CARL VON OSSIETZKY universität OLDENBURG

IfM INSTITUT FÜR MATHEMATIK

Elliptische Kurven und Kryptographie

Vorlesung im Sommersemester 2014 – Prof. Dr. Jan Steffen Müller

Vorlesungsinhalt Eine *elliptische Kurve* E über einem Körper K ist eine Kurve, die durch eine Gleichung der Form

$$y^2 = x^3 + Ax + B, \quad A, B \in K, \quad 4A^3 + 27B^2 \neq 0$$

beschrieben werden kann (jedenfalls für $\mathrm{char}(K) \neq 2, 3$). Elliptische Kurven sind seit geraumer Zeit Gegenstand intensiver Forschung in so unterschiedlichen mathematischen Gebieten wie Zahlentheorie, algebraischer Geometrie, Funktionentheorie und Kryptographie. Eine der wichtigsten (und überraschendsten) Eigenschaften einer solchen Kurve besteht darin, dass die Menge $E(K)$ der Punkte auf E mit Koordinaten in K eine *abelsche Gruppe* bildet. In der Vorlesung werden wir diese Gruppe für verschiedene Körper untersuchen.
Unser Hauptaugenmerk werden wir auf zahlentheoretische Aspekte legen, genauer auf den Fall $K = \mathbb{Q}$. Hier gilt der Satz von Mordell: Die Gruppe $E(\mathbb{Q})$ ist *endlich erzeugt*. Neben dem Beweis des Satzes werden wir Methoden zur Berechnung von Erzeugern dieser Gruppe behandeln. Dies steht in engem Zusammenhang mit der *Vermutung von Birch und Swinnerton-Dyer*, die sich auf der Liste der 6 ungelösten Millenium-Probleme findet.
Außerdem werden wir uns u.a. mit elliptischen Kurven über den komplexen Zahlen sowie über endlichen Körpern beschäftigen; letztere spielen eine zentrale Rolle in der modernen Kryptographie.

Vorkenntnisse Inhalte der Algebra-Module aus dem Bachelorstudium werden vorausgesetzt. Vorkenntnisse aus der (algebraischen) Zahlentheorie, der Funktionentheorie oder der Theorie algebraischer Kurven sind vereinzelt hilfreich, werden aber nicht vorausgesetzt.

Modul Die Vorlesung bildet den ersten Teil des Mastermoduls „Elliptische Kurven und Kryptographie“, welches im WS 2014/15 mit einem Reading Course (2 SWS) fortgesetzt wird, Sie eignet sich als Vorbereitung auf eine Masterarbeit in der arithmetischen Geometrie.

Zeit und Ort Mo 10-12 Uhr, W01 0-012 sowie Mi 14-16 Uhr, W01 1-109

Weitere Informationen Per Email: jan.steffen.mueller@uni-oldenburg.de.
Siehe auch die Modulbeschreibung sowie die Stud.IP-Seite der Veranstaltung.

http://www.uni-ol.de/jan-steffen-mueller +49 (0)441 798-3221