M. Witte
Universität Paderborn
Sommersemester 2015

Seminar über elementare Zahlentheorie (HRG)

Inhalt

Elementare Zahlentheorie ist ein Teilgebiet der Mathematik, das sich in erster Linie mit Eigenschaften der ganzen Zahlen beschäftigt. Bis ins siebzehnte Jahrhundert hinein waren die wichtigsten Hilfsmittel dabei die Primfaktorzerlegung, Teilbarkeitsregeln und das Rechnen mit Kongruenzen. Einige zentrale Resultate, die sich mit Hilfe dieser elementaren Methoden erzielen lassen, werden wir in diesem Seminar diskutieren.

Teilnehmerkreis und Vorkenntnisse

Das Seminar richtet sich vornehmlich an Studenten im Studiengang *Master Lehramt Mathematik HRG*. Grundlegende Kenntnisse der Schulmathematik werden vorausgesetzt.

Prüfungsmodalitäten

Studienleistung: aktive Teilnahme, Vorbesprechung zum Vortrag
Prüfungsleistung: Vortrag
Wiederholung der Prüfungsleistung bei Nichtbestehen: schriftliche Ausarbeitung des Vortrags

Anmeldung und Vortragsvergabe

Bitte melden Sie sich frühzeitig bei PAUL zu dieser Veranstaltung an. Sobald die Liste der Teilnehmer feststeht, wird an je zwei Studenten eines der Themen aus der untenstehenden Liste vergeben. Über den genauen Vergabemodus werde ich die angemeldeten Teilnehmer rechtzeitig informieren.

Kontakt

Malte Witte,
Universität Paderborn, D3.221
malte.witte@math.uni-paderborn.de,
Tel. +49-5251-60-2647

Zum Ablauf

Zu den jeweiligen Termin halten die beiden Studenten gemeinsam einen Vortrag über das ihnen zugeteilte Thema. Ziel des Vortragenden sollte es sein, den von ihm zu behandelnden Stoff selbst zu verstehen und ihn auch versändlich an die übrigen Seminarteilnehmer vermitteln zu können.

Sie sollten den Vortrag in etwa gleichmäßig unter sich aufteilen. Insgesamt soll die Dauer von 90 Minuten nicht überschritten werden. Wenn die Vortragszeit nicht auszureichen scheint, muss eine sinnvolle Auswahl des Stoffes getroffen werden.

Die Vorträge sollen an der Tafel gehalten werden. Ausnahmen davon sind nach Rücksprache mit mir möglich. Eine schriftliche Ausarbeitung wird nicht verlangt; jedoch kann durch sie ein mangelhafter Vortrag ausgeglichen werden. Eine aktive und konstruktive Seminarteilnahme wird erwartet.

Für Rückfragen und zur Klärung von Verständnisschwierigkeiten bei der Vortragsausarbeitung stehe ich Ihnen gerne zur Verfügung. Bitte vereinbaren Sie dazu möglichst frühzeitig gemeinsam mit Ihrem Vortragspartner einen Termin mit mir. Ein Termin spätestens eine Woche vor Ihrem Vortrag ist dabei Pflicht. Dort sollten Sie mit mir Ihr Vortragskonzept durchsprechen.

Eine ausführliche Anleitung, wie man einen guten Seminarvortrag hält, findet man hier:

`http://www.mathematik.uni-mainz.de/Members/lehn/le/seminarvortrag`

Vorträge

1. Vortrag: **Teilbarkeit und Primfaktorzerlegung**

Zunächst sollen die Teilbarkeitsrelation auf den ganzen Zahlen eingeführt und einige elementare Eigenschaften nachgewiesen werden [P, Kap. I, §1–§3, Def. 4]. Anschließend soll gezeigt werden, dass jede natürliche Zahl $n > 1$ eine eindeutige Primfaktorzerlegung besitzt [P, Kap. II, §1, §2].

2. Vortrag: **Der ggT und der euklidische Algorithmus**

Es soll der größte gemeinsame Teiler zweier natürlicher Zahlen a, b eingeführt werden und es soll gezeigt werden, wie man ihn aus der Primfaktorzerlegung von a und b bestimmen kann [P, Kap. III, §1, §2]. Danach soll der euklidische Algorithmus zur Berechnung des ggT vorgestellt werden [P, Kap. III, §3.1–3.3]. Falls die Zeit es zulässt, kann danach noch auf lineare diophantische Gleichungen mit 2 Variablen eingegangen werden [P, Kap. III, §3.4].

3. Vortrag: **Kongruenzen**

In diesem Vortrag wird das Rechnen mit Restklassen eingeführt und es wird gezeigt, dass die Menge der Restklassen zu einem festen Modul eine Partition der ganzen Zahlen bildet [P, Kap. IV, §1–§3, Satz 9]. Je nachdem, wie es die Zeit erlaubt, kann der Stoff dadurch angereichert werden, dass einige der Übungsaufgaben aus [P, Kap. IV, §2] vorgeführt werden.

4. Vortrag: **Kongruenzen II**

Es sollen die Restklassenaddition und -multiplikation eingeführt werden. Die Menge der Restklassen zu einem festen Modul bildet bezüglich dieser beiden Verknüpfungen einen kommutativen Ring. Es wird untersucht, wann dieser Ring nullteilerfrei ist [P, Kap. IV, §3, ab Satz 10]. Anschließend werden die Sätze von Euler und Fermat bewiesen und es wird auf Teilbarkeitsregeln eingegangen, welche die dezimale Quersumme benutzen [P, Kap. IV, §4.1, §4.2].

5. Vortrag: **Primzahlen**

Zunächst soll durch den klassischen Beweis von Euklid gezeigt werden, dass es unendlich viele Primzahlen gibt. Danach sollen noch einige weitere Beweise für diese Tatsache gegeben werden [AZ, Kap. I]. Im Anschluss daran soll das „Sieb des Eratosthenes“ vorgestellt werden [P, Kap. V, §1] und es sollen noch einige elementare Aussagen über die Verteilung der Primzahlen gezeigt werden [P, Kap. V, §1, ab Satz 2, §2].

6. Vortrag: **Die Eulersche φ-Funktion**

Es wird die eulersche φ-Funktion eingeführt und gezeigt, dass für teilerfremde natürliche Zahlen m, n die Gleichung $\varphi(mn) = \varphi(m)\varphi(n)$ gilt. Anschließend wird eine auf Gauß zurückgehende Summenformel für die eulersche φ-Funktion gezeigt [P, Kap. VI, §1, §2]. Der Vortragsstoff kann dadurch angereichert werden, dass einige der Übungsaufgaben aus [P, Kap. VI, §1] vorgeführt werden.

7. Vortrag: **g-adische Zahlsysteme**

In diesem Vortrag wird gezeigt, dass sich – in Verallgemeinerung der üblichen Dezimaldarstellung – jede natürliche Zahl bezüglich einer beliebigen Basis $g \in \mathbb{N} \setminus \{1\}$ eindeutig entwickeln lässt. Es werden die Algorithmen für die Grundrechenoperationen studiert und Teilbarkeitsregeln unter Verwendung der g-adischen Entwicklung hergeleitet [P, Kap. VII, §1–§3].

8. Vortrag: **Dezimalbrüche**

Der Vortrag beschäftigt sich mit der Dezimalbruchentwicklung rationaler Zahlen. Es sollen Kriterien dafür hergeleitet werden, wann die Dezimalbruchentwicklung einer rationalen Zahl endlich bzw. (rein) periodisch ist [P, Kap. VIII, §1–§3]. Je nachdem, wie es die Zeit erlaubt, kann auch noch auf Verallgemeinerungen im Hinblick auf g-adische Entwicklungen eingegangen werden [P, Kap. VIII, §4].

9. Vortrag: **Vollkommene Zahlen / Fibonaccizahlen**

Im ersten Teil des Vortrages werden die sogenannten vollkommenen Zahlen studiert. Eine natürliche Zahl n heißt vollkommen, wenn die Summe der positiven Teiler von n genau $2n$ ergibt. Insbesondere soll eine auf Euler zurückgehende Charakterisierung vollkommener Zahlen gezeigt werden [P, Kap. IX, §1]. Der zweite Teil des Vortrags ist den Fibonacci-Zahlen gewidmet. Es werden vorschiedene Rekursionsformeln hergeleitet [P, Kap. IX, §2].

10. Vortrag: **Das RSA-Verfahren**

In diesem Vortrag soll das RSA-Verfahren vorgestellt werden – ein Verschlüsselungsverfahren, dessen Grundidee elementar zahlentheoretischer Natur ist [B, Kap. 7, §1, §2].

11. Vortrag: **Die Funktion $[x]$**

Für reelle Zahlen x bezeichnet $[x]$ die größte ganze Zahl kleiner oder gleich x. Im Vortrag werden einige Eigenschaften dieser Funktion studiert [NZ1, Kap. 4, §1]. Als Anwendung soll eine Formel zur Bestimmung des Wochentages aus dem Datum diskutiert werden [NZ2, S. 357].

12. Vortrag: **Das Bertrand'sche Postulat**

Das Bertrand'sche Postulat besagt, dass es für jede natürliche Zahl n stets eine Primzahl gibt, welche im Intervall $[n, 2n]$ liegt. Es soll der von Erdös gegebene Beweis dieser Aussage vorgeführt werden [AZ, Kap. 2].

13. Vortrag: **Summen von zwei Quadraten**

Eine natürliche Zahl n kann genau dann als Summe von 2 Quadraten geschrieben werden, wenn in der Primfaktorzerlegung von n jeder Primfaktor der Form $p = 4m + 3$ mit geradem Exponenten auftritt. In diesem Vortrag soll ein sehr eleganter, auf Heath-Brown zurückgehender Beweis dieser Aussage vorgeführt werden [AZ, Kap. 4]. Zur besseren Illustration des Beweises sollte ein Beispiel komplett ausgearbeitet werden.

Literatur

[AZ] Aigner, M., Ziegler, G.: *Das Buch der Beweise*, Springer Verlag, Berlin 2002

[B] Buchmann, J.: *Einführung in die Kryptographie*, Springer Verlag, Heidelberg 2004

[NZ1] Niven, I., Zuckerman, H. S.: *Einführung in die Zahlentheorie I*, BI Wissenschaftsverlag, Mannheim 1976

[NZ2] Niven, I., Zuckerman, H. S.: *Einführung in die Zahlentheorie II*, BI Wissenschaftsverlag, Mannheim 1976

[P] Padberg, F.: *Elementare Zahlentheorie*, BI Wissenschaftsverlag, Mannheim 1989