# Reductions of CM Elliptic Curves

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over $\mathbb{Q}$. As we discussed, the endomorphism ring $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ is either isomorphic to $\mathbb{Z}$ or isomorphic to an order $\mathcal{O}$ of an imaginary quadratic field $K$ which is a free $\mathbb{Z}$-module of rank 2.

For all but finitely many primes $p$, the reduction of $E$ at $p$ is an elliptic curve $\mathcal{E}_p$ defined over $\mathbb{F}_p$. The Endomorphism ring $\mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E}_p)$ is either isomorphic to an order of an imaginary quadratic field or isomorphic to an order of a quaternion algebra which is a free $\mathbb{Z}$-module of rank 4.

Given a fixed elliptic curve $E/\mathbb{Q}$, We want to discuss the set of primes at which the reduction of $E$ has a larger Endomorphism ring.

## 1 Endomorphism Rings of Elliptic Curves over Finite fields

Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_q$ defined by $y^2 = x^3 + ax + b, a, b \in \mathbb{F}_q$. Let $p$ be the characteristic of $\mathbb{F}_q$. The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \simeq \widehat{\mathbb{Z}}$ is topologically generated by a single element $\sigma$, often referred to as the Frobenius element. For $\alpha \in \overline{\mathbb{F}}_p$, $\sigma(\alpha) = \alpha^p$. Recall the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ acts on the set of elliptic curves defined over $\overline{\mathbb{F}}_p$ with $\sigma$ maps $\mathcal{E}$ to $\mathcal{E}^\sigma : y^2 = x^3 + a^p x + b^p$. Note that the map $\mathcal{E} \to \mathcal{E}^\sigma : (x, y) \mapsto (x^p, y^p)$ is an algebraic map (different from a Galois element in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ case), thus an isogeny.

Since $\mathcal{E}$ is defined over $\mathbb{F}_q$, it admits an endomorphism $\phi : (x, y) \mapsto (x^q, y^q)$, the $q$-th power Frobenius map. The map $\phi$ is purely inseparable of degree $q$.

For simplicity, we can consider $\mathcal{E}$ defined over a prime field $\mathbb{F}_p$ with $p \neq 2$. Since the Frobenius morphism has degree $p$, we can see that the ring $\mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E})$ has an element with norm $p$. If $\mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E})$ is isomorphic to an order $\mathcal{O}$ of an imaginary quadratic field $K$, then $p$ has to split in $K/\mathbb{Q}$. In this case, we say $\mathcal{E}$ is ordinary.

**Definition 1.1.** A definite quaternion algebra $B$ over $\mathbb{Q}$ is the $\mathbb{Q}$-algebra defined by

$$B = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

with multiplication defined by

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2, \beta^2 < 0, \quad \beta\alpha = -\alpha\beta.$$

For any prime $p$, the $\mathbb{Q}_p$ algebra $B \otimes \mathbb{Q}_p$ is either still a division algebra or isomorphic to the matrix algebra $M_2(\mathbb{Q}_p)$. If $B \otimes \mathbb{Q}_p \simeq M_2(\mathbb{Q}_p)$, then we say $p$ is split or unramified for $B$, and if $B \otimes \mathbb{Q}_p$ is a division algebra, then we call $p$ ramified. Every quaternion algebra is ramified at finitely many primes and this set of primes determines $B$.

An order $O \subset B$ is a lattice (a finitely generated $\mathbb{Z}$-module satisfying $O \otimes \mathbb{Q} = B$) that is also a subring of $B$. An order is maximal if it is not properly contained in another order.

If $\mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E})$ is not isomorphic to an order of an imaginary quadratic field, then $B = \mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E}) \otimes \mathbb{Q}$ is a definite quaternion algebra over $\mathbb{Q}$ with the only ramified finite prime being $p$. The Endomorphism ring $\mathrm{End}_{\overline{\mathbb{F}}_p}(\mathcal{E})$ is isomorphic to $O \subset B$ which a maximal order of $B$. In this case, we say $\mathcal{E}$ is supersingular.

Note that from our definition, the property for an elliptic curve $\mathcal{E}/\mathbb{F}_q$ being ordinary or supersingular does not change under base field extensions. Thus, they are determined by the $j$-invariants.

When $p$ is ramified in $B$, the division algebra $B \otimes \mathbb{Q}_p$ has a unique maximal order $O_p$ which contains all elements with non-negative valuation with respect to the unique valuation on $B \otimes \mathbb{Q}_p$ extending the $p$-adic valuation of $\mathbb{Q}_p$. The ring $O_p$ has a unique maximal ideal $P_p$ whose residue field is isomorphic to $\mathbb{F}_{p^2}$. Moreover, $P_p^2 = pO$ and the algebra $B \otimes \mathbb{Q}_{p^2} \simeq M_2(\mathbb{Q}_{p^2})$. The quadratic fields $K/\mathbb{Q}$ contained in $B$ are the ones satisfying $B \otimes K \simeq M_2(K)$, these are exactly the imaginary quadratic fields $K/\mathbb{Q}$ in which $p$ is inert or ramified.

# 2 Density of Supersingular Primes

Let $E/\mathbb{Q}$ be an elliptic curve. Let $p > 3$ be a prime of good reduction for $E$. The reduction of $E$ at $p$ is an elliptic curve $\mathcal{E}_p/\mathbb{F}_p$. Let $a_p \in \mathbb{Z}$ be the trace of Frobenius action on $\mathcal{E}_p[\ell^\infty]$. Then $\mathcal{E}_p$ is supersingular if and only if $a_p = 0$. From the Hasse bound, we know that $-2\sqrt{p} \leq a_p \leq 2\sqrt{p}$. Thus, if $a_p$ is randomly distributed, then the probability of $a_p = 0$ should be roughly $\frac{1}{4\sqrt{p}}$. If we sum over all primes $p$, the number of primes $p < X$ such that $\mathcal{E}_p$ is a supersingular elliptic curve is about $\frac{\sqrt{X}}{\log X}$. This is a special case of the Lang–Trotter conjecture predicting the expectation for the number of supersingular primes for a general elliptic curve. When an elliptic curve $E$ has complex multiplication, the distribution of $a_p$ is known to be not random.

**Theorem 2.1** (Shimura–Taniyama)**.** *Let $E/L$ be an elliptic curve with complex multiplication by $\mathcal{O} \subset K$. Let $\mathfrak{p} \subset L$ be a prime lying above the rational prime $p$ at which $E$ admits good reduction. If $p$ splits in $K/\mathbb{Q}$, then the reduction $\mathcal{E}_\mathfrak{p}$ is ordinary. If $p$ is inert or ramified in $K/\mathbb{Q}$, then the reduction $\mathcal{E}_\mathfrak{p}$ is supersingular.*

Extending the field $L$ if necessary such that $K \subset L$, this theorem follows from the fact that $\mathrm{End}_L(E) \to \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\mathcal{E}_\mathfrak{p})$ is injective. As we discussed in the previous section, the endomorphism algebra $\mathrm{End}_{\overline{\mathbb{F}}_\mathfrak{p}}(\mathcal{E}_\mathfrak{p}) \otimes \mathbb{Q}$ contains an imaginary quadratic field $K/\mathbb{Q}$ in which $p$ splits if and only if $\mathcal{E}_p$ is ordinary.

**Theorem 2.2** (Serre)**.** *Let $E$ be an elliptic curve without complex multiplication defined over $\mathbb{Q}$, the set of primes $p$ at which the reduction of $E$ is ordinary has density* 1*.*

# 3 Elkies's Theorem

**Theorem 3.1** (Elkies)**.** *Let $E$ be an elliptic curve defined over $\mathbb{Q}$. There exist infinitely many primes $p$ such that the reduction of $E$ at $p$ is supersingular.*

When $E$ is a CM elliptic curve, the statement follows from the theorem of Shimura–Taniyama. So we will assume $E$ does not have CM.

Idea of proof: Assume $E$ admits supersingular reduction at finitely many primes. Let the finite set $S$ contain all supersingular primes and all primes at which $E$ admits bad reduction. We would want to construct a prime $p \notin S$ such that $\mathcal{E}_p$ is supersingular.

To construct such a $p$, we will construct a CM elliptic curve $E_0$ such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E_0) \otimes \mathbb{Q} \simeq K$, $\mathcal{E}_p$ is isomorphic to the reduction of $E_0$ at a prime above $p$ over $\overline{\mathbb{F}}_p$, and $p$ does not split in $K/\mathbb{Q}$. In fact, instead of constructing a $E_0$, in practice, we construct the field $K$ which guarantees the existence of a desired $E_0$.

Next we will give a sketch of the proof in a simplified case.

Goal: given $E/\mathbb{Q}$ with $j_E < 1728$ and a finite set $S$ of primes, construct a supersingular prime $p \notin S$.

1. Let $D$ be a prime satisfying
   (a) $D \equiv 3 \bmod 4$;
   (b) for each $p \in S$ or $p \mid (j_E - 1728)$, we have $p$ splits in $K = \mathbb{Q}(\sqrt{-D})/\mathbb{Q}$;
   (c) $D$ is sufficiently large.

Such a prime $D$ exists by Dirichlet's theorem which states that there exist infinitely many primes in any congruence class $a \pmod b$ when $\gcd(a, b) = 1$.

Note that $D \equiv 3 \bmod 4$ implies $\left(\frac{-1}{D}\right) = -1$ which is of important use in the proof.

2. Consider elliptic curves $E_1, \cdots, E_n$ with complex multiplication by the maximal order $\mathcal{O}_K \subset K$.

   Any $p$ non-split in $K/\mathbb{Q}$ is a supersingular prime for $E_1, \cdots, E_n$.

3. Define the following monic irreducible polynomial

$$P_D(x) = \prod_{i=1}^{n}(x - j_i) \in \mathbb{Z}[x]$$

   whose roots are the $j$-invariants of $E_1, \cdots, E_n$.

   Recall that $P_D(x)$ has all coefficients in $\mathbb{Z}$ because $j_1, \cdots, j_n$ are Galois conjugates and they are all algebraic integers.

   Moreover, for any prime $p \mid P_D(j_E)$, the reduction $\mathcal{E}_p$ is isomorphic to the reduction of some $E_i$ at a prime above $p$ over $\overline{\mathbb{F}}_p$.

4. Show $(j_E - 1728)P_D(j_E) \equiv \square \bmod D$.

   This statement follows from Deuring's lifting lemma.

   This implies either

$$D \mid (j_E - 1728)P_D(j_E) \text{ recall } D \nmid (j_E - 1728) \text{ by our assumption}$$

   or the Legendre symbol $\left(\frac{(j_E - 1728)P_D(j_E)}{D}\right) = 1$.

5. $P_D(x)$ has a unique real root and $(j_E - 1728)P_D(j_E) < 0$ as long as $D$ is sufficiently large.

   To determine the sign of $P_D(j_E)$, we need to analyze the real roots of $P_D(x)$. The real $j$-invariants correspond to lattices which are fixed by complex conjugation. These are the fractional ideal classes $\mathfrak{a} \subset cl(\mathcal{O}_K)$ such that $\mathfrak{a}^{-1} = \bar{\mathfrak{a}} = \mathfrak{a}$, thus they are in $cl(\mathcal{O}_K)[2]$. From genus theory, for imaginary quadratic field with prime discriminant, the group $cl(\mathcal{O}_K)[2]$ is trivial. Thus the only real CM $j$-invariant is $j(\frac{1+\sqrt{-D}}{2})$.

   Recall $j(\tau) = q^{-1} + 744 + 196884q + \cdots, \quad q = e^{2\pi i \tau}$.

   Thus $j(\frac{1+\sqrt{-D}}{2}) < 0$ for $D$ sufficiently large. Combine this fact with our assumption $j_E < 1728$.

   If $D \nmid P_D(j_E)$, we deduce the Legendre symbol

$$\left(\frac{(j_E - 1728)P_D(j_E)}{D}\right) = \left(\frac{(-1)|(j_E - 1728)P_D(j_E)|}{D}\right) = 1.$$

   Combined with $\left(\frac{-1}{D}\right) = -1$, we get $\left(\frac{|(j_E - 1728)P_D(j_E)|}{D}\right) = -1$.

6. Recall that the Legendre symbol is multiplicative.

   There either exists a positive $p \mid P_D(j_E)$ such that (recall all $p \mid (j_E - 1728)$ splits in $\mathbb{Q}(-D)/\mathbb{Q}$)

$$\left(\frac{p}{D}\right) = \left(\frac{-D}{p}\right) = -1;$$

   or $D \mid P_D(j_E)$. Either way, we obtain a non-split prime $p$ or $D$ which is a supersingular prime for $E$ not contained in $S$.