MATEMATIK
Chalmers tekniska högskola

Lösningar tenta tillämpade diskreta strukturer 07 mars 1998

1. a) Från TENTAMEN får vi 20 5 14 20 1 13 5 14. Då $r^3 \equiv r \pmod 3$ och $(\pm 2)^3 \equiv \pm 8 \pmod 1)1$, $(\pm 3)^3 \equiv \pm 5 \pmod{11}$, $(\pm 4)^3 \equiv \pm 9 \pmod{11}$ och $(\pm 5)^3 \equiv \pm 4 \pmod{11}$ hittar man lätt $r^3 \bmod 33$. Vi får: 14 26 5 14 1 19 26 4 eller NÅENASÅE.
b) Då $\phi(33) = 2 \cdot 10$ och $3 \cdot 7 \equiv 1 \pmod{20}$ är $d = 7$. Vi har $r^7 \equiv r \pmod 3$ och $(\pm 2)^7 \equiv \pm 7 \pmod{11}$, $(\pm 3)^7 \equiv \pm 9 \pmod{11}$, $(\pm 4)^7 \equiv \pm 5 \pmod{11}$ och $(\pm 5)^7 \equiv \pm 3 \pmod{11}$. Från L@ÄKABNCLL = 12 30 27 11 1 2 14 3 12 12 får vi 12 24 3 11 1 29 20 9 12 12 = LYCKA TILL.

2. a) $SGD(a,n) = 1$ omm det finns $x, y \in \mathbb{Z}$ med $xa + yn = 1$, omm det finns $x \in \mathbb{Z}_n$ med $xa \equiv 1 \pmod n$, vad som betyder att $a \in \mathbb{Z}_n$ har en invers.
b) Ringen $\mathbb{Z}_n$ är en kropp omm varje element $a \in \mathbb{Z}_n \setminus \{0\}$ har en invers, dvs $SGD(a,n) = 1$ för alla $0 < a < n$. Men detta är så omm n är ett primtal.

3. $f\colon \mathbb{Z}_{1221} \to \mathbb{Z}_{33} \times \mathbb{Z}_{37}$, $n \mapsto (n \bmod 33, n \bmod 37)$. Vi har $f(37) = (4,0)$ alltså $-8 \cdot f(37) = (1,0)$ och $f^{-1}(1,0) = 925$. $f^{-1}(0,1) = 9 \cdot 33 = 297$. Alltså är $f^{-1}(10,20) \equiv -10 \cdot 8 \cdot 37 + 20 \cdot 9 \cdot 33 \equiv 20(9 \cdot 33 - 4 \cdot 37) \equiv 20(5 \cdot 33 - 16) \equiv 20 \cdot 149 \equiv 2980 \equiv 538$.

4. $f(x,y,z) = \overline{x}y + \overline{y(x+z)} = \overline{x}y + \overline{y} + \overline{x+z} = \overline{x}y + \overline{y} + \overline{x}\overline{z} = \overline{x}yz + \overline{x}y\overline{z} + \overline{y} + \overline{x}\overline{y}\overline{z} + \overline{x}y\overline{z} = \overline{x}yz + \overline{x}y\overline{z} + x\overline{y}z + x\overline{y}\overline{z} + \overline{x}\overline{y}z + \overline{x}\overline{y}\overline{z}$.
$\overline{f} = xyz + xy\overline{z}$ (mintermer som saknas i f).

5. Polynomet $p(X) = X^5 + X^3 + X^2 + X + 1$ har inga linjarfaktorer ty $p(0) = p(1) = 1$. Det är inte delbart med $X^2 + X + 1$ ty $SGD(X^5 + X^3 + X^2 + X + 1, X^3 + 1) = SGD(X^3 + 1, X) = 1$. Därför är p irreducibelt. Eftersom multiplikativa gruppen i kroppen $\mathbb{Z}_2[X]/(p(X))$ har 31 element har $\alpha = [X]$ ordning 31 och p är primitivt i $\mathbb{Z}_2[X]$.
För en BCH-kod med vikt minst $5 = 2 \cdot 2 + 1$ behöver vi ett polynom med nollställen α, α^2, α^3 och α^4. Polynomet $g_1 := p$ har nollställen α, α^2 och α^4. Vi beräknar $\alpha^6 = \alpha + \alpha^2 + \alpha^3 + \alpha^4$, $\alpha^9 = \alpha^3 \cdot \alpha^6 = \alpha + \alpha^4$, $\alpha^{12} = 1 + \alpha$ och $\alpha^{15} = \alpha^3 + \alpha^4$. Man ser nu att α^3 uppfyller $g_3(X) = 1 + X + X^3 + X^4 + X^5 = 0$ och kodningspolynomet blir $g(X) = g_1(X)g_3(X) = 1 + X^3 + X^4 + X^9 + X^{10}$.

6. Periodiska sekvensen $s = (1,0,0,0,1,1,0,0,0,1,\ldots)$ över $\mathbb{Z}_2$ har period 5. Det gäller $s_{n+5} = s_n$. Motsvarande polynomet $X^5 + 1$ är reducibelt: $X^5 + 1 = (X+1)(X^4 + X^3 + X^2 + X + 1)$. Sekvensen uppfyller också $s_{n+4} = s_{n+3} + s_{n+2} + s_{n+1} + s_n$. Då $X^4 + X^3 + X^2 + X + 1$ är irreducibelt (men inte primitivt) är $\mathcal{A}(1,1,1,1)$ det minsta skiftregistret.

7. $GL(2,\mathbb{Z}_2)$ är en grupp: matrismultiplikation är associativ, $\det(AB) = \det A \det B$, neutrala elementet är $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, en matris A är inverterbar omm $\det A \neq 0$.
Låt $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Ingen kolonn eller rad är noll, så om $a = 0$ är $b = c = 1$ och vi får element $J = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ med ordning 2 och $C = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ med $C^2 = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ och $C^3 = I$. Om $a \neq 0$ och $d = 0$ har vi C^2. Annars är $d = 1$ och vi får I, $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ och ${}^tT = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. (observera att $\det\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) = 0$). $T^2 =^t T^2 = I$.
En delgrupp har ordning 1, 2, 3 eller 6. Delgrupper är $\{I\}$, $\{I,J\}$, $\{I,T\}$, $\{I,^tT\}$, $\{I,C,C^2\}$ och $GL(2,\mathbb{Z}_2)$. Fler finns inte ty $T^tT = JT = C$. Gruppen är isomorf med den symmetriska gruppen S_3.

8. Vi har $\omega^0 = 1$, $\omega^1 = 2$, $\omega^2 = 4$, $\omega^3 = 8$, $\omega^4 = -1$, $\omega^5 = -2$, $\omega^6 = -4$, $\omega^7 = -8$ och $\omega^8 = 1$ i $\mathbb{Z}_{17}$. Vi beräkna FFTen genom att dela motsvarande polynom med $X^4 - 1$, $X^4 + 1$, sen $X^2 - 1$, $X^2 + 1$, $X^2 - 4$, $X^2 + 4$ och sen med $X - 1$, $X + 1$, $X - 4$, $X + 4$, $X - 2$, $X + 2$, $X - 8$, $X + 8$. Från $1 + X + 3X^2 + 3X^3$ får vi $8\ 0\ 7\ 6\ 5\ 4\ 3\ -8$ och från $1 + 3X^2 + X^3$: $5\ 3\ -6\ 2\ 4\ 5\ 8\ 4$. Koefficientvis multiplikation ger $6\ 0\ -8\ -5\ 3\ 3\ 7\ 2$. Vi använder FFT met ω^{-1} (dvs vi dela med $X^4 - 1$, $X^4 + 1$, sen $X^2 - 1$, $X^2 + 1$, $X^2 + 4$, $X^2 - 4$ och sen med $X - 1$, $X + 1$, $X + 4$, $X - 4$, $X + 8$, $X - 8$, $X + 2$, $X - 2$) på $6 + 3X - 8X^2 + 7X^3 + 3X^5 - 5X^6 + 2X^7$ med resultat $8\ -5\ -3\ 7\ 8\ -6\ 5\ 0$. Slutligen delar vi med 8, dvs multiplicerar med -2 och får $1\ 10\ 6\ 3\ 1\ 12\ 7\ 0$. Produktet är alltså $1 + X + 6X^2 + 7X^3 + 10X^4 + 12X^5 + 3X^6$. Vi beräknar produktet också modulo 4: $(1 + X - X^2 - X^3)(1 - X^2 + X^3) = 1 + X - 2X^2 - X^3 + 2X^4 - X^6$ och konstaterar att produktet är $1 + X + 6X^2 + 7X^3 + 10X^4 + 12X^5 + 3X^6$ även över $\mathbb{Z}$.
Från `F5` får vi $1 + X + 3X^2 + 3X^3$ och $1 + 3X^2 + X^3$ från `71`. Produktet $1 + X + 6X^2 + 7X^3 + 10X^4 + 12X^5 + 3X^6$ ger $1 + 4 + 6 \cdot 4^2 + 7 \cdot 4^3 + 10 \cdot 4^4 + 12 \cdot 4^5 + 3 \cdot 4^6 = 5 + (6 + 7 \cdot 4)16 + (10 + 12 \cdot 4)16^2 + 3 \cdot 16^3 = \texttt{6C25} = 27685$.