

Übungen zur Vorlesung Computeralgebra  
Blatt 6

Prof. Dr. Klaus Madlener

Abgabe bis 04.06.2010

**Aufgabe 1:**

- a) Seien  $f(x) = x^3 - x^2 + 2$  und  $g(x) = x^2 + x + 1$  Polynome über  $\mathbb{Q}$ . Berechnen Sie eine Darstellung von  $h(x) = x^4 + 2x$  als  $h(x) = p(x)f(x) + q(x)g(x)$  mit  $\deg p < 2$  und  $\deg q < 3$ .
- b) Berechnen Sie das Polynom  $r(x) \in \mathbb{Q}[x]$  kleinsten Grades, das die Kongruenzen

$$\begin{aligned} r(x) &\equiv 2x^2 + 1 \pmod{x^3 + x^2 - 1} \\ r(x) &\equiv x + 2 \pmod{x^2 + 2x + 2} \end{aligned}$$

erfüllt.

**Aufgabe 2:**

Wir betrachten den Algorithmus von Garner aus der Vorlesung.

- a) Der zweite Schritt benutzt die Formeln

$$\begin{aligned} \nu_0 &\equiv u_0 \pmod{m_0} \\ \nu_k &\equiv \left( u_k - \left( \nu_0 + \nu_1 m_0 + \cdots + \nu_{k-1} \prod_{i=0}^{k-2} m_i \right) \right) \left( \prod_{i=0}^{k-1} m_i \right)^{-1} \\ &\pmod{m_k} \text{ für } k \geq 1. \end{aligned}$$

Zeigen Sie, dass man die gemischten Basiskoeffizienten  $\nu_k$  auch mit Hilfe der Formeln

$$\begin{aligned} \nu_0 &\equiv u_0 \pmod{m_0} \\ \nu_k &\equiv \left( \cdots \left( (u_k - \nu_0) m_0^{-1} - \nu_1 \right) m_1^{-1} - \cdots - \nu_{k-1} \right) m_{k-1}^{-1} \\ &\pmod{m_k} \text{ für } k \geq 1 \end{aligned}$$

berechnen kann. (Beachten Sie: Die Inversen in dieser Formel sind Inverse modulo  $m_k$ .)

- b) Wenn man den zweiten Schritt wie in a) realisiert, welche Menge von Inversen muss dann im ersten Schritt berechnet werden? Wie viele Inverse werden benötigt?
- c) Vergleichen Sie die Zeitkomplexität beider Varianten. Betrachten Sie einmal den Fall, dass die Menge  $\{m_i\}$  der Reste fest ist, d. h. die Inversenbildung im ersten Schritt ein einen Vorberechnungsschritt ausgelagert werden kann, und auch den Fall, dass dies nicht möglich ist.

**Aufgabe 3:**

Bestimmen Sie mit Hilfe der 7-adischen linearen Newton-Iteration die dritte Wurzel des Polynoms

$$a(x) = x^6 - 531x^5 + 94137x^4 - 5598333x^3 + 4706850x^2 - 1327500x + 125000$$

mit  $a(x) \in \mathbb{Z}[x]$ . Führen Sie diese Rechnung mit Hilfe eines Computeralgebra-Systems durch.

**Aufgabe 4:**

- a) Es seien  $I = \langle x, y \rangle$  und  $J = \langle x \rangle$  Ideale in  $\mathbb{Z}[x, y]$ . Beschreiben Sie zunächst die Elemente von  $I$  und  $J$  sowie die Teilmengenbeziehung zwischen  $I$  und  $J$ . Beschreiben Sie dann die Elemente von  $I + J$ ,  $I \cdot J$  und  $I^2$  und geben Sie erzeugende Elemente dieser Ideale an. Untersuchen Sie schließlich die Teilmengenbeziehungen zwischen  $I + J$ ,  $I \cdot J$  und  $I^2$ .
- b) Beschreiben Sie das Ideal  $\langle x^e \rangle$ , wobei  $e \in \mathbb{N}$  fest sei, in  $\mathbb{Q}[[x]]$ .
- c) Betrachten Sie den kanonischen Homomorphismus

$$\phi_{\langle x^e \rangle} : \mathbb{Q}[[x]] \rightarrow \mathbb{Q}[[x]]/\langle x^e \rangle.$$

Beschreiben Sie die Elemente des homomorphen Bildes in  $\mathbb{Q}[[x]]/\langle x^e \rangle$ . Geben Sie auch eine praktische Darstellung dieser Elemente an.

- d) Geben Sie eine Darstellung der Elemente von  $\mathbb{Q}[x]/\langle x^2 + 1 \rangle$  an. Zeigen Sie, dass dieser Quotientenring ein Körper ist.
- e) Beschreiben Sie  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ .
- f) Ist  $\mathbb{Z}[x]/\langle x^2 + 1 \rangle$  ein Körper? Ein Integritätsbereich? Beschreiben Sie den Zusammenhang zwischen diesem Quotientenring und den ganzen Gaußschen Zahlen  $G = \{a + b \cdot \sqrt{-1} \mid a, b \in \mathbb{Z}\}$ .