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

Wintersemester 2011/12
Übungsblatt 8
5. Dezember 2011

Diskrete Strukturen

Abgabetermin: 13. Dezember 2011, 14 Uhr in die **DS Briefkästen**

Hausaufgabe 1 (5 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 $A = \langle S, \circ \rangle$ 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 (3 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?

Hausaufgabe 3 (4 Punkte)

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

1. Sei $U = \{x \in \mathbb{Z}_n \setminus \{0\} \, ; \, x \cdot_n x = 1\}$. 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 (3 Punkte)

Berechnen Sie mit Hllfe des erweiterten Euklidischen Algorithmus ganze Zahlen a, b, so dass

$$a \cdot 53 + b \cdot 36 = 2 .$$

Hausaufgabe 5 (5 Punkte)

Wir betrachten die multiplikative Gruppe $\langle \mathbb{Z}^*_{1000}, \cdot_{1000}, 1\rangle$ mit
$\mathbb{Z}^*_{1000} = \{x \in \mathbb{N}\,;\, x < 1000 \text{ und } \mathrm{ggT}(1000, x) = 1\}$.

1. Führen Sie den Euklidschen Algorithmus aus, um den größten gemeinsamen Teiler von 1000 und 69 zu berechnen. Protokollieren Sie die Berechnungsschritte.

2. Berechnen Sie auf der Grundlage Ihres Protokolls der Berechnung des $\mathrm{ggT}(1000, 69)$ Zahlen $a, b \in \mathbb{Z}$, so dass gilt

$$a \cdot 1000 + b \cdot 69 = \mathrm{ggT}(1000, 69)\,.$$

3. Es gilt $69 \in \mathbb{Z}^*_{1000}$. Bestimmen Sie in der multiplikativen Gruppe $\langle \mathbb{Z}^*_{1000}, \cdot_{1000}, 1\rangle$ das Inverse $(69)^{-1}$ von 69.

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

1. Sei $p(x) \in \mathbb{C}[x]$ ein Polynom vom Grad $n-1$ mit den Koeffizienten $\vec{a} = (a_0, a_1, \ldots, a_{n-1})$, d. h.
$$p(x) = P_{\vec{a}}(x)\,.$$
Wir betrachten speziell $n = 8$, $\vec{a} = (1,1,1,1,1,1,1,1)$ und $\omega = e^{\frac{2\pi i}{8}}$.
Berechnen Sie die Fouriertransformierte
$$\mathcal{F}_{n,\omega}(\vec{a}) = (P_{\vec{a}}(1), P_{\vec{a}}(\omega), \ldots, P_{\vec{a}}(\omega^{n-1}))$$
auf zwei verschiedene Arten:
   i) Durch Ausführung des Divide-and-Conquer Algorithmus $\texttt{DFT}(\vec{a}, \omega)$.
   ii) Durch direkte Berechnung unter Ausnutzung der Formel
$$x^n - 1 = (x^{n-1} + \ldots + x^2 + x + 1)(x-1)\,.$$
2. Durch welche Matrix kann die Fouriertransformation $\mathcal{F}_{8,e^{\frac{2\pi i}{8}}}$ dargestellt werden?

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

Tutoraufgabe 3

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.