

Proseminar Zahlentheorie

Ulrich Derenthal
derenthal@math.uni-hannover.de

Sommersemester 2023, dienstags, 14–16 Uhr, Raum A 410

Zum Proseminar gehören ein 90-minütiger Vortrag mit einer schriftlichen Ausarbeitung. Auch die aktive Teilnahme an den anderen Vorträgen wird erwartet. Jeder Vortrag sollte mit mir vorbesprochen werden (spätestens in der Vorwoche des Vortrags); dann sollten Sie sich schon intensiv mit den Inhalten auseinandergesetzt haben, und der Vortrag sollte möglichst weit vorbereitet sein.

Die Literatur finden Sie im *Semesterapparat* zum Proseminar in der TIB und größtenteils auch online (in StudIP unter *Dateien* verlinkt, aus dem Uni-Netz oder von zu Hause per VPN frei zugänglich).

Die Inhalte und Literaturhinweise zu den Vorträgen sind als Anhaltspunkte gedacht – darauf aufbauend müssen Sie selbst einen interessanten und lehrreichen Vortrag gestalten. Beachten Sie unbedingt die Hinweise *Wie halte ich einen gelungenen Seminarvortrag?*

1. Primzahlen (25.4.)

Satz von Euklid; Aussage des Primzahlsatzes; Vermutungen über Primzahlen; Satz von Tschebyscheff. [Wol11, 1.4], [Apo76, 4.1–4.5], [Cha68, VII.1–VII.2].

2. Euklidischer Algorithmus und Kettenbrüche (2.5.)

Größter gemeinsamer Teiler; Euklidischer Algorithmus; Eindeutigkeit der Primfaktorzerlegung; Kettenbruchalgorithmus für rationale Zahlen. [Sch07, 1.1–1.2], [MSP11, 10 (bis 10.5)], [Apo76, 1], [HW79, I–II, X].

3. Unendliche Kettenbrüche (9.5.)

Kettenbruchalgorithmus für irrationale Zahlen; Konvergenz der Kettenbruchentwicklung; periodische Kettenbrüche (Euler/Lagrange); rationale Approximation. [MSP11, 10 (bis 10.11 und 10.20)], [HW79, X].

4. Restklassen und Kongruenzen I (16.5.)

Die additive Gruppe $\mathbb{Z}/n\mathbb{Z}$; die multiplikative Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$; Rechnen mit Restklassen; Euler'sche φ -Funktion; kleiner Satz von Fermat; Anwendung: RSA-Verfahren. [Sch07, 1.3–1.4], [MSP11, Seite 29/30], [Apo76, 5.1–5.2, 5.4], [Cha68, II.1–II.2], [HW79, 5.2, 5.4, 5.5, 6.1].

5. Restklassen und Kongruenzen II (23.5.)

Polynomkongruenzen; Primitivwurzeln; Anwendung: Diffie–Hellmann-Protokoll. [Sch07, 1.6–1.7], [MSP11, Seite 28/29, §7], [RU08, 6.2].

6. Lineare und quadratische Kongruenzen (6.6.)

Chinesischer Restsatz; lineare und polynomiale Kongruenzen; quadratische Reste und Legendre-Symbol; Formulierung des quadratischen Reziprozitätsgesetzes. [Sch07, 1.3, 2.1–2.2], [RU08, 7.1–7.2], [Apo76, 5.3, 5.5–5.8, 9.1–9.2], [Cha68, II.3, IV.1], [HW79, 6.5].

7. Quadratisches Reziprozitätsgesetz (13.6.)

Beweis des quadratischen Reziprozitätsgesetzes, Anwendungen. [Sch07, 2.2–2.3], [RU08, 7.2], [Dud78, 12], [Apo76, 9.3–9.6], [HW79, 6.6–6.13].

8. Diophantische Gleichungen I (20.6.)

Hindernisse für die Lösung diophantischer Gleichungen, lineare Gleichungssysteme. [Sch07, 3.1–3.2].

9. Diophantische Gleichungen II (27.6)

Satz von Chevalley–Warning, Newton-Verfahren für Lösungen modulo Primzahlpotenzen. [Sch07, 3.3–3.4].

10. Die Gleichung von Lind und Reichardt (4.7.)

Eine unlösbare diophantische Gleichung ohne lokale Hindernisse. [Sch07, 3.5].

11. Summen von Quadraten (11.7.)

Summen von zwei Quadraten; Satz von Lagrange über Summen von vier Quadraten. [Sch07, 2.4], [Dud78, 19], [Cha68, IV.3–IV.4], [HW79, XX].

12. Rationale Approximation (18.7.)

Approximation von irrationalen durch rationale Zahlen; Satz von Hurwitz. [Cha68, III].

Literatur

- [Apo76] T. M. Apostol. *Introduction to analytic number theory*. Springer-Verlag, New York, 1976. Undergraduate Texts in Mathematics.
- [Cha68] K. Chandrasekharan. *Introduction to analytic number theory*. Die Grundlehren der mathematischen Wissenschaften, Band 148. Springer-Verlag New York Inc., New York, 1968.
- [Dud78] U. Dudley. *Elementary number theory*. W. H. Freeman and Co., San Francisco, Calif., second edition, 1978. A Series of Books in the Mathematical Sciences.
- [HW79] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.
- [MSP11] S. Müller-Stach and J. Piontkowski. *Elementare und algebraische Zahlentheorie*. Vieweg + Teubner, Wiesbaden, second edition, 2011.
- [RU08] R. Remmert and P. Ullrich. *Elementare Zahlentheorie*. Grundstudium Mathematik. [Basic Study of Mathematics]. Birkhäuser Verlag, Basel, third edition, 2008.
- [Sch07] A. Schmidt. *Einführung in die algebraische Zahlentheorie*. Berlin: Springer, 2007.
- [Wol11] J. Wolfart. *Einführung in die Zahlentheorie und Algebra*. Wiesbaden: Vieweg+Teubner, 2nd revised and extended ed. edition, 2011.