Exercise Sheet 6

Discussed on 02.06.2021

Problem 1. Let k be a field and E an elliptic curve over k with an embedding $E \hookrightarrow \mathbb{P}^2_k$ via a Weierstraß equation. In particular we have the coordinate functions $x, y \in k(E)$. Let $e := \infty \in E(k)$ and pick any $p, q \in E(k)$.

(a) Show that up to scaling, there is a unique non-zero function $f \in \Gamma(E, \mathcal{O}(3e - p - q))$. It is of the form $f = ax + by + c$ for some $a, b, c \in k$ such that p and q lie on the line

$$L_{p,q} := V_+(ax + by + cz) \subset \mathbb{P}^2_k.$$

Hint: Recall that $\Gamma(E, \mathcal{O}(3e))$ is generated by $1, x, y$ over k.

(b) Using f we obtain an exact sequence

$$0 \to \mathcal{O} \xrightarrow{f} \mathcal{O}(3e - p - q) \to \mathcal{F} \to 0,$$

of sheaves on E, where $\mathcal{F}$ is a skyscraper sheaf concentrated at $r := p + q \in E(k)$. Show that r is the third intersection of $L_{p,q}$ with E (counted with multiplicity).

Problem 2. Let p be a prime, $q = p^n$ for some $n \geq 0$ and E an elliptic curve over $\mathbb{F}_q$.

(a) For every $\mathbb{F}_p$-scheme X, the *absolute Frobenius* $F_X \colon X \to X$ is the morphism of schemes which is the identity on topological spaces and maps $a \mapsto a^p$ on coordinate rings. Show that $f := F_E^n \colon E \to E$ is an isogeny of E of degree q.

(b) Compute $\ker(f)$. Deduce that if E is ordinary[1] then $f \notin \mathbb{Z}$, hence $\mathrm{End}^0(E)$ is at least a quadratic extension of $\mathbb{Q}$.

(c) Assume that E is ordinary. Show that for all $m \geq 1$, $E[p^m](\overline{\mathbb{F}}_q) \cong \mathbb{Z}/p^m\mathbb{Z}$. We define the p-adic Tate module

$$T_pE := \varprojlim_m E[p^m](\overline{\mathbb{F}}_q) \cong \mathbb{Z}_p.$$

Show that $\mathrm{End}(E)$ acts on T_pE and hence cannot be a quaternion algebra. Deduce that $\mathrm{End}^0(E)$ is a quadratic extension of $\mathbb{Q}$.

Hint on (c): For the first part, show first that for any field k and any surjection of finite-type k-schemes $X \twoheadrightarrow Y$, the map $X(\overline{k}) \twoheadrightarrow Y(\overline{k})$ is surjective.

[1] Recall that E is ordinary iff $E[p](\overline{\mathbb{F}}_q) \cong \mathbb{Z}/p\mathbb{Z}$.

Problem 3. Let k be a field of characteristic $p > 0$ and let E be an elliptic curve over k.

(a) Show that there are natural projection maps $\mathrm{End}(E[p^n]) \to \mathrm{End}(E[p^{n-1}])$ for all $n > 1$.

(b) Show that there is a natural map

$$\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \varprojlim_n \mathrm{End}(E[p^n]).$$

Show that this map is injective.

Hint: Use the same strategy as in the ℓ-adic case (see lecture).