Computer Algebra

Sebastian Iwanowski
FH Wedel

8. Effiziente Faktorisierung von Polynomen
8.1 Faktorisierung in $\mathbb{Z}_p$[x] und GF(q)[x]

Referenzen zum Nacharbeiten und Vertiefen:

Köpf 8.1-8.3
Kaplan 6.2, 6.3
Seminararbeit 9 (Sebastian Wenzel)

Computer Algebra 8

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 $b(x) \in \mathbb{Z}_p[x]$ existiert mit $a(x) \mid ((b(x))^p - b(x))$ und $\deg(b(x)) < \deg(a(x))$
$\Rightarrow a(x) = (ggT(a(x),b(x)) \bullet (ggT(a(x),b(x)-1)) \bullet \ldots \bullet (ggT(a(x),b(x)-(p-1))$

Ziel: Gegeben a(x) mit Grad n, suche ein $b(x)=b_{n-1}x^{n-1}+\ldots+b_1x+b_0$ 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,...,n-1 — $O(n^3p^2)$
2. Löse das Gleichungssystem $b_{n-1}r_{n-1}(x) + \ldots + b_1r_1(x) + b_0 - b(x) = 0$
   (n Gleichungen mit n Variablen b_i durch Koeffizientenvergleich) — $O(n^2)$
3. Berechne ggT(a(x),b(x)), ggT(a(x),b(x)-1)) , … , ggT(a(x),b(x)-(p-1)) — $O(pn^2)$

Computer Algebra 8

Matrixdarstellung des Berlekampalgorithmus

Sei $r_j(x) = r_{n-1,j}x^{n-1}+\ldots+r_{1,j}x+r_{0,j}$ die Koeffizientendarstellung der Restepolynome von Berlekamp

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

$$\begin{pmatrix} r_{0,0}-1 & r_{0,1} & \cdots & r_{0,n-1} \\ r_{1,0} & r_{1,1}-1 & \cdots & r_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n-1,0} & r_{n-1,1} & \cdots & r_{n-1,n-1}-1 \end{pmatrix} \bullet \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

↑ Matrix R - E

Rang (R – E) ≤ n-1 ↓

Satz: dim (Lösungsraum (R-E)) = n - dim (Bildraum (R-E))

= Anzahl der verschiedenen irreduziblen Faktoren für a(x)

↑ Kern (R-E) ≥ 1 (= 1 => a(x) ist selbst irreduzibel)

↑ weil die erste Spalte nur Nullen enthält

Computer Algebra 8

Quadratfreie Faktorisierung in GF(q)[x]

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

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) ≢ 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) ≡ 0:

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

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

Laufzeit: $O(mp^{n-2})$