Übungsblatt 9

Aufgabe 49 ***10 Punkte***

(a) Bestimmen Sie in $\mathbb{Z}_7[x]/3x^2+1$ den Repräsentanten für die Restklasse, in der das Polynom $p(x) = 2x^5 + x^4 + 4x + 3$ enthalten ist.

(b) Bestimmen Sie alle irreduziblen Polynome $m(x)$ vom Grad 2 in $\mathbb{Z}_3[x]$.

(c) Stellen Sie die Additions- und Multiplikationstafeln für den Polynomrestklassenring $\mathbb{Z}_3[x]/m(x)$ auf, wobei $m(x)$ das lexikographisch kleinste irreduzible Polynom vom Grad 2 in $\mathbb{Z}_3[x]$ ist.

Aufgabe 50 ***mündlich***

(a) Berechnen Sie die Rundenschlüssel $K^0, \ldots, K^{10}$, die sich aus dem externen 128-Bit-AES-Schlüssel $K =$ `2B7E151628AED2A6ABF7158809CF4F3C` ergeben.

(b) Verschlüsseln Sie mit K den Klartext $x =$ `3243F6A8885A308D313198A2E0370734`

Aufgabe 51 ***mündlich***

Der »normale« Ablauf einer Entschlüsselung beim AES erfolgt nach folgendem Schema:

```
1 AddRoundKey(K^10)
2 ShiftRows^-1
3 SubBytes^-1
4 for i ← 9 downto 1 do
5     AddRoundKey(K^i)
6     MixColumns^-1
7     ShiftRows^-1
8     SubBytes^-1
9 AddRoundKey(K^0)
```

Zeigen Sie, dass alternativ auch dieselbe Reihenfolge der Operationen wie bei der Verschlüsselung benutzt werden kann.

Aufgabe 52 ***10 Punkte***

Sei R der Polynom-Restklassenring $\mathbb{F}_{2^8}[y]/(y^4+1)$.

(a) Zeigen Sie, dass R kein Körper ist.

(b) Ist das Ringelement $a(y) = 03y^3 + 01y^2 + 01y + 02$ in R invertierbar?

(c) Zeigen Sie, dass die AES-Operation MixColumns eine multiplikative Chiffre mit festem Schlüssel $a(y)$ im Ring R realisiert.

Aufgabe 53 ***mündlich***

Zeigen Sie, dass für jede Primzahlpotenz p^k ($p > 2$, $k \geq 1$) die Kongruenz $x^2 \equiv_{p^k} 1$ genau zwei Lösungen $\pm a$ besitzt.

Hinweis: p kann nicht sowohl $a+1$ als auch $a-1$ teilen.

Aufgabe 54 ***mündlich***

Sei $a \in G$ ein Gruppenelement der Ordnung k. Zeigen Sie, dass $\mathrm{ord}(a^i) = k/\,\mathrm{ggT}(k,i)$ ist.

Aufgabe 55 ***mündlich***

(a) Zeigen Sie, dass $\mathbb{F}_{p^n}$ zusammen mit der Addition auf $\mathbb{F}_{p^n}$ und der Einschränkung der Multiplikation auf Skalarprodukte der Form $a(x)b(x)$ mit $a(x) = a_0 \in \mathbb{F}_p$ und $b(x) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in \mathbb{F}_{p^n}$ einen n-dimensionalen Vektorraum $(\mathbb{F}_p)^n$ über $\mathbb{F}_p$ bildet (falls wir $b(x) \in \mathbb{F}_{p^n}$ als Vektor $(b_{n-1}, \ldots, b_0)$ darstellen).

(b) Zeigen Sie, dass die Multiplikation mit einem festen Körperelement $a = (a_{n-1}, \ldots, a_0)$ in $\mathbb{F}_{p^n}$, also die Abbildung $f_a\colon (b_{n-1}, \ldots, b_0) \mapsto (a_{n-1}, \ldots, a_0) \cdot (b_{n-1}, \ldots, b_0)$ eine lineare Abbildung $f_a\colon (\mathbb{F}_p)^n \to (\mathbb{F}_p)^n$ ist.

(c) Folgern Sie, dass jede lineare Abbildung $f\colon (\mathbb{F}_{p^n})^l \to (\mathbb{F}_{p^n})^k$ über dem Körper $\mathbb{F}_{p^n}$ auch eine lineare Abbildung $f\colon (\mathbb{F}_p)^{nl} \to (\mathbb{F}_p)^{nk}$ über $\mathbb{F}_p$ ist. Gilt hiervon auch die Umkehrung?

Aufgabe 56 ***mündlich***

Sei G eine endliche Gruppe der Ordnung $\|G\| = m$ und sei 1 das neutrale Element von G.

(a) Zeigen Sie, dass für jedes $a \in G$ ein $k > 0$ existiert mit $a^k = 1$.

(b) Sei nun $\mathrm{ord}(a) = k$. Zeigen Sie, dass die Menge $[a] = \{a^i \mid i \geq 0\}$ eine Untergruppe von G mit genau k Elementen bildet. Folgern Sie $k|m$ und $a^m = 1$.

(c) Zeigen Sie, dass genau dann $a^i = a^j$ ist, wenn $i \equiv_{\mathrm{ord}(a)} j$ gilt.

(d) Geben Sie einen Isomorphismus zwischen den beiden Gruppen $[a]$ und $(\mathbb{Z}_k, +)$ an.