

Sidste gang:

Kinesiske Restklasse-Sætning (KRS)

Lad $m_1, \dots, m_n \in \mathbb{Z}$

$a_1, \dots, a_n \in \mathbb{Z}$

$$m = m_1 \cdot \dots \cdot m_n$$

Hvis $m_1, \dots, m_n$ er parvis indbyrdes primiske, da har

$$x \equiv a_1 \pmod{m_1}$$

$\vdots$

$$x \equiv a_n \pmod{m_n}$$

en unik løsning modulo m

Der kan godt være en løsning, selvom m_i 'erne ikke er parvis indbyrdes primiske, men metoder fra beviset for KRS kan ikke bruges.

Fermats Lille Sætning

Lad $a, p \in \mathbb{Z}$, p primtal

$$(1) \quad p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

$$(2) \quad a^p \equiv a \pmod{p}$$

Afsnit 4.3, s. 266 : Euklids Algoritme

$$\gcd(287, 91) = ?$$

$$287 = 91 \cdot 3 + 14$$

$$91 = 14 \cdot 6 + \textcircled{7}$$

$$14 = 7 \cdot 2 + 0$$

$$\gcd(287, 91) = 7$$

$$\text{Check: } 91 = 7 \cdot 13$$

$$287 = 7 \cdot 41$$

Hvorfør virker det?

Lemma 1:

Hvis $a = bq + r$, hvor $a, b, q, r \in \mathbb{Z}$,
da er $\gcd(a, b) = \gcd(b, r)$.

Bevis:

Vil vise, at $\gcd(a, b) = \gcd(b, r)$.

(dvs a og b har de samme divisorer til fælles
som b og r)

$$\gcd(b, r) \leq \gcd(a, b):$$

$$\begin{aligned} d \mid b \wedge d \mid r &\Rightarrow d \mid (qb + r), \text{ ifølge Kor. 4.1.1} \\ &\Leftrightarrow d \mid a \end{aligned}$$

$$\gcd(a, b) \leq \gcd(b, r):$$

$$\begin{aligned} d \mid a \wedge d \mid b &\Rightarrow d \mid (a - qb), \text{ ————— " —————} \\ &\Leftrightarrow d \mid r \end{aligned}$$

□

Ifølge Lemma 1 betyder udregningene ovenfor, at

$$\begin{aligned}\gcd(287, 91) &= \gcd(91, 14) = \gcd(14, 7) \\ &= \gcd(7, 0) = 7\end{aligned}$$

Ved at regne baglæns, kan man skrive $\gcd(a, b)$ som linear-kombination af a og b . (Sætning 6)

I eks. ovenfor:

$$\begin{aligned}7 &= 91 - 14 \cdot 6 \\ &= 91 - (287 - 3 \cdot 91) \cdot 6 \\ &= 91 - 6 \cdot 287 + 18 \cdot 91 \\ &= 19 \cdot 91 - 6 \cdot 287\end{aligned}$$

Hvornår kunne vi være interesserede i det?

Hvis vi f.eks. gerne vil finde en multiplikativ invers:

$$a\bar{a} \equiv 1 \pmod{m}$$

$\bar{a}$ eksisterer, hvis $\gcd(a, m) = 1$

$$1 = sa + tm, \quad s, t \in \mathbb{Z} \quad \Rightarrow$$

$$1 \equiv sa \pmod{m}$$

Euklids Udvidede Algoritme beregner både $\gcd(a, b)$, s og t . Mere om det i DM534...

Matricer (afsnit 2.6)

$$A = \begin{bmatrix} 2 & 3 & 4 \\ 1 & 0 & 2 \end{bmatrix} \quad \begin{array}{l} 2 \text{ rækker} \\ 3 \text{ søjler} \end{array}$$

A er en 2×3 -matrix

Matrix-regning kan bruges til at løse ligningssystemer med flere ubekendte.

Bruges også til computergrafik og meget andet.

I skal bruge dem i DM534 om en måned.

Vi kommer også til at bruge dem i forbindelse med relationer

Vi skal se på, hvordan man kan manipulere matricer:
addere, gange, transponere

Addition

$$B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix}$$

$$C = A + B = \begin{bmatrix} 2+1 & 3+1 & 4+0 \\ 1+0 & 0+1 & 2+0 \end{bmatrix} = \begin{bmatrix} 3 & 4 & 4 \\ 1 & 1 & 2 \end{bmatrix}$$

$$c_{ij} = a_{ij} + b_{ij} \quad (\text{Def. 3})$$

A og B kan lægges sammen, fordi de har samme dimensioner, men de kan ikke ganges.

Multiplikation:

$$D = \begin{bmatrix} 1 & 2 & 0 \\ 1 & 1 & 1 \\ 2 & 0 & 1 \end{bmatrix} \quad 3 \times 3 \text{ matrix}$$

$$\begin{aligned} A \cdot D &= \begin{bmatrix} 2 \cdot 1 + 3 \cdot 1 + 4 \cdot 2 & 2 \cdot 2 + 3 \cdot 1 + 4 \cdot 0 & 2 \cdot 0 + 3 \cdot 1 + 4 \cdot 1 \\ 1 \cdot 1 + 1 \cdot 0 + 2 \cdot 2 & 1 \cdot 2 + 0 \cdot 1 + 2 \cdot 0 & 1 \cdot 0 + 0 \cdot 1 + 2 \cdot 1 \end{bmatrix} \\ &= \begin{bmatrix} 13 & 7 & 7 \\ 5 & 2 & 2 \end{bmatrix} = E \quad 2 \times 3 \text{ - matrix} \end{aligned}$$

$$e_{ij} = a_{i1}d_{1j} + a_{i2}d_{2j} + a_{i3}d_{3j} = \sum_{k=1}^3 a_{ik}d_{kj}$$

Generelt:

$$\begin{matrix} k & \boxed{F} & \times & \boxed{G} & = & k & \boxed{H} \\ & \textcircled{m} & & \textcircled{m} & & & \textcircled{m} \\ & n & & n & & & n \end{matrix}$$

$$h_{ij} = \sum_{k=1}^m f_{ik} g_{kj} \quad (\text{Def. 4}) \quad - \quad m \text{ mult.}$$

H har $k \cdot n$ pladser
D.v.s. ialt $k \cdot m \cdot n$ mult.

D.A er ikke defineret:

$$\begin{bmatrix} 1 & 2 & 0 \\ 1 & 1 & 1 \\ 2 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 3 & 4 \\ 1 & 0 & 2 \end{bmatrix}$$

A.A er heller ikke defineret.

Mw det er D.D, for D er kvadratisk,
d.v.s. $\# \text{rækker} = \# \text{søjler}$ (Def. 1)

Eks 1':

$$X = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad Y = \begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix}$$

$$X \cdot Y = \begin{bmatrix} 2+1 & 0+1 \\ 0+1 & 0+1 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix} \neq$$

$$Y \cdot X = \begin{bmatrix} 2+0 & 2+0 \\ 1+0 & 1+1 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix}$$

D.v.s. matrix-mult. er ikke kommutativ.

Gælder der så heller ikke, at

$$D \cdot D^2 = D^2 \cdot D \quad ?$$

Jo, for matrix-mult. er associativ:

$$(M_1 \cdot M_2) \cdot M_3 = M_1 \cdot (M_2 \cdot M_3)$$

Neutrale matricer

$$A + O = A$$

$$O = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Neutral matrix m.h.t. + :

$$m_{ij} = 0$$

$$A \cdot \mathbb{I}_3 = A :$$

$$\begin{bmatrix} 2 & 3 & 4 \\ 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 4 \\ 1 & 0 & 2 \end{bmatrix}$$

Den neutrale matrices dimensioner ligger fast:

- Med antallet af rækker sørger vi for, at den kan ganges på A .
- Med antallet af søjler sørger vi for, at resultatet har det rigtige antal søjler.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 3 & 4 \\ 1 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 4 \\ 1 & 0 & 2 \end{bmatrix}$$

$$\mathbb{I}_2 \cdot A = A$$

Neutral matrix m.h.t. $\cdot$:

$$m_{ii} = 1$$

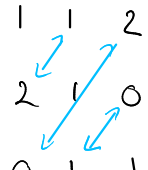
$$m_{ij} = 0, \quad i \neq j$$

Kaldes også en identitetsmatrix (Def. 5)

Transponering

$$A^t = \begin{bmatrix} 2 & 1 \\ 3 & 0 \\ 4 & 2 \end{bmatrix}$$

Byt om på rækker og søjler: $m_{ij}^t = m_{ji}$ (Def. 6)

$$D^t = \begin{bmatrix} 1 & 1 & 2 \\ 2 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$


Kvadratiske matrixer: spejl omkring diagonalen

Hvis $M = M^t$, er M symmetrisk (Def. 7)