Codierungstheorie – Praktikum 2

Schreiben Sie ein Programm zur Konstruktion eines endlichen Körpers $\mathbb{F}_{p^d} \simeq \mathbb{Z}_p[x]_{f(x)}$ mit p^d Elementen, p Primzahl, $d > 1$ natürliche Zahl.

1. Entwerfen Sie eine Datenstruktur für die Elemente aus $\mathbb{F}_{p^d}$, welche Polynome $a(x) = \sum_{i=0}^{d-1} a_i x^i$ mit Koeffizienten $a_i \in \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ sind.

2. Schreiben Sie eine Routine, welche die modulare Polynommultiplikation

$$a(x) \cdot_f b(x) := (a(x) \cdot b(x)) \mod f(x)$$

realisiert.

3. Durchlaufen Sie mit $a(x)$, $b(x)$ und $c(x)$ alle Polynome aus $\mathbb{Z}_p[x]_{f(x)}$ und testen Sie

$$\big(a(x) \cdot_f b(x)\big) \cdot_f c(x) = a(x) \cdot_f \big(b(x) \cdot_f c(x)\big)\,.$$

4. Testen Sie Ihr Programm für die endlichen Körper, die durch folgende irreduziblen Polynome definiert sind:

$$\begin{aligned}
f(x) &= x^2 + x + 1 \in \mathbb{Z}_2[x] \\
f(x) &= x^3 + x^2 + 1 \in \mathbb{Z}_2[x] \\
f(x) &= x^4 + x^3 + 1 \in \mathbb{Z}_2[x] \\
f(x) &= x^2 + x + 2 \in \mathbb{Z}_3[x] \\
f(x) &= x^2 + x + 2 \in \mathbb{Z}_5[x] \\
f(x) &= x^3 + 3x + 2 \in \mathbb{Z}_5[x]
\end{aligned}$$

5. Berechnen Sie die Additions- und Multiplikationstabelle für die Körper $\mathbb{F}_8 = \{0, 1, \ldots, 7\}$ und $\mathbb{F}_9 = \{0, 1, \ldots, 8\}$.

Spielregeln für die Abnahme des Praktikums

- Sie bearbeiten die Aufgabe im 2er Team. Die Teams werden in der ersten Vorlesung gebildet.
- Wenn Sie das Praktikum vollständig gelöst haben, senden Sie eine E-Mail mit dem Betreff „Abnahmetermin Codierungstheorie“ an den Dozenten (`michael.braun@h-da.de`). Sie bekommen dann den nächsten freien Zeitslot während Ihres Praktikumstermins zugewiesen, in dem die Abnahme stattfindet.
- Für die Abnahme bereiten Sie eine Kurzpräsentation vor (15 min) und senden den Foliensatz vorab als pdf an den Dozenten. Die Präsentation soll unter anderen
  - die nachvollziehbare Dokumentation der Lösungen bzw. Lösungswege der einzelnen Teilaufgaben,
  - sowie die nachvollziehbare Beschreibung der verwendeten Algorithmen (nicht nur ein Auszug des Quellcodes!)

  enthalten.