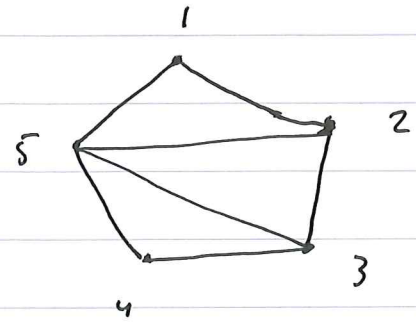
L. FORSLAG.

(1)

a) G:



b) Nabomatrise

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

c) En graf er Eulersk om det finns en sykel som inneholder hver kant nøyaktig en gang.

En graf er Hamiltonsk om det finns en sykel som inneholder hvert hjørne nøyaktig en gang.

En graf er Eulersk bare om hvert hjørne har et jevnt antall nabolr. Hjørnene 2 og 3 har tre nabolr så G er ikke Eulersk.
Sykelen 1 - 2 - 3 - 4 - 5 - 1 viser at G er Hamiltonsk.

1 d) Utspenningstrær i G:

Hvert utspenningstre må inneholde en kant til 1 : 2 stk
4 : 2 stk
to av de tre kantene mellom 2, 3 og 5 : 3 stk.

Til sammen $2 \times 2 \times 3 = 12$ utspenningstrær.

(2) $\pi : \{1 \dots n\} \to \{1 \dots n\}$ permutasjon.

$A_{n,k} = \#\{\pi \mid \pi(i) < \pi(i+1)$ for nøyaktig k tall $i\}$.
$= B_{n,k}$

a) $n = 4$: $(\pi(1), \pi(2), \pi(3), \pi(4)) =$

$(1\ 2\ 3\ 4) \in B_{4,3}$

$(1\ 3\ 2\ 4)\ (1\ 3\ 4\ 2)\ (1\ 2\ 4\ 3)\ (1\ 4\ 2\ 3)$
$(2\ 1\ 3\ 4)\ (2\ 3\ 1\ 4)\ (2\ 3\ 4\ 1)\ (2\ 4\ 1\ 3)$
$(3\ 1\ 2\ 4)\ (3\ 4\ 1\ 2)\ (4\ 1\ 2\ 3)$ $\Big\} \in B_{4,2}$

$(1\ 4\ 3\ 2)\ (2\ 1\ 4\ 3)\ (2\ 4\ 3\ 1)$
$(3\ 1\ 4\ 2)\ (3\ 2\ 1\ 4)\ (3\ 2\ 4\ 1)\ (3\ 4\ 2\ 1)$
$(4\ 1\ 3\ 2)\ (4\ 2\ 1\ 3)\ (4\ 2\ 3\ 1)\ (4\ 3\ 1\ 2)$ $\Big\} \in B_{4,1}$

$(4\ 3\ 2\ 1) \in B_{4,0}$

så $A_{4,0} = \# B_{4,0} = 1$

$A_{4,1} = \# B_{4,1} = 11$

$A_{4,2} = \# B_{4,2} = 11$

$A_{4,3} = \# B_{4,3} = 1$

(Kan og brukes 2G)

(2) c) La $\pi : \{1, \dots, n-1\} \to \{1, \dots, n-1\}$

være en permutasjon med k tall i slik at $\pi(i) < \pi(i+1)$. Utvid denne til en permutasjon $\pi' : \{1 \dots n\} \to \{1, \dots, n\}$ ved å

la $\pi'(i+1) = n$, $\pi'(j) = \pi(j)$ $j \le i$, $\pi'(j) = \pi(j-1)$, $j \ge i+2$.

for en i der $\pi(i) < \pi(i+1)$. Da vil $\pi' \in B_{n,k}$.

Det er $k+1$ slike muligheter for hver π

i alt $(k+1) \cdot A_{n-1,k}$.

La så $\pi : \{1, \dots, n-1\} \to \{1, \dots n-1\}$

være en permutasjon med $k-1$ tall i slik at $\pi(i) < \pi(i+1)$. Utvid denne til

en $\pi' : \{1 \dots n\} \to \{1 \dots n\}$

ved å la $\pi'(i+1) = n$, $\pi'(j) = \pi(j)$ $j \le i$, $\pi'(j) = \pi(j-1)$, $j \ge i+2$

for en i der $\pi(i) > \pi(i+1)$

Da vil $\pi' \in B_{n,k}$. Det er $n-k$ slike muligheter for hver π,

i alt $(n-k) A_{n-1,k-1}$

Hver $\pi' \in B_{n,k}$ er en av disse to muligheterne (se også oppg 1.36 i Bokc)

så $A_{n,k} = (n-k) A_{n-1,k-1} + (k+1) A_{n-1,k}$

(3)

$C \leq \{0,1\}^6$:

$$\{\underbrace{(000000)}_{A}, \underbrace{(110100)}_{B}, \underbrace{(101110)}_{C}, \underbrace{(011011)}_{D}, \underbrace{(100111)}_{E}\}$$

a) C er ikke lineær siden $|C| = \#C$ ikke er en potens av 2, eller også

$(110100), (101110) \in C$

mens $(110100) + (101110) = (011010) \notin C$.

b) Avstander:

$d(A,B) = 3$, $d(A,C) = 4$, $d(A,D) = 4$, $d(A,E) = 4$

$d(B,C) = 3$, $d(B,D) = 5$, $d(B,E) = 3$, $d(C,D) = 4$

$d(C,E) = 2$, $d(D,E) = 4$.

Minimumsdistansen er den minste av disse altså lik $\underline{\underline{2}}$.

c) (100000) har avstand 1 til $A = (000000)$ og bare dette kodeordet i C.

Siden minimumsavstanden er 2, så er $t = 1$ det største antall feil koden kan finne.

Siden $\frac{2}{2} - 1 = 0$ så kan C ikke rette en feil.

d) En syklisk kode i $\{0,1\}^6$ er generert av en faktor i $x^6 - 1 = (x+1)^2(x^2+x+1)^2$

Bruker faktor $x+1$ og får generator matrise

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

minste vekt = minimumsdistanse = 2 !

(4) RSA

$(n,k) = (33,3)$

a) $n = 3 \cdot 11$, så enhetene i $\mathbb{Z}_{33}$ er $\approx \mathbb{Z}_2 \cdot \mathbb{Z}_{10}$.

$3 \cdot k \equiv 1 \quad (20)$ — k privat nøkkel

så $\underline{k \equiv 7 \quad (20)}$ — 7 er Annes private nøkkel.

b) $m^3 \equiv 8 \quad (33)$

da er $\underline{\underline{m}} \equiv (m^3)^7 \equiv 8^7 \quad (33)$

$\equiv 64 \cdot 8^5 \quad (33)$

$\equiv (-2) \cdot 8^5 \quad (33)$

$\equiv (-2) \cdot (-2) \cdot (-2) \cdot 8 \quad (33)$

$= \underline{\underline{2}} \quad \underline{(33)}$

c) $(n,k) = (33,7)$. B's private nøkkel er 3

siden $3 \cdot 7 \equiv 1 \quad (20)$.

$m = m_1 m_2 m_3 m_4 m_5 m_6$.

$m_1^7 = 27 \quad m_2^7 = 20 \quad m_3^7 = 13 \quad m_4^7 = 16 \quad m_5^7 = 01 \quad m_6^7 = 28$

$m_1 \equiv (m_1^7)^3 \equiv 27^3 \equiv (-6)^3 \quad (33)$

$\equiv 3 \cdot (-6) \quad (33)$

$\equiv 15 \quad (33)$

$m_2 \equiv (m_2^7)^3 = 20^3 \equiv (-13)^3 \quad (33)$

$\equiv 4 \cdot (-13) \quad (33)$

$\equiv 14 \quad (33)$

$m_3 \equiv 13^3 \equiv -14 \equiv 19 \quad (33)$

$m_4 \equiv 16^3 \equiv -8 \cdot 16 \quad (33)$

$\equiv 4 \quad (33)$

$m_5 = 1^3 \equiv 1 \quad (33)$

$m_6 \equiv 28^3 \equiv (-5)^3 = 7 \quad (33)$

$15 = O \quad 14 = N \quad 19 = S \quad 04 = D \quad 01 = A \quad 07 = G$ så

$m = ONSDAG$.