Matematiska Institutionen
KTH

Några övningar, inför tentan moment B, på de avsnitt som inte omfattats av lappskrivningarna, Diskret matematik för D2 och F, vt08.

1. Ett RSA-krypto har $n = 187$ och $e = 23$. Kryptera meddelandet 2 och dekryptera meddelandet 3.

2. En 1-felsrättande kod C har kontrollmatrisen

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

   (a) Rätta ordet 111110.

   (b) Bestäm samtliga ord i C.

   (c) Hur många ord har avstånd minst två till samtliga ord i koden?

3. Konstruera en kropp med 49 element, dvs ange på lämpligt sätt de 49 elementen och beskriv hur dessa element adderas och multipliceras.

4. Låt $\bar{c}_1 = 11100000$, $\bar{c}_2 = 00111000$ och $\bar{c}_3 = 11000111$ vara binära ord av längd 8.

   (a) Bestäm en linjär kod C med så få ord som möjligt och sådan att $\bar{c}_1, \bar{c}_2, \bar{c}_3 \in C$.

   (b) Bestäm en kontrollmatris till den kod C du fann.

   (c) Bestäm en annan kontrollmatris till koden C.

5. Använd det irreducibla polynomet $p(x) = x^4 + x + 1$ i $Z_2[x]$ för att konstruera en kropp F_{16} med 16 element. Bestäm samtliga generatorer till den multiplikativa gruppen i F_{16}.

6. Bestäm med hjälp av sfärpackningsvillkoret en övre gräns för antalet ord i en e-felsrättande kod C bestående av binära ord av längd 10 för $e = 1$, $e = 2$ och $e = 3$. Bestäm också det maximala antalet ord linjära koder med dessa parametrar kan ha.

7. Bestäm antalet rötter till ekvationen $z^4 = 1$ i kroppen F_{128} med 128 element.

8. Kroppen F_9 konstrueras på sedvanligt sätt och med hjälp av det irreducibla polynomet $p(x) = x^2 + 1$.

   (a) Lös ekvationen $z^2 = 2$.

   (b) Lös ekvationen $z^2 = x + 1$.

   (c) Lös ekvationen $z^2 = x$.

9. Går det att använda den sk pq-formeln när man löser andragradsekvationer i ändliga kroppar eller är generellt metoden med kvadratkomplettering, dvs

$$x^2 + px + q = 0 \quad \Longleftrightarrow \quad (x + \frac{p}{2})^2 - \frac{p^2}{4} + q = 0$$

   att föredra?

10. Herr A vill efter att ha löst uppgifterna ovan nu tillslut konstruera en kropp med 81 element och på snabbast möjliga sätt. Hjälp honom.