PROSEMINAR "ELEMENTARE ZAHLENTHEORIE" IM WINTERSEMESTER 2025/26

Organisatorisches

Das Proseminar findet mittwochs 8–10 Uhr im SR 404 in der Ernst-Zermelo-Str. 1 statt.

Ein Vorbesprechung findet am 24. Juli 2025 von 13:00 Uhr bis 14:00 Uhr im SR 404 statt. Sie können sich zur Voranmeldung beim Assistenten in eine Liste eintragen. Studierende der Lehramtsstudiengänge und zur Vorbesprechung angemeldete Personen erhalten bevorzugt einen Platz im Proseminar.

Die Vorträge sollen 80 Minuten dauern, damit Zeit für eine Feedback-Runde bleibt. Eine gute Zielgröße für einen Probevortrag ohne Publikum ist 70 Minuten.

Fangen Sie mit der Vorbereitung rechtzeitig an! Bereiten Sie sich so vor, dass Sie die Mathematik sicher beherrschen und überlegen Sie sich, wie Sie sie am besten präsentieren können. Es ist nützlich, viele Beispiele parat zu haben, um die Bedeutung von Definitionen oder Sätzen klar zu machen. Bereiten Sie zu Ihrem Vortrag ein Handout mit den wichtigsten Definitionen und Sätzen vor und treffen Sie sich spätestens eine Woche vor Ihrem Vortrag mit dem Assistenten, um Ihren Vortrag einmal durchzusprechen.
Beamer-Vorträge sind möglich, melden Sie sich aber bitte frühzeitig, wenn Sie einen Beamer-Vortrag planen.

Prüfungsanmeldung: Beachten Sie bitte, dass Sie sich vor Semesterbeginn für die Prüfungsleistung anmelden müssen, nämlich im Zeitraum 01.09.2025 bis 08.10.2025.

Das Proseminar ist thematisch in mehrere Blöcke gegliedert. Wir beginnen mit mehreren Vorträgen, die für sich stehen und einen Einstieg in die Zahlentheorie bieten. Es folgt Blöcke, in denen die Vorträge aufeinander aufbauen, zu Kettenbrüchen, transzendenten Zahlen sowie Gauß- und Jacobisummen. Wir schließen mit einem kurzen Einblick zu einer großen zahlentheoretischen Vermutung.

1. Verschiedenes zur Einführung

Literatur: [HW79], [IR90], [K94] und [W11]

1.1. **Euklidischer Algorithmus [15.10.]** In diesem Vortrag soll der euklidische Algorithmus zur Berechnung des ggT vorgestellt und sein Laufzeitverhalten diskutiert werden. Schauen Sie in [W11] und [K94], nach.

- Erklären Sie den Divisonsalgorithmus ganzer Zahlen und definieren Sie den ggT
- 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 [W11], 1.2.3
- optional, falls Zeit bleibt: Auftauchen der Fibonacci-Zahlen in der Natur

1.2. **Kryptografie [22.10.]** Stellen Sie Public-Key-Verfahren auf der Grundlage von [K94] vor.

- Grundprinzip von Public-Key-Verfahren
- Erklären Sie RSA
- Diskreter Logarithmus

1.3. **Primzahltests [29.10.]** Vor dem Hintergrund von RSA sind Primzahltests von großer praktischer Bedeutung. Wählen Sie aus [W11] Abschnitt 5.2 und 5.3 aus.

- Kleiner Satz von Fermat als Primzahltest
- Probabilistischer Test und Riemannsche Vermutung

1.4. **Das Henselsche Lemma [05.11.]** Das Henselsche Lemma ist ein grundlegendes Resultat der algebraischen Zahlentheorie, das wir kennenlernen wollen.

- Führen Sie Restklassenkörper ein und definieren Sie $\mathbb{Z}_p$
- Beweisen Sie das Henselsche Lemma (Orientierung bietet [H14], Kapitel 9)
- Erklären Sie (einfache) Anwendungen

1.5. **Der Vier-Quadrate-Satz [12.11.]** Wir wollen zeigen, dass jede positive ganze Zahl sich als Summe von vier Quadraten schreiben lässt. Folgen Sie z.B. [IR90] 17, §7.

- Erklären Sie den Zwei-Quadrate-Satz
- Präsentieren Sie Lemma 1 und 2
- Beweisen Sie Proposition 17.7.1 (Vier-Quadrate-Satz)
- optional: Erläutern Sie Proposition 17.7.2

2. Kettenbrüche

Literatur: [B08], Kapitel 5, und [HW79], Kapitel 10.

2.1. **Kettenbrüche I [19.11.]** In diesem Vortrag sollen Grundlagen zu Kettenbrüchen dargestellt werden.

- 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

2.2. **Kettenbrüche II [26.11.]** In diesem Vortrag soll die Konvergenz von Kettenbrüchen untersucht werden.

- Konvergenzuntersuchung
- Abschätzung des Fehlerterms
- Satz über Approximierbarkeit: Ist a/b Approximation bis auf $1/2b^2$, so kommt a/b in der Kettenbruchentwicklung vor.
- Falls Zeit bleibt: Instruktive Beispiele wie π, e, $\sqrt{2}$.

2.3. **Kettenbrüche III [03.12.]** In diesem Vortrag geht es um die Frage, für welche Zahlen die Kettenbruchentwicklung periodisch ist.

- Kettenbruchentwicklung von $\sqrt{D}$ für $D \in N$
- Periodischen Kettenbrüche stellen quadratische Irrationalzahlen dar, d.h. Sätze von Euler und Lagrange

3. Transzendente Zahlen

Literatur: [HW79], Kapitel 11.

3.1. **Liouvilles Kriterium [10.12.]**

- Definieren Sie algebraische und transzendente Zahlen
- Existenz transzendenter Zahlen über Abzählbarkeit
- Kriterium von Liouville mit Beweis (evtl. Zusammenhang zu Kettenbrüchen)
- Beispiele

3.2. ***Transzendenz von e und π [17.12.]** Zeigen Sie die Transzendenz von e und π.

4. Gauss- und Jacobisummen

Literatur: [IR90]

4.1. **Multiplikative Charaktere [07.01.]** Folgen Sie [IR90] Kapitel 8.

- Führen Sie multiplikative Charaktere ein
- Zeigen Sie elementare Eigenschaften
- Definieren Sie Gaußsummen

4.2. **Gauß- und Jacobisummen [14.01.]**

- Führen Sie Jacobisummen ein und zeigen Sie Theorem 1 in [IR90] Kapitel 8
- Beweisen Sie Proposition 8.3.3 und Proposition 8.5.1.
- optional: Weitere Resultate aus diesem Kapitel

4.3. **Die Kongruenz $X^n + Y^n \equiv 1$ modulo p [21.01.]**

- Präsentieren Sie [IR90] Kapitel 8 §4
- Zeigen Sie Theorem 3 des Kapitels
- Erklären Sie eine Anwendung

5. *abc*-Vermutung

Literatur: [L25].

5.1. **Einführung zur *abc*-Vermutung [28.01.]** Erklären Sie die klassische Formulierung der *abc*-Vermutung und zeigen Sie die äquivalenten Aussagen in [L25].

- Erläutern Sie Theorem 1.1.
- Geben Sie einen Überblick dazu, welche anderen zahlentheoretischen Vermutungen mit der *abc*-Vermutung in Zusammenhang stehen (siehe auch [GT02]).

5.2. **Beweis der Abschätzung [04.02.]** Beweisen Sie Theorem 1.1 in [L25] vollständig.

Literatur

[B08] P. Bundschuh: *Einführung in die Zahlentheorie*. Springer-Verlag Berlin Heidelberg, sechste Auflage, 2008.

[GT02] A. Granville, T.J. Tucker: *It's As Easy As abc*. Notices of the AMS, Vol. 49, Number 10, pp. 1224–1231. Abrufbar unter https://www.ams.org/notices/200210/fea-granville.pdf

[H14] A. Huber-Klawitter: *Skript Algebraische Zahlentheorie, Sommersemester 2014*. Abrufbar unter https://home.mathematik.uni-freiburg.de/arithgeom/lehre/ss14/algzt/azt.pdf

[HW79] G.H. Hardy, E.M. Wright: *An Introduction to the Theory of Numbers*. Clarendon Press, Oxford, 1979.

[IR90] K. Ireland, M. Rosen: *A Classical Introduction to Modern Number Theory*. Springer-Verlag New York, zweite Auflage, 1990.

[K94] N. Koblitz: *A Course in Number Theory and Cryptography* . Springer-Verlag New York, 2. Auflage 1994.

[L25] J. D. Lichtman: *The abc conjecture is true almost always*. Abrufbar unter https://arxiv.org/abs/2505.13991

[W11] J. Wolfart: *Einführung in die Zahlentheorie und Algebra*. Vieweg 2011.