# MATEKING.HU

## Képletgyűjtemény

**SZÁMÍTÁSTUDOMÁNY ALAPJAI tantárgy**

Kiadás dátuma: 2026. 04. 16.

# Tartalomjegyzék

# Kombinatorika

Egy adott $n$ elemű halmaz elemeinek egy ismétlés nélküli permutációján az $n$ különböző elem egy sorba rendezését értjük.

$n$ darab különböző elem permutációinak száma:

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot n = n!$$

Megnézem a kapcsolódó epizódot

---

$n$ faktoriálisán az $n$-nél kisebb vagy egyenlő pozitív egész számok szorzatát értjük.

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots 3 \cdot 2 \cdot 1$$

pl.:

$$4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$$

$$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$$

$$1! = 1$$

Továbbá definíció szerint $0! = 1$.

Megnézem a kapcsolódó epizódot

---

Ha $n$ db. egymástól különböző elem közül kiválasztunk $k$ ($k \leq n$) db.-ot úgy, hogy a kiválasztott elemek sorrendje is számít, akkor az $n$ elem $k$-ad osztályú ismétlés nélküli variációját kapjuk.

$n$ darab különböző elemből kiválasztott $k$ darab elem variációinak száma:

$$n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-k+1) = \frac{n!}{(n-k)!}$$

Megnézem a kapcsolódó epizódot

---

Ha $n$ különböző elem közül kiválasztunk $k$ ($k \leq n$) db.-ot úgy, hogy a kiválasztott elemek sorrendjére nem vagyunk tekintettel, akkor $n$ elem $k$-ad osztályú ismétlés nélküli kombinációját kapjuk.

$n$ darab különböző elem közül kiválasztott $k$ darab elem kombinációinak száma:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Megnézem a kapcsolódó epizódot

---

Ha $n$ elem között van $k_1, k_2, \dots, k_r$ egymással megegyező, akkor az elemek egy sorba rendezését ismétléses permutációnak nevezzük.

$n$ elem közötti $k_1, k_2, \dots, k_r$ egymással megegyező ismétléses permutációinak száma:

$$\frac{n!}{k_1! \cdot k_2 \cdot \dots \cdot k_r!}$$

Megnézem a kapcsolódó epizódot

---

Ha $n$ db. egymástól különböző elem közül kiválasztunk $k$ db.-ot úgy, hogy a kiválasztott elemek sorrendje is számít és ugyanazt az elemet többször is választhatjuk, akkor az $n$ elem $k$-ad osztályú ismétléses variációját kapjuk.

Az $n$ elem $k$-ad osztályú ismétléses variációk száma: $n^k$.

Megnézem a kapcsolódó epizódot

---

Ha kör alakban helyezünk el $n$ különböző elemet és azok sorrendjét vizsgáljuk, akkor ciklikus permutációról beszélünk.

$n$ darab különböző elem ciklikus permutációinak száma $\frac{n!}{n} = (n-1)!$

Megnézem a kapcsolódó epizódot

---

# Gráfelméleti alapok

A gráf csúcsokból és azokat összekötő élekből áll.

Megnézem a kapcsolódó epizódot

---

Egy gráf összefüggő, ha bármelyik csúcsából el lehet jutni bármelyik másik csúcsába élek mentén.

Megnézem a kapcsolódó epizódot

---

A gráf egy csúcsának fokszáma a gráf e csúcsában összefutó élek száma.

Megnézem a kapcsolódó epizódot

---

Egy gráfban körnek nevezünk egy olyan utat, amely csupa különböző csúcsokon és éleken haladva visszavezet a kiinduló csúcsába.

Megnézem a kapcsolódó epizódot

---

Ha egy gráfban nincs kör, de maga a gráf összefüggő, akkor fának nevezzük.

Egy $n$ csúcsú fának mindig $n-1$ darab éle van.

Megnézem a kapcsolódó epizódot

---

Azokat a gráfokat, ahol minden csúcs mindegyikkel össze van kötve, teljes gráfnak hívjuk.

Az $n$ csúcsú teljes gráf éleinek a száma:

$$\frac{n(n-1)}{2}$$

Megnézem a kapcsolódó epizódot

---

Egy gráf egyszerű, ha nincs benne sem többszörös él, sem hurokél.

Megnézem a kapcsolódó epizódot

---

Egy gráf Euler-köre olyan zárt élsorozat, amely a gráf összes élét pontosan egyszer tartalmazza.

Megnézem a kapcsolódó epizódot

---

# Gráfok bejárása és gráfalgoritmusok

Egy gráf feszítőfája a gráf minden csúcsát tartalmazó fa részgráf. Feszítőfából általában több is van.

Megnézem a kapcsolódó epizódot

---

A minimális feszítőfa egy gráfban a legkisebb élsúlyú feszítőfa.

Megnézem a kapcsolódó epizódot

---

A Kruskal algoritmus segítségével minimális feszítőfát lehet megtalálni.

Az első lépés, hogy keressük meg a gráfban a legkisebb súlyú élt. Ha több azonos súlyú él van, akkor válasszuk ki azt, amelyikhez kedvünk van.

Ezek után belépünk egy ciklusba, ahol minden lépésben az eddig még ki nem választott élekre alkalmazzuk az előző lépést úgy, hogy ne keletkezzen kör. Ha mégis kör keletkezne, akkor a legutolsó olyan élt, amelynek hozzávétele során a kört kapjuk, töröljük.

Ezt addig csináljuk, amíg kész nem vagyunk.

Megnézem a kapcsolódó epizódot

---

Gráfok egy adott pontjából való feltérképezésére alkalmas módszer a szélességi keresés (BFS = Breadth-first search).

Működése:

Elindulunk egy adott pontból, és megkeressük az összes szomszédos pontot. Ezek az 1 egység távolságra lévő szomszédok és mindegyikre ragasztunk egy 1-es címkét.

Most ezeknek keressük meg az 1 egység távoli szomszédjait. De csak azokat, akiken még nincsen címke.

Ők a kiinduló ponttól 2 egység távolságra vannak és 2-es címkét kapnak.

Ha valamelyik 2-es szomszédba több él is vezet, akkor csak az egyiket hagyjuk meg. Mindegy melyiket.

Az algoritmus aztán így folytatódik, és szép lassan végez.

Megnézem a kapcsolódó epizódot

---

A DFS (Depth-first search) algoritmus a gráf mélységi bejárása.

A DFS algoritmus lényege, hogy elindulunk egy úton, és megyünk, amíg csak tudunk.

Amikor elakadunk, mert már nem tudunk úgy továbbmenni, hogy olyan pontba jussunk, ahol még nem jártunk, akkor visszamegyünk egészen addig, ahonnan még lehet földerítetlen pontok felé haladni.

Amikor újra elakadunk, megint visszamegyünk, és ezt ismételjük, amíg az egész gráfot be nem jártuk.

Megnézem a kapcsolódó epizódot

---

A BFS és DFS algoritmusok végrehajtása során a gráfnak egy-egy feszítőfáját kapjuk. Ezeket nevezzük BFS és DFS fának.

Megnézem a kapcsolódó epizódot

---

Egy gráf csúcsainak bejárására van egy nagyon speciális módszer, amit Hamilton körnek nevezünk, és az a lényege, hogy egy olyan körön haladunk végig a gráfban, amely a gráf összes pontját tartalmazza.

Hamilton kör létezésének szükséges feltétele:

Ha egy gráfból $k$ darab csúcsot kitörlünk (a belőle kiinduló élekkel együtt), akkor a megmaradó gráfnak legfeljebb $k$ darab komponense lehet.

Megnézem a kapcsolódó epizódot

---

A Hamilton út egy olyan út, amely a gráf minden csúcsát tartalmazza.

Hamilton út létezésének szükséges feltétele:

Ha egy gráfból $k$ darab csúcsot kitörlünk (a belőle kiinduló élekkel együtt), akkor a megmaradó gráfnak legfeljebb $k+1$ darab komponense lehet.

Megnézem a kapcsolódó epizódot

---

A Dirac-tétel azt mondja ki, hogy ha egy $G$ egyszerű, $n \geq 3$ csúcsú gráfban minden csúcs foka legalább $\frac{n}{2}$, akkor a gráfban van Hamilton kör.

Megnézem a kapcsolódó epizódot

---

Az Ore-tétel azt mondja, hogy ha egy $G$ egyszerű, $n \geq 3$ csúcsú gráfban bármely $V_1$ és $V_j$ nem szomszédos csúcsra $d(V_i) + d(V_j) \geq n$ teljesül, akkor a gráfban van Hamilton kör.

Megnézem a kapcsolódó epizódot

---

# Gráfok izomorfiája és síkbarajzolhatósága

A $G$ gráf csúcsainak halmazát $V(G)$-vel jelöljük. Itt a $V$ az angol vertex = csúcs szóra utal.

A $G$ gráf éleinek halmazát $E(G)$-vel jelöljük. Itt $E$ az angol edge = él.

A $G$ gráf egy $(V(G), E(G))$ rendezett pár, ahol $V(G)$ egy nem üres halmaz, $E(G)$ pedig a $V(G)$-ből képezhető párok egy halmaza.

Megnézem a kapcsolódó epizódot

---

Ha a gráf egy csúcsából elindulunk, és teszünk egy sétát a gráfon, akkor egy élsorozatot kapunk.

Azokat az élsorozatokat, amelyek a gráf semelyik pontján nem haladnak át többször, útnak nevezzük.

Megnézem a kapcsolódó epizódot

---

Ha egy élsorozat ugyanabból a csúcsból indul, mint ahova érkezik, akkor körsétának nevezzük.

Megnézem a kapcsolódó epizódot

---

Minden gráfban a csúcsok fokszámainak összege az élek számának a kétszerese:

$$\sum d(V_n) = 2e$$

Megnézem a kapcsolódó epizódot

---

Ha egy gráfban nincs kör, de maga a gráf összefüggő, akkor fának nevezzük.

Egy $n$ csúcsú fának mindig $n-1$ darab éle van.

Megnézem a kapcsolódó epizódot

---

A nem összefüggő körmentes gráfok neve erdő.

Megnézem a kapcsolódó epizódot

---

Egy gráf komplementere azt a gráfot jelenti, aminek csúcsai ugyanazok, mint az eredeti gráfnak, és két csúcs pontosan akkor szomszédos benne, ha az eredeti gráfban nem.

Megnézem a kapcsolódó epizódot

---

A $G(V(G), E(G))$ gráf izomorf a $G'(V(G'), E(G'))$ gráffal, ha van egy bijekció a $V(G)$ és $V'(G)$ között, amire teljesül, hogy $G$-ben pontosan akkor szomszédos két pont, ha $G'$-ben a nekik megfelelő pontok szomszédosak, és szomszédos pontpárok esetén ugyanannyi él fut közöttük.

Megnézem a kapcsolódó epizódot

---

Egy gráfban topologikusan ekvivalens átalakításnak nevezzük azt, ha egy élt egy másodfokú csúcs beiktatásával két élre bontunk, vagy ha egy 2 fokú csúcsra illeszkedő éleket egybeolvasztunk, és a csúcsot elhagyjuk.

Két gráf akkor topologikusan izomorf, ha topologikusan ekvivalens lépések egymás utáni alkalmazásával el tudjuk érni, hogy a két gráf izomorf legyen.

Megnézem a kapcsolódó epizódot

---

A titkos recept gráfok izomorfiájának vizsgálatához:

1) Fokszámok vizsgálata

2) Utak hossza

3) Van-e kör?

4) Milyen hosszúak a körök?

5) Élek vizsgálata

Megnézem a kapcsolódó epizódot

---

Egy gráf síkbarajzolható, ha lerajzolható úgy, hogy élei csak a csúcspontokban találkozzanak.

Megnézem a kapcsolódó epizódot

---

A Kuratowski-tétel szerint egy gráf pontosan akkor nem síkbarajzolható, ha tartalmaz $K_{3,3}$ -mal vagy $K_5$-tel topológiailag izomorf részgráfot.

Megnézem a kapcsolódó epizódot

---

Azt mondja az Euler-féle poliéder-tétel, hogy ha egy konvex poliéder csúcsainak száma $V$, lapjainak száma $F$ és éleinek száma $E$, akkor

$$V + F = E + 2$$

Megnézem a kapcsolódó epizódot

---

Ha egy egyszerű gráfban minden kör legalább $k$ hosszú, akkor a síkbarajzolhatóság szükséges feltétele:

$$(k-2) \cdot E \leq k \cdot V - 2k$$

Megnézem a kapcsolódó epizódot

---

Ha egy egyszerű gráf síkbarajzolható, akkor meg kell felelnie ennek a feltételnek:

$$E \leq 3V - 6$$

Megnézem a kapcsolódó epizódot

---

# Irányított gráfok, gráfalgoritmusok irányított gráfokban

A DFS algoritmusnak az a lényege, hogy kiindulunk egy csúcsból, és megyünk ameddig tudunk.

Az, hogy merre megyünk, teljesen a véletlen műve.

Egyszer aztán elérkezünk egy olyan pontba, ahonnan már nincs tovább.

Innen már csak olyan csúcsba tudnánk továbblépni, ahol korábban már jártunk.

Ekkor visszaugrunk egészen addig, ahonnan még vezet út bejáratlan csúcsba.

Ha már minden csúcshoz eljutottunk, akkor a DFS algoritmus véget ér.

Megnézem a kapcsolódó epizódot

---

A DFS algoritmus eredményeként kapjuk a DFS-fát.

Hogyha a DFS-fába berajzoljuk az eredeti gráf többi élét is, akkor ezek az élek három típusba sorolhatóak. Vannak olyan élek, amelyek képesek lerövidíteni egy utat a DFS fában. Ezeket az éleket úgy hívjuk, hogy "előre-él". Ha az eredeti gráfban van fordított irányú él, akkor ezt az élt "vissza-él"-nek nevezzük. Hogyha az eredeti gráfban van $u$-ból $v$-be vezető él, akkor ezt az élt "kereszt-él"-nek nevezzük.

Megnézem a kapcsolódó epizódot

---

A BFS-algoritmus lényege, hogy kiindulunk egy csúcsból, aztán megkeressük a közvetlen szomszédjait. Innen folytatódik az algoritmus, és az új csúcsoknak keressük meg a szomszédjait. Ha több él is vezet egy szomszéd felé, mindegy melyiket választjuk. Az algoritmust addig ismételjük, amíg minden csúcsot meg nem találtunk.

Megnézem a kapcsolódó epizódot

---

A BFS algoritmus eredményeként kapjuk a BFS-fát.

Hogyha a BFS-fába berajzoljuk az eredeti gráf többi élét is, akkor ezek az élek három típusba sorolhatóak.

Vannak "előre-él"ek, "vissza-él"ek és "kereszt-él"ek.

Megnézem a kapcsolódó epizódot

---

A Dijkstra algoritmus képes megtalálni a gráf egy adott csúcsából a többi csúcsba vezető legrövidebb utat.

Az algoritmus lényege, hogy kiválasztunk egy pontot, és ebből a pontból kiindulva csúcsról csúcsra haladva felderítjük az egész gráfot.

Megnézem a kapcsolódó epizódot

---

# Menger tételei, többszörös összefüggőség

Egy $G$ gráf $k$-szorosan élösszefüggő, ha bárhogyan hagyunk el belőle $k$-nál kevesebb élt, a maradék gráf összefüggő marad.

Megnézem a kapcsolódó epizódot

---

Egy $G$ gráf $k$-szorosan pontösszefüggő, ha legalább $k+1$ pontja van és bárhogyan hagyunk el belőle $k$-nál kevesebb pontot, a maradék gráf összefüggő marad.

Megnézem a kapcsolódó epizódot

---

Egy $G$ irányított gráfban az $u$-ból $v$-be vezető élidegen utak maximális száma megegyezik az $u$-ból $v$-be vezető utakat lefogó élek minimális számával.

Egy $G$ gráfban az $u$-ból $v$-be vezető élidegen utak maximális száma megegyezik az $u$-ból $v$-be vezető utakat lefogó élek minimális számával.

Egy $G$ irányított gráfban $u$ és $v$ legyen két különböző nem szomszédos csúcs. Ekkor az $u$-ból $v$-be vezető pontidegen utak maximális száma megegyezik az $u$-ból $v$-be vezető utakat lefogó ($u$-tól és $v$-től különböző) pontok minimális számával.

Egy $G$ gráfban $u$ és $v$ legyen két különböző nem szomszédos csúcs. Ekkor az $u$-ból $v$-be vezető pontidegen utak maximális száma megegyezik az $u$-ból $v$-be vezető utakat lefogó ($u$-tól és $v$-től különböző) pontok minimális számával.

Megnézem a kapcsolódó epizódot

---

# CPM és PERT algoritmus

Mindig létezik egy olyan út, ami csak azokon a pontokon halad át, ahol a tartalékidő nulla, és az út hossza megegyezik a teljes folyamat hosszával. Ezt az utat kritikus útnak nevezzük.

Megnézem a kapcsolódó epizódot

# Páros gráfok, párosítások

Legyen $G(A,B,E)$ páros gráf és $X$ pedig $A$-nak egy tetszőleges részhalmaza. Az $X$-ben lévő csúcsok $B$-beli szomszédjainak halmazát hívjuk $N(X)$-nek. A $G$ gráfnak akkor és csak akkor van $A$-t fedő párosítása, ha bármely $X$ halmazra

$|X|\leq|N(X)|$

Megnézem a kapcsolódó epizódot

---

A $G(A,B,E)$ páros gráfban akkor és csak akkor létezik teljes párosítás, ha

$|A|=|B|$ és

$|X|\leq|N(X)|$ minden $X\subseteq A$ ponthalmazra.

Megnézem a kapcsolódó epizódot

---

# Kromatikus szám, klikk, perfekt gráfok

A legkevesebb színt, amivel egy gráf csúcsait kiszinezhetjük úgy, hogy a szomszédos csúcsok ne legyenek egyforma színűek, a gráf kromatikus számának nevezzük.

Jele: $\chi(G)$.

Megnézem a kapcsolódó epizódot

---

Egy $G$ egyszerű gráfban klikknek nevezzük azokat a részgráfokat, amelyek teljes gráfok.

Megnézem a kapcsolódó epizódot

---

Egy gráf klikkszáma a gráfban található maximális klikk elemszáma.

A $G$ gráf klikkszámát $\omega(G)$-vel jelöljük.

Minden gráfban a klikkszám alsó becslés a kromatikus számra:

$$\omega(G) \leq \chi(G)$$

Megnézem a kapcsolódó epizódot

---

A $G$ gráfban a $G'$ részgráf feszített részgráf, ha bármely két csúcs a $G'$ gráfban pontosan akkor szomszédos, ha $G$-ben is szomszédos.

Megnézem a kapcsolódó epizódot

---

Ha egy $G$ gráf minden $G'$ feszített részgráfjára igaz, hogy

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

akkor a $G$ gráfot perfekt gráfnak nevezzük.

Ha egy gráf perfekt, akkor a kromatikus száma egyenlő a klikkszámával. Az állítás fordítva nem igaz, abból, hogy $\omega(G') = \chi(G')$ még nem következik, hogy a gráf perfekt.

Megnézem a kapcsolódó epizódot

---

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

ahol $\omega(G)$ a gráf klikkszáma, $\chi(G)$ a kromatikus száma és $\Delta(G)$ a maximális fokszáma.

Megnézem a kapcsolódó epizódot

---

A mohó színezés egy algoritmus a gráfok színezésére.

Lényege, hogy sorba rakjuk a gráf csúcsait, és elkezdjük színezni úgy, hogy minden csúcs színezéséhez a lehető legkisebb sorszámú színt használjuk. Ezt addig folytatjuk, amíg az összes csúcs ki nem lesz színezve, és így elhasználunk legfeljebb $\Delta(G)+1$ darab színt.

Megnézem a kapcsolódó epizódot

---

Ha $G$ nem teljes gráf, vagy páratlan csúcsú kör, akkor

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

Megnézem a kapcsolódó epizódot

---

Egy $G$ gráfban azt a legkisebb számot, amire a gráfnak már van jó élszínezése, a $G$ gráf élkromatikus számának nevezzük.

Jele: $\chi_e$

Megnézem a kapcsolódó epizódot

---

A Vizing-tétel a gráfok élkromatikus számára ad alsó és felső becslést:

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

Vagyis a $G$ egyszerű gráfok két osztályba sorolhatók:

Első osztály: $\chi_e(G) = \Delta(G)$

Második osztály: $\chi_e(G) = \Delta(G)+1$

Megnézem a kapcsolódó epizódot

---

Az intervallumgráf egy olyan gráf, melynek csúcsai megfeleltethetőek a valós számok egy-egy intervallumának, és két csúcs között akkor vezet él, ha a nekik megfeleltethető két intervallum metszete nem üres.

Az intervallumgráfok mindig perfekt gráfok.

Megnézem a kapcsolódó epizódot

---

Egy $G$ gráfot páros gráfnak nevezünk, ha csúcsainak a $V(G)$ halmaza felbontható az $A$ és $B$ diszjunkt részhalmazokra, úgy hogy $A$-n és $B$-n belül nem vezetnek élek.

A páros gráfok kromatikus száma 2, élkromatikus számukra pedig König Dénesnek van egy remek tétele:

Ha $G$ páros gráf, akkor $\chi_e(G) = \Delta(G)$

Megnézem a kapcsolódó epizódot

---

Jan Mycielski lengyel matematikust nyugtalanította az a kérdés, hogy léteznek-e olyan gráfok, amelyeknek a kromatikus száma nagyon nagy, de a klikkszáma csak 2.

Létrehozott egy konstrukciót, amivel olyan gráfokat lehet alkotni, amelyek klikkszáma 2, a kromatikus számuk pedig bármilyen nagy lehet. Ezeket a gráfokat Mycielski-gráfoknak nevezzük.

Megnézem a kapcsolódó epizódot

# Gráfparaméterek, párosítások

A független ponthalmaz precíz definíciójára mindjárt kettő is van.

Íme az egyik:

Egy $G$ gráfban független csúcshalmaznak nevezzük a csúcsoknak az $A \subset V(G)$ részhalmazát, ha nincs olyan él, amelynek mindkét végpontja $A$-ban van.

És itt jön a másik:

Egy $G$ gráfban független csúcshalmaznak nevezzük a csúcsoknak az $A \subset V(G)$ részhalmazát, ha az $A$ által feszített részgráf nem tartalmaz élt.

Egy $G$ gráfban a független csúcsok maximális számát $\alpha(G)$-vel jelöljük.

Megnézem a kapcsolódó epizódot

---

Egy $G$ gráfban a $T \subset V(G)$ ponthalmaz lefogó ponthalmaz, ha $G$ minden élének legalább az egyik végpontja $T$-ben van.

Egy gráfban a minimális méretű lefogó ponthalmaz elemszámát $\tau(G)$-vel jelöljük.

A maximális lefogó ponthalmaz pedig a gráf összes csúcsa, és elemszáma éppen $|V(G)| = n$.

Megnézem a kapcsolódó epizódot

---

Ha vesszük egy gráfban a maximális számú független pontokat és a minimális számú lefogó pontokat, akkor épp megkapjuk a gráf összes pontját.

Ezt hívjuk első Gallai tételnek:

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

Megnézem a kapcsolódó epizódot

---

Egy $G$ gráf éleinek $M$ részhalmaza független élhalmaz, ha $M$ semelyik két elemének nincs közös végpontja.

Egy gráf független éleinek maximális számát $\nu(G)$-vel jelöljük.

Megnézem a kapcsolódó epizódot

---

Egy $G$ gráf éleinek $R$ részhalmaza lefogó élhalmaz, ha a gráf minden csúcsa valamelyik $R$-beli él végpontja.

Egy $G$ gráfban a lefogó élek minimális számát $\rho(G)$-vel jelöljük.

Megnézem a kapcsolódó epizódot

---

Ha vesszük egy gráfban a minimális számú lefogó éleket, és a maximális számú független éleket, akkor a gráf minden pontjához pontosan egy él fog tartozni.

Ez Gallai második tétele:

Ha egy $n$ csúcsú gráf nem tartalmaz izolált pontot, akkor

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

Megnézem a kapcsolódó epizódot

---

$$\alpha(G) \leq \rho(G) \quad \nu(G) \leq \tau(G)$$

Megnézem a kapcsolódó epizódot

---

Egy $G$ gráf akkor és csak akkor páros, ha minden $G$-ben szereplő kör páros hosszúságú.

Megnézem a kapcsolódó epizódot

---

Egy $G$ gráfban az $E(G)$ élhalmaznak egy $M$ részhalmazát párosításnak nevezzük, ha $M$ semelyik két elemének nincs közös végpontja.

Megnézem a kapcsolódó epizódot

---

Egy $G$ gráfban az $e_1, e_2, e_3, \ldots, e_n$ élsorozat az $M$ párosítás javító útja, ha

1) a megadott élsorozat egy páratlan hosszú út $G$-ben

2) az élek felváltva elemi $M$-nek:

$e_{2k} \in M$ és $e_{2k+1} \notin M$

3) az út kezdő és végpontja nem illeszkedik semelyik $M$-beli élre sem

Megnézem a kapcsolódó epizódot

---

Azokat a párosításokat nevezzük teljes párosításoknak, ami a gráf összes csúcsát lefedi.

Megnézem a kapcsolódó epizódot

---

Egy gráfban akkor és csakis akkor létezik teljes párosítás, ha bárhogyan hagyunk el a gráfból néhány pontot, a megmaradt gráfban a páratlan komponensek száma nem több az elhagyott pontok számánál.

Megnézem a kapcsolódó epizódot

---

# Maximális folyam, Ford-Fulkerson-algoritmus

Legyen $X$ a $V(G)$-nek egy olyan részhalmaza, ami $S$-t tartalmazza. Ekkor az $X$-ből a $V(G)-X$-be vezető éleket $(S,T)$ vágásnak nevezzük.

Megnézem a kapcsolódó epizódot

---

Egy $(S,T)$ vágás kapacitása, a vágásban szereplő élek kapacitásainak összege.

Megnézem a kapcsolódó epizódot

---

A Ford-Fulkerson algoritmus egy olyan algoritmus, amit a maximális folyam megkeresésére használunk. Az algoritmus lényege pedig az a javító gráf, amit az eredeti hálózat alapján készítünk el. A javító gráf megmutatja nekünk, hogy milyen útvonalon tudjuk növelni a meglévő folyamot.

Megnézem a kapcsolódó epizódot

---

Legyen $G$ egy irányított gráf és értelmezzünk a gráf élein egy $E \to R_0^+$ függvényt, ami minden élhez hozzárendeli a $c(e)$ nem negatív számot, amit az él kapacitásának nevezünk.

Megnézem a kapcsolódó epizódot

---

Legyen $G$ egy irányított gráf és értelmezzünk a gráf élein egy $E \to R_0^+$ függvényt, ami minden élhez hozzárendeli a $c(e)$ nem negatív számot, amit az él kapacitásának nevezünk.

Van továbbá két kitüntetett pont a gráfban, $S$ (source = forrás) és $T$ (target = cél).

Ekkor a $(G,S,T,c)$ egy hálózat.

Megnézem a kapcsolódó epizódot

---

A hálózatban folyamnak nevezünk egy olyan $f(e)$ $E \to R_0^+$ függvényt, amire teljesül, hogy bármely $e$ élre $0 \leq f(e) \leq c(e)$ és bármely $T$-től és $S$-től különböző $V$ csúcsra:

$$\sum_{Vbe} f(e) - \sum_{Vki} f(e) = 0$$

Megnézem a kapcsolódó epizódot

---

Egy folyam értékének az

$$m_f = \sum_{Ski} f(e) - \sum_{Sbe} f(e)$$

számot nevezzük.

Megnézem a kapcsolódó epizódot

---

A Ford-Fulkerson tétel azt mondja ki, hogy egy hálózatban a maximális folyam mindig megegyezik a minimális vágással.

Megnézem a kapcsolódó epizódot

# Mátrixok és vektorok

Egy nXk-as mátrix tulajdonképpen nem más, mint egy táblázat, aminek n darab sora és k darab oszlopa van.

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

Megnézem a kapcsolódó epizódot

---

Ha egy mátrixot egy számmal szorzunk, akkor amátrix összes elemét meg kell szorozni a számmal.

pl.: $3 \cdot \begin{pmatrix} 5 & 7 & -2 \\ 2 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 15 & 21 & -6 \\ 6 & 6 & 3 \end{pmatrix}$

Megnézem a kapcsolódó epizódot

---

Ha egy mátrixot osztunk egy számmal, akkor amátrix minden elemét osztani kell a számmal.

pl.: $\frac{\begin{pmatrix} 6 & 9 & -12 \\ 3 & 3 & 15 \end{pmatrix}}{3} = \begin{pmatrix} 2 & 3 & -4 \\ 1 & 1 & 5 \end{pmatrix}$

Megnézem a kapcsolódó epizódot

---

Két mátrix összeadásakor összeadjuk az ugyanazon pozícióban lévő elemeket. Két mátrixot csak akkor lehet összeadni, ha ugyanannyi soruk és oszlopuk van.

pl.: $\begin{pmatrix} 2 & 4 & 7 \\ 1 & 5 & 3 \end{pmatrix} + \begin{pmatrix} 1 & 7 & -2 \\ 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 11 & 5 \\ 5 & 7 & 4 \end{pmatrix}$

A mátrixok összeadása kommutatív, azaz

$$A + B = B + A$$

És asszociatív, azaz

$$(A + B) + C = A + (B + C)$$

Megnézem a kapcsolódó epizódot

---

Két mátrix kivonásakor kivonjuk az ugyanazon pozícióban lévő elemeket. Két mátrixot csak akkor lehet kivonni egymásból, ha ugyanannyi soruk és oszlopuk van.

pl.: $\begin{pmatrix} 2 & 4 & 7 \\ 1 & 5 & 3 \end{pmatrix} - \begin{pmatrix} 1 & 7 & -2 \\ 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -3 & 9 \\ -3 & 3 & 2 \end{pmatrix}$

Megnézem a kapcsolódó epizódot

---

Két mátrix szorzata akkor létezik, ha a bal oldalimátrix oszlopainak száma megegyezik a jobb oldalimátrix sorainak számával.

Ha az A mátrix m x n-es a B mátrix pedig n x k-s, akkor az eredménymátrix m x k-s lesz.

Az eredménymátrix i-edik sorának j-edik elemét úgy kapjuk, hogy a bal oldalimátrix i-edik sorát skalárisan szorozzuk a jobb oldali mátrix j-edik oszlopával. (Tehát az első elemet az elsővel, a másodikat a másodikkal stb. szorozzuk, majd összeadjuk)

pl.: $\begin{pmatrix} 3 & 4 \\ 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 2 & 4 & 7 \\ 1 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 10 & 32 & 33 \\ 7 & 29 & 22 \end{pmatrix}$

Megnézem a kapcsolódó epizódot

---

Két mátrixot csak akkor adhatunk össze, ha ugyanannyi soruk és oszlopuk van.

A mátrix összeadás kommutatív:

$$A+B=B+A$$

És asszociatív:

$$(A+B)+C=A+(B+C)$$

Megnézem a kapcsolódó epizódot

---

A mátrixszorzás nem kommutatív, azaz:

$$A \cdot B \neq B \cdot A$$

De asszociatív, azaz:

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)$$

Megnézem a kapcsolódó epizódot

---

A kvadratikus mátrix négyzetes mátrix vagyis ugyanannyi sora van, mint oszlopa.

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

Megnézem a kapcsolódó epizódot

---

A diagonális mátrix olyan kvadratikus mátrix, aminek a főátlóján kívüli elemek nullák.

pl.: $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Megnézem a kapcsolódó epizódot

---

Az egységmátrix olyan mátrix, ami azt tudja, hogy bármely $A$ mátrixra $A \cdot I = A$.

Az egységmátrixok olyan diagonális mátrixok, aminek minden főátló-eleme egy.

pl.: $I_{2x2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Megnézem a kapcsolódó epizódot

---

Az inverz mátrix jele $A^{-1}$ és ez egy olyan mátrix, ami azt tudja, hogy

$A \cdot A^{-1} = I$ (jobb inverz)

$A^{-1} \cdot A = I$ (bal inverz)

Megnézem a kapcsolódó epizódot

---

A transzponált a mátrix sorainak és oszlopainak felcserélése. Jele $A^T$ vagy $A^*$

pl.:

$$A = \begin{pmatrix} 2 & 3 & 5 \\ 1 & 4 & 1 \\ 2 & 5 & 7 \end{pmatrix} \Rightarrow A^T = \begin{pmatrix} 2 & 1 & 2 \\ 3 & 4 & 5 \\ 5 & 1 & 7 \end{pmatrix}$$

Megnézem a kapcsolódó epizódot

---

Azokat a mátrixokat, melyek transzponáltjuk önmaga, szimmetrikus mátrixnak nevezzük.

pl.: $A = \begin{pmatrix} 5 & 1 & 7 \\ 1 & 4 & 2 \\ 7 & 2 & 6 \end{pmatrix} \Rightarrow A^T = \begin{pmatrix} 5 & 1 & 7 \\ 1 & 4 & 2 \\ 7 & 2 & 6 \end{pmatrix}$

Megnézem a kapcsolódó epizódot

---

Vektort egy számmal úgy szorzunk, hogy a vektor minden koordinátáját megszorozzuk a számmal.

Pl.: $3 \cdot \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 3 \\ 9 \\ 15 \end{pmatrix}$

Megnézem a kapcsolódó epizódot

---

Vektort egy számmal úgy osztunk, hogy a vektor minden koordinátáját leosztjuk a számmal.

Pl.: $\frac{\begin{pmatrix}3\\6\\15\end{pmatrix}}{3}=\begin{pmatrix}1\\3\\5\end{pmatrix}$

Megnézem a kapcsolódó epizódot

---

Két vektort úgy adunk össze, hogy minden egyes koordinátájukat külön-külön össze adjuk.

Pl.: $\begin{pmatrix}2\\4\\-1\end{pmatrix}+\begin{pmatrix}4\\2\\7\end{pmatrix}=\begin{pmatrix}6\\6\\6\end{pmatrix}$

Tulajdonságok:

kommutatív: $\underline{a}+\underline{b}=\underline{b}+\underline{a}$

asszociatív: $(\underline{a}+\underline{b})+\underline{c}=\underline{a}+(\underline{b}+\underline{c})$

Megnézem a kapcsolódó epizódot

---

Két vektort úgy vonunk ki egymásból, hogy minden egyes koordinátájukat külön-külön kivonjuk egymásból.

Pl.: $\begin{pmatrix}2\\4\\-1\end{pmatrix}-\begin{pmatrix}4\\2\\7\end{pmatrix}=\begin{pmatrix}-2\\2\\-8\end{pmatrix}$

Megnézem a kapcsolódó epizódot

---

A skaláris szorzat két vektor közti művelet, ami csinál belőlük egy számot.

Pl.: $\underline{a}=\begin{pmatrix}3\\2\\5\end{pmatrix}\quad\underline{b}=\begin{pmatrix}4\\1\\2\end{pmatrix}$

$\underline{a}^T\cdot\underline{b}=3\cdot4+2\cdot1+5\cdot2=24$

Tulajdonságok:

kommutatív: $\underline{a}^T\cdot\underline{b}=\underline{b}^T\cdot\underline{a}$

nem asszociatív: $\left(\underline{a}^T\cdot\underline{b}\right)^T\cdot\underline{c}\neq\underline{a}^T\cdot\left(\underline{b}^T\cdot\underline{c}\right)$

Megnézem a kapcsolódó epizódot

---

Két vektor diadikus szorzata egy mátrix. Lássuk milyen.

Pl.: $\underline{a} = \begin{pmatrix} 3 \\ 2 \\ 5 \end{pmatrix} \quad \underline{b} = \begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix}$

$$\underline{a} \cdot \underline{b}^T = \begin{pmatrix} 12 & 3 & 6 \\ 8 & 2 & 4 \\ 20 & 5 & 10 \end{pmatrix}$$

Tulajdonságok:

nem kommutatív

nem asszociatív

Megnézem a kapcsolódó epizódot

---

Ha egy mátrixot beszorzunk az $\underline{I} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$ vektorral, akkor az szépen összeadja a mátrixunk soraiban lévő elemeket.

Megnézem a kapcsolódó epizódot

---

Ha egy mátrixot beszorzunk az $\underline{I}^T = (1 \quad 1 \quad \dots \quad 1)$ vektorral, akkor az szépen összeadja a mátrixunk oszlopaiban lévő elemeket.

Megnézem a kapcsolódó epizódot

---

Ha egy mátrixot megszorzunk jobbról egy $\underline{e}_i$ egységvektorral, akkor megkapjuk a mátrix i-edik oszlopát.

Megnézem a kapcsolódó epizódot

---

Ha egy mátrixot megszorzunk balról egy $\underline{e}_i$ egységvektorral, akkor megkapjuk a mátrix i-edik sorát.

Megnézem a kapcsolódó epizódot

---

# Vektorterek, független és összefüggő vektorok

A $V$ nem üres halmazt vektortérnek nevezzük a valós számok felett, ha a$V$ halmazon értelmezve van egy összeadás nevű művelet, úgy, hogy minden $V$-beli $\underline{v}_1$ és $\underline{v}_2$ vektorhoz hozzárendelünk egy $\underline{v}_1 + \underline{v}_2$ vektort, ami szintén eleme $V$-nek.

1. Az összeadás kommutatív: bármely $\underline{v}_1, \underline{v}_2$ $V$-beli vektorra

$$\underline{v}_1 + \underline{v}_2 = \underline{v}_2 + \underline{v}_1$$

2. Az összeadás asszociatív: bármely $\underline{v}_1, \underline{v}_2, \underline{v}_3$ $V$-beli vektorra

$$(\underline{v}_1 + \underline{v}_2) + \underline{v}_3 = \underline{v}_1 + (\underline{v}_2 + \underline{v}_3)$$

3. Létezik nullelem: van olyan $\underline{0}$ $V$-beli vektor, hogy bármely $\underline{v}_1$ $V$-beli vektorra

$$\underline{v}_1 + \underline{0} = \underline{0} + \underline{v}_1 = \underline{v}_1$$

4. Létezik ellentett: bármely $\underline{v}_1$ $V$ beli vektorra létezik olyan $-\underline{v}_1$ $V$-beli vektor, hogy

$$\underline{v}_1 + (-\underline{v}_1) = -\underline{v}_1 + \underline{v}_1 = \underline{0}$$

Értelmezve van egy skalárral való szorzás nevű művelet is úgy, hogy minden$V$-beli $\underline{v}_1$ vektorhoz és bármely valós számhoz hozzárendelünk egy $\lambda \cdot \underline{v}_1$ vektort, ami szintén $V$-beli.

5. A skalárszoros asszociatív: bármely $\underline{v}_1$ $V$-beli vektorra és $\lambda, \mu$ skalárra

$$(\lambda \cdot \mu) \cdot \underline{v}_1 = \lambda \cdot (\mu \cdot \underline{v}_1)$$

6. A skalárszoros disztributív a vektorokra: bármely $\underline{v}_1, \underline{v}_2$ $V$-beli vektorra és $\lambda$ skalárra

$$\lambda \cdot (\underline{v}_1 + \underline{v}_2) = \lambda \cdot \underline{v}_1 + \lambda \cdot \underline{v}_2$$

7. A skalárszoros disztributív a skalárokra: bármely $\underline{v}_1$ $V$-beli vektorra és $\lambda, \mu$ skalárra

$$(\lambda + \mu) \cdot \underline{v}_1 = \lambda \cdot \underline{v}_1 + \mu \cdot \underline{v}_1$$

8. Egységszeres: bármely $\underline{v}_1$ $V$-beli vektorra és az 1 valós számra

$$1 \cdot \underline{v}_1 = \underline{v}_1$$

Megnézem a kapcsolódó epizódot

---

A $\underline{v}_1, \underline{v}_2, \underline{v}_3, \ldots, \underline{v}_n$ vektorok lineárisan függetlenek, ha

$$\lambda_1 \cdot \underline{v}_1 + \lambda_2 \cdot \underline{v}_2 + \lambda_3 \cdot \underline{v}_3 + \cdots + \lambda_n \cdot \underline{v}_n = \underline{0}$$

csak úgy teljesül, ha minden $\lambda_i = 0$

Megnézem a kapcsolódó epizódot

---

A $\underline{v_1}, \underline{v_2}, \underline{v_3}, \ldots, \underline{v_n}$ vektorok lineárisan összefüggők, ha

$$\lambda_1 \cdot \underline{v_1} + \lambda_2 \cdot \underline{v_2} + \lambda_3 \cdot \underline{v_3} + \cdots + \lambda_n \cdot \underline{v_n} = \underline{0}$$

úgy is teljesül, hogy van olyan $\lambda_i \neq 0$

Megnézem a kapcsolódó epizódot

---

Egy $V$ vektortérben a $\underline{v_1}, \underline{v_2}, \underline{v_3}, \ldots, \underline{v_n}$ vektorok generátor-rendszert alkotnak, ha minden $\underline{w}$ vektor a $V$ vektortérben előáll $\underline{w} = \lambda_1 \cdot \underline{v_1} + \lambda_2 \cdot \underline{v_2} + \lambda_3 \cdot \underline{v_3} + \cdots + \lambda_n \cdot \underline{v_n}$ alakban.

Megnézem a kapcsolódó epizódot

---

A $\underline{v_1}, \underline{v_2}, \underline{v_3}, \ldots, \underline{v_n}$ vektorok független rendszert alkotnak, ha

$$\lambda_1 \cdot \underline{v_1} + \lambda_2 \cdot \underline{v_2} + \lambda_3 \cdot \underline{v_3} + \cdots + \lambda_n \cdot \underline{v_n} = \underline{0}$$

csak úgy teljesül, ha minden $\lambda_i = 0$

Megnézem a kapcsolódó epizódot

---

A bázis független generátorrendszer.

A bázis minden vektort egyértelműen előállít, míg $R^*$-ben azok a generátor-rendszerek pedig, amelyek $n$-nél több vektorból állnak, minden vektort végtelensokféleképpen.

Megnézem a kapcsolódó epizódot

---

Egy vektorrendszer rangja a benne lévő függetlenvektorok maximális száma. $R^3$-ban a rang például maximum három lehet.

Megnézem a kapcsolódó epizódot

---

A $V$ vektortérnek $W$ altere, ha $W \subset V$ és $W$ maga is vektortér a $V$-beli műveletekre.

Megnézem a kapcsolódó epizódot

---

A legfeljebb n-ed fokú polinomok vektorteret alkotnak az összeadás és a skalárral való szorzás műveletekre.

Megnézem a kapcsolódó epizódot

---

A $v_1$, $v_2$,...$v_k$ vektorok által generált altér ezen vektorok lineáris kombinációja.

Megnézem a kapcsolódó epizódot

---

Egy vektor akkor állítható egy vektorrendszerrel, ha előáll azon vektorok lineáris kombinációjaként.

Megnézem a kapcsolódó epizódot

---

# Lineáris egyenletrendszerek, mátrixok rangja és inverze

Egy egyenletrendszer együtthatómátrixa az x-ek együtthatóiból álló mátrix.

Megnézem a kapcsolódó epizódot

---

A Gauss-elimináció egy lineáris egyenletrendszerek megoldására használt algoritmus.

Az elimináció lényege, hogy egyenletrendszerünket visszavezetjük vagy valamely háromszög- vagy átlósmátrix alakra.

A Gauss-elimináció megengedett lépései:

- Két sort (egyenletet) felcserélhetünk
- Egy sort (egyenletet) nem nulla számmal szorozhatunk
- Egyik sorhoz (egyenlethez) hozzáadhatjuk egy másik sor (egyenlet) nem nulla számsorosát

Megnézem a kapcsolódó epizódot

---

Az elemi bázistranszformáció (Szuper-Gauss) a lineáris egyenletrendszerek megoldásának egy algoritmikus módja.

1. lépés: a generáló elem választása

Csak x-es oszlopból és e-s sorból választhatunk generáló elemet, nullát nem választhatunk és lehetőleg 1-et vagy mínusz 1-et érdemes.

2. lépés: a bázistranszformáció

A generáló elem sorát osztjuk a generáló elemmel, oszlopát elhagyjuk.

A többi elemből kivonjuk a generáló elem neki megfelelő sorában és oszlopában lévő számok szorzatát, osztva a generálóelemmel.

3. lépés: megint generáló elem választás

Újra és újra végrehatjuk a bázistranszformációt, amíg az összes oszlop el nem tűnik

4. lépés: az utolsó transzformáció és a megoldás

Megnézem a kapcsolódó epizódot

---

Az elemi bázistranszformáció (Szuper-Gauss) a lineáris egyenletrendszerek megoldásának egy algoritmikus módja.

1. lépés: a generáló elem választása

Csak x-es oszlopból és e-s sorból választhatunk generáló elemet, nullát nem választhatunk és lehetőleg 1-et vagy mínusz 1-et érdemes.

2. lépés: a bázistranszformáció

A generáló elem sorát osztjuk a generáló elemmel, oszlopát elhagyjuk.

A többi elemből kivonjuk a generáló elem neki megfelelő sorában és oszlopában lévő számok szorzatát, osztva a generálóelemmel.

3. lépés: megint generáló elem választás

Újra és újra végrehatjuk a bázistranszformációt, amíg az összes oszlop el nem tűnik

4. lépés: az utolsó transzformáció és a megoldás

Megnézem a kapcsolódó epizódot

---

Ha egy egyenletrendszernek több az ismeretlene, mint ahány egyenlete van, akkor az egyenletrendszernek nincs egyértelmű megoldása.

Bázistranszformációval, ha maradnak $\underline{e}$-s sorok ahol már nem tudunk generáló elemet választani, olyankor mindig végtelen sok megoldás van, vagy nincs megoldás.

Megnézem a kapcsolódó epizódot

---

Ha egy egyenletrendszerben két olyan egyenlet szerepel, ahol az ismeretlenek együtthatói megegyeznek, de más az eredményük, akkor az ellentmondó egyenletrendszer, aminek nincs megoldása.

Megnézem a kapcsolódó epizódot

---

A bázistranszformáció során fent maradt x-ek úgynevezett szabadváltozók. A szabadságfok a szabadváltozók száma, tehát ahány $x_i$ fönt marad.

Megnézem a kapcsolódó epizódot

---

A Gauss-Jordan elimináció a Gauss-elimináció pro változata. A dolog lényege az, hogy nemcsak a vezéregyesek alatt nullázzuk ki, hanem felettük is. Előnye, hogy így a megoldások az elimináció végeztével egyből leolvashatók.

Megnézem a kapcsolódó epizódot

---

Egy mátrix oszloprangja az oszlopvektorai közül kiválasztható független vektorok maximális száma.

Megnézem a kapcsolódó epizódot

---

Egy mátrix sorrangja a sorvektorai közül kiválasztható független vektorok maximális száma.

Megnézem a kapcsolódó epizódot

---

A mátrix rangja a mátrix Gauss elimináció során keletkezett vezéregyeseinek száma, amely megegyezik amátrix sorrangjával vagy oszlopvektorával

Megnézem a kapcsolódó epizódot

---

Egy mátrixot teljes oszloprangúnak nevezünk, hogyha az oszlopvektorai lineárisan független rendszert alkotnak.

Megnézem a kapcsolódó epizódot

---

Egy mátrixot teljes sorrangúnak nevezünk, hogyha a sorvektorai lineárisan független rendszert alkotnak.

Megnézem a kapcsolódó epizódot

---

Bármely mátrixot fel lehet bontani két olyan mátrix szorzatára, amelyek közül az egyik teljes oszloprangú, a másik pedig teljes sorrangú. Ezt bázisfelbontásnak hívják, és egy kiss Gauss-Jordan eliminációval tudjuk elkészíteni.

Megnézem a kapcsolódó epizódot

---

Négyzetes mátrixok inverzét a Gauss-elimináció segítségével úgy állíthatjuk elő, hogy megoldjuk az $Ax = b$ egyenletrendszert úgy, hogy a $b$ helyére beírjuk az egységmátrixot. Az eliminációs lépéseket addig kell végezni, amíg az egységmátrixot nem kapjuk az $A$ helyén, a $b$ helyén keletkezett mátrix pedig az $A$ mátrix inverze lesz.

Megnézem a kapcsolódó epizódot

---

Négyzetes mátrixok inverzét a bázistranszformáció segítségével úgy állíthatjuk elő, hogy megoldjuk az $Ax = b$ egyenletrendszert úgy, hogy a $b$ helyére beírjuk az egységmátrixot.

Megnézem a kapcsolódó epizódot

---

Négyzetes mátrixok inverzét a Gauss-Jordan elimináció segítségével úgy állíthatjuk elő, hogy megoldjuk az $Ax = b$ egyenletrendszert úgy, hogy a $b$ helyére beírjuk az egységmátrixot.

Megnézem a kapcsolódó epizódot

---

Az inverz kiszámolása rettentő egyszerű dolog. Mindössze annyit kell tennünk, hogy felírjuk a mátrixot a szokásos táblázatba, és mellé írjuk az egységmátrixot. Ezek után jön a bázistranszformáció. Ha nem tudjuk mindegyik x-et levinni, akkor nincs inverz. Ha mindet le tudjuk vinni, akkor van.

Megnézem a kapcsolódó epizódot

---

# Determináns, sajátérték, sajátvektor

Ha az $A$ egy $n$ $x$ $n$-es mátrix, akkor determinánsa

$det(A) = \sum_{\forall p}(-1)^{I(p)} \cdot \prod_{i=1}^{n} a_{ip(i)}$

ahol $p$ az oszlopindexek permutációi, $I(p)$ pedig ezen permutációk inverziószáma.

Megnézem a kapcsolódó epizódot

---

Egy 2x2-es mátrix determinánsa:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \det(A) = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \cdot d - b \cdot c$$

Megnézem a kapcsolódó epizódot

---

A 3x3-as mátrixok determinánsának kiszámolására van egy szabály, ami szarrusz szabály néven ismert. A szabály lényege, hogy fogjuk a mátrixot és leírjuk saját maga mögé még egyszer, majd vesszük a főátlókat és a mellékátlókat, így

$$\det(A) = -a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}$$

Megnézem a kapcsolódó epizódot

---

Ha az $A$ egy nxn-es mátrix, akkor determinánsa

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \cdot \det(A_{ij})$$

Itt $\det(A_{ij})$ az $a_{ij}$ elemhez tartozó aldeterminánsa.

Megnézem a kapcsolódó epizódot

---

Az $A$ mátrix determinánsa nulla, ha

- van csupa nulla sora
- van két azonos sora
- egyik sora a másik sor számszorosa
- egyik sora más sorok lineáris kombinációja
- mindez sor helyett oszlopra is elmondható

Determinánsok szorzási tétele:

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

$$\det(A^k) = \det(A)^k$$

Megnézem a kapcsolódó epizódot

---

Azokat a mátrixokat nevezzük szinguláris nak, amelyek determinánsa nulla.

Az $A$ mátrix szinguláris:

- $\det(A) = 0$
- Nem létezik $A^{-1}$ inverz mátrix
- RANG<n
- Az $A$ mátrix oszlopvektoraiból álló vektorrendszer lineárisan összefüggő
- Az $A \cdot \underline{x} = \underline{b}$ egyenletrendszernek vagy végtelen sok megoldása van vagy nincs megoldása
- Az $A \cdot \underline{x} = \underline{0}$ homogén lineáris egyenletrendszernek végtelen sok megoldása van

Megnézem a kapcsolódó epizódot

---

Azokat a mátrixokat nevezzük regulárisnak, amelyek determinánsa nem nulla.

Az $A$ mátrix reguláris:

- $\det(A) \neq 0$
- Létezik $A^{-1}$ inverz mátrix
- RANG=n
- Az $A$ mátrix oszlopvektoraiból álló vektorrendszer lineárisan független
- Az $A \cdot \underline{x} = \underline{b}$ egyenletrendszernek csak egy megoldása van
- Az $A \cdot \underline{x} = \underline{0}$ homogén lineáris egyenletrendszernek csak egy megoldása van (a triviális megoldás)

Megnézem a kapcsolódó epizódot

---

A Cramer szabály szerint az $A \cdot \underline{x} = \underline{b}$ egyenletrendszer megoldásai a következőképp állnak elő:

$$x_k = \frac{\det(A_k)}{\det(A)}$$

ahol $\det(A_k)$ annak a mátrixnak a determinánsát jelenti, hogy az $A$ mátrix k-adik oszlopát kicseréljük a $\underline{b}$ vektorral.

Megnézem a kapcsolódó epizódot

---

Ha egy nxn-es mátrixnak van n darab független sajátvektora, akkor létezik a mátrixnak egy úgynevezett diagonális alakja.

A diagonális alak így néz ki:

$$\mathrm{diag}(A) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

a főatlóban vannak a sajátértékek és az összes többi elem nulla.

A diagonális alakot a következő módon állítjuk elő:

$$\mathrm{diag}(A) = X^{-1} \cdot A \cdot X$$

itt $X = (\underline{v}_1 \quad \underline{v}_2 \quad \dots \underline{v}_n)$

Megnézem a kapcsolódó epizódot

Ha egy nxn-es mátrixnak van n darab független sajátvektora, akkor létezik a mátrixnak egy úgynevezett diagonális alakja.

A diagonális alak így néz ki:

$$\mathrm{diag}(A) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

a főatlóban vannak a sajátértékek és az összes többi elem nulla.

A diagonális alakot a következő módon állítjuk elő:

$$\mathrm{diag}(A) = X^{-1} \cdot A \cdot X$$

itt $X = (\underline{v}_1 \quad \underline{v}_2 \quad \dots \underline{v}_n)$

Megnézem a kapcsolódó epizódot

Ha egy nxn-es mátrixnak van n darab független sajátvektora, akkor létezik a mátrixnak egy úgynevezett diagonális alakja.

A diagonális alak így néz ki:

$$\mathrm{diag}(A) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

a főatlóban vannak a sajátértékek és az összes többi elem nulla.

A diagonális alakot a következő módon állítjuk elő:

$$\mathrm{diag}(A) = X^{-1} \cdot A \cdot X$$

itt $X = (\underline{v}_1 \quad \underline{v}_2 \quad \dots \underline{v}_n)$

Megnézem a kapcsolódó epizódot

---

Ha az $A$ mátrix egy $n$ x $n$-es diagonalizálható mátrix, akkor a sajátfelbontása:

$$A = X \cdot diag(A) \cdot X^{-1}$$

Itt $X = (\underline{v}_1 \quad \underline{v}_2 \quad \dots \quad \underline{v}_n)$ vagyis egyszerűen úgy keletkezi, hogy a sajátvektorokat fogjuk, és leírjuk egymás mellé és

$$diag(A) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

Megnézem a kapcsolódó epizódot

---

A spektrálfelbontás segítségével könnyebben hatványozhatunk:

$$A^n = X \cdot (diag(A))^n \cdot X^{-1}$$

Megnézem a kapcsolódó epizódot

---

Egy mátrix sarok főminor mátrixai a mátrix bal felső sarkától kezdődő sarok mátrixok determinánsai.

Pl.: $A = \begin{pmatrix} 2 & 3 & 5 & 1 \\ 4 & 7 & 2 & 1 \\ 2 & 1 & 14 & \\ 3 & 5 & 1 & 7 \end{pmatrix}$

első sarokfőminora a 2-es

második sarokfőminora a bal felső 2x2-es determináns

$$\det \begin{pmatrix} 2 & 3 \\ 4 & 7 \end{pmatrix} = 2 \cdot 7 - 3 \cdot 4 = 2$$

és így tovább

Megnézem a kapcsolódó epizódot

---

Egy mátrix főminor mátrixai a mátrix bal felső sarkától kezdődő sarok mátrixok determinánsai.

Pl.: $A = \begin{pmatrix} 2 & 3 & 5 & 1 \\ 4 & 7 & 2 & 1 \\ 2 & 1 & 14 & \\ 3 & 5 & 1 & 7 \end{pmatrix}$

első főminora a 2-es

második főminora a bal felső 2x2-es determináns

$$\det \begin{pmatrix} 2 & 3 \\ 4 & 7 \end{pmatrix} = 2 \cdot 7 - 3 \cdot 4 = 2$$

és így tovább

Megnézem a kapcsolódó epizódot

---

Az $A$ nxn-es mátrix pozitív definit, ha minden $\lambda$ sajátérték: $\lambda > 0$.

Vagy ha minden sarokfőminor pozitív.

Megnézem a kapcsolódó epizódot

---

Az $A$ nxn-es mátrix negatív definit, ha minden $\lambda$ sajátérték: $\lambda < 0$.

Vagy ha a sarokfőminorok váltakozva $- + - +$ de mínusszal indul.

Megnézem a kapcsolódó epizódot

---

Az $A$ nxn-es mátrix pozitív szemidefinit, ha minden $\lambda$ sajátérték: $\lambda \geq 0$.

2x2-es mátrixoknál, ha az első sarokfőminor pozitív, a második nulla.

Megnézem a kapcsolódó epizódot

---

Az $A$ nxn-es mátrix negatív szemidefinit, ha minden $\lambda$ sajátérték: $\lambda \leq 0$.

2x2-es mátrixoknál, ha az első sarokfőminor negatív, a második nulla.

Megnézem a kapcsolódó epizódot

---

Az $A$ nxn-es mátrix indefinit, ha van $\lambda_1$ és $\lambda_2$ sajátérték, hogy $\lambda_1 > 0$ és $\lambda_2 < 0$.

Ha $\det(A) \neq 0$ és nem pozitív vagy negatív definit, akkor indefinit.

Megnézem a kapcsolódó epizódot

---

Ha $A$ nxn-es szimmetrikus mátrix és $\underline{x}$ egy vektor $R^n$-ben, akkor a

$$Q(x) = \underline{x}^* \cdot A \cdot \underline{x}$$

kifejezést kvadratikus alaknak nevezzük.

Azért hívjuk kvadratikusnak vagyis négyzetesnek, mert ez mindig egy homogén másodfokú kifejezés.

Megnézem a kapcsolódó epizódot

---

A $Q(\underline{x}) = \underline{x}^* \cdot A \cdot \underline{x}$ kvadratikus alak

pozitív definit, ha minden $\underline{x} \neq \underline{0}$ vektorra $Q(\underline{x}) > 0$

negatív definit, ha minden $\underline{x} \neq \underline{0}$ vektorra $Q(\underline{x}) < 0$

pozitív szemidefinit, ha minden $\underline{x} \neq \underline{0}$ vektorra $Q(\underline{x}) \geq 0$

negatív szemidefinit, ha minden $\underline{x} \neq \underline{0}$ vektorra $Q(\underline{x}) \leq 0$

indefinit, ha van olyan $\underline{x} \neq \underline{0}$ és $\underline{y} \neq \underline{0}$, hogy $Q(\underline{x}) < 0$ és $Q(\underline{y}) > 0$

Megnézem a kapcsolódó epizódot

---

# Lineáris leképezések

A $\varphi$ leképezést lineáris leképezésnek nevezzük, ha bármely $\underline{v}_1, \underline{v}_2 \in V_1$ vektorokra és $\lambda \in R$ számra teljesül, hogy

$$\varphi(\underline{v}_1 + \underline{v}_2) = \varphi(\underline{v}_1) + \varphi(\underline{v}_2)$$

$$\varphi(\lambda \cdot \underline{v}) = \lambda \cdot \varphi(\underline{v})$$

Megnézem a kapcsolódó epizódot

---

A $V_1 \to V_2$ lineáris leképezésnél $V_2$-nek azt a részét, amely a leképezés során előáll, a leképezés képterének nevezzük és $Im\varphi$-vel jelöljük.

Megnézem a kapcsolódó epizódot

---

A nullvektorból minden lineáris leképezés nullvektort csinál, vagyis $\underline{0}$ képe mindig $\underline{0}$, de előfordulhat, hogy más $V_1$-beli vektorok képe is nullvektor lesz. Ezen vektorok halmazát nevezzük a leképezés magterének és $Ker\varphi$-vel jelöljük.

Megnézem a kapcsolódó epizódot

---

A képtér és a magtér dimenziója összesen éppen kiadja $V_1$ dimenzióját.

Ezt az összefüggést dimenziótételnek nevezzük:

$$\dim(Ker\varphi) + \dim(Im\varphi) = \dim(V_1)$$

Megnézem a kapcsolódó epizódot

---

Minden lineáris leképezést jellemezhetünk egy mátrixszal. Valójában mindegyiket végtelen sok mátrixszal jellemezhetjük, ezek a mátrixok pedig úgy keletkeznek, hogy veszünk egy tetszőleges bázist $V_1$-ben és a bázisvektorok képeit egymás mellé írjuk.

Megnézem a kapcsolódó epizódot

---

A $\varphi$ leképezésben minden vektor képét így kapjuk:

$$\varphi(\underline{v}) = (\varphi)_b \cdot \underline{v}$$

Megnézem a kapcsolódó epizódot

---

Egy leképezésnek pontosan akkor létezik inverze, ha a $(\varphi)_b$ mátrixnak létezik inverze, és az inverz leképezés mátrixa:

$\varphi^{-1}$ mátrixa $(\varphi)_b^{-1}$

Megnézem a kapcsolódó epizódot

---

A $\varphi \circ \mu$ leképezés mátrixa:

$$(\varphi \circ \mu)_b = (\varphi)_b \cdot (\mu)_b$$

Megnézem a kapcsolódó epizódot

---

Ha egy nxn-es mátrixnak van n darab független sajátvektora, akkor létezik a mátrixnak egy úgynevezett diagonális alakja.

A diagonális alak így néz ki:

$$\mathrm{diag}(A) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

a főatlóban vannak a sajátértékek és az összes többi elem nulla.

A diagonális alakot a következő módon állítjuk elő:

$$\mathrm{diag}(A) = X^{-1} \cdot A \cdot X$$

itt $X = (\underline{v}_1 \quad \underline{v}_2 \quad \dots \underline{v}_n)$

Megnézem a kapcsolódó epizódot

---

A $\varphi$ lineáris leképezésnek a $\underline{b}_1\ \underline{b}_2\ \dots\ \underline{b}_n$ bázisban felírt mátrixát úgy kapjuk meg, hogy a bázisvektorok képeit egymás mellé írjuk:

$$(\varphi)_b = (\varphi(\underline{b}_1)\ \varphi(\underline{b}_2)\ \varphi(\underline{b}_3)\ \dots\ \varphi(\underline{b}_n))$$

Bármilyen bázist is választunk is $V_1$-ben, a leképezés mátrixa mindig egy nxn-esmátrix lesz. Ha ennek a mátrixnak van n darab független sajátvektora, akkor ezek a sajátvektorok szintén egy bázist alkotnak $V_1$-ben, amit sajátbázisnak nevezünk.

Megnézem a kapcsolódó epizódot

---

A $V_1 \to V_2$ lineáris leképezést másnéven homomorfizmusnak is nevezzük. Ezek a homomorfizmusok és azok mátrixai maguk is egy vektorteret alkotnak, ezt a vektorteret $Hom(V_1, V_2)$-nek nevezzük.

Megnézem a kapcsolódó epizódot

---

Ha $A$ és $B$ olyan mátrixok, hogy létezik egy $C$ mátrix úgy, hogy

$$A = C^{-1} \cdot B \cdot C$$

akkor a két mátrix egymáshoz hasonló.

Megnézem a kapcsolódó epizódot

---

# Oszthatóság

Az $a$ és $b$ szám legnagyobb közös osztója az a $d$ pozitív szám, amire $d \mid a$ és $d \mid b$, és e közös osztók közül ez a legnagyobb.

Jelölés: $d = (a, b)$

Megnézem a kapcsolódó epizódot

---

$a$ és $b$ relatív prímek, ha $(a, b) = 1$

Megnézem a kapcsolódó epizódot

---

Ha $a \mid c$ és $b \mid c$ és $(a, b) = 1$ akkor $ab \mid c$

Ha $c \mid ab$ és $(a, c) = 1$ akkor $c \mid b$

Megnézem a kapcsolódó epizódot

---

A nullától és az egységszorzóktól különböző összes $n$ egész szám felbontható prímek szorzatára a sorrendtől és az egységszeresektől eltekintve egyértelműen.

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ ahol $k \in Z^+$

Itt $k$ a felbontásban szereplő különböző prímek száma.

Megnézem a kapcsolódó epizódot

---

Egy $p$ szám prím, ha

$p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$

Megnézem a kapcsolódó epizódot

---

Egy $q$ szám felbonthatatlan, ha nem létezik olyan egységtől különböző$a$ és $b$ szám, hogy $q = ab$

Megnézem a kapcsolódó epizódot

---

# Euklideszi algoritmus & Diofantoszi egyenletek

Az euklideszi algoritmus egy formányos módszer két szám legnagyobb közös osztójának kiszámolására.

$a$ és $b$ számokra így néz ki az algoritmus:

$$a = q_1 \cdot b + r_1$$

$$b = q_2 \cdot r_1 + r_2$$

$$r_1 = q_3 \cdot r_2 + r_3$$

$$\vdots$$

$$r_{n-2} = q_n \cdot r_{n-1} + r_n$$

$$r_{n-1} = q_{n+1} \cdot r_n + 0$$

A legnagyobb közös osztó az utolsó nem $0$ maradék ($r_n$).

Az euklideszi algoritmussal továbbá a két szám legnagyobb közös osztója kifejezhető a két szám segítségével:

$$D = \alpha \cdot a + \beta \cdot b$$

Itt $D$ a legnagyobb közös osztó.

Megnézem a kapcsolódó epizódot

A Diofantoszi egyenletek így néznek ki:

$$ax + by = c$$

ahol $a, b, c \in Z$ és $x, y \in Z$

Megoldásukat azzal kezdjük, hogy kiszámoljuk $a$ és $b$ legnagyobb közös osztóját: $D$, és ezzel végig osztjuk az egyenletet, így kapjuk az

$$Ax + By = C$$

egyenletet, ahol $(A, B) = 1$.

A második lépés, hogy az euklideszi algoritmus segítségével kifejezzük $A$ és $B$ legnagyobb közös osztóját, ami az 1, így

$$\alpha \cdot A + \beta \cdot B = 1$$

egyenletet kapunk.

Ezt az egyenletet beszorozva $C$-vel megkapunk egy megoldást:

$$(\alpha \cdot C) \cdot A + (\beta \cdot C) \cdot B = C$$

Az általános megoldásokat a következő alakban kapjuk meg:

$$x = \alpha \cdot C + k \cdot B$$
$$y = \beta \cdot C - k \cdot A$$

Megnézem a kapcsolódó epizódot

# Kongruenciák

Ha $a$ és $b$ ugyanazt a maradékot adja $m$-mel osztva, akkor azt mondjuk, hogy $a$ és $b$ kongruensek modulo $m$, és ezt a tényt így jelöljük:

$$a \equiv b \bmod m$$

Megnézem a kapcsolódó epizódot

---

Reflexív:

$$a \equiv a \bmod m$$

Szimmetrikus:

$$a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$$

Tranzitív:

$$a \equiv b \bmod m \text{ és } b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$$

Összefüggés összeadásra:

$$a \equiv b \bmod m \text{ és } c \equiv d \bmod m \Rightarrow a + c \equiv b + d \bmod m$$

Összefüggés szorzásra:

$$a \equiv b \bmod m \text{ és } c \equiv d \bmod m \Rightarrow a \cdot c \equiv b \cdot d \bmod m$$

Megnézem a kapcsolódó epizódot

---

Legyenek $a$ és $b$ egész számok és $m$ pozitív egész szám.

Ekkor

$$a \equiv b \bmod m, \text{ ha } m \mid a - b$$

Megnézem a kapcsolódó epizódot

---

$$a \equiv b \bmod m \Rightarrow a \cdot c \equiv b \cdot c \bmod m$$
$$a \cdot c \equiv b \cdot c \bmod m \Rightarrow a \equiv b \bmod m \quad (m, c) = 1$$

Megnézem a kapcsolódó epizódot

---

Egy adott $m$ modulus esetén az $a$-val kongruens elemek halmazát az $a$ által reprezentált maradékosztálynak nevezzük.

Megnézem a kapcsolódó epizódot

---

Egy mod $m$ modulus esetén az $m$-hez relatív prím elemekből álló maradékosztályokat redukált maradékosztálynak nevezzük.

A redukált maradékosztályok számát a $\varphi(m)$ számelméleti függvény írja le.

Megnézem a kapcsolódó epizódot

---

Az euler féle $\varphi$ függvény azt adja meg, hogy hány $m$-nél nem nagyobb, $m$-hez relatív prím pozitív szám létezik.

Ha $p$ prím, akkor

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

$$\varphi(p^\alpha = p^\alpha - p^{\alpha-1}$$

És ha

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$$

akkor

$$\varphi(m) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \dots \cdot \left(p_n^{\alpha_n} - p_n^{\alpha_n - 1}\right)$$

Továbbá

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

Megnézem a kapcsolódó epizódot

---

$a^{\varphi(m)} \equiv 1 \bmod m$ ha $(a, m) = 1$

Megnézem a kapcsolódó epizódot

---

$a^p \equiv a \bmod p$ ha $p$ prím

Megnézem a kapcsolódó epizódot

---

A lineáris kongruenciák így néznek ki:

$$ax \equiv b \bmod m$$

És érdemes megjegyezni, hogy csak akkor oldhatók meg, ha $(a, m) \mid b$.

Megnézem a kapcsolódó epizódot

---

A lineáris kongruenciák így néznek ki:

$$ax \equiv b \bmod m$$

Megoldás csak akkor létezik, ha $(a,m) \mid b$.

A megoldás menete a következő:

1. lépés: Redukálunk

$$a_1 x \equiv b_1 \bmod m$$

2. lépés: Leosztunk $a_1$-gyel, de $b_1$-et lélekben fel kell erre készíteni

A megoldások száma: $(a,m)$

Megnézem a kapcsolódó epizódot

---

Az RSA lényege, hogy a titkosítás kulcsa nyilvános, vagyis azt bárki ismerheti. Csak a dekódolás kulcsa az, ami titkos.

Az alapötlete a következő:

Veszünk két jó nagy prímet, $p$-t és $q$-t amit csak mi ismerünk, ezek titkosak.

Elkészítjük az $N = p \cdot q$ számot és $\varphi(N)$-et, amit csak mi ismerünk.

Ha $p$ és $q$ többszázjegyű prímek, akkor $N$ prímfelbontása a jelenlegi számítógépekkel több ezer évig tartana, és így $\varphi(N)$ kiszámolása is lehetetlen.

Végül már csak egy dolog kell, egy $e$ kitevő, amire teljesül, hogy $(e, \varphi(N)) = 1$

Ezt követően jön a titkosítás.

A visszafejtéshez pedig az Euler-Fermat tétel kell, aminek segítségével megalkotjuk a $d$ megfejtő kulcsot.

Megnézem a kapcsolódó epizódot

---