Computeralgebra

WS 2001/2002
Prof. Dr. K. Madlener
Übungsblatt 10

Aufgabe 10.1
Sei $p \in \mathbb{N}$ eine Primzahl und $q = p^k$ für ein positives $k \in \mathbb{N}$, $f \in \mathbb{F}_q[x]$ ein monisches und quadratfreies Polynom vom Grade n sowie $R = \mathbb{F}_q[x]/\langle f \rangle$. Wir können den Frobenius-Endomorphismus $\alpha \mapsto \alpha^q$ von R über $\mathbb{F}_q$ im Berlekamp-Algorithmus von F 182 durch den absoluten Frobenius-Endomorphismus $\alpha \mapsto \alpha^p$ von R über dem Primkörper $\mathbb{F}_p$ ersetzen. Untersuchen Sie diese Variante und vergleichen Sie ihre Laufzeit mit der des ursprünglichen Algorithmus.

Aufgabe 10.2
Für $n \in \mathbb{N}^+$ sei

$$\Phi_n = \prod_{\substack{1 \le k < n \\ \mathrm{GGT}(k,n)=1}} (x - e^{2\pi i k/n}) = \prod_{\substack{\omega \in \mathbb{C} \text{ ist eine } n\text{-te} \\ \text{primitive Einheitswurzel}}} (x - \omega) \in \mathbb{C}[x]$$

das n-te Kreisteilungspolynom (siehe z. B. Heinz Lüneburg, *Galoisfelder, Kreisteilungskörper und Schieberegisterfolgen*, Bibliographisches Institut, 1979). Es gilt $\deg \Phi_n = \varphi(n)$.

a) Zeigen Sie: $x^n - 1 = \prod_{d|n} \Phi_d$.

b) Die Möbiusfunktion $\mu : \mathbb{N}^+ \to \{-1, 0, 1\}$ ist erklärt durch

$$\mu(n) = \begin{cases} 1 & \text{falls } n = 1, \\ (-1)^k & \text{falls } n \text{ das Produkt von } k \text{ verschiedenen Primzahlen ist,} \\ 0 & \text{falls } n \text{ nicht quadratfrei ist.} \end{cases}$$

Es gilt folgende Inversionsformel: Sei R ein kommutativer Ring mit 1 und $f, g : \mathbb{N}^+ \to R$ seien zwei Funktionen mit

$$f(n) = \sum_{d|n} g(d) \text{ für } n \in \mathbb{N}^+.$$

Dann gilt:

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) \text{ für } n \in \mathbb{N}^+.$$

Geben Sie nun unter Beachtung von a) eine Formel für Φ_n an.

c) Seien $n, k \in \mathbb{N}^+$. Dann gilt:

(i) $\Phi_n = x^{n-1} + x^{n-2} + \cdots + x + 1$, falls n prim ist.

(ii) $\Phi_{2n} = \Phi_n(-x)$, falls n ungerade ist.

(iii) $\Phi_{kn}\Phi_n = \Phi_n(x^k)$, falls k prim ist und n nicht teilt.

(iv) $\Phi_{kn} = \Phi_n(x^k)$, falls jeder Primteiler von k auch n teilt.

d) Geben Sie unter Verwendung der Ergebnisse aus c) einen Algorithmus an, der aus $n \in \mathbb{N}^+$ und den verschiedenen Primteilern $p_1, \ldots, p_r$ von n das Polynom Φ_n berechnet. Ihr Algorithmus soll eine Laufzeit von $O(M(n) \log n)$ Operationen in $\mathbb{Z}$ haben. (Zusatzfrage: Wieso gilt $\Phi_n \in \mathbb{Z}[x]$?)

Aufgabe 10.3

Von Kronecker (1882) stammt folgende Methode, das Faktorisierungsproblem für multivariate Polynome über einem ZPE-Ring R auf das Faktorisierungsproblem für univariate Polynome über R zu reduzieren.

a) Sei die Abbildung $S_d : R[x_1, \ldots, x_n] \to R[y]$ durch

$$h(x_1, \ldots, x_n) \mapsto h(y, y^d, \ldots, y^{d^{n-1}})$$

definiert (für $d \in \mathbb{N}$). Überzeugen Sie sich, dass S_d ein Homomorphismus ist, der für diejenigen Polynome invertiert werden kann, die in jeder Variablen einen Grad kleiner als d haben.

b) Wir wollen mit S_d^{-1} die additive Abbildung $R[y]/\langle y^{d^n} \rangle \to R[x_1, \ldots, x_n]$ bezeichnen, die

$$S_d^{-1}(c\, y^\alpha) = c\, x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

erfüllt, wobei $\alpha_1 + \alpha_2 d + \cdots + \alpha_n d^{n-1}$ die (positive) d-adische Darstellung von α sei.

Sei nun $f \in R[x_1, \ldots, x_n]$, $d > \max_{1 \le i \le n} \deg_{x_i}(f)$, und sei g ein Faktor von f. Zeigen Sie, dass es dann irreduzible Faktoren $g_1, \ldots, g_s$ von $S_d(f)$ gibt, so dass $g = S_d^{-1}(\prod_{j=1}^s g_j)$ ist.

c) Geben Sie nun einen Algorithmus an, der für ein $f \in R[x_1, \ldots, x_n]$ seine irreduziblen Faktoren $f_1, \ldots, f_s$ berechnet. Untersuchen Sie die Laufzeit Ihres Algorithmus.

d) Faktorisieren Sie das Polynom $f = -x^4y + x^3z + xz^2 + yz^2 \in \mathbb{F}_3[x, y, z]$ mit Ihrem Algorithmus.

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