Technische Universität München
Fakultät für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Ernst W. Mayr
Dr. Werner Meixner

Wintersemester 2012/13
Übungsblatt 9
10. Dezember 2012

# Diskrete Strukturen

*Abgabetermin: 18. Dezember 2012, 14 Uhr in die* **DS Briefkästen**

## Hausaufgabe 1 (4 Punkte)

Sei $M = \{1, 2, 3\}$. Eine Abbildung $f : M \to M$ ist genau dann nicht surjektiv, wenn gilt $(\exists y \in M\, \forall x \in M)\, [f(x) \neq y]$. Sei $S$ die Menge aller nicht surjektiven Abbildungen von $M$ in $M$.

1. Wie viele Elemente enthält $S$?
2. Es bezeichne $\circ$ die Komposition von Abbildungen. Man zeige, dass $A = (S, \circ)$ eine Algebra bildet, d. h. dass gilt $f, g \in S \Rightarrow f \circ g \in S$.
3. Beweisen Sie, dass $A$ keine Gruppe ist.

## Hausaufgabe 2 (4 Punkte)

1. Zeigen Sie für alle $m, n \in \mathbb{N}$ mit $m < n$, dass $\frac{x^{2^n}-1}{x^{2^m}+1}$ ein Polynom ist.
2. Man zeige: Die 6 rationalen Funktionen $x$, $\frac{1}{x}$, $1-x$, $\frac{1}{1-x}$, $\frac{x}{x-1}$, $\frac{x-1}{x}$ bilden eine Gruppe bezüglich der Komposition $f \circ g$.

## Hausaufgabe 3 (4 Punkte)

Berechnen Sie u.a. mit Hilfe des erweiterten Euklidischen Algorithmus ganze Zahlen $a, b$, so dass

$$a \cdot 58 + b \cdot 36 = 4\,.$$

## Hausaufgabe 4 (4 Punkte)

Bestimmen Sie Polynome $a(x), b(x), c(x)$ über den komplexen Zahlen mit imaginärer Einheit $i$ und $\mathrm{grad}(a) \leq 1$, $\mathrm{grad}(b) = 0$, $\mathrm{grad}(c) = 0$, so dass gilt:

$$\frac{2x^3 - 13x^2 + 18x - 4}{(x-3)^2(x+2i)(x-2i)} = \frac{a(x)}{(x-3)^2} + \frac{b(x)}{(x+2i)} + \frac{c(x)}{(x-2i)}\,.$$

## Hausaufgabe 5 (4 Punkte)

Gegeben seien die Polynome $a(x) = x^4 + x^3 + 3$ und $b(x) = 3x^2 + 4$ aus dem Polynomring $\mathbb{Z}_5[x]$ über dem Körper $\mathbb{Z}_5$.

1. Wie viele Elemente enthält die Menge $R_b$ aller Polynome $r(x) \in \mathbb{Z}_5[x]$ mit $\mathrm{grad}(r) < \mathrm{grad}(b)$?
2. Bestimmen Sie mit dem Euklidischen Algorithmus ein Polynom $s$ möglichst hohen Grades, das sowohl Teiler von $a$ als auch Teiler von $b$ ist.

***Hinweis:*** *Die Vorbereitungsaufgaben werden in der Zentralübung unterstützt.*

## Vorbereitung 1

Wir betrachten den Ring $R = \mathbb{Z}_3[x]$. Beachten und nutzen Sie im Folgenden die Isomorphie zwischen $(\mathbb{Z}_3[x]/(g), +, \cdot)$ und $(\mathbb{Z}_3[x]_{\mathrm{grad}(g)}, +_g, \cdot_g)$, die für alle $g \in R$ durch die Abbildung $[f]_g \to Rem_g(f)$ gegeben ist. Wir schreiben gelegentlich $p \in \mathbb{Z}_3[x]/(g)$ für $p \in \mathbb{Z}_3[x]_{\mathrm{grad}(g)}$.

Sei $g(x) = x^2 + 2x + 1$.

1. Bestimmen Sie alle Elemente des Rings $\mathbb{Z}_3[x]/(g)$.
2. Bestimmen Sie die Spalten der Additions- und Multiplikations-Verknüpfungstafeln zum Element $[x + 2]_g \in \mathbb{Z}_3[x]/(g)$.
3. Berechnen Sie Polynome $p(x) \in \mathbb{Z}_3[x]$ und $r(x) \in \mathbb{Z}_3[x]_2$ mit der Eigenschaft
$$x^4 + x + 1 = p(x) \cdot (x^2 + 2x + 1) + r(x)\,.$$
4. Ist der Restklassenring $\mathbb{Z}_3[x]/(g)$ ein Körper? Begründung!

## Vorbereitung 2

Ist $x^4 + x^3 + 1$ irreduzibel in GF(2)[x]? Begründung!

## Tutoraufgabe 1

Sei $\pi(x) = x^3 + 1$. Wir betrachten den Ring $R = (\mathbb{Z}_2[x]_3, +_{\pi(x)}, \cdot_{\pi(x)})$. Seine Elemente werden repräsentiert durch die Reste bei Polynomdivision durch $x^3 + 1$.

1. Geben Sie die Menge aller Elemente von $R$ an.
2. Wir betrachten das Element $a = x^2 \in \mathbb{Z}_2[x]_3$. Bestimmen Sie die Zeile der Multiplikationstafel des Ringes $R$, die für alle $b \in \mathbb{Z}_2[x]_3$ die Produkte $a \cdot_{\pi(x)} b$ auflistet.
3. Geben Sie die Menge der Nullteiler in $R$ an.

   Hinweis: $p \in \mathbb{Z}_2[x]_3$ mit $\mathrm{grad}(p) \neq 0$ heißt Nullteiler, falls es ein $q \in \mathbb{Z}_2[x]_3$ mit $\mathrm{grad}(q) \neq 0$ gibt, so dass gilt $p \cdot_{\pi(x)} q = 0$.

## Tutoraufgabe 2

1. Berechnen Sie $(1+1)^{100}$ in $GF(9)$. Beweisen Sie Ihr Ergebnis!
2. Sei $p$ ein primitives Element in $GF(9)$. Zeigen Sie, dass das Polynom

   $$\pi(x) = x^2 + px + p(p-1)$$

   über $GF(9)$ irreduzibel ist.

   Hinweis: Da $p$ primitiv ist, kann man aus $p$ nicht die Wurzel ziehen, d. h., es gibt kein $\alpha \in GF(9)$, so dass $\alpha^2 = p$ gilt.

## Tutoraufgabe 3

1. Seien $K$ ein Körper und $p \in K[x]$ ein Polynom über $K$ mit Unbestimmter $x$ vom Grad 1. Man zeige, dass die Restklassenalgebra $K[x]/(p)$ isomorph zu $K$ ist.
2. Gegeben sei das Polynom $p(x) = x^2 + 1$ über dem Körper der reellen Zahlen $\mathbb{R}$. Man zeige:

   (a) $p(x)$ ist irreduzibel in $\mathbb{R}[x]$.

   (b) Die Restklassenalgebra $\mathbb{R}[x]/(p)$ ist isomorph zum Körper $\mathbb{C}$ der komplexen Zahlen.