

Computer Algebra

Sebastian Iwanowski
FH Wedel

6. Faktorisierung von Polynomen
6.1 Faktorisierung in $\mathbb{Z}_p[x]$ und $\text{GF}(q)[x]$

Referenzen zum Nacharbeiten und Vertiefen:

Köpf 8.1-8.3

Kaplan 6.2, 6.3

Seminararbeit 9 (Sebastian Wenzel)

Computer Algebra 6

Polynomfaktorisierung in \mathbb{Z}_p durch Berlekampalgorithmus

Motivation: Schluss von $\mathbb{Z}_p[x]$ auf $\mathbb{Z}[x]$

\exists Primzahl p : $a[x]$ ist irreduzibel in $\mathbb{Z}_p[x] \Rightarrow a[x]$ ist irreduzibel in $\mathbb{Z}[x]$

Satz: Sei $a(x) \in \mathbb{Z}_p[x]$. Gesucht ist eine Faktorisierung von $a(x)$. ***gilt nur, wenn p Primzahl!***

Falls ein Polynom $b(x) \in \mathbb{Z}_p[x]$ existiert mit folgenden Voraussetzungen:

$$a(x) \mid ((b(x))^p - b(x)) \quad \text{und} \quad 0 < \deg(b(x)) < \deg(a(x))$$

Dann gilt: $a(x) = (\text{ggT}(a(x), b(x))) \cdot (\text{ggT}(a(x), b(x)-1)) \cdot \dots \cdot (\text{ggT}(a(x), b(x)-(p-1)))$
ist eine quadratfreie Faktorisierung von $a(x)$

Ziel: Gegeben $a(x)$ mit Grad n , suche ein $b(x) = b_{n-1}x^{n-1} + \dots + b_1x + b_0$ mit dieser Eigenschaft

Berlekamp-Algorithmus: Laufzeit: $O(n^3p^2)$ ***kann auf $GF(q)$ verallgemeinert werden***

1. Berechne $r_j(x) = x^{jp} \bmod a(x)$ für alle $j = 0, 1, \dots, n-1$ $O(n^3p^2)$
2. Löse das Gleichungssystem $b_{n-1}r_{n-1}(x) + \dots + b_1r_1(x) + b_0 - b(x) = 0$
(n Gleichungen mit n Variablen b_i durch Koeffizientenvergleich) $O(n^2)$
3. Berechne $\text{ggT}(a(x), b(x)), \text{ggT}(a(x), b(x)-1), \dots, \text{ggT}(a(x), b(x)-(p-1))$ $O(pn^2)$

Satz: Wenn $a(x)$ quadratfrei ist, dann führt das zur gewünschten Faktorisierung ***aber nur dann !***

Computer Algebra 6

Matrixdarstellung des Berlekampalgorithmus

Sei $r_i(x) = r_{n-1,i}x^{n-1} + \dots + r_{1,i}x + r_{0,i}$ die Koeffizientendarstellung der Restepolynome von Berlekamp

Dann gilt für die Koeffizienten b_{n-1}, \dots, b_1, b_0 :

$$\text{Matrix } R - E \rightarrow \begin{pmatrix} r_{0,0} - 1 & r_{0,1} & \cdots & r_{0,n-1} \\ r_{1,0} & r_{1,1} - 1 & \cdots & r_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n-1,0} & r_{n-1,1} & \cdots & r_{n-1,n-1} - 1 \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Satz: $\dim(\text{Lösungsraum}(R-E)) = \text{Anzahl der verschiedenen irreduziblen Faktoren für } a(x)$
 $= n - \dim(\text{Bildraum}(R-E))$

\uparrow
 $\text{Kern}(R-E) \geq 1$ $\text{Rang}(R-E) \leq n-1$
 \uparrow \uparrow
 weil die erste Spalte nur Nullen enthält (= 1 \Rightarrow $a(x)$ ist selbst irreduzibel)

Problem: Wenn $a(x)$ nicht quadratfrei ist, dann liefert Berlekamp nicht die Vielfachheit der irreduziblen Faktoren

Lösung: Finde erst eine quadratfreie Faktorisierung von $a(x)$

Computer Algebra 6

Quadratfreie Faktorisierung in $\text{GF}(q)[x]$ *q muss keine Primzahl sein!*

Sei $q = p^n$: Dann gilt für alle $a \in \text{GF}(q)$: $p \cdot a = \underbrace{(a + a + \dots + a)}_{p \text{ mal}} = 0$ und $a^{p^n} = \underbrace{(a \cdot a \cdot \dots \cdot a)}_{p^n \text{ mal}} = a$

Satz: $b(x)$ ist mehrfacher Teiler von $a(x) \Leftrightarrow b(x)$ teilt $a(x)$ und $a'(x)$ (Ableitung nach x)
gilt nur für $a'(x) \neq 0$

In diesem Fall kann derselbe Faktorisierungsalgorithmus wie für $\mathbb{Z}[x]$ angewendet werden.

Laufzeit: $O(m^3)$

↑
Grad von $a(x)$

Satz und Algorithmus für $a'(x) \equiv 0$:

$$\text{Sei } a(x) = a_{0,p} + a_{1,p}x^{1 \cdot p} + a_{2,p}x^{2 \cdot p} + \dots + a_{k,p}x^{k \cdot p}$$

Dann gilt: $a(x) = (b(x))^p$ für das Polynom $b(x) = b_k x^k + \dots + b_1 x + b_0$ mit $b_i = a_{i,p}^{p^{n-1}}$

Laufzeit: $O(mn)$