A feladatlista I.

Oszthatóság ①

$a \in \mathbb{Z}$ osztója $b \in \mathbb{Z}$-nek
ha létezik olyan $c \in \mathbb{Z}$
amire $a \cdot c = b$
Vagy ha b a-nak többszöröse
Ennek jele $a|b$
Ha a nem osztója b-nek $\Rightarrow a \nmid b$
Az a valódi osztója b-nek
ha $1 < |a| < |b|$

Prímszámok

$p \in \mathbb{Z}$ egészt prímnek nevezzük
ha $|p| > 1$ és nincs valódi osztója
Vagy ha $p = a \cdot b$ csak akkor
lehet ha $a = \pm 1$ vagy $b = \pm 1$
Ha $|p| > 1$ és nem prím akkor
összetett számnak mondjuk

Számelmélet alaptétele

I: Minden 1-től 0-tól és
-1-től különböző egész
szám felbontható prímek
szorzatára és ez a felbontás
sorrendtől és előjeltől
eltekintve egyértelmű

B: Megadunk egy eljárást
amely tetszőleges $n \in \mathbb{Z}$
$|n| > 1$ számot prímek
szorzatára bont
Legyen az n ± 1-től
különböző számok szorzata
akkor $n = a_1 \cdot a_2 \cdot \ldots \cdot a_k$
ha $a_1, a_2 \ldots a_k$ mind
prím akkor készen
vagyunk. Tfh nem
azok akkor legyen a_i
egy összetett szám
akkor $a_i = b \cdot c$ ahol
$|b|, |c| > 1$. Helyettesítsük
az n szorzatban a_i-t
$b \cdot c$-vel. Mivel n felbontása
minden lépésben növekszik
eggyel, és minden tényező
abszolút értéke legalább
2 ezért az eljárás
véges sok lépésben
(legfeljebb $\log_2 |n|$ tényezős
szorzattal) megáll s
megadja n egy prímtényezős
felbontását

Kongruencia

Legyenek $a, b, m \in \mathbb{Z}$ $m \neq 0$ egészek
a kongruens b-vel modulo m
ha a-t és b-t m-mel maradékosan
osztva azonos maradékot kapunk
Jele: $a \equiv b \ (m)$ az m a $a \equiv b \ (m)$
modulusa.
$a \equiv b \ (m) \Leftrightarrow$ ha $m | a - b$

Kongruencia műveletek

Tfh $a \equiv b \ (m)$ és $c \equiv d \ (m)$ és a, b, c, d,
m és $k \geq 1$ akkor:
(i) $a + c \equiv b + d \ (m)$
(ii) $a - c \equiv b - d \ (m)$
(iii) $a \cdot c \equiv b \cdot d \ (m)$
(iv) $a^k \equiv b^k \ (m)$

Definíció alapján $m | a - b$ és $m | c - d$
$\Rightarrow m | (a-b) + (c-d) = (a+c) - (b+d) \Rightarrow a + c \equiv b + d \ (m)$
$\Rightarrow m | (a-b) + (c-d) = (a-c) - (b-d) \Rightarrow a - c \equiv b - d \ (m)$
Mivel egy $m | a - b$ minden többszöröse
osztható m-el ezért $m | c(a-b) = ac - bc$
és $m | b(c-d) = bc - bd$
$\Rightarrow m | (ac - bc) + (bc - bd) = ac - bd \Rightarrow ac \equiv bd \ (m)$
(iv) pedig következik a (iii)-ból $a \cdot a \equiv b \cdot b \ (m)$

Legyen a, b, c, m tetsz. egészek és $d = (c, m)$
$\Rightarrow ac \equiv bc \ (m) \Leftrightarrow a \equiv b \ (\frac{m}{d})$

Legyen $c' = \frac{c}{d}$ és $d' = \frac{m}{d}$, akkor c' és d'
egészek és $(c', d') = 1$, mert ha nem akkor
$d \cdot (c', d')$ egy d-nél nagyobb közös osztója
lenne c-nek és m-nek
$ac \equiv bc \ (m) \Rightarrow m | ac - bc = c(a-b) \Rightarrow m'd |$
$\Rightarrow m'd | c'd(a-b) \Rightarrow m' | c'(a-b)$
$\Rightarrow m'k = c'(a-b)$ mivel $(c', m') = 1$
ezért $m'k = (a-b) \Rightarrow m' | a - b \Rightarrow$
$\Rightarrow a \equiv b \ (m')$

Lineáris kongruenciák ②

Azokat az x egészeket keressük (ha léteznek)
melyre $ax \equiv b \ (m)$ teljesül
Az $ax \equiv b \ (m) \Leftrightarrow (a, m) | b$, ha ez teljesül
akkor a megoldások száma mod m (a, m)

Legyen $d = (a, m)$ tfh $ax \equiv b \ (m)$ megoldható és legyen x_0 egy megoldás
$\Rightarrow a x_0 \equiv b \ (m) \Rightarrow m | a x_0 - b$ ebből $d | m$
miatt $d | a x_0 - b$ is következik, illetve $d | a$
miatt $d | a x_0$ is igaz $\Rightarrow d | b$
↑ Szükségesség
Elégségesség:
Először legyen $(a, m) = 1 \Rightarrow (a, m) | b$
Meg kell mutatni hogy $ax \equiv b \ (m)$ megoldható
ehhez az Euler Fermat tételt használjuk
$x = a^{\varphi(m) - 1} \cdot b \Rightarrow ax \equiv a^{\varphi(m)} b \equiv 1 \cdot b \equiv b \ (m)$
Így $x = a^{\varphi(m) - 1} \cdot b$ megoldás
Most legyen $(a, m) > 1$. Legyen $d = (a, m)$
és tfh $d | b$, ill legyen $a' = \frac{a}{d}$, $m' = \frac{m}{d}$, $b' = \frac{b}{d}$
akkor $(a', m') = 1$.
$ax \equiv b \ (m) \Leftrightarrow a'x \equiv b' \ (m')$, erre alkalmazható
az előbbi bizonyítás $\Rightarrow$ megoldható
A megoldások számához megint vegyük
az $(a, m) = 1$ esetet először. Tfh $x_1 \neq x_2$
és x_1, x_2 megoldások $\Rightarrow a x_1 \equiv a x_2 \ (m)$
$x_1 \equiv x_2 \ (m)$ tehát a modulus kompatibilis
ez csak 1 megoldás

Most vegyük az $(a, m) > 1$ esetet
$ax \equiv b \ (m) \Rightarrow a'x \equiv b' \ (m')$ és $(a', m') = 1$
tehát $a'x \equiv b' \ (m')$-nek pontosan 1 megoldása van (x_0).
Ekkor az összes megoldás $x = k \cdot m' + x_0$
alakú ahol k tetsz. egész
Legyenek $k_1 \neq k_2$ egészek
$k_1 m' + x_0 \equiv k_2 m' + x_0 \quad (m) \quad / - x_0$
$k_1 m' \equiv k_2 m' \quad (m) \quad / : m'$
$k_1 \equiv k_2 \quad (d) \qquad d = \frac{m}{(m, m')} = \frac{m}{m'}$
Tehát k helyére 0-tól $d-1$-ig bármely
számot írva megkapjuk az összes
megoldást, így a megoldások száma
mod m $d = (a, m)$

Euklideszi algoritmus

Bemenet: a, m
Kimenet: (a, m)

$m = t_1 a + r_1$
$a = t_2 r_1 + r_2$
$r_1 = t_3 r_2 + r_3$
$\vdots$
$r_k = t_{k+2} r_{k+1} + r_{k+2}$
$r_{k+1} = t_{k+3} r_{k+2} + 0$
akkor a kimenet $r_{k+2} = (a, m)$

$m \equiv r_1 \ (a)$, $(m, a) = (a, r_1)$ — 1. lépés
$a \equiv r_2 \ (r_1)$, $(a, r_1) = (r_1, r_2)$ — 2. lépés
$\vdots$
$r_{k+2} | r_{k+1} \Rightarrow (r_{k+1}, r_{k+2}) = r_{k+2}$

φ függvény ③

Ha $n \geq 2$ egész akkor az $1, 2 \ldots n-1$
számok közt az n-hez relatív prímek
számát $\varphi(n)$-nel jelöljük

Euler Fermat tétel

Ha a, m egész és $(a, m) = 1$ akkor
$a^{\varphi(m)} \equiv 1 \ (m)$

Legyen $R = \{c_1, c_2 \ldots c_k\}$ egy
redukált maradékrendszer mod
m. Mivel $(a, m) = 1 \Rightarrow R' = \{ac_1, ac_2 \ldots ac_k\}$
is egy redukált maradékrendszer
mod m.
$\Rightarrow c_1 c_2 \ldots c_k \equiv (ac_1)(ac_2) \ldots (ac_k) \ (m)$
$k = \varphi(m) \Rightarrow$
$\Rightarrow c_1 c_2 c_3 \ldots c_k \equiv a^{\varphi(m)} c_1 c_2 \ldots c_k \ (m)$
Mivel $(c_i, m) = 1 \Rightarrow$ oszthatunk $c_1 c_2 \ldots c_k$
-val $\Rightarrow 1 \equiv a^{\varphi(m)} \ (m)$

Egyenes egyenletrendszerei ⑤

Legyen e egy egyenes $\underline{V} = (a, b, c)$ az
egyenes egyik irányvektora, illetve
$\underline{P} = (x_0, y_0, z_0)$ az egyenes egyik pontja
akkor $P' \in e$ ha $\underline{P'} = \underline{P} + \lambda \cdot \underline{V}$ $\lambda \in \mathbb{R}$
$\underline{P_0} + \lambda \underline{V} = (x_0 + \lambda a, y_0 + \lambda b, z_0 + \lambda c)$

Ez az alábbival ekvivalens:

$x = x_0 + \lambda a$
$y = y_0 + \lambda b \qquad \lambda \in \mathbb{R}$
$z = z_0 + \lambda c$

Vagy

$$\frac{x-x_0}{a} = \frac{y-y_0}{b} = \frac{z-z_0}{c}$$

Sík egyenlete

Legyen egy S síknak egy $P_0(x_0,y_0,z_0)$ pontja és egy $\underline{n} \neq 0$ normálvektora. Ekkor egy $P(x,y,z)$ pontra $P \in S$ pontosan akkor igaz, ha
$ax+by+cz = ax_0+by_0+cz_0$

$P \in S$ pontosan akkor ha $\vec{P_0P} \parallel$ a síkkal

$\vec{P_0P} = (x-x_0, y-y_0, z-z_0)$

$\vec{P_0P}$ pontosan akkor $\parallel S$ ha $\perp \underline{n}$

Ez pedig (skaláris szorzat miatt) csak akkor igaz ha $\vec{P_0P} \cdot \underline{n} = 0$

$\vec{P_0P} \cdot \underline{n} = (x-x_0)a+(y-y_0)b+(z-z_0)c = 0$

$ax+by+zc = ax_0+by_0+z_0c$

Skaláris szorzat

$\underline{u} \cdot \underline{v} = |\underline{u}| \cdot |\underline{v}| \cdot \cos\varphi$

Legyen $\underline{u} = (u_1,u_2,u_3)$ és $\underline{v} = (v_1,v_2,v_3)$

Ekkor $\underline{u} \cdot \underline{v} = u_1v_1+u_2v_2+u_3v_3$

Vektoriális szorzat

$\underline{u} \times \underline{v}$ merőleges $\underline{u}$-ra és $\underline{v}$-re is illetve $|\underline{u} \times \underline{v}| = |\underline{u}| \cdot |\underline{v}| \cdot \sin\varphi$

$\mathbb{R}^n$ és $\mathbb{R}^n$ alterei (6)

Tetszőleges $n \geq 1$ n darab valós számból álló számoszlopok halmazát $\mathbb{R}^n$ jelöli

Legyen $\emptyset \neq V \subseteq \mathbb{R}^n$ az $\mathbb{R}^n$ egy altere ha

I. bármely $\underline{u}, \underline{v} \in V$ esetén $\underline{u}+\underline{v} \in V$

II. bármely $\underline{v} \in V$ esetén $\lambda \underline{v} \in V$

Jele: $V \leq \mathbb{R}^n$

Lineáris kombináció & generált altér

Legyenek $\underline{v}_1, \underline{v}_2 \dots \underline{v}_k \in \mathbb{R}^k$ vektorok és $\lambda_1, \lambda_2 \dots \lambda_k$ skalárok. Ekkor a $\lambda_1\underline{v}_1+\lambda_2\underline{v}_2 \dots \lambda_k\underline{v}_k$ vektort a $\underline{v}_1, \underline{v}_2 \dots \underline{v}_k$ vektorok $\lambda_1, \lambda_2 \dots \lambda_k$ skalárokkal vett lineáris kombinációjának nevezzük

Legyenek $\underline{v}_1, \underline{v}_2 \dots \underline{v}_k \in \mathbb{R}^n$ tetsz rögzített vektorok. Jelölje W az összes olyan $\mathbb{R}^n$-beli vektorok halmazát amelyek kifejezhetők $\underline{v}_1, \underline{v}_2 \dots \underline{v}_k$ lin. kombinációjával. Ekkor W altér $\mathbb{R}^n$-ben

Meg kell mutatni, hogy W zárt összeadásra és skalárral való szorzásra is, és $W \neq \emptyset$

Legyenek $\underline{w}_1, \underline{w}_2 \in W$

$\underline{w}_1 = \lambda_1\underline{v}_1+\lambda_2\underline{v}_2+\dots+\lambda_k\underline{v}_k$

$\underline{w}_2 = \beta_1\underline{v}_1+\beta_2\underline{v}_2+\dots+\beta_k\underline{v}_k$

$\Rightarrow \underline{w}_1+\underline{w}_2 = (\lambda_1+\beta_1)\underline{v}_1+(\lambda_2+\beta_2)\underline{v}_2+\dots+(\lambda_k+\beta_k)\underline{v}_k$

$\Rightarrow \underline{w}_1+\underline{w}_2 \in W$

$\alpha\underline{w}_1 = (\alpha\lambda_1)\underline{v}_1+(\alpha\lambda_2)\underline{v}_2+\dots+(\alpha\lambda_k)\underline{v}_k$

$\Rightarrow \alpha\underline{w}_1 \in W$

$\underline{0} \in W$ miatt $W \neq \emptyset$

↳ csupa 0 együtthatóval mindig kifejezhető

Lineáris függetlenség

A $\underline{v}_1, \underline{v}_2 \dots \underline{v}_k \in \mathbb{R}^n$ vektorrendszer akkor lin. független ha $\underline{v}_1, \underline{v}_2 \dots \underline{v}_k$ vektorok közül egyik sem fejezhető ki a többi lineáris kombinációjával

A $\underline{v}_1, \underline{v}_2 \dots \underline{v}_k \in \mathbb{R}$ lin. független $\Leftrightarrow$ $\lambda_1\underline{v}_1+\lambda_2\underline{v}_2+\dots\lambda_k\underline{v}_k = \underline{0}$ csak akkor teljesül ha $\lambda_1=\lambda_2=\dots=\lambda_k=0$

Tfh $\lambda_1\underline{v}_1+\lambda_2\underline{v}_2+\dots\lambda_k\underline{v}_k$ csak akkor teljesül ha $\lambda_1=\lambda_2=\dots=\lambda_k=0$

Tfh $\underline{v}_1, \underline{v}_2 \dots \underline{v}_k$ lineárisan összefüggő

$\Rightarrow$ Legyen $\underline{v}_1 = \alpha_2\underline{v}_2+\alpha_3\underline{v}_3+\dots+\alpha_k\underline{v}_k$

Átrendezve $1\cdot\underline{v}_1-\alpha_2\underline{v}_2+\alpha_3\underline{v}_3\dots-\alpha_k\underline{v}_k = \underline{0}$

↯

Tfh $\underline{v}_1, \underline{v}_2 \dots \underline{v}_k$ lin független

Tfh $\lambda_1\underline{v}_1+\lambda_2\underline{v}_2+\dots+\lambda_k\underline{v}_k = \underline{0}$-nál a $\lambda_1, \lambda_2 \dots \lambda_k$ számok közt van nemnulla együttható, legyen ez $\lambda_1 \Rightarrow$

$\Rightarrow \underline{v}_1 = -\frac{\lambda_2}{\lambda_1}\underline{v}_2-\frac{\lambda_3}{\lambda_1}\underline{v}_3-\dots-\frac{\lambda_k}{\lambda_1}\underline{v}_k$ ↯

F-G egyenlőtlenség

Legyen $V \leq \mathbb{R}^n$ altér, $\underline{f}_1, \underline{f}_2 \dots \underline{f}_k$ V-beli vektorokból álló lin. független rendszer $\underline{g}_1, \underline{g}_2 \dots \underline{g}_m$ pedig generátorrendszer V-ben. Ekkor $k \leq m$

Az alábbi lemma alapján egyértelmű (kicserélési lemma)

Legyen $V \leq \mathbb{R}^n$ altér, $\underline{f}_1, \underline{f}_2 \dots \underline{f}_k$ V-beli vektorokból álló lin fgetlen rendszer $\underline{g}_1, \underline{g}_2 \dots \underline{g}_m$ pedig generátorrendszer V-ben. Ekkor minden $i < k$ esetén található olyan $j \leq m$, hogy az $\underline{f}_1, \underline{f}_2 \dots \underline{f}_{i-1}, \underline{g}_j, \underline{f}_{i+1} \dots \underline{f}_k$ vektorrendszer is lin független

Tfh $\underline{f}_i$ igazából $\underline{f}_k$ $(i=k)$

Próbálkozzunk $\underline{g}_1$-el, ha $\underline{f}_1, \underline{f}_2 \dots \underline{f}_{k-1}, \underline{g}_1$ lin. fgetlen akkor kész vagyunk, ha nem akkor az újonnan érkezett vektor [illegible] miatt $\underline{g}_1 \in \langle \underline{f}_1, \underline{f}_2 \dots \rangle$

Ezt bármely $\underline{g}_j$-re megismételhetjük ha egyikre sem jó akkor hamis az állítás

De mivel $\langle \underline{f}_1, \underline{f}_2 \dots \underline{f}_{k-1} \rangle$ altér ezért zárt összeadásra, skalárral való szorzásra

Így $\underline{g}_1, \underline{g}_2 \dots \underline{g}_m$ vektorokkal együtt ezek minden lin. kombinációja is benne van $\langle \underline{f}_1, \underline{f}_2 \dots \underline{f}_{k-1} \rangle$-ben $\Rightarrow \underline{f}_k \in \langle \underline{f}_1, \underline{f}_2 \dots \underline{f}_{k-1} \rangle$ ↯

Mivel $\underline{g}_1, \underline{g}_2 \dots \underline{g}_m$ gen. rendszer

Bázis és dimenzió (7)

Legyen $V \leq \mathbb{R}^n$ altér. A V-ben $\underline{b}_1, \underline{b}_2 \dots \underline{b}_k$ vektorokat bázisnak nevezzük ha lin fgetlenek és gen rendszert alkotnak

Legyen a $V \leq \mathbb{R}^n$ altérben $\underline{b}_1, \underline{b}_2 \dots \underline{b}_k$ bázis. Ekkor V dimenziója k. Jele: $\dim V = k$

Standard bázis

Jelölje minden $1 \leq i \leq n$ esetén $\underline{e}_i$ azt az $\mathbb{R}^n$ beli vektort aminek minden koordinátája 0, kivéve az i. mert az 1. Ekkor $\underline{e}_1, \underline{e}_2 \dots \underline{e}_n$ bázist alkot.

$$\alpha_1\underline{e}_1+\alpha_2\underline{e}_2+\dots+\alpha_n\underline{e}_n = \begin{pmatrix}\alpha_1\\0\\\vdots\\0\end{pmatrix}+\begin{pmatrix}0\\\alpha_2\\\vdots\\0\end{pmatrix}+\dots+\begin{pmatrix}0\\\vdots\\0\\\alpha_n\end{pmatrix} = \begin{pmatrix}\alpha_1\\\alpha_2\\\vdots\\\alpha_n\end{pmatrix}$$

$\Rightarrow$ gen rendszer lin fgetlen, mert a $\underline{0}$ csak $\alpha_1=\alpha_2=\dots=\alpha_n=0$ esetén igaz

$\underline{e}_1, \underline{e}_2 \dots \underline{e}_n$ standard bázis $\mathbb{R}^n$-ben. Jele: E_n

Koordinátavektor fogalma

Legyen $V \leq \mathbb{R}^n$ altér $B=\{\underline{b}_1, \underline{b}_2 \dots \underline{b}_k\}$ bázis V-ben és $\underline{v} \in V$ tetszőleges vektor. Azt mondjuk hogy a $\underline{k} = \begin{pmatrix}\lambda_1\\\lambda_2\\\vdots\\\lambda_k\end{pmatrix} \in \mathbb{R}^k$ vektor a $\underline{v}$ vektor B szerinti koordinátavektora ha $\underline{v} = \lambda_1\underline{b}_1+\lambda_2\underline{b}_2+\dots+\lambda_k\underline{b}_k$

Ennek jelölése: $\underline{k} = [\underline{v}]_B$

Lin egyenlet rendszer megoldása Gauss elimmel

Sorekvivalens lépések:

(i) egy sor tagonkénti szorzása λ-val
(ii) egy sorhoz tagonként egy másik sor λ-szorosának hozzáadása
(iii) két sor cseréje
(iv) csupa nulla sor elhagyása

Az csak ilyen gauss eliminációt felsz azt csá

Megoldhatóság, megoldás egyértelműsége

(i) van tilos sor => nem megoldható
(ii) lépcsős alak + minden sorban vezéregyes => egyértelmű megoldás
(iii) lépcsős alak + nincs minden sorban vezéregyes => végtelen sok megoldás

Ha egy k egyenletből álló n ismeretlenes lineáris egyenletrendszer egyértelműen megoldható akkor $k \geq n$

Gauss elim lefuttatása után a sorok száma k'. $k' \leq k$
Mivel megoldható ezért minden sorban van vezéregyes így $k \geq k' = n$

Lépcsős alak

Egy kibővített együtthatómátrixot lépcsős alakúnak mondunk, ha:

(i) Minden sorában van nemnulla elem, és (balról) az első nemnulla egy egyes (vezéregyes)
(ii) Ha $1 \leq i < j \leq k$ akkor az i. sorban álló vezéregyes kisebb sorszámú oszlopban van mint a j. sorban álló
(iii) A vezéregyesekkel egy oszlopban azok alatt álló minden elem 0

Redukált lépcsős alak:

(iv) A vezéregyesekkel egy oszlopban az azok fölött álló minden elem is 0

Determináns (9)

Inverziószám:

Azt mondjuk, hogy a $\pi=(\pi_1,\pi_2\ldots\pi_n)$ permutációban π_i és π_j számok inverzióban állnak, ha $i<j$ de $\pi_i>\pi_j$
A permutáció inverziószáma az összes ilyen inverzióban álló számpár száma. Jele: $I(\pi)$

Bástyaelhelyezés:

Ha a mátrix minden sorából s oszlopából pontosan egy elem van kiválasztva. A permutáció soronként értendő

A feketelista II

(8)

Legyen adott egy $(n\times n)$-es A mátrix. Az A minden bástyaelhelyezésére szorozzuk össze az azt alkotó n elemet majd szorozzuk meg ezt $(-1)^{I(\pi)}$-el. Az így kapott szorzat lesz A determinánsa
Jele: $|A|$ vagy $\det A$

Legyen A egy $(n\times n)$-es mátrix

(i) Ha A-nak van csupa 0 elemet tartalmazó sora vagy oszlopa akkor $\det A = 0$
(ii) Ha A felső vagy alsóháromszög-mátrix akkor a determinánsa a főátlóbeli elemek szorzata

Legyen A egy $(n\times n)$-es mátrix, $\lambda\in\mathbb{R}$ skalár $1\leq i,j\leq n$, $i\neq j$ egészek

(i) Ha A egy sorát vagy oszlopát (tagonként) megszorozzuk λ-val akkor a kapott A' mátrix determinánsa λ szorosa A-énak $\det A' = \lambda\cdot\det A$
(ii) Ha A két sorát vagy két oszlopát felcseréljük akkor a kapott A' mátrix determinánsa ellentettje A-énak: $\det A' = (-1)\det A$
(iii) Ha A i-edik sorát helyettesítjük saját magának és a j-edik sor λ-szorosának (tagonként vett) összegével, akkor a kapott A' mátrix determinánsa megegyezik A-éval $\det A' = \det A$

(i):
Minden bástyaelhelyezésbe kerül egy egy új tag ami λ szorosa az eredetinek(A) így az összegből λ kiemelhető $\Rightarrow |A'| = \lambda\cdot\det A$

(ii):
Az eredeti és a felcserélt mátrixban a bástyaelhelyezések párba állíthatóak úgy, hogy közöttük két szám van csak a permutációban felcserélve (ez azt jelenti, hogy az inverziószámuk paritása más) így az (i)-hez hasonlóan -1 minden szorzatból kiemelhető $\Rightarrow |A'| = -|A|$

(iii):
Lemma:
Ha az $(n\times n)$-es X, Y és Z mátrixok az i-edik soraiktól eltekintve elemről elemre megegyeznek. Az i. soraikra viszont fennáll, hogy $z_{i,j}=x_{i,j}+y_{i,j}$ minden $1\leq j\leq n$ esetén vagyis a Z i. sora épp az X és az Y i. sorának (tagonként) összege. Akkor $\det Z = \det X + \det Y$

Vegyünk egy bástyaelhelyezést Z-ben

$(-1)^{I(\pi)} \cdot z_{1,\pi_1} \cdot \ldots \cdot z_{i,\pi_i} \cdot \ldots \cdot z_{n,\pi_n} =$

$=(-1)^{I(\pi)} \cdot z_{1,\pi_1}\cdot\ldots\cdot(x_{i,\pi_i}+y_{i,\pi_i})\cdot\ldots\cdot z_{n,\pi_n}$

$=(-1)^{I(\pi)}\cdot z_{1,\pi_1}\cdot\ldots\cdot x_{i,\pi_i}\cdot\ldots\cdot z_{n,\pi_n}+(-1)^{I(\pi)}\cdot z_{1,\pi_1}\cdot\ldots\cdot y_{i,\pi_i}\cdot\ldots =$

$=(-1)^{I(\pi)}\cdot x_{1,\pi_1}\cdot\ldots\cdot x_{i,\pi_i}\cdot\ldots\cdot x_{n,\pi_n}+(-1)^{I(\pi)}\cdot y_{1,\pi_1}\cdot\ldots\cdot y_{i,\pi_i}\cdot\ldots\cdot y_{n,\pi_n}$

$\rightsquigarrow \det X + \det Y$

Alkalmazzuk a lemmát.
Legyen $Z = A'$, $X = A$ és Y az a mátrix amely mindenhol megegyezik A-val kivéve az i. sorban mert ott a j. sor λ szorosa.
$\Rightarrow \det Z = \det A + \det Y$
Tehát kész leszünk, ha belátjuk, hogy $\det Y = 0$
Legyen Y' ugyanaz mint Y csak az i. sorban egy j. sor másolata áll. Akkor $|Y| = \lambda\cdot|Y'|$
Ha Y'-ben felcseréljük az i. és j. sort akkor $|Y''| = (-1)|Y'|$
Viszont változatlan marad mert a két felcserélt sor ugyanaz
$\Rightarrow \det Y = 0$

Determináns kiszámítása

Gauss elim a fenti szabályokkal

Kifejtési tétel (10)

Aldetermináns:
Az $(n\times n)$-es mátrix $a_{i,j}$ eleméhez tartozó előjeles aldetermináns-t úgy kapjuk meg, hogy A-ból elhagyjuk az i. sorát és j. oszlopát majd a kapott $(n-1)\times(n-1)$-es mátrix determinánsát $(-1)^{i+j}$-el szorozzuk

Ha az $(n\times n)$-es A mátrix valamely sorának/oszlopának minden elemét megszorozzuk a hozzá tartozó előjeles aldetermináns értékével s a kapott szorzatokat összeadva $\det A$-t kapjuk

Mátrix műveletek

Legyen $A,B,C \in \mathbb{R}^{k\times n}$, és $\lambda,\mu \in \mathbb{R}$

(i) $A+B=B+A$
(ii) $(A+B)+C = A+(B+C)$
(iii) $\lambda(A+B)=\lambda A+\lambda B$
(iv) $(\lambda+\mu)A = \lambda A+\mu A$
v $\lambda(\mu A)=(\lambda\mu)A$

$\lambda\cdot A$ esetén a mátrix összes tagját λ-val szorozzuk

A $(k\times n)$-es A és az $(n\times m)$-es B mátrixok szorzatának nevezzük és AB-vel jelöljük azt a $(k\times m)$-es C mátrixot amelyre minden $1\leq i\leq k$ és $1\leq j\leq m$ esetén
$c_{i,j}=a_{i,1}b_{1,j}+\ldots+a_{i,n}b_{n,j}$

Legyenek A,B,C mátrixok λ pedig egy skalár

(i) $(\lambda A)B = \lambda(AB) = A\cdot(\lambda B)$
(ii) $A(B+C)=AB+AC$ és $(B+C)A = BA+CA$
(iii) $(AB)C = A(BC)$

(i):
Legyen A egy $(k\times n)$-es mátrix. Ekkor λA is $(k\times n)$-es. Legyen B $(n\times m)$, legyen $X=A\cdot B$, $Y=\lambda(AB)$ és $Z=(\lambda A)\cdot B$. Ekkor minden $1\le i\le k$ és $1\le j\le m$ esetén $x_{i,j}=a_{i,1}\cdot b_{1,j}+\dots+a_{i,n}\cdot b_{n,j}$, így $y_{i,j}=\lambda(a_{i,1}\cdot b_{1,j}+\dots+a_{i,n}\cdot b_{n,j})$, illetve az is igaz hogy: $z_{i,j}=(\lambda a_{i,1})b_{1,j}+\dots+(\lambda a_{i,n})b_{n,j}$ ebből λ-t kiemelve $y_{i,j}=z_{i,j}$

(ii):
Legyen A $(k\times n)$-es B és C pedig $(n\times m)$-es mátrixok. Legyen $X=AB$, $Y=AC$, $Z=A(B+C)$, most definíció szerint $x_{i,j}=a_{i,1}\cdot b_{1,j}+\dots+a_{i,n}\cdot b_{n,j}$
$y_{i,j}=a_{i,1}\cdot c_{1,j}+\dots+a_{i,n}\cdot c_{n,j}$ és
$z_{i,j}=a_{i,1}\cdot(b_{1,j}+c_{1,j})+\dots+a_{i,n}(b_{n,j}+c_{n,j})$
Látszik, hogy $z_{i,j}=x_{i,j}+y_{i,j}$

(iii):
Legyen A $(k\times n)$-es, B $(n\times m)$-es. Ekkor a szorzat $(k\times m)$-es lesz. Ekkor ezt C-vel csak akkor tudjuk megszorozni ha az $(m\times t)$-s. A két oldal elvégezhetősége ekvivalens. Legyen $X=A\cdot B$ és $Y=(A\cdot B)\cdot C$
$\Rightarrow y_{i,j}=x_{i,1}\cdot c_{1,j}+\dots+x_{i,m}\cdot c_{m,j}$
$y_{i,j}=(a_{i,1}\cdot b_{1,1}+\dots+a_{i,n}\cdot b_{n,1})c_{1,j}+\dots+(a_{i,1}\cdot b_{1,m}+\dots+a_{i,n}\cdot b_{n,m})c_{m,j}$
így $y_{i,j}$ elemei $a_{i,r}\cdot b_{r,s}\cdot c_{s,j}$ féle szorzatok, a másik zárójelezés felbontásával és felírásával u ezt kapjuk, so its cool.

n×n-es lin egy. rendszer megoldhatósága (11)

Legyen $(A|b)$ egy n változós n egyenletes lin. egy. rszr. kibővített együttható mátrixa.
Az egy. rszr. egyértelműen megoldható $\Leftrightarrow \det A\neq\emptyset$

A Gauss elim. lépései nem változtatnak a mátrix det.-jának nulla vagy nemnullaságán.
1. Tilos sor $\det=\emptyset$ és $\nexists$ m.o.
2. Végtelen sok m.o. $\Rightarrow$ lépcsős alak ahol kevesebb sor van mint oszlop, tehát volt (elhagyott) $(n\times n)$ csupa 0 sor $\Rightarrow \det=\emptyset$ és $\nexists$ egyértelmű m.o.
3. Ugyanannyi sor mint oszlop a lépcsős alakban $\Rightarrow \det\neq\emptyset$ és $\exists$ egy. megoldás

Mátrix inverze (12)

Egy $(n\times n)$-es A mátrix inverzének nevezzük az $(n\times n)$-es X mátrixot, ha $A\cdot X=E=X\cdot A$.
Jele: A^{-1}

Az $(n\times n)$-es A mátrixnak létezik inverze $\Leftrightarrow \det A\neq\emptyset$. Ha A^{-1} létezik, akkor egyértelmű

Tfh $X=A^{-1}$ létezik.
Det. szorzástétel: $\det(A\cdot X)=\det E=1$
$\det A\cdot\det X=1\Rightarrow\det A\neq\emptyset$

Lemma:
Ha $A\in\mathbb{R}^{n\times n}$ és $\det A\neq\emptyset$, akkor egyértelműen létezik egy olyan $X\in\mathbb{R}^{n\times n}$ mátrix, amelyre $A\cdot X=E$

Legyenek $x_1,x_2\dots x_n$ az X mátrix oszlopai, ekkor $A\cdot\underline{x}_1=\underline{e}_1$, $A\cdot\underline{x}_2=\underline{e}_2\dots A\underline{x}_n=\underline{e}_n$
Mivel $\det A\neq\emptyset$ ezért $A\cdot\underline{x}_i=\underline{e}_i$ egyértelműen megoldható $\Rightarrow A\cdot X=E$ egyértelműen megtalálható

Lemma $\Rightarrow A^{-1}$ ha létezik $\Rightarrow$ egyértelmű
Még be kell látni, h $X\cdot A=E$ is igaz
Lemma $\Rightarrow X^{-1}$ létezik s egyértelmű mert $\det X\neq\emptyset$ $(\det A\cdot\det X=1)$
Legyen $X^{-1}=Y$, ha $A=Y$ akkor kész
$(AX)\cdot Y=A\cdot(XY)$, $AX=E\Rightarrow(AX)Y=EY=Y$
Hasonlóan $XY=E$ miatt $A(XY)=AE=A$
$\Rightarrow Y=A$ ✓✓

Kiszámítás
$$(A\mid E)\xrightarrow{\text{Gauss elim}}(E\mid X)$$

Rang

Legyen A tetsz. mátrix
(i) A oszloprangja r, ha A oszlopai közül kiválasztható r darab úgy, hogy a kiválasztott oszlopok lin. fgetlenek de r+1 nem választható már így ki
(ii) Ugyanez sorra
(iii) A determinánsrangja r, ha A-nak van nemnulla determinánsú $(r\times r)$-es részmátrixa de $((r+1)\times(r+1))$-es nincs

Legyen A $(k\times n)$-es mátrix az oszlopai legyenek $\underline{a}_1,\underline{a}_2\dots\underline{a}_n$. Ekkor $r(A)=\dim\langle a_1,a_2\dots a_n\rangle$

Válasszuk ki A oszlopai közül a lehető legtöbbet úgy, h ezek lin. fgetlenek legyenek. Ekkor ezek száma $r=r(A)$
Állítjuk, h $\underline{a}_1,\underline{a}_2\dots\underline{a}_r$ bázist alkot $\langle\underline{a}_1,\underline{a}_2\dots\underline{a}_n\rangle=W$
$\underline{a}_1,\underline{a}_2\dots\underline{a}_r$ lin. fgetlen. Legyen $\langle\underline{a}_1,\underline{a}_2\dots\underline{a}_r\rangle=U$. Célunk belátni h $U=W$. $U\subseteq W$, $W\subseteq U$ kell. Tetszőleges $r<i\le n$ esetén $\underline{a}_1,\underline{a}_2\dots\underline{a}_r,\underline{a}_i$ lin. öf. Az újonnan érkező vektor lemmája miatt $a_i\in\langle\underline{a}_1,\underline{a}_2\dots\underline{a}_r\rangle$ tehát $\underline{a}_1,\underline{a}_2\dots\underline{a}_n\in U\Rightarrow W\subseteq U$

Lin. leképezés fogalma, mátrixa (13)

Az $f:\mathbb{R}^n\to\mathbb{R}^k$ fgvt lin. leképezésnek hívjuk, ha létezik egy olyan $(k\times n)$-es A mátrix amelyre $f(\underline{x})=A\cdot\underline{x}$ teljesül minden $\underline{x}\in\mathbb{R}^n$ esetén
Az $n=k$ esetén f-et lin trafónak is nevezzük. Ha $f:\mathbb{R}^n\to\mathbb{R}^k$ lin leképezés és $f(\underline{x})=A\cdot\underline{x}$ minden $\underline{x}\in\mathbb{R}^n$-re akkor azt mondjuk h f-nek a mátrixa A. Jele $A=[f]$

Szükséges s elégséges feltétel
Az $f:\mathbb{R}^n\to\mathbb{R}^k$ függvény akkor és csak akkor lin. leképezés, ha teljesül rá az alábbi két tulajdonság
(i): $f(\underline{x}+\underline{y})=f(\underline{x})+f(\underline{y})$ igaz minden $x,y\in\mathbb{R}^n$ esetén
(ii): $f(\lambda\underline{x})=\lambda\cdot f(\underline{x})$ igaz minden $\lambda\in\mathbb{R}$ $\underline{x}\in\mathbb{R}^n$ esetén
Ha f ezeket teljesíti $\Rightarrow$ lin. leképezés és $[f]$ egyértelmű és azonos azzal a mátrixxal melynek minden i. oszlopa $1\le i\le n$ esetén $f(\underline{e}_i)$.

Tfh. f lin. lek. és $[f]=A$
A mátrix szorzás tulajdonságok miatt $f(\underline{x}+\underline{y})=A\cdot(\underline{x}+\underline{y})=A\cdot\underline{x}+A\underline{y}=$
$=f(\underline{x})+f(\underline{y})$ és $f(\lambda\cdot\underline{x})=A(\lambda\cdot\underline{x})=$
$=\lambda(A\cdot\underline{x})=\lambda\cdot f(\underline{x})$
Ha f lin. lek. $\Rightarrow[f]$ egyértelmű
Legyen f-nek A egy (lehetséges) mátrixa. Jelölje $\underline{a}_i$ A-nak i-edik oszlopát. $A\cdot\underline{e}_i=\underline{a}_i$, ekkor $[f]=A$ miatt $f(\underline{e}_i)=A\cdot\underline{e}_i=\underline{a}_i$
$\Rightarrow[f]$ egyértelmű
Végül belátjuk az elégségességet
Kell egy A mátrix melyre $f(\underline{x})=A\cdot\underline{x}$ teljesül minden $\underline{x}\in\mathbb{R}^n$ esetén
A fentiek alapján A i-edik oszlopa $\underline{a}_i=f(\underline{e}_i)$. Ekkor $f(\underline{x})=A\cdot\underline{x}$ teljesül minden $\underline{e}_i$-re
Legyen $V=\{\underline{x}\in\mathbb{R}^n: f(\underline{x})=A\cdot\underline{x}\}$, tudjuk hogy $\underline{e}_i\in V$, célunk $V=\mathbb{R}^n$ megmutatása
V altér, mert $f(\underline{u})=A\cdot\underline{u}$, $f(\underline{v})=A\cdot\underline{v}$ példákra szorzásra s összeadásra zárt. V altér $\mathbb{R}^n$-ben és tartalmazza az $\underline{e}_1,\underline{e}_2\dots\underline{e}_n$ vektorokat.
$\Rightarrow V=\mathbb{R}^n$ mert $e_1,e_2\dots e_n$ minden lin. kombinációját tartalmazza

Magtér, Képtér (14)

Legyen $f:\mathbb{R}^n\to\mathbb{R}^k$ lin. lek. f magterének nevezzük és Ker f-fel jelöljük azon $\mathbb{R}^n$-beli vektorok halmazát, amelyek a képe az $\mathbb{R}^k$-beli nullvektor
$\operatorname{Ker} f=\{\underline{x}\in\mathbb{R}^n: f(\underline{x})=0\}$
f képterének és Im f-fel jelöljük azon $\mathbb{R}^k$ vektorok halmazát amelyek megkaphatók (legalább) egy alkalmas $\mathbb{R}^n$-beli vektor f-fel vett képeként
$\operatorname{Im} f\{\underline{y}\in\mathbb{R}^k:\exists\underline{x}\in\mathbb{R}^n, f(\underline{x})=\underline{y}$

Sajátvektor, sajátérték (16)

Legyen A egy $(n \times n)$-es mátrix

(i) A sajátértékének nevezzük a $\lambda \in \mathbb{R}$ skalárt, ha létezik olyan $\underline{x} \in \mathbb{R}^n$, $\underline{x} \neq \underline{0}$ vektor amelyre $A \cdot \underline{x} = \lambda \cdot \underline{x}$ teljesül

(ii) A sajátvektorának nevezzük az $\underline{x} \in \mathbb{R}^n$ vektort, ha $\underline{x} \neq \underline{0}$ és létezik olyan $\lambda \in \mathbb{R}$ melyre $A \cdot \underline{x} = \lambda \cdot \underline{x}$ teljesül.

A négyzetes A mátrixnak a $\lambda \in \mathbb{R}$ skalár akkor és csak akkor sajátértéke, ha $\det(A - \lambda E) = 0$.

λ def szerint akkor sajátérték, ha $A \cdot \underline{x} = \lambda \cdot \underline{x}$-nek van egy $\underline{x} \neq \underline{0}$ megoldása. $\lambda \cdot \underline{x} = (\lambda \cdot E)\underline{x}$

$(\lambda \cdot E)\underline{x} = \lambda \cdot (E \cdot \underline{x}) = \lambda \cdot \underline{x}$. Az $A\underline{x} = (\lambda E)\underline{x}$ egyenletet átrendezve:

$$A \cdot \underline{x} - (\lambda \cdot E)\underline{x} = \underline{0}$$

$$(A - \lambda E)\underline{x} = \underline{0}$$

λ tehát csak akkor sajátérték ha $(A - \lambda E)\underline{x} = \underline{0}$ megoldható ez pedig csak akkor, ha $|A - \lambda E| = 0$

Primek száma (1)

A primek száma végtelen

Tfh a primek száma véges, ekkor legyen $p_1, p_2 \dots p_k$ az összes prim. Legyen $N = p_1 \cdot p_2 \cdots p_k + 1$. N vagy primek szorzata, vagy prim. De a $p_1, p_2 \dots p_k$ primek egyikével sem osztható (mindegyikkel 1 maradékot ad). Tehát vagy N prim, vagy van primtényezője ami nem eleme a $p_1 p_2 \dots p_k$ primeknek ↯

π(n) nagyságrendje

$\pi(n) \approx \frac{n}{\ln(n)}$, vagy $\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln(n)}} = 1$

Euklideszi algoritmus lépésszáma (2)

Az Euklideszi algoritmus legfeljebb $2\cdot\lceil \log_2 a\rceil$ maradékos osztás után megáll

Vizsgáljunk meg egy tetszőleges lépést $r_{i-2} = t_i \cdot r_{i-1} + r_i$ ahol $r_{i-2} > r_{i-1} > r_i$. $t_i \ge 1 \Rightarrow r_{i-2} \ge r_{i-1} + r_i$, $r_{i-1} > r_i \Rightarrow r_{i-2} \ge 2r_i$. Ennek $a = r_0 > 2r_2 > 4r_4 > \dots > 2^s \cdot r_{2s}$. Az $s = \lceil\log_2 a\rceil$ értékre $2^s \ge a$, feltéve hogy 2s-ig nem ér véget az eljárás $0 < r_{2s} < \frac{a}{2^s} \le 1$-et kapunk ↯

Euklideszi algoritmus kongruenciákra

Bemenet: a, b és m poz. egészek

Kimenet: A c és m' egészek amelyekre $a\cdot x \equiv b$ (m) lin. kongruencia megoldáshalmaza $x \equiv c$ (m') vagy ha nincs megoldás

(*) $m \cdot x \equiv 0$ (m)

(B) $a \cdot x \equiv b$ (m)

(*) $- t_1$(B): (1) $r_1 \cdot x \equiv -t_1 \cdot b = C_1$ (m)

(B) $- t_2$(1): (2) $r_2 \cdot x \equiv b - t_2 C_1 = C_2$ (m)

(1) $- t_3$(2): (3) $r_3 \cdot x \equiv C_1 - t_3 C_2 = C_3$ (m)

⋮

(k) $r_k \cdot x \equiv C_{k-2} - t_k C_{k-1} \equiv C_k$ (m)

Az algoritmus végén $r_k = 1 \Rightarrow x \equiv C_k$ (m) kongruenciát kapjuk.

φ meghatározása primhatványra (3)

Tfh $n = p^\alpha$ ahol p prim $\Rightarrow \varphi(n) = p^\alpha - p^{\alpha-1}$ ($\alpha \ge 1$)

Ekkor $(n,a) > 1 \iff p|a \Rightarrow$ az 1,2… n számok közül $\frac{n}{p} = \frac{p^\alpha}{p} = p^{\alpha-1}$ darab nem rel. prim n-hez $\Rightarrow \varphi(n) = p^\alpha - p^{\alpha-1}$

Redukált maradékrendszer

Az $R = \{c_1, c_2 \dots c_k\}$ számhalmaz redukált maradékrendszer mod m ha a következő feltételeknek eleget tesz

The Rest 1.

(i): $(c_i, m) = 1$ minden 1,2… k esetén

(ii): $c_i \not\equiv c_j$ (m) bármely $i \ne j$ $1 \le i,j \le k$ esetén

(iii) $k = \varphi(m)$

Legyen $R = \{c_1, c_2 \dots c_k\}$ redukált maradékrendszer mod m és legyen $(a,m)=1 \Rightarrow R' = \{a\cdot c_1, a\cdot c_2, \dots, a\cdot c_k\}$ is redukált maradékrendszer mod m

Meg kell mutatni, hogy R' is red. maradék rendszer mod m ha R' az.

(i): $(a \cdot c_i, m) = 1$ mivel $(a,m)=1$ és $(c_i,m)=1$ is igaz.

(ii): tfh $a\cdot c_i \equiv a \cdot c_j$ (m) /:a

$c_i \equiv c_j$ $\left(\frac{m}{(m,a)} = \frac{m}{1} = m\right)$ ↯

(iii): mivel ez R-re teljesül ezért R'-re is fog

Kis Fermat

Ha p prim és a tetsz egész $\Rightarrow a^p \equiv a$ (mod p)

Ha $p|a \Rightarrow$ egyértelmű

Ha $p \nmid a \Rightarrow (p,a) = 1$ ezután Euler-Fermat tételt alkalmazva és a-val szorozva megkapjuk a tétel állítását

Két kongruenciás kongruenciarendszer

$x \equiv a_1$ (m_1) $\Rightarrow x = k\cdot m_1 + a_1$

$x \equiv a_2$ (m_2)

$\Rightarrow k\cdot m_1 + a_1 \equiv a_2$ (m_2)

→ ezt megoldjuk k-ra, majd visszahelyettesítünk $x = k\cdot m_1 + a_1$-be

$k = m'\cdot l + c' \Rightarrow x = (m'\cdot l + c')m_1 + a_1$ itt mindent ismerünk ⇒ megvan a megoldás

Polinomiális futásidejű algoritmus (4)

A algoritmus S inputméretben akkor polinomiális ha léteznek c és k(k>0) konstansok, hogy minden $n \ge 1$, $n \in \mathbb{N}$ méretű inputra futtatva maximum $c \cdot n^k$ lépés után megáll

Számelméleti algoritmusok

Összeadás

Input: a, b

Méret: a: k db számjegy, b: l db számjegy } n db

Output: a+b

Legyen $k \ge l$ ⇒ A ciklust k-szor hajtjuk végre. A ciklusban, a számok következő két számjegyhez hozzáadjuk az előző két számjegy által kreált maradékot ⇒ a ciklusmag c db bitművelettel megvalósítható ⇒ a ciklus: c·k

Kivonásra ugyanez

Szorzás osztás:

Nem lineáris futásidejű. $c \cdot n^2$

Hatványozás:

Bemenet: a, b

Méret: a → k db, b → l db } n db

Output: a^b

Nem létezik polinomiális futásidejű algoritmus. Tfh $a = 2 \Rightarrow a^b$ jegyeinek száma $\approx \log_{10} 2^b = b \cdot \log_{10} 2 \ge \log_{10} 2 \cdot 10^k > 0{,}03 \cdot 10^k$ → Így a jegyek száma is exponenciális ⇒ kiírni sem polinomiális

Primtesztelés, Carmichael számok

Bemenet: m → n db jegy

Kimenet: m prim-e

Euler Fermat tételen alapszik: Ha m prim, és $1 \le a \le m-1$ tetsz, akkor $\varphi(m) = m$ és $(a,m)=1 \Rightarrow a^{m-1} \equiv 1$ (m). Ha sikerül találni a-t amire $a^{m-1} \not\equiv 1$ (m) akkor m nem prim

A Fermatteszt nevű algoritmus egymás után random a-k-ra megnézi ezt a kongruenciát.

Az algoritmus először generál a-t. Majd megnézi (a,m)-t ha ez nem 1 akkor m összetett s egy osztója is megvan. Ha (a,m)=1 akkor megnézzük az $a^{m-1} \equiv 1$ (m) kongruenciát. Ha ezen a teszten azon szám egy előre rögzített k darabszor átmegy akkor valószínűleg prim

Ha m összetett és $a^{m-1} \equiv 1$ (m) akkor a m cinkosa, ellenkező esetben pedig árulója

Az m>1 összes számot nevezzük álprimnek, vagy más szóval Carmichael számnak hívjuk ha nincs árulója, vagyis $\forall 1 \le a \le m$ $(a,m)=1$ számra $a^{m-1} \equiv 1$ (m)

RSA kód anyag

Kódolás: C(x) → kódoló → üzenet

$D(x) = C^{-1}(x)$ → dekódoló

$\Rightarrow D(C(x)) = x$

Legyen x egy rögzített 1–N egész

Olyan C, D kell amire:

(i): $\forall x \in \{0, 1 \dots N-1\}$-re $D(C(x)) = x$

(ii): C és D hatékonyan használható

(iii): C nyilvánosságra hozható s ettől D nem lesz kiszámolható

Legyenek p és q primek, illetve $N = pq$ ⇒ tetsz x és $k \ge 1$ egészre $x^{k\varphi(N)+1} \equiv x$ (N)

Ha $(x,N) = 1 \Rightarrow$ egyértelmű (E-F)

Ha $(x,N) \ne 1 \Rightarrow p|x$, vagy $q|x$, ha mindkettő igaz $\Rightarrow x^{k\varphi(N)+1} \equiv x \equiv 0$ (N)

tfh $p \nmid x$, $q|x \Rightarrow (p,x) = 1$ és $\varphi(p) = p-1$

$x^{p-1} \equiv 1$ (p). Mivel $\varphi(N) = (p-1)(q-1)$ ezért $(x^{p-1})^{k(q-1)} = x^{k\varphi(N)} \Rightarrow x^{k\varphi(N)} \equiv x$ (p)

Ez a $q|x$ miatt mod q-ra is fennáll.

$\Rightarrow p | x^{k\varphi(N)} - x$ és $q | x^{k\varphi(N)} - x \Rightarrow N | x^{k\varphi(N)} - x \Rightarrow$

$\Rightarrow x^{k\cdot\varphi(N)} \equiv x$ (N)

Actual shit:

Legyen p,q prím $N=p\cdot q$, C úgy hogy $(C,\varphi(N))=1$. Ekkor C fgv: $x\mapsto x^{C}\ (N)$
Ehhez keressünk $D: y\mapsto y^{d}\ (N)$
$D(C(x))\equiv x^{cd}\ (N) \Rightarrow x\equiv x^{cd}$
Így ha d értéke jó, akkor $cd=k\,\varphi(N)+1$
vagyis $\varphi(N)\mid c\cdot d-1$ vagyis $cd\equiv 1\ (\varphi(N))$
C és $\varphi(N)$ adottak, ezért ez d-re egy lineáris kongruencia ami a $(C,\varphi(N))=1$ miatt megoldható
$\varphi(N)$ ismeretéhez szükséges q és p
mivel $\varphi(N)=p\cdot q$

Térbeli koordgeo (5)

Térben egy pontot három koordináta határoz meg

Legyenek $u=(u_1,u_2,u_3)\in\mathbb{R}^3$ és $v=(v_1,v_2,v_3)\in\mathbb{R}$ térvektorok, és $\lambda\in\mathbb{R}$ skalár. Ekkor:
(i) $u+v=(u_1+v_1,u_2+v_2,u_3+v_3)$
(ii) $\lambda\cdot u=(\lambda u_1,\lambda u_2,\lambda u_3)$

Lin. fg., gen. rszr, bázis geo feltétele

Lineáris függetlenség:
1 vektor: nem párhuzamos
2 vektor: nincs benne a meghatározott síkban
3 vektor: nincs
az új vektor
Gen rszr:
Ugyan az mint fent csak lehet benne párhuzamos
N vektor amiben:
$\mathbb{R}^1$: –
$\mathbb{R}^2$: van 2 ami nem párhuzamos
$\mathbb{R}^3$: van 3 ami nem esik egy síkba
Bázis: Pontosan 1, 2, 3 amire igaz a gen. rszr és lin. fg feltétele is

Az újonnan érkező vektor lemmája (6)

Tfh $f_1,f_2\dots f_k$ lin. fgtlen, de $f_1,f_2\dots f_k,f_{k+1}$ lin. összefüggő $\Rightarrow f_{k+1}\in\langle f_1,f_2\dots f_k\rangle$

Mivel $f_1,f_2\dots f_k,f_{k+1}$ lin. öf. $\Rightarrow$
$\Rightarrow \lambda_1 f_1+\dots+\lambda_k f_k+\lambda_{k+1} f_{k+1}=0$
úgy, hogy $\lambda_{k+1}\neq 0$ (ha $\lambda_{k+1}=0$ lenne akkor $f_1,f_2\dots f_k$ nem lenne lin. fgtlen)
$\lambda_1 f_1+\lambda_2 f_2+\dots+\lambda_k f_k+\lambda_{k+1} f_{k+1}=0$-ból
$f_{k+1}=-\frac{\lambda_1}{\lambda_{k+1}}f_1-\frac{\lambda_2}{\lambda_{k+1}}f_2-\dots-\frac{\lambda_k}{\lambda_{k+1}}f_k$
$\Rightarrow f_{k+1}\in\langle f_1,f_2\dots f_k\rangle$

A dimenzió egyértelműsége (7)

Tfh $V\le\mathbb{R}^n$ altérben $b_1,b_2,\dots b_k$ és $c_1,c_2\dots c_m$ egyaránt bázisok $\Rightarrow k=m$

$b_1,b_2\dots b_k$ lin. fgtlen és $c_1,c_2\dots c_m$ gen. rszr V-ben. F–G egyenlőtlenség miatt $k\le m$. Ez fordítva is igaz: $k\ge m\Rightarrow k=m$

$\mathbb{R}^n$ dimenziója

A standard bázis létezése miatt egyértelmű, hogy $\dim\mathbb{R}^n=n$

Koordinátavektor egyértelműsége

A $V\le\mathbb{R}^n$ altérben $b_1,b_2\dots b_k$ vektorok bázist alkotnak $\Leftrightarrow \forall v\in V$ csak egyféleképp fejezhető ki b_i.

$\Leftarrow$: b_i
Mivel v kifejezhető $\Rightarrow b_1,b_2\dots b_k$ gen. rendszer
Ha $v=0$ akkor $\lambda_1=\lambda_2=\dots=\lambda_k=0$-val v kifejezhető, de mivel v csak egyértelműen fejezhető ki ezért $b_1,b_2\dots b_k$ lin. fgtlen $\Rightarrow$ bázis
$\Rightarrow$:
Tfh v kétféleképpen is kifejezhető
$\Rightarrow v=\lambda_1 b_1+\dots+\lambda_k b_k=\mu_1 b_1+\dots+\mu_k b_k$
$(\lambda_1-\mu_1)b_1+(\lambda_2-\mu_2)b_2+\dots+(\lambda_k-\mu_k)b_k=0$
Ekkor mivel $b_1,b_2\dots b_k$ lin fgtlen
$\lambda_1-\mu_1=\lambda_2-\mu_2=\dots=\lambda_k-\mu_k=0$
vagy $\lambda_1=\mu_1,\ \lambda_2=\mu_2\dots\lambda_k=\mu_k$
tehát a két kifejezés azonos.

Bázis létezése tetsz $\mathbb{R}^n$ altérben

Legyen $V\le\mathbb{R}^n$ altérben $f_1,f_2\dots f_k$ lin. fgtlen vektorok $\Rightarrow f_1,f_2\dots f_k$ kiegészíthető (esetleg nulla) véges sok vektorral, hogy az bázis legyen

Legyen $W=\langle f_1,f_2\dots f_k\rangle\Rightarrow W\subseteq V$
Ha $W=V\Rightarrow f_1,f_2\dots f_k$ gen rszr és bázis is.
Ha $W\neq V\Rightarrow\exists v\in V,\ v\notin W$. Ekkor $v,f_1,f_2\dots f_k$ lin. fgtlen, ellenkező esetben $v\in W$.
Ha $v,f_1,f_2\dots f_k$ gen rszr. V-ben akkor kész vagyunk, ha nem akkor folytatjuk.
Ez a folyamat egy ponton kell az $F\le G$ egyenlőtlenség miatt, mert $\mathbb{R}^n$-ben van n elemű gen rszr, így max n lin. fgtlen vektorból álló csoport lehet benne $\Rightarrow$ max $n-k$ lépés után megáll a folyamat

Transzponálás (10)

A $(k\times n)$-es A mátrix transzponáltjának nevezzük azt az $(n\times k)$-s B mátrixot, ha $b_{ij}=a_{ji}$ teljesül minden $1\le i\le n$ és $1\le j\le k$ esetén. Jele $B=A^T$

Ha az A és B mátrixokra $A\cdot B$ létezik $\Rightarrow B^T A^T$ is létezik, és $(A\cdot B)^T=A^T\cdot B^T$

Transzponált determinánsa

$\forall A$ négyzetes mátrixra $\det A^T=\det A$

Legyen A tetsz $(n\times n)$-es mátrix
B pedig legyen A^T
Legyen $\pi=(\pi_1,\pi_2\dots\pi_n)$ tetsz. perm

Ha A-ban a következő szorzat áll elő:
$(-1)^{I(\pi)}a_{1,\pi_1}\cdot a_{2,\pi_2}\cdot\ldots\cdot a_{n,\pi_n}$ ez B-ben előjel nélkül szintén megjelenik:
$b_{\pi_1,1}\cdot b_{\pi_2,2}\cdot\ldots\cdot b_{\pi_n,n}$
Legyen π' az a permutáció amiben az 1 a π_1. helyen a 2 a π_2 helyen … az n a π_n. helyen áll. Ekkor nevezzük π'-t π inverzének
A B elemiből írodott szorzat tehát:
$b_{1,\pi'_1}\cdot b_{2,\pi'_2}\cdot\ldots\cdot b_{n,\pi'_n}$ ami a $(-1)^{I(\pi')}$ előjelet kapja. Meg kell mutatnunk, hogy $I(\pi)=I(\pi')$
Legyen $\pi_i=k$ és $\pi'_j=l\Rightarrow\pi'_k=i$ és $\pi_l=j$
A k és l π-ben akkor állnak inverzióban, ha $i<j$ és $k>l\Rightarrow\pi'$-ben az i és j tagok állnak inverzióban, mert $k>l$
$\Rightarrow\pi$-ben π_i és π_j inverzióban állnak $\Leftrightarrow\pi'$-ben i és j állnak inverzióban
$\Rightarrow\pi$-beli inverziópárok kölcsönösen egyértelműen megfeleltethetőek π'-beli inverziópárokkal $\Rightarrow I(\pi)=I(\pi')$

Determinánsok szorzástétele

Bármely A és B $(n\times n)$-es mátrixra
$\det(A\cdot B)=\det A\cdot\det B$

Lin. egyenletrendszerek, $\mathbb{R}^n$-beli gen. altér és mátrixszorzásos mátrixegyenletek (11)

Legyenek $a_1,a_2\dots a_n,b\in\mathbb{R}^k$ vektorok és legyen A az a_i-k helyettesítésével keletkező $(k\times n)$-es mátrix $\Rightarrow$ (i),(ii),(iii) ekvivalensek
(i): Megoldható $A\cdot x=b$ mátrixegyenlet
(ii): Megoldható $(A|b)$ lin egyenletrszr
(iii): $b\in\langle a_1,a_2\dots a_n\rangle$

(iii) $\Rightarrow\lambda_1 a_1+\lambda_2 a_2+\dots+\lambda_n a_n=b$, i-t a vektorok i. koordinátája ($1\le i\le k$ esetén)
$a_{i,1}\lambda_1+a_{i,2}\lambda_2+\dots a_{i,n}\lambda_n=b_i$. ez épp az $(A|b)$ lin. egyenletrendszer.
Tehát (ii)$\Leftrightarrow$(iii)
Vegyük észre, h x csak $\mathbb{R}^n$-beli lehet. Ha x_j x j. koordinátája ($\forall\ 1\le j\le n$) $\Rightarrow a_{i,1}x_1+a_{i,2}x_2+\dots+a_{i,n}x_n=b_i$. Ezért $A\cdot x=b\Leftrightarrow(A|b)$
(i)$\Leftrightarrow$(ii)

Következmény:
(i) $A\cdot x=0$ egyetlen megoldása $x=0$
(ii) $a_1,a_2\dots a_n$ lin fgtlenek

Négyzetes mátrix det. és sorok/oszlopok lin fgtlensége közti kapcsolat

Legyen A $(n\times n)$-es mátrix
$\Rightarrow$ (i)$\Leftrightarrow$(ii)$\Leftrightarrow$(iii)
(i) A oszlopai lin fgtlenek
(ii) $\det A\neq 0$
(iii) A sorai lin fgtlenek

(i)$\Leftrightarrow Ax=0$ egyértelműen megoldható ez csak akkor, ha $\det A\neq 0\Rightarrow$(i)$\Leftrightarrow$(ii)
$|A|=|A^T|\Rightarrow$(ii)$\Leftrightarrow$(iii)

A rangfogalmak egyezősége (12)

$\forall$ mátrixra $\sigma(A)=s(A)=d(A)$

Elég belátni, hogy $\sigma(A)=d(A)$, mivel $s(A)=\sigma(A^T)$. Mivel $|A|=|A^T| \Rightarrow d(A)=d(A^T)$ (transzponálással nem változik meg a legnagyobb négyzetes részmátrix aminek a determinánsa nem nulla). Ha $\sigma(A)=d(A)$-t igaznak vesszük akkor $s(A)=\sigma(A^T)=d(A^T)=d(A)=\sigma(A)$

Először mutassuk meg, hogy $\sigma(A)\geq d(A)$

Tfh. $d(A)=r \Rightarrow$ kiválasztható egy $r\times r$-es nemnulla determinánsú részmátrix

Jelölje A_M azt a részmátrixot amiben a fent említett $r\times r$-es részmátrix A-beli megfelelői vannak ($(n\times r)$-es $\Rightarrow M$)

Tfh A_M oszlopai lin. öf. $\Rightarrow A_M\underline{x}=\underline{0}$-nak lenne egy $\underline{x}^*\neq\underline{0}$ megoldása. Akkor viszont $\underline{x}^*$ megoldása $M\cdot\underline{x}=\underline{0}$-nak is $\Rightarrow$ M oszlopai lin. öf $\Rightarrow |M|\neq 0$ (E) $\Rightarrow \sigma(A)\geq d(A)$

Lemma:

Legyen C $(k\times n)$-es mátrix melynek oszlopai lin fgtlenek. Ha $k>n \Rightarrow$ C sorai közül kiválasztható egy úgy, hogy azt elhagyva a kapott $(k-1)\times n$-es C' mátrix oszlopai szintén lin. fgtlenek

Legyenek C oszlopai $\underline{c}_1,\underline{c}_2\dots\underline{c}_n$ és $W=\{\underline{c}_1,\underline{c}_2\dots\underline{c}_n\}$. Mivel W-ben van n elemű gen. rsz. és $k>n$ ezért az F-G miatt nem lehet benne k elemű lin. fgtlen rsz. $\Rightarrow \mathbb{R}^k$-beli standard bázis vektorai közül van olyan amelyik nincs benne W-ben

Legyen ez $\underline{e}_j \Rightarrow$ C j. sora teljesíti a lemmát. Tfh nem $\Rightarrow C'\underline{x}=\underline{0}$-nak van egy $\underline{x}^*\neq\underline{0}$ megoldása. $\Rightarrow C\cdot\underline{x}^*\neq\underline{0}$ mert C oszlopai lin fgtlenek. $C\cdot\underline{x}^*$ csak abban különbözik $C'\underline{x}^*$-tól hogy azutóbbi kiegészül C j. sorának és $\underline{x}^*$-nak skaláris szorzatával. $\Rightarrow C\cdot\underline{x}^*$ j. sorának koordinátája $d\neq 0$ a többi pedig $0 \Rightarrow C\cdot(\frac{1}{d}\underline{x}^*)=\frac{1}{d}(C\cdot\underline{x}^*)=\underline{e}_j$. Ez ellentmond annak hogy $\underline{e}_j\notin W$

Most bizonyítsuk, hogy $r=\sigma(A)\leq d(A)$

Válasszunk A oszlopai közül r lin fgtlent alkossák ezek C mátrixát. Jelöljük A és C sorait k-val $\Rightarrow$ oszlopaik $\mathbb{R}^k$-beli vektorok $\Rightarrow k\geq r$. Szintén C-re a fenti lemma ismételt alkalmazásával eljutunk egy $r\times r$-es mátrixhoz ahol az oszlopok lin. fgtlenek $\Rightarrow \det C^*\neq 0 \Rightarrow d(A)\geq r$

$\Rightarrow \sigma(A)=d(A)$

Lin. lek. szorzata, szorzatmátrixa (13)

Legyenek $f:\mathbb{R}^n\to\mathbb{R}^k$ és $g:\mathbb{R}^k\to\mathbb{R}^m$ lin. lek. Akkor ezeknek a $g\circ f$ szorzata lin. lek. és $[g\circ f]=[g]\cdot[f]$

Legyen $[f]=A$ és $[g]=B \Rightarrow \forall\underline{x}\in\mathbb{R}^n$-re $f(\underline{x})=A\cdot\underline{x}$ és $\forall\underline{y}\in\mathbb{R}^k$-ra $f(\underline{y})=B\cdot\underline{y}$

Alkalmazzuk $g\circ f$ fgvt $\underline{x}\in\mathbb{R}^n$-re

$(g\circ f)(\underline{x})=g(f(\underline{x}))=g(A\cdot\underline{x})=B\cdot(A\cdot\underline{x})=(B\cdot A)\underline{x}$

The Rest II.

Következmények: addiciós tételek

Tetsz α és β szögekre

(i) $\sin(\alpha+\beta)=\sin\alpha\cos\beta+\cos\alpha\sin\beta$

(ii) $\cos(\alpha+\beta)=\cos\alpha\cos\beta+\sin\alpha\sin\beta$

Legyen $f_\alpha\ \mathbb{R}^2\to\mathbb{R}^2$ illetve $f_\beta\ \mathbb{R}^2\to\mathbb{R}^2$ síkban origó körüli α és β szöggel történő forgatás. Ezek lin. lek.-ek $f_\alpha\circ f_\beta$ azonos $f_{\alpha+\beta}$-val (origó körüli $\alpha+\beta$ szögű elforgatással)

$[f_{\alpha+\beta}]=[f_\alpha]\cdot[f_\beta]$

$[f_\beta]=\begin{pmatrix}\cos\beta & -\sin\beta\\ \sin\beta & \cos\beta\end{pmatrix}$

$[f]_\alpha=\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}\begin{pmatrix}\cos(\alpha+\beta) & -\sin(\alpha+\beta)\\ \sin(\alpha+\beta) & \cos(\alpha+\beta)\end{pmatrix}$

$\cos(\alpha+\beta)=\cos\alpha\cos\beta-\sin\alpha\sin\beta$

$\sin(\alpha+\beta)=\sin\alpha\cos\beta+\cos\alpha\sin\beta$

Lin. trf. invertálhatósága

Egy $f:\mathbb{R}^n\to\mathbb{R}^n$ lin. trfó invertálható $\Leftrightarrow \det[f]\neq 0$, ha ez igaz $\Rightarrow [f^{-1}]=[f]^{-1}$

Legyen $[f]=A$ vagyis $f(\underline{x})=A\cdot\underline{x}$ $\forall x\in\mathbb{R}^n$-re.

Ha f invertálható $\Rightarrow \det A\neq 0$. Tfh $\det A=0 \Rightarrow$ A oszlopai lin. öf. ami $\Rightarrow A\cdot\underline{x}=\underline{0}$-nak van $\underline{x}^*\neq 0$ megoldása $\Rightarrow$ f nem invertálható mert $f(\underline{x}^*)=f(\underline{0})$

Ha $\det A\neq 0 \Rightarrow$ f invertálható:

$\det A\neq 0 \Rightarrow \exists A^{-1} \Rightarrow f(\underline{x})=\underline{y}$ esetén

$\underline{y}=A\cdot\underline{x}$ $\quad /\cdot\to A^{-1}$

$A^{-1}\cdot\underline{y}=A^{-1}\cdot A\cdot\underline{x}=E\cdot\underline{x}=\underline{x} \Rightarrow f^{-1}\ \exists$ és $[f^{-1}]=A^{-1}=[f]^{-1}$

Magtér, képtér altér volta (14)

Ha $f:\mathbb{R}^n\to\mathbb{R}^k$ lin. lek $\Rightarrow$

(i) $\operatorname{Ker} f\leq\mathbb{R}^n$

(ii) $\operatorname{Im} f\leq\mathbb{R}^k$

Meg kell mutatni, hogy bármely $\underline{x}_1,\underline{x}_2\in\operatorname{Ker} f$ és $\lambda\in\mathbb{R}$ esetén $\underline{x}_1+\underline{x}_2\in\operatorname{Ker} f$ és $\lambda\underline{x}_1\in\operatorname{Ker} f$.

Ha $\underline{x}_1,\underline{x}_2\in\operatorname{Ker} f \Rightarrow f(\underline{x}_1)=f(\underline{x}_2)=\underline{0}$

$f(\underline{x}_1+\underline{x}_2)=f(\underline{x}_1)+f(\underline{x}_2)=\underline{0}+\underline{0}=\underline{0}$

$f(\lambda\underline{x}_1)=\lambda\cdot f(\underline{x}_1)=\lambda\cdot\underline{0}=\underline{0}$

Ugyanezt kell belátni $\operatorname{Im} f$-re

$[f]=A \Rightarrow A\cdot\underline{x}=\underline{y} \Rightarrow \underline{y}\in\langle\underline{a}_1,\underline{a}_2\dots\underline{a}_n\rangle$ ami altér.

Dimenziótétel

Ha $f:\mathbb{R}^n\mapsto\mathbb{R}^k$ lin. lek. $\Rightarrow \dim\operatorname{Ker} f+\dim\operatorname{Im} f=n$.

Legyen $\dim\operatorname{Ker} f=m$ és válasszunk egy tetsz. bázist $\operatorname{Ker} f$-ben. Legyen ez a bázis $\underline{b}_1,\underline{b}_2\dots\underline{b}_m$, akkor ez kiegészíthető $n-m$ db vektorral úgy, h az bázis legyen $\mathbb{R}^n$-ben. Mutassuk meg, hogy $f(\underline{c}_1), f(\underline{c}_2),\dots f(\underline{c}_{n-m})$ bázis $\operatorname{Im} f$-ben. Ebből következik a tétel állítása

Lássuk be, hogy $f(\underline{c}_1), f(\underline{c}_2)\dots f(\underline{c}_{n-m})$ gen. rsz. $\operatorname{Im} f$-ben. Legyen $\underline{y}\in\operatorname{Im} f \Rightarrow \underline{y}=f(\underline{x})$. Mivel $\underline{b}_1\dots\underline{b}_m,\underline{c}_1\dots\underline{c}_{n-m}$ gen. rsz. $\mathbb{R}^n$ ezért

$\underline{x}=\beta_1\underline{b}_1+\dots+\beta_m\underline{b}_m+\gamma_1\underline{c}_1+\dots+\gamma_{n-m}\underline{c}_{n-m}$

$\underline{y}=f(\underline{x})=f(\beta_1\underline{b}_1+\dots+\beta_m\underline{b}_m+\gamma_1\underline{c}_1+\dots+\gamma_{n-m}\underline{c}_{n-m})=$

$=f(\beta_1\underline{b}_1)+\dots+f(\beta_m\underline{b}_m)+f(\gamma_1\underline{c}_1)+\dots+f(\gamma_{n-m}\underline{c}_{n-m})=$

$=\beta_1 f(\underline{b}_1)+\dots+\beta_m f(\underline{b}_m)+\gamma_1 f(\underline{c}_1)+\dots+\gamma_{n-m} f(\underline{c}_{n-m})=$

$=\gamma_1 f(\underline{c}_1)+\dots+\gamma_{n-m} f(\underline{c}_{n-m}) \Rightarrow$ tetsz $\underline{y}\in\operatorname{Im} f$ kifejezhető $f(\underline{c}_1), f(\underline{c}_2)\dots f(\underline{c}_{n-m})$ tehát gen. rsz.

Most belátjuk h $f(\underline{c}_1), f(\underline{c}_2)\dots f(\underline{c}_{n-m})$ lin fgtlen.

Tfh $\gamma_1 f(\underline{c}_1)+\dots+\gamma_{n-m} f(\underline{c}_{n-m})=\underline{0} \Leftrightarrow \gamma_1=\dots=\gamma_{n-m}=0$

$\underline{0}=\gamma_1 f(\underline{c}_1)+\dots+\gamma_{n-m} f(\underline{c}_{n-m})=f(\gamma_1\underline{c}_1)+\dots+f(\gamma_{n-m}\underline{c}_{n-m})=f(\gamma_1\underline{c}_1+\dots+\gamma_{n-m}\underline{c}_{n-m}) \Rightarrow$

$\gamma_1\underline{c}_1+\dots+\gamma_{n-m}\underline{c}_{n-m}\in\operatorname{Ker} f \Rightarrow$

$\gamma_1\underline{c}_1+\dots+\gamma_{n-m}\underline{c}_{n-m}\in\langle\underline{b}_1,\dots\underline{b}_m\rangle$

$\Rightarrow \gamma_1\underline{c}_1+\dots\gamma_{n-m}\underline{c}_{n-m}=\beta_1\underline{b}_1+\dots\beta_m\underline{b}_m$

$-\beta_1\underline{b}_1-\dots-\beta_m\underline{b}_m+\gamma_1\underline{c}_1+\dots+\gamma_{n-m}\underline{c}_{n-m}=\underline{0}$

De $\underline{b}_1\dots\underline{b}_m,\underline{c}_1\dots\underline{c}_{n-m}$ lin fgtlen mert bázis $\Rightarrow \beta_1=\dots=\beta_m=\gamma_1=\dots=\gamma_{n-m}=0$

$\Rightarrow f(\underline{c}_1)\dots f(\underline{c}_{n-m})$ lin fgtlen.

Bázistranszformáció (15)

Egy lineáris leképezés melynek eredményeként egy adott ~~koordináta~~ pont másik bázis beli koordinátáit kapjuk

Lin trafó mátrixa adott bázis szerint

Legyen $f:\mathbb{R}^n\to\mathbb{R}^n$ lin. trafó, és B egy $(n\times n)$-es mátrix amelynek az oszlopai bázist alkotnak $\mathbb{R}^n$-ben. Jelölje $g:\mathbb{R}^n\to\mathbb{R}^n$ azt a függvényt amely $\forall\underline{x}\in\mathbb{R}^n$ esetén $[\underline{x}]_B$-hez $[f(\underline{x})]_B$-t rendeli. Akkor g is lin. trafó és $[g]=B^{-1}\cdot[f]\cdot B$

Vegyük észre, hogy B oszlopai bázist alkotnak $\Leftrightarrow \det B\neq 0$. $\mathbb{R}^n$ bázisai n tagú lin fgtlen rendszerek $\Rightarrow \det B\neq 0 \Rightarrow B^{-1}\ \exists$.

Lemma:

Legyen $h:\mathbb{R}^n\to\mathbb{R}^n$ az a fgv, mely minden $\underline{x}\in\mathbb{R}^n$ esetén $[\underline{x}]_B$-hez $\underline{x}$-et rendeli. Akkor h lin. trafó, melynek mátrixa $[h]=B$

Jelölje $\underline{x}\in\mathbb{R}^n$-re az $[\underline{x}]_B$ i. koordinátáját $\alpha_i \Rightarrow \underline{x}=\alpha_1\underline{b}_1+\dots+\alpha_n\underline{b}_n$. Ez ekvivalens $\underline{x}=B\cdot[\underline{x}]_B$-vel $\Rightarrow$ h lin. trafó s mátrixa B

Mivel $\det B\neq 0 \Rightarrow [h^{-1}]\ \exists$ és mátrixa $[h^{-1}]=[h]^{-1}=B^{-1}$, ez nyilván $\forall\underline{x}$-hez $[\underline{x}]_B$-t rendeli

g azonos a $h^{-1}\circ f\circ h$ fgv-el így

$[g]=[h^{-1}]\cdot[f]\cdot[h]=B^{-1}\cdot[f]\cdot B$

Karakterisztikus polinom (16)

Az $(n\times n)$-es A mátrix karakterisztikus polinomjának nevezzük a $\det(A-\lambda E)$ determináns értékét, ahol λ változó. Ennek a jele: $k_A(\lambda)$

Sg sg diagonalitás

Legyen $f:\mathbb{R}^n\to\mathbb{R}^n$ lin. trafó és $B=\{\underline{b}_1,\underline{b}_2\dots\underline{b}_n\}$ bázis $\mathbb{R}^n$-ben. Akkor $[f]_B$ diagonális $\Leftrightarrow$ B minden eleme sajátvektora $[f]$

$[f]_B$ pontosan akkor diagonális ha minden $1\leq i\leq n$ esetén i. oszlopa

egyenlő $\lambda_i \cdot \underline{b}_i$-vel $\Rightarrow [f(\underline{b}_i)]_B = \lambda_i \underline{b}_i \Rightarrow$
$f(\underline{b}_i) = 0 \cdot \underline{b}_1 + \ldots + 0 \cdot \underline{b}_{i-1} + \lambda_i \underline{b}_i + 0 \cdot \underline{b}_{i+1} + \ldots + 0 \cdot \underline{b}_n$
$\Rightarrow [f] \cdot \underline{b}_i = \lambda \cdot \underline{b}_i \Rightarrow \underline{b}_i$ saját vektora $[f]$-nek