

RSA:

$$n = p \cdot q$$

$$\gcd(e, (p-1)(q-1)) = 1$$

$$de \equiv 1 \pmod{(p-1)(q-1)}$$

$$P(M) = M^e \pmod{n}$$

$$S(C) = C^d \pmod{n}$$

RSA „virker“, dvs. $S(P(M)) = M$

Beviset bruger den kinesiske Restklasse-Sætning og

Fermats Lille Sætning (Sætning 4.4.3):

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

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

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

Bevis for $S(P(M)) = M$:

Beviser, at

$$(1) \quad S(P(M)) \equiv M \pmod{p} \quad \text{og}$$

$$(2) \quad S(P(M)) \equiv M \pmod{q}$$

- Klart, at begge kongruenser er opfyldt, hvis $S(P(M)) = M$
- Ifølge KRS er der kun et tal mellem 0 og $n-1$, som opfylder begge kongruenser

Da $0 \leq S(P(M)) \leq n-1$ betyder det, at $S(P(M)) = M$ er eneste mulighed

$$\begin{aligned}
S(P(M)) &= S(M^e \bmod n) \\
&= (M^e \bmod n)^d \bmod n \\
&= (M^e)^d \bmod n, \quad \text{ifølge Kr. 4.1.2} \\
&= M^{ed} \bmod n \\
&= M^{1+k(p-1)(q-1)} \bmod n, \quad k \in \mathbb{Z}, \text{ da } ed \equiv 1 \pmod{(p-1)(q-1)} \\
&= M \cdot M^{k(p-1)(q-1)} \bmod n \\
&= M \cdot (M^{p-1})^{k(q-1)} \bmod n \\
&= M \cdot (M^{q-1})^{k(p-1)} \bmod n
\end{aligned}$$

(1) $S(P(M)) \equiv M \pmod{p}$:

hvis $p \nmid M$:

$$\begin{aligned}
M \cdot (M^{p-1})^{k(q-1)} &\equiv M \cdot 1^{k(q-1)} \pmod{p}, \quad \text{iflg. Fermat (1)} \\
&\equiv M \pmod{p}
\end{aligned}$$

Ellers

$$M \equiv 0 \pmod{p}$$

D.v.s.

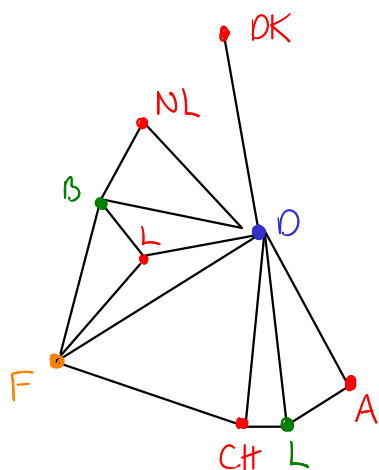
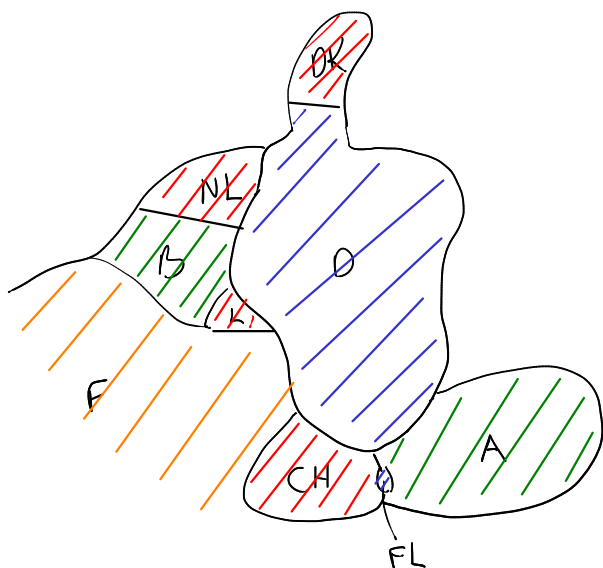
$$\begin{aligned}
M \cdot M^{k(p-1)(q-1)} &\equiv 0 \pmod{p} \\
&\equiv M \pmod{p}
\end{aligned}$$

(2) $S(P(M)) \equiv M \pmod{q}$:

Tilsvarende

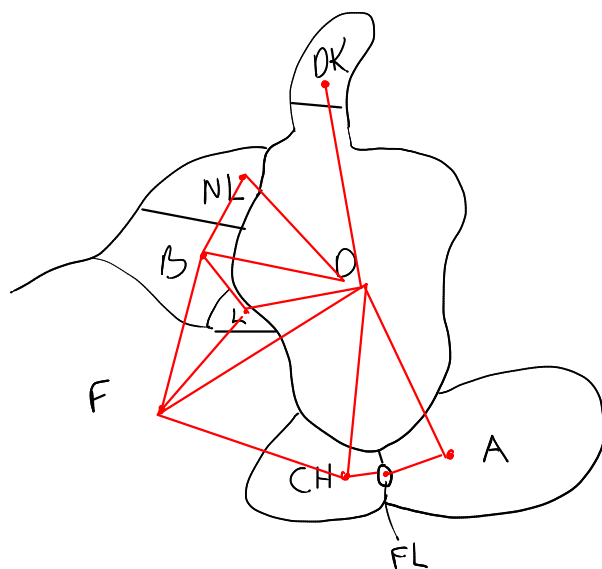
Graffarvning (Afsnit 10.8)

Et landkort kan altid farves med fire farver:



Konstruer den **duale graf**:

- Placer en knude i hvert land
- Forbind knuder, hvis lande deler en grænse (i mere end ét punkt):



Den duale graf er altid en **plan** graf, d.v.s. den kan tegnes, så ingen kanter krydser hinanden.

Def. 10.8.1:

En **farvning** af en graf er en tildeling af farver til knuderne i grafen, hvor intet par af naboknuder får samme farve.

Fire-Farve-Sætningen (Sætning 10.8.1)

En plan graf kan altid farves med højst fire farver

Fire-Farve-Sætningen blev formuleret som en påstand i 1850 og bevist i 1976 v.h.a. computer. Checkede et par tusinde grafer.

Simplere bevis i 1997, men stadig v.h.a. computer.

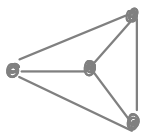
Def. 10.8.2:

Det kromatiske tal, $\chi(G)$, for en graf G , er det mindste #farver, man kan farve G med.

χ (græsk bogstav)

Det kromatiske tal for grafen ovenfor er 4:

- Højst 4, da grafen kan farves med 4 farver, som vist.
- Mindst 4, da grafen indeholder denne delgraf



, hvor hver af de fire knuder er nabo til alle tre andre knuder.

Fire-Farve-Sætningen kan også formuleres sådan:

For enhver plan graf G er $\chi(G) \leq 4$.

„Eks 5“: Eksamensplanlægning

Kurser tilmeldte

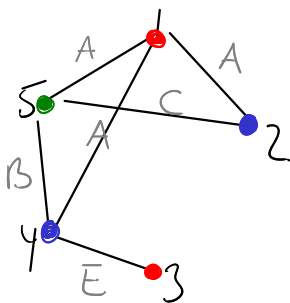
1 A, B

2 A, C, D

3 E, F

4 B, E

5 B, C



Eksamen 1 og 3 kan afvikles samme dag.

Eksamen 2 og 4 kan afvikles samme dag.

Eksamen 1, 2, 5 skal afvikles på tre forskellige dage.

„Eks 6“: Frekvens-tildeling

To sendemaster må kun bruge samme frekvens, hvis de er mindst 10 km fra hinanden.

	A	B	C	D
A		5	13	7
B			10	9
C				8
D				

