

wiener @ cs.bme.hu
cs.bme.hu / bsz2.

2 ZH + VIZSGA

↳ 6 feladat, 24 pont min., 90. perc

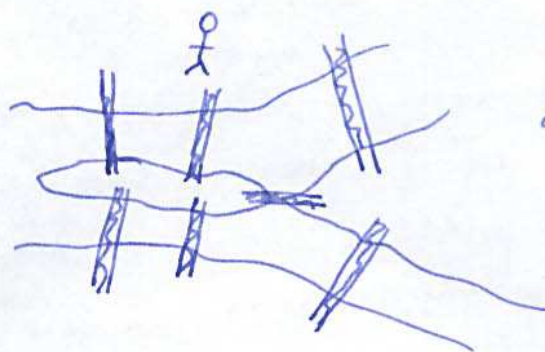
- gráfelmélet
- számelmélet
- absztrakt algebra
- alkalmazások, kódolás, titkosítás

Gráfelmélet

Euler-körök és utak

Königsbergi hidak problémája:

↳ hidak pontosan 1x végigmegy,
még visszajut



Leonhard Euler

kínyg-vízg-kínyg

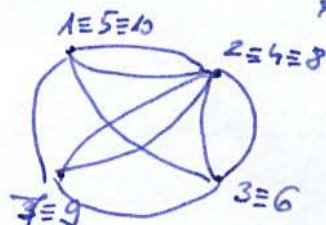
nem tud visszajutni

fokszám páratlan $\Rightarrow$ nem lehet

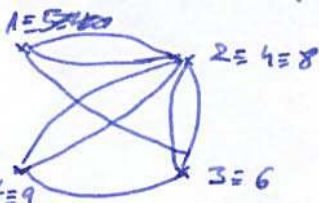


Elegendes feltétel a körkéthára: $\forall$ fok páros.

Euler-kör: olyan zárt élsorozat a gráfban, amely $\forall$ élet pontosan 1x tartalmaz. (! nem kör!)



Euler-út: $\forall$ élet pontosan egyszer tartalmazó élsorozat.



G összefüggő.

Áll: $\exists$ Euler-kör $\Rightarrow \forall$ fok páros

tlh. $\exists$, vegyük egy telj. pontot

átalad: $(kínyg, kínyg) \times n$

kezdődik: kínyg, amikor kínyg,
majd vagy kínyg és vízg, vagy nem
az élet ponton állunk

↳ Königsbergi hidak nem járhatók be jól.

Nem elegendes: $\triangle$ $\square$ nem jó, mert nem összefüggő

Kell: összefüggő vagy 1 körrel és 1 komponens izolált pont.

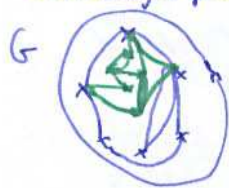
All: G összefüggő

G -ben van Euler-kör $\Leftrightarrow \forall$ fok páros.

Biz: " $\Rightarrow$ " megvolt

" $\Leftarrow$ ": G öf, $\forall$ fok páros

teljesen pont-sétálok, amíg ~~teh~~ tudunk



Ez csak a kezdőpontban érhet véget, mert ha egy pontba bementünk, pt. pont élet használtunk el $\Rightarrow$ nem még min. 1. $\Rightarrow$ ki tudunk jönni csak akkor áll le, ha a kezdőpontból is az összes élet bejött.

tfr. van olyan él, amit még nem jártunk be. $\rightarrow$ abból a pontból is tudunk egy kört tenni $\rightarrow$ ez a kört mentőre beillesztjük (kül. életet jártunk be.) a maradék pontokat a maradék fokai párosak.

Ezt addig csináljuk, míg $\exists$ olyan él, ami érintett pontokból megy ki.

All: akkor Euler-kör van

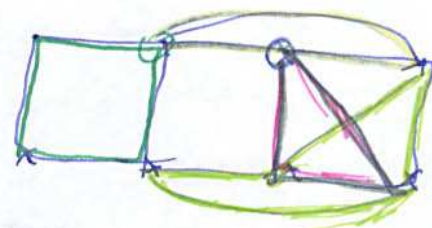
• Zárt ciklusok

• $\forall$ élet tartalmaz: tfr. $\exists$ amit nem

$\exists$ olyan része, ami nem szerepel a sétában

de a G összefüggő $\Rightarrow \exists$ egy él, ami ezt a részt a mással összeköti.

~~vissza~~ Ellentmondás: azt mondtuk, hogy az elő résznek minden élet elfoglalt.



G öf. gráf.

G -ben $\exists$ Euler-séta $\Leftrightarrow$ a pt fokú pontok száma ≤ 2 (0 v. 2) $\Rightarrow$ $\exists$ kezdő pont.

csak a kezdőpont és a végpontokra lehet páratlan $\Rightarrow$ max 2.

ha 0 $\Rightarrow$ jó mert $\exists$ Euler-kör $\rightarrow$ séta is.

ha 2: ezeket kössük össze még egy éllel $\Rightarrow \forall$ fok páros $\Rightarrow \exists$ Euler-kör

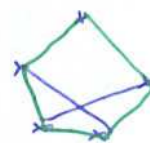
vegyük el a plusz élet $\Rightarrow$ Euler-séta, a kezdőpontot a pt fokú pont

Hamilton-kör és -út.

Def: H Hamilton-kör, ha kör és $\forall$ csúcsot tartalmaz.

Hamilton-út: olyan út a gráfban, amely $\forall$ csúcsot pontosan 1x tartalmaz

nincs szükséges és elégséges feltétel.



Szükséges felt. Hamilton-körre:

BSE II.

2008.02.11.
Wiener János

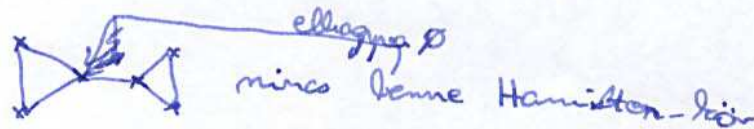
- összefüggő

- $\forall$ k pontját elhagyva max k komponens keletkezik, ha $\exists$ Hamilton-kör.

Hamilton-út: -

- $\exists$ Hamilton-út $\forall$ k pontot elhagyva max $k+1$ komponens keletkezik.

Alk:



Nem elégséges feltétel:

Petersen-gráf



A teljes gráfokban $\exists$ H-kör:

De olyan, aminek sok éle van, és mégis nincs!



Dirac-tétel: Ha G -ben $\forall$ $fok \geq \frac{n}{2}$ (ahol n a csúcsok száma) $\Rightarrow \exists$ H-kör.
(ez nagyon sok)

Ore-tétel: G -ben $\exists$ $\forall$ nem szomszédos x, y pontpárra $d(x) + d(y) \geq n \Rightarrow \exists$ H-kör.
 $\exists$ G -ben H-kör.
a Dirac engélyezés

Biz:



- ha $\exists$ H-kör $\Rightarrow \checkmark$

- ha $\exists$: bebizonyít egy éle, hogy továbbra is legyen.
ha nincs, békén hagyom.

- ez addig, míg G olyan, hogy bárhogy húzok be éleket, $\exists$ H-kör.
pl: x és y összekötése H-kör.
ha plusz éleket húzunk be G -be a feltétel nem változik el $\Rightarrow$ erre a G' -re is igaz.



bebizonyítjuk x szomszédait:

bebizonyítjuk az x -ket megérintő pontokat:

$\forall$ pontot nem lehetnek összekötni y -val, mert akkor lenne H-kör

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

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

de x és y nem szomszédos $\hookrightarrow d(x) + d(y) \leq n-1$
-3-

Biz: $1, 2, \dots, D+1$ min



szóba vehetünk, csak ama figyelek, hogy más legyen, mint a
a szomszédai (mindig lehet)

↑
más szomszéd

Gráfok színezése: a csomópontok színe különbözően.



$\Delta: G(V, E)$ [egyszerű] gráf
 $f: V \rightarrow \{1, 2, \dots, n\}$ $\forall$ csúcsra hozzárendelünk 1 színt (v. színt)
 $f = \text{jó színezés}$, ha $(x, y) \in E$ esetén $f(x) \neq f(y)$

$1 \leq \chi(G) \leq |V(G)|$
 (keli G)

All: G 2-színezhető $\Leftrightarrow G$ csomópontja felbontható 2 részre úgy, hogy az élak csak a 2 rész között menjenek.

$\chi(G) \leq 2$



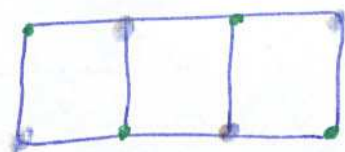
2 rész, hogy a részeken belül nem mennek

Elvezetés: G páros gráf, ha $\chi(G) \leq 2$

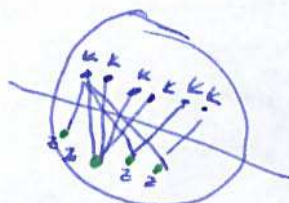
$G = (A, B)$
 ↑
 osztályok



1. el kezdődik színezés, ennek csomópontait színez, annak csomópontait színez...

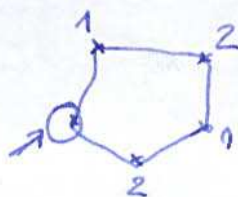


2-színezhető, módszer:

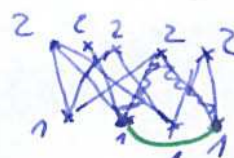


All: páros gráf $\Leftrightarrow G$ -ben nem létezik páratlan (hosszú) kör

Biz: " $\Rightarrow$ " ps $\rightarrow$ pt lenne pt kör



" $\Leftarrow$ " $\nexists$ pt. kör, ellentétet okozni a fenti módszerrel.

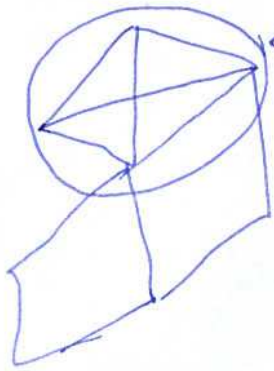


Ez jó: • mindkét részre van kettő a köld 2 rész, mert akkor a komponensek színezhetők ps körrel út (fél-kör), ha a köldet le akarjuk húzni akkor pt lenne.

- így körökön dönthető, ~~egy~~ gráfok, hogy 2-színezhető-e.

A 3-színezhetőség az eldöntés exponenciális probléma.

Becsleket a kromatikus számról.



klkt. teljes részgráf

klkiszám(klkismérete): a legnagyobb klkt mérete.
 $\omega(G)$

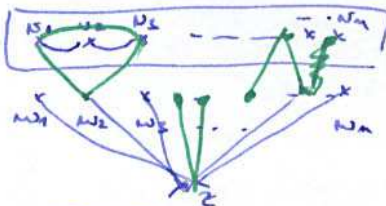
$$\chi(G) \geq \omega(G)$$

(mert a teljes gráf csúcsait mindegyik 2 különböző színre szívné)

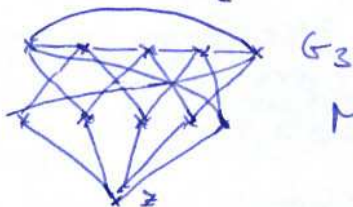
Dc: $\omega=2$
 $\chi=3$ } kétet nem egyenlő

Tétel: $\forall k$ -hoz $\exists G_k$ gráf, hogy $\omega(G_k)=2$
 $\chi(G_k)=k$

Bizs: $k=2$ $\rightarrow G_2$
 $k=3$ $\rightarrow G_3$
 $G_k \rightarrow G_{k+1}$



G_k
 egyéssel mindenel összekötve, viszont z -i mellett van összekötve mint v_i .
 ezért felvesszük $k+1$, összekötöm minden v_i -vel.



Mycicloski - konstrukció: azért jó, hogy megmutassuk,
 a $\chi \geq \omega$, és nem tud éles lenni, felülről nem
 tudjuk ω -val korlátozni

Teljes indukció: G_k -ban nincs háromszög $\Rightarrow G_{k+1}$ -ben sincs

1. eset G_k -ban van 3 $\hookrightarrow$
2. eset G_k -ban van 2 $\hookrightarrow$
3. eset G_k -ban van 1 $\hookrightarrow$
4. eset G_k -ban van 0 $\hookrightarrow$

$$pl: (v_2-v_1) \text{ és } (v_2-v_3) \Rightarrow (v_1-v_2) \text{ és } (v_2-v_3) \Rightarrow v_1 v_2 v_3 \Delta \hookrightarrow$$

$\Rightarrow$
 valóban háromszögmentes

Ind. felt: $\chi(G_k)=k$

k -re: $\chi(G_{k+1})=k+1$: $k+1$ színnel színezhető, de kevesebbvel nem.



az indukciós feltevéssel n -ben színezhető, mint az eredeti.

Indukciós lépés G_k a z kap egy $k+1$. színt (kell, mert k már előfordul)

$$\chi(G_{k+1}) \leq k+1 \quad \uparrow$$

$$\chi(G_{k+1}) \geq k+1 \quad (k \text{ már nem elég})$$

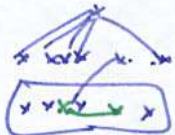
tegyük fel indukciót
2-es szám legyen 1.

$$\chi(G_{2n}) \leq 2 \Rightarrow 1. \text{ szín nem szerepel a } 2n \text{ között (2 miatt)}$$

↓
azaz az eredetiben sem szerepel $\Rightarrow$ kész.

Ha van 1-es szín: azt a színt cseréljük az első színre

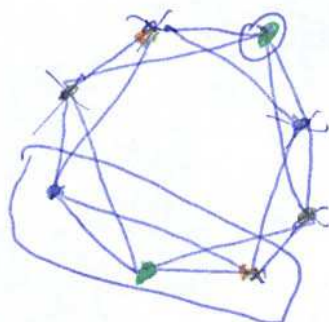
3 eset:

1.  cél: egy színpontjai külszínűvé.

mindent színpont váltott: ~~az~~ mincs baj, mert eredetileg mindkettő 1.
volt közöttük, ami meg nem lehetne.

2. egyik sem változott: eredetileg külszínű volt, most is az (van él közöttük)

3. csak az egyik változott, a másik nem: vált. utána külszínű.
az jó, mert van él a 2 rész között $\Rightarrow$ kész minél.



$$\omega = 3$$

az 4 színnel környék

$$\chi \leq 4$$

$$\chi = 4$$

bizonyos χ és ω között minőségileg van az az eset lehet
 $(4) \times 2 = 8$

független pontok: olyan pontok, amelyek között nincs él
fkt pontok maximális száma: $\alpha(G)$

$$\text{itt: } \alpha(G) \leq 2$$

A minőségileg fkt. halmazok.

$$\chi(G) \cdot \alpha(G) \geq |V(G)|$$

$$\chi(G) \geq \frac{|V(G)|}{\alpha(G)}$$

$$\boxed{\chi(G) = \omega(\bar{G})}$$

egyszerűen szemléltetve 2 minőségi erőre, a másikban bármelyik 2.



$$\chi = \frac{n}{2} + 1$$

$$\frac{|V(G)|}{\alpha} = \frac{n}{\frac{n}{2} + 1} \Rightarrow \chi \geq 2 \quad (\chi = \frac{n}{2})$$

↑
ez a becslés nem túl erős.

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

↓
max fokszám a gráfban

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

pontatlan :



Mikor élős?

teljes gráf:

$$\Delta = n - 1$$

$$\chi = n$$



pt. kör:

$$\Delta = 2$$

C_{2n+1}



$$\chi = 3$$

Példából:

G (márcs)



$$\Delta = n - 1$$

$$\chi = n$$

itt is élős, de a gráf nem összefüggő.

Ha összefüggő $\Rightarrow$ csak ezek a példák élősök (lehető biz)

Reguláris gráf: $\forall$ fok egyenlő

pl: n -reguláris gráf

All: ha G öf, nem reguláris $\Rightarrow \chi(G) \leq \Delta(G)$ (a beadás nem élős)

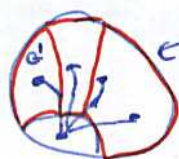
Biz: teljes ind.



Tfl: $\forall G$ gráf, aminek kevesebb, mint n csúcsa van: ✓

Kéne: igaz másképp is.

nem reguláris $\Rightarrow \exists$ olyan csúcs, hogy fok $\leq \Delta \rightarrow$ ezt elhagyjuk



$\forall$ komponensenként $\leq n$ csúcsa van
összefüggő

Kéne: nem reguláris

$\forall$ komponensben van olyan csúcs, aminek fok $< \Delta(G)$

1) lecsökkent: $\Delta(G') < \Delta(G)$

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

(Cél: $\forall$ komponens megmérhető $\Delta(G)$ mellett
erre között nem vezet el $\Rightarrow$ kész vagyunk)

2.) nem változik a Δ ($\Delta(G') = \Delta(G)$)

indukció feltétele miatt megmérhető $\Delta(G)$ mellett

$$\chi(G') \leq \Delta(G)$$

Maradt: az elhagyott pont mérésére.

lehet mérni, mert fok kisebb, mint Δ , de Δ mellett mérhető $\Rightarrow$ ✓

(Att: ha reguláris és nem páratlan kör vagy)

Brooks-tétel: G öf, nem teljes gráf, nem pt. kör $\Rightarrow \chi(G) \leq \Delta(G)$

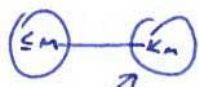
nem kell tudni a bizonyítást.

Ellenpéldák: 



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

Mikor: $\chi = \omega$?



ez a rész hat. meg $\chi = \omega$: $\chi = n$
 $\omega = n$

+1 él: χ és ω is maradt

összefüggőség nem elég $\Rightarrow \chi = \omega$ felt. kevés

ha a részgráfokra is megfigyeltem $\Rightarrow$ tük. sz.  $\chi = 3$
 $\omega = 2$

Def: G perfekta ha $(\chi(G) = \omega(G) \text{ és } \forall G' \text{ feszített részgráfra } \chi(G') = \omega(G'))$
még mindig erős, és $\forall$ köztük futó él.



$\forall$ gráf saját maga feszített részgráfja is.

All: $\forall$ ps. gráf perfekta.

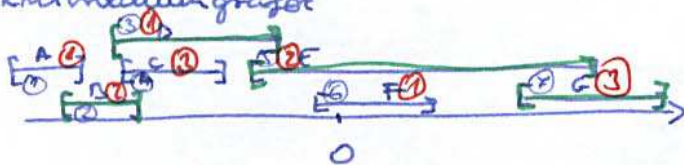
Biz: G páros $\Rightarrow \chi = 2$

mivel benne pt. kör $\Rightarrow \Delta$ nem $\Rightarrow \omega = 2$

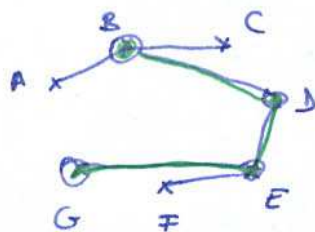
$\Rightarrow \chi = \omega$

ps gráf összes feszített részgráfja is ps.

Def: intervallumgráf



Itkon köztük össze, ha van közös pontjuk



Tétel: az intervallumgráf perfekta.

feszített részgráfja is intervallumgráf.

(tetszőleges részgráfja nem igaz).

elég: $\forall$ intervallumgráfra $\chi = \omega$:

G : tetszőleges intervallumgráf.

$\omega = \omega(G)$

tudjuk: $\chi \geq \omega$

léte: $\chi \leq \omega$ (létezik min. ω szín)

Algoritmus: úgy számolom, hogy a következőnél a legkorábbi kezdőpontja

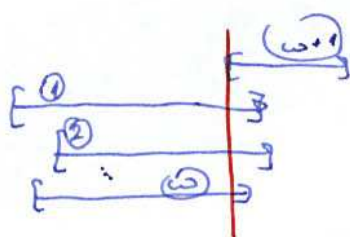
Eljárás: a legkisebb olyan min. színre, ami lehetséges
Még mindig a kezdőpont min. színre.

All: $\exists$ a részgráf $\leq \omega$ rész használat.

Biz: induktív:

tfk kell valószínű.

Mikor jön először elő az $\omega+1$ szám?



Több balra kezdődik és nem ér véget a kezdő-pontjaig.

Van közöttük $1, 2, \dots, \omega$ szám

a közös pont bármelyik 2 -ben benne van $\Rightarrow$ van benne teljes gráf

Van benne $\omega+1$ -es is lehet ω

elég az ω szám.

- a ps. gráfok komplementerei is ps. gráfok

(Berge-rejtés)

Lawson tétel: G perfekt $\Leftrightarrow \bar{G}$ perfekt.

7B

Erős perfekt-gráf tétel: G perfekt $\Leftrightarrow G$ -nek $\nexists$ olyan feszített részgráfja, ami legalább 5 hosszú út. kör, vagy illyennek a komplementere.

7B

Síkgráfok színezése

Négyzetes rejtés: $\forall$ síkba rajzolható gráfok $\chi(G) \leq 4$

Négyzetes-tétel $\nearrow$: első számítógépes bizonyítás nem esetre.

5-szín tétel: $\chi(G) \leq 5$

Biz:

All: $\forall$ síkba rajzolható egyszerű gráfok $\exists$ max 5 fokú pontja
($e \leq 3n-6$)

Ind: $\forall$ fok $\geq 6 \Rightarrow \exists$ fokos $\geq 6n \Rightarrow e \geq 3n$

Teljes ind: $\leq n$ csúcsú síkba rajzolható gráfok $\chi \leq 5$

Kéne n csúcsúra is $\chi \leq 5$

fok $\leq 5 \rightarrow$

1. eset: fok $\leq 4 \Rightarrow$ elhagyjuk, a maradék 5 színnel színezhető, mely 5 szomszédja van $\Rightarrow$

2. eset: fok $= 5 \Rightarrow$ egyszerű maradék. $\leftarrow$

x és y mindegyik szomszédjának (különböző lenne lenne K_6 $\leftarrow$ állítás)
 x -et és y -t behúzzuk A -ba $\rightarrow$ x, y, A (a "delet diagon")

$\rightarrow$ 2-vel kevesebb pontja van $\Rightarrow$ színezés 5 színnel.
Még mindig csak x, y, A csúcsok vannak $\Rightarrow$ A más legyen (lehet, mert 5 szomszédja x -nek és y -nek van)

Gráfok élromatikus száma: $\chi_e(G) \geq \Delta(G)$

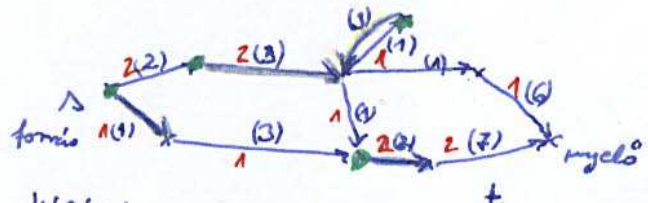
ez nem mindig éles: $\Delta=2$
 $\chi_e=3$



Vizing Tétel: G egyszerű $\Rightarrow \Delta(G)+1 \geq \chi_e(G) \geq \Delta(G)$
fontos, hogy egyszerű:



Hálózati folyamat



Hálózat: $\langle G, n, t, c \rangle$
 G : irányított gráf
 n : forrás (ke nem megjelölve)
 t : nyelő (ke nem megjelölve)
 c : kapacitás

$c: E \rightarrow \mathbb{R}^+$

folyam, $f: E \rightarrow \mathbb{R}^+$

- ① $0 \leq f(e) \leq c(e) \quad \forall e \in E$
- ② $\sum_{e \text{ u-ből ki}} f(e) = \sum_{e \text{ u-ba} \text{ bel} \text{be}} f(e) \quad \forall u \in V \setminus \{s, t\}$

folyam értéke: $m(f) = \sum_{e \text{ s-ből ki}} f(e) = \sum_{e \text{ t-be} \text{ bel} \text{be}} f(e)$

Hálózat vágása

$X \subseteq V, s \in X, t \notin X$
 X vágás, éllet



Vágás kapacitása: $c(X)$

$c(X) = \sum_{e \text{ s-ből ki}} c(e)$

adott hálózat

? : max f folyam
maximális vágás

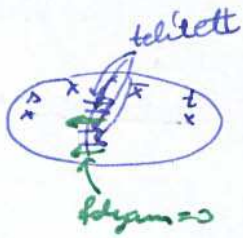
$\max m(f) \leq \min c(X)$
 X vágás

All: $\forall f$ folyamra és X vágásra: $m(f) \leq c(X)$

Tfűt találni olyat, hogy $\max m(f) = \min c(X)$

Ford - Fulkerson Tétel: $\max m(f) = \min c(X)$

Biz: elég: $\exists f$ folyam, X vágás: $m(f) = c(X)$



ez az él mincor a gráfban telített

(javított: irányított s-t út a segédgráfban)

$$\sum_{x \rightarrow x \text{ élre}} \text{folyamított} = C(x)$$

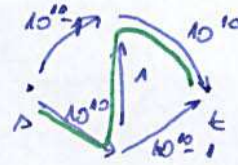
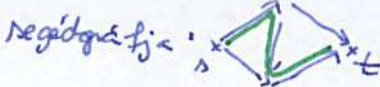
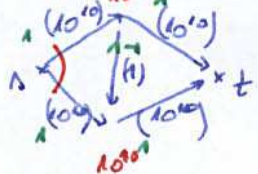
$$m(f) = \sum_{e \text{ s-ből kiindul}} f(e) - \sum_{e \text{ s-béltérbe fut be}} f(e) = \sum_{e \text{ s-ből kiindul}} f(e) - \sum_{e \text{ s-béltérbe fut be}} f(e) = C(x)$$

A részben belüli élér ki nullázódna.

Tehát, ha találunk olyat, hogy $m(f) > C(x)$, akkor ez jó.

→ Ford-Fulkerson tétel (MFNC - max flow-min cut)

Mi van, ha van algoritmus, de lassú?



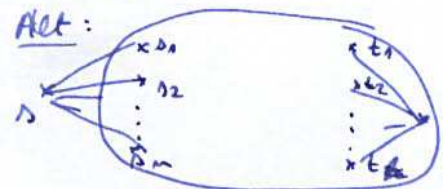
2. 10^{10} lépésben is meg lehet találni 2 helyett! → probléma

A javítások között megkülönböztetés kell.

Edmonds-Karp: Ha mindig a legrövidebb úton javítunk, az algoritmus lépésszáma $|V(G)|$ polinomjával becsülhető felülről
($\exists c_1, c_2 : \text{lépésszám} \leq c_1 \cdot |V(G)|^{c_2}$)

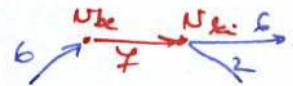
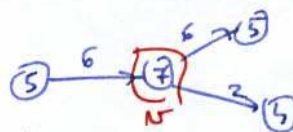
Égészértékiségi lemma: Ha egy hálózaton $\forall$ kapacitás egész, akkor $\exists$ max folyam, ami $\forall$ élen egész értéket vesz fel.

• A javításos algoritmus során $\forall$ élen egész számmal javít, a csomó 0 egész fé-lől indul $\Rightarrow$ a végén is egész.



Több szereplő esetén felvesz egy s és egy t új pontot az kapacitással.

Alt: a csomók is adott kapacitást:



széleskörű a csomók adott kapacitási állé

Alt: Nem irányított él is szerepel



Többszörös összeruggóság (Menger tételai)

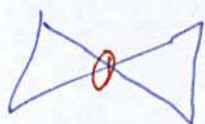
Def: G gráf k -szorosan előszerű, ha bármely, legfeljebb $k-1$ db-t elhagyva még összeruggó.

Def: $u-v$ pontösszerű, ha legfeljebb $k-1$ pontja van, és bármely, legfeljebb $k-1$ pontot elhagyva még összeruggó.

Pl:



$1 \times$ előszerű, de $2 \times$ nem pontf.



$2 \times$ előf (de $3 \times$ nem)

$1 \times$ pontf.

Pontdiszjunkt utak: azonos végpontok, de más közös pont nincs.



$K(s, t)$: s és t közötti pontdiszjunkt utak max száma.

$\lambda(s, t)$: s és t közötti éldiszjunkt

Def: $s \rightarrow t$ utakat lefoglaló ponttalmas: olyan ponttalmas, amelyet elhagyva (más) minos $s \rightarrow t$ út

$K'(s, t)$: minimális lefoglaló ponttalmas mérete

Def: $\lambda'(s, t)$: $s \rightarrow t$ utakat lefoglaló élhalmaszat min. mérete.

$s \rightarrow t$ utakat lefoglaló élhalmaszat: elhagyásával már minos $s \rightarrow t$ út G -ben

Ezek irányítatlan gráfokból száltak. Irányított gráfokkal is működik ($s \rightarrow t$ irányított út).

Menger tételai:

- G irányított gráf $\Rightarrow \lambda(s, t) = \lambda'(s, t)$
- $u-v$ pontösszerű, u és v nem szomszédos: $K(s, t) = K'(s, t)$
- G irányítatlan gráf, s és t nem szomszédos: $K(s, t) = K'(s, t)$
- $u-v$ pontösszerű, $\lambda(s, t) = \lambda'(s, t)$

1) Irányított, éldiszjunkt.



$\lambda(s, t) = 3$

$\lambda'(s, t) \geq \lambda(s, t)$, mert az egyes utaktól külön-külön 1 -et el lehet hagyni.

A minit 3 esetben is igaz.

$k := \lambda'(s, t)$ ennyi él elhagyásával minos út s és t között.

Lehet: $\exists k$ db út s -ből t -be.

$\langle G, s, t, k \rangle$: legyen az a hálózata.

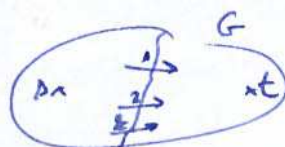
Hétköz ar k -os kapacitásműködés

min. költség a hálózaton k értékre

(azaz az utat kihasználva a feltételhez)

Er a költség minimális.

FF miatt másképpen is k megkérjük



egyensúlyosság

lemon

-2-

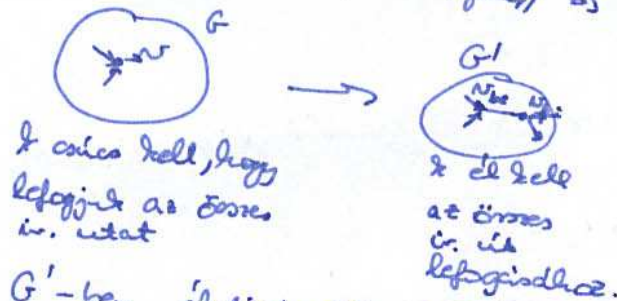
$\exists$ olyan max folyam, hogy vagy 0 vagy 1 meg k $\forall$ élen, értéke k .

Menger-tétel

$\lambda(s, t)$ - előszörjunkt utak max száma $K(s, t)$ - pontdiszjunkt...
 $\lambda'(s, t)$ - lefogó él max száma $K'(s, t)$

1.) Irányított gráfban $\lambda = \lambda'$, ~~$K = K'$~~

2.) s, t nem össze $(G$ ir. gráf) $\Rightarrow K(s, t) = K'(s, t)$



$$K'_s(s, t) = \lambda'_s(s, t) = \lambda_{G'}(s, t)$$

G' -ben előszörjunkt utak $\equiv G$ -ben pontdiszjunkt utak

$$\left. \begin{array}{l} K' \leq K \\ \text{de } K' \geq K \end{array} \right\} \Rightarrow K = K'$$

3.) s, t nem össze, G irányítatlan $\Rightarrow K(s, t) = K'(s, t)$



$$K'_G(s, t) = K_{G'}(s, t)$$

$$\text{tíli } K'_G(s, t) = 2$$

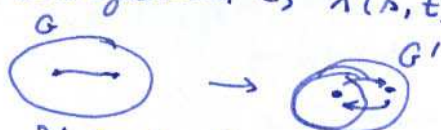
Ha ezt tekintjük G' -ben, és nem fogadjuk le $\Rightarrow$ lenne még irányított út is
 Ha G' -ben lefogja, akkor u. eset G -ben is, de tñk még marad. Vissza.
 akkor ez megjelenik G' -ben is

$$K'_G(s, t) = K_{G'}(s, t)$$

G' -ben a 2 db pontdiszjunkt ir. utak G -ben is megfelel 2 db pontdiszjunkt ir.

$$\exists K'(s, t)$$

4.) G irányítatlan $\Rightarrow \lambda(s, t) = \lambda'(s, t)$



$$\lambda'_G(s, t) = 2$$

$$\text{All: } \lambda'_G(s, t) \geq 2$$

Biz: Ind: $\lambda_{G'}(s, t) \leq 2-1 \Rightarrow G'$ -ben 2-1 ir. él elhagyva kéne lenni két közt ir.
 Ezt elvisszavetjük G -be ...

$$\lambda_{G'}(s, t) = 2$$

$\exists G'$ -ben 2 irányított út két közt.

Probléma lehet, hogy az egyik utat oda - vissza használhatjuk:



→ de akkor kihagyhatjuk ezt az élet.

Ha ilyen eset volt, akkor az élet elhagyva el tudtuk tényszerűsíteni.

Véges sok lépés után az összes ilyen eltűnt. Következésképpen az élethosszú utat nem változott. $\Rightarrow$ Mt.

Tétel: 1) G k -élj. $\Leftrightarrow \forall s, t \in V(G) : \lambda(s, t) \geq k$ (lokális élethosszúság)
2.) Legyen $G : n, k+1$ pontú gráf, akkor

G k -élj $\Leftrightarrow \forall s, t \in V(G) : K(s, t) \geq k$

1) Biz: " $\Leftarrow$ " Ind.: tfl nem k -szorosán élj. $\Rightarrow \exists$ max. $k-1$ él, amit elhagyva már nem élj.



$$\lambda'(s, t) \leq k-1$$

$$\stackrel{n}{\Rightarrow} \lambda(s, t) \leq k-1$$

" $\Rightarrow$ " Ind.: s és t között max $k-1$ él van:

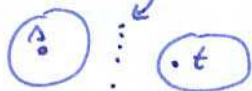


$$\lambda(s, t) \leq k$$

$$\stackrel{u}{\Rightarrow} \lambda(s, t) \leq k \quad \text{a gráf } k\text{-élj.}$$

2) Biz: " $\Leftarrow$ " $\forall$ pontpár $K(s, t) \geq k$

Ind.: tfl $\exists$ $k-1$ pont, amit elhagyva szétvált



$$K'(s, t) \leq k-1$$

s és t között nincs él

$$\stackrel{n}{\Rightarrow} K'(s, t) = K(s, t) \leq k-1$$

" $\Rightarrow$ " Ind.: tfl G k -élj, $\exists$ $t : K(s, t) \leq k-1$



$$a) \quad s \text{ és } t \text{ nem szomsz.} \Rightarrow K_G(s, t) = K'_G(s, t) \leq k-2$$

$k-1$ pontot elhagyva a gráf szétvált $\Rightarrow$ nem k -élj

b.) Szomszédosak

$\rightarrow$ ezt az élet elhagyjuk $\Rightarrow$ már nem szomsz. egyenlő gráf)

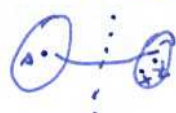


$$Uj \text{ gráfban } (G') \quad K_{G'}(s, t) = k-2$$

$$K'_{G'}(s, t) = k-2$$

G' -ből $k-2$ pontot elhagyva szétvált.

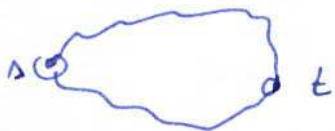
Eztet visszahelyezem G -be



Elhagyva a k max $k-2$ pontot és a $t-t$ a gráf szétvált.

$\exists x$, melytől min $k+1$ pont van G -ben $\Rightarrow s$ és x között mincs él

G 2-öf $\Leftrightarrow \forall s, t$ -re $\exists$ 2 pontdiszjunkt út



Altdef: G 2-öf $\Leftrightarrow$ bármely 2 pontján át $\exists$ kör.

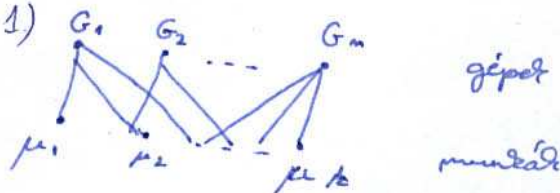
Dirac : G k-öf $\Rightarrow \forall k$ pontján át van kör.

Visszafelé nem igaz.



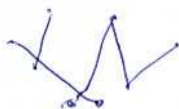
bármely 6 csúcsra át van kör, mégis csak 2-öf.

Párosítás



- Igaz-e, hogy egyszerre az összes munkát tudunk megoldani?
- Mennyi az a max munka, amit egyszerre tudunk végezni?

2) projektcsoport, egyes párokat tudunk ~~együtt~~ ^{együtt} megoldani $\rightarrow$ megoldható-e egyszerre az egész csoport



Párosítás: olyan élhalmaz, hogy minden 2 élnek nincs közös végpontja
↓
független él

Fgt él max száma a gráfban: $\nu(G)$

Teljes párosítás: $\forall$ csúcsra illeszthető él.

- 1) páros gráf $\rightarrow$ lehet plusz feltétel.
- 2) nem páros gráf

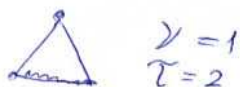
$\tau(G)$ = lefogló pontok minimális száma.

lefogló pont halmaz: $\forall$ élnek legalább az egyik végpontját tartalmazza.

Alt: $\tau(G) \geq \nu(G)$



azaz csak a fgt. élét lefoglaláshoz kell elszakítani.



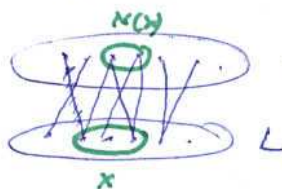
$\nu=1$
 $\tau=2$

König-tétel:

Alt: Páros gráfokban

$\tau(G) = \nu(G)$

Vagy olyan párosítás, hogy $\forall L$ legyen jó F -t.
Nem, mert kevesebb jó F , mint L .



$x \rightarrow N(x)$
 pontokhoz szomszédai

Hall-tétel:

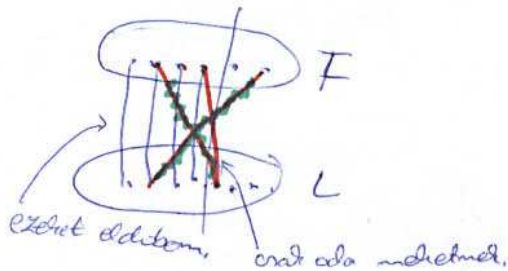
$G(L, F)$ páros gráfban L -et fedő párosítás $\Leftrightarrow \underbrace{\forall x \subseteq L : |N(x)| \geq |x|}_{\text{Hall-feltétel}}$

Frobenius-tétel:

$G(L, F)$ -ben $\exists$ teljes párosítás $\Leftrightarrow |L| = |F|$ és $\forall x \subseteq L : |N(x)| \geq |x|$

Hall-t. biz:

Javító utat módszere / jav. utas alg.



a zöld-párosítást kioldásvázzuk $(+2)$, helyettük egyet elhagyunk $(-1) \rightarrow$ továbbra is párosítás.

Javítás: L fedetlen részében fedődik, F fedetlen élében én véget, ps. szabadik éle a fedett részét közt meg.

Ha hi tudunk beilleszteni F fedetlen részén, akkor $\exists$ párosítás, ha nincs, akkor nincs.

$\mathbb{Z}$

Def: $a|b$ (a osztja b-nek), ha $\exists k \in \mathbb{Z} : a \cdot k = b$

$1|1$ $1|5$ $1|-17$, $-1|1$ $1|127$ 0|0
 $7|0$ $25|0$...

$2 \neq 0, 1, -1$ felbonthatatlan, ha csak $1, -1, 2$ és -2 osztja.
 pl: $1|7$ $-1|7$ $2|14$ $-2|14$

Számelmélet alaptétele: $\forall$ 0-tól, 1-től és -1-től kül. egész

1.) felbontható felbonthatatlanok szorzata.

2.) ez a felbontható egyértelmű (nem számítva a sorrendet és az esetleges (-1) -es szorzót).

$$20 = 2 \cdot 2 \cdot 5 = 2 \cdot 5 \cdot 2 = (-2) \cdot (-5) \cdot 2$$

2. verzió: $\forall$ 1-nél nagyobb egész:

1.) felbontható pr. felbonthatatlanok szorzataként

2.) ez a felírás a sorrendtől eltérőre egyértelmű

$$20 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5$$

$$\begin{array}{r}
 120 : 2 \\
 60 : 2 \\
 30 : 2 \\
 15 : 3 \\
 5 : 5
 \end{array}
 \quad
 120 = 2^3 \cdot 5 \cdot 3$$

Biz: 1.) a 2. verziótól az első azonnal következik: a negatívot megszorozzuk (-1) -gyel $\Rightarrow$ pozitív, amit egyértelműen fel tudunk bontani. $\rightarrow$ melyikre még hozzatekintünk egy (-1) -es szorzót.

2.) n ha felbonthatatlan $\Rightarrow$ —

ha nem: $n = a \cdot b$, $a \neq n$, $b \neq n$. ($\Rightarrow a < n, b < n$)

$\downarrow$
 ha nem felbonthatatlan: $a = a_1 \cdot a_2$
 $b = b_1 \cdot b_2$
 $\vdots$

amikor ezt már nem tudom folytatni $\rightarrow$ felbonthatatlanokat kaptunk.

ez az eljárás végetér legfeljebb $\log n$ lépésben, utána.

Vagy: teljes indukcióval:

2 ✓

Ha $\forall$ n -nél kisebbekre ✓

Kéna: n is felbontható $\rightarrow n$ felbonthatatlan $\Rightarrow$ —

$\Rightarrow n$ is felbontható

Egyszerűség: teljes ind:

2.1

Tfl, hogy n -nél kisebb (1 -nél nagyobb) számot felbonthatunk egyébr
Kéne. n felbontható is egyébr.

Ind: $n = p_1 \cdot p_2 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot \dots \cdot q_l$

Vegyük észre, hogy $p_i \neq q_j \quad \forall i, j$ -re, mert különben lecsökkenthetnénk a szorzatot.
Azaz ind. feltétel: 2 olyan kisebb számot kapunk, ami 2-féleképpen is felbontható (ind. felt.)

Legyen p_1 a legkisebb a p_i -k közül
 q_1 a q_i -k közül.

$$n' = p_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_l \quad (q_1\text{-et kicseréltük } p_1\text{-re})$$

$$n' = p_1 (p_2 \cdot \dots \cdot p_r - q_2 \cdot \dots \cdot q_r) = (q_1 - p_1) q_2 \cdot q_3 \cdot \dots \cdot q_l$$

1.) $n' > 0$ igaz, mert p_1 a legkisebb a p_i -k és q_i -k közül $\Rightarrow q_1 - p_1 > 0$

2.) $p_1 \mid n'$

3.) $n' > 1$

4.) $n' < n$ (n -ből pos. számot levontunk)

3, 4. $\Rightarrow n'$ felírása egyértelmű (felbonthatatlanok szorzataként)

$p_1 \mid n' \Rightarrow \exists$ olyan felírás ami p_1 -et tartalmazza. $\Rightarrow \forall$ felírásban benne van,
mert az a sorrendben tér el.

$$q_1 - p_1 := t_1 \cdot t_2 \cdot \dots \cdot t_s \Rightarrow \text{az } n' \text{ felbonthatatlanok szorzata. } (t_1 \cdot \dots \cdot t_s \cdot q_2 \cdot \dots \cdot q_l)$$

$$t_j = p_1$$

$p_1 \mid (q_1 - p_1) \Rightarrow p_1 \mid q_1$ $\frac{1}{2}$ mert q_1 -nek lehetne
olyan pos. osztója, és nem 1 és nem önmag.

Def: p prím tulajdonságú (prím), ha $p \mid ab \Rightarrow p \mid a$ v. $p \mid b$

All: 1) $\forall$ prím felbonthatatlan

2) $\forall$ felbonthatatlan prím

Biz: 1) p prím, tfl nem felbontható: $p = a \cdot b$ $\Rightarrow p \mid a \cdot b \begin{cases} \nearrow p \mid a \\ \searrow p \mid b \end{cases}$
 $a, b \neq p$

(a tfl a Flóris-jegyzetben, bocsi)

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

$(a, b) := \max \{ d : d|a \text{ és } d|b \}$ legnagyobb közös osztó

a, b relatív prím, ha $(a, b) = 1$

$[a, b] = \min \{ m \in \mathbb{N} : a|m, b|m \}$ legkisebb közös többszörös

Alapt. kör: $a|b \Rightarrow a$ kanonikus alakjában szereplő $\forall$ prím szerepel b -ben is, és legalább akkora kitevővel, mint a -ban.

(P) $(7, 14) = 7$ $(m, 1) = 1$ $(m, 0) = |m|$
 $(6, 8) = 2$ $(a, b) = (b, a)$ $(0, 0)$ nem def.

(T) (a, b) -t úgy kapjuk, hogy a és b kanonikus alakjából a közös prímszorzat a kisebb kitevő összeadásával.

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k}$$

(α_i és $\beta_i = 0$ is megengedett)

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdot \dots \cdot p_k^{\min(\alpha_k, \beta_k)}$$

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdot \dots \cdot p_k^{\max(\alpha_k, \beta_k)}$$

$$(a, b) \cdot [a, b] = a \cdot b$$

Def : $d(n) := n$ pozitív osztóinak száma.

All : $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} \Rightarrow d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \dots \cdot (\alpha_k + 1)$

↑
 osztó lehetséges kanonikus alakjainak száma (0 és α_i között minden, ezek összes kombinációja)

All : $(a, b) = (a-b, b)$

Biz: $d|a, d|b \Rightarrow d|a-b \Rightarrow a$ és b közös osztói osztják $a-b$ -t is.
 $d'|a-b, d'|b \Rightarrow d'|a-b+b=a \Rightarrow a-b$ és b közös osztója osztja a -t is $\Rightarrow$ közös osztóik, így a legnagyobb is.

Köv: $(a, b) = (a-b, b) = (a-k \cdot b, b)$

Euclidesei algoritmus:

Input: $a > b$ egész

Output: (a, b)

$$a_0 = a \quad a_1 = b$$

$$a_0 = a_1 \cdot h_1 + a_2$$

$$0 \leq a_2 < a_1$$

$$\begin{aligned} a_1 &= a_2 \cdot h_2 + a_3 & 0 \leq a_3 < a_2 \\ &\vdots \\ a_{k-1} &= a_k \cdot h_k + 0 \\ (a_0, a_1) &= (a_1, a_2) = \dots = (a_k, a_{k+1}) = (a_k, 0) = a_k \end{aligned}$$

$$(216, 144) = (144, 72) = (72, 0) = 72$$

Ez egy gyors algoritmus:

$$a_{k+2} < \frac{a_k}{2} \rightarrow \text{gyorsan csökkennek a számok.}$$

Alk: ~~(a,b)~~ $a, b \in \mathbb{Z} \Rightarrow \exists k, l \in \mathbb{Z} : \underline{a = k \cdot a + l \cdot b}$
 $k \cdot a + l \cdot b = (a, b)$

Legyen $a_0 = a, a_1 = b$.

Tekintsük az Euklideszi algoritmust. Kapjuk az $a_1, a_2, \dots$ számokat.

Világos, hogy ha a_i és a_{i+1} előáll a és b egész ^{egyszerűsített} lin. komb. jatekát $\Rightarrow$ a_{i+1} is előáll. Eukl. alg-ból k és l is kiszámítható

Tétel: Végtelen sok prím van.

Biz: Elég, hogy teljesítse $\exists$ n -nél nagyobb prím.

Tekintsük: $n! + 1 = t$.

$1 \leq d \leq n \Rightarrow d \nmid n! + 1 = t. \Rightarrow N$ kanonikus alakjában csak n -nél nagyobb prímek vannak.

Tétel: Szomsz. prímsz. közt mindig ^{egyszerűsített} többszörösen nagy lehet

Chebisev-tétel: $n > 1$ n és $2n$ között $\exists$ prím

Biz: n megítélt.

Tel: $n! + 2, n! + 3, \dots, n! + n \leftarrow n-1$ db szám.

$i \mid n! + i \Rightarrow$ találtam $n-1$ ^{egyszerűsített} összetett számot $\rightarrow$ teljes. sor.

Dirichlet-tétel: (a, d) rel. prímek $\Rightarrow a, a+d, a+2d, a+3d, \dots$ sorrel. prímek

Def: $a \equiv b \pmod{m}$ - hivatkozás jelölés

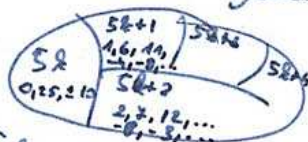
$a \equiv b \pmod{m}$, ha $m \mid a-b$ ("a és b m -mel osztva m -at a maradékot adják")

Pl: $2 \equiv 17 \pmod{15}$

2-nel kongr. számok mod 15: 2, 17, 32, 47, ..., -3, -8, -13, ...

Teljes $m > 2$ -re $\mathbb{Z}$ m diszjunkt ~~res~~ osztályba (maradék osztályba) sorolható:

- azonos osztálybeliek kongr. mod m .
- küll osztálybeliek nem kongr. mod m .



Def: Teljes maradékrendszer mod m : $a_1, a_2, \dots, a_m \in \mathbb{Z}$ úgy, hogy $\forall$ maradék osztályból (mod m) választott egy többszörösen szám.

Pl: mod 5: 0, -3, 3, 8, 15 THM
 0, 1, 2, 3, 4 THM

Alk: $a \equiv b \pmod{m}$
 $c \equiv d \pmod{m}$
 $b \equiv a \pmod{m}$

$$\Rightarrow \begin{aligned} a+c &\equiv b+d \pmod{m} \\ a-c &\equiv b-d \pmod{m} \\ a \cdot c &\equiv c \cdot d \pmod{m} \end{aligned}$$

$$\begin{aligned} a+c-(b+d) &= (a-b) + (c-d) \\ &\equiv 0 \pmod{m} \quad \begin{matrix} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{matrix} \end{aligned}$$

$$\begin{aligned} a \cdot c - b \cdot d &= ac - bc + bc + bd = \\ &= (a-b)c + b(c+d) \\ &\equiv 0 \pmod{m} \quad \begin{matrix} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{matrix} \end{aligned}$$

All: $k \in \mathbb{Z}$ $a \equiv b \pmod{m} \Leftrightarrow a+k \equiv b+k \pmod{m} \Leftrightarrow a-k \equiv b-k \pmod{m}$

Biz: $m \mid a-b \Leftrightarrow m \mid (a+k)-(b+k)$

All: $d \mid a, d \mid b : a \equiv b \pmod{m} \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{(m,d)}}$

Biz: $a = a' \cdot d$

$b = b' \cdot d$

$D = (m, d) \rightarrow m = m' \cdot d$

$a = a' \cdot d$

$a \equiv b \pmod{m} \Leftrightarrow m \mid a-b \Leftrightarrow m' \cdot d \mid a' \cdot d - b' \cdot d = d(a'-b') =$

$= d \cdot d'(a'-b') \Leftrightarrow m' \mid d'(a'-b')$

$(m', d') = 1$, mert a h -val osztottunk d -vel.

d' kanonikus alakjában nem szerepelhet m' prímszorosa.

$m' \mid d'(a'-b') \Rightarrow m' \mid a'-b' \Leftrightarrow a' \equiv b' \pmod{m'}$

$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{(m,d)}}$

Kör: Tfl $a_1, a_2, \dots, a_m$ TMR mod $m, k \in \mathbb{Z}$

(teljes maradék rendszer)

$(a, m) = 1 \Rightarrow a_1+k, a_2+k, \dots, a_m+k$ TMR
 $a \cdot a_1, a \cdot a_2, \dots, a \cdot a_m$ TMR

Biz:

m szám pontosan akkor alkot TMR-t mod m , ha páronként nem kongruens egymással.

Tfl $a_i+k \equiv a_j+k \pmod{m} \Rightarrow a_i \equiv a_j \pmod{m} \Rightarrow i=j$ ✓

Tfl $a \cdot a_i \equiv a \cdot a_j \pmod{m} \Rightarrow a_i \equiv a_j \pmod{\frac{m}{(m,a)}} \Rightarrow a_i \equiv a_j \pmod{m} \Leftrightarrow a_i = a_j$

Lineáris kongruencia : $ax \equiv b \pmod{m}$, ahol $a, b, m \in \mathbb{Z}$ adott és x ismeretlen

Tétel: Az $ax \equiv b \pmod{m}$ lin kongruencia megoldható $\Leftrightarrow (a, m) \mid b$

Ha megoldható $\Rightarrow$ a megoldások (a, m) db mod m maradékok osztályát alkotnak

$5x \equiv 3 \pmod{7}$
 $15x \equiv 9 \pmod{7}$
 $15 \equiv 1 \pmod{7}$
 $9 \equiv 2 \pmod{7}$
 $x \equiv 2 \pmod{7}$

Biz: $d = (a, m)$ $ax \equiv b \pmod{m} \Leftrightarrow m \mid ax-b \Rightarrow d \mid ax-b \Rightarrow d \mid a \Rightarrow d \mid ax$ $\Rightarrow d \mid b$

Ha a kongr. mo-lható $\Rightarrow (a, m) \mid b$

" Tfl $d \mid b$ Cél: d maradékosztály elégíti ki a kongruenciát.

$a = a' \cdot d$ $ax \equiv b \pmod{m} \Leftrightarrow a' \cdot dx \equiv b' \cdot d \pmod{m' \cdot d} \Leftrightarrow a'x \equiv b' \pmod{m'}$
 $m = m' \cdot d$
 $b = b' \cdot d$ $\text{Itt } (a', m') = 1$

Euklideszi algoritmust elvégezve a' és m' számokra fel tudjuk írni h -t a két szám egységes kombinációjaként: $1 = h \cdot a' + l \cdot m' \Rightarrow h \cdot a' \equiv 1 - l \cdot m' \pmod{m'}$

$a'x \equiv b' \pmod{m'} \Rightarrow h \cdot a'x \equiv h \cdot b' \pmod{m'} \Leftrightarrow (1 - l \cdot m')x \equiv h \cdot b' \pmod{m'} \Leftrightarrow x - l \cdot m'x \equiv h \cdot b' \pmod{m'}$

$\Rightarrow \boxed{x \equiv h \cdot b' \pmod{m'}}$ Azaz a mo-t pontosan 1 db mod m' maradékosztályt alkotnak.

Atkérlek ezt mod m maradékosztályra:

$$x \equiv b' (m) \Leftrightarrow x \equiv b' (m) \text{ vagy } x \equiv b' + m' (m) \text{ vagy } x \equiv b' + 2m' (m) \text{ vagy}$$

$$\text{vagy } x \equiv b' + (d-1)m' (m) \quad \checkmark$$

Megf: $a \equiv b (m) \Leftrightarrow (a, m) = (b, m)$

Biz: $m | a-b \Leftrightarrow b = a + m \cdot k$

$$(a, b) = (a, a + mk)$$

$$(b, m) = (a + mk, m) \stackrel{p}{=} (a + mk - mk, m) = (a, m) \quad \text{Q.E.D.}$$

Lemma: $(x, y) = (x+ty, y) = (x+ly, y)$

Köv: Ha egy mod m maradékosztályban egy eleme m -hez rel. prím $\Rightarrow$
 $\forall$ eleme rel. prím m -hez.



Def: az m -hez rel. prímeket tartalmazó

mod m maradékosztályok számát $\varphi(m)$ jelöli

$a_1, a_2, \dots, a_{\varphi(m)}$ redukált maradékhalmaz (RMR), ha $\forall$ rel. prím
 maradékosztályból választottunk 1-1 elemet

Elv: RMR = Éggy TMR-ből elhagyjuk az m -hez nem rel. prím részeket.

Köv: $\varphi(m)$ úgy is definiálható, hogy az $0, 1, 2, \dots, m-1$ TMR-ből az
 m -hez relatív prím részeket számlálva.

R: $\varphi(6) = 2 \quad \varphi(3) = 2 \quad \varphi(4) = 2 \quad p \text{ prím } \varphi(p) = p-1 \quad \varphi(p^n) = p^n - p^{n-1}$

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

Lemma: $a_1, a_2, \dots, a_{\varphi(m)}$ RMR^T, $(a, m) = 1 \Rightarrow a a_1, a a_2, \dots, a a_{\varphi(m)}$ RMR^(mod m)

Biz: Csak az kell, hogy $\forall$ rel. prím. maradékosztályból pontosan 1 elemet
 tartalmaz az $a a_1, \dots, a a_{\varphi(m)}$ sorozat

Kell: (1) $a a_i$ rel. prím m -hez

(2) $a a_i$ részek páronként különbözőek mod m -ben tartoznak

(1): $(a a_i, m) = 1$, mert m -nek nincs közös prímszorosa sem a -val,
 sem a_i -vel. $\checkmark$

(2): If $a a_i \equiv a a_j (m) \Rightarrow a_i \equiv a_j \left(\frac{m}{(m, a)} \right) \Rightarrow a_i \equiv a_j (m) \Rightarrow i=j$ Q.E.D.

Biz (E-F): Legyen $a_1, a_2, \dots, a_{\varphi(m)}$ RMR $\pmod{m}$. Adott a , amire $(a, m) = 1$.

Lemma miatt $a a_1, a a_2, \dots, a a_{\varphi(m)}$ is RMR $\Rightarrow a \cdot a_1 \cdot a_2 \cdot \dots \cdot a_{\varphi(m)} \equiv a \cdot a_1 a_2 \dots a_{\varphi(m)}$
 $\prod_{i=1}^{\varphi(m)} a_i \equiv a^{\varphi(m)} \cdot \prod_{i=1}^{\varphi(m)} a_i \pmod{m} \Rightarrow a^{\varphi(m)} A \equiv A \pmod{m} \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$

$A \rightarrow$

$(m, A) = 1$ (mert minden rel. pr. számok szorzata)

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

□

Köv. Kis Fermat tétel: p prím $\Rightarrow a^p \equiv a \pmod{p}$

Biz: I: $(a, p) = 1 \rightarrow EF$ miatt $a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod{p} \quad / \cdot a$

$$a^p \equiv a \pmod{p}$$

II: $(a, p) \neq 1 \Rightarrow p | a \Rightarrow a^p \equiv 0 \pmod{p} \Rightarrow a \equiv 0 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$

Lemma: $(m, n) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ (φ multiplikatív függvény)

Biz: $1, 2, 3, \dots, m \cdot n - 1$ számok közül az $m \cdot n$ -hez rel. prímek száma $\varphi(m \cdot n)$

a rel. prím $m \cdot n$ -hez az a sem n , sem m prímtényezőjével nem osztható

($\Rightarrow$) a és n rel. prím
 a és m rel. prím.

Teljesítmények: $1, 2, 3, \dots, m$
 $m+1, m+2, \dots, 2m$
 $2m+1, 2m+2, \dots, 3m$
 $\vdots$
 $(n-1)m+1, (n-1)m+2, \dots, nm$

Itt az m -hez rel. prím számok $\varphi(m)$ oszlop

állhatnak ($\forall$ oszlop n -es $a \pmod{m}$ m.ig)

Tel. egy oszlop: $i, m+i, 2m+i, \dots, (n-1)m+i$

$0, 1, 2, \dots, m-1$ TMR $\pmod{m} \Rightarrow 0, m, 2m, \dots, (n-1)m$ TMR $\pmod{m} \Rightarrow$

$\Rightarrow i, m+i, 2m+i, 3m+i, \dots, (n-1)m+i$ TMR

$\forall$ oszlop TMR $\pmod{m} \Rightarrow \forall$ oszlopban $\varphi(m)$ db m -hez rel. prím szám van.

A keresett számok $\varphi(m)$ oszlopban azok, amik m -hez rel. prímek. $\forall$ oszlop TMR (m)

$\Rightarrow \forall$ oszlopban $\varphi(m)$ db m -hez rel. prím áll $\Rightarrow \varphi(m) \cdot \varphi(n)$ db a rel. prímek száma

Köv. $n = \prod_{i=1}^k p_i^{\alpha_i} \Rightarrow \varphi(n) = \varphi\left(\prod_{i=1}^k p_i^{\alpha_i}\right) = \prod_{i=1}^k \varphi(p_i^{\alpha_i}) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1})$

$$= \prod_{i=1}^k p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^k p_i^{\alpha_i} \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Biz (E-F): Legyen $a_1, a_2, \dots, a_{\varphi(m)}$ RMR $\pmod{m}$. Adott a , amire $(a, m) = 1$.

Lemma miatt $a a_1, a a_2, \dots, a a_{\varphi(m)}$ is RMR $\Rightarrow a_1 \cdot a_2 \cdot \dots \cdot a_{\varphi(m)} \equiv a \cdot a_1 \cdot a_2 \cdot \dots \cdot a_{\varphi(m)}$
 $\prod_{i=1}^{\varphi(m)} a_i \equiv a^{\varphi(m)} \cdot \prod_{i=1}^{\varphi(m)} a_i \pmod{m} \Rightarrow a^{\varphi(m)} A \equiv A \pmod{m} \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$

$A \rightarrow$

$(m, A) = 1$ (mert minden rel. pr. számok szorzata)

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

□

Köv: Kis Fermat tétel: p prím $\Rightarrow a^p \equiv a \pmod{p}$

Biz: I: $(a, p) = 1 \rightarrow$ EF miatt $a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod{p} \quad / \cdot a$

$$a^p \equiv a \pmod{p}$$

II: $(a, p) \neq 1 \Rightarrow p | a \Rightarrow a^p \equiv 0 \pmod{p} \Rightarrow a \equiv 0 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$

Lemma: $(m, n) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ (φ multiplikatív függvény)

Biz: $1, 2, 3, \dots, m \cdot n - 1$ számok közül az $m \cdot n$ -hez rel. prímek száma $= \varphi(m \cdot n)$

a rel. prím $m \cdot n$ -hez az a sem n , sem m prímtényezőjével nem osztható

($\Rightarrow$) a és n rel. prím
 a és m rel. prím.

Teljesítmények: $1, 2, 3, \dots, m$
 $m+1, m+2, \dots, 2m$
 $2m+1, 2m+2, \dots, 3m$
 $\vdots$
 $(n-1)m+1, (n-1)m+2, \dots, nm$

Itt az m -hez rel. prímek száma $\varphi(m)$ oszlopot

alkotnak ($\forall$ oszlop n -es $a \pmod{m}$ m.ig)

Tel. egy oszlop: $i, m+i, 2m+i, \dots, (n-1)m+i$

$0, 1, 2, \dots, m-1$ TMR $\pmod{m} \Rightarrow 0, m, 2m, \dots, (n-1)m$ TMR $\pmod{m} \Rightarrow$

$\Rightarrow i, m+i, 2m+i, 3m+i, \dots, (n-1)m+i$ TMR

$\forall$ oszlop TMR $\pmod{m} \Rightarrow \forall$ oszlopban $\varphi(m)$ db m -hez rel. prím szám van.

A keresett számok $\varphi(m)$ oszlopban azok, amik m -hez rel. prímek. $\forall$ oszlop TMR (m)

$\Rightarrow \forall$ oszlopban $\varphi(m)$ db m -hez rel. prím áll $\Rightarrow \varphi(m) \cdot \varphi(n)$ db a rel. prímek száma

Köv: $n = \prod_{i=1}^k p_i^{\alpha_i} \Rightarrow \varphi(n) = \varphi\left(\prod_{i=1}^k p_i^{\alpha_i}\right) = \prod_{i=1}^k \varphi(p_i^{\alpha_i}) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1})$

$$= \prod_{i=1}^k p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^k p_i^{\alpha_i} \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Algebra

Def: H halmazon n -változós művelet $f: H^n \rightarrow H$ leképezés.
(egy szám - esetleges egy ugyanazon halmazbeli számot rendel)

Pé: $f(a, b, c) := a(b+c)$ $a, b, c \in \mathbb{R}$, 3 változós művelet

$f(x) = x^2 + 3x - 5$ $x \in \mathbb{R}$ 1 változós művelet

$+$: $\mathbb{R}^2 \rightarrow \mathbb{R}$ Jel: $+(a, b)$ helyett $a+b$

V vektortér ($\mathbb{R}$ felett), $+$ V -n művelet

$V \times V \rightarrow V$, skalárral való szorzás nem művelet (mert nem ugyanaból a halmazból származik)

Def: $S = \langle H, \{f_i: i \in I\} \rangle$ egy algebrai struktúra, ha $\forall f_i$ egy (valahány változós) művelet a H -n.

Pé: $\langle \mathbb{R}, \{+, -\} \rangle$

Def: Tegyük fel, hogy $*$ egy (2 változós) művelet H -n. $*$ kommutatív (felcserélhető), ha $a * b = b * a \quad \forall a, b \in H$.

Pé: $+$, $\cdot$ $\mathbb{R}$ -n, $-$ nem
 N hatványozás nem.

$*$ asszociatív (átrendezhető), ha $(a * b) * c = a * (b * c) \quad \forall a, b, c \in H$

Pé: $+$, $\cdot$ ($\mathbb{R}$ -n) asszociatív, $-$ nem assz.: $a - (b - c) \neq (a - b) - c$

Def: $S = \langle H, * \rangle$ félcsoport, ha $*$ asszociatív.

Abel-félcsoport, ha $*$ kommutatív és asszociatív.

$\mathbb{R}$ az előzőkben:

	assa	nem assz
kommut	$+$, $\cdot$	$\mathbb{R}$ -n szorzat. híz: $\frac{a+b}{2}$ ($\neq$ lecserélési)
nem kommut	$m \times n$ -es mtr. szorzása	N -n hatványozás

Pé: $m \times n$ -es mtr. szorzása

$m \times n$ -es szimmetrikus mtr. szorzása Abel-félcsoport

Def: $S = \langle H, * \rangle$ str., $e \in H$ egységelem, ha $e * a = a * e = a \quad \forall a \in H$

Pé: $\langle \mathbb{R}, \{+, \cdot\} \rangle$ $+$ egységeleme: 0
 $\cdot$ egységeleme: 1

$m \times n$ mtr. szorz. $+$ egységeleme: $\mathbb{Q}$
 $\cdot$ egységeleme: I_n - 1

Alt: Ha $\langle H, * \rangle \exists$ egységelem, akkor az egységelemű.

Biz: $e, e' \in H$ egységelemek

$$e = e * e' = e' \Rightarrow e = e' \quad (\text{transzitiv})$$

Def: $\langle H, * \rangle$ $e \in H$ egység. $h \in H$ inverze az a $h' \in H$, amire
 $h * h' = h' * h = e$

Pé: $\langle \mathbb{R}, \{+, \cdot\} \rangle$ + inverze: $-a \rightarrow \forall \text{ elem} \exists \text{ inverze}$

• inverze: $\frac{1}{a} \rightarrow \forall \text{ elem} \exists \text{ inverze}$.

Meg: h inverzének jelölése h^{-1}

Def: $\langle G, \cdot \rangle$ strukturális csoport, ha

félcsoport (=assziatív)

$\exists$ egységelem.

$\forall g \in G \exists g^{-1}$ inverze.

$\langle G, \cdot \rangle$ Abel-csoport, ha $\langle G, \cdot \rangle$ csoport és $\cdot$ kommutatív.

Konvenció: Ha a csop. művelete a $\cdot$, és es nem szokás félredőltet, akkor a csoportot G -vel jelöljük.

Pé: $\langle \mathbb{R}, + \rangle$ Abel csoport

$\langle \mathbb{Z}, + \rangle$ Abel csop.

$\langle \mathbb{N}, + \rangle$ nem csop. (micsin inverzelem)

$\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$ Abel-csop

$\langle \mathbb{R}^{n \times k}, + \rangle$ Abel-csop

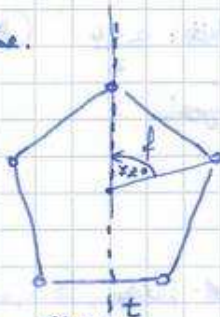
$n \times n$ -es invertálható mtr.-ok a $+$ -ra:

- | | |
|-------------|--|
| (1) műv. | (2) nem kommut. |
| (1) assz. ✓ | (3) $\exists 1$ |
| | (4) $\exists$ invers $\Rightarrow$ csop. |

Def: D_n dieder-csoport elemei a szabályos

n szög egybevágóságai. A művelet pedig a kompozíció, azaz az egybevágóságok egymásután végezte.

Pé: D_5 elemei:



$f, f^2 = f \cdot f, f^3 = f \cdot f \cdot f, f^4, f^5 = \text{id} \rightarrow$ egységelem

t is szimmetria: $t, t^2 = t \cdot t = \text{id}$

$t \cdot f =$ forgat majd tükröz.

$t \cdot f = f^{-1} \cdot t$



Alt: D_n csoport, de nem Abel!

(2) D_n -nek $2n$ eleme van.

Biz: (1) (0) műveletünk van. ✓

(1) assz.: $f \circ g$ kompozíciója assz.: $f(g(h(x))) = (f \circ g)(h(x))$

(2) egységelem az id. egybevágóság.

(3) $\exists$ invers: t kétsz. egybevágóság, $t^{-1} = t$ inverze, és az is fenn hagyja a szab. n -szöget

(2) m db forg. szám és n db teng. szám.

Def: G csoport rendje $|G|$

Az előző állítás: $|D_n| = 2n$.

Def: $H \leq G$ csoport és $H \leq G$. H normális ($H \trianglelefteq G$), ha H csoportot alkot G műveletére nézve (Azaz (1) G művelete nem vezet ki H -ből.

$$(2) e \in G \Rightarrow e \in H$$

$$(3.) \forall h \in H \ h^{-1} \in H.$$

$$\exists \langle \mathbb{Z}, + \rangle \leq \langle \mathbb{R}, + \rangle$$

All: (1) G csoport. $H, K \leq G \Rightarrow H \cap K \leq G$ ($\forall$ 2 részcsop. metszete részcsop.)

(2) Tetszőlegesen sok részcsop. metszete részcsop.

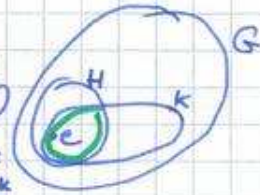
Biz: (1) Kell: (0) műv. nem vezet ki $H \cap K$ -ből.

$$\begin{aligned} \text{Tgk. } a, b \in H \cap K &\Rightarrow a, b \in H \Rightarrow a \cdot b \in H \\ &\Rightarrow a, b \in K \Rightarrow a \cdot b \in K \\ &a \cdot b \in H \cap K \end{aligned}$$

$$(1) e \in H \cap K, de e \in H, e \in K \Rightarrow e \in H \cap K$$

$$(2) g \in H \cap K \Rightarrow g \in H \Rightarrow g^{-1} \in H \Rightarrow g^{-1} \in H \cap K$$

$$\Rightarrow g \in K \Rightarrow g^{-1} \in K$$



(2) $\neg B$

Def: G csoport, $K \leq G$ a K által generált részcsop. ($\langle K \rangle$) a K -t tartalmazó részcsop. metszete.

Def: A G csoport triviális részcsop. : $G, \{e\}$

Megf: A $\langle K \rangle$ jól definiált és az a legszűkebb olyan részcsop. G -nek, ami K -t tartalmazza.

$$\text{Pl: } \langle \mathbb{Z}, + \rangle \quad K := \{6, 18, 12, 9\}$$

$$\langle K \rangle \ni 6, 18, 12, 9, 0, -6, -12, -18, -9, 30, 15, -30, -15, \dots$$

$$\langle K \rangle = \langle 3\mathbb{Z}, + \rangle \text{ (3-mal osztható számok halmaza)}$$

Def: G csoport ciklikus, ha $\exists g \in G: G = \langle g \rangle$ (Egy elem által generált csoport)
 g a generátorelem.

Ha g gen. elem $\Rightarrow e, g, g^2, g^3, \dots, g^{-1}, g^{-2}, g^{-3}, \dots \in \langle g \rangle$

① $e, g, g^2, \dots$ köl. elemek.

All: Ellen $g^{-i} = g^i$

Biz: Eft $g^{-i} = g^i \Rightarrow g^{-i} \cdot g^i = g^i \cdot g^i$

$$g^{-i} \cdot g^i = (\underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{i \text{ db}}) \cdot (\underbrace{g \cdot g \cdot g \cdot \dots \cdot g}_{i \text{ db}}) = (g^{-1} (g^{-1} \dots (g^{-1} g) \dots g) g) = e$$

$$g^i \cdot g^i = (\underbrace{g \cdot g \cdot \dots \cdot g}_{i \text{ db}}) (\underbrace{g \cdot g \cdot \dots \cdot g}_{i \text{ db}}) = g^{2i} \Rightarrow g^{2i} = e \quad \text{ha}$$



① -ban a $\langle g \rangle = G$ elemei: $e, g, g^{-1}, g^2, g^{-2}, \dots$ művelet $g^a \cdot g^b = g^{a+b}$

Pl: $\langle \mathbb{Z}, + \rangle =$ ciklikus csoport

② $g^i = g^j \quad i < j \Rightarrow g^{j-i} = g^i \cdot g^{-i} = g^j \cdot g^{-i} = (g \cdot g \cdot \dots \cdot g) \cdot g^{-i} = (g \cdot g \cdot \dots \cdot g) (g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}) = g^{j-i} = g^i$

Ellen vizsgáljuk (másképp k) hatványait e lesz. Ellen $g^k = e$
 (k a legkisebb ilyen egész)

$$g^{-1} = g^{k-1}, \text{ hisz } g \cdot g^{k-1} = g^k = e$$

$$g^i \cdot g^j = g^{i+j} = g^{i+j \pmod k}$$

$$e = g^{k-i}$$

Ellen a ciklikus csoportnak k eleme van, és a művelet is adott.

Pl: $\langle \mathbb{Z}_m, + \rangle$, ahol $\mathbb{Z}_m$ a mod m maradékosztályok halmaza

Itt $\mathbb{Z}_m$ -re lehet úgy is gondolni, hogy $\langle \mathbb{Z}_m, + \rangle \cong \langle \{0, 1, \dots, m-1\}, +_m \rangle$

$$\langle \mathbb{Z}_m, + \rangle = \langle 1 \rangle$$

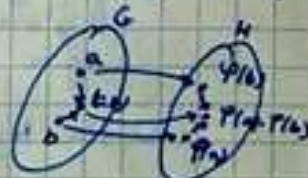
mind k elemű

Tétel: G ciklikus $\Rightarrow G$ Abel. Tetszőleges $H \leq G$ esetén H ciklikus.

Def: G in H csoport izomorf, ha $\exists \varphi: G \rightarrow H$ bijekció: $\forall a, b \in G \quad \varphi(a) \cdot \varphi(b) = \varphi(ab)$

Def: G csoport rendje $|G|$, azaz G elemszáma

$g \in G$ rendje $\langle g \rangle$ rendje, azaz $|\langle g \rangle|$.



All: g rendje a legkisebb olyan k , amire $g^k = e$. Ha nincs ilyen k , akkor a rendje végtelen.

Szimmetrikus csoportok

Def: Az S_n szimmetrikus csoport elemei az $1, 2, \dots, n$ elemek permutációi. A művelet pedig a kompozíció, azaz a permutációk egymásután végzése

Meg: $|S_n| = n!$

$$P\ell: \pi = \begin{array}{|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 \\ \hline 3 & 2 & 4 & 1 & 5 \\ \hline \end{array}$$

$$\sigma = \begin{array}{|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 \\ \hline 3 & 4 & 5 & 1 & 2 \\ \hline \end{array}$$

$$\pi \circ \sigma = \begin{array}{|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 \\ \hline 4 & 1 & 5 & 3 & 2 \\ \hline \end{array}$$

$$\pi \circ \sigma(k) = \pi(\sigma(k))$$

G_n csoport: 0 művelet

$$(\pi \circ \sigma) \circ \rho = \pi \circ (\sigma \circ \rho) \text{ asszociatív}$$

$$e = id.$$

π^{-1} inverzpermutáció



Tétel: G véges cirkuláris csoport $\Leftrightarrow \exists g \in G$, amire g rendje $= |G|$

Biz: cirkuláris $\Rightarrow \exists$ gen. elem és az jó

$$g \text{ rendje } n \Rightarrow |\langle g \rangle| = n = |G| \text{ és } \langle g \rangle \leq G \Rightarrow \langle g \rangle = G \Rightarrow G \text{ cirkuláris}$$

Megjegyzés: $D_n \leq S_n$

$n > 2$ -re S_n nem Abel

Def: Permutáció csoport: S_n részcsoportha valamilyen n -re.

Cayley-tétel: Tetszőleges véges G csoport izomorf egy permutáció csoporttal. 7B.

Def: $H, K \leq G$ csop. $H \cdot K = \{h \cdot k : h \in H, k \in K\}$ komplementumok

$$H \leq G \Rightarrow g \quad H \cdot g = H \cdot \{g\}, \quad g \cdot H = \{g\} \cdot H \text{ jobb és baloldali mellékcsoporth}$$

Pé: $G = \langle \mathbb{Z}, + \rangle$ $H = 10\mathbb{Z}$ mellékcsoporthot: $H + m$ m maradékosztály mod 10
 $\hookrightarrow$ Abel $\Rightarrow$ jobb és bal mellékcsoporth egyenlő.

Megf: $H \leq G \ni g, g'$:

- (1) $g \in H \cdot g$
- (2) $g' \in H \cdot g \Rightarrow H \cdot g = H \cdot g'$
- (3) vagy $H \cdot g = H \cdot g'$ vagy $H \cdot g \cap H \cdot g' = \emptyset$
- (4) $|H \cdot g| = |H|$

Biz: (1) $g \in e \cdot g \in H \cdot g$
 (2) $g' \in H \cdot g \Rightarrow g' = h \cdot g \Rightarrow h^{-1} \cdot g' = h^{-1} \cdot (h \cdot g) = e \cdot g = g \Rightarrow H \cdot g = H \cdot g'$
 $H \cdot g' = H(h \cdot g) = (H \cdot h) \cdot g \in H \cdot g$
 $H \cdot g = H(h^{-1} \cdot g') = (H \cdot h^{-1}) \cdot g' \subseteq H \cdot g$

(3) Ha $H \cdot g \cap H \cdot g' \neq \emptyset \Rightarrow g'' \in H \cdot g \cap H \cdot g'$ (2) miatt $H \cdot g = H \cdot g'' = H \cdot g'$

(4) T.é. $h \mapsto h \cdot g$ megfeleltetés, $\mathbb{Z}$ H -ből $H \cdot g$ -be hat és bijektív: injektív -
 injektív: $h \cdot g = h' \cdot g \Rightarrow \frac{h \cdot g \cdot g^{-1}}{h} = \frac{h' \cdot g \cdot g^{-1}}{h'}$

Lagrange tétele: $H \leq G \Rightarrow |H| \mid |G|$



Biz: Tekintsd a H szerint jobbra. oszt. hat. A két. m.o. g osztályokba. H elemek

fednek. (1) Ezek mindeke abba H -ba miatt. Ha g alsó két. mellék. van $\Rightarrow |G| = k \cdot |H|$

Lagrange-t. kőr: $g \in G \Rightarrow g$ rendje osztja $|G|$

Biz: g rendje = $\langle g \rangle$ rendje.

Def: $\langle R, \{+, \cdot\} \rangle$ gyűrű, ha

- (1) $\langle R, + \rangle$ csoport (egységjelle 0)
- (2) $\langle R, \cdot \rangle$ félcsoport (egységjelle 1, ha van)
- (3) Distributivitás igaz: $(a+b) \cdot c = a \cdot c + b \cdot c$
 $a(b+c) = ab + ac$ $\forall a, b, c \in R$

R kommutatív, ha $\cdot$ kommutatív

Pé: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

nem gyűrű pl $\mathbb{N}$ (mivel az összeadás irány)

$n \in \mathbb{Z}$

$\mathbb{Z}_m$ tulajdonképpen $\{0, 1, \dots, m-1\}$ elemeken a $+$ és $\cdot$.

Boole gyűrű: $\langle \mathcal{P}(H), \{\Delta, \cap\} \rangle$

$\langle \mathcal{P}(H), \Delta \rangle$ Abel-csopt.
 $0 = \emptyset, A^{-1} = A$

kommutatív gyűrű



Def: R gyűrű $n \in \mathbb{Z}$ nullasztó, ha $n \neq 0$ és $\exists 0 \neq r \in R: n \cdot r = 0$

R gyűrű nullszorzómentes, ha $\nexists$ nullasztó

R gyűrű integritási tartomány, ha R nullszorzómentes és kommutatív.

Pé: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ m.o.m.

$\mathbb{Z}_m$ m.o.m. $\Leftrightarrow m$ prím.

Boole gyűrű: $\forall$ valódi részalgebra nullasztó

Def: T test, ha (1) T gyűrű
 (2) $\langle T \setminus \{0\}, \cdot \rangle$ csoport.

T test, ha felede test és $\cdot$ kommut.

Megf: R gyűrű $\Rightarrow 0 \cdot a = 0 \quad \forall a \in R$.

$$0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a \quad (+ (0a)^{-1})$$

$$\Downarrow$$

$$0 = 0 \cdot a.$$

van-e inverze? $0 = 0+0 \Rightarrow 1 = 0 \cdot 0^{-1} = (0+0) \cdot 0^{-1} = 0 \cdot 0^{-1} + 0 \cdot 0^{-1} = 1+1=2 \neq 1$

All: R véges integritási tartomány $\Rightarrow$ test.

Pé: (1) $\mathbb{Z}$ nem test

(2) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ test

(3) $\mathbb{Z}_m$ test $\Leftrightarrow m=p$ prím, ugyanis ekkor $\mathbb{Z}_p$ m.o.m. $\Rightarrow$ int. tart. $\Rightarrow$ test.
 Jel: $\mathbb{F}_p$ prím test.

m és k jegyű

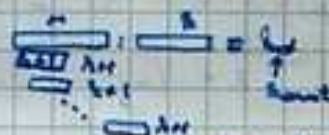
+ konst. $\max(m, k) \leq \text{konst.} \cdot (m+k)$



• konst. $(m+k)^2$

1. —————

a^b jegyzet szám



számítások
jegyzetét $\leq \text{konst.} \cdot k$
legfeljebb m -szer kell
ezt kiszámítani: $m \cdot \text{konst.} \cdot k \leq (mk)^2 \cdot \text{konst.}$



$m \cdot k + k \cdot \text{konst.} \leq \text{konst.} \cdot (m+k)^2$
 $\leq \text{konst.} \cdot (m+k)^2$
 $\leq \text{konst.} \cdot (m+k)^2$

$a > 2^m$
 $b > 2^k$

$a^b > (2^m)^{2^k} = 2^{m \cdot 2^k} \Rightarrow a^b$ legalább $m \cdot 2^k$ jegyű $\Rightarrow$ legalább $m \cdot 2^k$ lépés kell

Induktív mod m

Input: a, b (m és k jegyű), $m > 1$

Output: $a^b \pmod m$

$m = m_0 m_1 \dots m_{l-1}$

$b = b_0 b_1 \dots b_{k-1} \quad b_0 = b_{k-1} \cdot 2^0 + b_{k-2} \cdot 2^1 + \dots + 2 b_1 + b_0$

$a^b \pmod m = a^{b_0 + 2 b_1 + 2^2 b_2 + \dots + 2^{k-1} b_{k-1}} \pmod m = (a^{2^{k-1}})^{b_{k-1}} \cdot (a^{2^{k-2}})^{b_{k-2}} \cdot \dots \cdot (a^2)^{b_2} \cdot a^{b_0} \pmod m$

Kiszámítja $a, a^2, (a^2)^2 = a^{2^2}, ((a^2)^2)^2 = a^{2^3}, \dots$ $\forall$ tetszőleges i vagy $a^{2^i} \pmod m$

Ha már tudjuk $a^{2^i} \pmod m$ -t, akkor $a^{2^{i+1}} = a^{2^i} \cdot a^{2^i}$ miatt egyetlen szorzást kell végrehajtani, és az eredmény mod m maradéka kiszámítani. Két legfeljebb $k+1$ jegyű $\Rightarrow$ konst. k^2 művelet vétele: konst. $(3k)^2$

Eddig $k \cdot \text{konst.} \cdot k^2$ művelet. Kell még k db szorzás mod m $\Rightarrow$ konst. k^3

$\text{konst.} (k \cdot k^2 + k^2) \leq \text{konst.} (k^3 + k^2)$

Primerizálás: Input: n jegyű szám

Output: prímszám

Náiv: Egyszerűsítési kísérlet: $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, \dots$

legalább 2^m lépés kell hozzá.

$\sqrt{x}$ -ig ellenőrzés, $x = p \cdot x'$

$$p \leq \sqrt{x} \quad x' \leq \sqrt{x}$$

$\sqrt{x}$ értéke elég, de $\sqrt{x} \geq 2^{1/2}$ sok.

Véletlen algoritmus: 2-féle válasz $\rightarrow$ nem prím
 $\rightarrow$ valószínűleg prím.

Euler-Fermat tétel: p prím $(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

Ha tudjuk, hogy $(a, n) = 1$, de $a^{n-1} \not\equiv 1 \pmod{n} \Rightarrow n$ nem prím
 $\uparrow$
Euklidész alga. (gcd-meghatározás)

Fermat tesz: Input: n

Output: $\rightarrow$ nem prím
 $\rightarrow$ valószínűleg prím.

Véletlenül egy véletlen a számot 2 és n között.

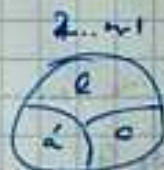
$$a^{n-1} \equiv 1 \pmod{n} \rightarrow \text{meg. prím.}$$

$$a^{n-1} \not\equiv 1 \pmod{n} \rightarrow \text{nem prím: soron kívül.}$$

Def: a az n áruktja, ha $a^{n-1} \not\equiv 1 \pmod{n}$ és $(a, n) = 1$

a az n áruktja, ha $(a, n) = 1$ és $a^{n-1} \equiv 1 \pmod{n}$

a az n leleplezője, ha $(a, n) \neq 1$



Megf: n prím $\Rightarrow$ csak áruktja van.

Ha n nem prím $\Rightarrow \exists$ leleplezője

Ha n összetett és $\exists$ áruktja $\Rightarrow$ legalább egy áruktja van, mint áruktja

Biz: Tfh $c_1, c_2, \dots, c_k$ áruktja és a áruktja $\Rightarrow a \in c_1, a \in c_2, \dots, a \in c_k$ két áruktja.

Kell: $(a, c_i) = 1$ igaz, mert $(a, n) = 1$ és $(c_i, n) = 1$

Tfh. $a, c_i \equiv a, c_j \pmod{n}$. a -val összehasonlítva a kongruenciát $c_i \equiv c_j \pmod{\frac{n}{(n, a)}} \Rightarrow c_i \equiv c_j \pmod{\frac{n}{(n, a)}}$

A prímteszt nem tökéletes, de elég jó. Van olyan módszer is, ami ezt
biztosítja.

Isomorfizmus

Def: $f: X \rightarrow X$ fr eggyirányú, ha (1) f bijekció

(2) f^{-1} $\exists$ hatékony algoritmus.

(3) f ismerete nem elegendő ahhoz, hogy f^{-1} -re hatékony algoritmust találjunk.

R : telefonszámok

f : kiegészítő egyirányú fr, ha f egyirányú, de f^{-1} -re $\exists$ hatékony algoritmus

ilyet még soha senki nem bizonyított.

Nyilvánvaló tulajdonság: $A \rightarrow B$ üzenet. B titkosít egy f és f^{-1} függvényekkel, hogy B ismerje f^{-1} -t. A üzenet M . A elküldi $f(M)$ -t B-nek. B ki tudja számítani: $f^{-1}(f(M)) = M$ -t (tud dekódolni). Lehetséges lenne $f(M)$ -t, de nem tudja f^{-1} -t számítani, így M ismeret nélkül nem tudja megfejteni M -t.

Digitális aláírás $A \xrightarrow{f_s} B \xrightarrow{f_v} A$ adata M -t B-nek küldeni.

Alapból A $f_s(M)$ -t küldi (nem titkosít).

Titkosít: A először aláírja M -t: $f_v^{-1}(M)$. Ezt titkosítja, és B-nek elküldi $f_s(f_v^{-1}(M))$ -t. Ezt B vissza tudja fejtetni: $f_v(f_s^{-1}(f_s(f_v^{-1}(M)))) = f_v(f_v^{-1}(M)) = M$.

B biztos lehet arról, hogy ezt A küldte.

Sőt: a f_v -t feladatára nélkül is a hitelesség ellenőrizhető.

R: RSA algoritmus:

(p) (q) nagy prímek. $n = p \cdot q$

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

Választunk egy e számot, amire $(e, \phi(n)) = 1$.

$$e \cdot d \equiv 1 \pmod{\phi(n)} \quad d\text{-re megoldható, } d \text{ a megoldás}$$

Nyilván: n, e .

Tfl: az M üzenet a $\mathbb{Z}_n$ körében van leírva. $M \in \mathbb{Z}_n^*$ (ha hirtelen alacsony darabokra vágjuk. Az M körülfut egy $\mathbb{Z}_n$ alapján $\mathbb{Z}_n$ -ben lehet t-jeggyű számunk).

Ha M egy 1 és $|\mathbb{Z}_n|^t$ közötti számunk körülfut.

$$\left. \begin{aligned} f(M) &= M^e \pmod{n} \\ f^{-1}(X) &= X^d \pmod{n} \end{aligned} \right\} \text{All: } f^{-1}(f(M)) = M$$

$$\text{Biz: } (M^e)^d \pmod{n} = M^{e \cdot d} \pmod{n} = M^{1 + k \cdot \phi(n)} \pmod{n} = M \cdot (M^{\phi(n)})^k \pmod{n} = M \cdot 1^k = M$$

- ez nyilvánvalóan teljesül egyenlőség miatt.

$M^{\phi(n)} \equiv 1 \pmod{n}$ E-7 miatt
ha $(M, n) = 1$, de
"amikor jó".