Computeralgebra

WS 2001/2002
Prof. Dr. K. Madlener
Übungsblatt 3

Aufgabe 3.1
Sei $n \in \mathbb{N}^+$. Eine Additionskette für n ist eine endliche Folge positiver ganzer Zahlen $a_0, \ldots, a_r$ mit $a_0 = 1$, $a_r = n$, und für alle $i = 1, \ldots, r$ gibt es j und k mit $k \leq j < i$, so dass $a_i = a_j + a_k$; r bezeichnen wir als die Länge der Additionskette. Es bezeichne weiter $l(n)$ die minimale Länge einer Additionskette für n.

a) Welcher Zusammenhang besteht zwischen $l(n)$ und der Berechnung von x^n? Ist die Anzahl der Multiplikationen der binären Potenzierungsmethode zur Berechnung von x^n immer minimal?

b) Sei $s(n)$ die Summe der Bits in der Binärdarstellung von n (also die Anzahl der Einsen). Zeigen Sie: $l(n) \leq \lfloor \log_2 n \rfloor + s(n) - 1$ und $l(mn) \leq l(m) + l(n)$.

c) Seien $a > b \geq 0$ ganze Zahlen. Zeigen Sie, dass $l(2^a) = a$ und $l(2^a + 2^b) = a + 1$.

Aufgabe 3.2

a) Wir wollen die Fibonacci-Zahlen F_k modulo $n \in \mathbb{N}$ berechnen. Geben Sie eine asymptotische obere Schranke für die Anzahl der Bitoperationen eines naiven Verfahrens zur Berechnung von F_k modulo n im schlechtesten Fall an.

Ein anderes Verfahren benutzt die Tatsache, dass F_{k+1} sich wie folgt gewinnen lässt:

$$\begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix} = \begin{pmatrix} F_k & F_{k-1} \\ F_{k-1} & F_{k-2} \end{pmatrix} \cdot X,$$

wobei X von Ihnen anzugeben ist. Konkretisieren Sie nun dieses Verfahren zur Berechnung von F_k modulo n und geben Sie ebenfalls eine asymptotische obere Schranke für die Anzahl der Bitoperationen im schlechtesten Fall an.

b) Zeigen Sie, wie man $1 + x + \cdots + x^{n-1} \pmod{m}$ für $x, n, m \in \mathbb{N}^+$ mit $O(\lambda(n)\lambda(m)^2)$ Bitoperationen im schlechtesten Fall berechnet. Beachten Sie besonders den Fall, dass m keine Primzahl ist.

Aufgabe 3.3
Finden Sie „einfachste“ Ausdrücke, die äquivalent zu den folgenden Ausdrücken sind:

- $a(x,y) = \dfrac{1}{x^9 + x^8y + x^7y^2 + x^6y^3 + x^5y^4 + x^4y^5 + x^3y^6 + x^2y^7 + xy^8 + y^9}$

- $b(x,y) = \dfrac{x-4}{x^5 + x^4y + x^3y^2 + x^2y^3 + xy^4 + y^5} - \dfrac{x^2 - xy + y^2}{x^6 - y^6}$

Aufgabe 3.4

Gegeben sei ein Körper F der Charakteristik 0.

a) Wir untersuchen Lösungen von linearen Differentialgleichungen der Form

$$p_\nu(x)y^{(\nu)} + \cdots + p_1(x)y' + p_0(x)y = r(x),$$

wobei die p_i $(0 \leq i \leq \nu)$ und r Polynome in x seien und y die unbekannte Funktion in x bezeichne. Ableitungen sind (wie gewohnt) mit Strichen bzw. geklammerten Exponenten notiert.

Zeigen Sie: Wenn die Differentialgleichung eine Potenzreihenlösung $y(x) = \sum_{k=0}^{\infty} y_k x^k$ hat, können die Koeffizienten $y_k \in F$ durch eine lineare Rekurrenzgleichung dargestellt werden, genauer:

Für $k \geq K$ $(K, n$ fest) ist $y_k = u_1(k)y_{k-1} + u_2(k)y_{k-2} + \cdots + u_n(k)y_{k-n}$, wobei die $u_i(k)$ rationale Ausdrücke in k über F sind.

Somit kann die Lösung in diesem Falle endlich dargestellt werden.

b) Zeigen Sie: Die Koeffizienten $a_k \in F$ für $k \geq K$ (K fest) einer Potenzreihe $a(x) = \sum_{k=0}^{\infty} a_k x^k$ können genau dann durch eine lineare Rekurrenzgleichung mit konstanten Koeffizienten $a_k = u_1 a_{k-1} + u_2 a_{k-2} + \cdots + u_n a_{k-n}$ (n fest) über F dargestellt werden, wenn $a(x)$ als rationale Funktion in x über F dargestellt werden kann.

Informationen zur Vorlesung:
http://www-madlener.informatik.uni-kl.de/ag-madlener/teaching/ws2001-2002/ca/ca.html