Prof. Dr. Stefan Schreieder Sommersemester 2021

Proseminar Zahlentheorie

Di 16:15-17:45

Dieses Proseminar bietet eine Einführung in die Zahlentheorie. Dabei werden mehrere klassische, berühmte und wichtige Ergebnisse über die ganzen Zahlen und der Lösbarkeit von Gleichungen in den ganzen (oder rationalen) Zahlen besprochen.

Die primäre Quelle für das Seminar ist das exzellente Buch von Schmidt [Sch07], welches über die TIB als e-book frei zugänglich ist. Das Buch von Schmidt ist oft etwas knapp aber auch sehr elegant formuliert. Eine etwas ausführlichere Quelle für den ersten Teil des Seminars ist zum Beispiel durch das Buch von Bundschuh gegeben [Bun02].

Der oder die Vortragende soll ihren Teil vollständig verstanden haben und in eigenen Worten und selbstständiger Ausschmückung (zB mit kleinen Beispielen) vorstellen. Ziel dabei muss immer sein, dass die Kommilitonen Ihren Vortrag möglichst gut verstehen können. Sie sprechen also in erster Linie zu den Kommilitonen und nicht zu mir.

Ein Vortrag der sich im Wesentlichen darauf beschränkt das Buch vorzulesen, ohne dass die Inhalte verstanden wurden, wird mit nicht ausreichend bewertet.

Das Seminar wird online auf zoom stattfinden (der link geht per email an alle TeilnehmerInnen). Vorträge sollen live gehalten werden, zB indem man sich mit der Handykamera eine Dokumentenkamera bastelt und damit ein weißes Blatt Papier filmt, auf dem man schreiben kann. Ebenso kann natürlich auch ein Tablet als Eingabegerät verwendet werden, wenn Ihnen dies zur Verfügung steht. Grundsätzlich wäre auch das Verwenden einer Präsentation denkbar, die man zB auf LaTex mit der Documentclass beamer erstellen kann (ähnlich zu powerpoint, das im Grunde auch verwendet werden kann, aber in der Mathematik eigentlich unüblich ist). Hier ist allerdings darauf zu achten, dass Folienvorträge in der Mathematik oft zu schnell und dadurch unverständlich sind, sodass man hier besonders sorgfältig vorgehen müsste.

Zusätzlich zu Ihrem Vortrag muss jede Teilnehmerin und jeder Teilnehmer eine Ausarbeitung mit TeX (`https://de.wikipedia.org/wiki/TeX`) anfertigen. Diese soll wenige Seiten umfassen und nicht länger als max. 6 Seiten sein. Die Ausarbeitung kann Teile Ihres Vortrags umfassen, sowie Übungsaufgaben die in [Sch07] angegeben werden und zu Ihrem Thema passen. Es geht hier in erster Linie darum, dass Sie bereits vor der Bachelorarbeit den Umgang mit TeX bzw LaTeX erlernen und das Verfassen von mathematischen Texten üben.

Jede(r) Vortragende soll etwa zwei Wochen vor dem Vortragstermin den Vortrag kurz mit mir besprechen. Bei dieser Gelegenheit können auch Fragen gestellt werden. In der Regel sollen diese Besprechungen direkt nach dem regulären Sitzungstermin (Di 16:15-17:45) stattfinden. Die ersten beiden Vortragenden sollen bitte per email einen Termin mit mir vereinbaren.

1. **Primzahlen und Teilbarkeit [Sch07, §1.1-1.2], [Bun02, §1.1.1- 1.1.4] (Ce.Du. 13.4.)**

   In diesem Vortrag sollen die Ergebnisse aus [Sch07, §1.1] und der erste Teil von [Sch07, §1.2] vorgestellt werden.

   Stellen Sie die Inhalte aus [Sch07, §1.1] bis Satz 1.1.4 vor. Formulieren Sie Satz 1.1.4. Bevor Sie den Beweis angeben, wiederholen Sie was Division mit Rest bedeutet und

warum eine solche Division mit Rest existiert; dies wird im Detail in [Bun02, §1.2.2] erklärt. Jetzt können Sie den Beweis von [Sch07, Satz 1.1.4] angeben und danach die Anwendungen 1.1.5-1.1.7 besprechen.

Führen Sie Primzahlen ein und besprechen Sie [Sch07, §1.2] bis einschließlich Satz 1.2.3 und Korollar 1.2.4. Wenn Sie Lemma 1.2.2 besprechen, so zeigen Sie, dass eine natürliche Zahl $p > 1$ genau dann eine Primzahl ist, wenn aus $p \mid ab$ schon $p \mid a$ oder $p \mid b$ folgt.

2. **Primzahlverteilung, Kongruenzen und chinesischer Restsatz [Sch07, §1.2-1.3] (So.Sa. 20.4.)**

   Beweisen Sie [Sch07, Theorem 1.2.5] und erklären Sie, weshalb dies bedeutet, dass es in einem wohlbestimmten Sinne (viel) mehr Primzahlen als Quadratzahlen gibt. Beweisen Sie Satz 1.2.6.

   Wiederholen Sie kurz was es bedeutet, dass zwei Zahlen kongruent modulo einer dritten Zahl sind (siehe [Sch07, Definitionen 1.3.1 und 1.3,3]). Die Begriffe Relation und Äquivalenzrelation dürfen ebenso wie Lemma 1.3.2 als bekannt vorausgesetzt werden, es sollte lediglich kurz an diese Dinge erinnert werden. Die Schreibweise $a \equiv b \mod m$ ist eventuell neu (wurde zum Beispiel nicht in der Linearen Algebra 1 verwendet) und sollte erklärt werden. Ebenso sollte man an die Regeln in [Sch07, Lemma 1.3.4] erinnern.

   Beweisen Sie nun den chinesischen Restklassensatz [Sch07, Satz 1.3.5]. Erklären Sie die Bemerkung nach Satz 1.3.5. Erklären Sie, was prime Restklassen sind, zeigen Sie Lemma 1.3.7 und beweisen Sie Satz 1.3.9 und Korollare 1.3.10–1.3.12 in [Sch07].

3. **Eulersche φ-Funktion und Kleiner Satz von Fermat, [Sch07, §1.3-1.4] (Ay.Gü. 27.4.)**

   Führen Sie die Eulersche φ-Funktion ein (siehe Definition 1.3.13 in [Sch07]). Zeigen Sie 1.3.14–1.3.17.

   Zeigen Sie den Satz von Wilson sowie den kleinen Fermatschen Satz, siehe [Sch07, Satz 1.4.1 und 1.4.2]. Beweisen Sie [Sch07, Korollar 1.4.4]. Geben Sie einen alternativen Beweis von [Sch07, Korollar 1.4.4] indem Sie die Aufgabe am Ende von [Sch07, §1.4] lösen.

4. **Primzahlen zu vorgegebenen Resten und Polynomkongruenzen [Sch07, §1.5-1.6] (Fe.Go. 4.5.)**

   Erinnern Sie kurz an [Sch07, Korollar 1.2.4] sowie dessen Beweis. Erklären Sie nun den Beweis von Satz 1.5.1 und Satz 1.5.2 in [Sch07]. Warum funktioniert dieselbe Methode a priori nicht um zu zeigen, dass es unendlich viele Primzahlen kongruent 1 modulo 3 (bzw kongruent 1 modulo 4) gibt? Bearbeiten Sie die Aufgabe am Ende von [Sch07, §1.5] und stellen Sie das Ergebnis kurz vor.

   Erklären Sie, was ganzzahlige Polynome, also Elemente von $\mathbb{Z}[X]$ sind und wann diese kongruent modulo m sind (siehe [Sch07, Definition 1.6.1]). Beweisen Sie für sich Lemma 1.6.2 und stellen nur das Ergebnis im Vortrag vor. Beweisen Sie Satz 1.6.3 und 1.6.4.

5. **Primitive Wurzeln und quadratische Reste [Sch07, §1.7, §2.1] (Jo.Me. 11.5.)**

   Erklären Sie, was die Ordnung einer primen Restklasse modulo p ist, siehe [Sch07, Definition 1.7.1]. Beweisen Sie [Sch07, Satz 1.7.2]. Zeigen Sie [Sch07, Lemma 1.7.3] und geben Sie [Sch07, Definition 1.7.4] an. Beweisen Sie [Sch07, Satz 1.7.5 und Korollar 1.7.6].

   Stellen Sie [Sch07, §2.1] vor. Genauer: Geben Sie [Sch07, Definition 2.1.1] an und veranschaulichen es an einem Beispiel. Zeigen Sie [Sch07, Lemma 2.1.2]. Geben Sie [Sch07, Definition 2.1.3] an und zeigen Sie [Sch07, Lemma 2.1.4]. Zeigen Sie [Sch07, Korollar 2.1.5]. Beweisen Sie [Sch07, Satz 2.1.6 und Korollar 2.1.7] Zeigen Sie [Sch07, Satz

2.1.8] und vergleichen Sie das Ergebnis mit dem Fall von quadratischen Gleichungen $x^2 + ax + b = 0$ mit $a, b \in \mathbb{R}$ (erinnern Sie dazu insbesondere an die Lösungsformel für solche Gleichungen). Zeigen Sie [Sch07, Satz 2.1.9].

6. **Quadratisches Reziprozitätsgesetz [Sch07, §2.2] (To.Di. 18.5.)**

   Beweisen Sie das quadratische Reziprozitätsgesetz von Gauß (§2.2) samt den beiden Ergänzungssätzen (Theorem 2.2.2 und 2.2.3). (Als alternative Quelle, siehe zB [Bun02, §3.2.1 – §3.2.8].) Berechnen Sie als Anwendungen von Satz 2.1.6 und dem quadratischen Reziprozitätsgesetz (Theoreme 2.2.1-2.2.3) ein paar explizite Legendre-Symbole der Form $\left(\frac{a}{p}\right)$. Erklären Sie insbesondere, dass die oben erwähnten Resultate es theoretisch erlauben für jede Primzahl p und jede natürliche Zahl a das Legendre-Symbol $\left(\frac{a}{p}\right)$ zu berechnen.

   Falls noch Zeit bleibt, so stellen Sie den Satz in [Bun02, S. 129, §3.2.2] vor, welcher es erlaubt allgemein die Lösbarkeit von $x^2 \equiv c \mod m$ auf Legendre-Symbole zurückzuführen. Weiterhin könnte man damit die Anwendung in [Bun02, S. 136, §3.2.8] besprechen, die auf die Original Schrift von Gauß zurückgeht.

   Es könnte sich auch lohnen, kurz über die Geschichte des quadratischen Reziprozitätsgesetzes zu sprechen, siehe z.B. [Lem00, Chapter 1]

7. **Anwendungen des Quadratischen Reziprozitätsgesetzes [Sch07, §2.3] (Or.Yi. 1.6.)**

   Erinnern Sie an Satz 1.5.1 und Satz 1.5.2, sowie deren Beweis. Erinnern Sie auch daran, weshalb das analoge Argument nicht für Primzahlen kongruent 1 modulo 3 (bzw 1 modulo 4) funktioniert. Zeigen Sie nun wie das quadratische Reziprozitätsgesetz verwendet werden kann um diese Lücke zu schließen, siehe [Sch07, §2.3]. Genauer: Zeigen Sie Lemma 2.3.1 und Satz 2.3.2 in [Sch07]. Zeigen Sie nun Satz 2.3.3, sowie Lemma 2.3.5 und Satz 2.3.4. Beweisen Sie Satz 2.3.6. Lösen Sie Aufgabe 1 und 2 aus [Sch07, §2.3] und stellen Sie je nach verbleibender Zeit teile davon vor.

8. **Zwei-Quadrate und Vier-Quadrate Satz [Sch07, §2.4] (Pa.Ti. 8.6.)**

   Beweisen Sie den Zwei-Quadrate Satz (Satz 2.4.1 in [Sch07]) sowie den Vier-Quadrate Satz (Satz 2.4.5 in [Sch07]). Sätze 2.4.3. und 2.4.4 sollten gelesen und verstanden werden, können aber im Vortrag aus Zeitgründen weggelassen werden, der Rest von [Sch07, §2.4] sollte vorgestellt werden.

   In [Sch07] wird der Zwei-Quadrate Satz nur für Primzahlen bewiesen. Dieses Resultat kann (ohne großen Aufwand) verwendet werden um allgemein alle natürlichen Zahlen zu bestimmen, die als Summe zweier Quadrate darstellbar sind, siehe [Bun02, S. 157, §4.1.3]. Wenn zeitlich möglich könnte/sollte dieses allgemeinere Resultat als Anwendung von [Sch07, Satz 2.4.1] kurz erwähnt und erklärt werden.

9. **Diophantische Gleichungen und Hindernisse [Sch07, §3.1, 3.2] (Mi.Pa. 15.6.)**

   Erklären Sie was ein ganzzahliges Polynom in mehreren Variablen ist und geben Sie Beispiele an (zB $x_1^2 + x_2^2 - 1$). Formal muss man dazu den Polynomring $R[x]$ über einem kommutativen Ring R betrachten und diese Konstruktion iterative durchführen,. Damit kommt man also von $\mathbb{Z}$, zu $\mathbb{Z}[x_1]$, und davon zu $\mathbb{Z}[x_1, x_2]$, usw.

   Erklären Sie nun was eine Diophantische Gleichung ist, siehe [Sch07, §3]. Erklären Sie weiterhin was reelle Hindernisse und Hindernisse modulo m sind. Geben Sie Beispiele dafür an. Beweisen Sie Satz 3.1.1 und erklären Sie, dass dies im Spezialfall der Gleichung $x^2 - a = 0$ zeigt, dass es eine ganzzahlige Lösung gibt, falls keine Hindernisse modulo jeder (oder fast jeder) Primzahl bestehen.

   Stellen Sie den Inhalt aus [Sch07, §3.2] vor und beweisen Sie 3.2.1-3.2.4 aus [Sch07].

10. **Chevalley–Warning und Diophantische Gleichungen modulo Primpotenzen [Sch07, §3.3, 3.4] (He.Ei. 29.6.)**

    Erklären Sie die am Anfang von [Sch07, §3.3] dargestellte Problemstellung, dass man für eine Anzahl an ganzzahligen Polynomen nach simultanen Lösungen modulo einer Primzahl sucht. Geben Sie ein konkretes Beispiel dafür an. Beweisen Sie dann Theorem 3.3.1 und Korollar 3.3.2. Geben Sie Beispiele von Gleichungen an, in denen Theorem 3.3.1 nicht-triviale Lösungen modulo jeder Primzahl wie in Korollar 3.3.2 garantiert (siehe zB Aufgabe 1 in [Sch07, §3.3]).

    Beweisen Sie Satz 3.4.1 welcher es unter bestimmten Umständen erlaubt, Lösungen modulo beliebiger hoher Primzahl Potenzen zu konstruieren. Erklären Sie den wichtigen Spezialfall von Satz 3.4.1 der in Korollar 3.4.2 angegeben wird und geben Sie ein Beispiel dafür an.

11. **Eine Gleichung ohne rationale Lösungen obwohl keine Hindernisse dafür bestehen [Sch07, §3.5] (Ti.Mü. 6.7.)**

    Stellen Sie die Inhalte von [Sch07, §3.5] vor und beweisen Sie den Satz von Lind Reinhardt (siehe [Sch07, Theorem 3.5.1]).

12. **p-adischer Abstand [Sch07, §9.1] (Le.La. 13.7.)**

    Erinnern Sie an Korollar 3.4.2, welches es erlaubt in bestimmten Situationen von einer einzigen Lösung modulo p Lösungen modulo allen Potenzen von p zu konstruieren. Erklären Sie ebenso, dass die in Korolar 3.4.2 konstruierten Lösungen bezüglich verschiedener Potenzen von p kompatibel sind, in dem in Korollar 3.4.2 formulierten Sinne (die Reduktion bzgl einer gemeinsamen Potenz stimmt überein). Ziel der p-adischen Zahlen ist es, diese Menge an Lösungen elegant zusammenzufassen, zu den sogenannten p-adischen Zahlen.

    Stellen Sie die Ideen und Resultate aus [Sch07, §9.1] vor. Insbesondere sollen die p-Bewertung und der p-adische Abstand auf $\mathbb{Q}$ eingeführt und erklärt werden. Weiterhin sollen einfache Beispiele diskutiert werden und die etwas gewöhnungsbedürftigen Eigenschaften in Satz 9.1.6 erklärt und bewiesen werden.

13. **p-adische Zahlen [Sch07, §9.2] (Jo.Oe. 20.7.)**

    Stellen Sie die Ergebnisse aus [Sch07, §9.2] vor. Konstruieren Sie insbesondere den Körper der p-adischen Zahlen.

    Erklären Sie was die ganzen p-adischen Zahlen sind (siehe [Sch07, Definition 9.3.1]). Zeigen Sie Lemma 9.3.2 und 9.3.3, sowie Satz 9.3.4. Erklären Sie schließlich, dass eine p-adische ganze Zahle einer Folge $(a_n \in \mathbb{Z}/p^n\mathbb{Z})_n$ entspricht, sodass für $n \geq m$ gilt: $a_n \equiv a_m \mod p^m$.

    Verwenden Sie dies um das Resultat in Korollar 3.4.2 neu zu formulieren: Sei $f \in \mathbb{Z}[x]$ ein Polynom in einer Variablen und mit ganzzahligen Koeffizienten. Angenommen es gibt eine ganze Zahl $z_1 \in \mathbb{Z}$ mit $f(z_1) \equiv \mod p$ und $f'(z_1) \not\equiv 0 \mod p$. Dann gibt es eine p-adische ganze Zahl $z \in \mathbb{Z}_p$ mit $f(z) = 0$.

Literatur

[Bun02] P. Bundschuh, *Einführung in die Zahlentheorie*, Springer, Berlin, 2002.

[Lem00] F. Lemmermeier, *Reciprocity Laws – From Euler to Eisenstein*, Springer, Berlin, 2000.

[Sch07] A. Schmidt, *Einführung in die algebraische Zahlentheorie*, Springer, Berlin, 2007.