



Wolfgang K. Seiler

Im Frühjahrssemester 2008 werde ich lesen

Elliptische Kurven

Ort und Zeit: Dienstag, Mittwoch 10¹⁵ – 11⁴⁵ Uhr, C 013

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, der Geodäsie und der Kartographie spielen. Die dahinterstehende 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 sowie Studenten des entsprechenden Bachelorstudiengangs, die an einer Vertiefungsvorlesung aus dem Bereich algebraische Geometrie interessiert sind. Für Diplomstudenten bietet sich eine Kombination mit Kryptologie, Kodierungstheorie oder der im nächsten Semester angebotenen Computeralgebra an sowie natürlich mit künftigen Vorlesungen aus dem Bereich der algebraischen Geometrie.

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

Literaturangaben

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.

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 Kurven, behandelt mehr Stoff als das vorangehende Buch, verzichtet aber auf die Behandlung elliptischer Kurven über endlichen Körpern.

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.

HENRI COHEN, GERHARD FREY, ROBERTO AVANZI, CHRISTOPHE DOCHE, TANJA LANGE, KIM NGUYEN, FREDERIK VERCAUTEREN: Handbook of Elliptic and Hyperelliptic Curve Cryptography, Chapman & Hall/CRC, 2006
Derzeit wohl der vollständigste Überblick über die Anwendung elliptischer Kurven in der Kryptographie. Auch die mathematischen Grundlagen werden behandelt, allerdings meist ohne Beweise.

DARREL R. HANKERSON, ALFRED J. MENEZES, SCOTT A. VANSTONE: Guide to elliptic curve cryptography, Springer, 2004
Deutlich kürzer und elementarer, ebenfalls im Handbuchstil und meist ohne Beweise.

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 kürzeren Büchern, die sich mit elliptischen Kurven und Kryptographie beschäftigen, allerdings sind auch hier nicht alle Aussagen vollständig bewiesen.

IAN BLAKE, GADIEL SEROUSSI, NIGEL SMART [HRSG.]: Advances in Elliptic Curve Theory, London Mathematical Society Lecture Note Series **317**, Cambridge Univ. Press, 2005
Fortsetzung davon; verschiedene Autoren behandeln in Einzelaufsätzen Entwicklungen der Jahre 2000–2005.

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