Universität Hamburg

Department Mathematik
Algebra und Zahlentheorie
Jan Steffen Müller

Seminar 65-206: Arithmetik elliptischer Kurven

Inhalt

Elliptische Kurven spielen in vielen Bereichen der Mathematik eine wichtige Rolle, z.B. in der Funktionentheorie, der algebraischen Geometrie oder der Kryptographie. Wir wollen uns in diesem Seminar allerdings auf die Arithmetik, d.h. die zahlentheoretischen Aspekte elliptischer Kurven konzentrieren. Hierbei werden wir uns größtenteils an [2] orientieren.

Die spektakulärste Anwendung der Arithmetik elliptischer Kurven ist der Beweis des letzten Satzes von Fermat durch Andrew Wiles. Auch wenn dieser außerhalb der Reichweite des Seminars liegt, werden wir uns einigen äußerst wichtigen Sätzen zumindest in Spezialfällen widmen, z.B. dem Satz von Mordell, der aussagt, dass die $\mathbb{Q}$-rationalen Punkte auf einer elliptischen Kurve eine endlich erzeugte abelsche Gruppe bilden und dem Satz von Nagell–Lutz, der es erlaubt, die Punkte endlicher Ordnung dieser Gruppe leicht zu bestimmen.

Unsere Standardreferenz ist [2]. Das Buch [1] behandelt ähnliche Themen, allerdings auf einem deutlich höheren Abstraktionsniveau. Die Vorlesungsskripten [3] und [4] sind als vereinzelte Ergänzungen gedacht.

Voraussetzungen

Vorkenntnisse aus der Algebra I, der Algebraischen Geometrie und der Elementaren Zahlentheorie sind hilfreich, aber nicht notwendig. Insbesondere ist eine Teilnahme am Seminar bei gleichzeitigem Besuch der Vorlesung Elementare Zahlentheorie möglich.

Zeit und Ort

Mi 14.15-15.45, Geom 432

Ablauf und Organisation

Die Vorträge werden am 20.10. verteilt. Zur Einstimmung ist es hilfreich, die Einführung des Buches [2] zu lesen. Es wird erwartet, dass die Vortragenden ein Handout anfertigen, das im Anschluss an den Vortrag ausgeteilt werden soll. Vorträge in Englischer Sprache sind möglich.

Im ersten Teil des Seminars sollen weite Teile der ersten vier Kapitel von [2] vorgestellt werden.

20.10.	(Jan Steffen Müller) Vorbesprechung und Einführung.
27.10.	(Jan Steffen Müller) Ebene algebraische Kurven [2, Appendix A], [1, Chapter I,II], [3, §2.1].
3.11.	Elliptische Kurven, Weierstraß-Normalform und das Gruppengesetz [2, §I.2-4], [1, §III.1-3].
10.11.	Diophantische Gleichungen [2, §I.1, §III.7].
17.11.	Torsionspunkte [2, §II.1, §III.3-4].
24.11.	Höhen [2, §III.1], [1, §VIII.4].
1.12.	Höhenabschätzungen [2, §III.2-3], [1, §VIII.4].
8.12.	Elliptische Kurven über $\mathbb{C}$ und Isogenien [2, §II.2, §III.4], [4, Kapitel 1], [1, Chapter VI].
15.12.	Beweis des Satzes von Mordell für den Fall, dass die Kurve einen rationalen 2-Torsionspunkt besitzt [2, §III.5].
5.1.	Beispiele [2, §III.6].
12.1.	Elliptische Kurven über endlichen Körpern [2, §IV.1, §IV.3], [3, §3.2].

Weitere Vorträge werden in Absprache mit den Teilnehmern am 20.10. vereinbart. Es bieten sich folgende Themenkomplexe an, wobei auch einzelne Vorträge aus verschiedenen Komplexen denkbar sind.

Ganzzahlige Punkte auf elliptischen Kurven

(1) Der Satz von Siegel [2, §V.1-V.2].

(2) Der Satz von Thue [2, §V.3-V.8].

Der Satz von Mordell-Weil

Dies ist eine Verallgemeinerung des Satzes von Mordell auf elliptische Kurven über beliebigen Zahlkörpern. Sie erfordert Hintergrundwissen aus der Körpertheorie und der algebraischen Zahlentheorie. Insbesondere folgt der Satz von Mordell im allgemeinen Fall.

(1) Kummertheorie [1, §VIII.1].

(2) Beweis des (schwachen) Satzes von Mordell-Weil [1, §VIII.1]. Dieser Vortrag baut auf der Kummertheorie auf.

Anwendungen

Diese Vorträge verwenden alle die Theorie elliptischer Kurven über endlichen Körpern.

(1) Elliptische Kurven in der Kryptographie [3, Kapitel 5], [5, §1.2].

(2) Faktorisieren mit Elliptischen Kurven nach Lenstra [2, §IV.4], [3, §4.2.2].

(3) Der Primzahltest von Goldwasser-Kilian [3, §4.2.1].

(4) Der Punktezählalgorithmus für elliptische Kurven über endlichen Körpern von Schoof [5, §3.3].

Literatur

[1] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York (1984).

[2] J.H. Silverman und J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York (1992).

[3] M. Stoll, *Elliptische Kurven I*, Vorlesungsskript (2000). Siehe `http://mathe2.uni-bayreuth.de/stoll/vorlesungen/Elliptische-Kurven-SS2000.pdf`.

[4] M. Stoll, *Elliptische Kurven II*, Vorlesungsskript (2001). Siehe `http://mathe2.uni-bayreuth.de/stoll/vorlesungen/Elliptische-Kurven2-WS2000.pdf`.

[5] A. Werner, *Elliptische Kurven in der Kryptographie*, Springer-Verlag, Berlin (2002).