

Einführung in die Theorie der elliptischen Kurven

Seminar

Ort: M HS 4

Zeit: Do 14.00-16.00 Uhr

Beginn: 16.10.2003

Inhalt: Elliptische Kurven bilden eine Klasse von Kurven, die vielfältige Beziehungen zu verschiedenen Gebieten der Mathematik haben. In der Funktionentheorie begegnet man ihnen im Zusammenhang mit elliptischen Funktionen und sie sind nach der Riemannschen Zahlenkugel die ersten interessanten kompakten Riemannschen Flächen. Für die arithmetische Geometrie, ein Gebiet, das Zahlentheorie und Geometrie verbindet, sind sie besonders interessant, da sie zum einen relativ einfach durch explizite Gleichungen zu beschreiben sind, zum anderen die Struktur einer abelschen Gruppe besitzen. Obwohl sie sehr gut studiert sind und viele (sehr tiefe) Sätze über elliptische Kurven gezeigt sind (so zum die Modularitätsvermutung durch A.Wiles), gibt es immer noch offene Fragen. In diesem Seminar sollen in relativ elementarer Weise eine Reihe interessanter Ergebnisse bewiesen werden.

Eine elliptische Kurve kann ad hoc als Nullstellenmenge eines kubischen Polynoms in zwei Variablen definiert werden, also beispielsweise $y^2 = x^3 + Ax + B$ für rationale/ganze Koeffizienten A, B . Die Theorie der Diophantischen Gleichungen beschäftigt sich mit den Lösungen solcher Gleichungen in den rationalen bzw. ganzen Zahlen. Es stellt sich heraus, dass man eine Gruppenstruktur auf $E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q} \mid y^2 = x^3 + Ax + B\}$ definieren kann. Im Verlauf sollen insbesondere folgende Fragen behandelt werden:

- Geometrie und Beschreibung des Grppengesetzes einer elliptischen Kurve
- Notwendige Bedingungen für Punkte endlicher Ordnung (Satz von Nagell-Lutz)
- Die Gruppe der rationalen Punkte ist endlich erzeugt (Satz von Mordell-Weil)
- Ganze Punkte (Satz von Thue-Siegel)
- Kubische Kurven über endlichen Körpern

Literatur:

[Cas] J.W.S. Cassels, *Lectures on Elliptic Curves*, LMSST 24, Cambridge University Press

[ST] J.H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, UTM, Springer

[Sil] J.H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer

Vorkenntnisse: Das Seminar wendet sich an Studenten ab dem 5.Semester. Kenntnisse der Algebra und ein wenig Funktionentheorie sind wünschenswert.

Anmeldung: *ab sofort* bei S. Wortmann (wortmann@mathi.uni-heidelberg.de, Zi.108, INF 288) oder bei K. Wingberg. Eine **Vorbesprechung** findet in der ersten Sitzung statt.