MATEMATIK
Chalmers tekniska högskola

Tentamen i TILLÄMPADE DISKRETA STRUKTURER (TMA381)
05 mars 2001, kl 14.15–18.15

Hjälpmedel: Valfri miniräknare, men inga egna anteckningar.
Telefonvakt: Erik Svensson, 0740-459022

OBS! Linje och inskrivningsår samt namn och personnummer skall anges.

---

1. Vi definierar ett sk Hillkrypto över $\mathbb{Z}_{29}$. Vi koderar A–Ö som 1–28 och utropstecknet som 0. Matrisen $H = \begin{pmatrix} 3 & 7 \\ 3 & 26 \end{pmatrix}$ definierar en linjär avbildning från $\mathbb{Z}_{29}^2$ till $\mathbb{Z}_{29}^2$ som används för att kryptera $\binom{x}{y} \in \mathbb{Z}_{29}^2$. Beräkna H^{-1} och dekryptera

$$\begin{pmatrix} \mathrm{B} & \mathrm{S} & \mathrm{F} & \mathrm{A} & \mathrm{C} \\ \mathrm{E} & \mathrm{P} & \mathrm{B} & \text{Å} & \mathrm{C} \end{pmatrix} .$$

2. a) Konstruera en gruppkod som har tre informationssymboler, tre kontrollsymboler och korrigerar ett fel.
b) Avkoda 111011 och 100111.

3. Enligt Kinesiska restsatsen är $f\colon \mathbb{Z}_{2001} \to \mathbb{Z}_{29} \times \mathbb{Z}_{23} \times \mathbb{Z}_3$, $n \mapsto (n \bmod 29, n \bmod 23, n \bmod 3)$ en isomorfism. Ange inversen f^{-1} explicit och beräkna $f^{-1}(20, 0, 1)$.

4. Låt $\mathcal{B}$ vara en Boolesk algebra med addition '$+$', multiplication '$\cdot$' och konjugering $x \mapsto \bar{x}$. Definiera i mängden $\mathcal{B}$ operationen

$$x \oplus y = x \cdot \bar{y} + \bar{x} \cdot y .$$

Visa att $(\mathcal{B}, \oplus)$ är en abelsk grupp.

5. a) Låt K vara en kropp och $p(X)$ ett polynom i $K[X]$. Visa att ett element $[r(X)] \in K[X]/p(X)$ har en invers om och endast om $SGD(r(X), p(X)) = 1$.
b) Motivera att ringen $K[X]/p(X)$ är en kropp om och endast om polynomet $p(X)$ är irreducibelt.

6. Visa att polynomet $p(X) = X^5 + X^3 + 1$ är primitivt i $\mathbb{Z}_2[X]$. Använd detta för att konstruera kodningspolynomet för en BCH-kod med vikt minst 5.

7. Bestäm den kortaste perioden av rekurrensföljden över $\mathbb{Z}_3$, definierad genom $s_{n+3} = s_{n+1} - s_n$, $s_0 = s_1 = s_2 = 1$.

8. Visa att $\omega = 2$ är en primitiv åttonde enhetsrot i $\mathbb{Z}_{17}$ med $\omega^4 = -1$ och använd snabb Fouriertransform baserad på ω för att beräkna

$$(3 + 3X + 3X^2 + 3X^3)^2$$

i $\mathbb{Z}_{17}[X]$. Använd resultatet för att beräkna $\texttt{FF}^2$, där $\texttt{FF}$ är 255 skriven hexadecimalt.
(8 p)

Lycka till!

Jan Stevens