Seminar „Algorithmische Algebra“
im Wintersemester 2018/19
Dienstags, 14-16 Uhr, INF 205, SR 7

Allgemeiner Hinweis:
Illustrieren Sie die Algorithmen auch an Beispielen.

1 Addition und Multiplikation von Polynomen

- Landau-Symbole
- Darstellungsendliche Ringe
- Laufzeit für Addition von Polynomen
- Laufzeit für gewöhnliche Multiplikation von Polynomen
- Laufzeit für Karatsuba-Multiplikation von Polynomen

Literatur: [M], Ch. 1.1,1.2,1.4

2 Diskrete Fouriertransformation und schnelle Multiplikation

- allgemeine diskrete Fouriertransformierte
- Aufwand der Fouriertransformation bei Verwendung von Einheitswurzeln
- Aufwand ihrer Inversen bei Verwendung von Einheitswurzeln
- Schnelle Polynommultiplikation

Literatur: [M], Ch. 2.1,2.2,2.3

3 Division und schnelle Division

- Division mit Rest von Polynomen (Satz 1.14(b)+ Satz 1.18(b));
- Newton-Approximation
- Inversenberechnung in $K[[T]]$
- Schnelle Polynomdivision mit Rest

Literatur: [M], Ch. 1.3,2.4

4 Euklidscher Algorithmus

- Euklidscher Ring, ggT und kgV
- Euklidscher Algorithmus und erweiterter Euklidscher Algorithmus zur ggT-Berechnung zweier Elemente
- Laufzeit mit gewöhnlicher Rechnung (Satz 4.8)
- Schneller Euklidscher Algorithmus nach Schönhage; nur Laufzeit-Angabe und Idee

Literatur: [M], Ch. 4.1,4.2,4.3

5 Polynomwertberechnung und Interpolation

- Hauptsatz über simultane Kongruenzen (nur für Euklidsche Ringe), d.h. Zusatz 7.3+ das was von Satz 7.1 dazu benötigt wird
- Polynomwertberechnung und Interpolation (Satz 7.5)
- Beispiel für $n = 4$ (selbst aussuchen)

Literatur: [M], Ch. 7.1,7.2

6 Polynome über Integritätsbereichen I

- Pseudo-Division mit Rest, Primitiver Euklidscher Algorithmus
- Sylvestermatrix und Resultante
- Eliminationsverfahren für nicht-lineare Gleichungssysteme

Literatur: [M], Ch. 6.1 (bis Bsp. 6.7), 5.1,5.4

7 Polynome über Integritätsbereichen II

- Produktformel der Resultante
- Polynome, deren Nullstellen Summen, Differenzen, Produkte oder Quotienten anderer Polynomnullstellen sind (Satz 9.5)
- Diskriminante

Literatur: [M], Ch. 5.2, 9.2, 5.3

8 Teilfaktorisierung von Polynomen

- vollkommener Körper
- quadratfreie Faktorisierung; auch für Charakteristik 0
- Faktorisierung nach Grad der Primteiler
- Nullstellenberechnung über endlichen Körpern

Literatur: [M], Ch. 18.1,18.4

9 Berlekamp-Algorithmus

- Zerlegende Polynome
- Berlekamp-Matrix
- Berlekamp-Algorithmus
- Variante von Zassenhaus

Literatur: [M], Ch. 18.2,18.3

10 Hensel'sche Methode zur Faktorisierung in $\mathbb{Z}[T]$

- p-adische Zahlen
- Hensel'sche Lemma
- Primzerlegung in $\mathbb{Z}_p[T]$
- Zassenhaus-Algorithmus zur Primzerlegung in $\mathbb{Z}[T]$

Literatur: [M], Ch. 19 bis Bsp. 19.10

11 Gröbner-Basen

- Monomordnungen
- Leitterm,-koeffizient und -monom (=höchster Term etc.)
- Definition von Gröbner-Basen
- G-Rest und Satz 21.14
- Existenz von Gröbner-Basen ohne Beweis
- Reduzierte Gröbner-Basis
- Existenz und Eindeutigkeit reduzierter Gröbner-Basen

Literatur: [M], Ch. 21

12 Buchberger-Algorithmus

- Differenzpolynome
- Charakterisierung einer Gröbner-Basis (Satz 22.2)
- Buchberger-Algorithmus für Körper

Literatur: [M], Ch. 22.1,22.2

Literatur

[M] B. H. Matzat, *Computeralgebra*; Vorlesungsskript 2008, `https://wwwproxy.iwr.uni-heidelberg.de/~Heinrich.Matzat/publications.html`