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

Wintersemester 2012/13
Übungsblatt 8
3. Dezember 2012

Diskrete Strukturen

Abgabetermin: 11. Dezember 2012, 14 Uhr in die **DS Briefkästen**

Hausaufgabe 1 (4 Punkte)

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

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

2. Für $n > 0$ gilt:
$$\operatorname{ord}(g^n) = \frac{\operatorname{ord}(g)}{\operatorname{ggT}(\operatorname{ord}(g), n)}\,.$$

Hausaufgabe 2 (2 Punkte)

Man schreibe die folgende Permutation $\sigma \in S_{14}$ als Produkt von paarweise disjunkten Zyklen:
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 2 & 8 & 6 & 1 & 10 & 12 & 14 & 4 & 3 & 5 & 7 & 9 & 11 & 13 \end{pmatrix}\,.$$
Welche Ordnung besitzt σ?

Hausaufgabe 3 (4 Punkte)

Wir betrachten die Symmetrische Gruppe S_n aller Permutationen einer Teilmenge $[n]$ der natürlichen Zahlen mit der Komposition von Abbildungen als Gruppenverknüpfung.

1. Falls S_n zyklisch ist, dann gilt $n \leq 2$. Beweis!

2. Bestimmen Sie die größte Zahl k mit der Eigenschaft, dass es ein Element $p \in S_7$ gibt mit der Ordnung k, d. h. $\operatorname{ord}(p) = k$.

   Begründen Sie Ihre Herleitung und geben Sie eine entsprechende Permutation p an.

Hausaufgabe 4 (3 Punkte)

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

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 5 (4 Punkte)

Wir betrachten die Gruppen $G = (\mathbb{Z}_6, +_6, 0)$ und $H = (\mathbb{Z}_9^*, \cdot_9, 1)$, wobei $\mathbb{Z}_n = \{0, \ldots, n-1\}$ und $\mathbb{Z}_n^* = \{p \in \mathbb{Z}_n; ggT(n,p) = 1\}$ gilt. Die Verknüpfungen $+_n$ und $\cdot_n$ bezeichnen die Addition bzw. die Multiplikation modulo n.

1. Geben Sie die Mengen $\mathbb{Z}_6$ und $\mathbb{Z}_9^*$ extensional an und bestimmen Sie zu jedem Element aus G und H jeweils das entsprechende Inverse bezglüglich $+_6$ bzw. $\cdot_9$.

2. Geben Sie zu jedem Element aus G und H jeweils die Ordnung an und begründen Sie kurz, wieso G und H isomorph sind.

3. Zwischen G und H existiert ein Isomorphismus $h : \mathbb{Z}_6 \to \mathbb{Z}_9^*$ mit $h(1) = 5$. Bestimmen Sie $h(0), h(2), h(3), h(4)$ und $h(5)$.

Hausaufgabe 6 (3 Punkte)

Begründen Sie Ihre Antwort auf die folgenden Fragen:

1. Welche Charakteristik besitzt der Körper $\mathbb{Z}_7$? Welche Ordnung besitzt 2 in der additiven Gruppe von $\mathbb{Z}_7$?

2. Welche primitiven Elemente besitzt der Körper $\mathbb{Z}_7$?

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

Vorbereitung 1

Wir betrachten den Körper $\mathbb{C}$ der komplexen Zahlen. Es sei $i \in \mathbb{C}$ mit $i^2 = -1$.

1. Zeigen Sie, dass für jedes $n \in \mathbb{N}$ die komplexe Zahl $e^{\frac{2\pi i}{n}}$ eine multiplikative Untergruppe W_n von $\mathbb{C}$ erzeugt, die isomorph ist zu $\mathbb{Z}_n$.

2. Stellen Sie W_n in der Gaußchen Zahlenebene dar und machen Sie sich klar, was in Ihrer Darstellung die Multiplikation in W_n bedeutet.

Vorbereitung 2

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 $n = 8$, $\vec{a} = (2, 1, 2, 1, 2, 1, 2, 1)$ und $\omega = e^{\frac{2\pi i}{8}}$.
Berechnen Sie die Fouriertransformierte

$$\mathcal{F}_{n,\omega}(\vec{a}) = (P_{\vec{a}}(1), P_{\vec{a}}(\omega), \ldots, P_{\vec{a}}(\omega^{n-1}))$$

durch Ausführung des Divide-and-Conquer Algorithmus $\texttt{DFT}(\vec{a}, \omega)$.

Tutoraufgabe 1

Wir betrachten Polynome $p(x), q(x) \in \mathbb{Q}[x]$, d. h. Polynome p, q in einer Unbestimmten (Variablen) x und Koeffizienten aus dem Körper $\mathbb{Q}$ der rationalen Zahlen mit

$$\begin{aligned} p(x) &= x^5 - 3x^4 + 3x^3 - 9x^2 + 2x - 6\,, \\ q(x) &= x^3 + 3x^2 + x + 3\,. \end{aligned}$$

1. Berechnen Sie mit dem Euklidischen Algorithmus ein Polynom möglichst hohen Grades, das sowohl Teiler von $p(x)$ als auch Teiler von $q(x)$ ist ($\mathrm{ggT}(p, q)$).

2. Die Abbildung $m : \mathbb{Z} \to \mathbb{Z}_2$ sei gegeben durch $m(x) := x \bmod 2$. Dann erhalten wir aus $p(x)$ das Polynom

   $$\hat{p}(x) = m(1)x^5 + m(-3)x^4 + m(3)x^3 + m(-9)x^2 + m(2)x + m(-6)\,.$$

   Stellen Sie $\hat{p}$ im Ring $\mathbb{Z}_2[x]$ als Produkt einer geeigneten Anzahl von Linearfaktoren $x - \alpha_i$, mit geeigneten Konstanten $\alpha_1, \alpha_2, \ldots$ dar.

Tutoraufgabe 2

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 `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?