Seminarprogramm

Elementare Zahlentheorie

Universität Duisburg-Essen, Sommersemester 2014

Veranstalter: Prof. Dr. J. Kohlhaase
Ort und Zeit: Raum 3.03 (Thea-Leymann-Straße 9), Di 12–14
Teilnehmerkreis: vornehmlich Lehramt GyGe/Bk
Vorbesprechung: 25.03.2014, 12 c.t., Raum 3.03 (Thea-Leymann-Straße 9)

Inhalt: Die Zahlentheorie befasst sich mit der Struktur der ganzen Zahlen und den bei ihrer Untersuchung auftretenden Problemen. Viele Fragen, wie etwa eine schnelle Berechnung des größten gemeinsamen Teilers zweier ganzer Zahlen, treten bereits in der Schule auf. Das Seminar wird einen Einblick in die grundlegenden Denkweisen und Anwendungen der Zahlentheorie geben und richtet sich ausdrücklich an Studierende der Lehrämter.

Behandelte Themen: Primfaktorzerlegung, Euklidischer Algorithmus, Kongruenzen und Restklassenringe, Primzahlen und Kryptographie, quadratische Reziprozität, Diophantische Gleichungen, Kettenbrüche, Primzahltests.

Falls nicht anders angegeben, beziehen sich im Folgenden alle Referenzen auf die Hauptquelle [1].

1. Primzahlen [08.04.]: ganze Zahlen und Primzahlen; Sieb des Eratosthenes; Satz 1.1 (Euklid); Fermatsche Primzahlen und Lemma 1.4; Mersennesche Primzahlen und Lemma 1.5; recherchieren Sie die derzeit größte bekannte Mersennesche Primzahl; Satz 2.3 mit Beweis (Division mit Rest); beweisen Sie den Satz über die eindeutige Primfaktorzerlegung in $\mathbb{Z}$ (vgl. [2], Satz 1.2.3)

2. Euklidische Ringe [15.04.]: Wiederholen Sie die Begriffe Ring, Ideal, Integritätsring (Appendix B); Definition 2.1 (Teilbarkeit, Einheiten, Assoziiertheit); Assoziiertheit in $\mathbb{Z}$; Lemma 2.2 mit Beweis; Definition 2.5 (Euklidische Ringe); zeigen Sie, dass die Gaußschen Zahlen $\mathbb{Z}[i]$ einen Euklidischen Ring bilden

3. Hauptideal- und faktorielle Ringe [22.04.]: Definition 2.8 (Hauptidealringe); Satz 2.9 (Euklidische Ringe sind Hauptidealringe); Bemerkung 2.10 (Eindeutigkeit bis auf Assoziiertheit); Definition 2.11 (prim, irreduzibel, reduzibel); prim $\Rightarrow$ irreduzibel (Bemerkung 2.12), die Umkehrung gilt im Allgemeinen aber nicht (Aufgabe 2.13); Definition 2.14 (faktorielle Ringe); Lemma 2.15 (irreduzibel $\Rightarrow$ prim in faktoriellen Ringen, sowie Eindeutigkeit der Primfaktorzerlegung); Satz 2.18 (Hauptidealringe sind faktoriell)

4. Euklidischer Algorithmus [29.04.]: Definition 3.1 (ggT in faktoriellen Ringen); beweisen Sie Lemma 3.2 Teil 2; Satz 3.3 (Existenz des ggT); Satz 3.5 (ggT in Hauptidealringen); Sätze 3.7 & 3.9 (Euklidischer Algorithmus und seine Erweiterung); Erläuterung anhand eines Beispiels; Definition 3.12 (kgV); Satz 3.13. (Zusammenhang kgV & ggT)

5. Kongruenzrechnung [06.05.]: Definition 4.1 mit Beispielen; Satz 4.2 (Rechenregeln für Kongruenzen); Lemma 4.7 mit Beweis; beweisen Sie die Teilbarkeitskriterien für Division durch 3 bzw. 11; Satz 4.5 & Hilfssatz 4.6 (kleiner Satz von Fermat); lösen Sie Aufgabe 4.14; recherchieren Sie, was man unter dem großen Satz von Fermat versteht und wie man pythagoräische Tripel konstruiert

6. Chinesischer Restsatz [13.05.]: Satz 4.8 (Lösbarkeit von Gleichungen mit Kongruenzen); Erläuterung anhand von Aufgabe 4.9; Korollar 4.10 mit Beweis; Satz 4.11 (Chinesischer Restsatz, 1. Version) und anschließendes Beispiel; Korollar 4.12 (Lösungsmenge simultaner Kongruenzen) und anschließendes Beispiel; lösen Sie Aufgabe 4.18

7. Restklassenringe [20.05.]: Wiederholen Sie die Begriffe Äquivalenzrelation und Äquivalenzklasse; Lemma 5.1 und Definition 5.2 ($\mathbb{Z}/n\mathbb{Z}$ als Menge); Lemma 5.3 (Mächtigkeit von $\mathbb{Z}/n\mathbb{Z}$); Satz 5.4 (Ringstruktur); Verknüpfungstafel für $\mathbb{Z}/4\mathbb{Z}$; der Ringhomomorphismus $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ für $m|n$; Satz 5.5 (Chinesischer Restsatz, 2. Version) und Korollar 5.8; Definition 5.9 & Satz 5.10 (die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$)

8. Die Sätze von Euler und Wilson [27.05.]: Definition 5.12 (Eulersche φ-Funktion); Lemma 5.13 (Multiplikativität von φ); Lemma 5.14 & Satz 5.15 (Berechnung von φ); Satz 5.17 (Euler) ohne Beweis; erklären Sie aber, inwiefern es sich um eine Verallgemeinerung von Satz 4.5 handelt; erläutern Sie das RSA-Verfahren aus der Kryptographie; Satz 5.18 (wann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper); Satz 5.21 (Wilson)

9. Quadratische Reziprozität [03.06.]: Quadratische Reste und Nichreste modulo p; Definition 8.2 (Legendre-Symbol); formulieren Sie Satz 7.1 ohne Beweis und führen Sie den Begriff einer Primitivwurzel ein; Lemma 8.3 (Legendre-Symbol und Primitivwurzeln); Satz 8.5 (Rechenregeln für das Legendre-Symbol); Lemma 8.6 & Satz 8.7 ohne Beweis (Reziprozitätsgesetz und Ergänzungssatz); das Beispiel $\left(\frac{59}{89}\right) = -1$

10. Quadratsätze [10.06.]: Lemma 7.14 (Quadratwurzeln aus -1; Beweis mit Satz 8.5 Teil 2); Satz 9.1 (Primzahlen als Summe zweier Quadrate); Korollar 9.2 (Zwei-Quadrate-Satz); Lemma 9.5 (die Gleichung $x^2 + y^2 = -1 \mod p$); Satz 9.6 (Vier-Quadrate-Satz von Lagrange) ohne Beweis; erklären Sie aber ausführlich, wie man sich mit Hilfe der Hamiltonschen Quaternionen auf den Fall einer Primzahl beschränken kann

11. Kettenbrüche I [17.06.]: Definition von Kettenbrüchen; $[1, 1, 1, \ldots] = (1 + \sqrt{5})/2$; Kettenbruchalgorithmus; Satz 10.4 (Endlichkeit und Rationalität); Kettenbruchdarstellungen sind nicht eindeutig; Lemmata 10.6 & 10.7 (Vorbereitungen zum Konvergenzsatz)

12. Kettenbrüche II [24.06.]: Sätze 10.8 & 10.9 (Konvergenzsätze); Kettenbruchentwicklung von e; Approximation von π durch endliche Kettenbrüche; Satz 10.12 (periodische Kettenbrüche und quadratische Gleichungen)

13. Endlich erzeugte abelsche Gruppen [01.07.]: Definition 6.1 (Erzeugung von Untergruppen); Lemma 6.3 (Beschreibung erzeugter Untergruppen); Lemma 6.5 und anschließende Beispiele; Satz 6.6 (Struktur zyklischer Gruppen; recherchieren Sie für den Beweis, was der Homomorphiesatz für Gruppen besagt); Bemerkung 6.7 (Charakterisierung von Erzeugern); erklären Sie, was eine Präsentation einer endlich erzeugten abelschen Gruppe ist; formulieren Sie Lemma 6.11 ohne Beweis; erläutern Sie, wie man daraus zusammen mit dem Diagonalisierungsalgorithmus einen Beweis des grundlegenden Satzes 6.13 erhält

14. Die Einheitengruppen der Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ [08.07.]: Weisen Sie nach, dass die Gruppe U_7 zyklisch ist, die Gruppe U_8 aber nicht; Sätze 7.1 und 7.2 (endliche Untergruppen in Körpern); Definition 7.3 (Primitivwurzel); Lemma 7.4 (Charakterisierung von Primitivwurzeln) ohne Beweis, aber mit Beispiel; Hilfssatz 7.5; Satz 7.7 mit Beispiel (Zyklizität für ungerade Primzahlpotenzen); Satz 7.9 (Stuktur für Zweierpotenzen); Definition von $\exp_\zeta$, $\log_\zeta$ und Lemma 7.12; beweisen Sie als Anwendung Lemma 7.14

15. Primzahltests [15.07.]: Satz 11.1 mit Beispiel (Lucas-Lehmer-Test für Mersennesche Primzahlen); Satz 11.3 (Lucas-Test); Satz 11.5 (Pocklington-Test); Satz 11.6 mit Beispiel (Pepin-Test für Fermatsche Primzahlen); Definition 11.8 (Carmichael-Zahlen); Satz 11.9 ohne Beweis; leiten Sie daraus Korollar 11.8 ab; Beispiele von Carmichael-Zahlen; Satz 11.12 (Solovay-Strassen-Test); erläutern Sie hieran, was ein probabilistischer Primzahltest ist

Literatur

[1] S. Müller-Stach, J. Piontkowski: Elementare und algebraische Zahlentheorie – Ein moderner Zugang zu klassischen Themen, 2. Auflage, Vieweg+Teubner, 2011

[2] A. Schmidt: Einführung in die algebraische Zahlentheorie, Springer, 2007

Im Internet finden Sie darüber hinaus zahlreiche Skripten zur Elementaren Zahlentheorie, die Sie ergänzend hinzuziehen können.