Abgabe zu zweit vor der Vorlesung am Di., **01.07.14** um 10:15 Uhr im Raum E 20.

Aufgabe 22 (Zyklische RS-Codes)

Im Folgenden sei $\mathbb{F}_q$ ein endlicher Körper.

a) Bestimme die Zerlegung von $x^6 - 1$ in irreduzible Faktoren über $\mathbb{F}_7$.
Tipp: Welche Ordnung haben die Elemente in $\mathbb{F}_7^*$?

b) Wie viele zyklische $(6, 3)$-Codes gibt es über $\mathbb{F}_7$?

c) Wie viele (zyklische) $RS^{6,3}$-Codes gibt es über $\mathbb{F}_7$?
Tipp: Benutze den Tipp aus a).

d) Sei $\mathcal{C}$ ein zyklischer Code mit Erzeugerpolynom g über $\mathbb{F}_q$ und $\alpha \in \mathbb{F}_q$ eine Nullstelle von g.
Zeige: $c(\alpha) = 0 \;\; \forall\, c \in \mathcal{C}$.

e) Berechne das Erzeugerpolynom für den $RS^{6,3}$-Code mit $\beta = 3$ über $\mathbb{F}_7$ aus Aufgabe 19.

(1+1+1+0,5+1,5 = **6 P**)

Aufgabe 23 (Zyklische Codes)

Wir betrachten den binären Code $\mathcal{C}$ gegeben durch die Erzeugermatrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} .$$

a) Zeige, dass $\mathcal{C}$ zyklisch, aber nicht selbstdual ist.

b) Finde ein Codewort c von der Form $c = (c_0, c_1, c_2, c_3, 0, 0, 0) \in \mathcal{C}$.

c) Zeige: $c(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3$ ist das Erzeugerpolynom von $\mathcal{C}$.

d) Gibt es einen zyklischen $(7, 5)$-Code über $\mathbb{F}_2$? Begründe.
Hinweis: Über $\mathbb{F}_2$ gilt folgende Zerlegung in irreduzible Faktoren:
$x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$, wie wir auf Blatt 5, Aufgabe 11 d) gezeigt haben. Vergleiche auch mit Beispiel 4.1.8.

(1,5+1+0,5+1 = **4 P**)