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

Wintersemester 2010/11
Übungsblatt 8
6. Dezember 2010

Diskrete Strukturen

Abgabetermin: Keine Abgabe der Hausaufgaben

Hausaufgabe 1 (0 Punkte)

1. Berechnen Sie $(10^{117} + 5^{27} - 30^{1000}) \mod 3$.
2. Bestimmen Sie $2^{7333333100} \mod 12$.

Hausaufgabe 2 (0 Punkte)

Die Menge der Permutationen der Teilmenge $\{1, 2, 3, 4\}$ der natürlichen Zahlen bildet zusammen mit der Komposition $\circ$ von Abbildungen die Gruppe $\mathcal{S}_4$. Das neutrale Element der Gruppe sei id. Wir betrachten die in Zyklusschreibweise gegebenen Permutationen

$$p = (1\ 2)(3)(4) \qquad \text{und} \qquad q = (1)(2)(3\ 4)\,.$$

1. f heißt involutorisch, falls $f \circ f = id$ gilt. Zeigen Sie, dass p und q involutorisch sind.
2. Zeigen Sie, dass $p \circ q = q \circ p$ gilt.

Seien $r = p \circ q$ und $U = \{id, p, q, r\}$.

3. Geben Sie die $\circ$-Verknüpfungstafel für die Elemente aus U an.
4. Beweisen Sie, dass die Menge U mit jedem Element $x \in U$ auch sein Inverses x^{-1} enthält (mit $x \circ x^{-1} = id$).

Hausaufgabe 3 (0 Punkte)

Wir betrachten Algebren $A = \langle S, \circ \rangle$ mit einer 2-elementigen Trägermenge $S = \{a, b\}$ und einem 2-stelligen Operator $\circ$. Bekanntlich gibt es 16 verschiedene Algebren dieser Art, auf die wir uns im Folgenden beziehen.

1. Geben Sie eine Verknüpfungstafel für einen nicht assoziativen und gleichzeitig nicht kommutativen Operator $\circ$ an.
2. Zeigen Sie, dass es genau zwei kommutative und gleichzeitig nicht assoziative Operatoren $\circ$ gibt.
3. Geben Sie alle Booleschen Operatoren an, die kommutativ und gleichzeitig nicht assoziativ sind?

Hausaufgabe 4 (0 Punkte)

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

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

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

Mit $R = \mathbb{Z}_3[x]$ bezeichnen wir den Ring aller Polynome über einer Variablen x mit Koeffizienten aus dem Körper $\langle \mathbb{Z}_3, +_3, \cdot_3 \rangle$ der ganzen Zahlen modulo 3.
Seien $a(x), b(x) \in R$ gegeben durch

$$\begin{aligned} a(x) &= x^6 + 2x^4 + 2x^3 + x^2 + 1\,, \\ b(x) &= x^3 + x^2 + 1\,. \end{aligned}$$

1. Bestimmen Sie Polynome $r_2(x), r_3(x), q_1(x), q_2(x) \in R$ mit $\mathrm{grad}(r_3(x)) < \mathrm{grad}(r_2(x)) < \mathrm{grad}(b(x))$, so dass die folgenden Gleichungen gelten.

$$\begin{aligned} r_2(x) &= a(x) - q_1(x) \cdot b(x)\,, \\ r_3(x) &= b(x) - q_2(x) \cdot r_2(x)\,. \end{aligned}$$

2. Bestimmen Sie ein Polynom $t(x) \in R$ möglichst hohen Grades, das ein gemeinsamer Teiler von $a(x)$ und $b(x)$ ist.

Vorbereitung 2

Bestimmen Sie Polynome $a(x),\ b(x) \in \mathbb{Q}[x]$, so dass gilt

$$\frac{x^2 + x}{(x^2+1)(x^2+2)} = \frac{a(x)}{x^2+1} + \frac{b(x)}{x^2+2}\,.$$

Vorbereitung 3

Wir betrachten den Körper $\mathbb{C}$ der komplexen Zahlen. Es sei $i \in \mathbb{C}$ mit $i^2 = -1$.
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 $\mathbb{Z}_n$.
Stellen Sie W_n in der Gaußchen Zahlenebene dar und machen Sie sich klar, was in Ihrer Darstellung die Multiplikation in W_n bedeutet.

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 Euklidschen 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

Gegeben sei der Bruch $f(x) = \frac{p(x)}{q(x)}$ mit den Polynomen $p(x), q(x) \in \mathbb{C}[x]$,

$$p(x) = 3x^3 - 52x + 16 \quad \text{und} \quad q(x) = x^4 - x^3 - 8x^2 - 4x - 48\,.$$

1. Man bestimme einen größten gemeinsamen Teiler $r(x)$ von $p(x)$ und $q(x)$ und dividiere Zähler und Nenner von $f(x)$ durch $r(x)$. Das Ergebnis nennen wir den vollständig gekürzten Bruch $F(x)$.

2. Bestimmen Sie die vollständige Partialbruchzerlegung von $F(x)$, d. h., berechnen Sie $\alpha, \beta, \gamma, A, B, C \in \mathbb{C}$ so, dass gilt

   $$F(x) = \frac{A}{x + \alpha} + \frac{B}{x + \beta} + \frac{C}{x + \gamma}\,.$$

Tutoraufgabe 3

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?