

Sidste gang:

Euklids Algoritme

Eks:

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

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

D.v.s.

$$\gcd(11, 4) = 1, \text{ og}$$

$$\begin{aligned} 1 &\stackrel{(ii)}{=} 4 - 3 \stackrel{(i)}{=} 4 - (11 - 4 \cdot 2) = 4 \cdot 3 - 11 \\ \Leftrightarrow 4 \cdot 3 &\equiv 1 \pmod{11} \end{aligned}$$

D.v.s.

3 er multiplikativt invers til 4 modulo 11
(og omvendt).

$$\begin{aligned} \Leftrightarrow \exists \bar{a} \in \mathbb{Z} : \bar{a}a &\equiv 1 \pmod{m} \\ \gcd(a, m) &= 1 \end{aligned}$$

(Sætning 4.4.1 + opgave 4.4.8)

Lineære kongruenser

Eks:

$$\Leftrightarrow 4x \equiv 5 \pmod{11}$$

$$\Leftrightarrow 3 \cdot 4x \equiv 3 \cdot 5 \pmod{11} \quad \Leftrightarrow \text{følge af Sætning 4.3.7}$$

$$\Leftrightarrow x \equiv 4 \pmod{11}$$

D.v.s.

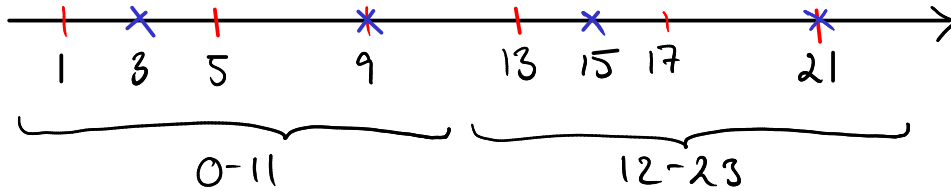
Løsningsmængde: $\{4 + 11k \mid k \in \mathbb{Z}\}$

Kongruensystemer

Eks:

$$x \equiv 1 \pmod{4}$$

$$x \equiv 3 \pmod{6}$$



Eks:

$$\begin{array}{ll} x \equiv 2 \pmod{3} & a_1=2, m_1=3, M_1=5 \cdot 7=35, y_1=2 \\ x \equiv 3 \pmod{5} & a_2=3, m_2=5, M_2=3 \cdot 7=21, y_2=1 \\ x \equiv 2 \pmod{7} & a_3=2, m_3=7, M_3=3 \cdot 5=15, y_3=1 \\ & m=3 \cdot 5 \cdot 7=105 \end{array}$$

$$\Downarrow \quad x = 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233 \equiv 23 \pmod{105}$$

$$\left\{ \begin{array}{ll} x \equiv 2 \cdot 1 + 3 \cdot 0 + 2 \cdot 0 & \pmod{3} \\ x \equiv 2 \cdot 0 + 3 \cdot 1 + 2 \cdot 0 & \pmod{5} \\ x \equiv 2 \cdot 0 + 3 \cdot 0 + 2 \cdot 1 & \pmod{7} \end{array} \right.$$

$$b_1 = M_1 y_1 = 70$$

$$b_2 = M_2 y_2 = 21$$

$$b_3 = M_3 y_3 = 15$$

Sætning 4.4.2 (Kinesiske Restklasse-Sætning)

Hvis

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

$m_1, m_2, \dots, m_n \in \mathbb{Z}$ 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 $\mathbb{Z}_m$)

NB: Der kan godt være en løsning, selvom m_i 'erne ikke er parvis indbyrdes primiske, jvf. vores andet eksempel.

Bevis:

Eksisterer: Konstruktivt bevis:

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

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

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 $i \neq k$

D.v.s. for ethvert $y_k \in \mathbb{Z}$ gælder

$$M_k y_k \equiv 0 \pmod{m_i}, \text{ for } i \neq k$$

Så skal vi bare vælge y_k sådan,
at $M_k y_k \equiv 1 \pmod{m_k}$, og det er muligt:

- $\gcd(M_k, m_k) = 1$, 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

□

O.v.s.

Løsningsmetode:

For $1 \leq k \leq n$

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

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

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

F.eks. v.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 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.

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

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 4.4.1(1) med $a=7$, $p=11$:

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

D.v.s.

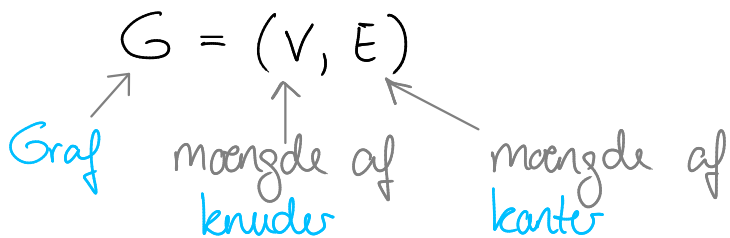
$$\begin{aligned} \Downarrow \quad 7^{222} &= 7^{22 \cdot 10 + 2} = (7^{10})^{22} \cdot 7^2 \\ \Downarrow \quad 7^{222} \pmod{11} &= 1^{22} \cdot 7^2 \pmod{11}, \text{ ifølge } (*) \text{ og Kor. 4.1.2} \\ &= 49 \pmod{11} \\ &= 5 \end{aligned}$$

Grafer Kapitel 10

Graftyper (Afsnit 10.1)

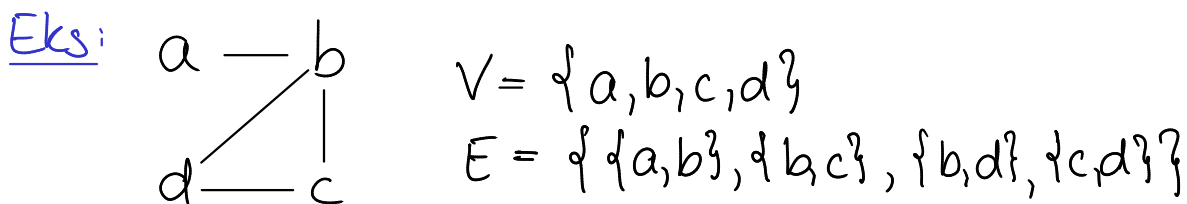
Simple grafer

D.v.s. hverken parallelle kanter eller loops.



Ikke-orienterede grafer:

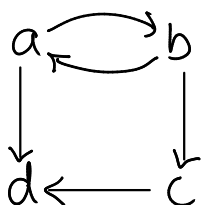
Kantene er uordnede par.



Orienterede grafer

Kantene er ordnede par af knuder.

Eks:



$$V = \{a, b, c, d\}$$

$$E = \{(a, b), (a, d), (b, a), (b, c), (c, d)\}$$

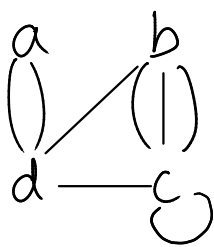
Multigrafer

D.v.s. parallelle kanter og/eller loops.

$$G = (V, E)$$

↑
multimængde

Eks: Ikke-orienteret multigraf



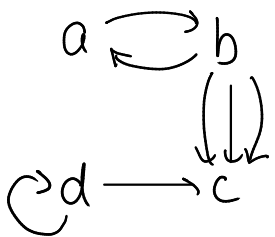
$$V = \{a, b, c, d\}$$

$$E = \{ \{a, d\}, \{a, d\}, \{b, c\}, \{b, c\}, \{b, c\}, \{b, d\}, \{c, c\}, \{c, d\} \}$$

Bogen skelner mellem

- multigrafer (ingen loops)
- pseudografer (loops og evt. parallelle kanter)

Eks: Orienteret multigraf

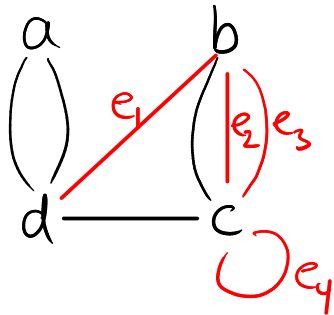


$$V = \{a, b, c, d\}$$

$$E = \{ (a, b), (a, b), (b, c), (b, c), (b, c), (d, c), (d, d) \}$$

Terminologi og grafklasser (Afsnit 10.2)

Ex: Ikke-orienterede grafer



e_1 forbinder b og d / er incident med b og d / har endepunkterne b og d .

b og d er naboer / adjacente.

e_1 og e_2 er adjacente, fordi de har ét fælles endepunkt.

e_2 og e_3 er parallelle, fordi de deler begge endepunkter.

$N(b) = \{c, d\}$ er b 's nabomængde (neighborhood)
 $N(\{b, d\}) = N(b) \cup N(d) = \{c, d\} \cup \{a, b, c\} = \{a, b, c, d\}.$

Graden af a er $\deg(a) = 2$, da to kanter er incidente til a .

$$\deg(b) = \deg(d) = 4$$

$$\deg(c) = 6 \text{ (begge } e_i\text{'s ender bidrager til } \deg(c)\text{)}$$

$$\boxed{\sum_{x \in V} \deg(x) = \deg(a) + \deg(b) + \deg(c) + \deg(d)}$$
$$= 2 + 4 + 6 + 4 = 16 = 2 \cdot |E|$$

↑

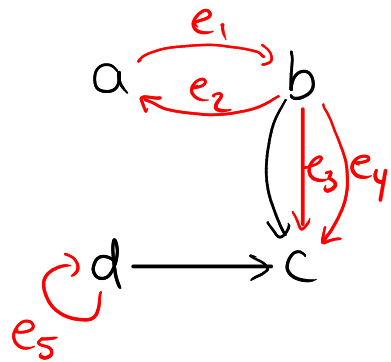
Håndtryks-Sætningen (Sætning 10.2.1)

Håndtryks-Sætningen medfører:

Sætning 10.2.2: Enhver ikke-orienteret graf har et lige #knuder med ulige grad.

Eks: Orienterede grafer

e_1 og e_2 er antiparallelle



e_3 og e_4 er parallelle

e_1 har startknode a og slutknode b
 e_1 er incident fra a og incident til b
d er både start- og slutknode for e_5

Indgraden af a er $\deg^-(a) = 1$ og

udgraden af a er $\deg^+(a) = 1$.

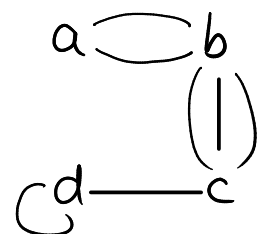
$$\deg^-(b) = 1, \quad \deg^+(b) = 4$$

$$\deg^-(c) = 4, \quad \deg^+(c) = 0$$

$$\deg^-(d) = 1, \quad \deg^+(d) = 2$$

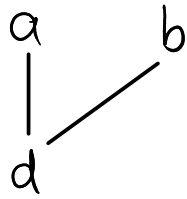
$$\sum_{x \in V} \deg^-(x) = 7 = \sum_{x \in V} \deg^+(x) = |E| \quad (\text{Sætning 10.2.3})$$

Den underliggende ikke-orienterede graf opnås ved at fjerne kantens orientering:

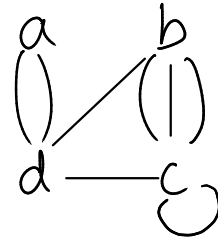


En **delgraf** består af (nogle af) knuderne og (nogle af) kanterne imellem dem.

Eks:



er en delgraf af



Delgrafer **induceret** af $\{a, b, d\}$ består af knuderne a, b, d og alle kanter imellem dem:

