

Sidste gang

Afsnit 4.3:

$$\gcd(a,b) \cdot \text{lcm}(a,b) = a \cdot b$$

Euklids (udvidede) Algoritme

Dividere på begge sider af en kongruens

$$\gcd(c,m)=1 \Downarrow \begin{matrix} ac \equiv bc \pmod{m} \\ a \equiv b \pmod{m} \end{matrix} \quad (\text{Sætning 4.3.7})$$

Multiplikativ invers

$$\Updownarrow \begin{matrix} \exists \bar{a} : \bar{a}a \equiv 1 \pmod{m} \\ \gcd(a,m)=1 \end{matrix}$$

$\bar{a}$ kan findes v.h.a. Euklids Udvidede Alg.

Eks: $a=4, m=11$

$$11 = 4 \cdot 2 + 3 \quad (*)$$

$$4 = 3 \cdot 1 + 1 \quad (**)$$

D.v.s.

$$1 \stackrel{(***)}{=} 4 - 3 \stackrel{(*)}{=} 4 - (11 - 4 \cdot 2) = 4 \cdot 3 - 11$$

$$\Downarrow 4 \cdot 3 \equiv 1 \pmod{11}$$

Afsnit 4.4:

Lineære kongruenser

$$\begin{aligned} \gcd(a, m) = 1 & \iff ax \equiv b \pmod{m} \\ & \iff \bar{a}ax \equiv \bar{a}b \pmod{m} \\ & \iff x \equiv \bar{a}b \pmod{m} \end{aligned}$$

↑ følger af
Sætning 4.3.7, da
a mult. invers
til $\bar{a}$ modulo m
⇓
 $\gcd(\bar{a}, m) = 1$

$$\begin{aligned} \text{Eks: } 4x &\equiv 5 \pmod{11} \\ \iff 3 \cdot 4x &\equiv 3 \cdot 5 \pmod{11} \\ \iff x &\equiv 15 \pmod{11} \\ \iff x &\equiv 4 \pmod{11} \end{aligned}$$

Kongruenssystemer

(afsnit 4.4)

Eks:

$$x \equiv 2 \pmod{3} \quad 2, 5, 8, 11, 14, 17, 20, 23, 26, \dots$$

$$x \equiv 3 \pmod{5} \quad 3, 8, 13, 18, 23, 28, 33, \dots$$

$$x \equiv 2 \pmod{7} \quad 2, 9, 16, 23, \dots$$

$x=23$ er en løsning

Men findes der en nemmere løsningsmetode?

Lad $x = 2 \cdot b_1 + 3 \cdot b_2 + 2 \cdot b_3$, hvor

$$b_1 \equiv \begin{cases} 1 \pmod{3} \\ 0 \pmod{5} \\ 0 \pmod{7} \end{cases}$$

$$b_2 \equiv \begin{cases} 0 \pmod{3} \\ 1 \pmod{5} \\ 0 \pmod{7} \end{cases}$$

$$b_3 \equiv \begin{cases} 0 \pmod{3} \\ 0 \pmod{5} \\ 1 \pmod{7} \end{cases}$$

Da er

$$x \equiv \begin{cases} 2 \cdot 1 + 0 + 0 \pmod{3} \\ 0 + 3 \cdot 1 + 0 \pmod{5} \\ 0 + 0 + 2 \cdot 1 \pmod{7} \end{cases}$$

Men findes b_1, b_2 og b_3 ??

Ja (fordi 3, 5 og 7 er parvis indbyrdes primiske):

Sætning 4.4.2 (Kinesiske Restklasse-Sætning)

Hvis

$$a_1, a_2, \dots, a_n \in \mathbb{Z},$$

$m_1, m_2, \dots, m_n \in \mathbb{Z}^+ \setminus \{1\}$ er parvis indbyrdes primiske, og

$$m = m_1 \cdot m_2 \cdot \dots \cdot m_n$$

Da har

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

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

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

en unik løsning modulo m (d.v.s. $\exists!$ løsning i $\mathbb{Z}_m$)

Beweis:

Eksisterer: Konstruktivt bevis:

Ide: Lad $x = \sum_{k=1}^n b_k a_k$, hvor

$$b_k \equiv \begin{cases} 0 & \pmod{m_i}, \text{ for } i \neq k \\ 1 & \pmod{m_k} \end{cases}$$

Lad $M_k = \frac{m}{m_k} = m_1 \cdot m_2 \cdots m_{k-1} \cdot m_{k+1} \cdots m_n$

Da gælder

- $M_k \equiv 0 \pmod{m_i}$, for $i \neq k$
- $\gcd(M_k, m_k) = 1$, da m_k ikke har nogen divisorer til fælles med nogen af de andre m_i 'er.

D.v.s. ifølge Sætn. 4.4.1 findes der et $y_k \in \mathbb{Z}$, så

$$M_k y_k \equiv 1 \pmod{m_k}$$

D.v.s. vi kan vælge $b_k = M_k y_k$,

hvor y_k er en multiplikativ invers til M_k modulo m_k

D.v.s.

$$x = \sum_{k=1}^n \overbrace{M_k y_k}^{b_k} a_k, \text{ hvor } M_k y_k \equiv 1 \pmod{m_k},$$

er en løsning til kongruenssystemet

Unik modulo m :

Opgave 29 og 30



Bemærk, at

$$x + km \equiv x \pmod{m_i}, \quad 1 \leq i \leq n,$$

da $m_i | m$, $1 \leq i \leq n$

O.v.s.

Løsningsmetode:

For $1 \leq k \leq n$

$$\text{Beregn } M_k = \frac{m}{m_k}$$

$$\text{Find } y_k, \text{ så } M_k y_k \equiv 1 \pmod{m_k}$$

$$\text{Beregn } x = \sum_{k=1}^n M_k y_k a_k$$

F.eks. o.h.a.
Euklids Udvidede
Algoritme

Løsningsmængde: $\{x + km \mid k \in \mathbb{Z}\}$

OBS: Hvis $m_1, \dots, m_n$ ikke er parvis indbyrdes primiske, kan der godt være en løsning, men man kan ikke bruge ovenstående metode (hvorfor ikke?)

Eks fra før:

$$m = 3 \cdot 5 \cdot 7 = 105$$

$$M_1 = 5 \cdot 7 = 35$$

$$M_2 = 3 \cdot 7 = 21$$

$$M_3 = 3 \cdot 5 = 15$$

$$\begin{aligned} & \Updownarrow M_1 y_1 \equiv 1 \pmod{m_1} \\ & \Updownarrow 35 y_1 \equiv 1 \pmod{3} \\ & \Updownarrow y_1 = 2 \end{aligned}$$

$$\begin{aligned} & \Updownarrow M_2 y_2 \equiv 1 \pmod{m_2} \\ & \Updownarrow 21 y_2 \equiv 1 \pmod{5} \\ & \Updownarrow y_2 = 1 \end{aligned}$$

$$\begin{aligned} & \Updownarrow M_3 y_3 \equiv 1 \pmod{m_3} \\ & \Updownarrow 15 y_3 \equiv 1 \pmod{7} \\ & \Updownarrow y_3 = 1 \end{aligned}$$

D.v.s.

$$\begin{aligned} x &= M_1 y_1 a_1 + M_2 y_2 a_2 + M_3 y_3 a_3 \\ &= 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 \\ &= 233 \\ &= 2 \cdot 105 + 23 \end{aligned}$$

D.v.s.

$$\begin{aligned} \text{Løsningsmængde: } & \{ 23 + 105c \mid c \in \mathbb{Z} \} = \\ & \{ \dots, -187, -82, 23, 128, 233, \dots \} \end{aligned}$$

Fermats lille Sætning (1) kan sammen med KRS bruges til at bevise, at RSA virker.
Den kan desuden være nyttig i modulo-beregninger.

Fermats lille Sætning (Sætning 4.4.3)

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

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

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

Eks 9: Beregn $7^{222} \pmod{11}$

11 er et primtal, og $11 \nmid 7$
D.v.s. vi kan bruge Sætning 4.4.3 (1):

$$7^{10} \equiv 1 \pmod{11} \quad (*)$$

D.v.s.

$$\begin{aligned} 7^{222} &= 7^{22 \cdot 10 + 2} = (7^{10})^{22} \cdot 7^2 \\ \Downarrow \\ 7^{222} \pmod{11} &= 1^{22} \cdot 7^2 \pmod{11}, \text{ ifølge } (*) \text{ og Kor. 4.1.2} \\ &= 49 \pmod{11} \\ &= \underline{\underline{5}} \end{aligned}$$

Matricer (afsnit 2.6)

Vi har allerede brugt matricer til at repr. relationer. Datalogerne har set matricer i DM534, og kommer til at se dem igen.

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

Bruges desuden til computergrafik og meget andet.

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

Desuden skal vi se, at matricer kan være kvadratiske og symmetriske, og vi skal se på neutrale matricer m.h.t. addition og multiplikation.

Eks:

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

3 søjler

A er en 2×3 -matrix

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}$$

Addition

Eks:

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

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

$$c_{ij} = a_{ij} + b_{ij} \quad (\text{Def. 2.6.3})$$

A og B kan adderes, fordi de har samme dimensioner.
Men de kan ikke ganges...

Multiplikation

Eks:

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

2 × 3

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

3 × 3

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

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

Når man skal gange matrixer sammen, kan det være bekvemt at skrive dem forskudt:

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

$$\begin{bmatrix} 2 & 3 & 4 \\ 1 & 0 & 2 \end{bmatrix} \quad \begin{bmatrix} 13 & 7 & 7 \\ 5 & 2 & 2 \end{bmatrix}$$

Generelt:

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

$$h_{ij} = \sum_{l=1}^m \underbrace{f_{il} g_{lj}}_{m \text{ mult.}} \quad (\text{Def. 2.6.4})$$

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

Eks:

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

Men det er D.D, for D er kvadratisk,
d.v.s. #rækker = #søjler (Def. 2.6.1)

„Eks 4“: Matrix mult. er ikke kommutativ:

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

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

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

Matrix-mult. er assosiativ:

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