Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

SS 2009
24. Juni 2009

Algorithmische Zahlentheorie

Übungsblatt 10

Aufgabe 37

a) Man bestimme sämtliche irreduziblen Polynome vom Grad $d = 1, 2, 3, 4$ über dem Körper $\mathbb{F}_2$.

b) Sei $f(X) = \sum_{k=0}^{n} a_k X^k$, $a_n \neq 0, a_0 \neq 0$, ein Polynom vom Grad $n \geqslant 2$ über einem Körper K.
Man beweise: Genau dann ist $f(X)$ irreduzibel, wenn das Polynom $g(X) := \sum_{k=0}^{n} a_{n-k} X^k$ irreduzibel ist.

Aufgabe 38

Die Elemente des Körpers $\mathbb{F}_{2^4} = \mathbb{F}_2[X]/(\phi(X))$, wobei $\phi(X) := X^4 + X + 1$, seien mit Bitvektoren der Länge 4 identifiziert, wobei dem Körperelement $\xi = \sum_{i=0}^{3} b_i X^i \bmod \phi(X)$ der Bitvektor $(b_3 b_2 b_1 b_0)$ zugeordnet sei. Diese Elemente seien wie üblich durch die Hexadezimal-Ziffern

`0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F`

bezeichnet.

a) Man stelle eine Tafel der Quadrate aller Elemente von $\mathbb{F}_{16}$ auf.

b) Man zeige, dass das Element $g :=$ `3` eine Primitivwurzel, d.h. ein erzeugendes Element der Gruppe $\mathbb{F}_{16}^*$ ist.

Aufgabe 39

a) Man zeige, dass für jedes $k \in \mathbb{F}_{16}$ die Abbildung

$$E_k : \mathbb{F}_{16} \to \mathbb{F}_{16}, \qquad x \mapsto (x + k)^2 + 1,$$

bijektiv ist.

b) Man bestimme die Fixpunkte von E_k (in Abhängigkeit von k).

c) Die Funktion E_k werde als Block-Verschlüsselung für Blöcke der Bitlänge 4 aufgefasst. Man verschlüssele den Text

`AFFE2009` $\in (\mathbb{F}_{16})^8$

mit E_7 im ECB-, CBC- und OFB-Modus. Der Initialisierungs-Vektor sei $iv =$ `5`.

---

b.w.

Aufgabe 40

Mit $F(X) := X^8 + 1 \in \mathbb{F}_2[X]$ werde der Ring $R := \mathbb{F}_2[X]/(F(X))$ definiert. R ist ein 8-dimensionaler Vektorraum über $\mathbb{F}_2$. Sei

$$G(X) := X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X].$$

Man betrachte die Abbildung

$$\psi : R \to R, \quad f \mapsto \psi(f) := G \cdot f \bmod F.$$

a) Man zeige: Die Matrix von ψ bzgl. der Basis $(\overline{X^7}, \overline{X^6}, \ldots, \overline{X}, 1)$ von R ist

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{M}(8 \times 8, \mathbb{F}_2).$$

b) Man zeige $\gcd(F, G) = 1$ und berechne mittels des erweiterten euklidischen Algorithmus das Inverse von G mod F im Ring R.

c) Unter Benutzung von b) bestimme man das Inverse der Matrix M.

Abgabetermin: Freitag, 3. Juli 2009, 14 Uhr, Übungskasten im 1. Stock