Generating supersingular curves with modular polynomials

Simon Pohmann

August 3, 2022

Contents

1 Introduction

2 Ordinary isogeny graphs

2.1 Imaginary quadratic orders

For this part, let $\mathcal{O}$ be an order in an imaginary quadratic number field K.

Lemma 2.1. *Let $\mathfrak{p} \leq \mathcal{O}_K$ be a prime with $\mathfrak{N}(\mathfrak{p}) \perp [\mathcal{O}_K : \mathcal{O}]$. Then $\mathfrak{p}$ has a set of generators in $\mathcal{O}$.*

Proof. Suppose $\mathfrak{p}$ is a prime over p, and let $\mathcal{O} = \mathbb{Z}[\phi]$. We use the decomposition law in Dedekind ring extensions. Since $\mathfrak{N}(\mathfrak{p}) \perp [\mathcal{O}_K : \mathcal{O}]$ are coprime, we can apply it with a generator ϕ of $\mathcal{O}$.

If $\mathrm{MiPo}(\phi) = f(X)g(X) \mod p$ splits, then have

$$p\mathcal{O}_K = (p, f(\phi))(p, g(\phi))$$

and so the prime ideals over p are $(p, f(\phi))$ and $(p, g(\phi))$. If $\mathrm{MiPo}(\phi) \mod p$ is irreducible, then have that $p\mathcal{O}_K$ is prime and thus the only prime ideal over p. Hence, all prime ideals over p (including $\mathfrak{p}$) have a set of generators in $\mathcal{O}$. □

Corollary 2.2. *Let $\mathfrak{a} \leq \mathcal{O}_K$ be an ideal with $\mathfrak{N}(\mathfrak{a}) \perp [\mathcal{O}_K : \mathcal{O}]$. Then $\mathfrak{a}$ has a set of generators in $\mathcal{O}$.*

Proposition 2.3. *Let $\mathfrak{p} \leq \mathcal{O}$ be a prime ideal with $\mathfrak{N}(\mathfrak{p}) \perp [\mathcal{O}_K : \mathcal{O}]$ and $\mathfrak{p}' = \mathfrak{p}\mathcal{O}_K$. Then $\mathcal{O}_\mathfrak{p} = (\mathcal{O}_K)_{\mathfrak{p}'}$.*

Proof. We have $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\mathcal{O} = \mathbb{Z}[f\alpha]$ where $f = [\mathcal{O}_K : \mathcal{O}]$. Thus $f \notin \mathfrak{p}$ and so $f \in \mathcal{O}_\mathfrak{p}^*$. Therefore $\mathcal{O}_K \subseteq \mathcal{O}_\mathfrak{p}$ and thus $(\mathcal{O}_K)_{\mathfrak{p}'} \subseteq \mathcal{O}_\mathfrak{p}$. □

Proposition 2.4. *Let $\mathfrak{I}(\mathcal{O})$ resp. $\mathfrak{I}(\mathcal{O}_K)$ denote the set of invertible ideals of norm $\perp [\mathcal{O}_K : \mathcal{O}]$. Then*

$$\mathfrak{I}(\mathcal{O}) \to \mathfrak{I}(\mathcal{O}_K), \quad \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$$

is a monoid isomorphism with inverse

$$\mathfrak{I}(\mathcal{O}_K) \to \mathfrak{I}(\mathcal{O}), \quad \mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$$

Proof. Clearly, this is a well-defined monoid homomorphism. Hence, we have to show that it is bijective.

By Corollary 2.2, we know that any $\mathfrak{a} \leq \mathcal{O}_K$ with $\mathfrak{N}(\mathfrak{a}) \perp [\mathcal{O}_K : \mathcal{O}]$ has generators in $\mathcal{O}$, thus $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{a}$. This shows that $\mathfrak{a} \cap \mathcal{O}$ is a preimage of $\mathfrak{a}$, and so the map is surjective.

Assume now $\mathfrak{a}, \mathfrak{b} \leq \mathcal{O}$ with $\mathfrak{a}\mathcal{O}_K = \mathfrak{b}\mathcal{O}_K$ and $\mathfrak{N}(\mathfrak{a}), \mathfrak{N}(\mathfrak{b}) \perp [\mathcal{O}_K : \mathcal{O}]$. We show that $\mathfrak{a}_\mathfrak{p} = \mathfrak{b}_\mathfrak{p}$ for all primes $\mathfrak{p} \leq \mathcal{O}$. Note that if $\mathfrak{N}(\mathfrak{p}) \not\perp [\mathcal{O}_K : \mathcal{O}]$, this holds trivially, as $\mathfrak{a}_\mathfrak{p} = \mathcal{O}_\mathfrak{p} = \mathfrak{b}_\mathfrak{p}$. Otherwise, note that

$$\mathfrak{a}_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathfrak{a}(\mathcal{O}_K)_\mathfrak{p} = \mathfrak{a}\mathcal{O}_K(\mathcal{O}_K)_\mathfrak{p} = \mathfrak{b}\mathcal{O}_K(\mathcal{O}_K)_\mathfrak{p} = \mathfrak{b}_\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p} = \mathfrak{b}_\mathfrak{p}$$

as $\mathcal{O}_\mathfrak{p} = (\mathcal{O}_K)_\mathfrak{p}$. This shows that $\mathfrak{a}_\mathfrak{p} = \mathfrak{b}_\mathfrak{p}$ at all primes, so $\mathfrak{a} = \mathfrak{b}$ and our map is injective. Furthermore, since $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{a}$, we see that it has the inverse

$$\mathfrak{I}(\mathcal{O}_K) \to \mathfrak{I}(\mathcal{O}), \quad \mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$$

which must then be well-defined. □

2.2 The class group action

The class group action that we will define in the following is the most important tool when working with isogeny graphs of ordinary curves. Because of this, it is mentioned in more or less all the literature dealing with the topic. For me, it was thus quite surprising that I could nowhere find a precise and relatively elementary proof for the statement in the case of finite fields.

Most sources cite [Wat69, Thm 4.5], however the statement there is not as explicit as one might wish, and the proof is done in the much more general theory of abelian schemes. Apart from that, there are many references to the corresponding statement for curves over $\mathbb{C}$, but these ignore some of the subtleties introduced by non-separable isogenies. Therefore, we now present a relatively simple proof of the class group action for ordinary curves defined over a finite field and explicitly handle the non-separable case.

Definition 2.5. For an integral ideal $\mathfrak{a} \leq \mathrm{End}(E)$ of an ordinary Elliptic Curve E, define the $\mathfrak{a}$-torsion

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

From now on, we will often compare endomorphism rings of isogeneous curves. To do so, we embed those rings into an imaginary quadratic number field K. However, the field K and its orders can have nontrivial automorphisms, which means the embedding $\mathrm{End}(E) \to K$ cannot be unique. Fortunately, there is a unique embedding that is canonical in the following sense.

Lemma 2.6. *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 $\Phi = \Psi$.

If we set $K = \mathrm{End}(E) \otimes \mathbb{Q}$, then of course this gives a canonical embedding $\mathrm{End}(E') \to K$ for each curve E' isogeneous to E. From now on, whenever we consider such an embedding, or identify isomorphic endomorphism rings of isogeneous curves, this embedding shall be used.

Proposition 2.7. *Let $\phi : E \to E'$ be an isogeny of prime degree p between (not necessarily ordinary) Elliptic Curves. 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.

Furthermore, we will sometimes talk about horizontal or vertical isogenies *at a prime l*, which is defined by the next proposition. The advantage is that this is defined for all isogenies, not just those of prime degree.

Proposition 2.8. *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.

Now we can make a step towards the class group action and present how we assign isogenies to (integral, invertible) ideals of the endomorphism ring.

Definition 2.9. For an ordinary Elliptic Curve E and an integral, invertible ideal [1] $\mathfrak{a} = \mathfrak{b}(p, \pi_E)^r \leq \mathrm{End}(E)$ 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.

In order to define a group action later, we need to be able to chain such isogenies given by ideals. The obvious difficulty here is that the ideals are all in the same ring, but subsequent isogenies will have different curves as domain. Hence, we need to be able to view an ideal $\mathfrak{a} \leq \mathrm{End}(E)$ as an ideal of another endomorphism ring $\mathrm{End}(E')$. As it turns out, the endomorphism rings we consider are all isomorphic, and so this works out nicely.

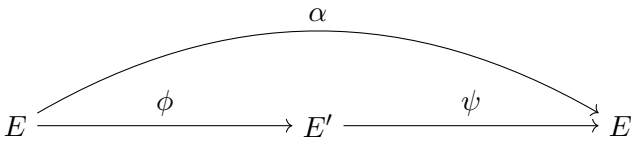
Lemma 2.10. *Let* E *be an ordinary Elliptic Curve and* $\mathfrak{a} \leq \mathrm{End}(E)$ *an integral, invertible ideal. Then* $\mathrm{End}(E) \cong \mathrm{End}(E_{\mathfrak{a}})$. *In particular,* $\phi_{E,\mathfrak{a}}$ *is horizontal at every prime* l.

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 separable isogeny $\phi := \phi_{E,\mathfrak{b}}$ 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



[1] By Prop. 2.4, this representation of an ideal $\mathfrak{a}$ is well-defined and unique, as $\mathfrak{N}((p, \pi)) = p \nmid [\mathcal{O}_{\mathrm{End}(E)\otimes\mathbb{Q}} : \mathrm{End}(E)] \mid d(\mathrm{End}(E))$.

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). □

Next, we prove that ideal multiplication is compatible with chaining of isogenies. Note that the condition $p \nmid [\mathcal{O}_K : \mathcal{O}]$ is just equivalent to all curves E with $\mathrm{End}(E) \cong \mathcal{O}$ being ordinary.

Lemma 2.11. *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

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

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 p^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 $\ker(\phi_{E_\mathfrak{a},\mathfrak{b}} \circ \phi_{E,\mathfrak{a}}) = E[\mathfrak{ab}]$. For simplicity of notation, write $\phi = \phi_{E,\mathfrak{a}}$ and $\psi = \phi_{E_\mathfrak{a},\mathfrak{b}}$. Hence, we want to show that $\ker(\psi \circ \phi) = E[\mathfrak{ab}]$.

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

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

The equality at $(*)$ holds, since

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

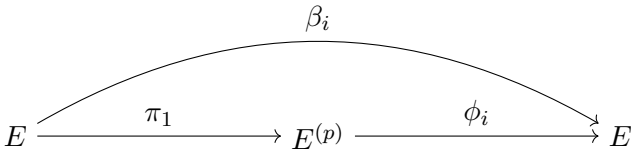
The whole reason why the ideal (p, π) plays such a special role is that it consists of exactly the inseparable endomorphisms.

Lemma 2.12. *Let E be an ordinary curve and $\alpha \in \mathrm{End}(E)$. Then α inseparable if and only if $\alpha \in (p, \pi)$.*

Proof. First, consider

$$\mathfrak{b} := \{\beta \in \mathrm{End}(E) \mid \beta \text{ inseparable}\}$$

This is an ideal, as for two inseparable $\beta_1, \beta_2 \in \mathrm{End}(E)$ have that they factor as



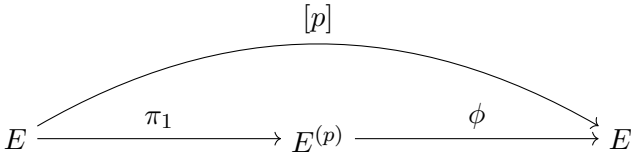
with the p-th power Frobenius π_1. Now $\beta_1 + \beta_2 = (\phi_1 + \phi_2) \circ \pi_1$ is inseparable, and clearly $\beta\gamma$ is inseparable for $\beta \in \mathfrak{b}$ and $\gamma \in \mathrm{End}(E)$ (just compare separability degrees).

Furthermore, p and π are inseparable, so $(p, \pi) \subseteq \mathfrak{b}$. Note that in the imaginary quadratic order $\mathrm{End}(E)$, every prime ideal is maximal. Since $\mathfrak{N}((p, \pi)) = p \perp d(\mathrm{End}(E))$, Prop. 2.4 shows that (p, π) is prime, and thus $(p, \pi) = \mathfrak{b}$ (clearly, $\mathfrak{b} \neq \mathrm{End}(E)$). $\square$

Lemma 2.13. *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.*

Proof. First, we show the direction $\Leftarrow$. By assumption, there are $\alpha, \beta \in \mathcal{O}$ such that $\alpha\mathfrak{a} = \beta\mathfrak{b}$. Thus $E_{\alpha\mathfrak{a}} = E_{\beta\mathfrak{b}}$ and it suffices to show that for any Elliptic Curve E and $\alpha \in \mathrm{End}(E)$, have $E_{(\alpha)} \cong E$.

Write $(\alpha) = (p, \pi)^r\mathfrak{a}$ and assume that E is defined over $\mathbb{F}_{p^s}$. Then $(\alpha)(p)^{\lceil r/s \rceil s - r} = (\pi)^{\lceil r/s \rceil}(\alpha')$ since $(p) = (p, \pi)(p, \pi - t)$ and $(p, \pi)^s = (\pi)$ by an easy computation. Furthermore, $\alpha' \notin (p, \pi)$. Now note that for any curve E, have $E_{(\pi)} = E^{(p^s)} \cong E$ and $E_{(p)} \cong E$, where the latter holds, since in the ordinary case, p factors as

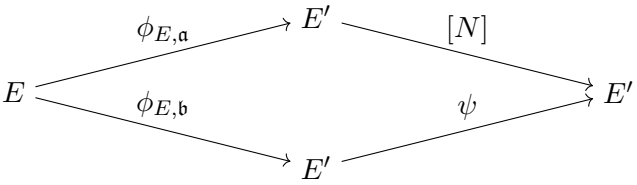


with the p-th power Frobenius π_1 and ϕ is separable with $\ker(\phi) = E[p] = \ker([p]) \cap \ker(\pi - t)$. Thus we see that $E_{(\alpha)} \cong E_{(\alpha')}$ and can assume wlog that $\alpha = \alpha' \notin (p, \pi)$.

By Lemma 2.12, we now see that α is separable, and so clearly $\ker(\alpha) = E[(\alpha)]$. Since $\alpha : E \to E$ is the separable isogeny on E with kernel $E[(\alpha)]$, we see that $E_{(\alpha)} = E/E[(\alpha)] \cong E$.

Now we consider the other direction $\Rightarrow$. Again, write $\mathfrak{a} = \tilde{\mathfrak{a}}(p, \pi)^r$ and assume that E is defined over $\mathbb{F}_{p^s}$. Then we have as before that $\mathfrak{a}(p)^{\lceil r/s \rceil s - r} = (\pi)^{\lceil r/s \rceil}\mathfrak{a}'$ for the ideal $\mathfrak{a}' = \tilde{\mathfrak{a}}(p, \pi - t)^{\lceil r/s \rceil s - r}$. Now clearly $[\mathfrak{a}] = [\mathfrak{a}']$ are in the same ideal class and $\mathfrak{a}' \perp (p, \pi)$. Furthermore, by the direction $\Leftarrow$, have $E_\mathfrak{a} \cong E_{\mathfrak{a}'}$. Doing the same with $\mathfrak{b}$, we can assume wlog that $\mathfrak{a} = \mathfrak{a}'$ and $\mathfrak{b} = \mathfrak{b}'$ are ideals coprime to (p, π).

Therefore, the isogenies $\phi_{E,\mathfrak{a}}$ and $\phi_{E,\mathfrak{b}}$ are separable. Write $E' := E_\mathfrak{a} = E_\mathfrak{b}$. Choose $N > 0$ such that $[N]^{-1}(E[\mathfrak{a}]) \supseteq E[\mathfrak{b}]$. Now the isogeny $[N] \circ \phi_{E,\mathfrak{a}}$ factors through $\phi_{E,\mathfrak{b}}$, i.e. we get a commutative diagram



for some endomorphism $\psi : E' \to E'$. Clearly the isogenies $[N]$ and ψ are given by the ideals (N) resp. (ψ), and so we find

$$(N)\mathfrak{a} = (\psi)\mathfrak{b}$$

and the claim follows. □

Now we have proven almost everything we need. The final ingredient, from which it will then follow that the class group action is transitive, is a theorem of Tate. Since it

uses much of the theory on general abelian varieties, we will present it without proof here. For a proof, the reader is referred to the work of Tate [Tat66].

Theorem 2.14 (Isogeny theorem)**.** *Let E, E' be Elliptic Curves defined over $\mathbb{F}_q$. Then there is a separable isogeny $E \to E'$ if and only if $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.*

Note that this condition is also equivalent to $\mathrm{End}(E) \otimes \mathbb{Q} \cong \mathrm{End}(E') \otimes \mathbb{Q}$ or that the q-th power Frobenius endomorphisms have the same trace.

Theorem 2.15. *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 $[\mathfrak{a}]$.

Proof. Well-definedness and freeness follow from all the previous lemmas. So it is left to derive the transitivity from Thm 2.14. Let E and E' be curves in $\mathrm{Ell}(\mathcal{O})$. Clearly, we then have $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ and so there is a separable isogeny $\phi : E \to E'$. Everything we have to show is that $\phi = \phi_{E,\mathfrak{a}}$ for some ideal $\mathfrak{a} \leq \mathcal{O}$.

□

A similar class group action exists in many other cases, since it is really founded in the theory of abelian varieties, see [Wat69]. Notable examples are the CSIDH class group action for supersingular curves defined over $\mathbb{F}_p$ (see [Cas+18]), its generalization to so-called oriented curves (see [CK20]), and the very classical class group action of Elliptic Curves with complex multiplication (over $\mathbb{C}$). More concretely, if we consider an order $\mathcal{O}$ in a quadratic imaginary number field and write $\mathrm{Ell}(\mathcal{O})$ for the set of (isomorphism classes of) curves over $\mathbb{C}$ with endomorphism ring $\mathcal{O}$ (these are said to have *complex multiplication*), then there is a free and transitive class group action

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

where we choose $\mathfrak{a}$ to be an integral ideal representative of $[\mathfrak{a}]$. Note that for ideals $\mathfrak{a} \perp (p, \pi)$, this is analogous to our action defined above. However, since the Frobenius has trivial kernel, one needs some addition in the finite field case.

Note that one can still keep the simpler definition

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

also in the finite field case, if we require $\mathfrak{a}$ to be an (integral) ideal representative of $[\mathfrak{a}]$ that is coprime to (p, π). Clearly, every ideal class has such a representative, since we can multiply with the principal ideal $(p) = (p, \pi)(p, \pi - t)$ and divide out the principal ideal $(\pi) = (p, \pi)^s$. However, some sources do not explicitly mention that $\mathfrak{a}$ must be chosen coprime to (p, π), which caused me some confusion.

2.3 Vulcanoes

Once we have the class group action, we can derive a lot of information about the structure of the ordinary part of an isogeny graph.

Definition 2.16. Denote by $\Gamma_l(\mathbb{F}_q)$ the graph whose vertices are isomorphism classes of Elliptic Curves over $\mathbb{F}_q$, and the edges are the degree l isogenies between them (with multiplicity).

Since there is never an isogeny between ordinary and supersingular curves, we will continue to talk of ordinary and supersingular connected components of $\Gamma_l(\mathbb{F}_q)$. Note that by the j-invariant, an isomorphism class of an Elliptic Curve E is in 1-to-1 correspondence with the j-invariant $j(E)$, and so we could also say that the vertices of $\Gamma_l(\mathbb{F}_q)$ are just the elements of $\mathbb{F}_q$. Furthermore that the existence of the dual isogeny implies that $\Gamma_l(\mathbb{F}_q)$ is undirected.

Definition 2.17. For $l > 0, d \geq 0$, a graph G is called *l-vulcano of depth d*, if its vertices can be partitioned into a set C (the "crater") and a set L (the "lava flows") such that

- $G[C]$ is either a single vertex (possibly with one or two loops), two connected vertices or a cycle
- $G[V]$ is a forest of complete l-ary trees with depth d
- Every vertex $v \in C$ is connected to the roots of $l + 1 - \deg_{G[C]}(v)$ trees in $G[V]$

In particular, every vertex in G except the leaves of the trees has degree $l + 1$.

The term "vulcano" was introduced by [FM02], after Kohel had mostly determined the structure of ordinary connected components in his PhD thesis. Most of this follows from the above class group action, and for the remaining details we refer the reader to Kohel's thesis [Koh96, Prop. 23].

Theorem 2.18. *Let G be a connected component of $\Gamma_l(\mathbb{F}_q)$. Suppose that G is ordinary, i.e. its vertices are (isomorphism classes of) ordinary curves. Then G is an l-vulcano. Further, we have*

- *All curves on the crater have the same endomorphism ring $\mathcal{O}$ with $l \nmid [\mathcal{O}_{\mathcal{O}\otimes\mathbb{Q}} : \mathcal{O}]$.*
- *All curves on the i-th tree level of a lava flow have the endomorphism ring $\mathbb{Z}+l^i\mathcal{O}$.*
- *The size of the crater is the order of $\mathfrak{l}_1$ in $\mathrm{Cl}(\mathcal{O})$, where $(l) = \mathfrak{l}_1\mathfrak{l}_2$ in $\mathcal{O}$, or 1 if l is inert in $\mathcal{O}$.*

3 Supersingular isogeny graphs

After studying the ordinary connected components of the l-isogeny graph $\Gamma_l(\mathbb{F}_q)$, we now come to the supersingular component(s). First, note that all supersingular j-invariants are defined over $\mathbb{F}_{p^2}$, and so we will assume $q = p^2$ for this section.

In the supersingular setting, the endomorphism ring is now non-commutative. There still exists a non-commutative analogue of the class group action, but using that structure is significantly harder. Mainly, because the theory of quaternion algebras is more complicated, and its class group structure is less studied.

Instead, there is the famous result of Pizer, which states that supersingular isogeny graphs (i.e. the supersingular part of $\Gamma_l(\mathbb{F}_q)$) are so called Ramajuan graphs, that is have excellent expander properties. We will introduce this result in this section, but without proof.

Definition 3.1. A d-regular graph G is called ϵ-expander, if the eigenvalues $\lambda_1 > ... > \lambda_n$ of its adjacency matrix satisfy

$$|\lambda_2|, |\lambda_n| \leq (1 - \epsilon)d$$

In the literature, expander graphs are often defined by the use of the expansion ration

$$h(G) := \min_{S \subseteq V,\ \#S \leq \frac{n}{2}} \frac{\#\partial S}{\#S}$$

of a graph $G = (V, E)$. Here ∂S is the edge boundary, i.e. the set of edges between a point in S and a point in $V \setminus S$.

The connection between those two definitions is then given by the Cheeger-inequality

Proposition 3.2. *Let G be a d-regular graph such that its adjacency matrix has eigenvalues $\lambda_1 > ... > \lambda_n$. Then*

$$\frac{d - \lambda_2}{2} \leq h(G) \leq \sqrt{2d(d - \lambda_2)}$$

Proof. See e.g. [Che69]. □

This inequality only correlates the so-called spectral gap $d - \lambda_2$ with $h(G)$, and does not bound $|\lambda_2|$. In many cases, bounds on the spectral gap or expansion ration already suffice to show properties of expanders. Because of this, expanders are usually defined as graphs for which λ_2 or $h(G)$ are bounded. Our definition 3.1 is then sometimes called "two-sided expander". However, we will never use one-sided expanders in this work, hence the above definition shall be sufficient.

The nice thing about the expansion ratio is, that it gives more intuition on what the expander property means. In particular, an expander graph is densely connected, i.e. by deleting a small number of edges, it is impossible to make the graph split into two (or more) connected components of relatively large size.

Definition 3.3. A connected d-regular graph is called Ramajuan, if

$$|\lambda_2|, |\lambda_n| \leq 2\sqrt{d-1}$$

where $\lambda_1 > ... > \lambda_n$ are again the eigenvalues of the adjacency matrix.

It is known that the bound $2\sqrt{d-1}$ is asymptotically optimal, i.e. for sufficiently large n, all d-regular graphs of n vertices have $\lambda_2 \geq 2\sqrt{d-1} - \epsilon$. In that sense, we can say Ramajuan graphs are graphs with asymptotically optimal expansion properties.

One of the main properties of expander graphs is random walks on them mix rapidly. That is, the final vertex of relatively short random walks is distributed almost uniformly among all vertices.

Theorem 3.4. *Let $G = (V, E)$ be a d-regular ϵ-expander graph and $v \in V$ a vertex. Then the distribution of the final vertex of a random walk starting from v of length t is close to uniform, in particular, the ℓ_2-statistical distance is bounded by $(1-\epsilon)^t$.*

For a proof of this theorem, see e.g. Thm 3.3 in this excellent survey on expander graphs [HL06]. Note that expander graphs used in cryptography are usually of exponential size, so this theorem says that a random walk of polynomial length already reaches all vertices of the graph.

Now we come to the anticipated result, that supersingular isogeny graphs are expander graphs.

Definition 3.5. The *supersingular l-isogeny graph over $\mathbb{F}_{p^2}$* is the subgraph of $\Gamma_l(\mathbb{F}_{p^2})$ induced by all (isomorphism classes of) supersingular curves over $\mathbb{F}_{p^2}$.

Since the supersingular l-isogeny graph is disconnected from the rest of $\Gamma_l(\mathbb{F}_{p^2})$, we see that it is an $(l+1)$-regular graph. We also know its size exactly, which directly follows from a classical result on the number of supersingular curves over $\mathbb{F}_{p^2}$.

Proposition 3.6. *For $p \geq 5$, there are exactly*

$$\left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \mod 12 \\ 1 & \text{if } p \equiv 5, 7 \mod 12 \\ 2 & \text{if } p \equiv 11 \mod 12 \end{cases}$$

supersingular Elliptic Curves over $\mathbb{F}_{p^2}$.

For a proof of this statement, see e.g. [Sil09, Thm V.4.1].

In [Piz90], Pizer has now shown that

Theorem 3.7. *The supersingular l-isogeny graph is Ramajuan.*

This shows that there is a huge difference between the ordinary and supersingular graphs. For example, there is always a path of length $O(\log(p))$ between two curves in the supersingular graph, but in the ordinary graph, such a path does not exist in many cases. We will try to quantify this in the last section. The idea of our research is to utilize these differences in order to find random, supersingular curves.

4 Generating supersingular curves

References

[Cas+18] Wouter Castryck et al. *CSIDH: An Efficient Post-Quantum Commutative Group Action*. Cryptology ePrint Archive, Paper 2018/383. 2018. URL: https://eprint.iacr.org/2018/383.

[Che69] Jeff Cheeger. "A lower bound for the smallest eigenvalue of the Laplacian". English (US). In: *Proceedings of the Princeton conference in honor of Professor S. Bochner*. 1969, pp. 195–199.

[CK20] Leonardo Colò and David Kohel. *Orienting supersingular isogeny graphs*. Cryptology ePrint Archive, Paper 2020/985. https://eprint.iacr.org/2020/985. 2020. URL: https://eprint.iacr.org/2020/985.

[FM02] Mireille Fouquet and François Morain. "Isogeny Volcanoes and the SEA Algorithm". In: *Algorithmic Number Theory*. Ed. by Claus Fieker and David R. Kohel. Springer Berlin Heidelberg, 2002, pp. 276–291.

[HL06] Shlomo Hoory and Nathan Linial. "Expander Graphs and their Applications". In: *Bulletin of the American Mathematical Society* 43 (2006), pp. 439–561.

[Koh96] David Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. 1996.

[Piz90] Arnold Pizer. "Ramanujan graphs and Hecke operators". In: *Bulletin of the American Mathematical Society* 23 (1990), pp. 127–137.

[Sil09] Joseph Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.

[Tat66] J. Tate. "Endomorphisms of Abelian Varieties over Finite Fields." In: *Inventiones mathematicae* 2 (1966), pp. 134–144. URL: http://eudml.org/doc/141848.

[Wat69] William C. Waterhouse. "Abelian varieties over finite fields". In: *Annales scientifiques de l'École Normale Supérieure* Ser. 4, 2.4 (1969), pp. 521–560.