

L3/L4-Seminar: Computeralgebra

Wintersemester 2016/17

Prof. Werner M. Seiler, Ph.D.

1. Langzahlarithmetik. Komplexität der Schulverfahren zur Arithmetik; schnelle Multiplikation nach Karatsuba und deren Komplexität; Rekursion und Iteration; Divide&Conquer-Algorithmen. [K, 2.4, 2.6, 3.2], [B, 2.5], [P, 3.2], [GG, 2.1-3,8.1]

2. Division mit Rest. Strenge mathematische Formulierung und Beweis; Zusammenhang mit Zahldarstellungen; algorithmische Formulierung; Rechnen mit Resten. [K, 3.3], [S, 2], [SP, 1.1/2], [GG, 2.4]

3. Modulare Arithmetik. Äquivalenzrelationen; Grundbegriffe zu Ringen (Einheiten, Nullteiler, prim, irreduzibel); Restklassen und der Restklassenring. [K, 4.1], [S, 2, A], [F, II.1.1/2, II.1.7/8, II.3.2], [SP, 0.1]

4. (Erweiterter) Euklidischer Algorithmus. Größter gemeinsamer Teiler (Existenz, Eindeutigkeit, Bézout-Koeffizienten); (Erweiterter) Euklidischer Algorithmus; Komplexität; modulare Inverse (Restklassenkörper). [K, 3.4], [S, 4, 5], [B, 2.7-10], [SP, 3.1/3], [P, 3.3], [GG, 3,4.3]

5. Chinesischer Restesatz/Kleiner Fermat. Problemstellung beim Chinesischen Restesatz; Beweis des Satzes; Kleiner Satz von Fermat mit Beweis. [K, 4.3, 4.4], [S, 6, 7], [B, 3.11, 3.15], [F, II.2.11], [SP, 4.3], [P, 4.3], [GG, 5.4]

6. Codierungstheorie I. Grundbegriffe der Codierungstheorie; Präfixcodes; Prüfziffern mit Beispielen ISBN, EAN. [K, 5.1-3], [J, 1.1/2], [W, 1]

7. Codierungstheorie II. lineare Codes; fehlerkorrigierende Codes (insbesondere Reed-Solomon); Beispiel CD. [K, 5.4], [J, 1.3/4, 3.4/5], [W, 2,3]

8. Kryptographie. Grundbegriffe; symmetrische vs. asymmetrische Verfahren; Schlüsselaustausch nach Diffie-Hellman; RSA-Verfahren. [K, 5.5], [B, 4.1/2, 9.1, 9.3, 9.5], [GG, 20.1-3], [W, 12]

9. Der univariate Polynomring. Definition; Zusammenhang mit ganzen Zahlen; Arithmetik mit Komplexität; Übertragung Division mit Rest, Euklid, Karatsuba. [K, 6.1, 6.2, 6.3], [P, 6.1-3, 6.7], [GG, 2.2]

10. Schnelle Multiplikation mit FFT. Einheitswurzeln; diskrete Fourier-Transformation (DFT); inverse DFT; Multiplikation mit schneller Fourier-Transformation (FFT). [K, 6.3], [GG, 8.2]

11. Faktorisierung und Nullstellen. Existenz und Eindeutigkeit Faktorisierung; Zusammenhang mit Nullstellen; Quadratfreiheit; mehrfache Nullstellen; Vergleich \mathbb{Q} und $\mathbb{Z}/p\mathbb{Z}$. [K, 6.7, 6.8], [SP, 11.1], [P, 6.5]

12. Faktorisierung in Polynomringen I. Primitive Polynome, Lemma von Gauß, Zusammenhang \mathbb{Z} und \mathbb{Q} ; Kronecker-Faktorisierung. [K, 6.7, 8.1], [F, II.3.7], [GG, 6.2,15.1]

13. Faktorisierung in Polynomringen II. Berlekamp-Algorithmus; quadratfreie Faktorisierung. [K, 8.2, 8.3], [SP, 11.2], [GG, 14.8]

13. Faktorisierung in Polynomringen III. Zassenhaus-Algorithmus; Hensel-Lifting. [K, 8.4, 8.5], [GG, 15.4,15.6]

Literatur

- [B] J. Buchmann: Einführung in die Kryptographie
- [F] G. Fischer: Lehrbuch der Algebra
- [GG] J. von zur Gathen, J. Gerhard: Modern Computer Algebra
- [J] D. Jungnickel: Codierungstheorie
- [K] Wolfgang Koepf: Computeralgebra
- [P] A. Pethö: Algebraische Algorithmen
- [S] W.M. Seiler: Modulares Rechnen (Kurzschrift zur Schüler-AG)
- [SP] R. Schulze-Pillot: Elementare Algebra und Zahlentheorie
- [W] W. Willems: Codierungstheorie und Kryptographie