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

Wintersemester 2010/11
Übungsblatt 9
14. Dezember 2010

Diskrete Strukturen

Abgabetermin: 21. Dezember 2010, 10 Uhr in die **DS Briefkästen**

Hausaufgabe 1 (5 Punkte)

Sei G eine Gruppe mit e als neutralem Element, $g \in G$ mit $\text{ord}(g) < \infty$. Zeigen Sie:

1. Für $d > 0$ gilt:

$$d = \text{ord}(g) \quad \Leftrightarrow \quad g^d = e \text{ und für jedes } n > 0 \text{ mit } g^n = e \text{ gilt } d|n\,.$$

2. Für $n > 0$ gilt:

$$\text{ord}(g^n) = \frac{\text{ord}(g)}{\text{ggT}(\text{ord}(g), n)}\,.$$

Hausaufgabe 2 (5 Punkte)

Seien $G = \langle S, \circ, e\rangle$ eine Gruppe mit neutralem Element e und $U = \{x \in S\,;\, x^2 = e\}$.
Man zeige:

1. $\langle U, \circ\rangle$ ist eine Untergruppe von G.
2. Falls $U = S$ gilt, dann ist G abelsch.

Hausaufgabe 3 (5 Punkte)

Sei n eine Primzahl. Wir betrachten den Körper $K_n = \langle \mathbb{Z}_n, +_n, \cdot_n, 0, 1\rangle$.

1. Sei $U = \{x \in \mathbb{Z}_n \backslash \{0\}\,;\, x \cdot_n x = 1\}$. Man zeige: $U = \{1, n-1\}$.
2. Man zeige: $(n-1)! \equiv -1 \pmod{n}$.
   Beachten Sie die Schreibweise für die Fakultätsfunktion, d.h. $m! = \prod_{i=1}^{m} i$.

Hausaufgabe 4 (5 Punkte)

Man schreibe die folgende Permutation $\sigma \in S_{14}$ als Produkt von paarweise disjunkten Zyklen:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 4 & 6 & 8 & 10 & 12 & 14 & 1 & 3 & 5 & 7 & 9 & 11 & 13 \end{pmatrix}.$$

Welche Ordnung besitzt σ?

Hinweis: *Auf den Übungsblättern in diesem Semester wird es grundsätzlich die drei Aufgabentypen Vorbereitungsaufgabe, Tutoraufgabe und Hausaufgabe geben. Die als Vorbereitung bezeichneten Aufgaben dienen der häuslichen Vorbereitung der Tutoraufgaben. Tutoraufgaben werden in den Übungsgruppen bearbeitet. Dabei wird die Lösung der Vorbereitungsaufgaben vorausgesetzt. Die Vorbereitungsaufgaben werden in der Zentralübung unterstützt.*

Vorbereitung 1

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 $R_{\text{grad}(b)}$ aller Polynome $r(x) \in \mathbb{Z}_5[x]$ mit $\text{grad}(r) < \text{grad}(b)$?
2. Bestimmen Sie Polynome $q(x), r(x) \in \mathbb{Z}_5[x]$, so dass gilt $a(x) = q(x) \cdot b(x) + r(x)$ mit $\text{grad}(r) < 2$.

Vorbereitung 2

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

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 3

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

Tutoraufgabe 1

Bestimmen Sie mit dem erweiterten Euklidschen Algorithmus einen größten gemeinsamen Teiler der Polynome $x^5 - 5x^4 + 4x^3 + 2x^2 - 12x + 10$ und $x^2 - 1$. Die Polynome werden im Ring $Q[x]$ betrachtet.

Tutoraufgabe 2

Sei $\pi(x) = x^3 + 1$. Wir betrachten den Ring $R = \langle \mathbb{Z}_2[x]_3, +_{\pi(x)}, \cdot_{\pi(x)} \rangle$. 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: $p \in Z_2[x]_3$ mit $\text{grad}(p) \neq 0$ heißt Nullteiler, falls es ein $q \in Z_2[x]_3$ mit $\text{grad}(q) \neq 0$ gibt, so dass gilt $p \cdot_{\pi(x)} q = 0$.

Tutoraufgabe 3

Irreduzible Polynome über endlichen Körpern spielen in mannigfacher Weise eine bedeutende Rolle. Wir wollen uns einen Überblick verschaffen über die Menge aller irreduziblen Polynome über Z_2 höchstens vom Grad 5.

1. Versuchen Sie zunächst durch möglichst weitreichende hinreichende Bedingungen für die Reduzibilität der betreffenden Polynome die gesuchte Menge möglichst einzuschränken.

2. Für die verbleibende Menge von Polynomen entwerfe man einen systematischen Test auf Irreduzibilität. Führen Sie diesen Test aus.

   Welche Kardinalität besitzt die gesuchte Menge?