Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Ernst W. Mayr

WS 2003/04
Übungsblatt 5
21. November 2003

Diskrete Strukturen I

Abgabe bis Donnerstag, 27. November 2003, 12:15 Uhr (in Stellordner vor Raum 03.09.052)

Aufgabe 1

Zeigen Sie, dass $\mathbb{Z}_2$ ein Körper ist.

Aufgabe 2

Bei der Übertragung von Daten verwendet man zur Fehlererkennung häufig CRC-Prüfsummen (Cyclic Redundancy Check). Dabei interpretiert man die bitweise Darstellung der Nachricht als Folge der Koeffizienten eines Polynoms $a(x)$. An diese Folge möchte man k weitere (Prüf-)Bits anhängen (die einem Polynom $p(x)$ entsprechen), so dass das entstehende Polynom $b(x)$ durch ein festgelegtes Generatorpolynom $g(x)$ ohne Rest teilbar ist.
Es soll also gelten: $b(x) = a(x)x^k + p(x)$, sowie $b(x) = t(x)g(x)$.
Man kann daher die Prüfziffern berechnen, indem man den Rest einer Polynomdivision über $\mathbb{Z}_2$ von $a(x)x^k$ durch $g(x)$ bestimmt.
Auf der Empfängerseite kann man Übertragungsfehler feststellen, indem man die empfangene Bitfolge ebenfalls als Polynom $b'(x)$ interpretiert und überprüft, ob sich $b'(x)$ durch $g(x)$ ohne Rest teilen läßt.

a) Berechnen Sie die Prüfsumme für die Bitfolge 101001 (also $a(x) = x^5 + x^3 + 1$) und das Generatorpolynom $g(x) = x^3 + x + 1$ mit $k = 3$.

b) Bei einer weiteren Übertragung wurde das gleiche Generatorpolynom benutzt. Der Empfänger erhielt die Bitfolge 100101111. Stellen Sie fest, ob bei der Übertragung ein Fehler aufgetreten ist.

c) Kann man auf der Empfängerseite aus einer Teilbarkeit von $b'(x)$ durch $g(x)$ mit Sicherheit schlußfolgern, dass kein Übertragungsfehler aufgetreten ist?

Aufgabe 3

Die Möbiusfunktion $\mu : \mathbb{N} \to \mathbb{Z}$ ($\mathbb{N} = \{1, 2, \ldots\}$) ist wie folgt definiert: $\mu(1) = 1$ und für $1 < n \in \mathbb{N}$ sei

$$\mu(n) = \begin{cases} (-1)^r, & \text{falls } n = p_1 \cdots p_r \text{ mit paarweise verschiedenen Primzahlen } p_i \\ 0, & \text{falls } n \text{ nicht quadratfrei ist.} \end{cases}$$

Dabei heißt n *quadratfrei*, wenn $p^2 \nmid n$ (d.h. p^2 teilt nicht n) für jede Primzahl p gilt. Zeigen Sie:

a) Für alle $n > 1$ gilt $\sum_{d|n} \mu(d) = 0$.

b) Sei $f : \mathbb{N} \to \mathbb{C}$ eine Funktion und

$$F(n) := \sum_{d|n} f(d) \qquad (n \in \mathbb{N})$$

ihre summatorische Funktion. Dann gilt

$$f(N) = \sum_{d|N} \mu(d) F(\frac{N}{d}) \qquad (N \in \mathbb{N}).$$

(Bem.: Insbesondere gilt der Möbiussche Umkehrsatz: $\varphi(n) = \sum_{d|n} d\mu(n/d)$, wobei φ die Eulersche φ-Funktion ist.)

Aufgabe 4

Sei $R = \mathbb{Q}[x]$ der Polynomring über $\mathbb{Q}$ in der Unbestimmten x. Zu $f_0, \ldots, f_s \in R$ bezeichne $\mathrm{ggT}(f_0, \ldots, f_s)$ den größten gemeinsamen Teiler von $f_0, \ldots, f_s$ in R.

a) Zeigen Sie, dass $\mathrm{ggT}(f_0, \ldots, f_s) = \mathrm{ggT}(\mathrm{ggT}(f_0, \ldots, f_{s-1}), f_s)$ gilt.

b) Mit Hilfe des erweiterten euklidischen Algorithmus kann man Polynome $g_0, \ldots, g_s \in R$ berechnen, so dass gilt:

$$\mathrm{ggT}(f_0, \ldots, f_s) = g_0 f_0 + \ldots + g_s f_s.$$

Für den Fall $s = 1$ soll dies nun explizit gezeigt werden. Man führt solange sukzessive Polynomdivision mit Rest durch ($p_0 = f_0,\ p_1 = f_1$)

$$p_{i-1} = q_i f_i + p_{i+1}, \qquad i = 1, \ldots, n$$

bis der Rest 0 bleibt, d.h. $p_{n+1} = 0$ und $p_n \neq 0$ gilt.

1. Zeigen Sie, dass $p_n = \mathrm{ggT}(f_0, f_1)$ gilt.
2. Bestimmen Sie eine Matrix Q_i ($i = 1, \ldots, n$), so dass gilt:
$$\begin{pmatrix} p_i \\ p_{i+1} \end{pmatrix} = Q_i \begin{pmatrix} p_{i-1} \\ p_i \end{pmatrix}.$$
3. Bestimmen Sie nun eine Matrix Q, so dass gilt:
$$\begin{pmatrix} p_n \\ p_{n+1} \end{pmatrix} = Q \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}.$$
4. Wie erhält man aus Q die Polynome g_0, g_1, so dass $\mathrm{ggT}(f_0, f_1) = g_0 f_0 + g_1 f_1$ gilt?
5. Erläutern Sie, wie man im allgemeinen Fall die Polynome $g_0, \ldots, g_s$ berechnen kann!