



Im Herbstsemester 2013 werde ich lesen

## Elliptische Kurven

**Ort und Zeit:** Dienstag 13<sup>45</sup> – 15<sup>15</sup> und Donnerstag, 15<sup>30</sup> – 17<sup>00</sup>, C 012

**Übungen:** Dienstag 15<sup>30</sup> – 17<sup>00</sup>, C 012

Elliptische Kurven sind ebene Kurven dritten Grades; der Name kommt daher, daß sie im Zusammenhang mit der Berechnung von Bogenlängen auf einer Ellipse auftreten. In dieser Vorlesung soll es allerdings in erster Linie um kryptographische Anwendungen elliptischer Kurven gehen wie beispielsweise die elektronische Unterschriftenfunktion der neuen deutschen Personalausweise.

Die Vorlesung beginnt mit einer Kapitel über ebene algebraische Kurven; danach wird bewiesen, daß die Punkte einer elliptischen Kurve über einem festen Körper eine Gruppe bilden, in der man gut rechnen kann. Kryptographische Anwendungen beruhen darauf, daß Vielfache eines Punktes leicht bestimmt werden können, daß es aber rechnerisch sehr aufwendig ist, ausgehend von einem Punkt  $P$  und einem Vielfachen  $Q = nP$  die Zahl  $n$  zu ermitteln.

Kryptoverfahren auf der Basis elliptischer Kurven sind bei gleicher Größenordnung der Zahlen deutlich sicherer als solche die auf dem Rechnen modulo einer Primzahl beruhen, da der wichtigste Angriff gegen solche Verfahren im Fall elliptischer Kurven im allgemeinen nicht funktioniert. In speziellen Fällen gibt es jedoch Angriffe, mit denen sich die Vorlesung als nächstes beschäftigen wird. Auch Anwendungen elliptischer Kurven für Primzahltests und die Faktorisierung ganzer Zahlen sollen behandelt werden.

**Hörerkreis:** Die Vorlesung wendet sich in erster Linie an Masterstudenten. Vorausgesetzt werden nur die Grundvorlesungen; die Hörer müssen sich allerdings auf Beweise und Verfahren einstellen, die deutlich komplexer sind als die aus Bachelorvorlesungen gewohnten.

**Literaturauswahl:** Hauptreferenz ist

LAWRENCE C. WASHINGTON: Elliptic curves: Number Theory and Cryptography, *CRC* 2009

Für einen ersten Überblick dienen kann auch

ANNETTE WERNER: Elliptische Kurven und Kryptographie, *Springer* 2002

Kryptographische Anwendungen sind ausführlich beschrieben z.B. in

HENRI COHEN, GERHARD FREY ET AL.: Handbook of Elliptic and Hyperelliptic Curve Cryptography, *CRC* 2005

SAN LING, HUAXIONG WANG, CHAOPING XING: Algebraic Curves in Cryptography, *CRC* 2013

Die Geometrie ebener algebraischer Kurven findet man z.B. in

EGBERT BRIESKORN, HORST KNÖRRER: Ebene Algebraische Kurven, *Springer* 1981

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>