SS 2010 28.06.2010

Übungen zur Vorlesung Computeralgebra
Blatt 10

Prof. Dr. Klaus Madlener Abgabe bis 02.07.2010

Aufgabe 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 2:
für $n \in \mathbb{N}^+$ sei

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

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 $n > 3$ und 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 3:

1. Zeigen Sie das Eisenstein-Kriterium: Wenn $f \in \mathbb{Z}[x]$ und $p \in \mathbb{N}$ eine Primzahl, so dass $p \nmid \mathrm{lc}(f)$, p alle anderen Koeffizienten von f teilt, und $p^2 \nmid f(0)$, dann ist f irreduzibel in $\mathbb{Q}[x]$.
2. Folgern Sie, dass für beliebige $n \in \mathbb{N}$ das Polynom $x^n - p$ irreduzibel in $\mathbb{Q}[x]$ ist.