Universität Mannheim

Lehrstuhl VI für Mathematik

Wolfgang K. Seiler

Im Sommersemester 2005 werde ich lesen

Elliptische Kurven

Ort und Zeit: Dienstag, $15^{30} - 17^{00}$ Uhr und Mittwoch, $10^{15} - 11^{45}$ Uhr, C 015

Elliptische Kurven haben ihren Namen von den elliptischen Integralen, mit denen sich die Längen von Ellipsenbögen berechnen lassen und die deshalb eine große Rolle u.a. im Maschinenbau und der Geodäsie spielen. Diese analytische Theorie erlaubt es, viele wesentliche Eigenschaften elliptischer Kurven über den komplexen Zahlen schnell und anschaulich herzuleiten.

Die Vorlesung wird daher zunächst elliptische Kurven über $\mathbb{C}$ betrachten, allerdings sollen die Ergebnisse möglichst schnell verallgemeinert werden auf Kurven über beliebigen Körpern.

Schwerpunkt der Vorlesung sind elliptische Kurven über endlichen Körpern und deren Anwendungen in der Kryptographie sowie der algorithmischen Zahlentheorie.

Die Vorlesung wendet sich an Studenten im Hauptstudium des Integrierten Studiengangs Mathematik und Informatik mit Vertiefung in Algebra oder Geometrie. Bei Vertiefung in Algebra bietet sich eine Kombination mit Kryptologie, Kodierungstheorie oder Computeralgebra an, bei Vertiefung in Geometrie mit Computeralgebra oder Vorlesungen aus dem Bereich der algebraischen Geometrie.

Obwohl die Vorlesung sehr algebraisch sein wird, reichen zum Verständnis die Vorlesungen des Grundstudiums. Die notwendigen Methoden aus der Algebra haben wenig mit dem Standardstoff einer Algebra I zu tun und werden daher in der Vorlesung selbst entwickelt.

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

Literaturangaben

ROBERTO AVANZI, HENRI COHEN, CHRISTOPHE DOCHE: Handbook of Elliptic and Hyperelliptic Curve Cryptography, *Chapman & Hall/CRC,* Juni 2005 (?)
Sollte nach der Verlagsankündigung sehr gut für die Vorlesung geeignet sein, kommt aber wahrscheinlich zu spät.

IAN BLAKE, GADIEL SEROUSSI, NIGEL SMART: Elliptic curves in cryptography, *London Mathematical Society Lecture Note Series* **265**, Cambridge Univ. Press, 2000
Das mathematischste unter den Büchern, die sich mit elliptischen Kurven und Kryptographie beschäftigen, allerdings sind nicht alle Aussagen vollständig bewiesen.

DARREL R. HANKERSON, ALFRED J. MENEZES, SCOTT A. VANSTONE: Guide to elliptic curve cryptography, *Springer,* 2004
Überblick über kryptographische Anwendungen, größtenteils ohne Beweise.

MICHAEL ROSING: Implementing Elliptic Curve Cryptography, *Manning Publications,* 1999
Stellt die wichtigsten Standards vor und diskutiert deren Implementierung. Praktisch keine mathematische Theorie.

JOSEPH H. SILVERMAN, JOHN TATE: Rational points on elliptic curves (Undergraduate Texts in Mathematics), *Springer,* 1992
Sehr gut lesbare Einführung in die Theorie der elliptischen Kurve, geht allerdings nicht sehr weit.

JOSEPH H. SILVERMAN: The arithmetic of elliptic curves (Graduate Texts in Mathematics **106**), *Springer,* 2002
Eines der wenigen fortgeschrittenen Lehrbücher, in denen auch elliptische Kurven über endlichen Körpern ausführlich behandelt werden. Eine Standardreferenz.

LAWRENCE C. WASHINGTON: Elliptic curves, *Chapman & Hall/CRC,* 2003
Etwas einfacher zu lesen als Silverman, allerdings auch nicht so vollständig.

ANNETTE WERNER: Elliptische Kurven in der Kryptographie, *Springer,* 2002
Sehr elementare Einführung, die selbst bei relativ einfachen Sätzen gelegentlich auf vollständige Beweise verzichtet. Trotzdem gut geeignet für einen ersten Überblick.