

# Zusammenfassung: Computer-Algebra

## Kapitel 1: Arbeiten mit Maxima

Was kann ein Computer-Algebra-System? (Stichworte: exaktes Rechnen mit Symbolen)

~~Arbeiten mit dem Werkzeug Maxima~~

## Kapitel 2: Ganzzahlarithmetik

Darstellung ganzer Zahlen, logarithmisches Kostenmaß für die Algorithmen.

Basis-Algorithmen für Addition, Subtraktion und Multiplikation, Algorithmus von Karatsuba.

Teilen mit Rest, ~~Details der Implementierung des Schulalgorithmus~~, **Idee und praktische**

**Bedeutung des Verfahrens von Pope-Stein, ~~Details dazu,~~**

Euklidischer Algorithmus (auch in erweiterter Form), **Bedeutung für die Kryptographie**

Anwendung der Ganzzahlarithmetik: Rationale Arithmetik (Bruchdarstellung, Kürzen)

von allem: Laufzeitabschätzungen (ohne exakte Beweise).

# Zusammenfassung: Computer-Algebra

## Kapitel 3: Modulare Arithmetik

Funktionsweise und Effizienz von Addition, Subtraktion, Multiplikation und Division mit Restklassen (Überblick)

Potenzieren, Radizieren und Logarithmieren: Definition, Beispiele, Effizienzbetrachtungen

Fiat-Shamir-Protokoll (Schwierigkeit des Wurzelziehens),

Diffie-Hellman-Schlüsselaustausch (Schwierigkeit des Logarithmierens)

~~Grundprinzip RSA~~

Kleiner Satz von Fermat

Rabin-Miller-Test im Detail, Bedeutung des Verfahrens

AKS-Test: Idee und Bedeutung des Verfahrens

## Kapitel 4: Polynomarithmetik

Darstellung von Polynomen, Einheitskostenmaß für die Algorithmen

Addition, Subtraktion, Schulmethode der Multiplikation

~~Karatsuba für Polynome~~

Schnelle Fouriertransformierte im Detail (mit Grundlagen der komplexen Zahlen)

Polynome über algebraischen Strukturen: Zusammenhang zwischen  $\mathbb{Z}[x]$  und  $\mathbb{Q}[x]$

Allgemeines Verständnis der Erweiterung von einem Ring auf einen Körper über

rationale Funktionen, Notwendigkeit des Kürzens

Konkret: Polynomdivision mit dem Euklidischen Algorithmus

Konkrete Anwendung der Polynomarithmetik auf rationale Funktionen

# Zusammenfassung: Computer-Algebra

## Kapitel 5: Polynomiale Gleichungssysteme

Algebraische Grundlagen dazu: Matrizen und Determinanten

~~Algebraische Körpererweiterungen~~

Sylvestermatrix und Resultante

Definition und algebraisches Grundverständnis: Was können wir als Lösung erwarten?

Lösung eines Gleichungssystems mit Resultanten und Faktorisierung bei der Rücksubstitution

## Kapitel 6: Faktorisierung von Polynomen

Beschränkung auf  $\mathbb{Z}[x]$ , Faktorisierung von Polynomen nach Kronecker

Effiziente quadratfreie Faktorisierung von Polynomen

Berlekamp-Algorithmus für  $\mathbb{Z}_p$  (Funktionsweise, Beispiele, Grenzen(quadratfrei!))

~~Interpretation der Lösung in Matrixdarstellung~~

Quadratfreie Faktorisierung für Spezialfall  $a'(x) \equiv 0$ , Begründung, warum der gebraucht wird

Polynomfaktorisierung mit der Zassenhaus-Schranke: Schluss von  $\mathbb{Z}_p$  auf  $\mathbb{Z}$

Grundprinzip und Vorteil des Hensel-Liftings