

Elliptische Funktionen und elliptische Kurven

Übungsaufgaben zum 9. Tutorium am 18.12.2018

Aufgabe 31

Seien $(C_1, \mathcal{O}_1)$ und $(C_2, \mathcal{O}_2)$ elliptische Kurven über einem endlichen Körper $\mathbb{F}_q$, und sei $\varphi : C_1 \rightarrow C_2$ eine nicht-konstante Isogenie, die über $\mathbb{F}_q$ definiert ist. Zeigen Sie:

$$|C_1(\mathbb{F}_q)| = |C_2(\mathbb{F}_q)|.$$

Aufgabe 32

Sei $F \in \mathbb{F}_2[X, Y, Z]$ mit $F(X, Y, Z) := Y^2Z + YZ^2 + X^3$, und $C := V(F)$ die dadurch definierte Kurve über $\mathbb{F}_2$.

- a) Zeigen Sie, dass C glatt ist.
- b) Überprüfen Sie die Weil-Vermutungen, indem Sie die Gruppen $C(\mathbb{F}_2)$ und $C(\mathbb{F}_4)$ explizit bestimmen.

Aufgabe 33

Sei p eine Primzahl mit $p \equiv 2 \pmod{3}$. Sei $C = V(F)$ eine elliptische Kurve über $\mathbb{F}_p$, die gegeben wird durch ein Polynom der Form $F(X, Y, Z) = Y^2Z - X^3 - bZ^3$, mit $b \in \mathbb{F}_p$. Bestimmen Sie die Anzahl $|C(\mathbb{F}_p)|$.

Aufgabe 34

Sei $\mathbb{F}_q$ ein endlicher Körper, mit Charakteristik $\text{char}(\mathbb{F}_q) \notin \{2, 3\}$. Der Körper enthalte ein Element $\rho \in \mathbb{F}_q$ mit der Eigenschaft $\rho^3 = 1$ und $\rho \neq 1$. Sei $C := V(Y^2Z - X^3 - bZ^3)$ eine elliptische Kurve über $\mathbb{F}_q$, mit $b \neq 0$. Zeigen Sie:

- a) Durch $\tau(X : Y : Z) := (\rho X : Y : Z)$ wird ein Endomorphismus auf C definiert.
- b) Es gilt die Gleichheit von Endomorphismen $(\tau - \tau^2)^2 = -3$.

Keine Abgabe, nur zur Vorbereitung auf das Tutorium!