Computeralgebra

SS 2000
Prof. Dr. K. Madlener
Übungsblatt 2

Aufgabe 2.1

a) Sei F_i für $i \in \mathbb{N}$ die i-te Fibonacci-Zahl (also $F_0 = 0$, $F_1 = 1$ und $F_i = F_{i-1} + F_{i-2}$ für $i \geq 2$). Zeigen Sie, dass $\lfloor F_{i+2}/F_{i+1} \rfloor = 1$ und $F_{i-1} = F_{i+1} \bmod F_i$ für alle $i \geq 2$.

b) Sei $F[x]$ der euklidische univariate Polynomring über einem Körper F. Seien weiter $a, b \in F[x] \setminus \{0\}$ und $g = GGT(a, b) \in F[x]$. Zeigen Sie, dass es dann für jedes Polynom $c \in F[x]$ mit $g \mid c$ eindeutige Polynome $\sigma, \tau \in F[x]$ gibt, so dass $\sigma a + \tau b = c$ und $\deg(\sigma) < \deg(b) - \deg(g)$ gilt; wenn zudem noch $\deg(c) < \deg(a) + \deg(b) - \deg(g)$ ist, so gilt $\deg(\tau) < \deg(a) - \deg(g)$.

c) Seien $a, b \in \mathbb{N}^+$ und $a > b$. Wir wollen entscheiden, ob es $i, j \in \mathbb{N}^+$ gibt, so dass $a^i = b^j$ ist. Betrachten Sie dazu folgendes Entscheidungsverfahren für dieses Problem:

Teste zuerst, ob $b \mid a$. Wenn nicht, so antworte „nein“. Ansonsten ersetze (a, b) durch $(a/b, b)$, wenn $a \geq b^2$, bzw. durch $(b, a/b)$, wenn $a < b^2$. Wenn durch Iterieren schließlich ein Paar $(a', 1)$ erreicht wird, antworte „ja“.

Zeigen Sie, dass dieses Verfahren das Problem für jede Eingabe korrekt löst (und terminiert) und im schlechtesten Fall $O(\lambda(a)^2)$ Bitoperationen benötigt.

Aufgabe 2.2

a) Wir betrachten noch einmal den Algorithmus zur Division mit Rest nichtnegativer ganzer Zahlen zur Basis $b \geq 2$. Es seien $u = (u_0 \cdots u_n)_b$ sowie $v = (v_1 \cdots v_n)_b$ mit $\lfloor u/v \rfloor < b$. Es sei wie in der Vorlesung $\hat{q} = \min\left(\left\lfloor \frac{u_0 b + u_1}{v_1} \right\rfloor, b - 1\right)$ die Schätzung für $q = \lfloor u/v \rfloor$ mit $u = qv + r$ und $0 \leq r < v$.

Zeigen Sie, dass $\hat{q} \geq q$ und für $v_1 \geq \lfloor b/2 \rfloor$ auch $\hat{q} - 2 \leq q$.

b) Finden Sie ein Beispiel für u und v bei Basis 10, so dass die Notwendigkeit der bedingten Anweisung

$$\textbf{if } (u_j \cdots u_{j+n})_b < \hat{q} \cdot (v_1 \cdots v_n)_b \textbf{ then } \hat{q} := \hat{q} - 1$$

im Algorithmus aus der Vorlesung klar wird.

Aufgabe 2.3

a) Ist für Integritätsbereiche R, S der Ring $R + S$ ebenfalls immer ein Integritätsbereich? Zeigen oder widerlegen Sie.

b) Sei $I = \{f \in \mathbb{R}[x] \mid f(5) = 0\}$ die Menge der reellen Polynome, die 5 als eine Nullstelle haben. Zeigen Sie, dass I ein Ideal in $\mathbb{R}[x]$ ist. Geben Sie einen Isomorphismus $\mathbb{R}[x]/I \to \mathbb{R}$ an.

Aufgabe 2.4

a) Bestimmen Sie in $\mathbb{Z}[[x]]$ das Inverse zur formalen Potenzreihe

$$a(x) = \sum_{k=0}^{\infty} a_k x^k = 1 + x + 2x^2 + 3x^3 + 5x^4 + \cdots$$

mit $a_k = a_{k-1} + a_{k-2}$ für $k \geq 2$.

b) Betrachten Sie die folgende „Definition“ einer *expandierten kanonischen Form* für multivariate Polynom-Ausdrücke über einem Integritätsbereich D:

1. Ausmultiplizieren aller Produkte von Polynomen
2. Terme gleichen Grades zusammenfassen
3. Terme nach fallenden Grad ordnen

Ist dies ein kanonischer Simplifikator gemäß der Definition aus der Vorlesung? Welche Angaben brauchen Sie, um diese Frage beantworten zu können? Ist die obige Definition eindeutig?

Wenden Sie die Vorschrift auf den Ausdruck

$$\begin{aligned} a(x,y) \quad &= \quad ((x^2 - xy + x) + (x^2 + 3) \cdot (x - y + 1)) \cdot \\ & \qquad ((y^3 - 3y^2 - 9y - 5) + x^4 \cdot (y^2 + 2y + 1)) \end{aligned}$$

an.

Abgabe am 25.4.2000 bis 9.00 Uhr, Übungskasten in Bau 34, zweites OG.

Informationen zur Vorlesung:
http://www-madlener.informatik.uni-kl.de/ag-madlener/lectures/compalg/ss2000/compalg.html