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

WS 2003/04
Übungsblatt 6
28. November 2003

Diskrete Strukturen I

Abgabe bis Donnerstag, 4. Dezember 2003, 12:15 Uhr (in Stellordner vor Raum 03.09.052)

Aufgabe 1

Eine wichtige Operation (z.B. für die Implementation von Primzahltests, die bei der Kryptographie eine Rolle spielen) ist die Bestimmung von Potenzen $a^k \mod n$. Dieser Wert läßt sich mit Hilfe der Binärdarstellung von k durch sukzessives Quadrieren sehr schnell berechnen, z.B. $a = 43, k = 50 = (110010)_2, n = 67$:

$$43^{50} \equiv (((((43^2) \cdot 43)^2 \cdot 1)^2 \cdot 1)^2 \cdot 43)^2 \cdot 1 \mod 67$$

Damit die Zahlen nicht zu groß werden, wird dabei nach jeder Operation (Quadrieren bzw. Multiplizieren) der Modulus berechnet.

a) Berechnen Sie den Wert des Polynoms $5 \cdot x^{107} - 1$ über dem Ring $\langle \mathbb{Z}_{13}, +_{13}, \cdot_{13} \rangle$ an der Stelle $x = 7$.

b) Wieviele Multiplikationen braucht man im Allgemeinen höchstens für die Bestimmung einer Potenz (ohne Koeffizient)?

c) Wieviele Multiplikationen braucht man, wenn man das Horner-Schema anwendet?

Aufgabe 2

Stellen Sie mit Hilfe einer Partialbruchzerlegung den Bruch $\frac{x^2+3x-5}{x^3-2x^2-5x+6}$ in der Form

$$\frac{A}{x+2} + \frac{B}{x-1} + \frac{C}{x-3}$$

dar!

Aufgabe 3

Bestimmen Sie einen größten gemeinsamen Teiler der beiden Polynome

$$4x^4 + 12x^3 - 3x^2 + 3x - 1 \qquad \text{und} \qquad 3x^3 + 11x^2 + 3x - 2$$

(also ein Polynom mit größtmöglichem Grad, das beide Polynome teilt).

Aufgabe 4

Sei $n = 4$. Dann ist $\omega = i = \sqrt{-1}$ eine primitive n-te Einheitswurzel.

a) Bestimmen Sie die (komplexzahligen) Einträge der Fouriermatrix F mit

$$F_{k,l} = \omega^{k \cdot l}, \qquad k, l \in \{0 \dots n-1\}.$$

b) Was kann man über die Spalten der Fouriermatrix aussagen?

c) Sei a der Vektor, der die Koeffizienten des Polynoms enthält. Führen Sie die Diskrete Fouriertransformation $b = f(a) = F \cdot a$ für den folgenden Vektor durch:
$a = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$

d) Berechnen Sie die inverse Fouriermatrix F^{-1} mit den (ebenfalls komplexenwertigen) Elementen $F^{-1}_{k,l} = \omega^{-k \cdot l}/n, \qquad k, l \in \{0 \dots n-1\}$

e) Berechnen Sie die inverse Fouriertransformation $c = F^{-1} \cdot b$ des Vektors b.
Welche Komplexität bezüglich n hat die Fouriertransformation *in dieser Form*?