

# Proseminar Zahlentheorie

Wintersemester 2019/2020

Giuliano Gagliardi  
gagliardi@math.uni-hannover.de  
Raum g020

Anmeldung und Themenvergabe per E-Mail oder persönlich

Dieses Proseminar behandelt Themen aus der elementaren Zahlentheorie. Zum Proseminar gehören ein 90-minütiger Vortrag, eine schriftliche Ausarbeitung sowie die aktive Teilnahme an den anderen Vorträgen.

Die Themenvergabe erfolgt per E-Mail oder persönlich. Beginnen Sie möglichst früh mit der Vorbereitung. Ungefähr eine Woche vor dem Vortrag sollte dieser mit mir vorbesprochen werden (und schon möglichst weit vorbereitet sein).

Die Literatur finden Sie in der TIB. Im Laufe des Septembers wird sie dort zur leichteren Auffindbarkeit in einen Semesterapparat zum Proseminar eingestellt werden.

## 1 Primzahlen

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

Größter gemeinsamer Teiler; Euklidischer Algorithmus; Eindeutigkeit der Primfaktorzerlegung; Kettenbruchalgorithmus für rationale Zahlen. [Sch07, 1.1–1.2], [MSP11, 10 (bis 10.5)], [Apo76, 1], [HW08, I–II, X].

## 3 Unendliche Kettenbrüche

Kettenbruchalgorithmus für irrationale Zahlen; Konvergenz der Kettenbruchentwicklung; periodische Kettenbrüche (Euler/Lagrange); rationale Approximation. [MSP11, 10 (10.6–10.20)], [HW08, X].

## 4 Restklassen und Kongruenzen I

Die additive Gruppe  $\mathbb{Z}/n\mathbb{Z}$ ; die multiplikative Gruppe  $(\mathbb{Z}/n\mathbb{Z})^*$ ; Rechnen mit Restklassen; Eulersche  $\phi$ -Funktion; kleiner Satz von Fermat; Anwendung: RSA-Verfahren. [Sch07, 1.3–1.4], [MSP11, Zweites Beispiel nach Satz 5.17], [Apo76, 5.1–5.2, 5.4], [Cha68, II.1–II.2], [HW08, 5.2, 5.4, 5.5, 6.1].

## 5 Restklassen und Kongruenzen II

Polynomkongruenzen; Primitivwurzeln; Anwendung: Diffie–Hellmann-Protokoll. [Sch07, 1.6–1.7], [MSP11, Erstes Beispiel nach Satz 5.17 und Kapitel 3], [RU08, Kapitel 6, § 2].

## 6 Lineare und quadratische Kongruenzen

Chinesischer Restsatz; lineare und polynomiale Kongruenzen; quadratische Reste und Legendre-Symbol; Formulierung des quadratischen Reziprozitätsgesetzes. [Sch07, 1.3, 2.1–2.2], [RU08, Kapitel 7, § 1–2], [Apo76, 5.3, 5.5–5.8, 9.1–9.2], [Cha68, II.3, IV.1], [HW08, 6.5].

## 7 Quadratisches Reziprozitätsgesetz

Beweis des quadratischen Reziprozitätsgesetzes; Anwendungen. [Sch07, 2.2–2.3], [RU08, Kapitel 7, § 2], [Dud78, 12], [Apo76, 9.3–9.6], [HW08, 6.6–6.13].

## 8 Diophantische Gleichungen I

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

## 9 Diophantische Gleichungen II

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

## 10 Die Gleichung von Lind und Reichardt

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

## 11 Summen von Quadraten

Summen von zwei Quadraten; Satz von Lagrange über Summen von vier Quadraten. [Sch07, 2.4], [Dud78, 19], [Cha68, IV.3–IV.4], [HW08, XX].

## Literatur

- [Apo76] Tom M. Apostol. *Introduction to analytic number theory*. Springer-Verlag, New York-Heidelberg, 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] Underwood Dudley. *Elementary number theory*. W. H. Freeman and Co., San Francisco, Calif., second edition, 1978. A Series of Books in the Mathematical Sciences.
- [HW08] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.
- [MSP11] Stefan Müller-Stach and Jens Piontkowski. *Elementare und algebraische Zahlentheorie*. Vieweg + Teubner, Wiesbaden, second edition, 2011.
- [RU08] Reinhold Remmert and Peter Ullrich. *Elementare Zahlentheorie*. Grundstudium Mathematik. Birkhäuser Verlag, Basel, third edition, 2008.
- [Sch07] Alexander Schmidt. *Einführung in die algebraische Zahlentheorie*. Springer, Berlin, 2007.
- [Wol11] Jürgen Wolfart. *Einführung in die Zahlentheorie und Algebra*. Wiesbaden: Vieweg+Teubner, 2nd revised and extended edition, 2011.