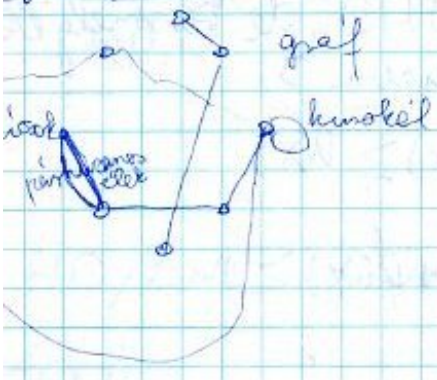
Wiener Mester visszatérést!
wiener@cs.bme.hu

7 Izh 8 pót
13 II 2h 14 pót

"Ez egy speciális igényeket kielégítő tárgy."

Gráfelmélet



nincs hurok-, párh. él => egyszerű gráf
teljes gr.: bármelyik 2 pont össze van kötve
fokszám $d(v)$
$\sum_{v \in V} d(v) = 2|E|$

összefüggő gr: bármely 2 pont között vezet
komponensek: maximális összefüggő részei a gráfnak.
elsorozat (séta) $(v_0, e_1, v_1, e_2, v_2, e_3, v_3, e_4, v_4)$
ha $v_0 \equiv v_4$ => zárt elsorozat
út: olyan séta, amiben $\forall$ pont max 1x fordul elő
kör: ...

Euler & Hamilton körök & utak

Def $G = (V, E)$ HO: olyan kör, ami $\forall$ csúcsot tartalmaz

D EO: (nem pont kör) olyan körséta, ami $\forall$ élet tartalmaz pontosan 1x
Hút: $\forall$ csúcsot tart.-ó út
Eút/séta: $\forall$ élet tart.-ó út/séta.

Szükséges felt.: of. (nem áll) /ha ez nem teljesül => $\nexists$ HO)
áll: G-ben $\exists$ HO => bármely k pontot elhagyva max k db komponens keletkezik.
áll: G ben $\exists$ Hút => $\forall$ k pontot elhagyva max $k+1$ komp. lesz.

Elégséges feltételek

Dirac-t.: G egyszerű gr és $\forall v \in V: d(v) \geq \frac{n}{2} \Rightarrow$ FHO (d-felt.)

Ore-t.: $\forall x,y \in V$ nem szomszédos pont: $d(x)+d(y) \geq n \Rightarrow$ FHO (Ore-felt.)

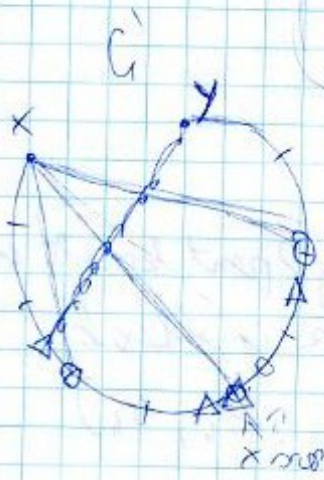
Ore **Biz:** indirekt: tfh: G telj. Ore-t és $\not\exists$ HO

$G \rightarrow G'$ – ben FHO, de bármely élt behúzva ↳.

$d'(x) \geq d(x)$

$\forall x \neq x$

$d'(x)+d'(y) \geq d(x)+d(y) \geq n$



Megfigyelés:

$d(y) \leq n-(d(x)+1)$

$\leq n-d(x)-1$

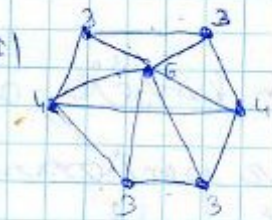
$d(x)+d(y) \leq n-1$ ↳

#06.09.12

Gyakorlat

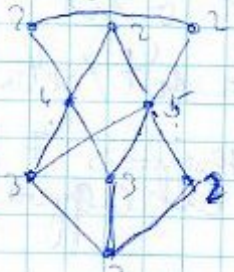
Bozóta Zsolt
NEEL@cs.bme.hu
cs.bme.hu/~neel

1) a)



csúcs: 7
él: 13
csúcsok fokszáma:

b)



csúcs: 9
él: 13

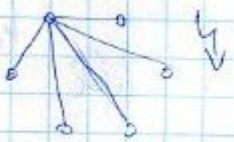
2) egyszerű gr:

a) 2 4 3 4 3 2
b) 3 2 4 4 3 2 3 ?
c) 6 2 1 3 4 2 ↳

a)

b)

c)



II. Előadás

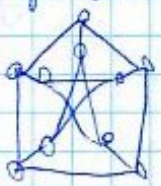
Zh

7. hét	okt 24.	kedd	18°°	IB028	I Zh
8. hét	~ 30.	kedd	~	IB028	I pót
13. ~	dec 4	kedd	~	~	II. Zh
14. ~	~ 11	~	~	~	II pót

Dirac $\Rightarrow$ Ore $\Rightarrow$ ZHO $\Rightarrow$ nincs

$\not\Rightarrow$ $\not\Leftarrow$

petersen-gr



G EO $\Leftrightarrow \forall$ fok ps + G öf

biz: G öf gr, $\forall$ fok ps. kéne: G benne EO

- veszünk egy maximális sétát (S)

(1) S körséta

tfh: Q kül $\Rightarrow$ 1 pontja be, aztán ki. ha a kezdőpont $\neq$ vp.

$\Rightarrow$ páratlan fokú lenne $\Rightarrow$ mivel G ps, ezért lehetne hozzátoldani élet $\Rightarrow$ S nem maximális ↯

(ha Q tartalmazná a gr. összes élét a séta, tovább lehetne menni a vp.-ból)

$\Rightarrow$ (2) A kpz.-ből menő összes élet S tart.

(3) A (2) $\forall$ pontra igaz

(4) S pontjai egy komponenst alkotnak

komp: max öf részek

részgr.

[$\forall$ él részgr]

- összes élet & pontot tart

↳ EO

Euler - vonal:

max 2 ptl fokú pont

(1) 0 ptl $\Rightarrow$ EO $\Rightarrow$ Eút

(2) 2 ptl fokú van

- összekötjük egymással $\Rightarrow$ EO $\Rightarrow$ Eút

Színezés, kromatikus szám

T — $T_1, T_2, \dots T_{100}$

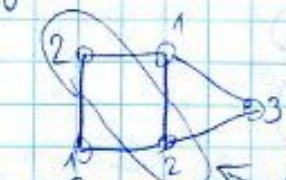
20 fő

$G = (V, E)$

$f: V \to \{1, 2, \dots r\}$

x színe, y színe

jó színezése G-nek, ha $x,y \in E \Rightarrow f(x) \neq f(y)$



$\chi(G) \geq 3$

(D) $\Leftarrow$ független ponthalmaz, $\Rightarrow X \subseteq V$

ha semelyik 2 csúcsa között nem vezet él.

(D) kromatikus szám: az a legkisebb k, hogy k színnel

$\chi(G)$ még lehet színezni a gr.-ot jól.

$\chi(K_n) = n$

(D.) klikkszám $\omega(G)$

legnagyobb teljes részgráf mérete

$\omega = 2$

$\omega = 3$

$\chi(G) \geq \omega(G)$

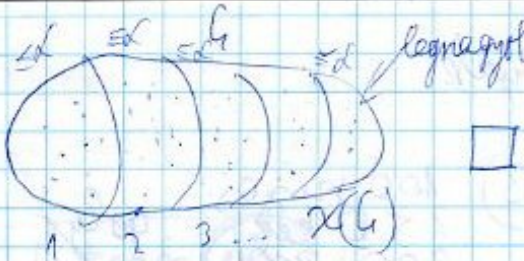
$\chi(C_{2k+1}) = 3$

(D) Max. független ponthalmaz mérete: $\alpha(G)$

$$\alpha(G) = \omega(\overline{G})$$

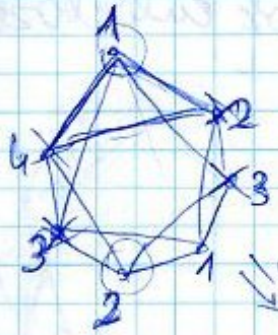
(all) $\chi(G) \cdot \alpha(G) \geq n \quad (= |V|)$

$\chi(G) \geq \frac{n}{\alpha(G)}$ $\Rightarrow$



egy jó színezés ↑

□



$\chi \geq \omega$
$\| \quad \|$
$3 \quad 3$

$\Rightarrow \alpha = 2$

$\chi \geq \frac{n}{\alpha} = \frac{7}{2} \Rightarrow \chi \geq 3{,}5$

$\chi \geq 4$

Mycielski - konstrukció

$G_3, G_4, G_5 \ldots$

$\forall k: \omega(G_k) = 2$

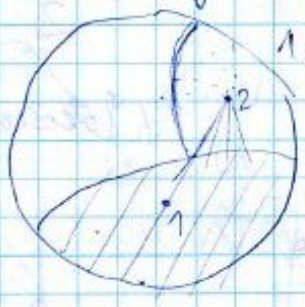
$\chi(G_k) = k$

$\chi(G) \equiv$ ~~kk~~ $(= |V|)$

$\Delta(G) =$ maxfok

(ttt): $\chi(G) \leq \Delta(G) + 1$

Bis: Mohó-alg.



$K_n \quad \Delta = n-1$

⊠

éles: teljes gr.
(legalább 3 hosszú) pll körök

Brooks-tétel: ha G összef., Δ-teljes, nem pll kör $\Rightarrow \chi \leq \Delta(G)$

11) Sakktábla mező $\Leftrightarrow$ gr. csúcsai
ott van él, amelyet bástyával elérhetők.

$\chi(G) = ?$

Az első sorhoz/oszlophoz mindenképp kell 8 szín, mert mindegyik szomszédos.

$\Rightarrow \omega \geq 8 \Rightarrow \chi(G) \geq 8$, ennyi elég is.

Folytatjuk a színezéseket 060925

$G_2, G_3, G_4 \dots$

$\chi(G) \geq \omega(G)$

$\forall k$: $\chi(G_k) = k$

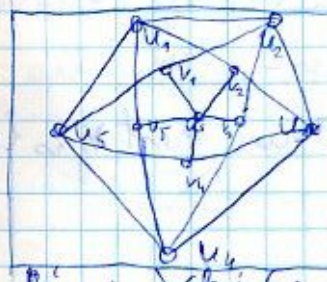
$\omega(G_k) = 2$ — G_2 G_3

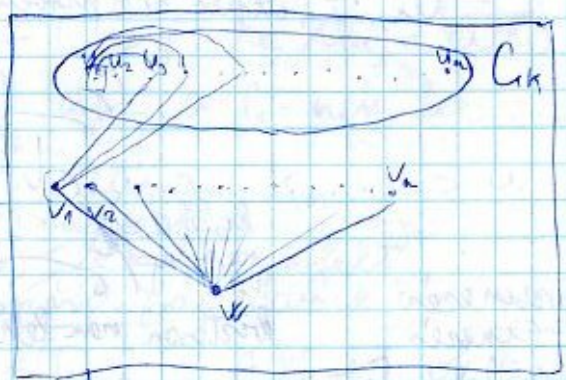
Mindet az előzőből kezdve létre $\Rightarrow$ Mycielski-konstrukció

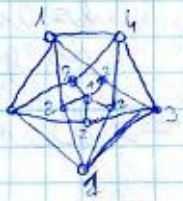
G_{k+1} létrehozása G_k-ból

v az összes v-vel

v_1-et pedig csak az u_1 szomszédjaival. (u_1-gyel nem)







Kéne: $\forall k$: G_k-ban $\not\exists \Delta$

ind. felt: G_k-ban $\not\exists \Delta$

Kéne: G_{k+1}-ben sincs

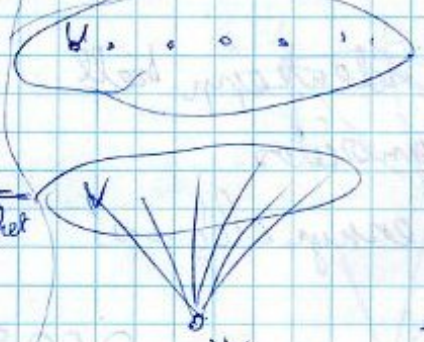
se u, se v sem szerepel Δ-ban
sőt, V-ben sem, mert nincs ilyen összekötve
$\forall$ ha Δ-ben lenne, az azt jelentené,
h. G_k-ban is van Δ. $\Rightarrow$

$\Rightarrow \omega = 2$

ind. felt.: G_k k-színezhető

kéne: G_{k+1} $(k+1)$-színnel

① eseket vizsgálni és kizárni*



V_{n_a}-kal szomszédos összes, egymással nem $\Rightarrow$ ugyanolyan szín $\Rightarrow$ $+1$ szín: W

$V_1 = U_1$ színe

$\Rightarrow$ $k+1$ ✓

nem színezhető 1-es

① W $+1$ színe: $\chi(G_k) \geq k$

ind. felt.: $\chi(G_k) \geq k$

kéne: $\chi(G_{k+1}) \geq k+1$

indirekt tfh: $\chi(G_{k+1}) \leq k$ $\Rightarrow$ színezhető k színnel

*: ha új színe ① $\Rightarrow$ legyen „új" színe azonos V_j színével. (amit nem lehet ①)

- olyan pontból: 2× változtattam $\Rightarrow$ 2 végpontot változtattam
- 1× ~
- 0× ~ itt nem lehet probléma, jó a szín

1-es voltak, de ez ↯ $\Rightarrow$ nem lehetett elő ✓

biztosan nem lehet ℓ a színe, mert V_j is ℓ lesz, $\Rightarrow$ ↯ ✓

és az új színezés is egy jó színezés $\Rightarrow$ ellentmondás, mert az jó színe ki:

$\chi(G_k) \geq k$ ← eredeti ind. felt, de ez jött ki:

$\chi(G_k) \geq k-1 \Rightarrow$ ↯

□

$\chi(G) \geq \omega(G)$

$\chi(G) \leq \Delta(G)+1$

Hogy nézhetek ki azok a gr.-ok, akkor $\chi = \omega$

$\omega = n$ Túl sok vizsgálandó

$\chi = n$

plusz elvárás: összes részgr.-ra is!
túl kevés

$\Rightarrow$ nem az összes, hanem csak a feszítő részgr.-okra!

$\omega \geq 5$
$\parallel$
$\chi \geq 5$

D: fesz. részgr.: H fesz. részgr.-ja G-nek, ha H csúcsai G csúcsai, H-nek, ott vesszük az összes szereplő élet be kell venni

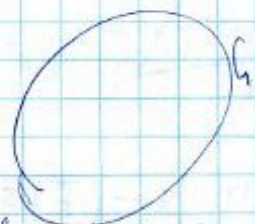
$V(H) \subseteq V(G)$ és $\forall$ G-beli él, ami H-beli pontok közt megy, szerepel

$\Rightarrow$ ilyen gráfok: **perfekt gráfok**

- G perf., ha $\chi(G) = \omega(G)$ $\forall$ olyan G'-re, ami a G-nek fesz. részgr.-ja.

- Perfekt gráfok: összes teljes gr. K_n $\Rightarrow \omega = n$, $\chi = n$ (üres gr. is perf.)
(összes feszített részgr.-ja)

áll: ha G-re $\chi(G) \leq 2 \Rightarrow G$ perfekt
$\Leftrightarrow$ páros gráfok (amik kirajzolhatók 2 színnel jól)



$\chi(G) = 2$
$\omega(G) = 2$

(APS gr.-ok fesz. részgr.-jai)

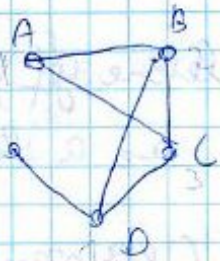
(Intervallumgráfok)

egy ivg. fesz részgr.-ja $\Rightarrow$ ivg.

tétel: $\forall$ ivg. perfekt

(1) $\checkmark$

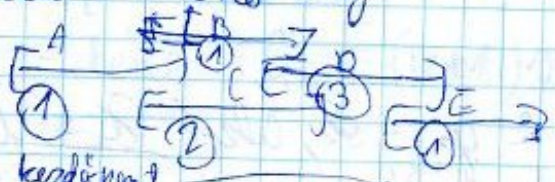
(2) ha G ivg., $\Rightarrow \chi(G) = \omega(G)$



$\omega = 3$
$\chi = 3$

Nem perf.:
$C_{2k+1} \geq 5$
fesz. részgráfként C_{2k+1} ezeknek komplementere

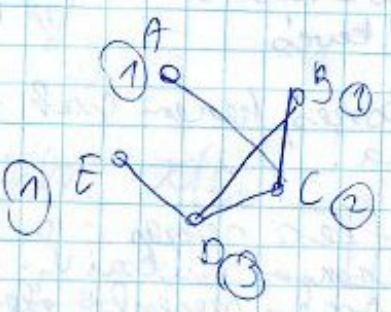
⇒ kiszínezése mohó alg:



sorbarakjuk kezdőpont szerint

ACBDE

színezésem: végigmegyek a pontokon és ún. színezek, h. a már már használt színnel, vele nem szomszédos színnel megszínezettekkel ..., akkorral, ami kisebb sorszámú pontjuk



tfh: $k \geq w+1$ szín kellett (vagy több)

Ω +1-re színezne

mert nem kaphatta az ①②..Ω színeket

mert valahol korábban kiszínezett ilyen pontok

$w+1$-es élek, de ilyen nem lehet, mert max w-s élek lehetek ⇒ ↯

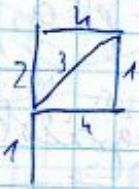
G perfekt $\Leftrightarrow$ $\overline{G}$ perfekt

1972 Lovász bizonyítás: perfekt gráf tétele

1960 Berge sejtés: ez az összes nemperfekt

Erős perfekt gráf tétel (3 éve)

Élek színezése



$\chi_e(G) \leq 4$

Def: G gr. élszínezése: $f: E \to \{1,2 \dots s\}$

~~$\forall e$~~ $\forall f$ szomsz. élekre $g(f) \neq g(e)$

Def: Elkromatikus szám: az a k, hogy k színnel élszínezhető a gráf (jól)

$\chi_e(G) \geq \Delta(G)$

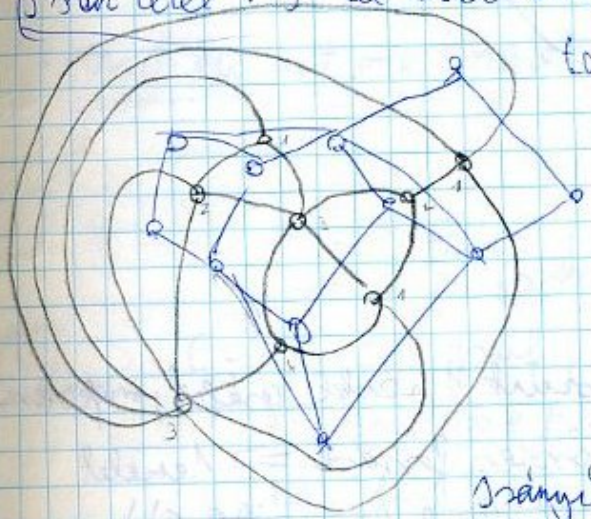
G egyszerű gr:

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

Síkbarajzolható gráfok színezése

körök rejtés ⇒ 4-szín tétel

(5-szín tétel : 5-ös tétel bizt.sán)



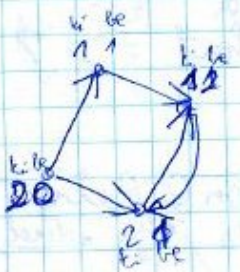
tartományszínezés ⇒ csúcsszínezés ✓

duális

$\boxed{G \text{ sík} \Rightarrow \chi(G) \leq 4}$ bizonyítás

[5-szín-t: bizonyítás: könyvből!]

Irányított gráfok



kifok: kimenő élek száma
befok: befutó ~

kifok = 0 ⇒ nyelő

befok = 0 ⇒ forrás

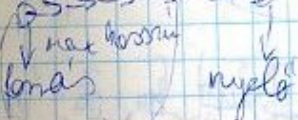
Def.: irányított kör:

acyclikus irányított gráfok: ha nincs benne irányított kör

áll: egy a.g.-ban ∀ kell forrás és nyelő is.

(csak véges gráfokra,) (nincs leghosszabb út!)

Biz: vegyünk egy leghosszabb irányított utat.

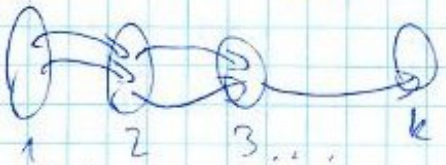


kezdőpontja forrás, végpontja nyelő

ha nem lenne forrás, akkor menne bele él, de nem mehet, mert akkor ~~nem~~ lenne kör

ha nem ~~lenne nyelő~~ ⇒ egy ~~egy~~ meglevőből jönne bele él ⇒ ~~el~~ 1-gyel hosszabb lenne ⇒ nem ~~nem~~ leghosszabb ugyanez.

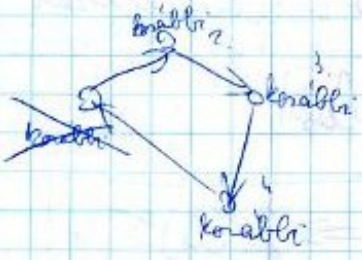
áll: ha G aciklikus $\Rightarrow$ csúcsok rétegekbe sorolhatók



él csak kisebb sorszámúból nagyobba mehet.

emeletekre bontás $\Rightarrow$ kör, be: igaz, $\exists$ emeletekre bontás!

fordítottja: $\exists$ e.l., $\Rightarrow$ G aciklikus ✓



$\Rightarrow$ triv ⇈

$\Leftarrow$

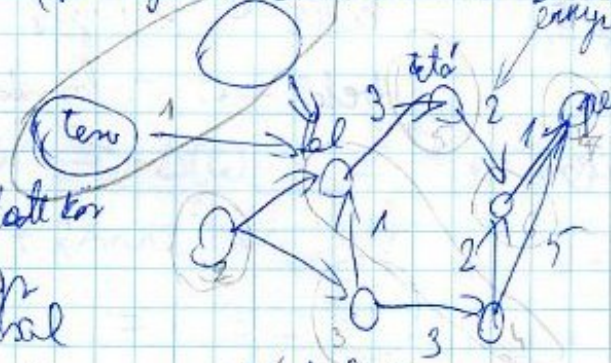
vesszük 1 aciklikus gráfot, megkeressük az összes forrást $\Rightarrow$ 1. emelet

$\Rightarrow$ ezeket kitöröljük. ($\Rightarrow$ aciklikus G')

$\Rightarrow$ vesszük az új forrásokat $\Rightarrow$ 2. emelet

$\Rightarrow$ rekurzió

PERT - módszer (Program Evaluation & Review Technique)

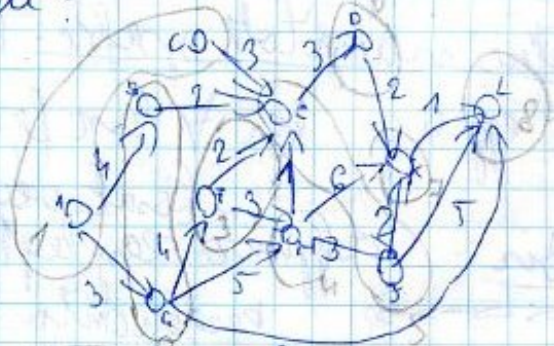


nem lehet irányítatlan $\Rightarrow$ aciklikus gr. élsúlyozásával

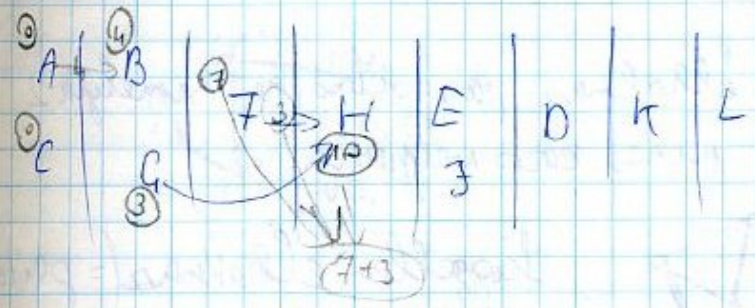
Mennyi idő kell?

$\Rightarrow$

1) emeletek
2) időpontokra bontom
   - megnézem kitől függ, és hogy mennyi a kezdési ideje
   max(kezd. idő + mi él értéke)
   $\Rightarrow$ nyelő lesz az (összes) szükséges idő



bármely kiegészítő él $\Rightarrow$ projekt késése



kritikus út módszere

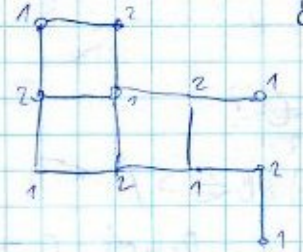
Páros gráfok és Párosítások

Def.: $G=(A,B)$ ps gráf, ha az összes csak A és B közt fut. (A és B-n belül nincsenek élek.)

Tétel: G ps $\iff \chi(G)=2$

Bis: A ① ≡ B ② ⇒ ✓

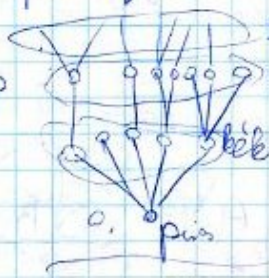
Tétel: Egy gr. akkor ps, ha nincs benne ptl. hosszú kör.

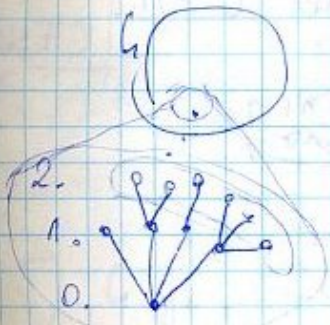


Bis: ⇒ : ha ptl kör lenne benne ⇒ $\chi \geq 3$ ⇒ ¬ps ↯ ✓

⇐

páros szintek: p
pél: kör





ha ∀ pontot lefed: jó, ha nem ⇒ ¬of

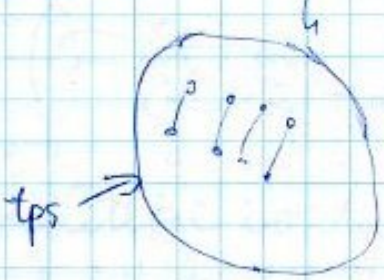
megfúrja

ha nincs ilyen
⇐
elég 2 szín

l -dik éle van a közös őstől
$k \geq l$ ($k=l+1$)
⇐ $k-l=$ páros

de! ⇐ $k+p=$ ps
találtunk egy ptl hosszú kört ⇒ ↯
(azonos paritású élnek kört nem lehet ír)

Párosítás



$E' \subseteq E$ élhalmaz párosítás, ha semelyik 2 élnek nincs közös végpontja.

független élhalmaz (= párosítás)

$\nu(G)$ = G-ben a maximális, független élhalmaz mérete

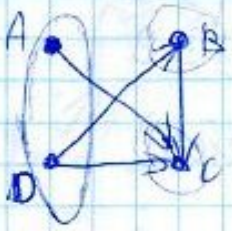
$\nu(G) = 3$

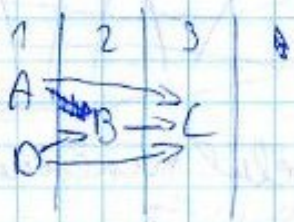
ha nincs nálánál nagyobb.

teljes párosítás:
ha $\forall$ csúcsot lefed.
- pl csúcsnál $\nexists$ tps.

Gyak

06 10 03





1)

$G: n \geq 3$, megszámozva ezeket RANDOM ; $\forall A, B: A \neq B$

a) $A \to B \iff A \mid B$

Emeletekre bontható?
$\Rightarrow$ van-e benne ~~kört~~ irányítási kör?
$\Rightarrow$ nem lehet, mert $A \mid B \iff A < B$, így
$A \to B$, $B \to C$, de nem lehet $C \to A$!

$A < B < C < D < E \not< A$

b) $A \nmid B \Rightarrow B \to A$ él. Emeletekre bontható?
(nem osztója)

HF 1

PS gráf

PSítás

061009

olyan élhalmaz, hogy semelyik 2 élnek nincs közös pontja.

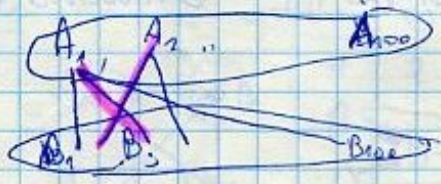
Most bánt támadják az amcsik.

munkatársak: $A_1, A_2, A_3 \dots, A_{100}$

részfeladatok: $B_1, B_2, \dots, B_{100}$

A_1: B_1, B_3, B_{100} ⇐ ezeket tudja csak.

[1 ember csak 1 feladaton dolgozhat.]



kérdés: ∃-e teljes psítás?

[ha nincs]

P_1 ∃ tps?

P_2 ∃-e A-t lefedő ps?

P_3 max. psítás mérete?

} algoritmus, ami megad TP-t, max ps-t

ezek 10 ember bármit megtud csinálni

$\chi'(G) = 90$

az első 50-et mindenki megtudja csinálni, a többit senki.

⇒ olyan él nincs, aminek se A_{10}, se B_{50}-ben nincs végpontja

lefogó ponthalmaz: igaz: ∀ élnek legalább az egyik végpontját tartalmazzák.

∃tp: |||||||| ⇐ 100 db, 100 pont kéne

⇒ legkisebb lefogó ponthalmaz mérete:

$\tau(G)$

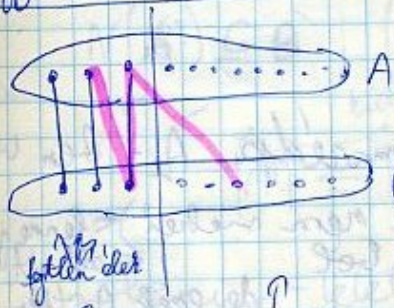
till: $\nu(G) \leq \tau(G)$

Biz:

09

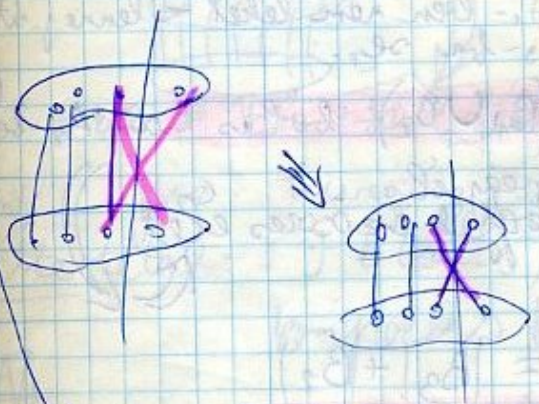
Tétel: G ps gr $\Rightarrow$ $\nu(G) = \tau(G)$ **König-tétel** [König Dénes]

Magyar-módszer: megtalálja egy ps gráf max. ps-itását.



Def.: **Alternáló út** (P ps-itásra nézve)
- P élei váltják egymást (fedetlen-ből indul)
- felváltva tartalmaz P-beli és nem P-beli élet

Def: **Javító út**: (P ps-itásra nézve)
fedetlen A-beli pontban végződő alternáló út.
- segítségével tudok csinálni egy 1-gyel nagyobb ps-ítást.



ps-t

(1) Keresünk egy valamelyik ps-ítást.
(2) Keresünk a p-re nézve javítóutat.
(3) Ha van j. út $\Rightarrow$ annak mentén javítunk
(P-beli és nem P-beli éleit kicseréljük)
$\Rightarrow$ a ps-ítás élszáma nőtt eggyel. GOTO (2)
(4) Ha nincs j. út $\Rightarrow$ STOP

[P3] antja

állítás: Ez talál 1 max ps-ítást.

Biz: (1) **áll.** Ha G-ben találunk k csúcsú lefogó ponthalmazt és k élű ps-ítást, akkor a ps-ítás max., a lefogó ponthalmaz pedig min. (=> a talált ps-ítás max.)

Biz: $\tau(G) \leq k$ $\quad \nu(G) \geq k$ $\quad \tau(G) \geq \nu(G)$

$\Rightarrow k \leq \nu(G) \leq \tau(G) \leq k$ ✓

$\Rightarrow \nu(G) = k = \tau(G)$ (+ König-t is kijött)

M. módszer végén: (Q-ja itt)

A_2: ide el tudunk jutni alternáló úton B_1-ből

A_3: maradék

B_2: B-ben fedetlen pont

(maradék A_3 párjai) (A_2 párjai)

$|P| = |B_2| + |B_3|$

tfh: • B_1 $\forall$ szomszédja A_2-ben van.

(A_1-be nem mehet) ⇐ lenne j. út
(se A_3-ból) ⇐ alt. út lenne, de ezek A_2-ben vannak

⇒

• B_2 $\forall$ szomszédja szintén A_2-ben van.

⇐ (A_1-ben nem lehet ⇐ lenne j. út)
(A_3-ba se ...)

⇒ $(B_1 \cup_{\text{unió}} B_2)$-ből is csak A_2-be megy él.

állítás: A_2 és B_3 együtt lefogják az összes élet.

⇒ $(A_2 \cup B_3)$ lefogó

⇒ $|B_3| + |A_2| = |B_3| + |B_2|$

⇒ tp ⇒ $\forall$ ps gráfban. ($\nu = \tau$, ezzel bizonyítva König)

$X \subseteq A$

$N(X)$: X szomszédsága

[P2] **Hall-tétel** $\exists A$-t fedő párosítás ⇔

$[\exists X:]$ $\forall X \subseteq A : |N(X)| \geq |X|$

$[\exists X \subseteq A : |N(X)| < |X|]$

$\nexists A$-t lefedő párosítás

⇒ Hall feltétel

Biz: $\nu(G) = \tau(G)$ (mert G ps gr.)

Kell: Hall-feltétel ⇒ $\exists A$-t fedő ps.; $\exists |A|$ méretű ps

$A' \cup B'$ min. lefogó ponthalmaz

kell: $\tau(G) \geq |A|$

$|A' \cup B'| \geq |A|$

$\nu(G) \geq |A|$

$\tau(G) \geq |A|$

$|A''| + |B'| \geq |A| \Rightarrow |B'| \geq |A| - |A'| = |A''| \Rightarrow |B'| \geq |A''|$

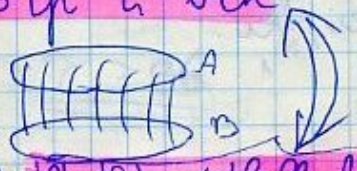
B'' szomszédai nem lehetnek A''-ben $\Rightarrow$ mindegyik A-ban van

$N(A'') \subseteq B$ (mert különben akkor nem lenne lefogó)

$A'' \sim$ kiválasztott $\Rightarrow |A''| \leq |N(A'')| \leq B'$ B'-ben ✓ □

{Pl} Frobenius-tétel

$\exists$ tp G-ben



kell: $|A| = |B|$ + áll felt. A-ra

Biz: triviális. □

/tét/ Jutte-tétel: $\exists$ k csúcs, amit elhagyva $\geq k$ ptl komponens keletkezik $\Leftrightarrow \nexists$ tp.

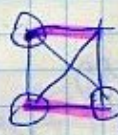
$\exists$ Tp $\Leftrightarrow \nexists$ k csúcs, amit elhagyva $> k$ ptl komponens keletkezik.

Gyak

G: $n \geq 3$ → számozva

$A \overset{*}{\rightarrow} B \Rightarrow B \rightarrow A$ Éreletek bonthatók-e?

ν (nű)	lefogó élek max. száma	
α (alfa)	lefogó csúcsok max száma	
β (bé)	lefogó élek min. száma	
τ (tau)	lefogó pontok min száma	



← lefogó élhalmaz

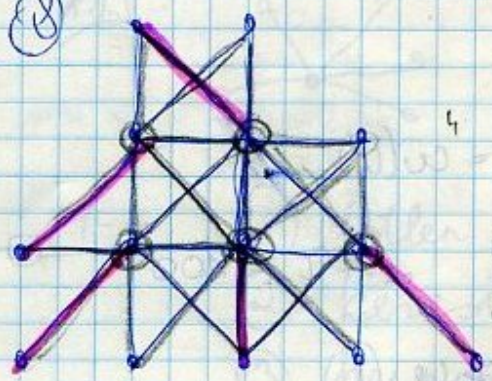
← lefogó ponthalmaz

Gallai azonosságok:

$\alpha + \tau = n$

$\nu + \beta = n$

8)



$\nu = ?$
$\tau = ?$

$\tau \geq \nu$

$\tau \geq 5$
$\nu \geq 5$

$\tau \geq \tau \geq \nu \geq 5$

$\nu = 3 = \tau$

$\nu = 3 = \tau$

Mi ?

HF4 r-reguláris ps gráf

↳ Biz. be: $\exists$ telj. psítás. $\forall d(v) = r$

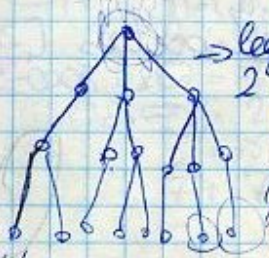
$k = 1$ tuti $k = 2$

Frobenius

$r = \frac{n}{2}$: $\exists$ benne $\frac{n}{2} - 1$ párosítás $\Rightarrow$ tp.

9) Biz. be, h. $\forall$ fa ps gráf és max 1 telj. psítás van benne.

↳ ptl $\Rightarrow$ 2 színnel színezhető $\Rightarrow$ ps. ✓



Ha van elsőfokú csúcs $\Rightarrow$ szomszédjával együtt kivesszük $\Rightarrow$ amíg el nem fogynak. Ha maradnak izolált pontok: $\not\exists$ tpsítás

06 10 16

Előadás

$\nu(G)$ – max. független élhalmaz
$\tau(G)$ – min. lefogó ponthalmaz
$\alpha(G)$ – max. független ponthalmaz
$\beta(G)$ – min. lefogó élhalmaz → Csak izolált pontmentes gráfokra

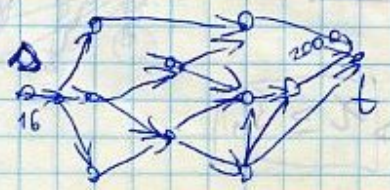
$\forall G$ gr.: $\nu(G) \leq \tau(G)$
G páros gr.: $\nu(G) = \tau(G)$

Gallai tételei:

$\nu(G) + \beta(G) = n$
$\alpha(G) + \tau(G) = n$

Biz: könyvből.

Hálózati folyamok



G irányított gr., $c, t, c: E \to \mathbb{R}^+$ (forrás, nyelő)

$\langle G, c, t, c \rangle$: hálózat

$f: E \to \mathbb{R}^+$ megengedett fv. (folyam) ha

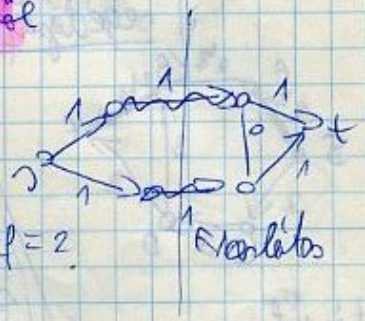
① $\forall e \in E: f(e) \leq c(e)$

② $\forall x \in V \setminus \{s,t\}$:

$$\sum_{\substack{e \text{ befut} \\ x\text{-be}}} f(e) = \sum_{\substack{e \text{ kifut} \\ x\text{-ből}}} f(e)$$

folyam értéke:

$$m_f = \sum_{\substack{e \\ s\text{-ből ki}}} f(e) = \sum_{\substack{e \\ t\text{-be befutó}}} f(e)$$



① max m_f = ?

② algoritmus, ami megtalálja max m_f-hez tartozó folyamot.

③ biz.: max?

Algoritmus max. folyam keresése & találása

Def. vágás: $X \subseteq V$ ponthalmaz; $s \in X$, $t \notin X$

$X \to (V \setminus X)$

X-ből $V \setminus X$-be menő élek = alkotnak egy vágást

$c(X) = X \to (V \setminus X)$ élek kapacitás összege.

↑ vágás kapacitása

$$c(X) = \sum_{\substack{e \\ X\text{-ből} \\ (V \setminus X)\text{-be} \\ \text{megy}}} c(e)$$

tétel: X tetsz. vágás, f tetsz. folyam $\Rightarrow c(X) \geq m_f$

$\min c(X) \geq \max m_f$

Tétel: (Ford-Fulkerson) max folyam = min vágás

tétel: $\exists$ a értékű f folyam és a kapacitású X vágás

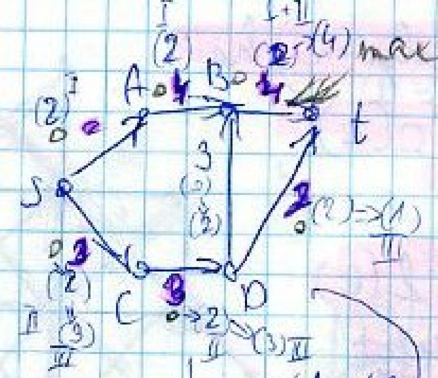
$\Rightarrow f$ max, X min.

Biz: $m_f = a$

$a = c(X)$; $\Rightarrow \max m_f \geq a$ $\quad a = \max m_f \leq \min c(X) \leq a$

$\min c(X) \leq a$

Alg.:



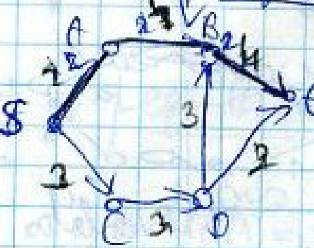
① f tetsz. folyam (azonosan nulla) ($f \equiv 0$)

② javítás, amíg lehet

③ ha nincs több jav ⇒ ∃ folyammal azonos értékű vágás

(1)

segédgráf

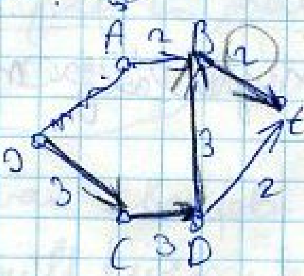


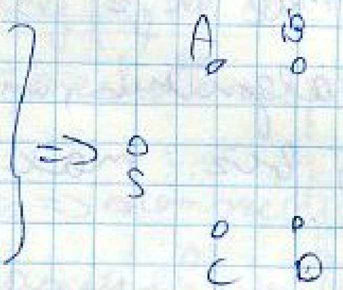
2 fajta él kerül bele:

① xy élet beletesszük, ha $f(xy) < c(xy)$; ráírjuk: $c(xy) - f(xy)$

② yx —— || —— $f(xy) > 0$, $f(xy)$

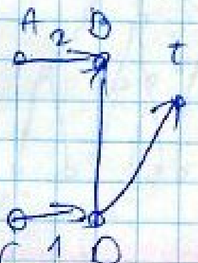
sg II.

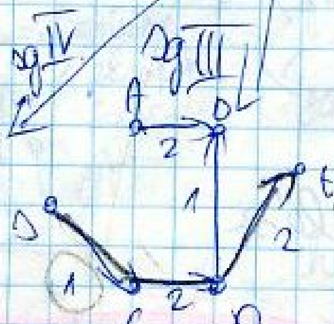




b) javító út s→t G'-ben

sg IV. sg III.

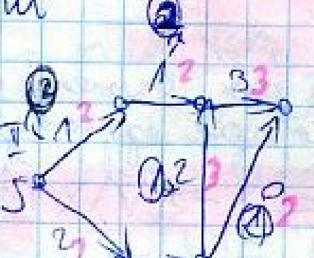




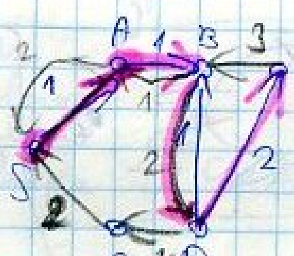
c) vesszük a j. út legkisebb élét és ezzel javítunk

⇓ ∅ több j. út

(2)



① típ. I, II



⇒ legkisebb: 1
⇒ ezzel javítható, eredeti úton +1, fordított úton −1!

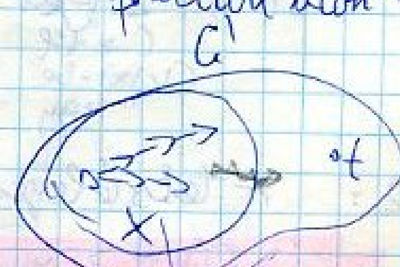
nincs j. út s→t : G'-ben

Áll: a kapott folyam maximális

Kéne: m_f kapacitású vágás

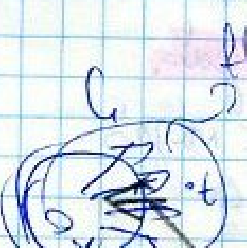
$f(e) = c(e)$ ∀ kilépő e-re

G'

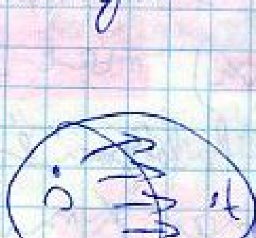


X-ből elérhető pontok
⇒ ez lesz a vágás

G



ezeken $f(e) = 0$



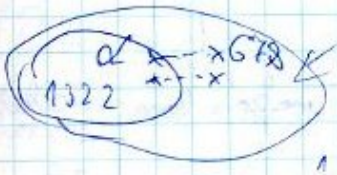
folyam. ki − folyam. be = m_f

Edmonds – Karp:

Ha mindig a legrövidebb j. út mentén javítunk, akkor polinomiális időben ($c \cdot n^3$) időben le fog futni az alg.
↳ az egész probléma kódolásának mérete

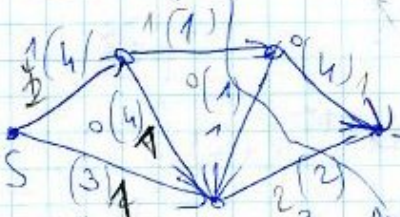
Gyak 061017

$n = 2000$
$\tau = 678$ ∅ tpr.
$d = n - \tau = 1322$



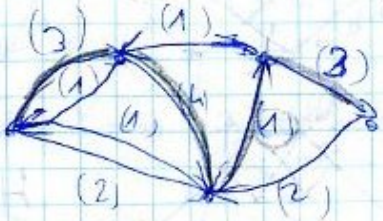
nem tudunk mindnek párt találni
⇒ ∄ tpr.

Folyam

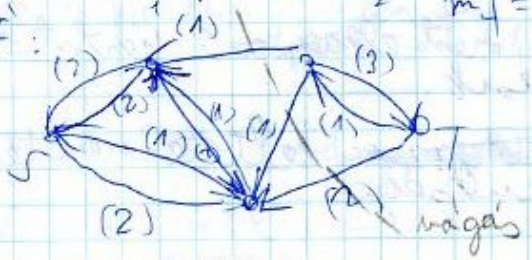


$|f| = 3$

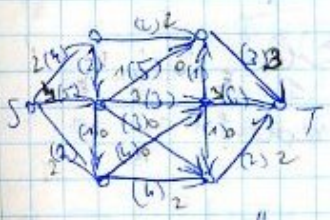
h_f:



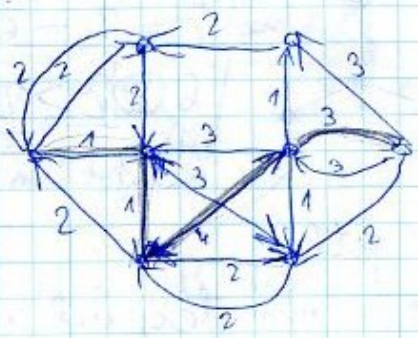
$h_{f'}$:

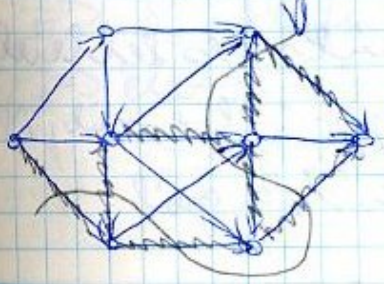


2-vel lehet többés
1-gyel lehet kevesebb.



⇒

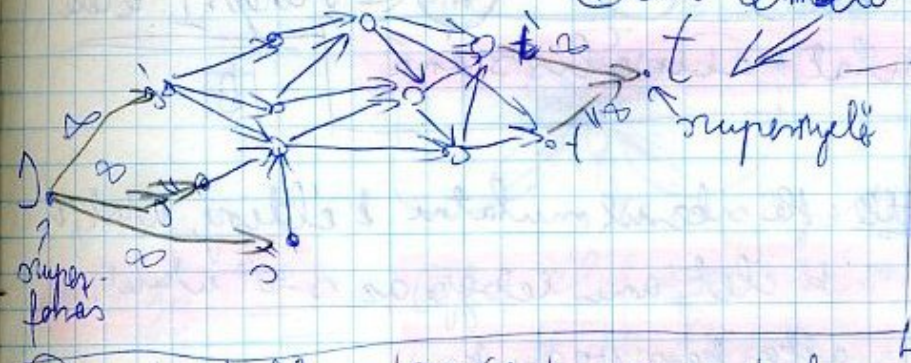


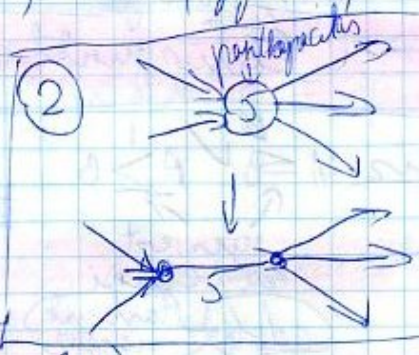


t folyamprobléma általánosítása

06.10.30

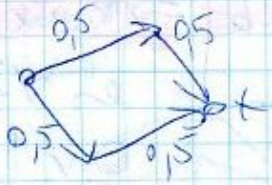
① több termelő, több fogyasztó





③ irányítatlan élek (bármely irányban mehet)

I. Egészértékűség - lemma:



- Ha egy hálózatban minden kapacitás egész ⇒ ∃ olyan max folyam, ami minden élen egész értéket vesz föl.

Biz.: Indulunk az azonosan 0 folyamból

[ts első segédgr.-ban csak egész számértékű élek lesznek] és mindig egésszel javítunk.

⇒ ez az alg. megadja a max folyamot. □

Többszörös összefüggőség & Menger-tételek

kitüntetett csúcsok

Def.: G irányított gr. s, t

Néhány élt **lefog** az s → t ir. utakat, ha őket elhagyva nem létezik s → t ir. út.

Def.: Néhány csúcs **lefogja** az s → t ir. utakat, ha ezeket a csúcsokat elhagyva már nem lesz s → t ir. út.

rendőrök :-)

T. s→t irányított utakat lefogó élek minimális száma [A]

[Hány rendű kell?] (VI) (II) ≤ Menger I. tétele

s→t éldiszjunkt irányított utak maximális száma [B]

Biz: A ≤ B ✓ A ≥ B

ezt kell belátni

adott — Hartyánk tétele

Fph: k=B él, ami lefogja

tfh: Ha sikerül mutatni k éldiszj. utat, és k élet, ami lefogja az s→t utakat, akkor kész vagyunk.

Biz: A ≥ k B ≤ k ≤ A □

G

∀ élre 1 a kapacitás

min. vágás = k ⇒ max folyam ≥ k (Ford-Fulkerson egészért. lemma)

és ∀ élen a folyamérték 0 v. 1.

T Menger II:

s-t-be menő irányítatlan éldiszj. utak max. száma = s-t-be menő irányítatlan utakat lefogó élek min. száma

Menger III: u. az, mint MI, csak él helyett pontok

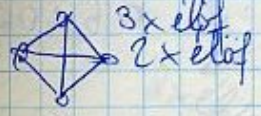
Menger IV: ~ MII ~

Bizonyítás: könyvben

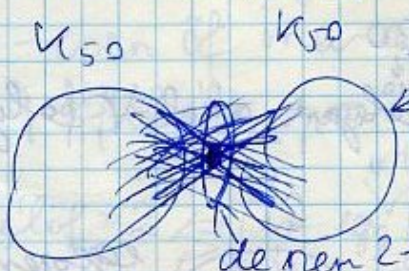
Def: Egy G gr. k-szorosan élösszefüggő, ha k-nál kevesebb élet elhagyva a gráfból, a gr. öf. marad (összefüggő)

Def: G k-szorosan (pont)összefüggő, ha (k-összefüggő)

- ① ha van legalább k+1 pontja
- ② ha k-nál kevesebb (bárhogyan) pontot elhagyva a gr. még öf. marad



k x-osan élő $\Rightarrow$ $(k-1)$ x-esen is élő



Δ x pont ő $\equiv$ ő

de nem 2-pontú.

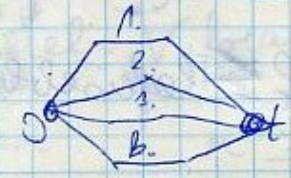
Menger V. G k-élő $\Leftrightarrow$ bármely 2 csúcsa között van k db éldiszjunkt út.

($\forall s,t \in V(G)$: $\exists$ k db éldisz. s-t út)

Menger VI. : G kx-pontő $\Leftrightarrow$ - $\geq k+1$ pontú és
- $\forall s,t \in V(G)$:
$\exists$ k db pontdisz. s-t út

$\Rightarrow$ **G k-pontő $\Rightarrow$ G k-élő.**

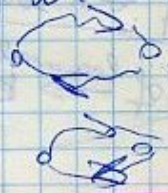
Biz: $\Leftarrow$:



$\Rightarrow$: kéne: s,t között $\exists$ k éldisz. út
s-t éldj. utak száma = s-t utakat lefogó élek min. száma
kéne: az s-t utakat nem lehet lefogni $k-1$ éllel.

Áll: G 2-ő $\Leftrightarrow$ bármely ($\forall$) 2 pontján át megy kör.

biz.: $\exists$ 2 pontdj út $\Rightarrow$ kör
pontdj $\Rightarrow$ egyetlen pont sem ismétlődik $\Rightarrow$ kör



$\Leftarrow$

□

Dirac-tétel: G k-ő $\Rightarrow$ bármely k pontján át vezet kör.

biz: Ø

Gráfok bejárási, gráfok ábrázolásai

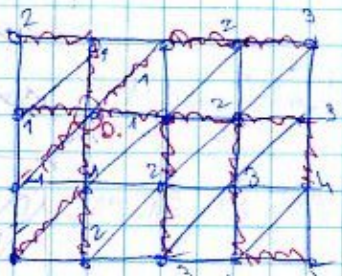
06.11.06

Breadth first search (BFS)
szélességi keresés

Def. Feszítőfa

G-nek T feszítőfája
ha: - T részgráfja G-nek
- T a G összes csúcsát tartalmazza
- T fa

áll: G-nek T feszfája $\Leftrightarrow$ G ö.f.

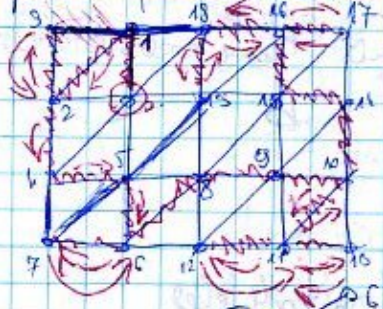


$\sum d(v) = 2 \cdot e$

meglátogatás sorrendje = szomszédok száma

szomszédok látogatása $\Rightarrow$ látogatottan $\Leftarrow$ 1. szint

Mélységi keresés,
DFS = Depth first search



DFS-fa

elindulunk valamerre, addig megyünk, amíg tudunk (amíg van olyan csúcs, ahol még nem jártunk)
ha nincs, akkor vissza egyet (az apjába)

3 a 2-nek a gyereke
2 a 3 szülője
5 a 2-nek a leszármazottja
2 az 5-nek az őse
6 és 5 között semelyik irányban nem áll fenn

áll: T a G-nek DFS-fája, $\Rightarrow$

$\forall e \in E(G) \setminus E(T)$

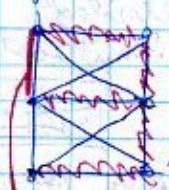
$e = (x, y)$ ahol x az y őse (vagy fordítva)

Biz:

Kell: nem létezik olyan él amelynek az egyik végpontja az őse a másiknak (kulcsfontosságú)

Tfh: T nyílt ágban nem léphettünk vissza, amíg tovább nem mentünk minden lehetséges csúcsba

alapfeltevés: $\forall$ körben legyen olyan él, ami a többiben nem lehet benne



$\star$ élek $\geq n - 1 + r$

$e \geq n - 1 + r$

$r \leq e - n + 1$

Ha behúzunk 1 élet $\Rightarrow$ +1 kör

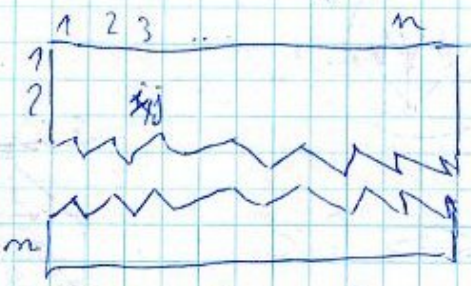
$e - (n-1) = e - n + 1$ kört kaptam

- mélységi keresés, amikor kereszttől visszalépve megtaláltuk a kört.

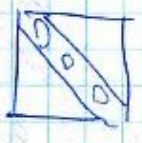
Gráfok ábrázolásai

1) szomszédsági mx

- $G = (V, E)$ $|V| = n$ n-csúcsú gráf



$$A_{ij} = \begin{cases} 0, & \text{ha } i \text{ és } j \text{ nincs összekötve} \\ k, & \text{ha } \sim \text{ közt van } k \text{ db } (i \neq j) \text{ különböző élből} \\ l, & \text{ha } i = j \text{ és } l \text{ hurokél illeszkedik rá} \end{cases}$$



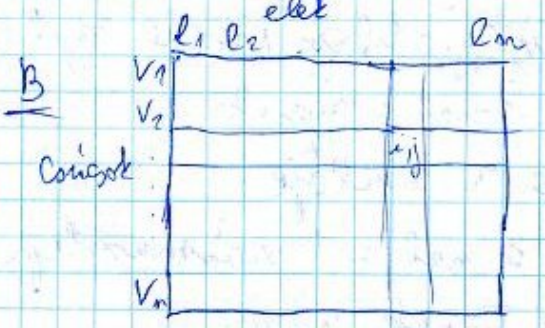
egyszerűség. $\Rightarrow$ főátlója csupa 0

$A_{ij} = A_{ji}$, szimmetrikus mx

T: $(A^2)_{ij}$ = i és j közti 2 hosszú elsorozatok száma (hány közös szomszédjuk volt)

$(A^k)_{ij}$ = $\sim$ k $\sim$

2. Illeszkedési mx



irányított élek

$$B_{i,j} = \begin{cases} 0, & \text{ha } v_i \text{ nem illeszkedik az } e_j\text{-re} \\ 1, & \text{ha az } e_j \text{ } v_i\text{-ből indul} \\ -1, & \text{ha az } e_j \text{ } v_i\text{-be fut be} \end{cases}$$

Minden oszlopban 1 db 1-es, 1 db -1-es és egy csupa 0

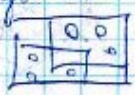
$\Rightarrow$ inkább elvi jelentősége van

T: G gr. c db komponenssel

$\Rightarrow$ $B(G)$ mx rangja $n - c$.

vezér egy tetszőleges irányításával

$r(B(G)) = n - c$ $\quad n = |V|$



Bizonyítás: könyvből ← nem nagyon bonyolult, kell a szép jegyzet

- **Vágás-mx, Körmx** ← könyvből (bizonyításokat itt nem magyarázom el)

nem egyértelműen határozzák meg a gráfot

- **élliste** – egy tömbben felsoroljuk a csúcsokat, mindhez megadjuk, mik a szomszédai (sorrendben)

/leghasznosabb/

< end of gráfelmélet >

< begin of számelmélet >

$\mathbb{N} = \{0, 1, \dots\}$

$a \mid b$ – a osztja b-t, b többszöröse a-nak, ha $\exists k \in \mathbb{N}$:

$k \cdot a = b$

Def: **prím**: pontosan 2 osztója van (1 nem prím!)

$a \mid a \quad a \mid 1 \Rightarrow a = 1 \cdot a$

2, 3, 5, 7, 11, 13, 17, 19, 23, 29,

‡ **Számelmélet alaptétele:**

$\forall$ pozitív egész felírható (sorrendtől eltekintve) egyértelműen prímek szorzataként.

$30 = 2 \cdot 3 \cdot 5 \; (= 3 \cdot 5 \cdot 2)$

Biz: ☹

I kanonikus alak / prímtényezős felbontás

Mire jó ez:

(1) $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot p_3^{\alpha_3} \dots p_r^{\alpha_r} \quad \alpha_i \geq 1$

osztók meghatározása $p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_r^{\beta_r} \quad \alpha_i \geq \beta_i \geq 0$

(2) osztók számának meghatározása

$d(n) = n$

$d(30) = 2 \cdot 2 \cdot 2 = 8$ $\quad (2^1 \cdot 3^1 \cdot 5^1)$

$d(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \dots \cdot (\alpha_r + 1)$ ($\beta_1, \beta_2, \beta_r$: lehetőség)

30: pl sok osztó

36: ptl sok osztó

1·36, 36·1, 2·18, 3·12, 4·9, 6·6

LNKO, LKKT

$a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$

$b = q_1^{\beta_1} \dots q_s^{\beta_s}$

közös prímtényezők, kiselőbbkitevőn LNKO

$30 = 2 \cdot 3 \cdot 5$

$110 = 2 \cdot 5 \cdot 11$

$2 \cdot 5 = 10$

összes ~ nagyobb ~ LKKT

$2^2 \cdot 3 \cdot 5 \cdot 7 = 420$

(3) a, b ptl $\quad (a^2+b^2, 4) = ?$ — 5-tel 3 maradékot ad: $5k+3$

$a^2+b^2 \mid 2$

$4 = 2^2$

$a = 2k+1$
$b = 2l+1$

$(2k+1)^2+(2l+1)^2 = 4k^2+4k+1+4l^2+4l+1 = 4k^2+4k+4l^2+4l+2 = 4(k^2+k+l^2+l)+2$

$= 2(2(k^2+k+l^2+l)+1)$

1, (2), 4

4 nem lehet, mert 2 maradékot ad

2 lehet $\Rightarrow (a^2+b^2, 4) = 2$

$4m+2 \Rightarrow$ 4-gyel 2 maradékot ad

HF1 a, b, c relatív prím ($lnko = 1$) $\not\Rightarrow$ ebből következik-e: páronként is rel. prímek?

HF2 $b \mid a \quad (a, a+b) = ?$

$a, b \in \mathbb{Z} \quad (2a, a-b) = ?$

HF3 $(a; 4) = (b; 4) = 2$

$(a+b, 4) = ?$

$a \sim 10^{55}$
$b \sim 10^{55}$ $\sim 10^{50}$ lépés

OG1115

Euklideszi algoritmus

$lnko(a, b) = ?$

Def: maradékos osztás — maradék

$a : b \qquad a = x \cdot b + r \qquad 0 \le r < b$

$85 : 12 \qquad 85 = 7 \cdot 12 + 1$

$a > b$

$a : b \quad a = x_1 \cdot b + r_1 \quad 0 \le r_1 < b$
$b : r_1 \quad b = x_2 \cdot r_1 + r_2 \quad 0 \le r_2 < r_1$
$r_1 : r_2 \quad r_1 = x_3 \cdot r_2 + r_3 \quad 0 \le r_3 < r_2$
$\vdots$
$r_{k-1} : r_k \quad r_{k-1} = x_{k+1} \cdot r_k + r_{k+1}$
$r_k = x_{k+2} \cdot r_{k+1} + r_{k+2} \quad (r_{k+2} = 0)$

$r_{k+1} \Rightarrow lnko$

$lnko(240, 72) = ?$

$240 = 3 \cdot 72 + 24 \Rightarrow 72 = 2 \cdot 24 + 24$
$24 = 1 \cdot 24 + 0$

$72 = 2 \cdot 24 + 24$
$24 = 1 \cdot 24 + 0$

$72 = 3 \cdot 24 + 0$
$24 = 1 \cdot 24 + 0$

$24 = lnko$

Biz: (Euklideszi alg. helyessége)

① $r_{k+1} \mid a$

$r_{k+1} \mid b$

$r_k : r_{k+1} \Rightarrow r_k = x_{k+2} \cdot r_{k+1} + r_{k+2}$

$\Downarrow$

$r_{k+1} \mid r_k \Rightarrow r_{k-1} = x_{k-1} \cdot r_{k-2} + r_{k-1}$

$r_{k+1} \mid r_{k-1} \Rightarrow r_{k-2} = x_{k-2} \cdot r_{k-3} + r_{k-2}$

$\vdots$

$r \mid r_1$

$r \mid r_2$

$r \mid r_3$

$r \mid r_{k+1}$

② r_{k+1} a legn. K.O.

$r \mid a, r \mid b \Rightarrow r \leq r_{k+1}$

$\Downarrow$

lépések száma $\leq 2 \log_2 a$

$a \sim 10^{99} \rightarrow 2 \log_2 10^{99} \approx 10^3 \leq 10^{10}$

$10^{99} = (10^3)^{33} < 2^{330}$ (660)

□

Prímszámok

tétel: végtelen sok prím létezik

Biz: indirekt: csak végesen sok van

tfh: $p_1, p_2, \dots p_n$ az összes prím

$N = \sum_{i=1}^{n} p_i + 1$ ⇐ N nem osztható p_1-gyel, se p_2 ... p_n-nel se

$\Rightarrow$ ha ez az összes szám, akkor az N nem lehetne prím

Ha nem prím, akkor van olyan prím osztója ami itt nem szerepel $\Rightarrow$ ↯

□

2, 3, 5, 7, ...

tétel: (Léteznek bármekkora hosszúságú sok az egymás egyenesen, amelyben nincs prím)

$\exists$ 100 egymást követő nemprím szám

$n!$

2-vel osztható $\rightarrow$ 101! + 2

3-mal

$\vdots$

101-gyel | 101! + 101

} 100 db $\Rightarrow$ olyan szám.

$(n-1)! + 2$

$\vdots$

$(n-1)! + n-1$

} n db

Csebisev-tétel: $n > 1$

n és 2n között mindig van prím.

biz: ◻

ikerprímek: különbségük 2

pl. 3,5 ; 11,13 ; 29,31 ; 35

sejtés: ∞-sok ikerpr. van.

(Nagy) prímszámtétel

$\pi(n)$ = n-nél kisebb-egyenlő prímek száma

$\pi(7) = 4$ (2,3,5,7)

$\pi(n) \sim \frac{n}{\ln n}$ nagyságrendű.

$\left(\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1\right)$

T Goldbach-sejtés:

$\forall$ (2-nél nagyobb) páros szám előáll 2 prím összegeként.

kongruenciák

Def: $a, b, m \in \mathbb{Z}$

$a \equiv b \pmod m \iff m \mid a-b$ (m osztja $a-b$-t)

pl: $7 \equiv 17 \pmod 5$

$24 \equiv 35 \pmod{11}$

Tulajdonságok

≡ ekvivalenciareláció

1. reflexív $a \equiv a \ (m)$
2. szimmetrikus (ha $a \equiv b \ (m) \Rightarrow b \equiv a \ (m)$)
3. tranzitív $\left.\begin{matrix} a \equiv b \pmod m \\ b \equiv c \pmod m \end{matrix}\right\} \Rightarrow a \equiv c \ (m)$

$m \mid a-b$, $m \mid b-c$ $\Rightarrow m \mid a-c$, $a \overset{II}{\equiv} c \ (m)$

$(\bmod 5)$

$-9 \equiv -4 \equiv \overset{0}{1} \equiv 6 \equiv 11 \equiv 16$

$\begin{matrix} 2 \\ 3 \\ 4 \end{matrix}$

$a \equiv b \ (m)$, $c \equiv d \ (m)$ $\quad m \mid a-b$, $m \mid c-d$ $\rightarrow$

áll: ① $a+c \equiv b+d \ (m)$ $\quad m \mid (a+c)-(b+d)$ ✓

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

③ $ac \equiv bd \ (m)$ $\quad m \mid (c-d)$, $m \mid b(c-d)$

④ $a^k \equiv b^k \ (m)$ $\quad m \mid ac - bc + bc - bd$ ✓

(4). hármas alapján ✓

999^{2006} utolsó 3 számjegye?

⇓

1000-rel osztva mit ad

?

$\pmod{1000} \Rightarrow 999 \equiv -1 \pmod{1000}$ (4)-es trükk

⇓

$999^{2006} \equiv (-1)^{2006} \pmod{1000}$

$\Rightarrow 1 \Rightarrow \boxed{001}$

$35 \equiv 21 \pmod{14}$ /:7

$5 \equiv 3 \pmod{14}$

⇓

$5 \equiv 3$ (2)

all. $ac \equiv bc \pmod{mc}$ ⇓ $a \equiv b \pmod{m}$

$\Rightarrow mc \mid ac - bc$

$\Rightarrow \exists k : k \cdot mc = ac - bc$

$\Rightarrow m \mid a - b$

all: $ca \equiv cb \pmod{m}$

⇓

$a \equiv b \pmod{\frac{m}{(m,c)}}$ ← Euklid (m,c)

Biz: $m \mid ac - bc = c(a-b)$

$(m,c) = d$

$m = m' \cdot d$

$c = c' \cdot d$

$m'd \mid c'd(a-b)$

$\Rightarrow \exists k : k \cdot m'd = c'd(a-b)$

$k \cdot m' = c'(a-b)$

$(m', c') = 1$

$\Rightarrow m' \mid c'(a-b) \Rightarrow m' \mid a-b$

$a \equiv b \pmod{m'}$

T: $ca \equiv bc \pmod{m}$ és $(m,c) = 1 \Rightarrow a \equiv b \pmod{m}$

Diofantikus egyenletek

80 tallér

18 tallér

$a \cdot 80 + b \cdot 18 = 1000 \quad a, b \in \mathbb{Z}$

$18b = 1000 - 80a \Rightarrow 80a \equiv 1000 \pmod{18}$

$2a \equiv 2 \pmod{18}$ $\left(\frac{18}{(18,40)} = 9\right)$

$-2 \equiv 2a \pmod{9}$

$2a \equiv -2 \pmod{9}$

$a \equiv -1 \equiv 8 \pmod{9}$

$80 \cdot (9k+8) + 18b = 1000 \Leftarrow a \equiv 9k+8$

$\Rightarrow b \equiv \ldots$

$720k + 640 + 18b \equiv 1000$

$720k + 18b = 360 \quad / :18$

$40k + b = \frac{360}{18} = 20$

$b = 20 - 40k$

pl. $k = 0$

$a = 8$

$b = 20$

6 $x \equiv 2 \ (3) \overset{?}{\Rightarrow} x \equiv 5 \ (6)$

$x = 3k+2$ $\qquad$ $x = 6\ell+5$

	1	2	3	4	5	6
(3)	1	2	0	1	2	0
(6)	1	✗	3	4	5	0

$3k+2 = 6\ell+5$

$3k = 6\ell+3$

$k = 2\ell+1$

ellenpélda: $x=2$ $\qquad$ $2 \equiv 2 \ (3) \Rightarrow \not\equiv 5 \ (6)$

7 $14x \equiv 7 \ (21) \ /:7 \quad (21,7) = 7$

$2x \equiv 1 \ (3)$

$4x \equiv 2 \ (3)$ $\quad$ v. $\quad -1x \equiv 1 \ (3)$

$x \equiv 2 \ (3)$ $\quad$ $x \equiv -1 \equiv 2 \ (3)$

$\Rightarrow$ visszaírás $\boxed{x \equiv 2, 5, 8, 11, 14, 17, 20} \Rightarrow$ 7 db mo.

HF3 $ax \equiv 3 \ (21)$ $\quad a = 7; 8; 9$ lehet

HF4 11863, 10839 3 db egymást követő kettő hatvánnyal osztva azonos maradékot ad.

$\Rightarrow$ melyik hatványok ezek?

Előadás $\qquad$ 06.11.20

1, 2, 3, 4, 5, ... $\quad \infty$ sok prím

1, 3, 5, 7, 9, ... $\quad$? ~ -"-

1, 5, 9, 13, 17, ... $\quad$ 2 ~ -"-

3, 7, 11, 15, 19, ... $\quad$? ~ -"-

(2), 4, 6, 8, 10, ... $\quad \infty$ sok prím

4, 10, 16, 22, ... $\quad$ -"- $\Rightarrow$

15, 21, 27, 33, 39, ... $\quad$ -"- $\Rightarrow$

kezdőtag, differencia

$\boxed{a + k \cdot d}, \ (a,d) = 1$

$\Rightarrow \infty$ végtelen sok prím a sorozatban

T $\Rightarrow$ **Dirichlet-tétel:** Legyen $(a,d) = 1 \Rightarrow$ az $a, a+d, a+2d, a+3d, \ldots$ számtani sorozatban ∞ sok prím van.

$ax \equiv b \ (m)$ $\quad a, b, m$ rögzítettek

$x = ? \quad \Rightarrow x \equiv ? \ (m)$

Ha b nem osztja (a,m)-et $\Rightarrow \not\exists$ mo.

$b \nmid (a,m)$

$\exists$ mo $\Leftrightarrow b \mid (a,m)$

biz: $\Rightarrow$ ✓

$\Leftarrow$: 1: definiáljunk néhány fontosabb alaptulajdonságot

Def: teljes maradékrendszer mod m:

$\{a_1, a_2, \dots a_m\}$ t.m.r. mod m, ha

1) $a_i \not\equiv a_j \pmod m$, ha $i \neq j$ (inkongruens)

(2.) számuk m (db)

pl: $\{1,2,3,4,5\}$ mod 5 ⇐ ez egy jó t.m.r.

$\{11, 22, -7, 4, 105\}$ mod 5

1 2 3 4 0

Def $\varphi(n)$ (redukált maradékrendszer-hez)

$\varphi : \mathbb{N} \to \mathbb{N}$ az n-hez képest relatív prímek száma

$1, 2, 3, \dots, n-1$ (közül hány relatív prím n-hez)

pl.: $\varphi(10) = ?$

$1, 2, 3, 4, 5, 6, 7, 8, 9 \Rightarrow \varphi(10) = 4$

$\varphi(29) = 28$ prímszám ⇒ mindkettő rel. prím

$1, 2 \dots 28$

$\varphi(p) = p - 1$ $\forall$ prímszám esetén

Def Redukált maradékrendszer mod m

$\{a_1, a_2, \dots a_{\varphi(m)}\}$ r.m.r. mod m, ha

1.) $a_i \not\equiv a_j \pmod m$, ha $i \neq j$

2) $(a_i, m) = 1$ $i = 1, 2, \dots \varphi(m)$

(3) $\varphi(m)$ db van belőlük

pl.: $\{1, 3, 7, 9\}$ r.m.r. (10)

$\{-9, 13, 37, 109\}$ — " —

Áll: teljes m.r.-t tartalmaz redukált m.r.-t.

biz: def-ből

Áll: $(x, m) = 1 \Rightarrow (y, m) = 1$

$y \equiv x \pmod m$

Biz: $m \mid y - x$

triviális

Áfh: $(y, m) \neq 1 \Rightarrow \exists d \mid y$ és $d \mid m$ $(d > 1)$

$\Leftrightarrow m \mid y - x \Rightarrow d \mid y - x$

1. Lemma $\{a_1, a_2, \dots a_m\}$ t.m.r. mod m, $x \in \mathbb{Z}$
$\Rightarrow \{a_1+x, a_2+x, \dots a_m+x\}$ is t.m.r.

Biz: $a_i + x \not\equiv a_j + x \pmod m$
$a_i \not\equiv a_j$ ✓ (m)

2. Lemma $\{a_1, a_2 \dots a_m\}$ t.m.r. (m), $c \in \mathbb{Z}$, $(c, m) = 1$
$\Rightarrow \{ca_1, c \cdot a_2 \dots ca_m\}$ is t.m.r. (m)

pl: $\{1,2,3,4,5\}$ $c = 7 \pmod 5$ Biz: ugyanúgy
$\{7, 14, 21, 28, 35\}$
2 4 1 3 0 ✓

$ca_i \not\equiv ca_j \pmod m$ $i \neq j$
$a_i \not\equiv a_j \pmod m$ ✓
$(m, c) = 1$
tfh: $c \cdot a_i \equiv c \cdot a_j \pmod m$
$\Downarrow$
$a_i \equiv a_j$ ↯

3. Lemma: $\{a_1, a_2, \dots a_{\varphi(m)}\}$ r.m.r. (m) és $c \in \mathbb{Z}$ $(c, m) = 1$
$\Rightarrow \{c \cdot a_1, c \cdot a_2, \dots c a_{\varphi(m)}\}$ is r.m.r. (m)

Biz: 1. ✓
3 ✓ lettek
2. ✓ lesz

1) $\varphi(p) = p - 1$, ha p prím
2) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ —11—
$1, 2, \dots p, \dots 2p \dots, p^\alpha$ kihúzod: $\frac{p^\alpha}{p} = p^{\alpha-1}$
nem kihúzott $p^\alpha - p^{\alpha-1}$

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}$

$\Rightarrow$ **Tétel**: $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
ha $(a, b) = 1$ ⇐ multiplikatív függvény

Most: $a = p_1^{\alpha_1}$ $n = a \cdot b$
$b = p_2^{\alpha_2} p_3^{\alpha_3} \dots p_r^{\alpha_r}$ $\varphi(n) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) =$
$= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot \varphi(b) =$
$\varphi(a)$
$= (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \dots (p_r^{\alpha_r} - p_r^{\alpha_r-1}) =$
$= \boxed{n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)}$

$\varphi(1500) = ?$

1500	2
750	2
375	3
125	5
25	5
5	5
1	

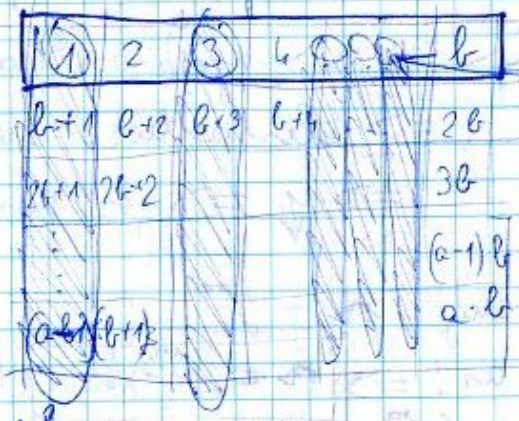
$1500 = 2^2 \cdot 3 \cdot 5^3$

$\varphi(1500) = 1500 \cdot \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 400$

$= (2^2 - 2)(3^1 - 3^0)(5^3 - 5^2) = 400$

$\varphi(a \cdot b) = \varphi(a)\varphi(b)$

↳ Biz: $\varphi(a \cdot b) = ab$-nél kisebb, a-hoz és b-hez relatív prímek száma



kész: körülírtak kit relatív prímek a-hoz is

áll: $\forall$ oszlop 1 teljes mr. mod a.

biz: $\forall$

1) $\{0, b, 2b, \dots (a-1)b\}$ tmr. mod a

2. lemmából kov. ✓

$1, b+1, 2b+1, \dots (a-1)b+1$ ✓ □

áll: $\forall$ oszlopban $\varphi(a)$ db elem rel. prím a-hoz.

~~elvétve~~ lebizonyítottuk

$\varphi(1000) = 400$

$999^{2006} \equiv ?$ (1000)

$(-1)^{2006} = 1$ (1000)

$457^{2006} = ?$ (1000)

$457^{2006} \equiv 457^{6}$ (1000)

17^{34} utolsó számjegye $\Rightarrow$ $17^{34} \equiv ?$ (10)

$7^{34} \equiv ?$ (10)

1	2	3	4	5
7	9	3	1	7

$4 = \varphi(10)$

$\Leftarrow$

$7^{34} = (7^{32}) \cdot 7^2 = 9$

$(7^8) \equiv 1$ (9)

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

biz:

3. lemma: $\{C_1, C_2, \dots C_{\varphi(m)}\}$ r.m.r. (m) ; $(a, m) = 1$

$\Rightarrow \{aC_1, aC_2, \dots aC_{\varphi(m)}\}$ r.m.r. (m)

$\{1, 3, 7, 9\}$

$\{7, 21, 49, 63\}$

$\Rightarrow C_1 C_2 \dots C_{\varphi(m)} \equiv aC_1 \cdot aC_2 \dots aC_{\varphi(m)} \ (m)$

$a^{\varphi(m)} C_1 C_2 \dots C_{\varphi(m)}$

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

Redukált maradékrendszer $\forall C_i$: $(C_i, m) = 1$

10) $4^{90}+1 \equiv 0 \quad (17)$ $\varphi(17)=16$

$4^{90} \equiv -1 \quad (17)$

$4^{80+10} \equiv 1 \quad (17)$

$4^{10} \equiv -1 \quad (17)$

$4^{10}+1^{10} = 0 \quad (17)$

(

$5555^{2222}-2 \equiv 0 \quad (7)$ $\varphi(7)=6$

$5555^{2}-2 \equiv 0 \quad (7)$

$(555\underbrace{1+4}_{0})^2-2 \equiv 0$

$4^2-2 \equiv 0$

$16-2 \equiv 0$

$14 \equiv 0$ ✓

Zh jövő héten OC 1 127

- számelmélet ig, csoportelmélet nem lesz

1 Kis Fermat tétel: ha $p \nmid a \Rightarrow a^{p-1} \equiv 1 \ (p)$

/sajen spec. esete/ ekv. alak: $a^p \equiv a \ (p)$

~~ax~~ $\equiv b \ (m)$ a, b, m adott van-e mo., hány mo. van?

- szükséges feltételek: $(a,m) \mid b$

tll: ez elégséges is.

Biz $ax \equiv b \ (m)$ $d=(a,m)$ $a=a'\cdot d$, $b=b'\cdot d$, $m=m'\cdot d$ $\Rightarrow (a',m')=1$

ha benne akar lenni nem d benne az Lnko

$a'x \equiv b' \ (m')$ Lnko

$x = b'\cdot a'^{\varphi(m')-1}$

$\Rightarrow b'\cdot a'\cdot a'^{\varphi(m')-1} = b'\cdot a'^{\varphi(m')} = b'$ □

All: A mod m mo.-ok száma (a,m).

Biz: 1 mo. $d\cdot m' = m$

0 m' $2m'$ ... $m-1$ m

dll: mod m $\exists$ mo

tfh: x_1, x_2 mo:

$ax_1 \equiv b \ (m')$

$ax_2 \equiv b \ (m')$

$\Rightarrow a(x_1-x_2) \equiv 0 \ (m')$

$\Rightarrow x_1-x_2 \equiv 0 \Rightarrow x_1 \equiv x_2 \ (m')$

csoportelmélet lesz ki

Számelméleti algoritmusok

akkor keresünk egy alg.-t, ha polinomiális időben fut

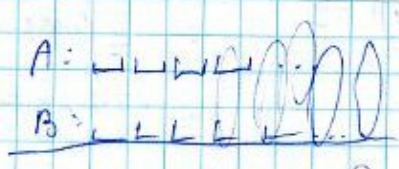
1) összeadás: futás: $\leq C_1 \cdot n^{C_2}$ (n: bemenet mérete)

A, B

a jegyű, b jegyű

$a \geq b$

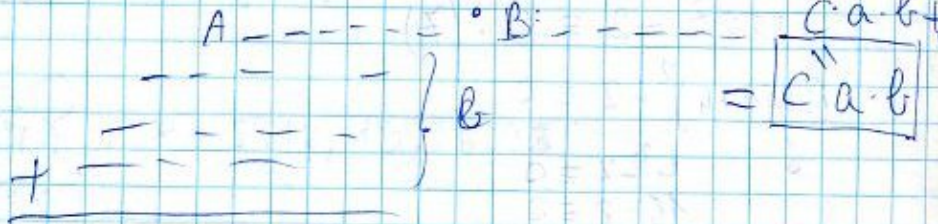
$A + B$



$c \cdot a$ idejű

2.) Szorzás: $A \cdot 9$

$c \cdot a$



$c \cdot a \cdot b + c \cdot ab = c'' \cdot a \cdot b$

3) osztás (maradékos): $A : B =$

$c \cdot b \cdot a$

4) hatványozás: A^B

$\lg A^B = B \lg A$ ha $a \cdot 10^b$ akkor $\lg a \cdot 10^b$

2^{100}

5) hatványozás mod M M: n jegyű

$A^B \equiv ?$ (M) eredménye legfeljebb M-1

$3^{25} \equiv ?$ (37)

$3 \equiv 3$ (37) /^2 (x^2)

$3^2 = 9 \equiv 9$ (37)

$3^4 = 9^2 \equiv 81 \equiv 7$ (37)

$3^8 \equiv 12$

$3^{16} \equiv 144 \equiv -4 \equiv 33$ /* (maradék)

négyzetre emelés

$25 = 16 + 8 + 1$

(11001)

$3^{25} \equiv 4$ (37)

$3^{25} \equiv 3^{16} \cdot 3^8 \cdot 3^1 \equiv 33 \cdot 12 \cdot 3 \equiv -144 \equiv -33 \equiv 4$

$c \cdot m^2 \cdot \log B$

$\sim b$

$c' \cdot m^2 b$ ⇒ gyorsabb

[illegible]

- A prím-e?
- A kerosikus alakja?

$\lg \sqrt{A} = \frac{1}{2} \lg A \approx \frac{1}{2} a$

nem lehet tudni

$\Rightarrow 10^{\frac{1}{2}a}$ ← nem hatékony

$\Rightarrow$ ezen alapul az RSA

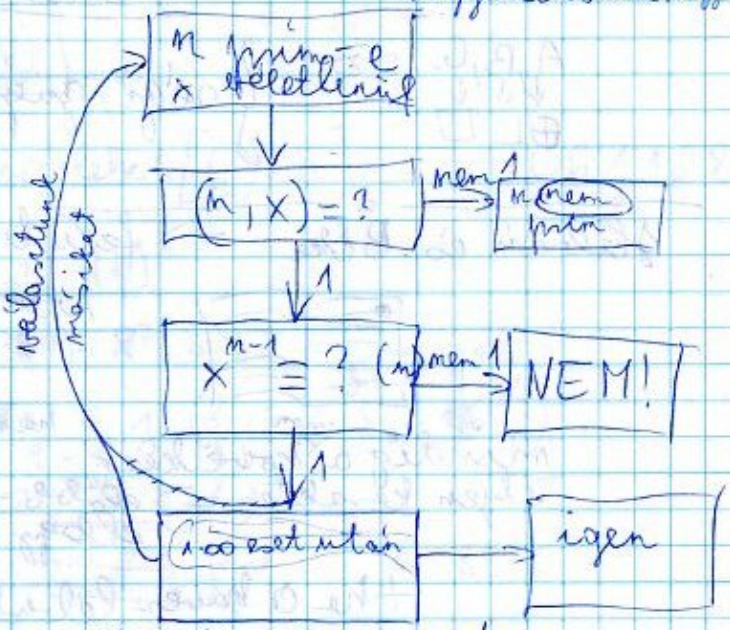
$a^{p-1} \equiv 1 \ (p)$

ha $p \nmid a$

2 ✓
3 ✓
5 ✓
7 ✓
11 ← $\sqrt{131}$

- n prím-e?

$\forall 1 < x < n$ véletlen (egyenletes eloszlással)



Fermat-teszt

áll: jó es

biz: tfh: n nem prím.

maradék: 0, 1, ... n-1

x maradékcíntosa n-nek ha

lepkezi n nemprimitásait

$x^{n-1} \equiv 1 \ (n)$ $((x,n)=1)$

igy viselkedik ⇒

áruló: többek

$(x,n) \neq 1$ v. $x^{n-1} \not\equiv 1 \ (n)$

redukált maradékrendszer fele legalább

áll: ha ∃ áruló ⇒ ∃ áruló is. (⇒ ½ relatív prím n-hez)

Biz: (a) áruló

$c_1, c_2, \dots c_k$ címtosok

áll: $a c_1, a c_2, \dots a c_k$ is áruló, különböző

áruló

cím címtost mutatok, tudok mutatni legalább ugyanannyi ~~címtost~~.

(a) áruló $\Rightarrow a^{n-1} \not\equiv 1 \ (n)$

$c_i^{n-1} \equiv 1 \ (n)$

$(a c_i)^{n-1} = a^{n-1} c_i^{n-1} \not\equiv 1 \ (n)$

$aC_i \not\equiv aC_j \pmod n$ kell: $(a,n)=1$

$\Uparrow$

$C_i \equiv C_j \pmod n$

egyszer sem bukik le:

$$\frac{1}{2^{100}} \approx 0.$$

- ha nincs áruló: $a^{n-1} \equiv 1 \pmod n$ $\forall a$-ra, amire $(a,n)=1$

$\Downarrow$ ha prím

univerzális álprím
Carmichael-szám:

pl.: 1729 $a^{1729} \equiv 1$

Miller - Rentra - Rabin teszt $\Leftarrow$ ehhez a teszthez nincs álprím

Titkosítások

$A, B, C, \ldots Z$
$\oplus \; \sqcup \; \square$ } régi, gugyi módszer (Rózsakeresztje c. film)

Hősök és Béke $\Rightarrow$ feltűnő az első 2 olyan oldalon, ahol nem szöveg $\Rightarrow$

A támadás
hanyadik
17
mindig a következő nem
ilyen karakter $\Rightarrow$ előbb-utóbb
előjön a könyv
} de megfejthetetlen.

+ ha a hacker lebukik $\Rightarrow$ megfejtik $\Rightarrow$ álüzenetek sorolhat

Nyilvános kulcsú titkosítás

- nem betűket kódolok $\Rightarrow$ pl. oldalt: 2 soronként: kb. 35 betű: 35^{120} eset

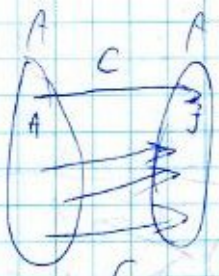
$A: \{1, \ldots N-1\}$ $N \approx 35^{120}$ (vagy nagyobb)

C: kódoló fv. $C: A \to A$ fv, $D: A \to A$ fv

Adél és Béla levelernek

Adél elküldi a $C(x)$-et B-nek.
dekódoló: D

kell: $D(C(x)) = x$



irányat-nagy halmazok

Áll: $(a,n)=1 \Rightarrow a^{k\cdot\varphi(n)+1} \equiv a \ (n)$

Biz: $a^{\varphi(n)} \equiv 1 \ (n)$

$a^{k\varphi(n)\cdot a} \equiv 1^{k\cdot a} \equiv 1^a \ (n)$ □

Próbálok kódolásra-t előállítani

$\boxed{N = p\cdot q}$ ← ez tudom mások nem, mert csak nem ismek polinomidejű alg.-t a faktorizálásra

p, q: 100 jegyű prímek

$\boxed{(c, \varphi(N)) = 1}$

$\boxed{\varphi(N) = (p-1)(q-1)}$

Nyilvánosságra hozom: N, C

$C(x) := \boxed{x^C \equiv ? \ (N)}$

Egészértékűségemma még benne lehet [GYAK] 06 11 28

1) $5x \equiv 3 \ (7)$ és $3x \equiv 7 \ (8)$

$5x \equiv 10 \ (7)$

$x \equiv 2 \ (7)$

$x \equiv m \ (7)$

$\Rightarrow x = 7k+m$

$x = 7k+2$

$3(7k+2) \equiv 7 \ (8)$

$21x \equiv 1 \ (8)$

$21x \equiv 9 \ (8)$

$21x \equiv 3 \ (8)$

~~$3x \equiv 3 \ (8)$~~

~~$x \equiv 1 \ (8)$~~

$5x \equiv 1^{\cdot 5} \ (8)$

$5x \equiv 5 \ (8)$

$x \equiv 13 \ (8)$

$k = 8l+5$

$x = 7k+2 = 7(8l+5)+2 = 56l+37$

$\Rightarrow \underline{x \equiv 37 \ (56)}$

2) $42^{600} \equiv ? \ (13) \Rightarrow \varphi(13) = 12$

$42^{600} \equiv 42^{50\cdot 12} \equiv 1 \ (13)$

ε-F-t

$(a,m)=1$

$a^{\varphi(13)} \equiv 1 \ (13)$

$\varphi(p) = p^{?}$

$\varphi(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot p_3^{\alpha_3}\dots p_n^{\alpha_n}) =$

$= \prod \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$

(7) $a^{1999} \equiv 5 \ (13)$ $\quad (a,13) \overset{1}{<} 13 \ (\neq 1)$ ↯ $\quad a = 13k$

1) $a^{-1} \equiv 5 \ (13)$ $\quad \varphi(13) = 12$ $\quad 13k = (a,13) = 13$

$a^{11} \equiv 5 \ (13) \ / \cdot a$ $\quad a^{\varphi(13)} \equiv 1 \ (13)$

2) $13k^{1999} \equiv 0 \not\equiv 5$ ↯ $\quad a^{12} \equiv 1 \ (13)$

$1 \equiv a^{12} \equiv 25 \ (13)$

$5a \equiv 1 \ (13)$

$(3 \cdot 5 + 1)a \equiv 8 \ (13)$

$a \equiv 8 \ (13)$

GY.F: /páthára :-)/

1) $3x \equiv 2 \ (5)$ és $4x \equiv 1 \ (7)$ és $5x \equiv 1 \ (8)$ szimultán kongruenciarendszer

2) $(n,17) = 1 \Rightarrow n^8 \equiv ? \ (17)$

3) $\varphi(6!) = ?$

4) n-re teljesül: $25n - 17$ és $2n+3$ ugyanazt a maradékot adja 136-tal osztva. Mennyi ez a maradék?

T. Wilson-tétel: $\forall k \geq 2$-re

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

$N = p \cdot q$ (100 jegyű prímek)

$(C, \varphi(N)) = 1$ ⇐ ezt teszik körbe ⇒ C, N

$\varphi(N) = (p-1)(q-1)$

kódolás: $C(x) \equiv x^c \ (N)$ (x: üzenet)

dekódolás: $D(C(x)) = x \Leftrightarrow C(D(x)) = x$ $\quad x^{c \cdot d} \equiv x \ (N)$

$\exists d : [x^{cd} \equiv x \ (N)]$ ez teljesül: $c \cdot d = k \cdot \varphi(N) + 1 \quad k \in \mathbb{Z}^+$

$[D(y) = y^d \ (N)]$ $\quad (x^{k \cdot \varphi(N)+1} \equiv x \ (N))$ ⇕

$cd - 1 = k \cdot \varphi(N)$

$cd \equiv 1 \ (\varphi(N)) \Leftrightarrow \varphi(N) \mid cd - 1$

megoldható d-re
értelem a d-t, de mások nem.

aki üzenetet akar nekem küldeni
⇒ megnézi C-t és N-et
⇒ az üzenetét C-re emeli mod N
⇒ én, csak d-re emelem mod N
és dekódolva van.

Ádél Béla

C_A C_B

(D_A) (D_B)

Ádélnak is akarja írni
⇒ $C_B(x)$ helyett először
D_A-val megnyitja x-et,
majd titkosítja:

$[C_B(D_A(x))]$

$\Rightarrow D_B(C_B(D_A(x))) = D_A(x)$

$C_A(D_A(x)) = x$

$C_B(D_A(x))$ } odaadom a bíróknak ⇒ a bíró ismeri $C_A(D_A(x))$
$D_A(x)$ } hogy tényleg én küldtem / $C_B(C_A(D_A(x)))$
tényleg A küldte: / A

anélkül, h megismerte volna a dekódolót

$[c = 7 \quad N = 33] \Rightarrow 3 \cdot 11 \Rightarrow \varphi(N) = 2 \cdot 10 = 20$

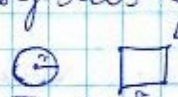
$x = 2$

$2^7 = ? \ (33)$
29
ez kell

$d = ?$
$cd \equiv 1 \ (\varphi(N))$
$7d \equiv 1 \ (20)$
$7d \equiv 21 \ (10)$
$d \equiv 3 \ (10)$

$29^3 \equiv (-4)^3 \equiv -64 \Rightarrow 2 \ (33)$

Csoportelmélet

Görög problémák:
1) kockakétszerezés →  ⇒ szeretnék 2x akkora kockát szerkeszteni
⇒ $\sqrt[3]{2}$ hosszú szakaszt 
- szögharmadolás →  körzővel, vonalzóval...
- körnégyszögesítés 

Nincs megoldóképlet 5-ödfokú egyenletekre

- magasabb egyenletek megoldhatósága ⇑

⇒ ezeket a csoportelmélettel lehetett megoldani
(Galois-elmélet)
↳ 21 évet élt, párbajban halt meg

(H, műveletek) → függvény
H: halmaz
Hány van megadva

n-változós művelet: $f: H^n \to H$ | $f: H^2 \to H$

$(a,b) \in H^2$ rendezés

H-beli párokhoz H-beli elemet rendel

(P1) $\mathbb{Z}, +$
$+(5,4) = 5+4 = 9$ ✓ zárt

$P_{\mathbb{N}}: \mathbb{N}, -$
$-(7,3) = 7-3 = 4$
$-(3,7) = 3-7 = -4$ ↯
⇒ nem egy művelet

(P2) $n \times n$-es $m \times$, oszlopos $m \times$ szám-ra

⇒ ez művelet ✓

(P3) {a föld összes zsiráfjai}, $*$ művelet
$Z_1 * Z_2 =$ a magasabbik
ez is művelet. ✓

(P4) {az összes ember}, $\square$ a $\square$ $b = b$
ez is művelet. ✓
- nem komm. - asszoc.

$(H, *)$
$\forall a, b \in H: a * b = b * a$ kommutatív ⇐ ezt nem mindig követeli meg
$(a * b * c) \Rightarrow a*(b*c) = (a*b)*c$ asszociatív ⇐ ez már fontosabb
$a-(b-c) \overset{?}{=} (a-b)-c$
$a-b+c \neq a-b-c$

$(H, *)$ * asszoc. művelet
⇒ félcsoport

- $\exists$ e? e: egységelem

$a * e = e * a = a$

- inverzelem: $\forall a \Rightarrow \exists e \quad \overset{*}{a}^{-1} : \quad \overset{*}{a}^{-1} * a = a * \overset{*}{a}^{-1} = e$

- Ha van inverzelem és mindekhez egységelem

$\Rightarrow$ csoport

- $(\mathbb{Z}, +)$ ~~$\mathbb{Z}, \cdot \not\downarrow$~~ $(\frac{1}{5}, \cdot)$
- $(\mathbb{Q}, +)$ $\mathbb{Q}, \cdot \not\downarrow (\frac{1}{5}, 0) \Rightarrow \mathbb{Q}\setminus\{0\}, \cdot$ ✓
- $(\mathbb{R}, +)$ $\mathbb{R}\setminus\{0\}, \cdot$ ✓
- $(\mathbb{C}, +)$ $\mathbb{C}, \cdot$ ✓

10 elemű: $\mathbb{Z}_m \sim \{0, 1, \dots 9\}, \oplus \mod 10$ (mod 10)

$a \oplus b \equiv a + b \ (10)$

pl.: $7 \oplus 6 \equiv 3$

Csoport? ✓
- művelet ✓
- egységelem? $=0$ ✓
- inverz? a^{-1} $a \Rightarrow -a \ (10)$

$7^{-1} \Rightarrow 3$

$5^{-1} \equiv 5$ ✓

véges csoport

$\{1, \dots p-1\}, \cdot \pmod p$ csoport? ✓

$\{1 \dots 6\}, \cdot \mod 7 \Rightarrow -3 \odot 5 \equiv 1$ ✓

$-e = 1$ ✓

$1 \odot 1 = 1$
$2 \odot 4 = 8 = 1$
$3 \odot 5 = 1$
$6 \odot 6 = 1$ ✓

$-a^{-1} = x \Leftrightarrow a \cdot x \equiv 1 \ (p)$

$\exists m \Leftrightarrow (a, p) = 1$ (relatív prímek)

tétel: $\exists$ inverz $\Rightarrow$ egyértelmű

tétel: $\exists$ egységelem $\Rightarrow \sim$

bizt: Tfh: $\exists e, e' \Rightarrow e \cdot e' = ? = e' = e$ □

bizt: tfh: a-nak b és c is inverze.

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

Példa: (véges nemkommutatív) Diéder-csoport

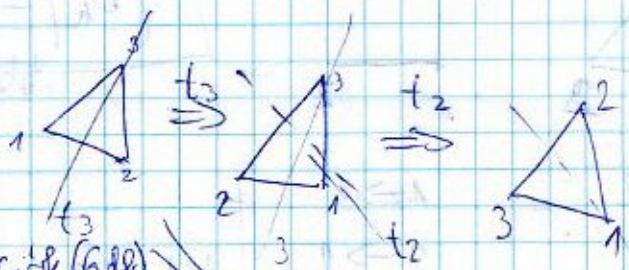
D_3:

Transzformációk, amire a $\triangle$ helybenmarad

1) 120° 3 forgatás / $k \cdot 60°$ / (360°) } 3 forgatás
2) helybenhagyás = identitás
3) 240° ...

• tükrözés

$\Rightarrow$ 3 tükrözés



a csoport

elemei: a transzformációk (6 db)

{120°-forg, 240°-forg, id, t_1, t_2, t_3 - tükrözés} 120°-os forg

művelet: egymás után végezzük előbb

$$(T_{t_1} \cdot T_{t_2})(x) = (T_{t_1}(T_{t_2}(x)))$$

XII. 14. 16^{00}

I. 4. 17^{00}

11. 17^{00}

18. 17^{00}

$\Leftarrow$ konvex

1B134

06.12.1

$I \cdot T_{t_1} = T_{t_1}$

$(a \cdot b) \cdot c \ (x) = (ab)(c(x)) = a(b(c(x)))$

$a \cdot (bc)(x) = a(bc(x)) = a(b(cx))$

invers: $T_{t_1}^{-1} = T_{t_1}$ $\quad T_{120°}^{-1} = T_{240°}$

$T_{t_1}^{-1} \cdot T_{t_1} = I$

$\forall a, b : a \cdot b = b \cdot a$

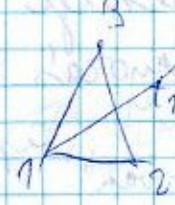
Abel-csoport (= kommutatív a szorzás művelete)

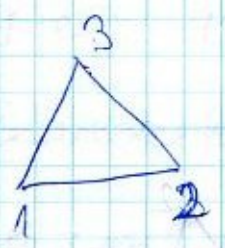
$T_{t_2} = T_{t_1} \cdot T_{120°}$ | $T_{120°} \cdot T_{t_1} = T_{t_3}$

$1 \to 3$ $\quad 1 \to 2$

$2 \to 2$ $\quad 2 \to 1$

$3 \to 2$ $\quad 3 \to 3$





$|D_n| = 2n$ elemű

$1 \to 2$
$2 \to 3$
$3 \to 1$

$1 \to 2$
$2 \to 1$
$3 \to 4$
$4 \to 3$

tetszőlegesen
$\Rightarrow$ csúcsok egy permutációja

$\Rightarrow$ permutációcsoport / szimmetrikus csop /
elemei az összes permutáció
$S_n = n!$

$(\Rightarrow D_3 \subset S_3)$

$$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$$

identitás: $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$

inverz:

$$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\left[\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\right]\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$

Csoport rendje: $|G|$ [elemszáma] (ha véges)
elem rendje: a legkisebb $k \in \mathbb{Z}^+$, amire $a^k = e$
hatványozás: $a \in G$ csop $k \in \mathbb{Z}^+$ $a^k = \underbrace{a \cdot a \cdot a \cdot a \cdots a}_{k}$
mért $\exists$? véges csop-ban $a, a^2, a^3, a^4, \ldots \Rightarrow \exists x, y: a^x = a^y$ $x \neq y$

$x < y$

$\underbrace{a \cdot a \cdot a \cdots a}_{x} = \underbrace{a \cdots a}_{y}$

$a^{-1}a \cdot a \cdots a = a^{-1}a \underbrace{a \cdots a}_{y-1}$

$\underbrace{a \cdots a}_{x-1}$

$e = \underbrace{a \cdots a}_{y-x} \Rightarrow e = a^{y-x}$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

$\oplus$: mod 6 összeadás

$o(0) = 1$

$o(1) = 6$

$o(2) = 3$ $\quad 3 \equiv 0 \ (6)$

$o(3) = 2$

$o(4) = 3$

$o(5) = 6$ $\quad 5+5 = 10 = 4 \Rightarrow 4+5 = 9 = 3 \quad 3+5 = 8 = 2$

$2+5 = 7 = 1$

Véges csop.-ban: $\forall$ elem rendje osztója a csop rendjének

$\Rightarrow$ Lagrange-tétel

Részcsoport; G csop., H részcsoportja G-nek ($H \leq G$)

ha $H \subseteq G$ és H csop. ugyanarra a műveletre

Tétel: $H \leq G \Leftrightarrow H \subseteq G$ és H zárt a G-beli műveletekre

pl.: (forgatások) $\leq D_3$

Z_6 $\quad 1 \ldots 5, 0 \quad 0, 2, 4$ + mod 6

Biz: $\Rightarrow$ ✓

$\Leftarrow$ $a \in H \quad a^{-1} \in H$

$a, a^{-1} \in H \Rightarrow e \in H$

Ciklikus csoport: G ciklikus, ha $\exists g \in G$, hogy

$\{g$ hatványai$\} = G$

$1^2 = 1, \ 1^2 = 2, \ 1^3 = 3 \ \ldots \ 1^5 = 5 \quad 1^6 = 0$

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

Biz: $\Leftarrow$ $g, g^2, \dots g^{|G|}$

Tfh: $g^x = g^y \qquad 0 < x < y \leq |G|$

$e = g^{y-x} \qquad y - x < |G| \Rightarrow o(y) < |G|$ ↯

$\Rightarrow$ Tfh. $\{g$ hatványai$\} = G$

Tfh: $o(g) < |G|$

Áll: $\forall$ prímrendű csoport ciklikus.

Biz: (Lagrange-t.) $|G| = p$ ✓

Def: Mellékosztály:

G, $H \leq G$, $g \in G$

$gH := \{gh \mid h \in H\}$

$Hg := \{hg \mid h \in H\}$

$(\{0,2,4\}, \oplus) \leq Z_6$

$g = 1$

$gH = \{1 \oplus 0, 1 \oplus 2, 1 \oplus 4\} = \{1,3,5\}$

$g' = 4$

$g'H = \{4 \oplus 0, 4 \oplus 2, 4 \oplus 4\} = \{4,0,2\}$

① Áll: gH és $g'H$ nem azonos $\Rightarrow$ egy közös elemük sincs

$gH \cap g'H = \emptyset$

Biz: Tfh: $x \in gH \cap g'H$

$\exists h \in H : x = gh$

$\exists h' \in H : x = g'h'$

$gh = g'h' \in H^*$

h^*

$g = g'h^* \Rightarrow g \in g'H$

all: $gk \in gH$

$g(h^*h)$ benyílik benne van.

② $|gH| = |H|$

Ph: $g^{-}g = g(\dots)$

③ g-hez $\exists$ ét tartalmazó mellékosztály

Tétel: $|H| \mid |G|$

Gyűrűk $(H, +, \circ)$

$(H, +)$ abel-csop (egységelem: 0)

$(H \setminus \{0\}, \circ)$ félcsoport

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

$(a+b)c = ac + bc$

Ha a félcsoport csoport $\Rightarrow$ test

+ izomorfia

+ Cayley-tétel