Matematiska Institutionen
KTH

Lösningar till lappskrivning nr 6, variant B, på kursen Diskret matematik, 5B1118, för IT 1, måndagen den 5 december 2005, 10.15-11.00.

1. Betrakta permutationen φ beskriven med hjälp av tablån

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 1 & 3 & 6 & 5 & 7 \end{pmatrix}.$$

   Avgör om permutationen är udda eller jämn.

   Lösning: Som produkta av disjunkta cykler blir $\varphi = (1\ 2\ 4\ 3)(5\ 6)(7)$ som kan splittras upp i transpositioner tex som

$$\varphi = (1\ 3)(1\ 4)(1\ 2)(5\ 6).$$

   Ett jämnt antal transpositioner ger att permutationen är jämn.

2. Betrakta ett RSA-krypto med $n = 69$ och $e = 9$. Dekryptera meddelandet $b = 2$

   Lösning: $n = 3 \cdot 23$ ger att $m = (3-1)(23-1) = 44$. Allmänt gäller att $e \cdot d \equiv_m 1$. Vi ser att $9 \cdot 5 = 45 \equiv_{44} 1$. Alltså $d = 5$. Det gäller att att $D(2) = 2^d \pmod{69}$. Alltså

   Svar: $2^5 \pmod{69} = 32$.

3. Betrakta en linjär kod C med parity-check matrisen

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

   (a) Bestäm antalet kodord.
   Lösning: $2^{6-3} = 8$.

   (b) Ordet 111011 ligger på avståndet ett från ett ord $c \in C$. Bestäm c.
   Lösning:

$$H \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

   Detta är kolonn nummer två i matrisen H och alltså är det fel i andra positionen.
   Svar: 101011.

   (c) Bestäm antalet ord som inte ligger på avståndet ett eller noll från något ord i C.
   Lösning: Varje sfär med radien 1 runt ett kodord innehåller förutom kodordet själv, som ligger på avståndet 0 från sig själv, precis sex stycken ord på avståndet 1. Totalt alltså sju ord i varje sfär med radien ett. Det finns totalt åtta kodord och då sfärer med radien 1 runt kodord är disjunkta, ligger alltså totalt $8 \cdot 7 = 56$ ord på avstånd högst ett från något kodord. Det återstår åtta ord av de 64 möjliga orden, som inte gör det.
   Svar: 8.