Zusammenfassung: Computer-Algebra

Kapitel 1: Arbeiten mit Maxima

Was kann ein Computer-Algebra-System? (Stichworte: exaktes Rechnen mit Symbolen)
~~Arbeiten mit dem Werkzeug Maxima~~
~~Anwendung Kurvendiskussionen~~
Anwendung Matrixmanipulation
Anwendung Gleichungssysteme

Kapitel 2: Ganzzahlarithmetik

Darstellung ganzer Zahlen, logarithmisches Kostenmaß für die Algorithmen
Basis-Algorithmen für Addition, Subtraktion und Multiplikation
Algorithmus von Karatsuba
Teilen mit Rest, Euklidischer Algorithmus (auch in erweiterter Form), ~~ggT für k Zahlen~~
Anwendung der Ganzzahlarithmetik: Rationale Arithmetik (Bruchdarstellung, Kürzen)

Kapitel 3: Modulare Arithmetik

Funktionsweise und Effizienz von Addition, Subtraktion, Multiplikation und Division mit Restklassen (Überblick)
Potenzieren, Radizieren und Logarithmieren: Definition, Beispiele, Effizienzbetrachtungen
Algorithmus von Karatsuba
Teilen mit Rest, Euklidischer Algorithmus (auch in erweiterter Form), ggT für k Zahlen
Anwendung der Ganzzahlarithmetik: Rationale Arithmetik (Bruchdarstellung, Kürzen)

Zusammenfassung: Computer-Algebra

Kapitel 4: Anwendungen in der Kryptographie

Fiat-Shamir-Protokoll
Diffie-Hellman-Schlüsselaustausch
~~Grundprinzip RSA~~
Faktorisierung ganzer Zahlen: nur Probedivision

Kapitel 5: Spezialthema: Primzahltest

Kleiner Satz von Fermat
Rabin-Miller-Test im Detail
AKS-Test: Idee und Bedeutung des Verfahrens

Kapitel 6: 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 (Klassifizierung)
Polynomdivision mit dem Euklidischen Algorithmus
Beschränkung auf $\mathbb{Z}$[x], Faktorisierung von Polynomen nach Kronecker
Effiziente quadratfreie Faktorisierung von Polynomen
Anwendung der Polynomarithmetik: Rationale Funktionen (Bruchdarstellung, Kürzen)

Zusammenfassung: Computer-Algebra

Kapitel 7: Polynomiale Gleichungssysteme

Algebraische Grundlagen dazu: Matrizen und Determinanten
Sylvestermatrix und Resultante
Definition und algebraisches Grundverständnis: Was können wir als Lösung erwarten?
Lösung eines Gleichungssystems mit Resultanten und Faktorisierung bei der Rücksubstitution

Kapitel 8: Effiziente Faktorisierung von Polynomen

Berlekamp-Algorithmus für $\mathbb{Z}_p$ (Funktionsweise und Beispiele)
Interpretation der Lösung in Matrixdarstellung
Quadratfreie Faktorisierung für Spezialfall a‘(x) ≡ 0
Polynomfaktorisierung mit der Zassenhaus-Schranke: Schluss von $\mathbb{Z}_p$ auf $\mathbb{Z}$
Grundprinzip und Vorteil des Hensel-Liftings