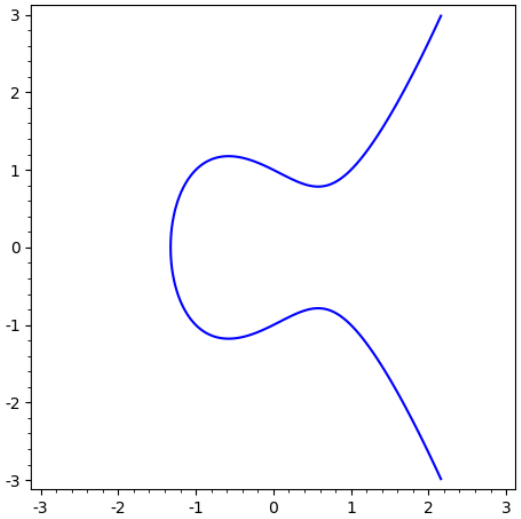
Blockseminar Algebra/Zahlentheorie

Ankündigung

Jun. Prof. Dr. Jeroen Sijsling
Institut für Reine Mathematik
Wintersemester 2019-2020
✉ *jeroen.sijsling@uni-ulm.de*

Eine elliptische Kurve ist eine Kurve E mit einer Gleichung der Form $E : y^2 = x^3 + ax + b$. Solche Kurven wurden zuerst verwendet bei der Berechnung von Bogenlängen von elliptischen Planetbahnen. Überraschenderweise haben sie auch viele Anwendungen in anderen wissenschaftlichen Bereichen, wie der Zahlentheorie und der Kryptographie.



Der Grund für diese Relevanz, ist dass neben der "normalen" Zahlengerade elliptische Kurven die einzigen anderen geometrischen Objekten von Dimension 1 sind, auf denen es ein einfaches (algebraisches) Gruppengesetz gibt. Dieses Gesetz wird verwendet in allen algebraischen Anwendungen, sowie auf Chipkarten wie Sie diese wahrscheinlich in Ihrer Tasche haben.

Das erste, mehr theoretische und sehr faszinierendes Teilthema des Seminars ist die Theorie der elliptischen Funktionen, die am Anfang der Geschichte der elliptischen Kurven entwickelt wurde. Dies Thema ist auch interessant für Studierenden mit Interessen in der Analyis, da es periodische meromorphe Funktionen auf der komplexe Ebene studiert.

Nächstes ist die Beschreibung der algebraischen (anstatt analytischen) Gruppenstruktur. Die Addition auf einer elliptischen Kurven lässt sich auch mithilfe geeigneter Durchschnitten der Kurve mit Geraden bilden. Unter dieser Addition bilden die Punkte auf der Kurven eine additive Gruppe. Das zweite Ziel ist, diese Gruppe zu beschreiben, nicht nur, wenn der Koeffizientenring CC ist, sondern auch, wenn sie $\mathbb{Q}$ oder sogar ein endlicher Körper ist.

Zuletzt spielen elliptische Kurven über endlichen Körpern eine Rolle in der Kryptographie. Das Gruppengesetz auf der endlichen Menge von Punkten auf solch einer elliptischen Kurve ist einfach genug, um schnell damit rechnen zu können, aber (anders als die Addition auf der Zahlengerade) kompliziert genug, um eine gute Verschlüsselung zu ermöglichen. Dies ist das Thema der Elliptische-Kurven-Kryptographie.

Zielgruppe und Voraussetzung

Das Seminar richtet sich an alle Studierende der mathematischen Studiengänge. Voraussetzung ist entweder *Elemente der Algebra* oder *Algebra*.

Teilnehmerzahl und Durchführung

12 Teilnehmer in einem wochentlichen Seminar.

Anmeldung

Per Email bis 31.08.2019 an `jeroen.sijsling@uni-ulm.de`, mit Angabe von:

- Name, Matrikelnummer, Studiengang, Fachsemester.
- Liste aller bisher gehörten mathematischen Vorlesungen.

Besprechung und Verteilung der Themen

Nach der Anmeldung wird das Programma weiter detailliert besprochen und verteilt nach einem kurzen Vortrag.