

**Svar och lösningsförslag till ks4, 28 april 2009,
i SF1610(/5B1118) Diskret matematik för CL**

1) (För varje delfråga ger rätt svar $\frac{1}{2}$ p, inget svar 0p, fel svar $-\frac{1}{2}$ p.
Totalpoängen på uppgiften rundas av uppåt till närmaste icke-negativa heltal.)

	sant	falskt
a) Låt $\mathcal{C} = \{00000000, 1011001, 0101010, 1010101\}$. Med koden $\mathcal{C}$ kan ett fel i ett kodord säkert rättas. [Nej. Avståndet mellan andra och sista ordet är bara 2.]		×
b) Om kontrollmatrisen H för en binär, linjär kod är av typ 5×12 , innehåller koden minst 128 olika ord. [Ja, rangen för H är ≤ 5 , så $k \geq 12 - 5 = 7$, så $\geq 2^7 = 128$ ord.]	×	
c) Låt $N \in \mathbb{N}$, $N > 2$. Om $2^{N-1} \equiv 1 \pmod{N}$ måste N vara ett primtal . [Nej, det villkoret är nödvändigt, men inte tillräckligt.]		×
d) Med ett RSA-system för kryptering kan parametrarna n , m och e offentliggöras. Bara d måste hållas hemlig. [Nej, inte alls. m och e ger lätt d (Euklides algoritm).]		×
e) Om $\mathcal{B}$ är en boolesk algebra gäller för $a, b \in \mathcal{B}$ säkert att det finns ett $c \in \mathcal{B}$ med $a + c = b$. [Nej, t.ex. är $1 + c = 1$, alla c , så med $a = 1 \neq b$ finns inget sådant c .]		×
f) $\neg(p \rightarrow q) \equiv p \wedge \neg q$ gäller för alla satslogiska sentenser p och q . (' $\equiv$ ' betecknar logisk ekvivalens). [Ja. Båda är sanna precis om p är sann och q falsk.]	×	

2a) (1p) Den binära koden $\mathcal{C} = \{00000000000, 1100101000, 0110011010, 1011000101, 1101011111, 0111101101, 1010110010, 0001110111\}$ är **linjär** (behöver inte visas).
Vad är minimala avståndet (minimidistansen) δ för $\mathcal{C}$?

Lösning:

För en linjär kod är $\delta = w_{\min}$, minimala 0-skilda vikten, = 4 i vårt fall.

Svar: Det sökta minimala avståndet $\delta = 4$.

b) (1p) I ett (pytte-)RSA-system används "det stora talet" $n = 91 (= 7 \cdot 13)$. Ange för vart och ett av följande tal om det är ett möjligt värde för krypteringsexponenten e eller inte. **2, 5, 12, 13, 35, 49**

Lösning:

$n = 91 = 7 \cdot 13$ ger $m = 6 \cdot 12 = 2^3 3^2$. Villkoret på e är att $\text{sgd}(e, m) = 1$, så

Svar: 5, 13, 35 och 49 är möjliga. 2 och 12 är inte möjliga.

c) (1p) Låt $a, b \in \mathcal{B}$, en boolesk algebra. Visa: om $a \cdot b = a$ så $a + b = b$.

Lösning:

Om $a \cdot b = a$ fås $a + b = a \cdot b + b = b$ (absorption och kommutativitet).

Saken är klar.

3) En linjär kod $\mathcal{C}$ definieras av kontrollmatrisen (i boken kallad checkmatrisen)

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

a) (1p) Vilket eller vilka (om något) av följande är ord i koden $\mathcal{C}$?

0001101, 1110101, 0111001

Lösning:

$\mathbf{H}(0001101)^T = (000)^T$, $\mathbf{H}(1110101)^T = (001)^T$, $\mathbf{H}(0111001)^T = (000)^T$, så

Svar: 0001101 och 0111001 är kodord, men inte 1110101.

b) (1p) Om man tar emot ordet **1010110** och högst ett fel har uppstått, vilket var det sända kodordet?

Lösning:

Eftersom $\mathbf{H}(1010110)^T = (001)^T$, $\mathbf{H}$'s tredje kolonn, har bit tre blivit fel, så

Svar: Det sända ordet var 1000110.

c) (1p) Finns det ord (binära, av längd 7) som varken tillhör $\mathcal{C}$ eller kan uppstå med ett fel i ett kodord? Motivera antingen varför inget sådant finns, eller ange ett.

Lösning:

Eftersom $\mathbf{H}$ innehåller alla 0-skilda kolonner i $\mathbb{Z}_2^3$, är för godtyckligt $z \in \mathbb{Z}_2^7$ $\mathbf{H}z$ antingen $(000)^T$ eller en kolonn i $\mathbf{H}$, så $z \in \mathcal{C}$ eller fås från $c \in \mathcal{C}$ med ett fel ($\mathcal{C}$ är en hammingkod). **Svar: Nej, något sådant ord finns inte.**

4) (3p) Vad blir (minsta icke-negativa) resten då 284^{2009} divideras med 7? Dvs finn x med $x \equiv 284^{2009} \pmod{7}$, $0 \leq x \leq 6$. Motivera ordentligt.

Lösning:

Eftersom $284 = 7 \cdot 40 + 4 \equiv 4 \pmod{7}$ är $284^{2009} \equiv 4^{2009} \pmod{7}$.

Enligt Fermats lilla sats är $4^6 \equiv 1 \pmod{7}$ (7 är primtal och $7 \nmid 4$).

$2009 = 6 \cdot 333 + 1 = 6 \cdot 334 + 5$, så $4^{2009} = (4^6)^{333} 4^5 \equiv 1 \cdot 4^5 = 16 \cdot 16 \cdot 4 \equiv 2 \cdot 2 \cdot 4 = 16 \equiv 2 \pmod{7}$, så **Svar: Den sökta resten blir 2.**

5) (3p) Uttryck den booleska funktionen $f(x, y, z) = xyz + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z}$ på **minimal disjunktiv form**, dvs disjunktiv form med så få '.' och '+' som möjligt. ('.' skall förstås räknas även när de underförstås.)

Lösning:

Uttrycket för f ger karnaughdiagrammet härintill.

Genom att, som i fig., täcka 1:orna med så stora rektanglar som möjligt med sidlängder 1, 2 eller 4, får vi att $f(x, y, z)$ är lika med $\bar{x}y + yz + \bar{y}\bar{z}$. Alternativt kan den liggande rektangeln ersättas med en stående. Det ger $\bar{x}\bar{z} + yz + \bar{y}\bar{z}$.

Svar: Uttrycket blir

$f(x, y, z) = \bar{x}y + yz + \bar{y}\bar{z} = \bar{x}\bar{z} + yz + \bar{y}\bar{z}$.

		z	
		0	1
xy	00	1	0
	01	1	1
	11	0	1
	10	1	0