

---

Übungen zur Vorlesung Computeralgebra  
Blatt 7

Prof. Dr. Klaus Madlener

Abgabe bis 15.06.2010

---

**Aufgabe 1:**

Betrachten Sie den Algorithmus aus der Vorlesung (F 102) zur Bestimmung eines polynomialen Inversen  $g \in D[x]$  modulo  $x^\ell$  ( $\ell \in \mathbb{N}$ ) zu gegebenem  $f \in D[x]$  mit  $f(0) = 1$ .

Zeigen Sie, dass, wenn  $\ell = 2^r$  eine Zweierpotenz ist, die Rechenzeit des Algorithmus höchstens  $3M(\ell) + \ell \in O(M(\ell))$  Operationen in  $D$  beträgt. ( $M(n)$  bezeichne die Rechenzeit einer Multiplikation zweier Polynome vom Grade  $\leq n$ .)

Wie könnte man vorgehen, um im Falle, dass  $\ell$  keine Zweierpotenz ist, die Berechnung zu vieler Koeffizienten des polynomialen Inversen zu vermeiden?

Zeigen Sie weiter, dass die Rechenzeit des Algorithmus aus der Vorlesung auf  $2M(\ell)$  Operationen in  $D$  fällt wenn  $\text{char}(D) = 2$  ist.

**Aufgabe 2:**

Sei  $R$  ein kommutativer Ring mit 1,  $F \in R[y]$ ,  $g \in R$ , wobei  $F(g) \equiv 0 \pmod{p}$  und  $F'(g)$  invertierbar modulo  $p$  sei, sei eine Anfangslösung, und  $\ell \in \mathbb{N}^+$ .

Zeigen Sie: Wenn  $h, h^* \in R$  Lösungen modulo  $p^\ell$  mit  $h \equiv g \equiv h^* \pmod{p}$  sind und  $F(h) \equiv 0 \equiv F(h^*) \pmod{p^\ell}$  gilt, so ist  $h \equiv h^* \pmod{p^\ell}$ .

**Aufgabe 3:**

Berechnen Sie in  $\mathbb{Z}_3[x, y, z]$  mit Hilfe der ideal-adischen Iteration und dem Ideal

$$I = \langle y - 1, z \rangle \subseteq \mathbb{Z}_3[x, y, z]$$

die Lösung der Gleichung

$$u^2 - u = x^6 + x^4y^2 + 2x^3z + x^2y^4 + xy^2z + z^2 + 2.$$

Bestimmen Sie dazu zunächst die  $I$ -adische Darstellung des Polynoms auf der rechten Seite.