MATEKING.HU

Képletgyűjtemény

SZÁMÍTÁSTUDOMÁNY tantárgy

Kiadás dátuma: 2026. 04. 16.

Tartalomjegyzék

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

Kuratowski gráfok, síkbarajzolhatóság

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 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

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

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: χ_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

Hálózati folyamok

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

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

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

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

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 különbözőa 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, RSA kódolás

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 φ 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

Boole-algebra alapjai

Az univerzális kvantor egy jelölése a "minden" kifejezésnek.

Jele: $\forall$

Megnézem a kapcsolódó epizódot

Az egzisztenciális kvantor egy jelölése a "létezik" vagy "van olyan" kifejezésnek.

Jele: $\exists$

Megnézem a kapcsolódó epizódot

Az állítás negációja (vagy tagadása) egy egyváltozós művelet. Egy A kijelentés negációja az a kijelentés, amely akkor igaz, ha A hamis és akkor hamis, ha A igaz.

Megnézem a kapcsolódó epizódot

Az állítás (vagy kijelentés) olyan kijelentő mondat, amelyről egyértelműen eldönthetjük, hogy az igaz vagy hamis.

Megnézem a kapcsolódó epizódot

A konjunkció két állítás közti logikai művelet. Két kijelentés konjunkciója pontosan akkor igaz, ha mindkét kijelentés igaz, különben hamis.

Jele: $A \wedge B$

Megnézem a kapcsolódó epizódot

A diszjunkció két állítás közti logikai művelet. Két kijelentés diszjunkciója pontosan akkor igaz, ha legalább az egyik kijelentés igaz, különben hamis.

Jele: $A \vee B$

Megnézem a kapcsolódó epizódot

A "ha A, akkor B" kapcsolatnak megfelelő logikai műveletet nevezzük implikációnak. Az implikáció akkor hamis, ha A igaz és B hamis, minden más esetben igaz.

Jele: $A \Rightarrow B$

Megnézem a kapcsolódó epizódot

Az ekvivalencia egy olyan logikai művelet, amikor $A \Rightarrow B$ és $A \Leftarrow B$. Az ekvivalencia akkor igaz, ha A és B logikai értéke azonos, különben hamis.

Jele: $A \Leftrightarrow B$

Megnézem a kapcsolódó epizódot

$$\neg(A \wedge B) = \neg A \vee \neg B$$

$$\neg(A \vee B) = \neg A \wedge \neg B$$

$$\neg(A \Rightarrow B) = A \wedge \neg B$$

$$\neg(A \Leftrightarrow B) = A \Leftrightarrow \neg B$$

Megnézem a kapcsolódó epizódot

A diszjunktív normálforma, röviden DNF egy olyan alakja egy logikai formuláknak, ahol a művelet a változóinak vagy negáltjainak konjunkcióinak diszjunkciója.

Megnézem a kapcsolódó epizódot