Computer Algebra

Sebastian Iwanowski
FH Wedel

4. Polynomarithmetik
Teil 2: Division und Einfache Faktorisierung

Referenzen zum Nacharbeiten:

Köpf 6.4-6.9
von zur Gathen, Gerhard, Kapitel 3, 5 (zur Vertiefung, u.a. für die Laufzeitabschätzung)
Seminararbeit 6 (Stefan Hasenbanck)

Computer Algebra 4

Division von Polynomen p und q

Definition:

Ein Ring R heißt Euklidischer Ring, wenn es für jedes Element $p \in R$ eine Gradfunktion deg: $R \rightarrow \mathbb{N}$ gibt mit:

i) $\forall\ p,q \in R\ \exists\ s,r \in R$: $p = s \bullet q + r$ und $\deg(r) < \deg(q)$

ii) $\deg(0) = 0$ und $\forall\ p,q \in R \setminus \{0\}$: $\deg(p \bullet q) \geq \deg(p)$

Beispiele:

- Jeder Körper ist ein Euklidischer Ring.
- $\mathbb{Z}$ ist ein Euklidischer Ring.
- Die Menge K[x] der Polynome über K bildet für jeden Körper K einen Euklidischen Ring.
- Die Menge $\mathbb{Z}$[x] der Polynome über $\mathbb{Z}$ bildet keinen Euklidischen Ring.

  aber beinahe:
  Es gilt: $\forall\ p[x],q[x] \in \mathbb{Z}[x]\ \exists\ a \in \mathbb{Z}$, $s[x],r[x] \in \mathbb{Z}[x]$: $a \bullet p[x] = s[x] \bullet q[x] + r[x]$ und $\deg(r) < \deg(q)$

Computer Algebra 4

Division von Polynomen p und q

Verallgemeinerung von $\mathbb{Z}$ auf beliebige Euklidische Ringe:

- Schulalgorithmus zur schriftlichen Division mit Rest
- Euklidischer Algorithmus zur Bestimmung des ggT
- Erweiterter Euklidischer Algorithmus zur Bestimmung von ggT und Bezout-Koeffizienten s und t: ggT(p,q) = s • p + t • q

Folgerung für Polynome:

- Schriftliche Polynomdivision — Laufzeit: $O(n^2)$
- Euklidischer Algorithmus zur Bestimmung des größten gemeinsamen Teilerpolynoms — Laufzeit: $O(n^2)$
- Erweiterter Euklidischer Algorithmus zur Bestimmung der Bezout-Polynome s[x] und t[x] für Polynome: ggT(p[x],q[x]) = s[x] • p[x] + t[x] • q[x]

Anm.: Das Teilerpolynom ist nur normiert eindeutig. Achtung: expression swell !
In $\mathbb{Z}$ muss zwischendurch mit den Leitkoeffizienten multipliziert werden.

Computer Algebra 4

Faktorisierung eines Polynoms p[x] ∈ ℚ[x] nach Kronecker

Laufzeit: O(exp(n))

Satz 1: Wenn p[x] = s[x] · q[x] für p[x], q[x], s[x] ∈ ℚ[x],
dann existieren a,b,c ∈ℤ und Polynome p*[x], q*[x], s*[x] ∈ ℤ[x]
mit p*[x] = a · p[x]; q*[x] = b · p[x]; s*[x] = c · s[x]

Folgerung: Weil die Teilerpolynome ohnehin nur bis auf Normierung eindeutig sind, lösen wir das Problem gleich in 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 ℤ[x] $O(n^2)$

Computer Algebra 4

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: $ggT(a_k(x), a_j(x)) = 1 \mid \forall k \neq j$.

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

q[x] ist quadratfrei

a_i[x] besteht aus den Faktoren, die genau i mal vorkommen.

Computer Algebra 4

Rationale Funktionen K(x) über einem Körper K

Definition:

K(x) ist die Menge aller rationalen **Funktionen der Form p[x] / q[x]**, wobei p[x], q[x] $\in$ K[x] für einen Körper K.

Satz: K(x) ist selbst ein Körper.

Rechenoperationen analog zu Brüchen:

- Addition / Subtraktion durch Erweitern und Addition/Subtraktion des Zählers
- Multiplikation / Division durch Multiplikation der Zähler bzw. Nenner

Computer Algebra 4

Rationale Funktionen K(x) über einem Körper K

Definition:

K(x) ist die Menge aller rationalen **Funktionen der Form p[x] / q[x]**, wobei p[x], q[x] $\in$ K[x] für einen Körper K.

Satz: K(x) ist selbst ein Körper.

Normierte Darstellung:

r(x) = p[x] / q[x] ist in normierter Darstellung, wenn ggT (p[x],q[x]) = 1

Errechnung der normierten Darstellung einer rationalen Funktion:

- Bestimmung von ggT(p[x],q[x])
- Kürzen: Polynomdivision von p[x] und q[x] durch ggT(p[x],q[x])

Alle rationalen Operationen in $O(n^2)$ möglich (Einheitskostenmaß!)