Svar och lösningsförslag till ks4, 25 april 2007,
i 5B1118 Diskret matematik för CL2 och CL3

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)	**Avståndet** (distansen) mellan orden 1101011 och 1001101 i en binär kod är 3. [Ja, olika i 3 positioner.]	X	
b)	Den linjära koden med kontrollmatris $\begin{smallmatrix}1&0&1&0&0&1\\0&1&0&1&0&1\end{smallmatrix}$ har dimension 3. [Nej, $6-2=4$.]		X
c)	I ett RSA-system med parametrar n, m, e, d offentliggörs normalt n, m och e. [Nej, m och e ger lätt d, så allt kan läsas!]		X
d)	Ett **carmichaeltal** är ett primtal som för minst en bas inte klarar fermattestet. [Nej, inget primtal. P-tal klarar f-test.]		X
e)	Med **boolesk algebra** kan man forma om satslogiska sentenser till logiskt ekvivalenta sentenser. [Ja, faktiskt.]	X	
f)	Den booleska funktionen $f(x,y,z,w) = x\overline{y}z + yz\overline{w}$ är given på **disjunktiv normalform**. [Nej, för få faktorer.]		X

2a) (1p) Man har en binär kod $\mathcal{C}$ av längd 6.
Hur många ord kan $\mathcal{C}$ högst innehålla, om man säkert kan rätta upp till två uppkomna fel i kodens ord? Man får inte förutsätta att $\mathcal{C}$ är linjär.
Motivera ditt svar.

Lösning:

Sfärpackningssatsen ger: (antalet ord) $\cdot(\underbrace{\binom{6}{0}+\binom{6}{1}+\binom{6}{2}}_{=1+6+15=22}) \leq 2^6 = 64$, så
koden innehåller högst 2 ord

---

b) (1p) Formulera **Fermats lilla sats**.
Var noga med att inte missa någon förutsättning.

Lösning:

Om p är ett primtal och a ett heltal så att $p \nmid a$, gäller $a^{p-1} \equiv 1 \pmod{p}$.

---

c) (1p) Skriv upp värdetabellen för den booleska funktionen
$f(x,y,z) = (\overline{x\overline{y}+yz})(x+\overline{y}z)$.

Lösning:

T.ex. $f(1,0,1) = (\overline{1\cdot\overline{0}+0\cdot 1})(1+\overline{0}\cdot 1) = (\overline{1\cdot 1+0\cdot 1})(1+1\cdot 1) = \overline{1}\cdot 1 = 0\cdot 1 = 0$
och motsvarande för övriga rader i tabellen

x	y	z	$f(x,y,z)$
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	0

3) En linjär kod definieras av kontrollmatrisen (i boken kallad checkmatrisen)

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

a) (1p) Vilket eller vilka (om något) av följande är ord i koden?
$010110, 111010, 111100$

Lösning:
$\mathbf{H}(010110)^T = (000)^T, \mathbf{H}(111010)^T = (010)^T, \mathbf{H}(111100)^T = (000)^T$,
så **010110 och 111100 är kodord**.

---

b) (2p) Om man tar emot 101101 och högst ett fel har uppstått, vilket var det sända kodordet?

Lösning:
$\mathbf{H}(101101)^T = (101)^T = \mathbf{H}$:s tredje kolonn, så fel i tredje positionen.
Det sända ordet var 100101.

---

4) (3p) I ett (pytte-)RSA-system används en offentlig nyckel för kryptering $(n, e) = (527, 113)$. $(527 = 17 \cdot 31)$
Finn talet d som behövs för att dekryptera meddelanden i detta system.

Lösning:
$n = 17 \cdot 31$, båda primtal, ger att $m = (17-1)(31-1) = 480 (= 2^5 \cdot 3 \cdot 5)$.
Villkoret som bestämmer d är $ed \equiv 1 \pmod{m}$, dvs $113d \equiv 1 \pmod{480}$.
Vi använder Euklides algoritm. $480 = 4 \cdot 113 + 28$, $113 = 4 \cdot 28 + 1$, så $1 = 113 - 4 \cdot 28 = 113 - 4(480 - 4 \cdot 113) = -4 \cdot 480 + 17 \cdot 113$, vilket ger att $17 \cdot 113 \equiv 1 \pmod{480}$, så **svaret: $\boldsymbol{d = 17}$**.

---

5) (3p) Betrakta den booleska funktion $f(x, y, z)$ som ges av värdetabellen

x	y	z	$f(x,y,z)$
1	1	1	0
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	1
0	1	0	0
0	0	1	1
0	0	0	1

a) (1p) Skriv $f(x, y, z)$ som ett booleskt uttryck (dvs ett uttryck med x, y, z och $+, \cdot, \bar{}$) på **disjunktiv normalform, dnf**.

Lösning:
Mot t.ex. raden 101 svarar termen $x\overline{y}z$ och motsvarande för de andra raderna med 1:or. Man får
$\boldsymbol{f(x,y,z) = x\overline{y}z + x\overline{y}\,\overline{z} + \overline{x}yz + \overline{x}\,\overline{y}z + \overline{x}\,\overline{y}\,\overline{z}}$

b) (2p) Uttryck med hjälp av ett **karnaughdiagram** $f(x, y, z)$ som ett **minimalt** disjunktivt uttryck.

Lösning:
Värdena i tabellen ger karnaughdiagrammet härintill.
Genom att, som i fig., täcka 1:orna med så stora rektanglar som möjligt (i fig. går en 2×2-rektangel "runt kanten" en gång) med sidlängder 1, 2 eller 4, får vi att $f(x, y, z)$ är ekvivalent med $\overline{y} + \overline{x}z$.
Svar: Uttrycket blir $\boldsymbol{f(x,y,z) = \overline{y} + \overline{x}z}$.

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