Proseminar Elementare Algebra und Zahlentheorie
Sommersemester 2014
Prof. Dr. A. Huber-Klawitter

Allgemeine Hinweise:

- In den modularisierten Studiengängen müssen Sie sich Anfang April online anmelden.
- Die Gegenstände, die wir behandeln, werden in unzähligen Büchern zur Zahlentheorie dargestellt. Es ist Ihre Aufgabe, sich das Material aus den Quellen zusammenzusuchen und zu einer kohärenten Darstellung zu kommen.
- Bitte sprechen Sie Ihren Entwurf rechtzeitig (mindestens eine Woche vorher) mit dem betreuenden Assistenten durch. Er/sie steht auch jederzeit für mathematische Fragen zur Verfügung. Bis ein Assistent feststeht, wenden Sie sich bitte in den gleichen Dingen direkt an die Dozentin.
- Der Vortrag dauert 75 Minuten + 15 Minuten für eine Feedbackdiskussion. Planen Sie Zeit für Zwischenfragen ein!
- Bitte bereiten Sie ein Handout vor, dass die wichtigsten Definitionen und Sätze für Ihre Kommilitonen zusammenfasst. Es gibt keine Formvorgaben – handschriftlich oder getippt. Latex eignet sich natürlich besonders.
- Überlegen Sie den Einsatz von Medien wie Folien und Beamer sorgfältig. Sie sind großartig für Bilder. Ein Beweis gelingt in der Regel an der Tafel besser.
- Fangen Sie rechtzeitig mit der Vortragsvorbereitung an! Nutzen Sie die Semesterferien, um sich einen Überblick über den Stoff Ihres Vortrags zu verschaffen. Das bewahrt Sie vor unangenehmen Überaschungen. Die Vorbereitung im vollen Semesterbetrieb wird mehrere Wochen dauern.
- Informationen verteilen wir über die Webseite und eine Mailingliste unter

  `prosem-ss14@math.uni-freiburg.de`

Bitte melden Sie sich mit einer Mail (Inhalt egal) an

`prosem-ss14-on@math.uni-freiburg.de`

an und antworten Sie auf die Rückmail per Reply.

Vortragsliste

1. **[28.04.] Euklidischer Algorithmus.** In diesem Vortrag soll der euklidische Algorithmus zur Berechnung des ggT vorgestellt werden und sein Laufzeitverhalten diskutiert werden.

   - Erklären Sie den Divisonsalgorithmus ganzer Zahlen und definieren Sie den ggT [Bundschuh, Kap. 1, §2 2.] oder [Wo, 1.2.1]
   - Definieren Sie die Folge der Fibonacci-Zahlen und zeigen Sie den Zusammenhang zum goldenen Schnitt.
   - Leiten Sie die Abschätzung für das Laufzeitverhalten des euklidischen Algorithmus her. [Wo, 1.2.3]
   - optional, falls Zeit bleibt: Definition von euklidischen Ringen, Beispiel $\mathbb{Z}[i]$ [SP, 3.3]
   - optional, falls Zeit bleibt: Auftauchen der Fibnonacci-Zahlen in der Natur

2. **[05.05.] Kettenbrüche I** In diesem Vortrag sollen endlichen und unendliche Kettenbrüche eingeführt werden. Das Material wird in [HW, Ch. X] behandelt, alternativ auch [Kh] oder [SO, 2.], [Bu, Kap. 5 §3],[Fr, Kap III], [Pe]

   - Endliche und unendliche Kettenbrüche, Rechenregeln
   - Kettenbruchentwicklung von reellen Zahlen ≥ 1: Algorithmus und Beispiele
   - Die Kettenbruchentwicklung bricht genau dann ab, wenn die Zahl rational ist. Arbeiten Sie den Zusammenhang zum euklidischen Algorithmus heraus.
   - Rekursionsformeln für die Partialbrüche

3. **[12.05.]Kettenbrüche II** Der Vortag setzt den obigen fort und benutzt die gleiche Literatur. In diesem Vortrag soll die Konvergenz von Kettenbrüchen untersucht werden.

(a) Konvergenzuntersuchung

(b) Abschätzung des Fehlerterms

(c) Satz über Approximierbarkeit: Ist a/b Approximation bis auf $1/2b^2$, so kommt a/b in der Kettenbruchentwicklung vor.

(d) Falls Zeit bleibt: Viele Instruktive Beispiele wie π, e, $\sqrt{2}$

4. **[19.05.] Kettenbrüche III** Dieser Vortrag setzt die obigen fort und benutzt die gleiche Literatur. Es geht um die Frage, für welche Zahlen die Kettenbruchentwicklung periodisch ist.

   - Kettenbruchentwicklung von $\sqrt{D}$ für $D \in \mathbb{N}$
   - Periodischen Kettenbrüche stellen quadratische Irrationalzahlen dar, dh. Sätze von Euler und Lagrange [Bundschuh, Kap. 5, §3] und [Frey, Kapitel III, §3]

5. **[26.05.] Pellsche Gleichung** Es geht um die Theorie der Gleichung $x^2 - Dy^2 = 1$ über den ganzen Zahlen.

   - Vorstellung der Pellschen Gleichung. Lösung mit Hilfe der Kettenbruchentwicklung von $\sqrt{D}$ z.B. nach [SO] ab Satz (4.20) [KP, 9.3], [Bu, Kap. 5,§3, 6.] Geben Sie Beispiele!
   - Zeigen Sie den Zusammenhang zu den Einheiten im Ring $\mathbb{Z}[\sqrt{D}]$ für $D \in \mathbb{N}$, [Sc, 6.7]
   - Charakterisierung aller Lösungen
   - optional, falls Zeit bleibt: der Fall $D < 0$.
   - optional, falls Zeit bleibt: Definition des Ganzheitsrings von $\mathbb{Q}(\sqrt{D})$, Berechnung der Einheitengruppe.

6. **[02.06.] Transzendente Zahlen I** Eine komplexe Zahl ist transzendent, wenn sie sich zu gut durch rationale Zahlen approximieren lässt.

   - Definition von algebraischen und transzendenten Zahlen, z.B. [HW, 11.5]
   - Existzenzbeweis mit dem Abzählbarkeitsargument, [HW, 11.6]
   - Der Begriff der Approximierbarkeit zur Ordnung n, [HW, 11.4]. Stellen Sie den Zusammenhang zum Vortrag Kettenbrüche II her.
   - Der Satz von Liouville, [HW, 11.7]
   - Anwendungen [HW, Thm 192]

7. **[16.06.]Transzendente Zahlen II** Dieser Vortrag setzt den obigen fort. Wir behandeln zwei besonders wichtige transzendente Zahlen.

   - Definition von e und π
   - Transzendenzbeweis [HW, 11.13, 11.14]
   - optional: Zusammenhang zur Quadratur des Kreises

8. **[23.06.] Zahnräder** Die Konstruktion von Getrieben, die gewisse Zahlenverhältnisse möglichst gut realisieren ist ein altes Problem der praktischen Mathematik, z.B. in der Uhrenherstellung. Dieser Vortrag soll weitgehend einem populärwissenschaftlichen Artikel folgen [Ha]. Mathematische Details sind entsprechend zu ergänzen!

   - Erwähnen Sie als motivierendes Beispiel die Zahnradkonstruktion von Christiaan Huygens im Jahre 1680 mittels Kettenbrüchen. [Bu, Kap. 5, §3, 9.] Die expliziten Zahlwerte sind online zu finden.
   - Stern-Brocot-Bäume: Definition, Eigenschaften
   - Zusammenhang zu Uhren
   - Zusammenhang zu Fibonacci-Zahlen

9. **[30.06.]Kryptografie** Wir stellen die Public Key-Verfahren vor. Die Quelle [Ko] enthält viel nicht-mathematischen Hintergrund, der gerne ebenfalls dargestellt werden kann. Die Übungsaufgaben enthalten viel weiteres Material.

   - Grundprinzip von Public Key Verfahren [Ko, IV 1.]
   - RSA [Ko, IV 2.]
   - Diskreter Logarithmus, [Ko, IV 3.]

10. **[07.07.] Primzahltests** Wie kann überprüft werden, ob eine gegebene Zahl eine Primzahl ist? Wie faktorisiert man zusammengesetzte Zahlen? Diese Fragen sind vor dem Hintergrund von RSA auch von großer praktischer Bedeutung. Aus der Vorlage [Wo] Kap. 5 soll ausgewählt werden.

    - Kleiner Satz von Fermat als Primzahltest [Wo, 5.2]
    - Probablistischer Test und Riemannsche Vermutung [Wo, 5.3]

11. **[14.07.] Geometrische Algebra I** In der linearen Algebra definieren wir die Ebene als den affinen Raum k^2, wobie k ein Körper ist. In

dieser Serie von Vorträgen geht es um die Umkehrung. Unter geeigneten Axiomen an eine ebene Geometrie E kann ein Körper k konstruiert werden mit $E = k^2$.

- Motivation [AE, Chapter II, 1.]
- Geben Sie die Axiome der affinen Geometrie [AE, Chapter II, 1.]
- Die Gruppen der Streckungen und Verschiebungen [AE, Chapter II, 2.]
- Erläutern Sie jeweils, was die Begriffe in einer Ebene der Form k^2 bedeuten, siehe auch [AE, Ch. 5]

12. **[21.07.] Geometrische Algebra II** Der Vortrag setzt den obigen fort und folgt derselben Quelle.

    - Konstruktion des Körpers, Beweis der Körperaxiome [AE, Chapter II, 3.]
    - Einführung von Koordinaten [E. Artin, Chapter II, 4.]
    - Verfolgen Sie wieder, was die Konstruktionen für k^2 bedeuten. Umkehrung. [AE, Chapter II, 5.]

13. **[28.07.] Geometrische Algebra III** Der Vortrag setzt die obigen fort und folgt derselben Quelle.

    - Beweis der Sätz von Desargues und Pappus [AE, Chapter II, 6.-7.]
    - Zeigen Sie, dass jede Desarguesche Ebene von k^2 herkommt.

Literatur

[AE] Artin, E. *Geometric algebra.* Interscience Publishers, Inc., New York-London, 1957. x+214 pp.

[AM] Artin, M. *Algebra.* Translated from the 1991 English original by Annette A'Campo. Birkhäuser Advanced Texts: Basler Lehrbücher. Birkhäuser Verlag, Basel, 1993. xiv+705 pp.

[Bu] Bundschuh, Peter; *Einführung in die Zahlentheorie.* Zweite Auflage. Springer-Lehrbuch. Springer-Verlag, Berlin, 1992. xiv+334 pp.

[Fr] Frey, Gerhard; *Elementare Zahlentheorie.* Vieweg Studium: Grundkurs Mathematik, 56. Friedr. Vieweg & Sohn, Braunschweig, 1984. ix+119 pp.

[HW] G.H. Hardy, E.M. Wright; An Introduction to the theory of numbers, Clarendon Press, Oxford, 1979.

[Ha] B. Hayes, *On the Teeth of Wheels*, American Scientist, vol 88, Nr 4 (2000), pp. 296–300.

[IR] Ireland, K.; Rosen, M.; *A Classical Introduction to Modern Number Theory*, Second Edition, Springer 1990. Chapter 1–8.

[Kh] Khintchine, A.; *Kettenbrüche*, B. G. Teubner Verlagsgesellschaft, Leipzig, 1956. vi+96 pp.

[Ko] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer 1987.

[KP] Koch, Helmut; Pieper, Herbert; *Zahlentheorie.* Ausgewählte Methoden und Ergebnisse. Studienbücherei. VEB Deutscher Verlag der Wissenschaften, Berlin, 1976. 232 pp.

[Pe] O. Perron: *Die Lehre von den Kettenbrüchen*, Teubner 1929.

[SO] W. Scharlau, H. Opolka; *Von Fermat bis Minkowski, eine Vorlesung über Zahlentheorie und ihre Entwicklung*; Springer 1980.

[Sc] A. Schmidt; *Einführung die algebraische Zahlentheorie*, Springer 2007.

[SP] R. Schulze-Pillot; *Einführung in die Algebra und Zahlentheorie*; Springer 2008.

[Wo] Wolfart, Jürgen; *Einführung in die Zahlentheorie und Algebra*, Vieweg 2011.