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

Wintersemester 2005
Übungsblatt 6
29. November 2005

Diskrete Strukturen

Abgabetermin: 2. Dezember 2005 **vor** *der Vorlesung*

Aufgabe 1

Wir betrachten die ganzzahlige Division $a \div b$ zweier Zahlen $a \in \mathbb{Z}, b \in \mathbb{N}$ und die zugehörige modulo-Operation $a \bmod b$, für die gilt

$$a = (a \div b) \cdot b + (a \mod b)\,,$$

mit $0 \leq a \bmod b < b$.

1. Zeigen Sie für alle $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$

$$\begin{aligned}(a+b) \mod m &= [(a \mod m) + (b \mod m)] \mod m\,,\\ (a \cdot b) \mod m &= [(a \mod m) \cdot (b \mod m)] \mod m\,,\\ a &\equiv (a \mod b) \mod b\,.\end{aligned}$$

2. Berechnen Sie $(10^{17} + 5^{23} - 30^{100}) \bmod 3$!

3. Berechnen Sie $7^{999999} \bmod 11$ und $2^{7346790100} \bmod 12$!

   Benutzen Sie, wenn möglich, den kleinen Satz von Fermat.

Aufgabe 2

1. Zeigen Sie: Die Menge aller Elemente endlicher Ordnung in einer abelschen Gruppe bildet eine Untergruppe.

2. Zeigen Sie: In einem beliebigen Ring $\langle R, +, \cdot, 0, 1\rangle$ gelten die folgenden Gleichungen.

$$\begin{aligned}a \cdot 0 &= 0 \cdot a = 0\,,\\ a \cdot (-b) &= (-a) \cdot b = -a \cdot b\,.\end{aligned}$$

3. Zeigen Sie, dass der Ring $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1\rangle$ ein Körper ist.

4. Die Charakteristik eines Körpers K, i. Z. $char(K)$, ist definiert als die Ordnung des Elements 1 in der additiven Gruppe von K. Man zeige:

$$p = char(K) \in \mathbb{N} \Rightarrow p \text{ ist eine Primzahl}\,.$$

5. Geben Sie die Verknüpfungstafeln eines Körpers mit 4 Elementen an. Welche Charakteristik hat dieser Körper?

   Begründen Sie Ihre Angaben!

Aufgabe 3

In gewissen kommutativen Ringen $R = \langle S, +, \cdot, 0, 1\rangle$ stellt sich der erweiterte Euklidsche Algorithmus zur Berechnung des größten gemeinsamen Teilers $ggT(a, b)$ zweier Elemente $a \in S$ und $b \in S$ dar als eine iterierte Transformation (Matrixmultiplikation) Q_i angewandt auf Δ_{i-1} wie folgt.

$$\Delta_0 = \begin{pmatrix} a \\ b \end{pmatrix}\,,\ \Delta_i = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = Q_i\Delta_{i-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}\,,\ i := 1, 2, \ldots, n \in \mathbb{N}\,.$$

Dabei werden die Quotienten q_i so gewählt (geschätzt), dass die Δ_i mit wachsendem i in einem gewissen Sinn stets echt kleiner werden. Eine Berechnung wird beendet, wenn die Folge der Δ_i maximale Länge besitzt, d. h. wenn kein Quotient existiert, der die Bildung eines noch kleineren Restes erlaubt. Zur Bemessung der Größe von Elementen eines Ringes dient beispielweise im Ring der ganzen Zahlen $\langle \mathbb{Z}, +, \cdot, 0, 1\rangle$ die Betragsfunktion. In Polynomringen wird der Grad eines Polynoms verwendet.
Wir betrachten im Folgenden den Ring $\langle \mathbb{Z}, +, \cdot, 0, 1\rangle$ der ganzen Zahlen.

1. Zeigen Sie für alle ensprechenden i

$$ggT(a, b) = ggT(r_i, r_{i+1}).$$

2. Berechnen Sie mit dem Euklidschen Algorithmus den $ggT(10800, 122)$.

3. Berechnen Sie mit dem erweiterten Euklidschen Algorithmus ganze Zahlen m, n, so dass

$$81m + 128n = 1.$$

4. 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.

Aufgabe 4

Wir betrachten im Folgenden den Ring $\langle \mathbb{Z}, +, \cdot, 0, 1\rangle$ der ganzen Zahlen.
Sei A eine nichtleere, endliche Teilmenge von $\mathbb{Z} \setminus \{0\}$. Dann definieren wir den größten gemeinsamen Teiler aller Elemente von A, i. Z. $ggT(A)$, als diejenige natürliche Zahl g für die gilt:
g ist Teiler aller $a \in A$ und jedes $g' \in \mathbb{N}$, das alle Elemente von A teilt, teilt auch g.

1. Seien A, B nichtleere, endliche Teilmengen von $\mathbb{Z} \setminus \{0\}$. Beweisen Sie

$$ggT(A \cup B) = ggT(ggT(A), ggT(B))\,.$$

   Zeigen Sie zunächst, dass $ggT(A)$ (bzw. $ggT(B)$) stets existiert.

2. Entwerfen Sie ein Verfahren zur Berechnung des $ggT(A)$ für endliche Mengen ganzer Zahlen auf der Basis des Euklidschen Algorithmus.

3. Sei $A = \{a_1, a_2, \ldots, a_n\}$. Entwerfen Sie ein Verfahren zur Berechnung ganzer Zahlen $m_1, m_2, \ldots, m_n$, so dass

$$ggT(A) = m_1a_1 + m_2a_2 + \ldots + m_na_n\,.$$