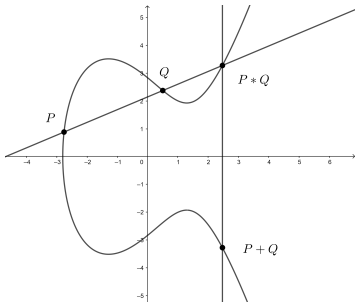
Thematisches Seminar – HS 2020

Elliptische Kurven

Verantwortliche :	Dr. Christine Zehrt
Zeit/Ort :	Mittwoch, 15h15 – 17h00 im Hörsaal 2.52, PER 08
	Beginn: 16. September 2020
Vorbesprechung :	2. September 2020 um 15h15 im Hörsaal 2.52, PER 08

Eine elliptische Kurve $E(K)$ über einem Körper K nennt man die Menge aller Punkte $(x, y) \in K^2$, die eine Gleichung der Form $y^2 = x^3 + ax + b$ erfüllen (wobei $a, b \in K$ mit $4a^3 + 27b^2 \neq 0$), zusammen mit einem Punkt im Unendlichen. Die Menge $E(K)$ bildet bezüglich einer geometrisch definierten Addition eine abelsche Gruppe. Das folgende Bild zeigt die elliptische Kurve $y^2 = x^3 - 5x + 8$ über $\mathbb{R}$ zusammen mit der Addition von zwei Punkten P und Q:



In diesem Seminar werden wir vor allem zahlentheoretische Aspekte von elliptischen Kurven studieren wie zum Beispiel, dass die Gruppe der rationalen Punkte $E(\mathbb{Q})$ endlich erzeugt ist (Satz von Mordell) und dass rationale Punkte von endlicher Ordnung ganzzahlige Koeffizienten haben, falls E über $\mathbb{Z}$ definiert ist (Satz von Nagell-Lutz). Weiter werden wir elliptische Kurven über endlichen Körpern betrachten und untersuchen, wie diese erfolgreich in der Kryptographie eingesetzt werden.

Grundlage dieses Seminars ist das Buch *Rational Points on Elliptic Curves* von J. H. Silverman und J. Tate, das online bei der KUB verfügbar ist.

Dieses Seminar richtet sich an Studierende ab dem 5. Semester. Vorausgesetzte Kenntnisse sind die Grundlagenvorlesungen aus den ersten zwei Bachelorjahren.

Die Vorträge können auf Deutsch, Französisch oder Englisch gehalten werden.

Bei Interesse melden Sie sich bei C. Zehrt (christine.zehrt@unifr.ch) und/oder kommen zur Vorbesprechung. Weitere Informationen unter: `https://homeweb.unifr.ch/zehrtc/pub/`