UNIVERSITÄT DES SAARLANDES
Fachbereich 14 – Informatik

Prof. J. Buchmann
Stefan Neis

20. Dezember 1995

9. Übung zu "Algebra für Informatiker"

1. Sei $f(x) \in \mathbb{Z}[x]$.
   (a) Sei φ ein Automorphismus von $\mathbb{Z}[x]$. Zeige: $f(x)$ ist genau dann irreduzibel, wenn $\varphi(f(x))$ irreduzibel ist. Bestimme alle Automorphismen von $\mathbb{Z}[x]$.
   (b) Für $p \in \mathbb{P}$ sei ψ_p der kanonische Homomorphismus von $\mathbb{Z}[x]$ nach $\mathbb{Z}/p\mathbb{Z}[x]$. Zeige: Ist f normiert und $\psi_p(f)$ irreduzibel über $\mathbb{Z}/p\mathbb{Z}$ für ein $p \in P$, so ist f irreduzibel über $\mathbb{Z}$.
2. Zeige mit Hilfe dieser Kriterien und mit dem Satz von Eisenstein die Irreduzibilität der folgenden Polynome über $\mathbb{Z}$:
   (a) $f(x) = x^4 + 5x^3 + 10x^2 + 2x - 3$.
   (b) $f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ für $p \in \mathbb{P}$.
   Hinweis: Es ist $f(x) = \frac{x^p-1}{x-1}$. Nun wende den Automorphismus φ mit $\varphi(x) = x + 1$ und den Satz von Eisenstein an.
   (c) $f(x) = x^6 + x^4 + x^2 + 3$.
   (d) $f(x) = x^4 + 2x^2 + 3$.
3. Bestimme alle Primideale und alle maximalen Ideale von $\mathbb{Z}[x]$.
4. Faktorisiere mit dem Algorithmus von Berlekamp
   $f(x) = x^{13} + x^{12} + 2x^{11} + 3x^{10} + 3x^9 + x^7 + 2x^6 + 3x^5 + 2x^4 + x^2 + 4x + 4$ über $\mathbb{Z}/5\mathbb{Z}[x]$.
   Hinweis: Nach "square free factorization" bleibt nur noch ein Polynom $u(x)$ vom Grade 8 übrig. Bestimme nun die Matrix $Q = \begin{pmatrix} q_{0,0} & \cdots & q_{0,n-1} \\ \vdots & \ddots & \vdots \\ q_{n-1,0} & \cdots & q_{n-1,n-1} \end{pmatrix}$ mit $x^{pk} \equiv q_{n-1,k}x^{n-1} + \ldots + q_{0,k}$ (modulo $u(x)$). Berechne eine Basis des Kerns von $Q - I$. Zur Kontrolle: Eine Basis ist $(1, x^6 + x^5 + 4x^4 + x^3 + x^2 + 4x, x^7 + 2x^5 + 4x^3 + x^2 + x)$. Bestimme nun die Faktorisierung von $u(x)$ und dann die Faktorisierung von $f(x)$.

Abgabe:

Donnerstag, 11. 1. 1996

Wir wünschen allen Hörern ein frohes Weihnachtsfest und
einen guten Rutsch ins neue Jahr.