Arithmetik Elliptischer Kurven

Universität Frankfurt
Institut für Mathematik
Marius Leonhardt

Blatt 04
Wintersemester 2024/25
Besprechung am 18.12.2024

Aufgabe 1 (Isogenie) Es sei K ein Körper mit $\mathrm{char}(K) \neq 2$ und E die über K definierte Elliptische Kurve

$$E\colon \quad y^2 = x(x^2 + ax + b),$$

also $a, b \in K$ mit $b(a^2 - 4b) \neq 0$. Es sei $T = (0,0) \in E(K)[2]$. In dieser Aufgabe[1] konstruieren wir eine über K definierte elliptische Kurve E' sowie eine über K definierte Isogenie $\Phi\colon E \to E'$ mit $\ker(\Phi) = \langle T \rangle$.

(a) Die Punkte $P = (x, y)$ und $P + T = (x', y')$ sollen unter Φ auf denselben Punkt abgebildet werden. Die Gerade durch P und T hat Steigung $\lambda = \frac{y}{x}$. Falls noch nicht geschehen, zeige Blatt 3, Aufgabe 2(c): $(x', y') = \left(\frac{b}{x}, -\frac{by}{x^2}\right)$.

(b) Für die Koordinaten von Φ wählen wir Ausdrücke, die symmetrisch in x, x' bzw. y, y' sind. Dazu sei $\xi := x + x' + a$ und $\eta = y + y'$. Zeige $\xi = \lambda^2$ und $\eta^2 = \xi(\xi^2 - 2a\xi + a^2 - 4b)$.

(c) Es seien $a' = -2a$ und $b' = a^2 - 4b$ sowie

$$E'\colon \quad y^2 = x(x^2 + a'x + b').$$

Zeige, dass E' eine Elliptische Kurve ist und dass $\Phi = [\xi : \eta : 1]$ eine Isogenie von E nach E' definiert. Zeige $\Phi(T) = O$ und bestimme $\deg(\Phi)$.

(d) Bestimme $\Phi(E[2])$ und die zu Φ duale Isogenie $\widehat{\Phi}\colon E' \to E$.

Aufgabe 2 (Elliptische Kurve über $\mathbb{F}_{13}$) Es sei E die über $\mathbb{F}_{13}$ definierte Elliptische Kurve

$$E\colon \quad y^2 = x^3 + x + 5.$$

(a) Bestimme $\#E(\mathbb{F}_{13})$ und zeige, dass $E(\mathbb{F}_{13})$ zyklisch ist.

(b) Finde eine elliptische Kurve E' über $\mathbb{F}_{13}$, für die $E'(\mathbb{F}_{13})$ nicht zyklisch ist. Gibt es E', sodass $E'(\mathbb{F}_{13})$ nicht von zwei Elementen erzeugt ist?

(c) Ohne die Punkte explizit anzugeben, bestimme $\#E(\mathbb{F}_{13^2})$. Ist $E(\mathbb{F}_{13^2})$ zyklisch?

Aufgabe 3 (Quadratische Twists) Es sei p eine ungerade Primzahl und $E/\mathbb{F}_p$ eine Elliptische Kurve.

(a) Konstruiere eine Elliptische Kurve E' über $\mathbb{F}_p$ mit $\#E(\mathbb{F}_p) + \#E'(\mathbb{F}_p) = 2(p+1)$.

(b) Zeige weiter, dass $E(\mathbb{F}_p) \times E'(\mathbb{F}_p)$ und $E(\mathbb{F}_{p^2})$ dieselbe Ordnung haben, aber nicht isomorph sein müssen.

Aufgabe 4 (Spur und Grad) Es sei E eine Elliptische Kurve sowie $\Phi, \Psi \in \mathrm{End}(E)$. Zeige:

(a) $\deg([n] + \Phi) = n^2 + n\,\mathrm{tr}(\Phi) + \deg(\Phi)$.

(b) $\mathrm{tr}(\Phi + \Psi) = \mathrm{tr}(\Phi) + \mathrm{tr}(\Psi)$.

(c) $\mathrm{tr}(\Phi^2) = \mathrm{tr}(\Phi)^2 - 2\deg(\Phi)$.

(d) $\Phi^2 - [\mathrm{tr}(\Phi)]\Phi + [\deg(\Phi)] = 0$.

Aufgabe 5 (Weil-Vermutungen)

(a) Überzeuge dich davon, dass wir die Weil-Vermutungen für eine Elliptische Kurve E über $\mathbb{F}_q$ bewiesen haben.

(b) Bestimme explizit die rationale Funktion $Z_{\mathbb{P}^1}(T)$ und zeige damit die Weil-Vermutungen für die Kurve $\mathbb{P}^1$ über $\mathbb{F}_q$.

---

[1] Wir schildern hier einen Spezialfall der Konstruktion aus [AEC, III.4.12]: Ist E eine Elliptische Kurve und H eine endliche Untergruppe von E, so gibt es eine eindeutig bestimmte Elliptische Kurve E' und eine separable Isogenie $\Phi\colon E \to E'$ mit $\ker(\Phi) = H$. Man schreibt oft $E' = E/H$. In unserem Beispiel ist $H = \langle T \rangle$.

Es gilt sogar die folgende Version [AEC, III.4.11] des Homomorphiesatzes: Ist $\Psi\colon E \to E''$ eine Isogenie mit $H \subset \ker(\Psi)$, so gibt es eine eindeutige Isogenie $\lambda\colon E' \to E''$, sodass $\lambda \circ \Phi = \Psi$.