

Seminar S1G1 “Elementare Zahlentheorie”

Donnerstag 10-12, Raum N 0.007

In diesem Seminar beschäftigen wir uns vor allem mit klassischen Fragestellungen aus der Zahlentheorie: Primfaktorzerlegung in \mathbb{Z} und ihre Analoga in allgemeineren Zahlbereichen, Verteilung von Primzahlen, Untersuchung von Restklassenringen. Wir gehen dabei hauptsächlich nach dem Buch “Elementare Zahlentheorie” [RU08] von Remmert und Ullrich vor.

Vortrag 1, 05.04.2012: *Primfaktorzerlegung, größter gemeinsamer Teiler und Euklidischer Algorithmus* ([RU08, Kapitel 1.2 und 2.1])

Vortrag 2, 12.04.2012: *Die schwache Version des Primzahlsatzes*
([RW09, Kapitel 4.3 - 4.4] oder [IR82, Kapitel 2.4])

Vortrag 3, 19.04.2012: *Zahlentheoretische Funktionen*
([RU08, Kapitel 2.3])

Vortrag 4, 26.04.2012: *Zahlentheorie in Integritätsringen*
([RU08, Kapitel 3.0 - 3.1])

Vortrag 5, 03.05.2012: *Faktorielle Ringe, Hauptidealringe und euklidische Ringe* ([RU08, Kapitel 3.2])

Vortrag 6, 10.05.2012: *Zahlentheorie in faktoriellen Ringen*
([RU08, Kapitel 3.3])

Vortrag 7, 24.05.2012: *Kongruenzen*
([RU08, Kapitel 5.1 - 5.2])

Vortrag 8, 14.06.2012: *Restklassenringe*
([RU08, Kapitel 5.3 - 6.1])

Vortrag 9, 21.06.2012: *Zyklische prime Restklassengruppen*
([RU08, Kapitel 6.2])

Vortrag 10, 28.06.2012: *Quadratische Reste*
([RU08, Kapitel 7.1])

Vortrag 11, 05.07.2012: *Das quadratische Reziprozitätsgesetz*
([RU08, Kapitel 7.2])

Vortrag 12, 12.07.2012: *Die Primzahltests von Solovay-Strassen und Miller-Rabin*
([Wol11, Kapitel 5] und [Buc10, Kapitel 8])

Literatur

- [Buc10] Johannes Buchmann. *Einführung in die Kryptographie*. Springer, Berlin, 5. Auflage, 2010. DOI:10.1007/978-3-642-11186-0.
- [IR82] Kenneth F. Ireland und Michael I. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.
- [RU08] Reinhold Remmert und Peter Ullrich. *Elementare Zahlentheorie*. Grundstudium Mathematik. Birkhäuser Verlag, Basel, 3. Auflage, 2008. DOI:10.1007/978-3-7643-7731-1.
- [RW09] Lasse Rempe und Rebecca Waldecker. *Primzahltests für Einsteiger Zahlentheorie – Algorithmik – Kryptographie*. Vieweg + Teubner, Wiesbaden, 2009. DOI:10.1007/978-3-8348-9597-4.
- [Wol11] Jürgen Wolfart. *Einführung in die Zahlentheorie und Algebra*. Vieweg + Teubner, Wiesbaden, 2. Auflage, 2011. DOI:10.1007/978-3-8348-9833-3.