Computer Algebra

Sebastian Iwanowski
FH Wedel

6. Effiziente Faktorisierung von Polynomen
6.2 Faktorisierung in $\mathbb{Q}$[x] über den Umweg $\mathbb{Z}_p$[x]

Referenzen zum Nacharbeiten und Vertiefen:

Köpf 8.4-8.5
Kaplan 6.4 (setzt Kap. 3 voraus, das in dieser Vorlesung nicht behandelt wurde)

Computer Algebra 6

Polynomfaktorisierung in $\mathbb{Q}$ mit der Zassenhaus-Schranke

Nach Satz 1 (CA42-4) können wir uns auf die Faktorisierung in $\mathbb{Z}$ beschränken.

Def.: Symmetrische Modulofunktion

Die Elemente von $\mathbb{Z}_p$ sollen in diesem Kapitel mit $\left\{-\frac{p-1}{2},-\frac{p-3}{2},\ldots,0,\ldots,\frac{p-3}{2},\frac{p-1}{2}\right\}$ bezeichnet werden.

Satz: Identische Faktorisierung in $\mathbb{Z}_p$ und $\mathbb{Z}$ für beschränkte Koeffizienten

Sei $a(x) \in \mathbb{Z}[x]$ ein normiertes Polynom ($a_n=1$) mit $a(x) \equiv b(x) \cdot c(x) \pmod p$ und $b(x), c(x) \in \mathbb{Z}_p[x]$ und $|d_i| < p/2$ für alle Koeffizienten d_i eines beliebigen Faktorpolynoms $d(x) \in \mathbb{Z}[x]$.

Falls $a(x) = b'(x) \cdot c'(x)$ mit $b'(x) \equiv b(x) \bmod p$ und $c'(x) \equiv c(x) \bmod p$
Dann gilt: $b'(x) = b(x)$ und $c'(x) = c(x)$

Satz: Zassenhaus-Schranke

Sei $a(x) \in \mathbb{Z}[x]$ ein normiertes Polynom ($a_n=1$)

1. $R_0 = \frac{1}{\sqrt[n]{2}-1} \cdot \max_{k=1,\ldots,n} \sqrt[k]{\frac{|a_{n-k}|}{\binom{n}{k}}}$ ist eine obere Schranke für den Betrag aller Nullstellen.

2. Für alle Koeffizienten b_i eines jeden normierten Faktors $b(x)$ von $a(x)$ gilt: $|b_i| \le \max_{k=1,\ldots,m} \binom{m}{k} R_0^k$
(m sei der Grad von b)

Computer Algebra 6

Polynomfaktorisierung in $\mathbb{Q}$ mit der Zassenhaus-Schranke

Algorithmus:

1. Berechne zu a(x) $\in \mathbb{Z}[x]$ die Zassenhaus-Schranke z für die Koeffizienten der potentiellen Faktoren.
2. Wähle eine Primzahl p **>** 2 · z.
3. Faktorisiere a(x) in $\mathbb{Z}_p$ mit dem Berlekamp-Algorithmus.

Laufzeit: $O(n^3z^2)$ wobei z die Zassenhaus-Schranke ist

Computer Algebra 6

Polynomfaktorisierung in $\mathbb{Q}$ mit dem Hensel-Lifting

Satz: Hensel-Lifting von $\mathbb{Z}_p$ auf $\mathbb{Z}_{p^2}$

Erweitert die Faktorisierung auch auf Nichtprimzahlen!

Sei $a(x) \in \mathbb{Z}[x]$ ein normiertes Polynom ($a_n=1$) mit $a(x) \equiv b(x) \cdot c(x) \pmod p$
wobei $b(x)$, $c(x)$ normiert und $ggT(b(x),c(x)) \equiv 1 \pmod p$

Dann gibt es $b'(x)$, $c'(x) \in \mathbb{Z}[x]$ mit $b(x)$, $c(x)$ normiert und $ggT(b'(x),c'(x)) \equiv 1 \pmod{p^2}$
und $b'(x) \equiv b(x) \pmod p$ und $c'(x) \equiv c(x) \pmod p$ und $a(x) = b'(x) \cdot c'(x) \pmod{p^2}$.

$b'(x)$ und $c'(x)$ sind eindeutig $(\mathrm{mod}\ p^2)$ und können mit dem Erweiterten Euklidischen Algorithmus bestimmt werden.

Algorithmus:

1. Suche zu $a(x) \in \mathbb{Z}[x]$ und kleinen Primzahlen p die Berlekamp-Faktorisierung, bis die Bedingungen des Hensel-Liftings erfüllt sind.
2. Berechne iterativ $b'(x)$ und $c'(x)$, bis p^2 das Doppelte der Zassenhaus-Schranke erreicht hat.

Anm.: Durch Probemultiplikation in $\mathbb{Z}[x]$ kann festgestellt werden, ob die Faktorisierung schon eher gefunden wurde.