Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Angelika Steger

WS 1998/99
Übungsblatt 12
9. Feb. 1999

Diskrete Strukturen I

(Abgabetermin: Dienstag, 16. Feb. 1999, vor der Vorlesung)

Aufgabe 1

(a) Bestimmen Sie die Faktorisierung von $x^4 + 1$ über $\mathbb{Z}_3[x]$.

(b) Bestimmen Sie den Rest von $2x^5 + 3x^2 + 2$ modulo $4x^2 + 1$ in $\mathbb{Z}_5[x]$.

Aufgabe 2

Als *Charakteristik* eines Körpers K bezeichnet man die kleinste natürliche Zahl n, so daß

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ mal}} = 0.$$

Falls kein solches n existiert, sagt man der Körper hat Charakteristik 0.
Zeigen Sie

(a) In jedem endlichen Körper ist die Charakteristik eine Primzahl.

(b) In einem Körper der Charakteristik p gilt

$$(a + b)^p = a^p + b^p \qquad \text{für alle } a, b \in K.$$

Aufgabe 3

(a) Welche der folgenden Polynome in $\mathbb{Z}_2[x]$ sind irreduzibel?

$$x^3 + 1 \qquad x^3 + x + 1 \qquad x^3 + x^2 + 1.$$

(b) Bestimmen Sie für die irreduziblen Polynome aus (a) jeweils den durch die in der Vorlesung beschriebene Konstruktion entstehenden Körper. Zeigen Sie, daß diese Körper isomorph sind.

Aufgabe 4

Schreiben Sie ein Programm, daß die Reed-Solomon Codierung des folgenden Satzes erzeugt:

Dies ist das letzte Aufgabenblatt in diesem Wintersemester.

Verwandeln Sie dazu zunächst jeden Buchstaben mit Hilfe der ASCII-Codierung in einen 0/1-String der Länge 7. Verwenden Sie dann die Reed-Solomon Codierung mit den Parametern $s = 6$ und $t = 2$. Ihr Programm soll die erzeugte Codierung in durch senkrechte Striche getrennten Blöcken von 0/1-Strings der Länge 6 ausgeben, mit 6 Blöcken pro Zeile.
Hinweis: $x^6 + x + 1$ ist ein irreduzibles Polynom vom Grad 6 über $\mathbb{Z}_2$.