$\nu(G) = \tau(G) = |U| = |U_A| + |U_B| \geq |U_A| + |N(X)| \geq |U_A| + |X| = |A| \checkmark$$

TÉTEL: (Frobenius) $G=(A,B;E)$ véges ps. gráf, $\exists$ teljes párosítás $\Longleftrightarrow$ $|A|=|B|$ és $\forall X \subseteq A$-ra $|X| \leq |N(X)|$

biz.: $\Rightarrow$: nyilvánvaló

$\Leftarrow$: teljesül a Hall-feltétel $\Rightarrow$ $\exists$ F-t fedő párosítás, de $|A|=|B|$ $\Rightarrow$ ez TP $\checkmark$

DEF.: $G(A,B;E)$ ps. gráf, M párosítás

alternáló út: párosítatlan A-beliből indul és $\forall$ második éle M-beli

javító út: olyan alternáló út, ami párosítatlan B-beliben ér véget

Magyar módszer (hatékony algoritmus max. élszámú párosítás megtalálására):

(I) független élek felvétele, amíg lehet.

(II) javító út keresése és emenén a párosítás növelése, amíg lehet.

Pl.

A módszer általános megfogalmazása: tfh. már van egy M párosításunk, ami lefedi az $X \subset A$ halmazt, de még van olyan $A-X$-beli pont, amit nem. X' jelölje X elemeinek M-beli párjait! Ha v-nek van szomszédja $B-X'$-ben, akkor egy élet hozzávehetünk M-hez, erről szólt az (I) lépés. Ha v-nek $\forall$ szomszédja X'-ben van, és van egy P-vel jelölt javító út, ami tehát $A-X$-beliből indul, $B-X'$-beli pontban végződik és $\forall$ második éle M-beli, akkor növelhetjük a párosítást: $M' := M \Delta P$ vagyis M-ből elhagyjuk a P-ben szereplő éleket és hozzávesszük a többi P-beli élet.

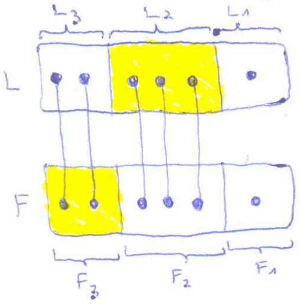
$\uparrow$ szimmetrikus differencia

(III) ha nincs javító út $\Rightarrow$ STOP

TÉTEL: $G(F,L;E)$, M párosítás, Ha nincs javító út $\Rightarrow$ M max. párosítás

biz.: tfh. az algoritmus k élű párosítást adott

cél: k pontú lefogó ponthalmazt találni! Mert ha találunk, akkor teljesül ez: $k \leq \nu(G) \leq \tau(G) \leq k$ $\Rightarrow$ $k = \nu(G)$ $\checkmark$



F_1: párosítatlan F-beliek, L_1: párosítatlan L-beliek

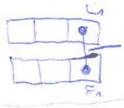
L_2: azon L-beliek, amikhez F_1-ből alt. úton el lehet jutni (ekkor $L_1 \cap L_2 = \emptyset$ mert javító út $\nexists$)

F_2: L_2-beliek párjai M szerint; L_3, F_3: maradék L/F-beliek

Állítás: $F_1 \cup F_2$-ből nem vezet él $L_1 \cup L_3$-ba

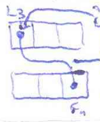
biz.: indirekt tfh.:

1. $\exists F_1L_1$ él:



1 élű jav. út lenne ↯

2. $\exists F_1L_3$ él:

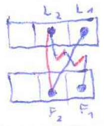


mert ez lefogja van! L_2-ben kéne lennie

1 élű alt. út

↯

3. $\exists F_2L_1$ él:

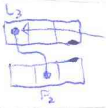


F_2: L_2 lágyak párjai, L_2 = amelyik párosítatlan F_1-ből elérhető alt. úton

$\Downarrow$

L_1 elérhető lenne F_1-ből jav. úton ↯

4. $\exists F_2L_3$ él:



ez mert lefogja van!

L_2-ben kéne lennie... ↯

$\Leftarrow$ $L_2 \cup F_3$ lefogó pont-halmaz és ez k méretű! $\checkmark$

Még egy kérdés: hogyan keressünk javító utat? Induljunk ki egy A-beli, M által le nem fedett v pontból és mintha szélességi keresést végeznénk, menjünk el ennek összes szomszédjába, amiket $b_1, \ldots, b_d$ jelöljön. Ezek nyilván mind B-beli pontok és mindet lefedi M. Mivel M lefedi a $b_1, \ldots, b_d$ pontokat, jelölje $a_1, \ldots, a_d$ ezek M által meghatározott párját. Most $\forall$ $a_1, \ldots, a_d$ pontból kiinduló, nem M-beli élen elérhető pontjába menjünk el. Látható, hogy ezek éppen azok a pontok, amelyekbe vezet v-ből 3 élből álló alt. út. Lényegében BFS-t alkalmazunk.

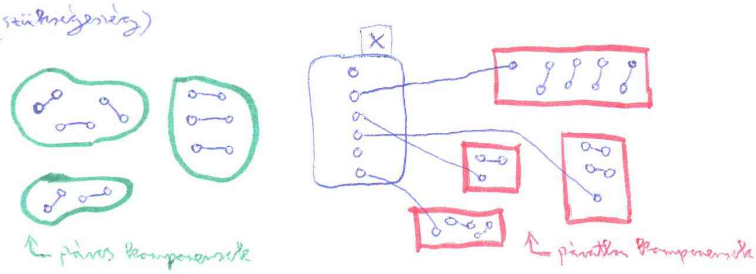
8. TÉTEL

Párosítások tetszőleges gráfban, Tutte tétele (csak a szükségesség bizonyításával). Gallai tételei.

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

TÉTEL: (Tutte) G-ben $\exists$ TP $\iff \forall X \subseteq V(G)$-re $c_p(\underbrace{G-X}_{\text{G-ből X-beli csúcsok elhagyása}}) \leq |X|$

biz.: (szükségesség)



Ha elhagyjuk a gráfból X-et, akkor az eredeti gráfban a páratlan komponensek mindegyikéből legalább egy párosításbeli él indul ki, és ezek az élek csak egy-egy különböző X-beli pontba mehetnek, tehát $c_p(G-X) \leq |X|$. ✓

DEF.:
- független élhalmaz: olyan élhalmaz, hogy semelyik két élnek nincs közös pontja (vagyis diszjunktak)
- $\nu(G)$: független élek max. száma (G-ben)
- $X \subseteq V(G)$ lefogó ponthalmaz, ha G $\forall$ éle tartalmaz X-beli csúcsot
- $\tau(G)$: lefogó pontok min. száma
- $X \subseteq V(G)$ független ponthalmaz, ha az X-beli csúcsok nem szomszédosak
- $\alpha(G)$: fgtl. pontok max. száma
- $Y \subseteq E(G)$ lefogó élhalmaz, ha G $\forall$ pontjára illeszkedik Y-beli él
- $\rho(G)$: lefogó élek min. száma

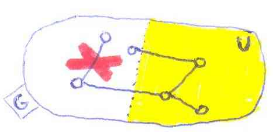
	f.-len max.	lef. min.
élek	NŰ ν	RÓ ρ
pontok	ALFA α	TAÚ τ

TÉTEL: (Gallai) G tetsz., n csúcsú

(1) $\alpha(G) + \tau(G) = n$ ha G hurokélmentes

(2) $\nu(G) + \rho(G) = n$ ha G-ben $\nexists$ izolált pont

biz.: (1)



Könnyen látható, hogy $U \subseteq V(G)$ pontosan akkor lefogó ponthalmaz, ha $V(G) \setminus U$ független ponthalmaz. Az állítás innen közvetlenül adódik.

(2) G-nek $\exists$ $\nu(G)$ diszjunkt éle, ezek $2\nu(G)$ pontot fognak le. A maradék $n - 2\nu(G)$ pont mindegyike lefogható egy-egy új éllel (mert nincs izolált pont) $\Rightarrow \nu(G) + n - 2\nu(G) = n - \nu(G)$ éllel $\forall$ pont lefogható $\Rightarrow \rho(G) \leq n - \nu(G) \Rightarrow \nu(G) + \rho(G) \leq n$.

Ha F egy min. méretű lefogó élhalmaz, akkor F körmentes és nem tartalmaz 3 hosszú utat sem, tehát F diszjunkt csillagok uniója. (A csillag olyan öf. gráf, melynek legfeljebb egy kivételével $\forall$ pontfoka 1.) Ha a min. lef. élhalmazban k csillag van, akkor a halmaz $n-k$ élt tartalmaz hiszen k komponensű erdőről van szó: $\rho(G) = n - k$. Másrészt a halmaz tartalmaz k diszjunkt élt: $k \leq \nu(G)$ ehhez hozzáadjuk az előző egyenlőséget $n - \cancel{k} + \cancel{k} \leq \nu(G) + \rho(G)$.

Tehát: $n \leq \nu(G) + \rho(G) \leq n \Rightarrow \nu(G) + \rho(G) = n$. ✓

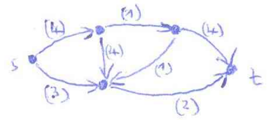
9. TÉTEL

Hálózati folyamok. Ford – Fulkerson tétel, Edmonds – Karp tétel (biz. nélkül). Egészértékűségi lemma. A folyamprobléma általánosításai.

DEF.: Hálózatnak nevezzük egy olyan $(\vec{G}, s, t, c)$ négyest, amelyben $\vec{G}$ egy irányított gráf, aminek s és t különböző csúcsai, továbbá $\vec{G}$ minden e élét jellemzi egy nemnegatív $c(e)$ szám, az e él kapacitása.

Röviden: ha $\vec{G}$ ir. gráf, $s, t \in V(\vec{G})$, $c: E(\vec{G}) \to \mathbb{R}^+$

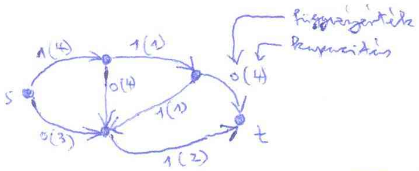
Példa:



DEF.: f folyam egy $f: E \to \mathbb{R}^+$ fv., amire: (1) $\forall e \in E(\vec{G})$-re $0 \le f(e) \le c(e)$

(2) $\forall v \in V(\vec{G})$, $v \ne s, t$-re $\sum_{v\vec{e}} f(e) = \sum_{\vec{e}v} f(e)$

Példa:



DEF.: f folyam értéke: $m_f = \sum_{s\vec{e}} f(e) - \sum_{\vec{e}s} f(e) = \sum_{\vec{e}t} f(e) - \sum_{t\vec{e}} f(e)$

A folyam értékének meghatározása az s, ill. t-n kívül:

$X \subseteq V(\vec{G})$, $s \in X \not\ni t$, $m_f = \sum_{X\vec{e}} f(e) - \sum_{\vec{e}X} f(e)$

DEF.: $X \subseteq V(\vec{G})$, $s \in X \not\ni t$

X és $V(\vec{G}) \setminus X$ között menő élek halmazát st-vágásnak nevezzük, jele: C értéke: $c(C) = \sum_{X\vec{e}} c(e)$

Állítás: Ha egy hálózatban f folyam, C vágás $\Longrightarrow$ $\underbrace{f \text{ értéke}}_{m_f} \le \underbrace{C \text{ vágás értéke}}_{c(C)}$

A feladat tehát a maximális értékű folyam meghatározása.

Algoritmus: I. kiindulunk egy tetsz. folyamból (pl. $f \equiv 0$)

II. javítás $\Longrightarrow$ m_f nő

III. ha nincs több javítás $\Longrightarrow$ STOP

A javítást egy ún. segédgráffal tudjuk elvégezni:

DEF.: a $(\vec{G}, s, t, c)$ hálózat f folyamához tartozó $\vec{H}_f$ segédgráf:

$V(\vec{H}_f) = V(\vec{G})$

(1) $\left.\begin{array}{l} \vec{xy} \in E(\vec{G}) \\ f(\vec{xy}) < c(\vec{xy}) \end{array}\right\} \Longrightarrow \vec{xy} \in \vec{H}_f$ (2) $\left.\begin{array}{l} \vec{xy} \in E(\vec{G}) \\ 0 < f(\vec{xy}) \end{array}\right\} \Longrightarrow \vec{yx} \in H_f$

javítóút: $\vec{H}_f$-ben irányított út s-ből t-be

Ha $\exists P$ javítóút, akkor növelhetjük a folyam értékét:

$d := \min\left(\{c(e) - f(e) : e \in P,\ e \text{ (1)-es}\} \cup \{f(e) : e \in P,\ e \text{ (2)-es}\}\right)$ $f(e) := \begin{cases} f(e) + d & \text{ha } e \in P,\ e \text{ (1)-es} \\ f(e) - d & \text{ha } e \in P,\ e \text{ (2)-es} \\ f(e) & \text{ha } e \notin P \end{cases}$

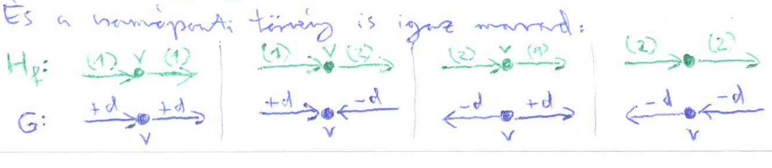
Fontos kiegészítés:

Ha van egy olyan irányított út s-ből t-be, amelynek $\forall$ éle telítetlen (vagyis $f(e) < c(e)$ $\forall e \in P$), akkor ezen út mentén a folyam értékét $\forall$ élen megnövelhetjük annyival, hogy az egyik él telített legyen. Ha nincs erre lehetőség, akkor ezután alkalmazzuk a segédgráfos módszert.

Állítás: a segédgráfos javítás után f folyam marad

biz.: Az biztos, hogy egyik élet sem „terheltük túl", mert d direkt így lett megválasztva a minimumfüggvényes előállítása által.

És a csomóponti törvény is igaz marad:

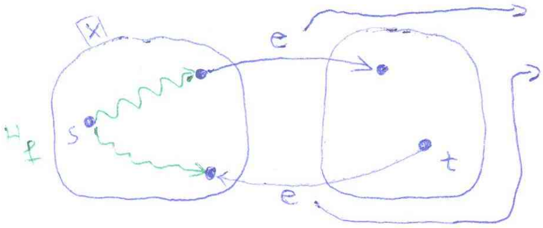


TÉTEL: Ha nincs javítóút H_f-ben $\iff$ f maximális folyam

biz.: tfh. az algoritmus t értékű folyamot adott: $m_f = t$

cél: mutassunk t értékű vágást

$X :=$ azon pontok halmaza, ahová H_f-ben s-ből vezet ir. út $\implies s \in X \not\ni t$



$f(e) = c(e)$ mert különben $\xleftarrow{e} \in H_f$ ↯

$f(e) = 0$ mert különben $\xrightarrow{e} \in H_f$ ↯

$\Downarrow$

$$m_f = \sum_{\underset{X}{\rightarrow}} f(e) - \sum_{\underset{X}{\leftarrow}} f(e) = \sum_{\underset{X}{\rightarrow}} c(e) - \sum_{\underset{X}{\leftarrow}} 0 = c(C) = t \checkmark$$

TÉTEL: (Ford-Fulkerson) $\max\limits_{f \text{ folyam}} m_f = \min\limits_{C \text{ vágás}} c(C)$ vagyis a maximális folyam értéke egyenlő a minimális vágás értékével.

biz.: A maximális folyam nyilván nem lehet nagyobb a minimális vágásnál, hiszen ha $\forall$ előremutató él telített, a visszafelé mutatókon pedig 0 a folyam értéke, akkor ezen a vágáson nem folyhat át több. Az előző tételben pedig láttuk, hogy ha létezik egy f maximális folyam, akkor van ilyen értékű vágás. ✓

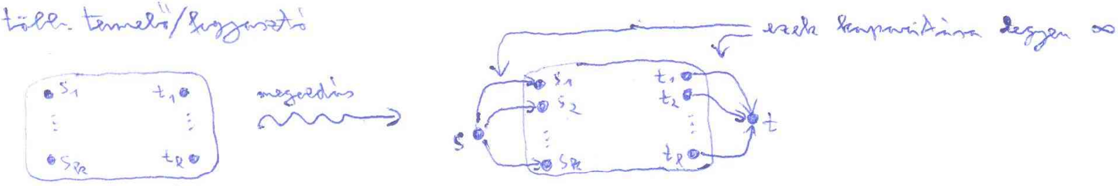
TÉTEL: (Edmonds-Karp) Ha H_f-ben mindig a legrövidebb utat választjuk, akkor az algoritmus véges sok lépésben leáll és polinomiális lépésszámú.

Egészértékűségi lemma: Ha $\forall e$ élre $c(e)$ egész $\implies \exists$ olyan f max. folyam, amire $\forall e$ élre $f(e)$ egész

biz.: az algoritmus nem lép ki $\mathbb{N}$-ből (csupa 0-ból indítva).

A folyamprobléma általánosításai:

(1) több termelő/fogyasztó



(2) irányítatlan élek

(3) kapacitással rendelkező csúcsok

10. TÉTEL

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

DEF.: a G gráf u pontjából v pontjába futó P és Q útjait éldiszjunktaknak / pontdiszjunktaknak nevezzük, ha $E(P) \cap E(Q) = \emptyset$ / $V(P) \cap V(Q) = \{u, v\}$.

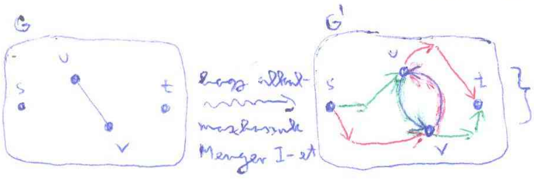
DEF.: G gráf U élhalmaza/ponthalmaza lefog $\forall$ uv utat, ha $G - U$-ban $\nexists$ u-ból v-be út.

TÉTEL: (Menger I.) Az s-ből t-be menő páronként éld. ir. utak max. száma = az st utakat lefogó élek min. számával

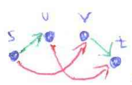
biz.: Ha $\exists$ G-ben k db ilyen ir. st út, akkor az st utakat lefogó élek száma nyilvánvalóan legalább k, tehát $\max\{\} \leq \min\{\}$. Tfh. k az st utakat lef. élek min. száma. Legyen $\forall$ él kapacitása 1. Az így kapott hálózatban a min. vágás értéke legalább k $\xRightarrow{F-F}$ a max. folyam is legalább k értékű. Van olyan max. folyam, melyben $\forall$ élen a folyamérték 0 vagy 1 (egészértékűségi lemma miatt). Lássuk be, hogy G-ben $\exists$ k éld. ir. st út! Egy ilyen út mindenképpen van, hiszen különben nem lehetne k a folyam értéke. Az ebben az útban szereplő élek kapacitását változtassuk 0-ra, így a folyamérték $k-1$ lesz. Ekkor viszont ismét kell lennie st útnak, és ennek nyilván nincs közös éle az előbbi úttal. Ezt k-szor végrehajtva k éld. ir. st utat kapunk. ✓

TÉTEL: (Menger II.) G irtl. gráf, $s, t \in V(G)$. Az s-ből t-be páronként éld. irtl. utak max. száma egyenlő az st utakat lefogó élek min. számával.

biz.: Készítsük el $\vec{G}$-t G-ből úgy, hogy G $\forall$ élét megirányítjuk oda és vissza.



előfordulhat ilyen probléma... $\xrightarrow{\text{megoldás}}$

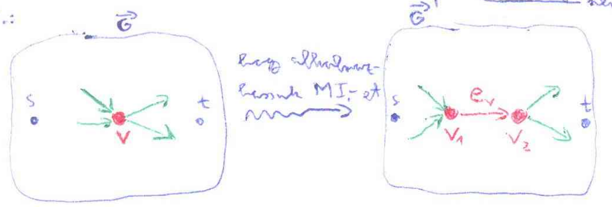


Az összes ilyen megszüntetése után az utak őseképei adnak G-ben k db st páronként éld. irtl. utat. ✓

Ha $\vec{G}$-ben van k db él, amik lefogják k db st ir. éld. utat $\longrightarrow$ ezeknek ősei lefogják az st utakat G-ben ✓

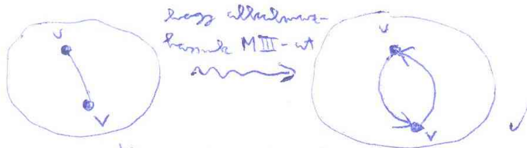
TÉTEL: (Menger III./IV.) G ir./irtl., $s, t \in V(G)$ Az st páronként pontdiszjunkt ir./irtl. utak max. száma = az st utakat (s és t használata nélkül) lefogó pontok min. számával.
(s és t: nem lehetnek szomszédosak!)

biz.: MIII.:



Ha $\vec{G}'$-ben van k éld. st út $\Rightarrow$ $\vec{G}$-ben van k db pontd. út.
Probléma: ha $\vec{G}'$-ben van k db él, amik lefogják az st utakat, akkor ezek $\vec{G}$-ben pontok vagy élek? Megoldás: válasszuk k db piros lefogó élt! $\Rightarrow$ ezeknek képei $\vec{G}$-ben k db lef. pont ✓

MIV.:



✓

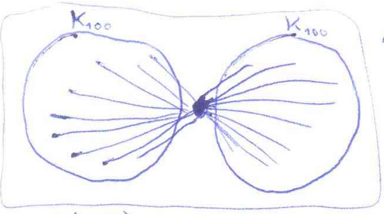
DEF.: G **k-szorosan élösszefüggő**, ha bárhogyan legfeljebb $k-1$ élét elhagyva öf. marad.
G **k-szorosan pontösszefüggő**, ha — " — " — pontot — " — " — és legalább $k+1$ pontja van.

Nyilván: k élöf. $\Rightarrow$ $k-1$ élöf., k öf. $\Rightarrow$ $k-1$ öf.

Ha külön nem emeljük ki, hogy pont- vagy élösszefüggőségről beszélünk, akkor az alapértelmezett a pontöf.!

Állítás: k öf. $\Rightarrow$ k élöf.
$\not\Leftarrow$

Ellenpélda:



$\leftarrow$ nem 2 öf., de 100 élöf.

TÉTEL: (Menger V, VI)

MV: G k-élöf. $\Leftrightarrow$ Bármely 2 pont között $\exists$ k db páronként éld. út

MVI: G k-öf. $\Leftrightarrow$ Bármely 2 pont között $\exists$ k db páronként pontd. út és $\geq k+1$ pontja van

biz.: $\overset{V,VI}{\Leftarrow}$: $k-1$ él/pont elhagyásakor tetszőleges s-ből t-be van út, mert volt k db éld./pontd. út, $k-1$ törlése csak $k-1$-et ronthatott el.

$\overset{V}{\Rightarrow}$: Tfh. s,t között nincs k db éld. út $\Rightarrow$ st éld. intl. utak max. száma $\leq k-1$ $\Rightarrow$ st utakat lefogó élek min. száma $\leq k-1$ $\Rightarrow$ le lehet fogni $\leq k-1$ éllel az st utakat $\Rightarrow$ $k-1$ élet törölve nincs st út! $\lightning$

$\overset{VI}{\Rightarrow}$: Tfh. s-ből t-be legfeljebb $k-1$ pontd. út van.

Ha st nem szomszédos, akkor Menger 4. tétele miatt az st utak lefoghatók max. $k-1$ ponttal. Ezek elhagyásakor G szétesne. $\lightning$

Ha st szomszédos, akkor az st él törlése után keletkező G gráf legfeljebb $k-2$ pontd. st utat tartalmaz, tehát Menger 4. tétele szerint létezik $k-2$ pontja, aminek elhagyásakor szétesik. A szétesett gráfban ismét összekötve az s és t pontokat egy legalább 3-pontú gráfot kapunk (mert G-nek min. $k+1$ pontja volt), mely az st él törlésétől szétesik. De akkor az st él helyett s vagy t valamelyike is törölhető, hogy a gráf szétessen.

Ismét azt kaptuk, hogy G legfeljebb $k-1$ alkalmas pont törlésével szétesik, ami a k-szoros összefüggőségnek ellentmond. $\lightning$

TÉTEL: (Dirac) Ha G k-öf. és $2 \leq k$ $\Rightarrow$ G bármely k pontján keresztül található kör G-ben

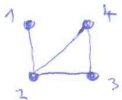
11. TÉTEL

Gráfok és mátrixok. Szomszédossági mátrix (hatványainak jelentése, reguláris gráf esetén egy sajátértéke). Illeszkedési mátrix, annak rangja.

DEF.: A $G=(V,E)$ irányított gráf szomszédossági mátrixa $A(G)=(a)_{i,j}\in\mathbb{R}^{V\times V}$, ahol $a_{i,j}$ legyen az i-ből j-be futó élek száma.

Megjegyzés: G v_i pontjának ki/befoka a mátrix i-edik sorában/oszlopában levő elemek összege.
Ha G irányítatlan, akkor A szimmetrikus a főátlóra: $A=A^T$.

Példa:



$$A=\begin{pmatrix}0&1&0&0\\1&0&1&1\\0&1&0&1\\0&1&1&0\end{pmatrix}$$

TÉTEL: Ha $G=(V,E)$ ir. gráf, akkor az A^k mx. (i,j) pozíciójában álló $(A^k)_i^j$ elem az i-ből j-be vezető k élű séták száma.

biz.: teljes indukcióval: $k=1$-re A definíciójából nyilvánvaló. Tfh. A^k-ra már bizonyítottuk az állítást.
Az i-ből j-be vezető k+1 élű séták száma: $\sum_{w\in V}(\text{k élű iw séták száma})\cdot(\text{wj élek száma}) = \underbrace{\sum_{w\in V}(A^k)_i^w\cdot(A)_w^j}_{\text{indukciós feltevésből}} = \underbrace{(A^{k+1})_i^j}_{\text{mx. szorzás}}$

Következmény: • Ha G egyszerű irtl. gráf $\Longrightarrow (A^2)_v^v = d(v)\quad \forall v\in V(G)$.
• A hurokélmentes gráfoknál A^3 főátlóbeli elemeinek összege a gráfban található 3 hosszú körök számának 6-szorosa.

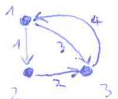
TÉTEL: Ha G irtl. gráf és λ_1 az A legnagyobb sajátértéke, akkor $\lambda_1\le\Delta$, egyenlőség reguláris gráfokra van.

biz.: Legyen $\underline{x}=(x_1,\dots,x_n)$ egy λ_1-hez tartozó sv., és k-adik eleme a legnagyobb. Mivel $\underline{x}\neq\underline{0}$, ezért (esetleg a $-\underline{x}$ sv.-ra áttérve) feltehető, hogy x_k pozitív.
Ekkor: $\lambda_1\cdot x_k=(A)_k\cdot\underline{x}=\sum_{i=1}^n a_{k,i}\cdot x_i\le\sum_{i=1}^n a_{k,i}\cdot x_k = x_k\cdot\sum_{i=1}^n a_{k,i} = x_k\cdot d(v_k)\le x_k\cdot\Delta \Longrightarrow \lambda_1\le\Delta$ ✓
Ha G Δ-reguláris, akkor az egységvektor a Δ sé.-hez tartozó sv., mert a fenti egyenlőtlenségek egyenlőséggel teljesülnek. ✓

DEF.: A $G=(V,E)$ ir. gráf illeszkedési mátrixa $B(G)\in\mathbb{R}^{V\times E}$, amire: $(B)_v^e=\begin{cases}1 & \text{ha } v \text{ az } e \text{ kezdőpontja: } \overset{v}{\bullet}\xrightarrow{e}\\ -1 & \text{ha } v \text{ az } e \text{ végpontja: } \overset{v}{\bullet}\xleftarrow{e}\\ 0 & \text{egyébként}\end{cases}$

/ ha G irtl., akkor $(B)_v^e=\begin{cases}1 & \text{ha } v \text{ az } e \text{ végpontja}\\ 0 & \text{egyébként}\end{cases}$

Példa:



$$B=\begin{pmatrix}1&0&1&-1\\-1&1&0&0\\0&-1&-1&1\end{pmatrix}$$

TÉTEL: A G n pontú irányított hurokélmentes c komponensű gráfnál $r(B)=n-c$.

biz.: Ha $1<c$, akkor komponensenként sorolva fel a pontokat és éleket, B blokkdiagonális szerkezetű lesz. Elég tehát egy p pontú komponensre belátni, hogy a neki megfelelő blokk rangja $p-1$. Mivel a blokk p sorából áll és összege a $\underline{0}$-t adja, a rang $\le p-1$. Legyen F egy p pontú, $p-1$ élű feszítőfa ebben a komponensben.

egy példa a blokkdiagonális szerkezetű mátrixra: $\begin{pmatrix}7&9&0&0\\4&2&0&0\\0&0&8&6\\0&0&1&1\end{pmatrix}$

Legyen v_1 egy elsőfokú pont F-ben és e_1 a hozzá illeszkedő él.
Legyen v_2 egy elsőfokú pont $F-\{v_1\}$-ben és e_2 a hozzá illeszkedő él, stb.
Ha a blokk sorait $v_1,v_2,\dots$ sorrendben soroljuk fel, oszlopait $e_1,e_2,\dots$ felsorolásával kezdjük, akkor egy $p\times(p-1)$ méretű részmátrixot kapunk, amelyből az utolsó sor elhagyásával egy alsó Δ mátrixot kapunk, melynek főátlóbeli elemei ±1 értékűek $\Longrightarrow$ találtunk $p-1$ lin. ftl. oszlopot.

TÉTEL: Az n pontú öf. hurokélmentes ir. G gráf illeszkedési mátrixában $n-1$ oszlop akkor és csak akkor lin. ftl., ha a megfelelő $n-1$ él G-nek egy fáját alkotja.

biz.: Az előző tételbizonyításnál láttuk, hogyha az élek fát alkotnak, akkor a megfelelő oszlopvektorok lin. ftl.-ek. Megmutatjuk a fordítottját: ha néhány él kört alkot $\Longrightarrow$ nekik megfelelő oszlopvektorok lin. öf.-ek. Ugyanis, ezek az oszlopok és a kört alkotó pontoknak megfelelő sorok alkalmas sor- ill. oszloppermutáció után a baloldali alakú mátrixot alkotják. Képezzük azt a lin. komb.-t, ahol az 1. oszlop eh.-ja a, a 2.-é b, stb. $\Longrightarrow$ összegük $\underline{0}$-t adja ✓

$$\begin{pmatrix}a&0&\cdots&-x\\-a&b&\cdots&0\\0&-b&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&x\end{pmatrix}$$

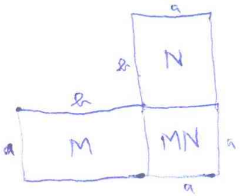
$\leftarrow a,b,\dots,x\in\{-1,+1\}$

DEF.: redukált illeszkedési mátrix: úgy kapjuk, hogy az eredeti ill. mx.-ból elhagyunk egy sort

jele: $B_0(\vec{G})$

TÉTEL: Az n pontú öf. ir. G gráfnál $\det(B_0 \cdot B_0^t) =$ feszítőfák száma

biz.: Felhasználhatjuk a Binet–Cauchy-tételt:



$$\det(MN) = \sum_{\binom{k}{a}\text{-féleképp}} \det M' \cdot \det N'$$

ahol M'-t/N'-t úgy kapjuk, hogy az eredetiből elhagyunk $(k-a)$ oszlopot/sort, hogy $a \times a$ méretű mátrixot kapjunk.

Pl.:
$$\left| \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \begin{pmatrix} g & h \\ i & j \\ k & l \end{pmatrix} \right| = \begin{vmatrix} a & b \\ d & e \end{vmatrix} \cdot \begin{vmatrix} g & h \\ i & j \end{vmatrix} + \begin{vmatrix} a & c \\ d & f \end{vmatrix} \cdot \begin{vmatrix} g & h \\ k & l \end{vmatrix} + \begin{vmatrix} b & c \\ e & f \end{vmatrix} \cdot \begin{vmatrix} i & j \\ k & l \end{vmatrix}$$

Ezek után a tétel állítása nyilvánvaló: B_0-ból mindenképp kiválasztva $n-1$ oszlopot, épp a fáknak megfelelő részmátrixok determinánsa lesz $\neq 0$, és egy ilyen determináns értéke ± 1, tehát a négyzete 1.

Példa: $G = K_n$ n pontú teljes gráf

$$B_0 B_0^t = \begin{pmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ -1 & n-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & n & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & n \end{pmatrix}$$

$$\Downarrow$$

$\det(B_0 B_0^t) = n^{n-2}$ } újabb bizonyítását kapjuk a Cayley tételére ✓

A tétel felhasználásához nem szükséges a B_0 mátrixot felírnunk. A $B_0 B_0^t = (d_{ij})$ elemeit az alábbi képlet is előállítja:

$$d_{ij} = \begin{cases} d(P_i) & \text{ha } i = j \\ -(\text{az } i \text{ és } j \text{ közt vezető élek száma}) & \text{ha } i \neq j \end{cases}$$

12. TÉTEL

Oszthatóság, felbonthatatlan és prímtulajdonságú számok, ezek kapcsolata (bizonyítás csak az egyik irányban), a számelmélet alaptétele. Osztók száma és összege. Nevezetes tételek prímszámokról: prímek száma, hézag a szomszédos prímek között, $\pi(n)$ nagyságrendje (biz. nélkül), prímek számtani sorozatokban (Dirichlet tétele) (biz. nélkül). Kongruencia fogalma, alapműveletek kongruenciákkal.

DEF.: <u>a osztója b-nek</u>, ha $\exists\ c \in \mathbb{Z}$, hogy $a \cdot c = b$. Jele: $a \mid b$

p <u>felbonthatatlan</u> ($|p| \neq 1$), ha $p = a \cdot b \implies |a| = 1$ vagy $|b| = 1$ — $a, b \in \mathbb{Z}$

p <u>prímszám</u>, ha $p \mid a \cdot b \implies p \mid a$ vagy $p \mid b$ — $|p| \neq 1$

<u>Példa:</u> a 6 nem prím, mert $6 \mid \underbrace{8 \cdot 9}_{72}$, de $6 \nmid 8$ és $6 \nmid 9$.

TÉTEL: p prím $\iff$ p felbonthatatlan

biz.: $\implies$: p prím, $p = a \cdot b$

$$p \mid a \cdot b \xrightarrow{p \text{ prím}} \begin{cases} p \mid a \text{ és } a \mid p \implies |a| = |p| \implies |b| = 1 \ \checkmark \\ p \mid b \text{ és } b \mid p \implies |b| = |p| \implies |a| = 1 \ \checkmark \end{cases}$$

$\Longleftarrow$: nem kell vizsgán.

TÉTEL: (számelmélet alaptétele) Minden n ($2 \leq n$) a sorrendtől és előjelektől eltekintve egyértelműen felbontható felbonthatatlanok szorzatára.

biz.: felbonthatóság bizonyítása:

n:
- felbonthatatlan ✓
- $n = a \cdot b$:
  - a, b felbonthatatlan ✓
  - ha pl. a felbontható: $n = a_1 \cdot a_2 \cdot b$:
    - a_1, a_2, b felbonthatatlan ✓
    - …

egyértelműség bizonyítása:

tfh. n két különböző módon felbontható: $n = p_1 p_2 \cdot \ldots \cdot p_k = q_1 q_2 \cdot \ldots \cdot q_l$

$p_1 \mid q_1 q_2 \cdot \ldots \cdot q_l \xrightarrow{p_1 \text{ prím}} p_1 \mid q_1$ vagy $p_1 \mid q_2$ vagy … vagy $p_1 \mid q_l$

Például: $\underbrace{p_1 \mid q_1}_{q_1 = p_1 \cdot c}$ de q_1 felbonthatatlan $\implies$ $|p_1| = 1$ de $|p_1|$ prím, nem lehet 1! ↯

vagy

$|c| = 1 \implies$ ez azt jelenti, hogy $|p_1| = |q_1|$

$\Downarrow$

visszavezettük a problémát egy egyszerűbb esetre:

$\underbrace{p_2 p_3 \cdot \ldots \cdot p_k = q_2 q_3 \cdot \ldots \cdot q_l}$

erre ismét alkalmazzuk az algoritmust, egészen addig, míg mindegyikük ki nem derül, hogy egyenlőek. ✓

<u>Következmény:</u> prímtényezős felbontás / kanonikus alak: $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots$

Figyeljük meg, hogy jóllehet ∞ sok prímszám van, csak véges sok kitevő lesz pozitív, tehát csak véges sok 1-től különböző szám szorzatát képezzük.

<u>Osztók száma:</u> jele: $d(n)$

Pl.: $n = 2^3 \cdot 3^2 \cdot 7^4$

$d \mid n$ ha $d = 2^{0,1,2,3} \cdot 3^{0,1,2} \cdot 7^{0,1,2,3,4}$ — $d(2^3 \cdot 3^2 \cdot 7^4) = (3+1)(2+1)(4+1)$

általánosan: $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ — $d(n) = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1)$

Osztók összege: jele: $\sigma(n)$ /n-nek a pozitív osztóinak összegét jelöljük)

pl.: $n = 36 = 2^2 \cdot 3^2$ $\sigma(36) = (1+2+2^2)(1+3+3^2)$

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

$$= \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \ldots \cdot \frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

TÉTEL: ∞ sok prímszám $\exists$

biz.: indirekt tfh. véges sok van: $p_1, p_2, \ldots, p_n$. $A := p_1 p_2 \ldots p_n + 1 \Rightarrow A$ nem prím, mert $\forall$ prímnél nagyobb $\Rightarrow$ A-nak van prímosztója, de A $p_1, \ldots, p_n$-nel osztva 1 maradékot ad. ↯

TÉTEL: $\forall N$-re $\exists\, p, q$ szomszédos prímek, amelyekre $N \leq |p-q|$

biz.: elég: $\exists$ N db szomszédos összetett szám

$2 \mid (N+1)! + 2$
$3 \mid (N+1)! + 3$
$\vdots$
$N+1 \mid (N+1)! + N + 1$
} N db, mindegyik összetett ✓

DEF.: $\pi(n)$: 1-től n-ig a prímek száma pl.: $\pi(10) = 4$

TÉTEL: („nagy prímszámtétel") $\pi(n) \approx \frac{n}{\ln n}$ aszimptotikus egyenlőség, jelentése: $\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$

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

pl.: ∞ sok $4k+1$, $4k+3$, $10k+1$, $10k+3$, $10k+7$, $10k+9$ alakú prím van

DEF1.: $a \equiv b \pmod m$ /a kongruens b-vel modulo m/ ha a és b m-mel osztva egyforma maradékot adja.

DEF2.: $a \equiv b\ (m) \iff m \mid a-b$

Példa: $17 \equiv 52 \equiv -4 \pmod 7$

TÉTEL:

$$\left.\begin{array}{l} a \equiv b\ (m) \\ c \equiv d\ (m) \\ k \in \mathbb{N} \end{array}\right\} \Longrightarrow \begin{array}{ll} (1) & a \pm c \equiv b \pm d\ (m) \\ (2) & ac \equiv bd\ (m) \\ (3) & a^k \equiv b^k\ (m) \end{array}$$

biz.: (1) $\left.\begin{array}{l} m \mid a-b \\ m \mid c-d \end{array}\right\} \overset{\pm}{\Longrightarrow} m \mid (a \pm c) - (b \pm d)$ ✓

(2) $\left.\begin{array}{l} m \mid a-b \overset{\cdot c}{\Longrightarrow} m \mid ac-bc \\ m \mid c-d \overset{\cdot b}{\Longrightarrow} m \mid bc-bd \end{array}\right\} \oplus \Longrightarrow m \mid ac-bd$ ✓

Speciális eset: $\left.\begin{array}{l} a \equiv b\ (m) \\ c \equiv c\ (m) \end{array}\right\} \Rightarrow ac \equiv bc\ (m)$

(3) $\left.\begin{array}{l} a \equiv b\ (m) \\ a \equiv b\ (m) \\ \vdots \\ a \equiv b\ (m) \end{array}\right\}$ k db, összeszorozzuk őket /mert (2)-t már bizonyítottuk/ ✓

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

$m := m' \cdot (m,c)$ $c := c' \cdot (m,c)$ $\Rightarrow (m', c') = 1$

$m \mid ac - bc \iff m \mid c(a-b) \iff m' \mid c'(a-b) \iff m' \mid a-b$ ✓

$\boxed{\text{13. TÉTEL}}$

Lineáris kongruenciák: a megoldhatóság szükséges és elégséges feltétele, a megoldások száma. Wilson tétele.

DEF.: lineáris kongruencia: $ax \equiv b\ (m)$ adottak: a, b, m kérdés: $x = ?$

Példa: $6x \equiv 7\ (15)$

$\underbrace{3 \mid}_{} \ 15 \mid \underbrace{6x}_{3\mid} - \underbrace{7}_{3\nmid} \implies \nexists$ megoldása!

TÉTEL: Az $ax \equiv b\ (m)$ $a \neq 0$ lin. kongruencia megoldható $\iff (a,m) \mid b$.
A kongruencia megoldáshalmaza (a,m) darab maradékosztály modulo m.

biz.: Legyen $d := (a,m)$, $a = a'd$, $m = m'd$, $b = b'd$

Ha $ax \equiv b\ (m)$ mo.-ható $\implies d \mid m \mid ax - b$ és $d \mid a \mid ax$ miatt $d \mid ax - (ax - b) = b$ ✓

Elégségesség bizonyítása: tfh. $d \mid b$. A kongruenciát d-vel végigosztva: $a'x \equiv b'\ (m')$ és $(a', m') = 1$

Az Euklideszi algoritmus segítségével kiszámítható olyan $k, l \in \mathbb{Z}$, amire $ka' + lm' = 1$, k-nak és m'-nek nem lehet közös p prímosztója, hiszen ha volna, akkor $p \mid ka' + lm' = 1$ állna. $\implies (k, m') = 1$

$$\left.\begin{aligned} a'x \equiv b'\ (m') \overset{(k,m')=1}{\iff} ka'x \equiv kb'\ (m') \iff (1 - lm')x &\equiv kb'\ (m') \\ lm'x &\equiv 0\ \ (m') \end{aligned}\right\} \oplus \implies \underline{\underline{x \equiv kb'\ (m')}}$$

Hátra van még, hogy a megoldásokat mod m adjuk meg. Mivel $m = m'd$, ezért $\forall$ m' szerinti maradékosztály pontosan d darab m szerinti maradékosztály uniója, a megoldások tehát:

$x \equiv kb' + \lambda m'\ (m)$ $\lambda = 0, 1, \ldots, (d-1)$

TÉTEL: (Wilson) Legyen $2 \leq k \in \mathbb{Z}$, akkor:

$$(k-1)! \equiv \begin{cases} -1 \pmod{k} & \text{ha } k \text{ prím} \\ 2 \pmod{k} & \text{ha } k = 4 \\ 0 \pmod{k} & \text{ha } 6 \leq k \text{ összetett szám} \end{cases}$$

biz.: $k = 4$-re nyilvánvaló: $3! = 2 \cdot 3 = 6 \equiv 2\ (4)$

Ha $6 \leq k$ összetett, akkor vagy található két olyan különböző $1 < a < b < k$ egész, melyekre $ab = k$, és akkor $1 \cdot 2 \cdot \ldots \cdot (k-1) = a b c \equiv 0\ (k)$, vagy $k = l^2$ és ilyenkor l és $2l$ szerepel a tényezők között.

Legyen végül $k = p$ prím:

$\forall$ $1 \leq a \leq p-1$ egészhez tartozik egy $1 \leq b \leq p-1$ egész, melyre $ab \equiv 1\ (p)$ hiszen az $ax \equiv 1\ (p)$ kongruenciát pontosan egy mod p maradékosztály elégíti ki. Látható, hogyha a-hoz b, akkor b-hez a tartozik, tehát az $1, 2, \ldots, p-1$ számok így rendezhetők párokba, hogy $\forall$ pár szorzata 1-et ad maradékul p-vel osztva. A párokba rendezés azért nem egészen pontos, mert bizonyos számok esetleg önmagukkal állnak párban. Ezekre az a számokra $a^2 \equiv 1\ (p)$ teljesül, azaz $p \mid a^2 - 1 \iff p \mid (a+1)(a-1) \overset{p \text{ prím}}{\implies} p \mid a+1$ vagy $p \mid a-1 \implies$ az önmagukkal párban álló számok kizárólag az 1 és $(p-1)$ lesznek. Átrendezve a $(p-1)!$-t, $\forall$ pár szorzata 1 lesz, és lesznek még a párosítatlanul maradt 1 és $(p-1)$ $\implies (p-1)! \equiv 1 \cdot 1 \cdot \ldots \cdot 1 \cdot (p-1) \equiv p-1 \equiv -1\ (p)$.

14. TÉTEL

Euklideszi algoritmus (ennek alkalmazása lineáris kongruenciák megoldására is). Kétismeretlenes, lineáris diofantikus egyenlet megoldása (konkrét példán). Két kongruenciából álló kongruenciarendszer megoldása (konkrét példán).

Euklideszi algoritmus: hatékony módszer két szám legnagyobb közös osztójának meghatározására

Input: $a, b \in \mathbb{Z}$ $(a \geq b)$ Output: (a, b)

Legyen $a_0 := a$, $a_1 := b$. Ha már meghatároztuk az $a_0 \geq a_1 \geq \ldots \geq a_i$ számokat, akkor legyen $a_{i-1} = q_i a_i + a_{i+1}$.
Az a_{i+1} tehát az a_{i-1} a_i-vel történő osztásakor keletkező maradék ((C nyelven: $a_{i+1} = a_{i-1} \% a_i$), tehát $0 \leq a_{i+1} < a_i$ teljesül. Az eljárás akkor ér véget, ha $a_{k+1} = 0$, ekkor $(a, b) = a_k$

Példa: $(360, 225) = ?$

$$360 = 1 \cdot 225 + 135$$
$$225 = 1 \cdot 135 + 90$$
$$135 = 1 \cdot 90 + 45$$
$$90 = 2 \cdot \underline{\underline{45}} + 0$$

Az euklideszi algoritmus véget is ér, azaz $a_{k+1} = 0$ lesz, mert (a_i) nemnegatív egészek szig. monoton csökkenő sorozata, tehát az eljárás lépésszámára $|a_0|$ felső korlát.

$$(a, b) = (a_0, a_1) = (\underbrace{a_0 - q_1 a_1}_{a_2}, a_1) = (a_1, a_2) = (\underbrace{a_1 - q_2 a_2}_{a_3}, a_2) = (a_2, a_3) = \ldots = (a_k, \overset{0}{a_{k+1}}) = a_k \quad ✓$$

Példa: lin. kongruencia megoldása eukl. alg. által

$59x \equiv 1 \ (101)$ $x = ?$

Először meghatározzuk lnko-t:

$(101, 59) = ?$

$$101 = 1 \cdot 59 + 42$$
$$59 = 1 \cdot 42 + 17$$
$$42 = 2 \cdot 17 + 8$$
$$17 = 2 \cdot 8 + 1$$
$$8 = 8 \cdot 1 + 0$$

$\hookrightarrow 1 | 1$ ✓ $\exists$ 1 mo.!

Ezután az egyenletekből kifejezzük a maradékokat:

$$42 = 101 - 1 \cdot 59 \equiv (-1) \cdot 59 \pmod{101}$$
$$17 = 59 - 42 \equiv 59 - (-1) \cdot 59 = 2 \cdot 59 \pmod{101}$$
$$8 = 42 - 2 \cdot 17 \equiv (-1) \cdot 59 - 2 \cdot 2 \cdot 59 = (-5) \cdot 59 \pmod{101}$$
$$1 = 17 - 2 \cdot 8 \equiv 2 \cdot 59 - 2 \cdot (-5) \cdot 59 = 12 \cdot 59 \pmod{101} \implies 1 \equiv 12 \cdot 59 \pmod{101}$$

$$59x \equiv 1 \equiv 12 \cdot 59 \pmod{101} \quad /:59$$
$$\underline{\underline{x \equiv 12 \pmod{101}}}$$

Példa: kétismeretlenes, lineáris diofantikus egyenlet megoldása

Általánosan: adott az $ax + by = c$ egyenlet és $a, b, c \in \mathbb{Z}$ egészek, kérdés: $x, y = ?$ $x, y \in \mathbb{Z}$

$by = c - ax$

$b | c - ax \implies ax \equiv c \ (b)$ Tehát visszavezettük a problémát egy lin. kongruencia megoldására.

$59x + 101y = 1$

$101y = 1 - 59x$

$101 | 1 - 59x \implies 59x \equiv 1 \ (101)$ Előzőleg láttuk, hogy ennek megoldása az $x \equiv 12 \ (101)$, tehát

$\underline{\underline{x = 101k + 12}}$ alakú $(k \in \mathbb{Z})$, $y = \frac{1 - 59x}{101} = \frac{1 - 59(101k + 12)}{101} = \frac{\overbrace{1 - 59 \cdot 12}^{-707}}{101} - 59k = \underline{\underline{-7 - 59k}}$ alakú

ellenőrzés: $59x + 101y = 59(101k + 12) + 101(-7 - 59k) = \cancel{59 \cdot 101k} + \underbrace{59 \cdot 12}_{708} - \underbrace{7 \cdot 101}_{707} - \cancel{101 \cdot 59k} = 1$ ✓

Példa: Két kongruenciából álló kongruenciarendszer megoldása

$$\left.\begin{array}{l} x \equiv 3 \ (7) \\ x \equiv -1 \ (8) \end{array}\right\} \qquad x = ?$$

Az elsőből következik, hogy $x = 7k+3$ ahol $k \in \mathbb{Z}$, ezt behelyettesítjük be a másodikba!

$$7k+3 \equiv -1 \ (8) \quad / -3$$
$$7k \equiv -4 \ (8) \quad / -8k$$
$$-k \equiv -4 \ (8) \quad / \cdot(-1)$$
$$k \equiv 4 \ (8) \implies k = 8l+4 \text{ ahol } l \in \mathbb{Z} \implies x = 7k+3 = \overbrace{7(8l+4)}^{56l+28}+3 =$$
$$= 56l+31 \text{ ahol}$$
$$\Downarrow$$
$$\underline{\underline{x \equiv 31 \ (56)}}$$

15. TÉTEL

Euler féle φ-függvény, redukált maradékrendszer, Euler-Fermat-tétel, kis Fermat-tétel.

DEF.: $\varphi(m)$: 1 és m között az m-hez relatív prímek száma

Példa: $\varphi(10)=4$ mert $1\ \cancel{2}\ 3\ \cancel{4}\ \cancel{5}\ \cancel{6}\ 7\ \cancel{8}\ 9\ \cancel{10}$

ha p prím: $\varphi(p)=p-1$ mert 1-től $(p-1)$-ig $\forall$ szám relatív prím p prímhez

$$\varphi(p^\alpha)=\underbrace{p^\alpha}_{\text{összes}}-\underbrace{p^{\alpha-1}}_{\text{„rossz"}}$$

TÉTEL: ha $(a,b)=1 \Rightarrow \varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$

Ha $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k} \Rightarrow \varphi(n)=\varphi(p_1^{\alpha_1})\cdot\varphi(p_2^{\alpha_2})\cdot\ldots\cdot\varphi(p_k^{\alpha_k})=(p_1^{\alpha_1}-p_1^{\alpha_1-1})(p_2^{\alpha_2}-p_2^{\alpha_2-1})\cdot\ldots\cdot(p_k^{\alpha_k}-p_k^{\alpha_k-1})=$

$$=\underbrace{p_1^{\alpha_1}p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}}_{n}\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)=n\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)$$

Példa: $\varphi(100)=?$

$100=2^2\cdot5^2$

$\varphi(100)=(2^2-2^1)\cdot(5^2-5^1)=\overbrace{(4-2)}^{2}\cdot\overbrace{(25-5)}^{20}=\underline{\underline{40}}$

DEF.: Redukált maradékrendszer modulo m (RMR mod m röviden):

az egy $\{c_1,c_2,\ldots,c_k\}$ ügy(halmaz), hogy teljesülnek a következők:

(1) $k=\varphi(m)$

(2) $1\le i,j\le k \quad i\ne j \Rightarrow c_i\not\equiv c_j \pmod m$

(3) $(c_i,m)=1 \quad \forall i$-re

Pl.: RMR mod 10: $\{1,3,7,9\}$ vagy $\{37,29,-59,33\}$

Állítás: ha $\{c_1,\ldots,c_k\}$ RMR mod m és $(a,m)=1 \Rightarrow \{ac_1,ac_2,\ldots,ac_k\}$ is RMR mod m

Pl.: $\{1,3,7,9\}$ RMR mod 10 $\quad /\cdot 7$ mert $(7,10)=1$

$\{7,21,49,63\}$ is RMR mod 10.

biz.: (1) a két halmaz elemszáma nyilván megegyezik ✓

(2) ha $ac_i\equiv ac_j\ (m) \quad /:a \quad (a,m)=1$

$c_i\equiv c_j\ (m)$

$\Downarrow$ tudjuk, hogy $\{c_1,\ldots,c_k\}$ RMR mod 10 volt

$i=j$ ✓

(3) tudjuk: $\left.\begin{array}{l}(a,m)=1\\(c_i,m)=1\end{array}\right\}\Rightarrow (ac_i,m)=1$ ✓

TÉTEL: (Euler-Fermat) $(a,m)=1 \Rightarrow a^{\varphi(m)}\equiv1\ (m)$

biz.: legyen $\{c_1,\ldots,c_k\}$ egy tetszőleges RMR mod m $\Rightarrow \varphi(m)=k$

Mivel $(a,m)=1 \Rightarrow \{ac_1,\ldots,ac_k\}$ is RMR mod m $\Rightarrow$ tehát az $ac_1,\ldots,ac_k$ számok valamilyen sorrendben kongruensek a $c_1,\ldots,c_k$ számokkal $\Rightarrow (ac_1)(ac_2)\cdot\ldots\cdot(ac_k)\equiv c_1c_2\cdot\ldots\cdot c_k\ (m)$ $/:c_1$ $/:c_2$ $\vdots$ $/:c_k$

$a^{\varphi(m)}\equiv1\ (m)$ ✓

TÉTEL: („kis" Fermat tétel) p prím, a tetszőleges egész $\Rightarrow a^p\equiv a\ (p)$

biz.: p prím $\Rightarrow \varphi(p)=p-1 \xRightarrow[\text{mert } (a,p)=1]{\text{E-F}} a^{p-1}\equiv1\ (p) \xRightarrow{\cdot a} a^p\equiv a\ (p)$ ✓

16. TÉTEL

Számelmélet és algoritmusok: alapműveletek, hatványozás az egész számok körében és modulo m. Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosítás.

Egy algoritmust akkor tekintünk jónak, ha lépésszáma felülről becsülhető az input hosszának polinomjával. Vizsgáljuk meg az alapműveletek lépésszámigényét!

Nyilván az iskolai összeadás és kivonás lépésszáma a számjegyek számával arányos, ezek tehát lineáris, azaz polinom rendű algoritmusok. Könnyű végiggondolni, hogy az iskolai szorzás és osztás is polinomiális (de már nem lineáris). Viszont a hatványozás nem végezhető el polinomrendben, hisz pl. 2^x végeredményének puszta kiírásához már $\log 2^x = x$ lépés kell, ami az input (vagyis $\log x$-nek) exponenciális függvénye. Az euklideszi algoritmus hatékony, mert polinomiális lépésszámú.

Ebből következik, hogy a maradékszámítás is polinomiális, mert kiszámításához egy osztásra, egy szorzásra és egy kivonásra van szükség: $a \% b \longleftrightarrow a-(a/b)*b$ /C szintaxissal írva/

Tehát a mod m $+, -, \cdot, /$ is polinomiális! Mi a helyzet a mod m hatványozással?

Az alábbi példa bemutatja, hogy a mod m hatványozás elvégezhető polinomidőben:

Példa: $3^{100} \equiv ?\ (7)$

$3^1 \equiv 3\ (7)$
$3^2 \equiv 9 \equiv 2\ (7)$
$3^4 \equiv 2^2 = 4\ (7)$
$3^8 \equiv 4^2 = 16 \equiv 2\ (7)$
$3^{16} \equiv 2^2 = 4\ (7)$
$3^{32} \equiv 4^2 = 16 \equiv 2\ (7)$
$3^{64} \equiv 4\ (7)$

Most írjuk fel a 100-at binárisan: $100_{(10)} = \overset{6}{1}\overset{5}{1}\overset{4}{0}\overset{3}{0}\overset{2}{1}\overset{1}{0}\overset{0}{0}{}_{(2)}$

$\Downarrow$

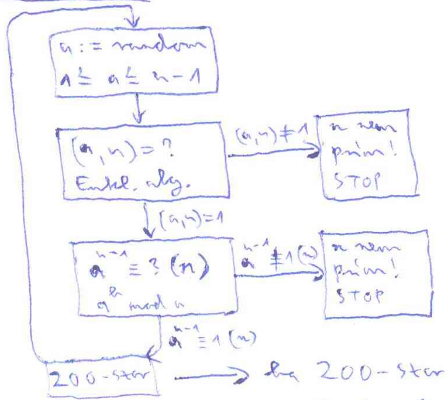
$$3^{100} \equiv 3^{2^6}\cdot 3^{2^5}\cdot 3^{2^2} = 3^{64}\cdot 3^{32}\cdot 3^{4}\ (7)$$

$$3^{100} \equiv 4\cdot 2\cdot 4 = 32 \equiv \underline{\underline{4}}\ (7)$$

Prímtesztelés

Egy egyszerű módszer, hogy 1-től $\sqrt{n}$-ig ellenőrizzük az oszthatóságot. Előnye, hogyha egy szám összetettnek bizonyul, akkor le megadja egy osztóját is, viszont exponenciális lépésszámú. Létezik ennél gyorsabb algoritmus is:

Fermat-teszt: kérdés: n prím-e?



→ ha 200-szor $a^{n-1} \equiv 1\ (n)$ → STOP: „n valószínűleg prím"

DEF.: $(a,n)=1$

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

a cinkosa n-nek, ha $a^{n-1} \equiv 1\ (n)$

TÉTEL: ha n-nek $\exists$ tanúja $\Longrightarrow$ RMR mod n legalább fele tanú!

biz.: legyen „a" egy tanú, $c_1, \dots, c_k$ cinkosok

Állítás: $a \cdot c_i$ tanú

biz.: $(a \cdot c_i)^{n-1} \equiv \underbrace{a^{n-1}}_{\not\equiv 1} \cdot \underbrace{c_i^{n-1}}_{\equiv 1} \ (n) \Longrightarrow (a \cdot c_i)^{n-1} \not\equiv 1 \ (n)$ ✓

Állítás: $ac_i \not\equiv ac_j \ (n)$ ha $c_i \not\equiv c_j \ (n)$

biz.: ha $ac_i \equiv ac_j \ (n)$ $\ /: a$ mert $(a,n)=1$

$c_i \equiv c_j \ (n)$ ✓

Következmény: ha van tanú $\Longrightarrow$ a Fermat-teszt legfeljebb $\left(\frac{1}{2}\right)^{200}$ valószínűséggel téved

DEF.: n Carmichael-szám, ha összetett, de $\nexists$ tanúja RMR-ben, azaz $\forall a \ (a,n)=1$-re $a^{n-1} \equiv 1 \ (n)$

pl.: 561

De van olyan teszt, aminek a működése olyan, hogy kiszűri a Carmichael-számokat.

Prím generálás: n legyen pl. egy 200 jegyű random szám $\rightarrow$ prímtesztelés. Ha összetett, megnézzük $(n+1)$-et, $(n+2)$-t, stb... A $\pi(n) \approx \frac{n}{\ln n}$ függvény szerint rövid időn belül prímre fogunk találni. ✓

Nyilvános kulcsú titkosítás

Bármilyen üzenet átalakítható számjegyek sorozatává, feltételezzük tehát, hogy a titkosítandó üzenet sokszámjegyű számok sorozata. A rejtjelezés alapja, hogy legyen egy kódoló és dekódoló függvény:

$x \overset{C}{\longmapsto} C(x)$, $\ y \overset{D}{\longmapsto} D(y)$ amire teljesül a visszafejthetőség: $D(C(x)) = x$

RSA-kód: $N := p \cdot q$ ahol p, q sokszámjegyű prímek

c választása úgy, hogy $\varphi(N) = (p-1)(q-1)$-hez relatív prím legyen: $(c, \varphi(N)) = 1$

kódolás: $x \longrightarrow x^c \bmod N$

nyilvános: N, c $\quad$ titkos: $p, q, d, \varphi(N)$

Megjegyzés: Ez az egész azért működik, mert számok prímtényezős felbontására hatékony algoritmus nem ismert!

dekódolás: $y \longrightarrow y^d \bmod N$

d jól van megválasztva $\Longleftrightarrow x^{c \cdot d} = (x^c)^d \equiv x \ (N)$ $\ \forall x$-re

Segédtétel: $(x,N)=1 \Longrightarrow x^{\varphi(N)} \equiv 1 \ (N) \Longrightarrow x^{k \cdot \varphi(N)} \equiv 1 \ (N) \Longrightarrow x^{k \cdot \varphi(N)+1} \equiv x \ (N)$

cél: $c \cdot d = k \cdot \varphi(N) + 1$ valamely k-ra, azaz $\underbrace{c \cdot d \equiv 1 \ (\varphi(N)) \text{ lin. kongruencia}}$ $\leftarrow$ Az euklideszi algoritmussal megoldható!

megoldható $\Longleftrightarrow \underbrace{(c, \varphi(N))}_{1} = 1$ ✓ $\qquad d \equiv \_\_ \ (\varphi(N))$

A d-t azért nem tudja bárki kiszámolni, mert nem tudja felírni a lin. kongruenciát, ugyanis a $\varphi(N)$ kiszámolásához szükséges p és q ismerete: $\varphi(N) = (p-1)(q-1)$.

Digitális aláírás

Előnye, hogy ha A üzenetet küld B-nek, akkor B meg tudja bizonyosodni arról, hogy az üzenetet csakis A-tól kaphatta.

$A \longrightarrow B$

$C_A \quad C_B$ } kódolófüggvények nyilvánosak

$D_A \quad D_B$ } dekódolófüggvények titkosak

$\Longrightarrow$

$x \longrightarrow y := D_A(C_B(x))$

$y \longrightarrow x := D_B(C_A(y))$

$\boxed{\text{17. TÉTEL}}$

Művelet fogalma, csoport, Abel-csoport. Példák: csoportok számokon, mátrixokon, rajzok szimmetriacsoportja, diédercsoport, szimmetrikus csoport

---

<u>DEF.:</u> az $f: H^2 \to H$ függvényt <u>műveletnek</u> hívjuk, ahol $H \neq \emptyset$. alaphalmaz és H^2 a H-ból képezhető rendezett párok halmaza

$\in H \quad \in H$ → művelet → $\in H$

<u>Ellenpélda:</u> a skaláris szorzás egy „őszvér" művelet, mert vektorokat kap, és skalárt ad vissza

$\underline{u}, \underline{v} \longrightarrow c \in \mathbb{R}$

<u>DEF.:</u> $*$ művelet: <u>kommutatív</u>, ha $a * b = b * a$

<u>asszociatív</u>, ha $(a * b) * c = a * (b * c) \quad \forall a, b, c \in H$-ra

S alaphalmaz, $*$ asszociatív művelet S-en $\Rightarrow (S, *)$ <u>félcsoport</u>

<u>DEF.:</u> ($*$ műv., H alaphalmaz) $e \in H$ <u>egységelem</u>, ha $\forall a \in H$-ra $e * a = a * e = a$

<u>Állítás:</u> az egységelem egyértelmű (ha van)

<u>biz.:</u> tfh. e, f különböző egységelemek: $f = \underset{\text{mert } e \text{ egységelem}}{e * f} \overset{\text{mert } f \text{ egységelem}}{=} e$ ↯

<u>DEF.:</u> e egységelem, az $a \in H$ <u>inverze</u> $b \in H$, ha $a * b = b * a = e$ jele: $b = a^{-1}$

<u>DEF.:</u> $(G, *)$ <u>csoport</u>, ha $*$ művelet G-n és:

- $*$ asszociatív
- $\exists$ egységelem
- $\forall$ elemnek $\exists$ inverze

<u>Állítás:</u> egy csoportban a^{-1} egyértelmű (ha van)

<u>biz.:</u> tfh. b, c az a két különböző inverze:

$a \to b, c \}$ inverzek $\qquad c = \overbrace{(b * a)}^{e} * c = b * \overbrace{(a * c)}^{e} = b$ ↯

<u>DEF.:</u> ha $(G, \circ)$ csoport és $\circ$ kommutatív, akkor $(G, \circ)$ <u>Abel-csoport</u>

<u>Példák:</u>

csoportok számokon:

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ csoport
- De pl. az $(\mathbb{N}, +)$ nem csoport, mert a pozitív tagoknak $\nexists$ inverze!
- $(\mathbb{R}, \cdot)$ nem csoport, mert a 0-nak $\nexists$ inverze!
- Viszont kivéve a halmazból a 0-t, már csoportok lesznek ezek: $(\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$

csoportok mátrixokon:

$H := \{n \times n$-es, $\det \neq 0$ mátrixok$\}$, a művelet legyen a mátrixszorzás. Ez vajon csoportot alkot-e?

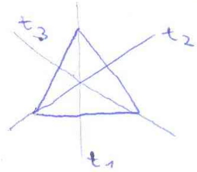
Először ellenőrizzük a zártságot: $\underbrace{\det(A \cdot B)}_{\neq 0 \ \checkmark} = \underbrace{\det A}_{\neq 0} \cdot \underbrace{\det B}_{\neq 0} \Leftarrow$ ← determinánsok szorzástétele miatt

- asszociativitás ✓
- egységelem := egységmátrix: $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \big\} n$ ✓
- inverz := invertmátrix $A \to A^{-1}$ ← ez is H-beli, és biztos $\exists A^{-1}$, mert $\det A \neq 0$ ✓

$\Rightarrow (\{n \times n$-es, $\det \neq 0$ mx.-ok$\}$, mátrixszorzás$)$ csoport ✓

rajzok szimmetriacsoportja:

Most tekintsük egy rajznak, pl. egy szabályos Δ-nek a szimmetriáit/egybevágósági transzformációit!



f_{120} ↻, ↺ f_{240}, $I \qquad H = \{1, f_{120}, f_{240}, t_1, t_2, t_3\}$

Legyen az alaphalmaz $H := \{R$ rajznak a szimmetriái$\}$, a művelet pedig a függvénykompozíció!

A fgv.kompozícióról tudjuk, hogy rendelkezik az asszociativitás tulajdonsággal:

$f, g, h: H \to H$ függvények $\quad (f \circ g) \circ h = f \circ (g \circ h)$

Állítás: az R szimmetriacsoport csoport

biz.: • a függvénykompozíció asszociatív ✓

• egységelem := identitás ✓

• inverz := inverzfüggvény (f^{-1}) ✓

DEF.: diédercsoportnak nevezzük az n-oldalú szabályos sokszög szimmetriacsoportját. Jele: D_n

$$D_n = \{1, f_\alpha, f_{2\alpha}, f_{3\alpha}, \dots, f_{(n-1)\alpha}, t_1, t_2, \dots, t_n\} \qquad \alpha = \frac{360^\circ}{n}$$

$$|D_n| = 2n$$

Az előző oldal alján lévő Δ-es példa a D_3-nak felel meg.

DEF.: $f: \{1,2,\dots,n\} \to \{1,2,\dots,n\}$ kölcsönösen egyértelmű függvényt permutációnak nevezzük

Példa:
$$\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 2 & 1 & 4 \end{matrix} \qquad \text{szokásos jelölés: } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

DEF.: S_n szimmetrikus csoport

elemei: $\{1,2,\dots,n\}$ permutációi, művelet: kompozíció $\qquad |S_n| = n!$

pl.: $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$$

pl. így áll elő: $4 \to 2 \to 5$

Állítás: S_n csoport

biz.: • a kompozíció asszociatív ✓

• egységelem := identitás $\to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ ✓

• inverz := inverzfüggvény ✓ $\xrightarrow{\text{pl.:}} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$

18. TÉTEL

Elem rendje (ez véges csoportban véges), ciklikus csoport. Részcsoport. Csoportok izomorfiája, Cayley tétele (biz. nélkül)

DEF.: G csoport rendje = az elemszámával, ezért jele: $|G|$ pl.: $|D_{10}| = 20$, $|S_{10}| = 10!$

DEF.: $(G, *)$ csoport, $g \in G$

$g^n := \underbrace{g * g * g * \ldots * g}_{n \text{ db}}$ Példa: $(\mathbb{Z}, +)$-nál $3^5 = 3+3+3+3+3 = 15$

D_3-nál $f_{120}^2 = f_{240}$, $f_{120}^3 = I$, $t_1^2 = I$

TÉTEL: G véges, $g \in G \implies \exists\, n \geq 1$, hogy $g^n = e$

biz.: soroljuk fel g hatványait: $g^1, g^2, g^3, \ldots, g^k, \ldots, g^l, \ldots$ Mivel G véges $\implies \exists\, 1 \leq k < l$ hogy $g^l = g^k$.

Szorozzuk ezt be g^{-1}-gyel jobbról: $\overbrace{g \cdot g \cdots g \cdot g^{-1}}^{l} = \overbrace{g \cdot g \cdots g \cdot g^{-1}}^{k} \implies g^{l-1} = g^{k-1}$. Ezt a g^{-1}-es szorzást

hajtsuk végre annyiszor, hogy végül $g^{l-k} = e$ egyenlőséget kapjunk, ekkor $n := l-k$. ✓

DEF.: $g \in G$, a g rendje k, ha k a legkisebb olyan kitevő, hogy $g^k = e$ $(1 \leq k)$ jele: $o(g) = k$ („order")

$\underbrace{g^1, g^2, \ldots, g^{k-1}}_{\text{különbözők}}, \underset{e}{g^k}, g^1, g^2, \ldots$ Ha nincs ilyen szám, végtelen rendű elemről beszélünk.

Példa: D_3-nál $o(f_{120}) = 3$, $o(t_1) = 2$

$(\{\pm 1, \pm i\}, \cdot)$-nál $o(i) = 4$, $o(-1) = 2$

DEF.: G ciklikus csoport, ha $\exists\, g \in G$ generátor elem, hogy g-ből G $\forall$ eleme kifejezhető a művelet és az inverzképzés segítségével, jele: C_n

Állítás: G véges, G ciklikus $\iff \exists\, g \in G$, amire $o(g) = |G|$

biz.: $\Leftarrow$: G tartalmazza g-t és annak hatványait, g különböző hatványainak száma $o(G)$, ami egyenlő $|G|$-vel, tehát g generálni tudja G $\forall$ elemét $\implies$ G ciklikus ✓

$\implies$: Mivel G ciklikus, $\exists$ egy g generátor elem, amivel elő lehet állítani G $\forall$ elemét $\implies o(g) = |G|$ ✓

Példa: $(\{\pm 1, \pm i\}, \cdot)$ ciklikus, D_3 nem ciklikus, $(\mathbb{Z}, +)$ ciklikus

Állítás: G ciklikus $\implies$ G Ábel

biz.: $a \cdot b = b \cdot a$

$g^i \cdot g^j = g^j \cdot g^i \implies g^{i+j} = g^{j+i}$ ✓

Állítás: Minden prímrendű csoport ciklikus

biz.: Legyen $|G| = p$ prím. A Lagrange-tétel miatt $\forall\, e \neq g \in G$-re $o(g) \mid p \implies \underbrace{o(g) = 1}_{\text{az egységelemet kizártuk}}$ vagy $p = |G|$ ✓

DEF.: $(G, *)$ izomorf $(H, \circ)$-val, ha $\exists\, f: G \to H$ kölcsönösen egyértelmű függvény (bijekció) úgy, hogy:

jele: $\cong$ $\forall\, a, b, c \in G$-re $a * b = c \iff f(a) \circ f(b) = f(c)$, másképpen: $\forall\, a, b \in G$-re $f(a * b) = f(a) \circ f(b)$

Példa: $G: (\mathbb{R}^+, \cdot)$, $H: (\mathbb{R}, +)$

$f: \mathbb{R}^+ \to \mathbb{R}$

$f(a \cdot b) = f(a) + f(b)$ } vegyük észre, hogy f a logaritmusfüggvény! $f = \log_a$, $0 < a \neq 1$

DEF.: $(G, \circ)$ csoport, $H \subseteq G$, H részcsoportja G-nek, ha H is csoport a $\circ$-ra nézve, jele: $H \leq G$

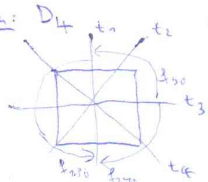
TÉTEL: $(G, \circ)$ csoport, $\emptyset \neq H \subseteq G$

H részcsoport $\iff$ (i) $a, b \in H \implies a \circ b \in H$
(ii) $a \in H \implies a^{-1} \in H$

biz.: $\implies$: a szükségesség nyilvánvaló

$\Leftarrow$: H-n $\circ$ művelet: – asszociatív (mert G-ben is az) ✓
– $g \in H \implies g^{-1} \in H \implies \underset{e}{g \cdot g^{-1}} \in H$ egységelem ✓
– (ii) miatt $\forall\, g \in H$-nak inverze is H-ban van ✓

Példa: D_4



$D_4 = \{I, f_{90}, f_{180}, f_{270}, t_1, t_2, t_3, t_4\}$ $|D_4| = 8$

$H_1 := \{I, f_{90}, f_{180}, f_{270}\}$ $|H_1| = 4$ $H_1 \leq G$

$H_2 := \{I, t_1\}$ $|H_2| = 2$ $H_2 \leq G$

$H_3 := \{I\}$ $|H_3| = 1$ $H_3 \leq G$

Állítás: Ciklikus csoport részcsoportja ciklikus

biz.: G ciklikus csoport generátoreleme legyen g, és legyen $H \leq G$ valódi részcsoport. Tekintsük a minimális $0 < k$-t, melyre $g^k \in H$. A cél belátni, hogy g^k generálja H-t. TFH. a g^k $g^l \in H$-t nem generálja, vagyis $k \nmid l$.

Legyen $l = qk + r \implies r$ maradék $(1 \leq r < k)$. Mivel $g^k, g^l \in H$: $g^l \cdot \left((g^k)^{-1}\right)^q = g^r \in H$ Ty

__Állítás:__ Azonos rendű ciklikus csoportok izomorfak

__biz.:__ $|G|=|H|=n$. Legyen g, h a G, H generátoreleme, ekkor g^n, h^n a G, H egységeleme. Mindkét csoport eleme g^i, h^i alakú, és könnyen látható, hogy $\varphi(g^i) := h^i$ izomorfizmus. ✓

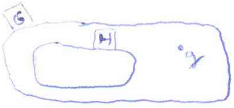
__TÉTEL:__ (Cayley) G véges csoport $\Longrightarrow$ $\exists n$, hogy S_n valamelyik H részcsoportjára $\overbrace{G \cong H}^{G \text{ izomorf } H\text{-val}}$.

19. TÉTEL

Mellékosztály, Lagrange tétele, elemrend és csoport rendjének kapcsolata.

DEF.: $(G,\circ)$ csoport, $g\in G$, $H\leq G$

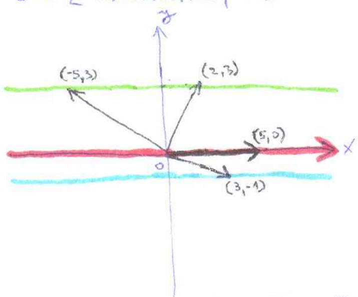
A $\{gh \mid h\in H\}$ halmaz a H részcsoport g szerinti baloldali mellékosztálya, jele: gH



$H=\{e, h_1, h_2, \dots\}$

$gH=\{g, gh_1, gh_2, \dots\}$

Példa: $G:=\{$síkvektorok$, +\}$ $H=\{x$-tengely vektorai$\}$



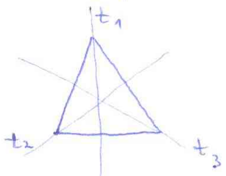
$g=(2,3) \to (2,3)+H$

$g=(3,-1) \to (3,-1)+H$

$g=(-5,3) \to (-5,3)+H$

$g=(5,0) \to (5,0)+H$

Példa: $G=D_3$, $H=\{I, f_{120}, f_{240}\}$



emlékezzünk vissza, hogy a diédercsoportot úgy definiáltuk, hogy a műveletet a függvénykompozíció, amit jobbról balra kell végrehajtani!

$g=t_1$

$gH=\{t_1I, t_1f_{120}, t_1f_{240}\}=\{t_1, t_2, t_3\}$

$t_2H=\{t_2, t_3, t_1\}$

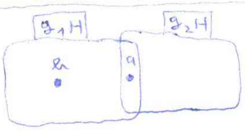
Tulajdonságok:

(1) $\boxed{g\in gH}$ ✓

biz.: mivel $e\in H \Rightarrow g=g\cdot e\in H$

(2) $\boxed{g_1H\cap g_2H\neq\emptyset \Rightarrow g_1H=g_2H}$

biz.:



$a\in g_1H\cap g_2H$, $h\in g_1H$ cél: $h\in g_2H$

$a=g_1h_1=g_2h_2$ $/\cdot h_1^{-1}$ jobbról $h_1, h_2\in H$

$g_1\underbrace{h_1h_1^{-1}}_{e}=g_2h_2h_1^{-1} \Rightarrow g_1=g_2h_2h_1^{-1}$

$b\in g_1H \Rightarrow h=g_1h_3$ $h_3\in H$ $h=g_2\underbrace{h_2h_1^{-1}h_3}_{:=h_4\in H}$ ✓

(3) $\boxed{H \text{ véges} \Rightarrow |H|=|gH|}$

biz.: $H=\{h_1, h_2, \dots, h_k\}$

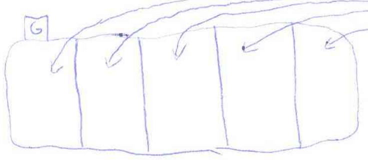
$gH=\{gh_1, gh_2, \dots, gh_k\}$

ha $gh_i=gh_j$ $/\cdot g^{-1}$ balról

$h_i=h_j$ ✓

TÉTEL: (Lagrange) G véges, $H\leq G \Rightarrow |H| \mid |G|$. Speciálisan, G bármely g $\overbrace{\text{elemének rendje}}^{o(g)}$ osztja G rendjét.

biz.:



H szerinti mellékosztályok, számuk: i

$|G|=|H|\cdot i \Rightarrow |H| \mid |G|$ ✓

szövegesen: Az előző megfigyelés szerint a G csoport előáll H szerinti (jobboldali) mellékosztályok uniója, és minden mellékosztály $|H|$ elemet tartalmaz. ✓

A tétel második felének bizonyítása:

Ha G csoportnak g egy eleme, akkor álljon H a g hatványaiból: $H=\{g^1, g^2, \dots, g^{k-1}, e\}$

k db különböző elem

Állítás: H részcsoport

biz.: (i) $g^i, g^j\in H$ $/g^i\cdot g^j=g^{i+j}/$

ha $i+j<k$ akkor $g^{i+j}\in H$ ✓

ha $k<i+j$ akkor $g^{i+j}=g^{i+j-k}\cdot \overset{e}{g^k}=g^{i+j-k}\in H$ ✓

(ii) $\underbrace{g^i\cdot g^{k-i}}_{g^k}=e \Rightarrow g^{k-i}=(g^i)^{-1}$ ✓

20. TÉTEL

Gyűrű és test fogalma. Nullosztómentes gyűrű, test nullosztómentessége. Példák: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $n\times n$-es mátrixok, polinomok, $\mathbb{Z}_n$ (az milyen n-re test), kvaterniók, $\mathbb{Q}(\sqrt{2})$.

Eddig egyműveletes struktúrákkal foglalkoztunk. Ha azonban a $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ számhalmazokról szeretnénk többet tudni, érdemes mindkét alapműveletet: az összeadást és a szorzást is figyelembe venni.

DEF.: R tetszőleges halmaz ($\neq \emptyset$), R-en két művelet: $+$, $\cdot$

(i) $a+b=b+a$ ($\forall a,b\in R$)

(ii) $(a+b)+c=a+(b+c)$

(iii) $\exists 0\in R$, amire $a+0=a$ $\forall a\in R$

(iv) $\forall a\in R$-re $\exists \underbrace{(-a)}_{\text{additív inverz}}\in R$ hogy $a+(-a)=0$

(i') $a\cdot b=b\cdot a$

(ii') $(a\cdot b)\cdot c=a\cdot(b\cdot c)$

(iii') $\exists 1\in R$, amire $a\cdot 1=1\cdot a=a$ $\forall a\in R$

(iv') $\forall \underset{\neq 0}{a}\in R$ $\exists \underbrace{a^{-1}}_{\text{multiplikatív inverz}}\in R$, amire $a\cdot a^{-1}=a^{-1}\cdot a=1$

(v) $a\cdot(b+c)=a\cdot b+a\cdot c$

$(b+c)\cdot a=b\cdot a+c\cdot a$

Ha $(R,+,\cdot)$-re teljesülnek akkor gyűrű.

— || — + akkor kommutatív gyűrű.

— || — + akkor ferdetest.

— || — + + akkor (kommutatív) test.

Példák: – $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$, $(\mathbb{Q},+,\cdot)$ test.

– $(\mathbb{Z},+,\cdot)$ nem test, mert $\nexists$ inverze $\forall$ elemnek, hanem csak kommutatív gyűrű.

– ($n\times n$-es mátrixok $\mathbb{R}$ felett, $+$, $\cdot$) vizsgálata:

(i) mátrixok összeadása kommutatív ✓

(ii) — || — asszociatív ✓

(iii) nullelem legyen a nullmátrix:

$$\underline{\underline{0}}=\begin{pmatrix}0&0&\cdots&0\\0&0&\cdots&0\\\vdots&&\ddots&\vdots\\0&0&\cdots&0\end{pmatrix} \quad ✓$$

(iv) additív inverz: $A\to -A$ ✓

~~(i')~~ mátrixszorzás nem kommutatív

(ii') — || — asszociatív ✓

(iii') egységelem legyen az egységmátrix:

$$E=\begin{pmatrix}1&&0\\&\ddots&\\0&&1\end{pmatrix} \quad ✓$$

~~(iv')~~ a 0 determinánsú mátrixoknak $\nexists$ inverze!

(v) disztributivitás teljesül ✓

emiatt ez csak gyűrű, egészen pontosan egységelemes gyűrű.
(mert a szorzásra nézve $\exists$ egységelem)

– az egész, vagy a valós együtthatós polinomok ($\mathbb{Z}[x]$, $\mathbb{R}[x]$) kommutatív gyűrűt alkotnak a szokásos pont. összeadásra, szorzásra nézve. Testet azért nem alkothatnak, mert pl. az x polinomnak az $\frac{1}{x}$ lehetne meg multiplikatív inverzének, de az $\frac{1}{x}$ nem polinom!

– a valós polinomok hányadosteste test: $\mathbb{R}(x) := \left\{\frac{p}{q} : p,q\in\mathbb{R}[x],\ q\neq 0\right\}$, a műveletek:

$\frac{p}{q}+\frac{r}{s}=\frac{ps+qr}{qs}$, ill. $\frac{p}{q}\cdot\frac{r}{s}=\frac{p\cdot r}{qs}$.

DEF.: R gyűrű nullosztómentes, ha $\forall a,b\in R$ esetén ha $a\cdot b=0 \Rightarrow a=0$ vagy $b=0$.

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

TÉTEL: $\forall$ test nullosztómentes

Biz.: $a\cdot b=0$ $\longrightarrow$ ha $a=0$ ✓

$\hookrightarrow$ ha $a\neq 0$: $a\cdot b=0$ $/\cdot a^{-1}$ balról

$\underbrace{a^{-1}\cdot a}_{1}\cdot b=\underbrace{a^{-1}\cdot 0}_{0} \Rightarrow b=0$ ✓

DEF.: A kommutatív nullosztómentes gyűrű neve integritási tartomány.

Példa: Az egész számok, a páros számok gyűrűje integritási tartomány.

$\mathbb{Z}_6$ nem integritási tartomány, mert pl. $2\cdot 3=0$ és $2\neq 0\neq 3$, tehát a 2 illetve a 3 nullosztók.

DEF.: $\mathbb{Z}_n$-nel jelöljük és <u>modulo n maradékosztályok gyűrűjének</u> nevezzük a $\mathbb{Z}_n = \{0, 1, 2, \dots, (n-1)\}$ halmazt a modulo összeadásra, ill. szorzásra nézve:

$a \oplus b := a + b \pmod n$

$a \odot b := a \cdot b \pmod n$

Példa: $\mathbb{Z}_{10}$-nél: $7 \oplus 8 = 5$, $7 \odot 8 = 6$

$2 \odot 5 = 0$, de a 2 és az 5 sem 0 $\Rightarrow$ $\mathbb{Z}_{10}$ nem nullosztómentes $\Rightarrow$ nem test.

TÉTEL: $\mathbb{Z}_n$ test $\iff$ n prím

biz.: $\Rightarrow$: tfh. n összetett: ekkor szorzattá alakítható az előző példához hasonlóan, vagyis $\mathbb{Z}_n$ nem nullosztómentes $\Rightarrow$ $\mathbb{Z}_n$ nem test! ↯

$\Leftarrow$: $n = p$ prím: (i), (ii), (iii), (iv) ✓

(i') ✓

(ii') ✓

(iii') ✓

(iv'): egyedül ez nem triviális:

$a \neq 0$, $a^{-1} := x$, $a \odot x = 1 \iff \underbrace{ax \equiv 1 \ (p)}_{\text{megoldható}} \iff \underbrace{(a, p)}_{=1 \text{ mert } p \text{ prím}} \mid 1$ ✓

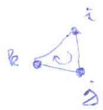
(v) ✓

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \subseteq ?$ $\longrightarrow$ a válasz: <u>kvaterniók</u>

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

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

$ij = k$, $jk = i$, $ki = j$ $\underbrace{(\text{de } ji = -k,\ kj = -i,\ ik = -j)}_{\text{tehát az már látszik, hogy nem kommutatív}}$



A kvaterniók ferdetestet alkotnak, mert:

(i), ..., (iv) ✓

~~(i')~~ nem komm.

(ii') ✓

(iii') ✓

(iv'): ha $x \neq 0$, $x^{-1} := \frac{1}{x} = \frac{1}{a + bi + cj + dk} = \frac{a - bi - cj - dk}{(a + bi + cj + dk) \cdot (a - bi - cj - dk)} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$

x konjugálttal bővítünk: $\bar{x} = a - bi - cj - dk$

a nevező most már valós ✓

(v) ✓

$\mathbb{Q} \subseteq \underbrace{\mathbb{Q}(\sqrt{2})} \subseteq \mathbb{R}$

$\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$

Ez is testet alkot, mert:

Könnyen látható, hogy ez is teljesíti az összes kritériumot, az egyetlen nemtriviális itt is az (iv') pont, vagyis a multiplikatív inverz: $(a + b\sqrt{2})^{-1} := \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \underbrace{\frac{a}{a^2 - 2b^2}}_{\in \mathbb{Q}} - \underbrace{\frac{b}{a^2 - 2b^2}}_{\in \mathbb{Q}} \cdot \sqrt{2}$ ✓

gyöktelenítés