Generating supersingular curves with modular polynomials

Simon Pohmann

July 27, 2022

1 Introduction

2 Ordinary isogeny graphs

Definition 2.1. For an integral ideal $\mathfrak{a} \leq \mathrm{End}(E)$ of an ordinary Elliptic Curve E, define the $\mathfrak{a}$-torsion

$$E[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\alpha)$$

Lemma 2.2. *Let $\phi : E \to E'$ be an isogeny. Then there is an isomorphism*

$$\Phi : \mathrm{End}(E) \otimes \mathbb{Q} \to \mathrm{End}(E') \to \mathbb{Q}, \quad \tau \mapsto \frac{1}{\deg(\phi)} \phi \circ \tau \circ \hat{\phi}$$

Furthermore, if we assume E to be ordinary, then this is canonical in the sense that for any other isogeny $\psi : E \to E'$ have $\Phi = \Psi$.

Proposition 2.3. *Let $\phi : E \to E'$ be an isogeny of prime degree p. Then (after embedding* $\mathrm{End}(E')$ *via* Φ *and* $\mathrm{End}(E)$ *into* $\mathrm{End}(E) \otimes \mathbb{Q}$*) exactly one of the following is the case.*

- $\mathrm{End}(E) = \mathrm{End}(E')$ *and we call ϕ* horizontal.
- $\mathrm{End}(E) \subseteq \mathrm{End}(E')$ *with* $[\mathrm{End}(E') : \mathrm{End}(E)] = p$. *We call ϕ* ascending.
- $\mathrm{End}(E) \supseteq \mathrm{End}(E')$ *with* $[\mathrm{End}(E) : \mathrm{End}(E')] = p$. *We call ϕ* descending.

Proposition 2.4. *Similarly, let $\phi : E \to E'$ be an isogeny of any degree n. Further, let l be a prime. Then (after embedding* $\mathrm{End}(E') \otimes \mathbb{Z}_{(l)}$ *via* Φ *and* $\mathrm{End}(E) \otimes \mathbb{Z}_{(l)}$ *into* $\mathrm{End}(E) \otimes \mathbb{Q}$*)exactly one of the following is the case.*

- $\mathrm{End}(E) \otimes \mathbb{Z}_{(l)} = \mathrm{End}(E') \otimes \mathbb{Z}_{(l)}$ *and we call ϕ* horizontal at l.
- $\mathrm{End}(E) \otimes \mathbb{Z}_{(l)} \subseteq \mathrm{End}(E') \otimes \mathbb{Z}_{(l)}$ *with* $[\mathrm{End}(E') \otimes \mathbb{Z}_{(l)} : \mathrm{End}(E) \otimes \mathbb{Z}_{(l)}] = l^r$ *for* $r > 0$. *We call ϕ* ascending at l.

- $\mathrm{End}(E) \otimes \mathbb{Z}_{(l)} \supseteq \mathrm{End}(E') \otimes \mathbb{Z}_{(l)}$ *with* $[\mathrm{End}(E) \otimes \mathbb{Z}_{(l)} : \mathrm{End}(E') \otimes \mathbb{Z}_{(l)}] = p$ *for* $r > 0$. *We call* ϕ descending at l.

Definition 2.5. For an ordinary Elliptic Curve E and an integral, invertible ideal $\mathfrak{a} = \mathfrak{b}(p, \pi_E)^r \leq \mathrm{End}(E)$ with $\mathfrak{b} \perp (p, \pi_E)$ define the isogeny

$$\phi_{E,\mathfrak{a}} : E \longrightarrow E/E[\mathfrak{b}] \xrightarrow{\pi} E_{\mathfrak{a}} := (E/E[\mathfrak{b}])^{(p^r)}$$

where $E \to E/E[\mathfrak{b}]$ is the separable isogeny with kernel $E[\mathfrak{b}]$ and $\pi : E/E[\mathfrak{b}] \to (E/E[\mathfrak{b}])^{(p^r)}$ is the r-th power Frobenius map.

Lemma 2.6. *Let E be an ordinary Elliptic Curve and $\mathfrak{a} \leq \mathrm{End}(E)$ an integral, invertible ideal. Then $\mathrm{End}(E) \cong \mathrm{End}(E_{\mathfrak{a}})$. In particular, $\phi_{E,\mathfrak{a}}$ is horizontal at every prime l.*

Proof. Let $\mathfrak{a} = \mathfrak{b}(p, \pi_E)^r$ with $\mathfrak{b} \perp (p, \pi_E)$. We show that $\mathrm{End}(E) \cong \mathrm{End}(E/E[\mathfrak{b}])$ and the claim follows, as for any Elliptic Curve E, have an isomorphism

$$\mathrm{End}(E) \to \mathrm{End}(E^{(p)}), \quad \alpha \mapsto \alpha^{(p)}$$

It suffices to show that the isogeny $\phi : E \to E' := E/E[\mathfrak{b}]$ is horizontal at each prime l.

Assume for a contradiction that ϕ is descending at l. In other words, there is $\tau \in \mathrm{End}(E)$ such that $\phi \circ \tau \circ \hat{\phi}$ is not divisible by l. Hence, $E'[l] \not\subseteq \ker(\phi \circ \tau \circ \hat{\phi})$ and there is a point $P \in E'[l]$ with $\phi(\tau(\hat{\phi}(P))) \neq O$. This implies $\tau(\hat{\phi}(P)) \notin E[\mathfrak{a}]$ and thus there is $\alpha \in \mathfrak{a}$ with $\tau(\hat{\phi}(P)) \notin \ker(\alpha)$. Note that α factors through ϕ as

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[rr, bend left, "\alpha"] & E' \arrow[r, "\psi"] & E \end{tikzcd}$$

We assume $l \mid n$, otherwise the claim is trivial. However, then we have the contradiction

$$\begin{aligned} \psi((\phi \circ \tau \circ \hat{\phi})(P)) &= (\psi \circ \phi \circ \tau \circ \hat{\phi})(P) = (\alpha \circ \tau \circ \hat{\phi})(P) \\ &= (\tau \circ \alpha \circ \hat{\phi})(P) = (\tau \circ \psi \circ [n])(P) = (\tau \circ \psi)(O) = O \end{aligned}$$

since $\tau \circ \alpha = \alpha \circ \tau$ ($\mathrm{End}(E)$ is commutative). ☐

Lemma 2.7. *Let $\mathcal{O}$ be a quadratic imaginary order with $p \nmid d(\mathcal{O})$ with two integral, invertible ideals $\mathfrak{a}, \mathfrak{b} \leq \mathcal{O}$. Let further E be an Elliptic Curve with $\mathrm{End}(E) \cong \mathcal{O}$. Identifying $\mathrm{End}(E_{\mathfrak{a}})$ with $\mathcal{O}$ by the canonical isomorphism $\Phi_{E,\mathfrak{a}} : \mathrm{End}(E) \xrightarrow{\sim} \mathrm{End}(E_{\mathfrak{a}})$, we have*

$$E_{\mathfrak{ab}} \cong (E_{\mathfrak{a}})_{\mathfrak{b}} \quad \textit{and} \quad \phi_{E,\mathfrak{ab}} = \phi_{E_{\mathfrak{a}},\mathfrak{b}} \circ \phi_{E,\mathfrak{a}}$$

Proof. First, we show that $\Phi_{E,\mathfrak{a}}(\pi_E) = \pi_{E_{\mathfrak{a}}}$ and so we can write $\pi \in \mathcal{O}$ for the unique element mapping to the Frobenius in $\mathrm{End}(E)$ resp. $\mathrm{End}(E_{\mathfrak{a}})$. We have that

$$\Phi_{E,\mathfrak{a}}(\pi_E) = \frac{1}{\deg(\phi_{E,\mathfrak{a}})} \phi_{E,\mathfrak{a}} \circ \pi_E \circ \hat{\phi}_{E,\mathfrak{a}}$$

and so

$$\phi_{E,\mathfrak{a}} \circ \hat{\phi}_{E,\mathfrak{a}} \circ \Phi_{E,\mathfrak{a}}(\pi_E) = \phi_{E,\mathfrak{a}} \circ \pi_E \circ \hat{\phi}_{E,\mathfrak{a}}$$

Counting separability degrees on both sides shows that $\Phi_{E,\mathfrak{a}}(\pi_E)$ is purely inseparable, thus must be the Frobenius $\pi_{E_\mathfrak{a}}$.

Now write $\mathfrak{a} = \tilde{\mathfrak{a}}(p,\pi)^r$ and $\mathfrak{b} = \tilde{\mathfrak{b}}(p,\pi)^s$. It is now the case that

$$\phi_{E,\mathfrak{a}\mathfrak{b}} = \phi_{E,\tilde{\mathfrak{a}}\tilde{\mathfrak{b}}}^{(p^{r+s})}$$

and

$$\phi_{E_\mathfrak{a},\mathfrak{b}} \circ \phi_{E,\mathfrak{a}} = (\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}} \circ \pi_r \circ \phi_{E,\tilde{\mathfrak{a}}})^{(p^s)} = (\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}} \circ \phi)^{(p^r)} = (\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}}^{(q/p^r)} \circ \phi_{E,\tilde{\mathfrak{a}}})^{(p^{r+s})}$$

where $\pi_r : E_{\tilde{\mathfrak{a}}} \to E_{\tilde{\mathfrak{a}}}^{(p^r)}$ is the r-th power Frobenius and $\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}}$ is defined over $\mathbb{F}_q$. Note that $\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}}$ is the separable isogeny with kernel $E_\mathfrak{a}[\tilde{\mathfrak{b}}]$ and thus $\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}}^{(q/p^r)}$ is the separable isogeny with kernel $E_\mathfrak{a}^{(q/p^r)}[\tilde{\mathfrak{b}}] = E_{\tilde{\mathfrak{a}}}[\tilde{\mathfrak{b}}]$. In other words, find

$$\phi_{E_\mathfrak{a},\tilde{\mathfrak{b}}}^{(q/p^r)} = \phi_{E_{\tilde{\mathfrak{a}}},\tilde{\mathfrak{b}}}$$

and so it suffices to show the claim in the case that $\mathfrak{a} = \tilde{\mathfrak{a}}$, $\mathfrak{b} = \tilde{\mathfrak{b}}$ are integral, invertible ideals coprime to (p,π).

Having reduced everything to the separable case, it now suffices to show that $\ker(\phi_{E_\mathfrak{a},\mathfrak{b}} \circ \phi_{E,\mathfrak{a}}) = E[\mathfrak{a}\mathfrak{b}]$. For simplicity of notation, write $\phi = \phi_{E,\mathfrak{a}}$ and $\psi = \phi_{E_\mathfrak{a},\mathfrak{b}}$. Hence, we want to show that $\ker(\psi \circ \phi) = E[\mathfrak{a}\mathfrak{b}]$.

The crucial point here is that our isomorphism $\mathrm{End}(E) \cong \mathrm{End}(E_\mathfrak{a})$ is given by Φ. Since the identification of $\mathrm{End}(E)$ and $\mathrm{End}(E_\mathfrak{a})$ would hide this, we will be explicit in this part and write

$$i : \mathcal{O} \to \mathrm{End}(E) \quad \text{and} \quad i' : \mathcal{O} \to \mathrm{End}(E')$$

for the isomorphisms. Note that $\Phi \circ i = i'$. We have

$$\begin{aligned}
\ker(\psi \circ \phi) =& \phi^{-1}(\ker \psi) = \phi^{-1}(E'[\mathfrak{a}]) = \phi^{-1}\Big(\bigcap_{\tau \in \mathfrak{a}} \ker(i'(\tau))\Big) \\
&= \bigcap_{\tau \in \mathfrak{a}} \phi^{-1}(\ker(i'(\tau))) = \bigcap_{\tau \in \mathfrak{a}} \ker(i'(\tau) \circ \phi) \overset{(*)}{=} \bigcap_{\tau \in \mathfrak{a}} \ker(\phi \circ i(\tau)) \\
&= \bigcap_{\tau \in \mathfrak{a}} i(\tau)^{-1}(\ker \phi) = \bigcap_{\tau \in \mathfrak{a}} i(\tau)^{-1}(E[\mathfrak{b}]) = \bigcap_{\tau \in \mathfrak{a},\ \rho \in \mathfrak{b}} i(\tau)^{-1}(\ker(i(\rho))) \\
&= \bigcap_{\tau \in \mathfrak{a},\ \rho \in \mathfrak{b}} \ker(\underbrace{i(\rho) \circ i(\tau)}_{= i(\rho\tau) \in i(\mathfrak{a}\mathfrak{b})}) = E[\mathfrak{b}\mathfrak{a}]
\end{aligned}$$

The equality at $(*)$ holds, since

$$i'(\tau) = (\Phi_* \circ i)(\tau) = \frac{1}{\deg(\phi)} \phi \circ i(\tau) \circ \hat{\phi} \qquad \square$$

Lemma 2.8. *Let E be an ordinary curve and $\mathfrak{a}, \mathfrak{b} \leq \mathrm{End}(E)$ two integral, invertible ideals. Then $E_{\mathfrak{a}} \cong E_{\mathfrak{b}}$ if and only if $[\mathfrak{a}] = [\mathfrak{b}] \in \mathrm{Cl}(\mathrm{End}(E))$ are in the same ideal class.*

Theorem 2.9. *Let $\mathcal{O}$ be an imaginary quadratic order with $p \nmid d(\mathcal{O})$ and denote by $\mathrm{Ell}(\mathcal{O})$ the set of isomorphism classes of all Elliptic Curves E over $\bar{\mathbb{F}}_p$ with $\mathrm{End}(E) \cong \mathcal{O}$. Then there is a free and transitive group action*

$$\mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}(\mathcal{O}) \to \mathrm{Ell}(\mathcal{O}), \quad ([\mathfrak{a}], E) \mapsto E_{\mathfrak{a}}$$

where $\mathfrak{a}$ is an integral, invertible ideal representative of the ideal class $[\mathfrak{a}]$.

3 Supersingular isogeny graphs

4 Generating supersingular curves