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

Sommersemester 2011
Übungsblatt 4
5. September 2011

Diskrete Strukturen

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

Hausaufgabe 1 (4 Punkte)

Wir fassen die aussagenlogischen Werte t (wahr) und f (falsch) zur booleschen Menge $\mathbb{B} = \{t, f\}$ zusammen und betrachten den aussagenlogischen Operator $\otimes : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ des „ausschließenden Oder“ (gleichbedeutend mit $\not\equiv$).

1. Zeigen Sie die Kommutativität und die Assoziativität von $\otimes$, d.h. $x \otimes y \equiv y \otimes x$ und $(x \otimes y) \otimes z \equiv x \otimes (y \otimes z)$ für alle $x, y, z \in \mathbb{B}$, durch Auswertung der entsprechenden Wahrheitswerttabellen.

2. Wir betrachten die Algebra $A = \langle \mathbb{B}, \otimes \rangle$. Geben Sie einen Isomorphismus f von A auf Z_2 an und beweisen Sie die entsprechende Homomorphieeigenschaft für f.

   Warum folgt bereits aus der Existenz des Isomorphismus f die Kommutativität und Assoziativität der Verknüpfung $\otimes$? Beweis!

Hausaufgabe 2 (5 Punkte)

Wahr oder falsch? Beweisen Sie Ihre Antworten.

1. $-7 \equiv 8 \ (mod\ 5)$.
2. $2^{16} \bmod 3 = 2, \quad 2^{33} \bmod 3 = 2, \quad 2^{1600} \bmod 3 = 1$.
3. Für alle $n \in \mathbb{N}$ gilt $\quad n^2 \bmod (n + 1) = 1$.
4. Für alle $n \in \mathbb{N}$ gilt $\quad (n \bmod 2) \bmod 7 = (n \bmod 7) \bmod 2$.
5. Sei $\div$ die ganzzahlige Division. Dann gilt $\quad (-10) \div 4 = 3$.

Hausaufgabe 3 (4 Punkte)

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

Hausaufgabe 4 (4 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 5 (5 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 6 (4 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. Sei G abelsch. Dann ist $\langle U, \circ \rangle$ eine Untergruppe von G.
2. Falls $U = S$ gilt, dann ist G abelsch.

Hausaufgabe 7 (4 Punkte)

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

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

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

Beweisen Sie:

1. Es gibt bis auf Isomorphie genau einen Ring $R = \langle S, \oplus, \odot, 0, 1\rangle$ mit drei Elementen, d. h. $S = \{0, 1, a\}$. Insbesondere also muss R isomorph sein zum Ring $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1\rangle$.

2. Der Ring $R = \langle S, \oplus, \odot, 0, 1\rangle$ mit drei Elementen ist ein Körper.

3. Sei t_x die Anzahl der *co*-Nullteiler eines Ringelementes $x \in S \setminus \{0\}$ eines endlichen, kommutativen Ringes $\langle S, \oplus, \odot, 0, 1\rangle$.

   Dann ist $t_x + 1$ ein Teiler der Anzahl $n = |S|$ aller Ringelemente.

   Dabei heiße $y \in S \setminus \{0\}$ *co*-Nullteiler von $x \in S \setminus \{0\}$, falls $x \odot y = 0$.

Vorbereitung 2

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 3

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 4

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 5

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 $[f]_g \to Rem_g(f)$ 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 6

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 7

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 $\mathbb{Q}[x]$ betrachtet.

Tutoraufgabe 1

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 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 $\mathtt{DFT}(\vec{a}, \omega)$.

   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 3

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