Computer Algebra

Sebastian Iwanowski
FH Wedel

6. Faktorisierung von Polynomen
6.1 Einfache Faktorisierung

Referenzen zum Nacharbeiten:

Köpf 6.5,6.7,6.8
Seminararbeit 6 (ab 2. Teil) (Stefan Hasenbanck)

Computer Algebra 6

Faktorisierung eines Polynoms $p[x] \in \mathbb{Q}[x]$ nach Kronecker

Laufzeit: O(exp(n))

Satz 1: Wenn $p[x] = s[x] \cdot q[x]$ für $p[x], q[x], s[x] \in \mathbb{Q}[x]$, dann existieren $a,b,c \in \mathbb{Z}$ und Polynome $p^*[x], q^*[x], s^*[x] \in \mathbb{Z}[x]$ mit $p^*[x] = a \cdot p[x]$; $q^*[x] = b \cdot p[x]$; $s^*[x] = c \cdot s[x]$

Folgerung: Weil die Teilerpolynome ohnehin nur bis auf Normierung eindeutig sind, lösen wir das Problem gleich in $\mathbb{Z}[x]$

Satz 2: Die Koeffizienten eines Polynoms vom Grad n sind durch die Angabe von n+1 Funktionswerten eindeutig bestimmt.

1. Erweitere p[x] zu einem ganzzahligen Polynom. — Laufzeit: O(n)
2. Berechne die ganzzahligen Funktionswerte an n/2 + 1 Stützstellen. — $O(n^2)$
3. Betrachte die ganzzahligen Teiler der n/2 + 1 Funktionswerte und bilde alle Kombinationen von (n/2 + 1)-Tupeln daraus. — O(exp(n)) mal:
4. Ermittle für jede Kombination das Kandidatenpolynom durch Interpolation. — $O(n^2)$
5. Teste jeden Kandidaten durch Polynomdivision in $\mathbb{Z}[x]$ — $O(n^2)$

Computer Algebra 6

Quadratfreie Faktorisierung mit Ableitungen

Laufzeit: $O(m^3)$

Die Quadratfreie Faktorisierung von einen Polynom a(x) ist gegeben durch:

$$a(x) = \prod_{k=1}^{m} a_k^k(x)$$

wobei m der Grad von a(x) ist und $a_k(x)$ nur in irreduzible Polynome zerlegt werden kann, die den Grad 1 haben.

Zudem muss gelten: $ggT(a_k(x), a_j(x)) = 1 \,\big|\, \forall k \neq j$.

Satz: q[x] ist mehrfacher Teiler von p[x] ⇔ q[x] teilt p[x] und p'[x] (Ableitung nach x)

1. Setze i auf 1 zur Bestimmung der einfachen Teiler.
2. Bestimme g[x] := ggT (p[x], p'[x])
3. Berechne q[x] := p[x] div g[x]

   q[x] ist quadratfrei
4. Berechne a_i[x] := q[x] div ggT (q[x], g[x])

   a_i[x] besteht aus den Faktoren, die genau i mal vorkommen.
5. Erhöhe i um1 zur Bestimmung der i+1-fachen Teiler.
6. Setze p[x] := g[x] und fahre fort bei Schritt 2 (Abbruch, wenn g[x]=1).