



Im Frühjahrssemester 2018 werde ich lesen

Zahlentheorie

Ort und Zeit: Dienstag 10¹⁵ – 11⁴⁵, C 015 und Donnerstag 8³⁰ – 10⁰⁰, C 014

Übungen: Donnerstag 10¹⁵ – 11⁴⁵, C 014

Die Zahlentheorie beschäftigt sich mit ganzen Zahlen; typische Probleme sind Lösungen diophantischer Gleichungen, Erkennen von Primzahlen, die Primzerlegung ganzer Zahlen und so weiter. Sie findet Anwendungen beispielsweise bei der sicheren Kommunikation im Internet, bei ganzzahligen Optimierungsproblemen, bei der Erklärung von physikalischen und biologischen Phänomenen, der Planung von Versuchen oder Umfragen und sogar bei der Planung von Konzertsälen. Je nach verwendeten Methoden unterscheidet man zwischen elementarer, algebraischer und analytischer Zahlentheorie.

In dieser Vorlesung wird es vor allem um elementare sowie Anfänge der algebraischen Zahlentheorie gehen. Sie beginnt mit dem sowohl theoretisch als auch praktisch sehr wichtigen EUKLIDischen Algorithmus und einigen seiner Anwendungen sowie mit dem Rechnen modulo einer ganzen Zahl. Danach sollen erste Anwendungen auf Verschlüsselungsverfahren und elektronische Unterschriften vorgestellt werden. Auch Verfahren zur Primzahlsuche sowie zur Primfaktorzerlegung ganzer Zahlen sind in diesem Zusammenhang wichtig.

Eine leichte Variation des EUKLIDischen Algorithmus führt zu Kettenbrüchen, die unter anderem für rationale Approximationen reeller Zahlen sowie für die Lösung gewisser quadratischer Gleichungen in ganzen Zahlen nützlich sind. Als eine Anwendung betrachten wir das Rechnen mit Kalenderdaten.

Zum besseren Verständnis nichtlinearer diophantischer Gleichungen empfiehlt es sich, ganze Zahlen auch in anderen Körpern als \mathbb{Q} zu betrachten; im Rahmen dieser Vorlesung soll dies für quadratische Zahlkörper geschehen, d.h. für Körper der Form $\mathbb{Q} \oplus \mathbb{Q}\sqrt{d}$ mit einer ganzen Zahl d , die keine Quadratzahl ist. Mit den hier entwickelten Methoden läßt sich dann beispielsweise entscheiden, ob und wie sich eine Zahl als Summe von Quadraten darstellen läßt, und dies wiederum führt auf Methoden, mit denen sich schnell viele Dezimalstellen von π berechnen lassen.

Letztes großes Thema ist die Lösbarkeit und ggf. Lösung von Gleichungen der Form $x^2 \equiv a \pmod{n}$ und einige von deren Anwendungen.

Hörerkreis: Bachelorstudenten der Wirtschaftsmathematik sowie Lehramtsstudenten der Mathematik (einschließlich Wirtschaftspädagogen)

Literaturauswahl: Parallel zur Vorlesung wird ein Skriptum erscheinen.

Unter den vielen Lehrbüchern seien genannt

PETER BUNDSCHUH: Einführung in die Zahlentheorie, *Springer*, 62008

RICHARD CRANDALL, CARL POMERANCE: Prime Numbers. A Computational Perspective, *Springer*, 2005

JAY GOLDMAN: The Queen of Mathematics. A Historically Motivated Guide to Number Theory, *AK Peters*, 2005

Vor allem für Lehrer zum Einstieg gut geeignet (wenn auch nicht ausreichend) ist

ANDREAS BARTHOLOMÉ, JOSEF RUNG, HANS KERN: Zahlentheorie für Einsteiger,

Vieweg+Teubner, 2008

Seminargebäude A5
D - 68131 Mannheim

Tel.: 0621 / 181 - 2515
Fax: 0621 / 181 - 2461

seiler@math.uni-mannheim.de
<http://hilbert.math.uni-mannheim.de/~seiler>