Übungsaufgaben zur Kodierungstheorie

1. *(4 Punkte)* Der Euklidische Algorithmus (Satz 8.11).
   Mittels des Euklidischen Algorithmus lassen sich Zahlen κ, λ bestimmen mit

   $$\mathrm{ggT}\,(a_0, a_1) = \kappa \cdot a_0 + \lambda \cdot a_1.$$

   (Vergleichen Sie dazu Satz 8.11(b)(I).) Diese Darstellung wird nun benutzt, um zu einem Element $a_1 \neq 0$ in einem endlichen Körper $\mathbb{F}_{q^l}$ ein inverses Element a_1^{-1} zu finden.

   (a) Sei $q = 103$ und $l = 1$. Es soll das Inverse von $a_1 = 24$ bestimmt werden. Da q eine Primzahl ist, gilt $\mathrm{ggT}\,(103, 24) = 1$. Führen Sie den Euklidischen Algorithmus *mit Zusatzinformation (Satz 8.11)* für $a_0 = 103$ und $a_1 = 24$ durch. Begründen Sie, dass g_{m+1} das Inverse zu 24 ist. Geben Sie $24^{-1} \in \mathbb{F}_{103}$ an.

   (b) Sei α ein erzeugendes Element von $\mathbb{F}_8 - \{0\}$ mit Minimalpolynom $g(x) = x^3 + x + 1$. Bestimmen Sie mit Hilfe des Euklidischen Algorithmus *mit Zusatzinformation (Satz 8.11)* das Inverse zu $a_1 := \alpha^2 + \alpha \in \mathbb{F}_8$.
   (Hinweise: Es ist $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$*. Da* $g(x)$ *irreduzibel in* $\mathbb{F}_2[x]$ *ist, folgt* $\mathrm{ggT}\,(g(x), f(x)) = 1$ *für alle* $f(x) \in \mathbb{F}_2[x]$ *mit* $f(x) \neq 0$*,* $deg(f(x)) \leq 2$*.)*

2. *(4+2 Punkte)*

   Sei R ein kommutativer Ring mit Eins. Dann ist der formale Potenzreihenring $R[[z]]$ definiert als

   $$R[[z]] := \Big\{ \sum_{i=0}^{\infty} a_i z^i \mid a_i \in R \Big\},$$

   und z ist eine Variable. $R[[z]]$ wird selbst zu einem kommutativen Ring mit Eins, wenn folgende Addition und Multiplikation auf $R[[z]]$ definiert werden:

   $$\sum_{i=0}^{\infty} a_i z^i + \sum_{i=0}^{\infty} b_i z^i := \sum_{i=0}^{\infty} (a_i + b_i) z^i \quad \text{und} \quad \Big(\sum_{i=0}^{\infty} a_i z^i \Big) \cdot \Big(\sum_{i=0}^{\infty} b_i z^i \Big) := \sum_{i=0}^{\infty} c_i z^i \text{ mit } c_i := \sum_{k=0}^{i} a_k b_{i-k}.$$

   Jedes Polynom aus $R[z]$ kann in natürlicher Weise als formale Potenzreihe betrachtet werden, in dem die Koeffizienten oberhalb des Polynomgrades als Null gesetzt werden. Die Eins in $R[[z]]$ ist dann das Polynom 1, d.h. $\sum_{i=0}^{\infty} a_i z^i$ mit $a_0 = 1$ und $a_i = 0$ für $i > 0$.

   Die formalen Potenzreihen über R können auch als Folgen über R betrachtet werden (mit dem Startindex Null), d.h. also $R[[z]] \sim R^{\mathbb{N}_0}$, und die Polynome über R als Folgen über R mit nur endlich vielen Einträgen ungleich Null, d.h. also $R[z] \sim R^{(\mathbb{N}_0)}$.

Bitte wenden!

(a) Beweisen Sie:

$$\sum_{i=0}^{\infty} a_i z^i \text{ ist eine Einheit in } R[[z]] \quad \Longleftrightarrow \quad a_0 \text{ ist eine Einheit in } R.$$

Bemerkung: Polynome mit einem Grad größer als Null sind nie Einheiten in ihrem Polynomring, können es aber als formale Potenzreihen betrachtet im formalen Potenzreihenring sein. Die Inverse eines solchen Polynoms ist dann immer eine „echte“ formale Potenzreihe.

(b) Nach dem ersten Teil ist das Polynom $-z+1$ als formale Potenzreihe eine Einheit in $R[[z]]$. Beweisen Sie in $R[[z]]$ die Gleichung:

$$\frac{z}{1-z} := z \cdot (1-z)^{-1} = \sum_{i=1}^{\infty} z^i.$$

Bemerkung: Die Aussagen dieser Aufgabe sind Teile des Beweises von Satz 8.10.

3. *(1+2+3 Punkte)* (Folgende Aufgabe ist eine Übung zu den Sätzen 6.16, 6.17 und 6.18.)

(a) Bestimmen Sie mit Hilfe der Formel für $|J_{m,p}|$ des Skriptes die Anzahl der irreduziblen Polynome vom Grad 4 in $\mathbb{F}_2[t]$ und geben Sie alle an.

(b) $f := t^4 + t^3 + 1$ ist ein irreduzibles Polynom in $\mathbb{F}_2[t]$, und es sei $\mathbb{F}_{16} := \mathbb{F}[t]/(f)$. Weiter sei $\alpha := [t] \in \mathbb{F}_2[t]/(f) = \mathbb{F}_{16}$. Geben Sie alle Elemente von $\mathbb{F}_{16}^* := \mathbb{F}_{16} \setminus \{0\}$ als Polynome in α an und deren Ordnungen als Elemente der multiplikativen Gruppe des Körpers. Die multiplikative Gruppe eines endlichen Körpers ist immer zyklisch. Geben Sie alle Erzeuger der zyklischen multiplikativen Gruppe $\mathbb{F}_{16}^*$ an. (Nutzen Sie: die Ordnung eines Gruppenelementes teilt die Ordnung der Gruppe.)

(c) Es sei $\varphi\colon \mathbb{F}_{16} \longrightarrow \mathbb{F}_{16}$ mit $x \mapsto x^2$ der Frobeniusautomorphismus von $\mathbb{F}_{16}$. Wegen $\varphi^4 = \mathrm{id}_{\mathbb{F}_{16}}$ ist dann $G := \{\mathrm{id}, \varphi, \varphi^2, \varphi^3\}$ eine zyklische Gruppe von Automorphismen von $\mathbb{F}_{16}$.
Für $x \in \mathbb{F}_{16}$ sei $G(x) := \{\, \eta(x) \mid \eta \in G \,\}$. Offensichtlich gilt für $y \in G(x)$ dann $G(x) = G(y)$, und es gibt für geeignete $x_i \in \mathbb{F}_{16}$ eine disjunkte Zerlegung von $\mathbb{F}_{16}$ der Form

$$\mathbb{F}_{16} = \dot{\bigcup} G(x_i).$$

Nach Satz 6.18.c) hat jedes $y \in G(x)$ das Minimalpolyom

$$\mu_y = \prod_{x_i \in G(x)} (t - x_i).$$

Bestimmen Sie die Mengen $G(x_i)$ obiger Zerlegung von $\mathbb{F}_{16}$ und daraus dann für jedes x_i (und damit für alle Elemente von $\mathbb{F}_{16}$) das Minimalpolynom.

Abgabe am Montag, den 07. Mai 2012, in der Übung