

Sidste gang

Talteori

Kinesiske Restklasse-System (KRS)

Chinese Remainder Theorem (CRT)

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

⋮

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

hvor $m_1, \dots, m_n$ er parvis indbyrdes primiske
har en unik løsning modulo $m = \prod_{i=1}^n m_i$.

$$x = \sum_{k=1}^n M_k y_k a_k, \quad \text{hvor kan f.eks. findes via Euklids Algoritme}$$
$$M_k = \frac{m}{m_k} \quad \text{og} \quad M_k y_k \equiv 1 \pmod{m_k}$$

er en løsning, og løsningsmængden er
 $\{x + km \mid k \in \mathbb{Z}\}$.

Hvis $m_1, \dots, m_n$ ikke er parvis indbyrdes primiske,
kan der være en løsning, men ovenstående metode kan
ikke bruges (der vil være mindst et M_k , som ikke
har en multiplikativ invers modulo m_k).

Eks:

$x \equiv 1 \pmod{5}$	$M_1 = 504$	$y_1 = 4$
$x \equiv 2 \pmod{7}$	$M_2 = 360$	$y_2 = 5$
$x \equiv 3 \pmod{8}$	$M_3 = 315$	$y_3 = 3$
$x \equiv 4 \pmod{9}$	$M_4 = 280$	$y_4 = 1$
	$m = 2520$	

$$x = 504 \cdot 4 \cdot 1 + 360 \cdot 5 \cdot 2 + 315 \cdot 3 \cdot 3 + 280 \cdot 1 \cdot 4 = 9571 \\ \equiv 2011 \pmod{2520}$$

Løsningerne til første kongruens ligger med en afstand af 5, løsningerne til anden kongruens ligger med en afstand af 7 o.s.v. Da disse afstande er indbyrdes primiske, er der kun sammenfald mellem disse afstande for hvert 2520. heltal. D.v.s.:

$$\text{Løsningsmængde} = \{ 2011 + 2520k \mid k \in \mathbb{Z} \}$$

Fermats lille Sætning:

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

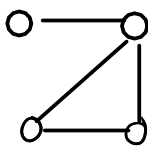
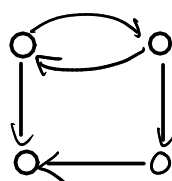
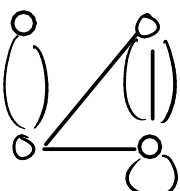
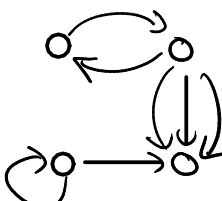
$$(1) \quad p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

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

Vi brugte (1) til at beregne $7^{222} \pmod{11}$.

Sammen med KRS kan (1) desuden bruges til at bevise, at RSA virker (DM534).

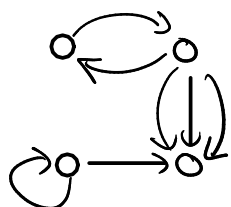
Grafer

	Ikke - orienterede	Orienterede
Simple grafer		
Multigrafer		

Begreber :

Parallell / anti-parallell kante, loop, incident, adjacent, nabo, nabomængde, grad, indgrad, udgrad

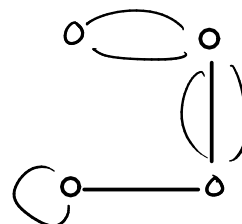
For grafer

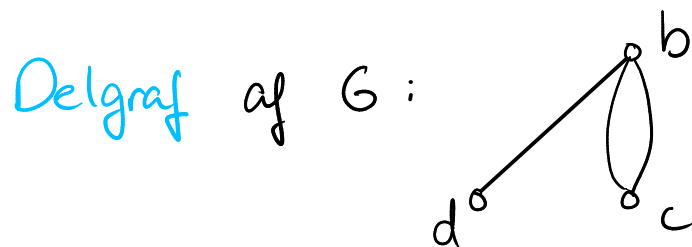
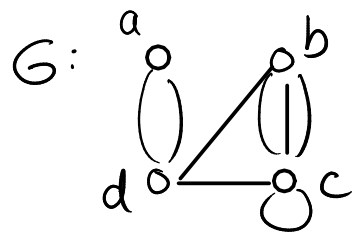


er den

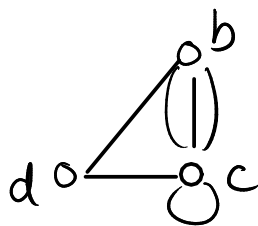
underliggende

ikke-orienterede graf





Delgrafer af G inducirt af $\{b, c, d\}$:

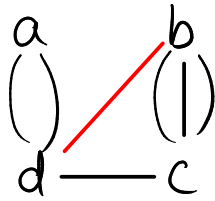


1 dag

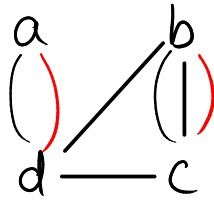
Pardannelser
 Grafklasser
 Isomorfi

En matching / pardannelse er en mængde af parvis ikke-adjacente kanter:

Maksimal matching:
(kan ikke udvides)



Maksimum matching:
(Størst mulig,
dvs grafer har
ingen matching med flere kanter)



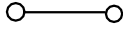
Særlige grafklasser:

Komplette grafer

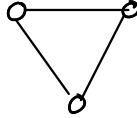
K_1 :



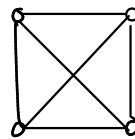
K_2 :



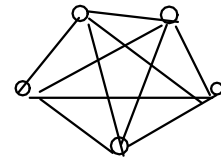
K_3 :



K_4 :



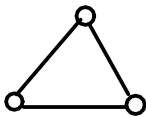
K_5 :



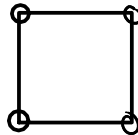
...

Kredse

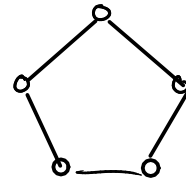
C_3 :



C_4 :



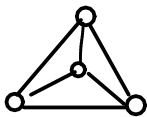
C_5 :



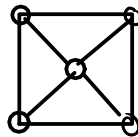
...

Hjul

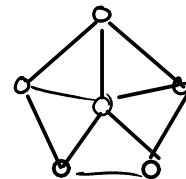
W_3 :



W_4 :



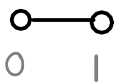
W_5 :



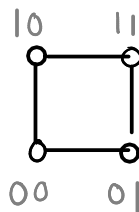
...

Hypercubes

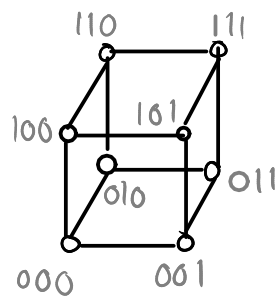
Q_1 :



Q_2 :



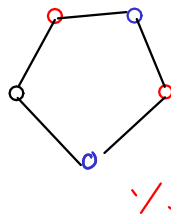
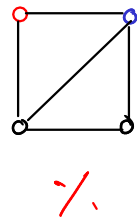
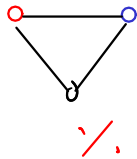
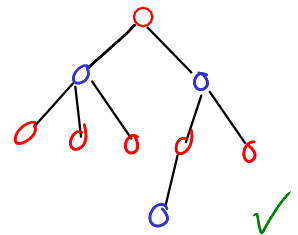
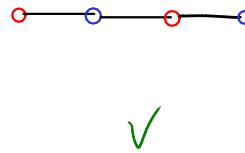
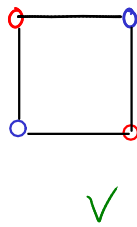
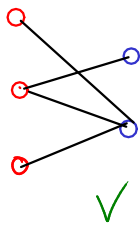
Q_3 :



Todelte grafer

Knudemængden V kan deles i to disjunkte mængder V_1 og V_2 , sådan at alle kanter går mellem V_1 og V_2 . (V_1 og V_2 er **uafhængige** mængder.)

Eks:

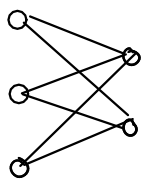


En **farvning** af en graf er en tildeling af farver til knuderne i grafer, sådan at naboknuder har forskellige farver.

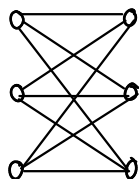
ætsning 10.2.4:

En simpel graf er todelte, hvis og kun hvis den kan tofarves

Komplette todelte grafer



$K_{3,2}$



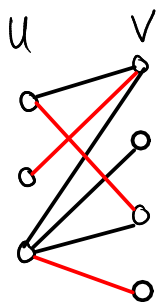
$K_{3,3}$

$G = (U \cup V, E)$: todelt graf

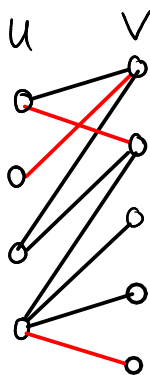
M : pardannelse i G

M er en **komplet pardannelse** fra U til V , hvis alle knuder i U er endepunkter i M , d.v.s. hvis $|U| = |M|$.

Eks:



✓



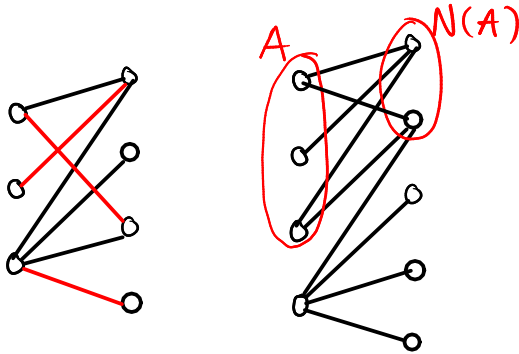
✗

Halls Sætning (Sætning 10.2.5)

$G = (U \cup V, E)$ totalt.

$\Updownarrow$ G har en komplet matching af U til V
 $|N(A)| \geq |A|$, for alle $A \subseteq U$

Eks:



Beris for Halls Sætning:

„ $|N(A)| \geq |A|$, for alle $A \subseteq U$ “ er klart en nødvendig betingelse.

Også tilstrækkelig (induktion over $|U|$):

Basis: $|U| = 1$

U indeholder præcis én knude u .

Da $N(u) \geq 1$, har u en nabo v , som den kan matches med.

Ind. ant.:

Sætningen gælder for grafer med $|U| \leq k$

Ind. skridt: $|U| = k+1$

Vi ser på to tilfælde:

$|N(A)| \geq |A| + 1$, for alle $A \subset U$:

Vælg en kant $\{u, v\}$.

Hvis vi fjerner v fra grafen, mister hver delmængde af U højst én nabo.

D.v.s. delgrafen af G induceret af $(U - \{u\}) \cup (V - \{v\})$ overholder betingelsen i Halls Sætning.

Ifølge ind. ant. betyder det, at den indeholder en komplet matching M af $U - \{u\}$.

$M \cup \{(u, v)\}$ udgør en komplet matching af U .

Der findes en mængde $A \subset U$, så $|N(A)| = |A| \geq 1$:

Grafen induceret af $A \cup V$ indeholder en komplet matching M af A , ifølge ind. ant. Lad $B = N(A)$ være knuderne, som M matcher A til.

Delgrafen induceret af $(U - A) \cup (V - B)$ overholder betingelsen i Halls Sætning:

Antag til modstrid, at der findes en delmængde $U_1 \subseteq U - A$, som har færre end $|U_1|$ naboer i $V - B$.

Da er

$$|N(A \cup U_1)| = \overbrace{|B|}^{=|A|} + \overbrace{|N_{V-B}(U_1)|}^{< |U_1|} < |A| + |U_1|$$

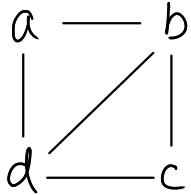
Men så overholder $A \cup U_1$ ikke betingelsen i sætningen $\downarrow$

□

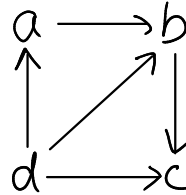
Afsnit 10.3

Representation of grafer:

Adjacenslister

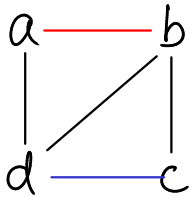


a: b, d
b: a, c, d
c: b, d
d: a, b, c

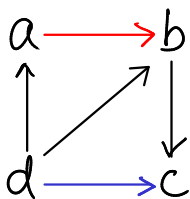


a: b
b: c
c:
d: a, b, c

Adjacensmatricer



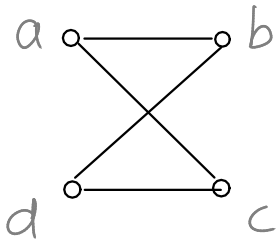
$$\begin{array}{c} \begin{matrix} & a & b & c & d \end{matrix} \\ \begin{matrix} a \\ b \\ c \\ d \end{matrix} \left[\begin{array}{cccc} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{array} \right] \end{array}$$



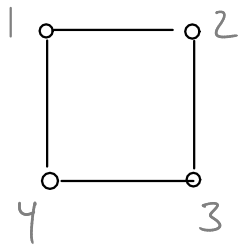
$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix} = A$$

Isomorfi:

Eks



$a: b, c$	$\xrightarrow{f}$	1: $f(b), f(c)$
$b: a, d$	$\longrightarrow$	2: $f(a), f(d)$
$c: a, d$	$\searrow$	3: $f(b), f(c)$
$d: b, c$	$\swarrow$	4: $f(a), f(d)$



1: 2, 4
2: 1, 3
3: 2, 4
4: 1, 3

Forskellige grafer?

Def. 1

Two simple graphs $G_1 = (V_1, E_1)$ og $G_2 = (V_2, E_2)$ er **isomorfe**, hvis $\exists$ **bijektion** $f: V_1 \rightarrow V_2$, så
 $\{a, b\} \in E_1 \iff \{f(a), f(b)\} \in E_2$,
for alle $a, b \in V_1$.

De to grafer i eks. ovenfor er isomorfe:

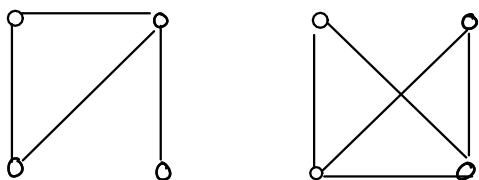
$$f(a) = 1$$

$$f(b) = 2$$

$$f(c) = 4$$

$$f(d) = 3$$

Eks:



Isomorfe?

Nej, der er ikke det samme #kanter.

Eks:

