Vorlesung — Arithmetik Elliptischer Kurven

SOMMERSEMESTER 2021

Marius Leonhardt

Gleichungen der Form

$$y^2 = x^3 + Ax + B \tag{1}$$

für fest gewählte A, B heißen *Elliptische Kurven*. Sie tauchen oft ganz unverhofft auf, z.B. bei der Frage, welche ganzen Zahlen genau zwischen einer Quadrat- und einer Kubikzahl liegen[1], oder bei der Suche nach rationalen Zahlen, die als Flächeninhalt eines rechtwinkligen Dreiecks mit rationalen Seitenlängen auftreten können.[2] Heutzutage finden sie Anwendung in der Kryptographie [5] und sind zum Beispiel auf dem Personalausweis gespeichert.

Elliptische Kurven sind deshalb so spannend, weil die Menge $E(K)$ ihrer K-wertigen Punkte, d.h. der $(x, y) \in K^2$, die (1) erfüllen, eine abelsche Gruppe bilden: Wir addieren zwei Punkte, indem wir die Gerade durch die beiden Punkte erneut mit E schneiden und den resultierenden Schnittpunkt an der x-Achse spiegeln, siehe Abbildung 1.

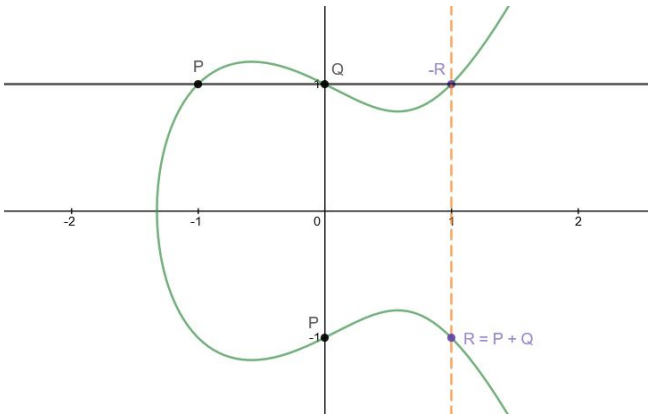

ABBILDUNG 1. Addition der Punkte $P = (-1, 1)$ und $Q = (0, 1)$ auf der Elliptischen Kurve $y^2 = x^3 - x + 1$.

Der Satz von Mordell–Weil besagt, dass die Menge der rationalen Punkte $E(\mathbb{Q})$ eine endlich erzeugte abelsche Gruppe bildet. Um den Rang dieser Gruppe rankt sich eines der berühmtesten Probleme der Mathematik, die Vermutung von Birch–Swinnerton-Dyer.

In der Vorlesung werden Elliptische Kurven eingeführt und deren grundlegende Eigenschaften studiert. Insbesondere das Verhalten von Gleichung (1) modulo verschiedener Primzahlen wird interessant werden. Außerdem betrachten wir die Kurve E über dem Körper $\mathbb{Q}_p$ der p-adischen Zahlen und finden Untergruppen

$$E(\mathbb{Q}_p) \supset E_0(\mathbb{Q}_p) \supset E_1(\mathbb{Q}_p) \supset \dots$$

Zum eingehenden Studium von $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ werden wir als Höhepunkt der Vorlesung das Néron-Modell von E berechnen. Dabei wird es nötig sein, Gruppenschemata und allgemein Modelle von Kurven wie (1) über Ringen wie $\mathbb{Z}$ oder $\mathbb{Z}_p$, die selbst keine Körper sind, zu betrachten. Dabei kommt eine bunte Mischung aus algebraisch-geometrischen und zahlentheoretischen Konzepten zusammen, die wir am konkreten Beispiel der Elliptischen Kurven in Aktion sehen werden.

[1] Die zugehörigen Gleichungen sind $y^2 = x^3 \pm 2$.

[2] Man nennt solche Zahlen D *kongruent*. Hier spielt die Elliptische Kurve $y^2 = x^3 - D^2x$ eine Rolle.

Vorkenntnisse: Algebraische Geometrie 1; Algebraische Zahlentheorie 1 (oder 2) ist ebenfalls nützlich. In den ersten Vorlesungen werden Themen behandelt, die im Seminar „Elliptische Kurven“ im Wintersemester vorgekommen sind; wer dieses besucht hat, ist auf jeden Fall bestens vorbereitet, aber dieses Wissen wird *nicht* vorausgesetzt.

Auch wenn man Algebraische Geometrie oder Zahlentheorie nicht gehört hat, eignet sich das Thema sehr gut, um Einblicke in die beiden Gebiete zu erhalten, nur müssen dann gewisse Resultate geglaubt oder nachgeholt werden. Auf die bestehenden Vorkenntnisse des Publikums wird eingegangen werden.

Zeit und Raum: Montag 11-13 Uhr, voraussichtlich über Webex.

Literatur: Wir folgen zunächst [3], bevor wir uns dem Schwerpunkt der Vorlesung [2, Ch. IV] zuwenden. Zum Anregen des Appetits (und ohne Vorkenntnisse in algebraischer Geometrie) ist [4] gut geeignet. Alle drei Bücher sind extrem gut geschrieben und zu empfehlen! [4] und [3] sind online abrufbar über HEIDI.

Für die Néron-Modelle werden wir gelegentlich auch einen Blick in [1] werfen.

Literatur

[1] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[2] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[3] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[4] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015.

[5] Annette Werner. *Elliptische Kurven in der Kryptographie*. Springer Lehrbuch. Springer-Verlag, Berlin, Heidelberg, 2002.