Summer term 2024 Dr. Andreas Mihatsch
Elliptic curves and their moduli spaces

Homework problems (due June 12)

Problem 1 (Examples of complex multiplication)

(a) Consider the complex elliptic curve E with affine Weierstrass equation $y^2 = x^3 + ax$. Show that $x \mapsto -x$, $y \mapsto iy$ extends to an endomorphism of E. Prove that $\mathrm{End}(E) \cong \mathbb{Z}[i]$.

(b) Let $\zeta = e^{2\pi i/3} \in \mathbb{C}$ be a primitive third root of unity. Let E be the complex elliptic curve with Weierstrass equation $y^2 = x^3 + b$. Show that $\mathrm{End}(E) \cong \mathbb{Z}[\zeta]$.

Problem 2 (Relative Weierstrass equation)

Let S be locally noetherian and let E/S be an elliptic curve. Prove that for every point $s \in S$ there exist an open neighborhood U and sections $a_1, a_2, a_3, a_4, a_6 \in \Gamma(U, \mathcal{O}_U)$ such that $U \times_S E \to U$ is defined by the affine Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Hint: Extend the method from the end of §6.6 of the lecture notes to a general base.

Further Problems

Problem 3 (Frobenius endomorphism)

Let $q = p^r$ be a prime power, and let $E/\mathbb{F}_q$ be an elliptic curve. Show that the absolute Frobenius $F : E \to E$ lies in $\mathrm{End}(E)$. Determine $\deg(F)$ and $\ker(F)$.

Recall that F is defined by $|F| = \mathrm{id}$ and $F^*(f) = f^q$ for every $U \subseteq E$, $f \in \mathcal{O}_E(U)$.

Assume that r is odd. Argue that in this case $F \notin \mathbb{Z}$, and that in particular $\mathbb{Z} \subsetneq \mathrm{End}(E)$.