

**Svar och lösningsförslag till ks4, 2 maj 2011,
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) Om det minimala avståndet (distansen) mellan ord i en binär kod är 6, kan man säkert rätta 3 fel med koden. [Nej. Det finns ett ord med avstånd 3 till två olika kodord.]		×
b) En linjär kod av längd $n = 7$ och dimension $k = 3$ har precis 8 olika kodord. [Javisst, antalet ord är 2^k .]	×	
c) Om p och q är olika primtal och $r \equiv 1 \pmod{(pq-1)}$ så är säkert $x^r \equiv x \pmod{(pq)}$ för alla $x \in \mathbb{Z}$. [Nej, $(p-1)(q-1)$ skall det vara. Motex: $p=2, q=3, r=6, x=2$.]		×
d) I ett RSA-system för kryptering med offentlig nyckel måste krypteringsexponenten e vara ett primtal eller en produkt av två primtal. [Nej, kravet är att $\text{sgd}(e, m) = 1$.]		×
e) Om $\mathcal{B}$ är en boolesk algebra gäller för $a, b, c \in \mathcal{B}$ säkert att $(a+b) \cdot \overline{a} \cdot c = a + (b \cdot \overline{c})$. [Ja. $(a+b) \cdot \overline{a} \cdot c = (a+b) \cdot (a+\overline{c}) = a + (b \cdot \overline{c})$, eller med värdetabell.]	×	
f) Om $f(x, y, z)$ är en boolesk funktion gäller säkert att $f(x, y, z) = f(\overline{x}, \overline{y}, \overline{z})$. [Nej, inte alls. $f(x, y, z) = x + y$ ger ju $f(x, y, z) = \overline{x} \cdot \overline{y} \neq \overline{x} + \overline{y} = f(\overline{x}, \overline{y}, \overline{z})$, motexempel.]		×

2a) (1p) Kan en linjär kod med kontrollmatrisen $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$ säkert rätta ett fel?

Rätta i så fall ordet 11101, ange annars ett ord med ett fel som inte kan rättas.

Lösning:

Nej, H :s kolonner 2 och 5 är lika, så 01001 är (liksom 00000) ett kodord och 00001 kan inte rättas. (Också 11100 och 10101 är kodord, så 11101 kan inte heller rättas.)

Svar: Nej. 00001 kan fås med ett fel, men kan inte rättas.

b) (1p) Formulera **fermattestet med bas b** för att avgöra om talet N är ett primtal. Vilka slutsatser kan dras av olika utfall av testet?

Lösning:

Enligt Fermats lilla sats är $b^{N-1} \equiv 1 \pmod{N}$ om N är primtal (och $N \nmid b$).

Svar: Testet, "är $b^{N-1} \equiv 1 \pmod{N}$ eller $N \nmid b$?",

slutsatser av svaren, "nej": N är sammansatt, "ja": vet ej (säkert).

c) (1p) Ge värdetabellen för booleska funktionen $f(x, y) = (\overline{x} \cdot \overline{y}) \cdot (\overline{x} \cdot \overline{y} + x)$.

Lösning:

Antingen med boolesk algebra: $f(x, y) = (x + \overline{y})(\overline{x} + \overline{y} + x) = (x + \overline{y})(\overline{y} + 1) = x + \overline{y}$, eller
t.ex. $f(1, 0) = (\overline{1} \cdot \overline{0}) \cdot (\overline{1} \cdot \overline{0} + 1) = \overline{0} \cdot 1 = 1$ och
motsvarande för övriga rader i tabellen

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

3) Den linjära binära koden $\mathcal{C}$ rättar (minst) 1 fel.

a) (2p) Finn det minsta möjliga värdet för $\mathcal{C}$:s längd (dvs längden av orden i $\mathcal{C}$), om den innehåller precis 16 ord, $|\mathcal{C}| = 16$.

b) (1p) Ange en möjlig kontrollmatris (checkmatris) H för koden $\mathcal{C}$.

Lösning:

a) $16 = 2^4$, så kodens dimension $k = 4$. Om dess längd är n och kontrollmatrisen har rang r , är $k = n - r$, dvs $n = 4 + r$. $\mathcal{C}$ rättar ett fel omm alla kolonner är olika och $\neq 0$, så $4 + r \leq 2^r - 1$. Minsta möjliga r , n är 3 och 7.

b) H en godtycklig 3×7 -matris med kolonner olika, alla $\neq 0$. ($\mathcal{C}$ en Hammingkod.)

Svar a): Minsta möjliga längd är 7, b): t.ex. $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$.

4) (3p) Vi söker (minsta icke-negativa) resten då $2^{5^{2011}}$ divideras med 13, dvs x med $x \equiv 2^{5^{2011}} \pmod{13}$, $0 \leq x \leq 12$.

Lösning:

Enligt Fermats lilla sats är $2^{12} \equiv 1 \pmod{13}$ (ty 13 är primtal och $13 \nmid 2$). $5^2 = 25 \equiv 1 \pmod{12}$, så $5^{2011} = 5^{2 \cdot 1005 + 1} \equiv 1^{1005} \cdot 5 = 5 \pmod{12}$ och $2^{5^{2011}} = 2^{k \cdot 12 + 5} \equiv 1^k \cdot 2^5 = 32 \equiv 6 \pmod{13}$, med något heltal k .

Svar: Den sökta resten är 6.

5) Vi betraktar den booleska funktion $f(x, y, z)$ med värdetabellen nedan.

a) (1p) Skriv $f(x, y, z)$ som ett booleskt uttryck på **disjunktiv normalform, dnf**.

b) (2p) Skriv med hjälp av ett **karnaughdiagram** $f(x, y, z)$ på **minimal** disjunktiv form.

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

Lösning:

a) Den disjunktiva normalformen är summan av mintermerna som svarar mot raderna med 1:or i tabellen, så $f(x, y, z) = xyz + xy\bar{z} + x\bar{y}z + \bar{x}\bar{y}z$.

b) Värdena i tabellen ger karnaughdiagrammet härintill.

Genom att, som i fig., täcka 1:orna med så stora rektanglar som möjligt (i fig. går en 2×1 -rektangel "runt kanten" en gång) med sidlängder 1, 2 eller 4, får vi att $f(x, y, z)$ är $xy + y\bar{z} + \bar{y}z$. Ett alternativt val av en rektangel ger $xz + y\bar{z} + \bar{y}z$.

Svar a): $f(x, y, z) = xyz + xy\bar{z} + x\bar{y}z + \bar{x}\bar{y}z$

b): $f(x, y, z) = xy + y\bar{z} + \bar{y}z = xz + y\bar{z} + \bar{y}z$.

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