MATEKING.HU

Képletgyűjtemény

ALKALMAZOTT MATEMATIKA 1 tantárgy

Kiadás dátuma: 2026. 04. 17.

Tartalomjegyzék

Komplex számok..... **2**

Maradékosztályok..... **5**

Független és összefüggő vektorok..... **6**

Egy kis geometria..... **8**

Mátrixok és vektorok..... **12**

Determináns, sajátérték, sajátvektor..... **17**

Lineáris egyenletrendszerek, mátrixok inverze..... **23**

Lineáris leképezések..... **26**

Oszthatóság..... **28**

Euklideszi algoritmus & Diofantoszi egyenletek..... **29**

Kongruenciák..... **31**

Komplex számok

Van itt két komplex szám: $z_1 = a + bi, z_2 = c + di$

A két komplex szám összege:
$z_1 + z_2 = (a + c) + (b + d)i$

A két komplex szám különbsége:
$z_1 - z_2 = (a - c) + (b - d)i$

Megnézem a kapcsolódó epizódot

Van itt két komplex szám: $z_1 = a + bi, z_2 = c + di$

A két komplex szám szorzata:
$z_1 \cdot z_2 = (a + bi) \cdot (c + di) = a \cdot c - b \cdot d + (a \cdot d + b \cdot c)i$

Megnézem a kapcsolódó epizódot

A komplex számok egy valós és egy imaginárius (képzetes) számból épülnek föl. A valós számok a szokásos x tengelyen helyezkednek el, míg az imaginárius számok egy erre merőleges y tengelyen, amit imaginárius tegelynek, vagy képzetes tengelynek nevezünk. Az imaginárius tengely egysége az i, ami olyan, mint a valós tengelyen az 1, csak éppen egy meglehetősen furcsa dolgot tud. Az imaginárius egység egy olyan komplex szám, aminek a négyzete -1 és i-vel jelöljük, azaz

$$i^2 = -1$$

Megnézem a kapcsolódó epizódot

A komplex számokat azért hívjuk "komplex"nek, mert két részből tevődnek össze. Egy valós és egy imaginárius (képzetes) számból épülnek föl. A valós számok a szokásos x tengelyen helyezkednek el, míg az imaginárius számok egy erre merőleges y tengelyen, amit imaginárius tegelynek, vagy képzetes tengelynek nevezünk. A komplex számok egy valós számból és egy imaginárius számból tevődnek össze:

$$z = a + bi$$

Itt a és b valós számok, az i pedig az imaginárius egység, ami azt tudja, hogy $i^2 = -1$.

Magukat a valós számokat és az imaginárius számokat is komplex számnak tekinthetjük. A valós számok olyan komplex számok, amelyeknek az imaginárius része nulla, míg az imaginárius számok olyankomplex számok, amelyeknek a valós része nulla. A komplex számok egy síkon, az úgynevezett komplex számsíkon helyezkednek el. Kicsit olyanok, mint a koordinátageometriában a kétdimenziós sík vektorai, ahol az i és j bázisvektorkat szokás használni, az x tengelynél az i és az y tengelynél a j vektorral. Ennek az analógiának köszönhetően vannak, akik az imaginárius számokat nem is i-vel, hanem j-vel jelölik. Bár ez segíthet erősíteni az analógiát a sík vektoraival, de mégis zavaró, mivel aki komolyabban is fogalakozik a komplex számokkal, a hivatalos jelöléssel fog találkozni, ahol az imaginárius tengelyen i-k vannak.

Megnézem a kapcsolódó epizódot

A valós számokat úgy érdemes elképzelni, mint egy koordinátarendszer x tengelyét. És minden helyet ki is töltenek a valós számok ezen a számegyenesen. A komplex számok egy valós és egy imaginárius (képzetes) részből épülnek föl, és szemléltetésükhöz nem egy, hanem két koordinátatengelyre van szükség. Az x tengelyen vannak a valós számok, az y tengelyen pedig az imaginárius, vagyis a képzetes számok. A valós számok tengelyén az egység a szokásos 1, míg az imaginárius számok tengelyén az egység az i. A kétb tengely által kifeszített síkot nevezzük komplex számsíknak, vagy másknt Gauss-féle számsíknak.

Megnézem a kapcsolódó epizódot

Van itt ez a komplex szám:

$$z = a + bi$$

Komplex számoknak van ilyenje, hogy imaginárius egység:

$$i^2 = -1$$

Komplex számok konjugáltja:

$$\overline{z} = a - bi$$

Megnézem a kapcsolódó epizódot

Van itt ez a komplex szám: $z = a + bi$

Ennek a komplex számnak az abszolútértéke:

$$|z| = \sqrt{a^2 + b^2}$$

Megnézem a kapcsolódó epizódot

A $z = a + bi$ komplex szám trigonometrikus alakja:

$z = r\left(\cos\theta + i\sin\theta\right)$, ahol

$r = \sqrt{a^2 + b^2} \qquad \cos\theta = \frac{a}{r}$

Megnézem a kapcsolódó epizódot

Van itt két komplex szám trigonometrikus alakban: $z_1 = r_1\left(\cos\theta_1 + i\sin\theta_1\right), z_2 = r_2\left(\cos\theta_2 + i\sin\theta_2\right)$

Komplex számok szorzása trigonometrikus alakban:

$$z_1 z_2 = r_1 r_2\left(\cos\left(\theta_1 + \theta_2\right) + i\sin\left(\theta_1 + \theta_2\right)\right)$$

Komplex számok osztása trigonometrikus alakban:

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}\left(\cos\left(\theta_1 - \theta_2\right) + i\sin\left(\theta_1 - \theta_2\right)\right)$$

Megnézem a kapcsolódó epizódot

Van itt ez a komplex szám trigonometrikus alakban:$r\left(\cos\theta+i\sin\theta\right)$

Ekkor ennek a komplex számnak az n-edik hatványa:

$$z^n=r^n\left(\cos n\theta+i\sin n\theta\right)$$

Megnézem a kapcsolódó epizódot

Van itt ez a komplex szám trigonometrikus alakban:$z=r\left(\cos\theta+i\sin\theta\right)$

Ekkor ennek a komplex számnak az n-edik gyöke:

$$\sqrt[n]{z}=\sqrt[n]{r}\left(\cos\frac{\theta+2k\pi}{n}+i\sin\frac{\theta+2k\pi}{n}\right)$$

Megnézem a kapcsolódó epizódot

Van itt két komplex szám exponenciális alakban:$z_1=r_1e^{i\theta_1}$, $z_2=r_2e^{i\theta_2}$

Komplex számok szorzása exponenciális alakban:

$$z_1z_2=r_1r_2e^{i(\theta_1+\theta_2)}$$

Komplex számok osztása exponenciális alakban:

$$\frac{z_1}{z_2}=\frac{r_1}{r_2}e^{i(\theta_1-\theta_2)}$$

Megnézem a kapcsolódó epizódot

Van itt ez a komplex szám exponenciális alakban:$z=re^{i\theta}$

Ekkor ennek a komplex számnak az n-edik hatványa:

$$z^n=r^ne^{ni\theta}$$

Megnézem a kapcsolódó epizódot

Van itt ez a komplex szám exponenciális alakban:$z=re^{i\theta}$

Ekkor ennek a komplex számnak az n-edik gyöke:

$$\sqrt[n]{z}=\sqrt[n]{r}e^{i\frac{\theta+2k\pi}{n}}$$

Megnézem a kapcsolódó epizódot

Maradékosztályok

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

Független és összefüggő vektorok

A V nem üres halmazt vektortérnek nevezzük a valós számok felett, ha aV 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 λ, μ 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 λ 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 λ, μ 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 független vektorok 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

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

Megnézem a kapcsolódó epizódot

Egy kis geometria

A vektor egy irányított szakasz.

Jelölése: $\underline{v} = \overrightarrow{AB}$

Megnézem a kapcsolódó epizódot

Van itt két vektor:$\underline{a} = (a_1, a_2), \underline{b} = (b_1, b_2)$

A két vektor összege:

$$\underline{a} + \underline{b} = (a_1 + b_1, a_2 + b_2)$$

A két vektor különbsége:

$$\underline{a} - \underline{b} = (a_1 - b_1, a_2 - b_2)$$

$$\overrightarrow{AB} = \underline{b} - \underline{a}$$

Megnézem a kapcsolódó epizódot

Van itt az $\underline{a} = (a_1, a_2)$ és $\underline{b} = (b_1, b_2)$ vektor.

Az $\underline{a}$ vektor hossza:

$$|\underline{a}| = \sqrt{a_1^2 + a_2^2}$$

Az $\overrightarrow{AB}$ vektor hossza:

$$\overrightarrow{AB} = |\underline{b} - \underline{a}| = \sqrt{(b_1 - a_1)^2 + (b_2 - a_2)^2}$$

És pont ugyanígy kapjuk meg az A és B pontok távolságát is.

Megnézem a kapcsolódó epizódot

Két pont közti vektor a végpontba mutató helyvektor minusz a kezdőpontba mutató helyvektor.

Tehát $\overrightarrow{AB} = \underline{b} - \underline{a}$

Megnézem a kapcsolódó epizódot

Van itt két vektor: $\underline{a} = (a_1, a_2), \underline{b} = (b_1, b_2)$.

Az $\underline{a}$ és $\underline{b}$ vektorok skaláris szorzata:

$$\underline{a} \cdot \underline{b} = |\underline{a}| \cdot |\underline{b}| \cdot \cos\gamma = a_1 \cdot b_1 + a_2 \cdot b_2$$

ahol γ a két vektor által bezárt szög

$|\underline{a}| = \sqrt{a_1^2 + a_2^2}$, vagyis az $\underline{a}$ vektor hossza

$|\underline{b}| = \sqrt{b_1^2 + b_2^2}$, vagyis a $\underline{b}$ vektor hossza

Két vektor merőleges egymásra, ha $\underline{a} \cdot \underline{b} = 0$.

Megnézem a kapcsolódó epizódot

Van itt az $\underline{a} = (a_1, a_2)$ vektor.

Az $\underline{a}$ +90°-os elforgatottja:

$$a^{+90^\circ} = (-a_2, a_1)$$

Az $\underline{a}$ -90°-os elforgatottja:

$$a^{-90^\circ} = (a_2, -a_1)$$

Megnézem a kapcsolódó epizódot

Két vektor skaláris szorzatát kiszámolhatjuk így:

$$\underline{a} \cdot \underline{b} = |\underline{a}| \cdot |\underline{b}| \cdot \cos\gamma$$

ahol γ a két vektor által bezárt szög,

$|\underline{a}| = \sqrt{a_1^2 + a_2^2}$, vagyis az $\underline{a}$ vektor hossza

$|\underline{b}| = \sqrt{b_1^2 + b_2^2}$, vagyis az $\underline{b}$ vektor hossza

Illetve kiszámolhatjuk így is:

$$\underline{a} \cdot \underline{b} = a_1 \cdot b_1 + a_2 \cdot b_2$$

Megnézem a kapcsolódó epizódot

Két vektor merőleges egymásra, ha skaláris szorzatuk 0, azaz ha $\underline{a} \cdot \underline{b} = 0$.

Megnézem a kapcsolódó epizódot

A $P(x_0, y_0)$ ponton átmenő és $\underline{n} = \begin{bmatrix} A \\ B \end{bmatrix}$ normálvektorú egyenes egyenlete:

$$A(x - x_0) + B(y - y_0) = 0$$

Megnézem a kapcsolódó epizódot

A $P(x_0, y_0, z_0)$ ponton átmenő és $\underline{n} = \begin{bmatrix} A \\ B \\ C \end{bmatrix}$ normálvektorú sík egyenlete:

$$A(x - x_0) + B(y - y_0) + C(z - z_0) = 0$$

Megnézem a kapcsolódó epizódot

Van a síkban két pont: $P(x_1, y_1)$ és $Q(x_2, y_2)$.

Ekkor a két pont közti vektor:

$$\overrightarrow{PQ} = \begin{bmatrix} x_2 - x_1 \\ y_2 - y_1 \end{bmatrix}$$

Ha a térben veszünk két pontot: $P(x_1, y_1, z_1)$ és $Q(x_2, y_2, z_2)$.

Akkor a két pont közti vektor:

$$\overrightarrow{PQ} = \begin{bmatrix} x_2 - x_1 \\ y_2 - y_1 \\ z_2 - z_1 \end{bmatrix}$$

Megnézem a kapcsolódó epizódot

Van itt két pont a síkban: $P(x_1, y_1)$ és $Q(x_2, y_2)$.

Ekkor a két pont közti távolság:

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

Ha a térben veszünk két pontot: $P(x_1, y_1, z_1)$ és $Q(x_2, y_2, z_2)$.

Akkor a két pont közti távolság a térben:

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}$$

Megnézem a kapcsolódó epizódot

A $P(x_0, y_0)$ ponton átmenő és $\underline{n} = \begin{pmatrix} A \\ B \end{pmatrix}$ normálvektorú egyenes egyenlete:

$$A \cdot (x - x_0) + B \cdot (y - y_0) = 0$$

Megnézem a kapcsolódó epizódot

A $P(x_0, y_0, z_0)$ ponton átmenő és $\underline{n} = \begin{pmatrix} A \\ B \\ C \end{pmatrix}$ normálvektorú sík egyenlete:

$$A \cdot (x - x_0) + B \cdot (y - y_0) + C \cdot (z - z_0) = 0$$

Megnézem a kapcsolódó epizódot

Van itt két vektor: $\underline{a} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}$ és $\underline{b} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}$

A két vektor vektoriális szorzata:

$$\underline{a} \times \underline{b} = \det \begin{bmatrix} \underline{e}_1 & \underline{e}_2 & \underline{e}_3 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{bmatrix}$$

Megnézem a kapcsolódó epizódot

Az $\underline{a}$ és $\underline{b}$ vektorok vektoriális szorzata az $\underline{a} \times \underline{b}$ vektor, ami merőleges az $\underline{a}$ és $\underline{b}$ vektorok által kifeszített síkra, és

$$\underline{a} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \quad \underline{b} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} \quad \underline{a} \times \underline{b} = \det \begin{pmatrix} \underline{e}_1 & \underline{e}_2 & \underline{e}_3 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$$

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 $\underline{I}^T = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}$ 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

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

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 sarokmátrixok 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 λ sajátérték: $\lambda > 0$.

Vagy ha minden sarokfőminor pozitív.

Megnézem a kapcsolódó epizódot

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

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

Megnézem a kapcsolódó epizódot

Az A nxn-es mátrix pozitív szemidefinit, ha minden λ 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 λ 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 λ_1 és λ_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 egyenletrendszerek, mátrixok 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

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

Lineáris leképezések

A φ 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 φ 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:

φ^{-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:

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

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

A diagonális alakot a következő módon állítjuk elő:

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

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

Megnézem a kapcsolódó epizódot

A φ 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 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

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
