Computeralgebra

SS 2000
Prof. Dr. K. Madlener
Übungsblatt 8

Aufgabe 8.1
Zeigen Sie den Satz auf F 119: Der Algorithmus für den quadratischen Hensel-Lifting-Schritt ist korrekt.

Aufgabe 8.2
Betrachten Sie das Faktorisierungsbeispiel aus der Vorlesung: Sei $a(x) = 12x^3 + 10x^2 - 36x + 35 \in \mathbb{Z}[x]$; eine Faktorisierung modulo 5 ist

$$\phi_5(a(x)) = 2 \cdot x \cdot (x^2 + 2) \in \mathbb{Z}_5[x].$$

Wenden Sie quadratisches Hensel-Lifting (s. F 136f.) an, um eine Faktorisierung von $a(x)$ in $\mathbb{Z}[x]$ zu berechnen.

Aufgabe 8.3
Wir definieren für ein Polynom $f = \sum_{0 \le i \le n} f_i x^i = f_n \prod_{1 \le i \le n} (x - z_i) \in \mathbb{C}[x]$ das Landau-Maß $M(f)$ durch

$$M(f) = |f_n| \cdot \prod_{1 \le i \le n} \max\{1, |z_i|\},$$

wobei $f_0, \ldots, f_n, z_1, \ldots, z_n \in \mathbb{C}$. Weiter definieren wir noch die Maximumsnorm $\|f\|_\infty$, die 1-Norm $\|f\|_1$ und die 2-Norm $\|f\|_2$ durch

$$\begin{aligned} \|f\|_\infty &= \max_{0 \le i \le n} |f_i| \\ \|f\|_1 &= \sum_{0 \le i \le n} |f_i| \\ \|f\|_2 &= \sqrt{\sum_{0 \le i \le n} |f_i|^2}. \end{aligned}$$

Dabei ist $|a| = \sqrt{a\bar{a}}$ für $a \in \mathbb{C}$ ($\bar{a}$ ist die $\mathbb{C}$-Konjugierte zu a).

a) Zeigen Sie, dass für jedes $f \in \mathbb{C}[x]$ gilt: (a.1) $M(f) \ge 1$, (a.2) $M(f) = M(g)M(h)$, falls $f = gh$ mit $g, h \in \mathbb{C}[x]$, und (a.3) $M(f) \le \|f\|_2$.

b) Wenn $h = \sum_{0 \le i \le m} h_i x^i \in \mathbb{C}[x]$ vom Grad m ein Teiler von $f = \sum_{0 \le i \le n} f_i x^i \in \mathbb{C}[x]$ vom Grad $n \ge m$ ist, so gilt:

$$\|h\|_2 \le \|h\|_1 \le 2^m M(h) \le 2^m \left| \frac{h_m}{f_n} \right| \|f\|_2.$$

c) Nun zum eigentlichen Ziel: Seien $f, g, h \in \mathbb{Z}[x]$ mit $\deg f = n \geq 1$, $\deg g = m$, $\deg h = k$ und es sei gh ein Teiler von f in $\mathbb{Z}[x]$. Zeigen Sie

$$\|g\|_\infty \|h\|_\infty \leq 2^{m+k} \|f\|_2 \leq \sqrt{n+1} \cdot 2^{m+k} \|f\|_\infty$$

sowie

$$\|h\|_\infty \leq \sqrt{n+1} \cdot 2^k \|f\|_\infty.$$

Aufgabe 8.4
Sei $f(x, y) = f_0 x^d + f_1 x^{d-1} y + f_2 x^{d-2} y^2 + \cdots + f_d y^d$ ein bivariates homogenes Polynom. Geben Sie eine Reduktion des Faktorisierungsproblems für solche Polynome auf das Faktorisierungsproblem für univariate Polynome an.

Abgabe am 5.6.2000 bis 10.30 Uhr, Übungskasten in Bau 34, zweites OG.

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