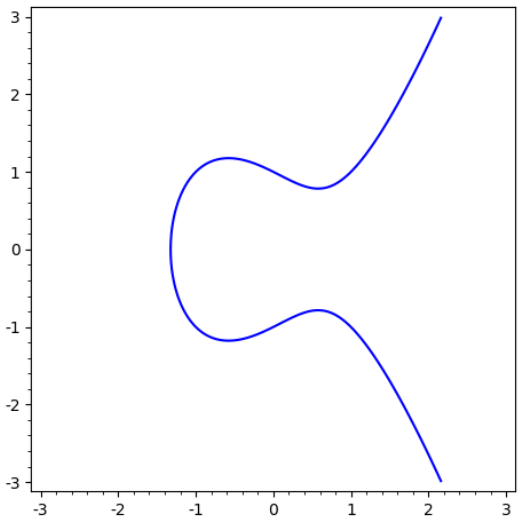
WiMa-Praktikum Elliptische Kurven

Ankündigung

Jun. Prof. Dr. Jeroen Sijsling
Institut für Algebra und Zahlentheorie
Sommersemester 2021
✉ *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.

Im ersten, theoretischen Teil des Praktikums beschreiben wir die algebraische Gruppenstruktur auf einer elliptischen Kurve. 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. Ziel ist, diese Gruppe zu beschreiben, inbesondere wenn der Koeffizientenring $\mathbb{Q}$ oder ein endlicher Körper ist.

Elliptische Kurven über endlichen Körpern spielen 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. Wir besprechen dies kurz im Kontext vom Computeralgebrasystem SageMath, in den Sie eine Einführung bekommen, und zwar in seiner Online-Form CoCalc.

Im zweiten Teil des Kurses arbeiten Sie in kleineren Gruppen an Einzelthemen, wie zum Beispiel:

- Berechnung der Weil-Paarung;
- Elliptische-Kurven-Faktorisierung;
- Elliptische-Kurven-Primzahltests;
- Diskrete Logarithmen auf Elliptischen Kurven;
- Den Schoof–Elkies–Atkin-Algorithmus.

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. Theoretische Erläuterung und Einführung in SageMath gefolgt durch Zusammenarbeit an Einzelthemen.

Wir verwenden das Buch *The Arithmetic of Elliptic Curves* von Joseph Silverman.

Anmeldung

Per Email bis 01.04.2021 an `jeroen.sijsling@uni-ulm.de`, mit Angabe von:

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

Vor dem Semesteranfang findet eine (nicht verpflichtete) Besprechung der Veranstaltung statt.