SUPERSINGULAR ISOGENY GRAPHS FROM ALGEBRAIC MODULAR CURVES

NADIR HAJOUJI

1. Introduction

We are interested in the problem of computing examples of supersingular isogeny graphs.

There are already algorithms for computing these graphs that work for all p, ℓ - for example, the algorithm we will describe for $\ell = 2, 3$ is essentially an optimized version of the algorithm described in [2]. Most existing algorithms essentially compute the graph by starting at a vertex, and computing all edges out of that vertex to find new vertices, and repeating the process until all vertices have been obtained, e.g. [2, 5]. This means one has to do the following:

- Find models of supersingular curves.
- Find generators of the torsion subgroup.
- Compute isogenies using Velu's formula.

We will describe an algorithm that essentially allows us to avoid having to do most of these things. Our approach is similar to the algorithm described in section 3.2 of [9]: we compute the isogeny graph by finding all points on modular curves $X_1(\ell)$ that represent supersingular curves.

The advantage of this strategy is that after one has done some work to obtain models of the modular curves $X_1(\ell)$, the process then boils down to evaluating certain polynomials at points on the modular curve until we have all of the information we need. We obtain these formulas for $\ell = 5, 7, 11, 13$ in (ADD REF).

To obtain the graph from these formulas, we also need:

- The set of supersingular j-invariants.
- A field $\mathbb{F}_q$ where we have models of elliptic curves with full ℓ-torsion for every supersingular j-invariant.

In section (), we prove that for every supersingular j-invariant in $\mathbb{F}_{p^2}$, there is a model $E/\mathbb{F}_{p^{2n}}$ with ℓ-torsion in $\mathbb{F}_{p^{2n}}$, where n is the least common multiple of 2 and the order of p in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. This addresses the second point.

In section (), we explain how to obtain the full set of supersingular j-invariants, provided we can find a single supersingular j-invariant $j_0 \in \mathbb{F}_{p^2}$ (or ideally, $j_0 \in \mathbb{F}_p$.) So, all we need to get started is a method for obtaining a single supersingular j-invariant.

To obtain j_0, we need to find a root ofa suitable Hilbert polynomial. In section (), we explain how to obtain the Hilbert polynomials we need using the models of $X_1(\ell)$ we found in ().

Finally, in section() we put it all together, and describe a self-contained algorithm that can be used to compute supersingular elliptic curves that can be run in Python, with no additional packages.

2. Supersingular Elliptic Curves

2.1. **Quadratic Twists.** Let $\mathbb{F}_q$ be a field of characteristic not equal to 2 or 3, let $d \in \mathbb{F}_q^\times$ be a nonsquare and let $E/\mathbb{F}_q$ be an elliptic curve given by a short Weierstrass equation:

$$E: \quad y^2 = x^3 + fx + g$$

We define the quadratic twist of $E/\mathbb{F}_q$ to be the elliptic curve:

$$(E_{\mathbb{F}_q})^{-1}: \quad dy^2 = x^3 + fx + g$$

We will drop the subscript if the field is clear from context. Note that $E^{-1}_{\mathbb{F}_{q^d}}$ is *not* isomorphic to the base change of $E^{-1}_{\mathbb{F}_q}$ if d is even, so the subscript *is* necessary at times. Note that the choice of nonsquare d in $\mathbb{F}_q$ is not important: replacing d by any other nonsquare d' in the defining equation for E^{-1} does not change the isomorphism type.[1]

Now, $E(\mathbb{F}_q), E^{-1}(\mathbb{F}_q)$ can both be "realized" as subgroups of $E(\mathbb{F}_{q^2})$. It's clear that $E(\mathbb{F}_q)$ is isomorphic to a subgroup of $E(\mathbb{F}_{q^2})$; to realize $E^{-1}(\mathbb{F}_q)$ as a subgroup of $E(\mathbb{F}_q)$, we simply observe that it coincides with the kernel of the trace map $E(\mathbb{F}_{q^2}) \to E(\mathbb{F}_q)$.

- $P \in E(\mathbb{F}_{q^2})$ is in the kernel of the trace map if and only if $\sigma(P) = -P$.
- On an elliptic curve given by a short Weierstrass equation, $\sigma(P) = -P$ is equivalent to $\sigma(x(P)) = x(P)$ and $\sigma(y(P)) = -y(P)$.
- Thus, P is in the kernel of the trace map if and only if $x(P) \in \mathbb{F}_q$, and either $y(P) = 0$ or $y(P)$ is an eigenvector of σ, i.e. $y(P) = \sqrt{d}$ for some nonsquare $d \in \mathbb{F}_q$.
- In all cases, P has the form $(x, \sqrt{d}y)$ so:

$$dy^2 = x^3 + fx + g$$

[1] On the other hand, if we replace d by c^2 for some nonzero $c \in \mathbb{F}_q$, we obtain a curve which is isomorphic to the original curve E.

so (x, y) is a point on $E^{-1}(\mathbb{F}_q)$. Conversely, given a point (x, y) on $E^{-1}(\mathbb{F}_q)$, $(x, \sqrt{d}y)$ is a point in the kernel of the trace map.

Viewing both $E(\mathbb{F}_q), E^{-1}(\mathbb{F}_q)$ as subgroups of $E(\mathbb{F}_{q^2})$ allows us to talk about their union and intersection:

- The intersection $E(\mathbb{F}_q) \cap E^{-1}(\mathbb{F}_q)$ coincides with the 2-torsion subgroup of E (over $\mathbb{F}_q$).
- The union of $E(\mathbb{F}_q) \cup E^{-1}(\mathbb{F}_q)$ coincides with the set of points $P \in E(\mathbb{F}_{q^2})$ that satisfy $x(P) \in \mathbb{F}_q$.

Now, for every $x \in \mathbb{F}_q$, exactly one of the following is true:

- $x^3 + fx + g = 0$. In this case, there is a 2-torsion point $(x, 0)$ on both E and E^{-1}.
- $x^3 + fx + g$ is a nonzero square in $\mathbb{F}_q$. In this case, we have two points on E with $x(P) = x$ and no points on E^{-1} with $x(P) = x$.
- $x^3 + fx + g$ is a nonzero square in $\mathbb{F}_q$. In this case, we have no points on E with $x(P) = x$ and 2 points on E^{-1} with $x(P) = x$.

Furthermore, every nonidentity point on $E(\mathbb{F}_q) \cup E^{-1}(\mathbb{F}_q)$ can be obtained in this way, so we deduce:

$$\#E(\mathbb{F}_q) + \#E^{-1}(\mathbb{F}_q) = 2q + 2$$

Writing $\tau(E, \mathbb{F}_q)$ to denote the trace of Frobenius, we can reformulate this result as:

$$\tau(E^{-1}, \mathbb{F}_q) = -\tau(E, \mathbb{F}_q)$$

2.2. **Frobenius.** Let $p > 3$ be a prime, let $E/\mathbb{F}_p$ a supersingular elliptic curve, and

Proposition 2.1. *Let $p > 3$ be a prime, let $E/\mathbb{F}_p$ be a supersingular elliptic curve, and let ℓ be a prime factor of $p^2 - 1 = (p-1)(p+1)$.*

- *If $\ell | p + 1$, then $E[\ell] \subset E(\mathbb{F}_{p^2})$.*
- *If $\ell | p - 1$, then $(E^{-1}_{\mathbb{F}_{p^2}}[\ell]) \subset E^{-1}_{\mathbb{F}_{p^2}}(\mathbb{F}_{p^2})$.*

In particular:

- *If $\ell = 2$, then $E, E^{-1}_{\mathbb{F}_{p^2}}$ have full 2-torsion in $\mathbb{F}_{p^2}$.*
- *For $\ell = 3$, exactly one of $E, E^{-1}_{\mathbb{F}_{p^2}}$ has full 3-torsion in $\mathbb{F}_{p^2}$, and the other does not*[2].

Proof. First, note that for an elliptic curve $E/\mathbb{F}_p$, E is supersingular if and only if $\tau(E, \mathbb{F}_p) = 0$. Thus, the characteristic polynomial of the $p$the power Frobenius map on E is:

$$x^2 + p$$

[2] If $p \equiv 1 \mod 3$, then E^{-1} contains the 3-torsion subgroup; otherwise E contains the 3-torsion subgroup.

so we deduce $\phi^2 = [-p]$.

Now, let $\phi_2 : E_{\mathbb{F}_{p^2}} \to E_{\mathbb{F}_{p^2}}$ the p^2-power Frobenius. Then $\phi_2 = \phi^2 = [-p]$ on $E_{\mathbb{F}_{p^2}}$. If $\ell | p+1$, then $p \equiv -1 \pmod{\ell}$, so $-p \equiv 1 \pmod{\ell}$. Thus, ϕ_2 acts as multiplication-by-1 on $E[\ell]$ - i.e. the ℓ-torsion points are fixed by ϕ_2, so they are defined over $\mathbb{F}_{p^2}$. This proves the first point.

To prove the second point, we will show that $\phi_2^{-1} = [p]$, where $\phi_2^{-1} : E_{\mathbb{F}_{p^2}} \to E_{\mathbb{F}_{p^2}}$ is the p^2-power Frobenius on the quadratic twist of E. Since we know the characteristic polynomial of ϕ_2 is $(x+p)^2$, and we know that $\tau(E^{-1}_{\mathbb{F}_p^2}, \mathbb{F}_{p^2}) = -\tau(E, \mathbb{F}_{p^2})$, it follows that the characteristic polynomial $E^{-1}_{\mathbb{F}_{p^2}}$ must be:

$$(x-p)^2$$

Furthermore, we know that $E, E^{-1}_{\mathbb{F}_{p^2}}$ are isomorphic over $\mathbb{F}_{p^4}$, so $(\phi_2^{-1})^2 = [p^2]$. Altogether, this means:

- ϕ_2^{-1} has a repeated eigenvalue of p.
- $(\phi_2^{-1})^2$ is diagonalizable, so ϕ_2 must be diagonalizable.

Thus, ϕ_2^{-1} is multiplication by $[p]$ as claimed, so for any prime factor ℓ of $p-1$, we have $p \equiv 1 \pmod{\ell}$, so ϕ_2^{-1} acts as the identity on the ℓ-torsion subgroup.

Finally, note that $2 | p \pm 1$ and 3 divides exactly one of $p \pm 1$, for all $p > 3$, which proves the last point. □

Next, we extend the result we just proved for supersingular curves $E/\mathbb{F}_p$ to include supersingular elliptic curves with $j(E) \notin \mathbb{F}_p$.

Proposition 2.2. *Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve and assume $j(E) \notin \mathbb{F}_p$.*

1. *$\tau(E, \mathbb{F}_{p^2}) \in \{-2p, 2p\}$.*
2. *E has at least one point of order 2 in $\mathbb{F}_{p^2}$, and necessarily has full 2-torsion in $\mathbb{F}_{p^4}$.*
3. *Exactly one of E, E^{-1} has a point of order 3 defined over $\mathbb{F}_{p^2}$. Furthermore, the model of E with a point of order 3 necessarily has all points of order 3 in $\mathbb{F}_{p^6}$.*

Proof. For a proof of (1), see [10] or [6].

Now, (1) implies that the characteristic polynomial of Frobenius is $(x \pm p)^2$. This means that the action of Frobenius on $E[\ell]$ can be represented by a matrix of the form $\pm \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}$, or $\pm \begin{pmatrix} p & 1 \\ 0 & p \end{pmatrix}$.

When $\ell = 2$, the matrix is either congruent to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (mod 2) or it is congruent to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (mod 2). In the first case, Frobenius acts trivially on the 2-torsion subgroup, so $E[2] \subset E(\mathbb{F}_{p^2}) \subset E(\mathbb{F}_{p^4})$, proving the first point. Otherwise, Frobenius acts as $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, so we have a 2-torsion point defined over $\mathbb{F}_{p^2}$ (because we have an eigenvector with eigenvalue 1), and since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has order 2 in $GL_2(\mathbb{F}_2)$, the other two torsion points are defined over $\mathbb{F}_{p^4}$.

For $\ell = 3$, we have the following possibilities:

- If Frobenius acts as the identity on $E[3]$, then we have full 3-torsion defined over $\mathbb{F}_{p^2}$. Note that Frobenius acts as either $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ on $E^{-1}[3]$, so E^{-1} has no points of order 3 in this case.
- If Frobenius acts as $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ on $E[3]$, then $E(\mathbb{F}_{p^2})$ contains a point of order 3 because $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has an eigenvector with eigenvalue 1. Furthermore, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has order 3 so we have full 3-torsion in $\mathbb{F}_{p^6}$.

□

Corollary 2.3. *Let $E_1, E_2/\mathbb{F}_{p^2}$ be supersingular elliptic curves, and assume $\tau(E_i) \in \{\pm 2p\}$ for $i = 1, 2$. Then $E_1(\mathbb{F}_{p^2})[2] \cong E_2(\mathbb{F}_{p^2})[2]$.*

Proof. Replacing E_i by E_i^{-1} if necessary, we may assume $E_i(\mathbb{F}_{p^2})$ contains a point of order 3. Note that this does not change the isomorphism type of the 2-torsion subgroup.

Now, we have models with full 3-torsion for every supersingular j-invariant over $\mathbb{F}_{p^6}$, and the 3-isogeny graph is connected, so there exists an isogeny $E_1 \to E_2$ of degree 3^r that is defined over $\mathbb{F}_{p^6}$. Since $2, 3^r$ are coprime, the isogeny $E_1 \to E_2$ induces an isomorphism $E_1[2](\mathbb{F}_{p^6}) \to E_2[2](\mathbb{F}_{p^6})$. But we know that both E_1, E_2 have full 2-torsion defined over $\mathbb{F}_{p^4}$, so $E_1[2], E_2[2]$ are isomorphic over $\mathbb{F}_{p^4} \cap \mathbb{F}_{p^6} = \mathbb{F}_{p^2}$.

□

Now, as long as we can find *one* supersingular elliptic curve over $\mathbb{F}_{p^2}$ that has full 2-torsion, it will follow that every supersingular curve over $\mathbb{F}_{p^2}$ has full 2-torsion in $\mathbb{F}_{p^2}$. Furthermore, we already know that supersingular elliptic curves that are defined over $\mathbb{F}_p$ have full 2-torsion in $\mathbb{F}_{p^2}$. Thus, we just need to show that there exists a supersingular elliptic curve over $\mathbb{F}_p$. This can be deduced from Prop 14.18 in [3]. In (), we give a list of algebraic integers that give rise to supersingular curves over $\mathbb{F}_p$ for all $p <$ (ADD MAX). See (ADD REF TO ALG) for an algorithm for $p >> 0$.

Corollary 2.4. *Let E_1, E_2 be supersingular elliptic curves over $\mathbb{F}_{p^2}$ and assume $\tau(E_1, \mathbb{F}_{p^2}) = \tau(E_2, \mathbb{F}_{p^2})$. Let ℓ be an odd integer. Then $E_1[\ell](\mathbb{F}_{p^2}) \cong E_2[\ell](\mathbb{F}_{p^2})$.*

Proof. We know that all of the models with $\tau \in \{\pm 2p\}$ have full 2-torsion in $\mathbb{F}_{p^2}$, so the 2-isogeny graph can be computed in $\mathbb{F}_{p^2}$. Thus, there exists an isogeny $E_1 \to E_2$ of degree 2^r over $\mathbb{F}_{p^2}$. This induces an isomorphism $E_1[\ell](\mathbb{F}_{p^2}) \to E_2[\ell](\mathbb{F}_{p^2})$ for all integers ℓ coprime to 2^r, i.e. all odd integers ℓ. □

Corollary 2.5. *For all prime factors ℓ of $p^2 - 1$, and every supersingular $j_1 \in \mathbb{F}_{p^2}$, there is an elliptic curve $E_1/\mathbb{F}_{p^2}$ with $j(E_1) = j_1$, and $E[\ell] \subset E(\mathbb{F}_{p^2})$.*

Proof. We know the result is true if $j_1 \in \mathbb{F}_p$. To prove the result for $j_1 \notin \mathbb{F}_p$, we use the fact that there exists a supersingular elliptic curve $E_0/\mathbb{F}_p$.

We know that E_0 (or $((E_0)_{\mathbb{F}_{p^2}})^{-1}$, when $\ell | p-1$) has full ℓ-torsion over $\mathbb{F}_{p^2}$. Now, choose an elliptic curve E_1 with $j(E_1) = j_1$ and $\tau(E_1, \mathbb{F}_{p^2}) = \tau(E_0, \mathbb{F}_{p^2})$ (resp. $\tau(E_1, \mathbb{F}_{p^2}) = -\tau(E_0, \mathbb{F}_{p^2})$ if $\ell | p-1$). Then:

$$E_1(\mathbb{F}_{p^2})[\ell] \cong E_0(\mathbb{F}_{p^2})[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z}) \times (\mathbb{Z}/\ell\mathbb{Z})$$

□

Corollary 2.6. *Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve with $j(E) \notin \mathbb{F}_p$. Let $\phi_2 : E \to E$ be the Frobenius map. Then ϕ_2 acts on E as $\pm[p]$.*

Proof. We know the characteristic polynomial of Frobenius is $(t \pm p)^2$. Let $\ell \neq p$ be a prime. Then Frobenius acts on $T_\ell(p)$ as $\begin{pmatrix} p & a \\ 0 & p \end{pmatrix}$. If $a \neq 0 \pmod{\ell}$, then the restriction of ϕ_2 to $E[\ell]$ has order divisible by ℓ, which contradicts the fact that $E[\ell]$ is fixed by $\phi_2^{\ell-1}$. Thus $a = 0 \pmod{\ell}$.

□

Now, if $p \neq \pm 1 \pmod{\ell}$, then supersingular curves over $\mathbb{F}_{p^2}$ do not contain *points* of order ℓ, but the *subgroups* of order ℓ will always be defined over $\mathbb{F}_{p^2}$: since Frobenius acts on supersingular elliptic curves as multiplication-by-$\pm \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}$, every cyclic subgroup of E order prime to p is fixed (as a set) by Frobenius. Thus, any isogeny $E \to E'$ between supersingular elliptic curves over $\mathbb{F}_{p^2}$ with cyclic kernel must be defined over $\mathbb{F}_{p^2}$.

3. Supersingular Isogeny Graphs for $\ell \geq 5$

We now turn our attention to isogeny graphs for $\ell > 3$. The algorithm we used in the previous section still works in principle (see [2]); however, even if we could find analogs of the "good models" we had in the $\ell = 2, 3$ cases, we would need to solve $\frac{p}{12}$ polynomials of degree $\ell > 3$. This is much more difficult without an analog of the quadratic/cubic formula.

However, when $\ell > 3$, we can use modular curves to avoid dealing with those issues. Instead of working our way through the graph vertex by vertex, we will do the following:

(1) Find the set of supersingular j-invariants, e.g. by computing the 2 or 3-isogeny graph.

(2) Find a set $X_\ell(\mathbb{F}_q)$ that contains (unique) representatives for each isogeny $E \to E'$ of degree ℓ between elliptic curves $E, E'/\mathbb{F}_q$, together with maps $j_\ell, j'_\ell : X_\ell(\mathbb{F}_q) \to \mathbb{F}_q$ such that $j_\ell(t)$ is the j-invariant of E and $j'_\ell(t) = E'$.

(3) For all $t \in X_\ell(\mathbb{F}_q)$:
   (a) Compute $j_\ell(t)$.
   (b) If $j_\ell(t)$ is in the list of supersingular j-invariants, compute $j'_\ell(t)$ and record that we have an edge $j_\ell(t) \to j'_\ell(t)$ on the supersingular isogeny graph.

One can take $X_\ell(\mathbb{F}_q) = X_0(\mathbb{F}_q)$, if one has an algebraic model of $X_0(\ell)$. However, we can work with a slightly smaller set: we will essentially be taking $X_\ell(\mathbb{F}_q)$ to be the image of $X_1(\ell)(\mathbb{F}_q)$ in $X_0(\ell)(\mathbb{F}_q)$.

To obtain models of $X_1(\ell)$, as well as the maps j_ℓ, j'_ℓ, and the automorphisms of $X_1(\ell) \to X_0(\ell)$, all we need is the "*universal elliptic curve with a point P of order* ≥ 4".[3] Explicitly, this is the family of elliptic curves over $\mathbb{A}^2 = \text{Spec } \mathbb{Z}[u, v]$ given by the equation:

$$\mathcal{E}_{u,v} : \quad y^2 + (1-u)xy - vy = x^3 - vx^2$$

Note that $(0, 0) \in \mathcal{E}_{u,v}(\mathbb{Z}[u, v])$ is a point of infinite order.

If E/K is any elliptic curve, and $P \in E(K)$ is a point of order ≥ 4, there is a unique point $(u_0, v_0) \in \mathbb{A}^2_K$ such that E is isomorphic to the fiber over (u_0, v_0) in $\mathcal{E}_{u,v} \times \text{Spec } K$, and in fact there is an isomorphism from E to the fiber that takes P to the point $(0, 0)$ on the fiber.

We will use $\mathcal{E}_{u,v} \to \mathbb{A}^2$ to obtain models of the modular curves $X_1(\ell)$, together with models for the universal elliptic curves with a point of order n. The process is straightforward and well-known: we compute multiples of the point $P_0 = (0, 0)$ using the group law on $\mathcal{E}$ and set suitable multiples equal to each other to obtain an algebraic relation between u, v that encodes the fact that $(0, 0)$ is a point of order ℓ. This algebraic relation can be interpreted

[3] See, e.g., Ex. 8.13 in [7].

as a model for a plane curve $C_\ell \subset \mathbb{A}^2$ which is birational to $X_1(\ell)$. We will find maps $X_1(\ell) \to C_\ell$ from smooth curves $X_1(\ell)$, and construct the universal curves with a point of order ℓ by pulling back the fibration $\mathcal{E}_{u,v} \to \mathbb{A}^2$ along the map $i_\ell : X_1(\ell) \to \mathbb{A}^2$.

Let $j_{\mathcal{E}} : \mathbb{A}^2 \to \mathbb{P}^1$ be the rational map:

$$j_{\mathcal{E}}(u,v) = \frac{\left(u^4 - 4u^3 - 8u^2v + 6u^2 - 8uv - 4u + 16v^2 + 16v + 1\right)^3}{v^3\left(u^4 - 3u^3 - 8u^2v + 3u^2 - 20uv - u + 16v^2 + v\right)} \tag{1}$$

Note that $j_{\mathcal{E}}(u,v)$ is the j-invariant of the fiber over (u,v). We will use $j_{\mathcal{E}}$ to compute j-invariants of elliptic curves represented by points on $X_1(\ell)$; we will denote these maps $j_\ell := j_{\mathcal{E}} \circ i_\ell$.

Next, define:

$$\alpha_{\mathcal{E}} : \mathbb{A}^2 \to \mathbb{A}^2 \qquad \alpha_{\mathcal{E}}(u,v) = \left(-\frac{u^2v - u^2 + 3uv - 2v^2}{u^4}, -\frac{v\left(u^2 + u - v\right)^3}{u^8}\right)$$

If $(u_0, v_0) \in \mathbb{A}^2$ represents a pair (E, P_0), then $\alpha_{\mathcal{E}}(u_0, v_0)$ represents $(E, 2P_0)$. In particular, $j_{\mathcal{E}} \circ \alpha_{\mathcal{E}} = j_{\mathcal{E}}$. We will restrict α to the modular curves we obtain to obtain generators of the automorphism group of $X_1(\ell)$ as an $X_0(\ell)$-scheme.

Now, the $\langle \alpha|_{X_1(\ell)} \rangle$-orbits of $X_1(\ell)$ represent isogenies of degree ℓ up to isomorphism. The only thing we need is a method for computing the j-invariant of the isogenous curve from this data. Precisely, we want a map $j'_\ell : X_1(\ell) \to \mathbb{P}^1$ that gives us the j-invariant of the curve we obtain by taking a quotient of E by the subgroup generated by $(0,0)$. This is also straightforward, and in fact there are two ways one can obtain the j-invariant of the isogenous curve:

- We have a model of our curve, and we have a generator of the ℓ-torsion subgroup. Thus, we can compute a model of the isogenous curve using Velu's formula, and compute the j-invariant of the isogenous curve using that model. In fact, we can do this for all curves at once, by applying Velu's formula to the universal curve over $X_1(\ell)$. We will do this for $\ell = 5, 7$.
- We will also describe an involution $\beta : X_1(\ell) \to X_1(\ell)$ that takes (E, P) to (E', P'), where:
  - $E' \cong E / \langle P \rangle$.
  - P' is a generator of the dual isogeny $E' \to E$.

  To obtain β, we simply need to find an involution that permutes the cusps of the modular curve in a particular way.

With this data, one can compute the ℓ-isogeny graph for any prime p by doing the following:

(1) First, find all the supersingular j-invariants in $\mathbb{F}_{p^2}$, e.g. by computing the 2-isogeny graph.
(2) Next, find a field $\mathbb{F}_q$ where we have a model with full ℓ-torsion for each supersingular j-invariant. As mentioned earlier, this simply boils down to computing the order of p in $(\mathbb{Z}/\ell\mathbb{Z})^\times$.
(3) For each $\langle\alpha\rangle$-orbit in $X_1(\ell)(\mathbb{F}_q)$, we find a representative P and compute the j-invariant of the associated curve using the composition $j_{\mathcal{E}} \circ i_\ell$.
(4) If the j-invariant is supersingular, then we've found an edge in the supersingular isogeny graph. We compute the j-invariant of the isogenous curve and record it.

Now, the problem of finding all points on a modular curve can be difficult if $X_1(\ell)$ is given by a "general" model as a plane curve. If our modular curve is hyperelliptic, then we can compute all points defined over a field $\mathbb{F}_q$ in $\mathcal{O}(q)$ time; we will be focusing on these examples. [4] For $\ell \leq 13$, $X_1(\ell)$ has genus ≤ 2, so we can find hyperelliptic models of $X_1(\ell)$. For that reason, we focus on $\ell \in \{5, 7, 11, 13\}$.

Now, at various points in this process, we will have to deal with points on $X_1(\ell)$ that represent singular elliptic curves. These points will be referred to as *cusps* of the modular curve. Attempting to evaluate $j_{\mathcal{E}}$ at a cusp will result in a division by 0, so we have to make sure to avoid them when we compute j-invariants. However, this is not a big deal, since the number of cusps is known in advance (there are always exactly $\ell - 1$ cusps on $X_1(\ell)$ when $\ell > 3$ is prime), and we can compute these in advance.[5] We will use the cusps to obtain involutions β that allow us to compute j-invariants for isogenous curves without needing Velu's formula. Before we starting computing algebraic models of modular curves, we review a few general results about cusps.

3.0.1. *Cusps.* Let $\ell > 3$ be a prime, and let $X_0(\ell) = \Gamma_0(\ell)\backslash\mathcal{H}^*$. Then $X_0(\ell)$ has precisely two cusps:

$$\Gamma_0(\ell) \cdot \infty = \{\infty\} \cup \left\{\frac{a}{b} \in \mathbb{Q} : p | b, p \not| a\right\}$$
$$\Gamma_0(\ell) \cdot 1 = \left\{\frac{a}{b} \in \mathbb{Q} : p \not| b\right\}$$

The cusp $\Gamma_0(\ell) \cdot \infty$ always has width 1, and the cusp $\Gamma_0(\ell) \cdot 1$ has width ℓ. The Fricke involution $X_0(\ell) \to X_0(\ell)$ swaps these two cusps.

[4] There are other situatons where we could compute all points in $\mathcal{O}(q)$ time, e.g. if we have a model of our modular curve as a bielliptic curve.

[5] Note, however, that half of them are defined over $\mathbb{Q}$, and the other half require a primitive ℓth root of unity to describe.

Now, these results carry over to the algebraic side. We are working with $X_1(\ell)$ on the algebraic side, so we also need to understand the cusps of the analytic version of $X_1(\ell)$, i.e. $\Gamma_1(\ell)\backslash\mathcal{H}^*$, The (analytic) map $X_1(\ell) \to X_0(\ell)$ is unramified over the cusps, so $X_1(\ell)$ has $\frac{\ell-1}{2}$ cusps of width 1 and $\frac{\ell-1}{2}$ cusps of width ℓ. We can use these ideas to compute j-invariants for isogenous curves without Velu's formula: all we need is a lift of the Fricke involution for our algebraic models of $X_1(\ell)$. Since the Fricke involution swaps the I_1, I_ℓ cusps on $X_0(\ell)$, any lift of the Fricke involution should swap the I_1 and I_ℓ fibers on $X_1(\ell)$. We will see that this condition is enough to determine β for $\ell \in \{5, 7, 11, 13\}$.

3.0.2. *Fundamental Domains.* For $\ell = 5, 7, 13$, we will describe a "fundamental domain" for $X_1(\ell) \to X_0(\ell)$ - precisely, this means we will describe a subset of $X_1(\ell)(\mathbb{F}_q)$ that contains exactly one element from each fiber of $X_1(\ell) \to X_0(\ell)$. We will describe these sets in terms of a primitive element $g \in \mathbb{F}_q^\times$.

Precisely, if $g \in \mathbb{F}_q^\times$ is a primitive element and $a < b$ are integers, we can write:

$$g^{[a,b]} = \left\{g^n \in \mathbb{F}_q^\times : a \leq n \leq b\right\}$$

We can embed $\mathbb{F}_q^\times \to \mathbb{P}^1$ via $g^a \mapsto [g^a : 1]$, so we can describe subsets of modular curves of genus 0 using this notation.

3.1. $\ell = 5$. We illustrate these ideas by going through the complete process when $\ell = 5$.

First, we compute $-P_0, \pm 2P_0, 3P_0$:

$$2P_0 = (v, uv) \qquad 3P_0 = (u, v-u)$$

$$-P_0 = (0, v) \qquad -2P_0 = (v, 0)$$

To obtain a description of $X_1(5)$, we set $3P = -2P_0$ to obtain an algebraic condition between u, v that encodes the fact that $(0,0)$ has order 5. For this value of ℓ, the algebraic relations that need to be satisfied are $u = v$ and $v - u = 0$; this means $X_1(5)$ is simply the (closure) of the diagonal $V(u-v) \subset \mathbb{A}^2$, and for any elliptic curve E in $\mathcal{E}_{u,v}$ that lies over the diagonal, the point $(0,0)$ has order 5.

Now, $X_1(5)$ is abstractly isomorphic to $\mathbb{P}^1$. If we fix an affine coordinate $t = \frac{t_0}{t_1}$ on $\mathbb{P}^1$, then the rational map $i_5 : X_1(5) \to \mathbb{A}^2$ is given by $i_5(t) = (t, t)$, and the universal elliptic curve with a point of over 5 is:

$$y^2 + (1-t)xy - ty = x^3 - tx^2 \tag{E5}$$

We compute $j_5 := j_{\mathcal{E}} \circ i_5$:

$$j_5(t) = \frac{\left(t^4 - 12t^3 + 14t^2 + 12t + 1\right)^3}{t^5\left(t^2 - 11t - 1\right)} \tag{J5}$$

3.1.1. *Velu.* To compute the j-invariant of the isogenous curve, we can use Velu's formula on the entire family over $X_1(5)$. This gives us a new family over $X_1(5)$ given by a Weierstrass equation:

$$y^2 + a_1' xy + a_3' y = x^3 + a_2' x^2 + a_4' x + a_6'$$

where:

$$\begin{aligned} a_1' &= 1 - t \quad (= a_1) \\ a_2' &= -t \quad (= a_2) \\ a_3' &= -t \quad (= a_3) \\ a_4' &= -5t\left(t^2 + 2t - 1\right) \\ a_6' &= -t\left(t^4 + 10t^3 - 5t^2 + 15t - 1\right) \end{aligned}$$

The j-invariant of this new family is:

$$\text{(J5')} \qquad j_5'(t) = \frac{\left(t^4 + 228t^3 + 494t^2 - 228t + 1\right)^3}{t\left(t^2 - 11t - 1\right)^5}$$

Now, to compute 5-isogeny graphs, we just need to compute j_5, j_5' for all $t \in X_1(5)$ - if $j_5(t)$ is supersingular, so is $j_5'(t)$ and the pair $(j_5(t), j_5'(t))$ represents an edge on the graph. However, this process will overcount the edges by a factor of 2. To avoid overcounting, we have to make sure we only check one element in each fiber of $X_1(5) \to X_0(5)$. Two elements t_1, t_2 are in the same fiber of $X_1(5) \to X_0(5)$ if and only if they are in the same orbit under the action of $\alpha_{\mathcal{E}}|_{X_1(5)}$. Define $\alpha_5(t) = \frac{-1}{t}$. A computation shows that:

$$\alpha_{\mathcal{E}} \circ i_5(t) = \left(\frac{-1}{t}, \frac{-1}{t}\right) = \alpha_{\mathcal{E}} \circ i_5 \circ \alpha_5(t)$$

Thus, $X_0(5) = X_1(5) / \langle \alpha_5 \rangle$, and we can compute the isogeny graph by computing j_5, j_5' for a representative of each orbit under $\langle \alpha_5 \rangle$.

3.1.2. *Cusps.* Note that $X_1(5)$ has cusps of type I_1 over $t = 0, \infty$ and cusps of type I_1 over the roots of $t^2 - 11t - 1 = 0$. When we compute $j_{\mathcal{E}}$, we have to avoid these points.

However, we can also use these points to obtain the formula for j_5' without using Velu's formula.

Let $\rho_1 = \frac{1}{2}\left(11 - 5\sqrt{5}\right)$ and $\rho_2 = \frac{1}{2}\left(11 + 5\sqrt{5}\right)$ be the roots of $t^2 - 11t - 1 = 0$. There is a 1-parameter family of Mobius transforms $X_1(5) \to X_1(5)$ that take ρ_1 to 0 and ρ_2 to ∞:

$$F_a(t) = a \cdot \frac{t - \rho_1}{t - \rho_2}$$

Furthermore, exactly one of these Moebius transforms is an involution: $t \mapsto \frac{at+b}{ct+d}$ has order 2 iff $a+d=0$, so $F_a(t)$ is an involution iff $a=\rho_2$. Define:

$$\beta_5(t) = \frac{\rho_2(t-\rho_1)}{t-\rho_2}$$

Then $\beta_5(t)$ is an involution of $X_1(5)$ that swaps the I_1 cusps with the I_5 cusps. There is only one other involution that swaps the I_1 cusps with the I_5 cusps, which can be obtained by composing β with $t \mapsto \frac{-1}{t}$.[6] A computation shows that $j_5 \circ \beta = j_5'$, where j_5, j_5' are given by the formulas above.

3.1.3. *Fundamental domain.* Let $t = g^a \in \mathbb{F}_q^\times$. Then:

- $-t = -1 \cdot t = g^{\frac{q-1}{2}} \cdot g^a$ - i.e. negation acts on the exponent as addition by $\frac{q-1}{2}$ (mod $q-1$). Note that this swaps $g^{[0,\frac{q-1}{2}]}$ and $g^{[\frac{q-1}{2},q-1]}$.
- $t^{-1} = g^{-a}$.

Let $a = \lfloor \frac{q-1}{4} \rfloor$ and $b = \lfloor \frac{3(q-1)}{4}$. Then the set $g^{[a,b]}$ is a fundamental domain for $\mathbb{F}_q^\times / \left\langle t \mapsto \frac{-1}{t} \right\rangle$: for every element $t \in \mathbb{F}_q^\times$, exactly one of $t, \frac{-1}{t}$ belongs to $g^{[a,b]}$. Note that the fixed points $t \mapsto \frac{-1}{t}$ are on the "boundary" of $g^{[a,b]}$.

3.1.4. *Quotient.* Since $X_0(5) = X_1(5)/\langle \alpha \rangle$, we can describe the map $X_1(5) \to X_0(5)$ as:

$$q_5(t) = \frac{t}{t^2-1}$$

Writing t for the affine coordinate on $X_0(5)$, we have:

$$\widetilde{j_5}(t) = \frac{(16t^2-12t+1)^3}{t^5(1-11t)} \tag{J5.0}$$

An easy computation shows that $j_5(t) = \widetilde{j_5} \circ q_5(t)$. Furthermore, we can define:

$$\widetilde{\beta_5}(t) = \frac{1-11t}{4t+11} \tag{B5.0}$$

Then $j_5'(t) = (\widetilde{j_5} \circ \widetilde{\beta_5} \circ q_5)(t)$

[6] Note that $\rho_2 = \frac{-1}{\rho_1}$ - this follows from the fact that the constant term in the minimal polynomial of ρ_1 is equal to -1.

3.2. $\ell = 7$. We've already computed a few multiples of P_0. We compute two more $(4P_0, -3P_0)$ and set them equal to each other to obtain a condition a relation between u, v:

$$C_7 : \quad u^3 + uv - v^2 = 0$$

This is a singular curve of genus 0. We take $X_1(7) = \mathbb{P}^1$. Writing $t = \frac{t_0}{t_1}$ for an affine coordinate on $X_1(7)$ as above, we can describe the map $X_1(7) \to C_7 \to \mathbb{A}^2$

$$i_7 : X_1(7) \to \mathbb{A}^2 \qquad t \mapsto (t^2 - t, t^3 - t^2)$$

The universal surface with a point of order 7 is therefore given by the following equation:

$$y^2 + (1 + t - t^2)xy + t^2(1 - t)y = x^3 + t^2(1 - t)x^2$$

We compute $j_7 = j_{\mathcal{E}} \circ i_7$:

$$j_7(t) = \frac{\left(t^2 - t + 1\right)^3 \left(t^6 - 11t^5 + 30t^4 - 15t^3 - 10t^2 + 5t + 1\right)^3}{t^7(t - 1)^7 \left(t^3 - 8t^2 + 5t + 1\right)} \tag{J7}$$

Next, we compute the involution $\beta : X_1(7) \to X_1(7)$. We have cusps of type I_7 at $t = 0, 1\infty$, and cusps of type I_1 over the roots of $t^3 - 8t^2 + 4t + 1 = 0$. Let ω_7 be a primitive 7th root of unity. For $m = 1, 2, 3$, define:

$$\xi_7^{(m)} = \omega_7^m + \omega_7^{-m}$$

Then:

$$\rho = -(4\xi_7^{(1)} + \xi_7^{(2)} + 3\xi_7^{(3)})$$

is a root of $t^3 - 8t^2 + 4t + 1 = 0$.

Now, we can construct β by finding a Moebius transform $\beta : \mathbb{P}^1 \to \mathbb{P}^1$ that takes $\rho \mapsto 0$, $\alpha(\rho) \mapsto \alpha(0), \alpha^2(\rho) \mapsto \alpha^2(0)$. Explicitly, one can take:

$$\beta_7(t) = \frac{\left(-2\omega_7^4 + \omega_7^3 - 3\omega_7^2 + \omega_7 - 2\right)t + \left(2\omega_7^4 - \omega_7^3 + 2\omega_7^2 - \omega_7 + 2\right)}{-\omega_7^2 t + \left(2 - \omega_7 + 3\omega_7^2 - \omega_7^3 + 2\omega_7^4\right)} \tag{B7}$$

Then β_7 is an involution of $X_1(7)$ that permutes the I_1 cusps and the I_7 cusps, and the only other involutions that permute the I_1 cusps and the I_7 cusps are $\beta \circ \alpha$ and $\beta \circ \alpha^2$. After a significant amount of simplification, one can show that that:

$$j_7'(t) = \frac{\left(t^2 - t + 1\right)^3 \left(t^6 + 229t^5 + 270t^4 - 1695t^3 + 1430t^2 - 235t + 1\right)^3}{t(t - 1)\left(t^3 - 8t^2 + 5t + 1\right)^7} \tag{J7'}$$

3.2.1. *Fundamental domain.* Let $\mathbb{F}_q$ be a finite field, and assume $q \equiv 1 \pmod 3$. Define $\alpha : \mathbb{P}^1_{\mathbb{F}_q} : \mathbb{P}^1_{\mathbb{F}_q}$ by $\alpha(t) = \frac{1}{1-t}$. The assumption $q \equiv 1 \pmod 3$ ensures that $\mathbb{F}_q$ contains a primitive cube root of unity, say $\omega_3 \in \mathbb{F}_q$. We define a change of variable map $F_7 : \mathbb{P}^1 \to \mathbb{P}^1$:

$$F_7(t) = \left(\frac{1-\omega_3}{1-\omega_3^2}\right) \cdot \frac{t-\omega_3^2}{t-\omega_3}$$

Now, let $\alpha_F = F \circ \alpha \circ F^{-1}$. A computation shows that $\alpha_F(t) = \omega_3 t$. Thus, we can take the set:

$$X_F = \left\{ g^e \in \mathbb{F}_q^\times : 0 \leq e < \frac{q-1}{3} \right\}$$

as a fundamental domain of $\mathbb{P}^1_{\mathbb{F}_q}$ under the action of α_F.

In other words, for every α_F orbit in $\mathbb{P}^1_{\mathbb{F}_q} - \{0, \infty\}$, there is precisely one representative of the orbit in X_F. Finally, we define $X_7(\mathbb{F}_q) = F(X_F)$. Then every orbit under the action of α has precisely one representative in $X_7(\mathbb{F}_q)$

3.2.2. *Quotient.* We can obtain a description of $X_0(7)$, as well as the j-map $X_0(7) \to X(1)$.

(Q7)
$$q_7(t) = \frac{(1-t)t}{t^3 - 3t^2 + 1}$$

(J7.0)
$$\widetilde{j_7}(t) = -\frac{(9t^2 - 3t + 1)\left(t^2 + 5t + 1\right)^3}{t^7(5t+1)}$$

(B7.0)
$$\widetilde{\beta_7}(t) = \frac{5t+1}{24t-5}$$

3.3. $\ell = 11$. As with $\ell = 7$, we can compute multiples of P_0 and set them equal to 0 to obtain the equation of a curve $C_{11} \subset \mathbb{A}^2$. Obtaining a nice model of $X_1(11)$, and a map $X_1(11) \to \mathbb{A}^2$, is more complicated; the model we will be using was found in [1]. We will use the following equation for $X_1(11)$:

(X11)
$$w^2 - w = z^3 - z^2$$

The map $i_{11} : X_1(11) \to \mathbb{A}^2$ is:

(I11)
$$(z, w) \mapsto \left(\frac{(w-1)(w+z-1)}{z}, \frac{w(w-1)(w+z-1)}{z} \right)$$

Note that $X_1(11)$ is a curve of genus 1 - in fact, the equation for $X_1(11)$ coincides with the equation of the fiber over $t = 1$ on $X_1(5)$ E5. In particular, this means that the point $(0,0) \in X_1(11)$ has order 5 with respect to the elliptic curve group law. Furthermore, the automorphism $\alpha : X_1(11) \to X_1(11)$ given by $\alpha(P) = (0,0) + P$ generates $Aut(X_1(11)/X_0(11))$.

3.3.1. *Cusps.* To classify all cusps on $X_1(11)$, we compute the discriminant of the universal curve over $X_1(11)$:

$$\frac{(w-1)^6 w^3 (w+z-1)^4 \left((z^6+z^5-3z^4-4z^3+9z^2-6z+1) - w\left(5z^4-12z^3+11z^2-6z+1\right)\right)}{z^7}$$

Now, if (z,w) is a cusp, then this expression necessarily vanishes. An easy computation shows that the factors $w, w-1, w+z-1$ only vanish on the 5-torsion subgroup. That just leaves:

$$\left(z^6+z^5-3z^4-4z^3+9z^2-6z+1\right) - w\left(5z^4-12z^3+11z^2-6z+1\right)$$

Now, this expression is linear in w, so it vanishes precisely when:

$$w = w(z) = \frac{z^6+z^5-3z^4-4z^3+9z^2-6z+1}{5z^4-12z^3+11z^2-6z+1}$$

Plugging $(z,w(z))$ into the defining equation for $X_1(11)$ and factoring gives us the condition:

$$-\frac{(z-1)^5 z^2 \left(z^5-18z^4+35z^3-16z^2-2z+1\right)}{\left(5z^4-12z^3+11z^2-6z+1\right)^2} = 0$$

Thus, in order for the last factor in the discriminant to vanish, either $z=1, z=0$ or z is a root of:

$$z^5-18z^4+35z^3-16z^2-2z+1=0$$

To obtain a representative of the I_1 orbit, we fix a primitive 11th root of unity ω_{11}, set $\xi_{11}^{(m)} = \omega_{11}^m + \omega_{11}^{-m}$, and define:

$$\rho = -\left(6\xi_{11}^{(1)} + \xi_{11}^{(2)} + 5\xi_{11}^{(3)} + 2\xi_{11}^{(4)} + 4\xi_{11}^{(5)}\right)$$

Then ρ is a root of the quintic. The $z=0,1$ factors vanish only at the points of order 5.

So, altogether, we have 10 cusps that can be partitioned into two orbits under the action of α:

- We have fibers of type I_{11} over the 5 points of order 5.
- We have fibers of type I_1 over the 5 points (z,w) where z is a root of (), and $w = w(z)$.

(ADD REFS TO EQS)

Now, the denominator of $j_{\mathcal{E}} \circ i_{11}$ only vanishes at the cusps of $X_1(11)$, so we can use the formula for $j_{\mathcal{E}}$ to compute $j_{11}(P)$ for any noncuspidal point on $X_1(11)$.

3.3.2. *Computing β.* We want an involution of $X_1(11)$ that swaps the set where we have I_{11} fibers with the set where we have I_1 fibers.

Since $X_1(11)$ is an elliptic curve, any automorphism of $X_1(11)$ can be factored into a composition of a translation map and an isogeny of degree 1. Since $j(X_1(11)) \neq 0, 1728$, the only isogenies of degree 1 are the identity and the negation map. Thus, any any automorphism of $X_1(11)$ has the form $P \mapsto P_0 + P$ or $P \mapsto P_0 - P$ for some fixed $P_0 \in X_1(11)$. Automorphisms of the form $P \mapsto P_0 + P$ have infinite order, but every automorphism of the form $P \mapsto P_0 - P$ is necessarily an involution. Furthermore, if we take P_0 to be any of the 5 points where we have an I_1 fiber, then the involution $P \mapsto P_0 - P$ swaps the set of 5-torsion points with the set of points with an I_1 fiber.

Thus, to compute $j'_{11}(P)$, where P is some point on $X_1(11)$, all we have to do is compute $P_0 - P$ for one of the points P_0, and then compute $j'_{11}(P) := j_{11}(P_0 - P)$ using the ordinary j_{11}-map. Replacing P_0 by a different I_1 point is like replacing P by $P + T$, where T is a torsion point, and since torsion points don't change the j-invariant, it does not matter which P_0 one chooses.

3.4. $\ell = 13$**.** We follow the same steps as $\ell = 11$ to obtain a curve $C_{13} \subset \mathbb{A}^2$. Let $\mathbb{P}^1 = \{[z_0 : z_1]\}$ and let $X_1(13)$ be the double cover of $\mathbb{P}^1$:

$$w_0^2 - w_0 z_0^3 - w_0 z_0^2 z_1 - w_0 z_1^3 - z_0^2 z_1^4 - z_0 z_1^5$$

We will mostly[7] work on the chart $z_1 = 1$, using affine coordinates $z = \frac{z_0}{z_1}$ and $w = \frac{w_0}{z_1}$. The equation of the curve in these coordinates is:

$$w^2 + wz^3 + wz^2 + w - z^2 - z = 0$$

and the the map $i_{13} : X_1(13) \to C_{13} \subset \mathbb{A}^2$ can be described in terms of these coordinates as:

$$(z, w) \mapsto \left(\frac{wz(wz - w - 1)}{w + 1}, \frac{wz(1 - wz)(wz - w - 1)}{w + 1} \right)$$

3.4.1. *Automorphism Group.* Because $X_1(13)$ has genus > 1, it only has finitely many automorphisms. In fact, the full automorphism group of $X_1(13)$ is isomorphic to the dihedral group with 12 elements - see [4]. This is great news:

- The cyclic group of order 6 must correspond to $Aut(X_1(13)/X_0(13))$.
- Let σ be any involution of $X_1(13)$ not contained in the cyclic subgroup of order 6. Then σ must be a lift of the Fricke involution.

[7] Later on, we will need a full list of the cusps of $X_1(13)$, and two of the cusps do not lie on the chart we are working on.

Explicit formulas for the generators of the automorphism group are computed in [4]. The automorphism of order 6 is defined over $\mathbb{Q}$:

$$\alpha_{13}(z,w) = \left(\frac{-1}{1+z}, \frac{w-z}{z+z^2-w} \right)$$

We can obtain the formula for β in the usual way, or look it up in [4].

We note, for convenience, that the I_{13} cusps can be found over the 6 points $([z_0 : z_1], w)$ where:

$$z_0 z_1 (z_0 + z_1) = 0$$

The I_1 cusps can be found over the points (z, w) (in affine coordinates) where:

$$z^3 + 4z^2 + z - 1 = 0$$

We can describe a root of this cubic if we have a primitive 13th root of unity ω_{13}:

$$\rho_{13} = \frac{-1}{\omega_{13} + \omega_{13}^5 + \omega_{13}^{-5} + \omega_{13}^{-1}} \tag{I1.13}$$

However, we can actually simplify things a great deal by using the data we have to obtain an algebraic model of $X_0(13)$: since $X_0(13)$ has genus 0, we will be able to describe the maps j'_{13}, j'_{13} explicitly, as we did for $\ell = 5, 7$ in J5,J5',J7,J7'.

3.4.2. *Quotient Map.* First, note that α_{13}^3 coincides with the hyperelliptic involution on $X_1(13)$. Thus, the quotient map $X_1(13) \to X_1(13)/\langle \alpha_{13}^3 \rangle \cong \mathbb{P}^1$ is simply given by $([z_0 : z_1], w) \mapsto [z_0 : z_1]$. The action of α_{13} on this partial quotient is $[z_0 : z_1] \mapsto [-z_0 : z_0 + z_1]$, or $z \mapsto \frac{-1}{1+z}$ in terms of the affine coordinate $z = \frac{z_0}{z_1}$. Thus, $X_0(13) \cong \mathbb{P}^1 / \left\langle z \mapsto \frac{-1}{1+z} \right\rangle$. We can define:

$$q_{13} : X_1(13) \to X_0(13) \qquad q_{13}([z_0 : z_1], w) = [z_0 z_1 (z_0 + z_1) : z_0^3 - 3 z_0 z_1^2 - z_1^3]$$

We use projective coordinates $[t_0 : t_1]$ on $X_0(13)$, we set $t = \frac{t_0}{t_1}$, and we define:

$$\widetilde{j_{13}(t)} : X_0(13) \to X(1)$$

$$\widetilde{j_{13}(t)} = -\frac{(9t^2 + 3t + 1)\left(53t^4 + 61t^3 + 32t^2 + 9t + 1\right)^3}{t^{13}(4t+1)} \tag{J13.0}$$

One can check that[8] $\widetilde{j_{13}} \circ q_{13} = j_{\mathcal{E}} \circ i_{13}$ - but $\widetilde{j_{13}} \circ q_{13}$ is much simpler to write out:

(J13)

$$-\frac{\left(z^2+z+1\right)^3 \left(z^{12} + 9z^{11} + 29z^{10} + 40z^9 + 22z^8 + 16z^7 + 40z^6 + 22z^5 - 23z^4 - 25z^3 - 4z^2 + 3z + 1\right)^3}{z^{13}(z+1)^{13}\left(z^3 + 4z^2 + z - 1\right)}$$

[8] They have the same associated divisor, so they agree up to a scalar multiple; and they evaluate to the same value at points which are not zeros or poles, so they must be equal.

Because the I_1 orbit becomes a single point on $X_0(13)$, we can describe the involution $\tilde{\beta_{13}} : X_0(13) \to X_0(13)$ over $\mathbb{Q}$:

$$\tilde{\beta_{13}}(t) = \frac{4t+1}{-3t-4} \tag{B13.0}$$

We compose to obtain:

$$\widetilde{j_{13}}'(t) = -\frac{(9t^2+3t+1)\left(5573t^4+61t^3+512t^2-231t+1\right)^3}{t(4t+1)^{13}} \tag{J13.0'}$$

3.4.3. $X_0(13) \to X_1(13)$. Given a point $t \in X_0(13)$, we can recover an explicit description of an elliptic curve E, together with a subgroup of order 13:

- First, find all z such that $q_{13}(z) = t$. The map q_{13} has degree 3, so this determines 3 choices for z.
- For each choice of z, there are two choices for w that give us a point on $X_1(13)$.
- Now the points on $X_1(13)$ give us pairs (E, P), where P is a generator of the subgroup of order 13. The fact that we have 6 points corresponds to the fact that there are 6 choices for the generator, if we treat $\pm P$ as the same point.

3.4.4. *Fundamental domain.* Let ω_3 be a primitive cube root of unity and let $F : \mathbb{P}^1 \to \mathbb{P}^1$ be the Moebius transform:

$$F(z) = \frac{\omega_3 + z + 1}{(\omega_3+1)(\omega_3 - z)}$$

A computation shows that $(F^{-1} \circ \alpha \circ F)(z) = \omega_3 z$, so we deduce that:

$$F\left(\left\{g^i : 0 \le i \le \frac{q-1}{3}\right\}\right)$$

is a fundamental domain for $\mathbb{P}^1$ under the order 3 action $z \mapsto \frac{-1}{1+z}$.

4. Class Polynomials

The one ingredient we need to get started is a way of obtaining a first supersingular elliptic curve $E_0/\mathbb{F}_p$. For $p \not\equiv 1 \pmod{12}$, at least one of $j = 0, 1728$ is supersingular, so we don't have to worry about this. When $p \equiv 1 \pmod{12}$, we have to work a little harder.

The problem when $p \equiv 1 \pmod{12}$ is that $-1, -3$ are squares in $\mathbb{F}_p$. To find a supersingular curve in this case, we have to find an integer $d < 0$ with the property that d is a nonsquare mod p, and an elliptic curve $E/\overline{\mathbb{Q}}$ which has complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{d})$.

Finding a nonsquare is easy - half of the elements in $\mathbb{F}_p^\times$ are nonsquares. The real problem is finding a value of d for which the second part of the problem is as easy as possible:

- In general, we want to choose d so that the class number is as small as possible.

- If the class number is odd, then one of the roots of the Hilbert class polynomial is guaranteed to have a root in $\mathbb{F}_p$.

If we can find d so that $\mathbb{Q}(\sqrt{-d})$ has class number 1 and d is a nonsquare in $\mathbb{F}_p$, then there is a unique elliptic curve $E/\mathbb{Q}$ with complex multiplication by $\mathbb{Q}(\sqrt{-d})$. There are 9 such values of d (the negatives of the Heegner numbers); models for the associated elliptic curves can be found in the appendix of [8].

Now, for most values of p, one of these choices of d is a nonsquare.

- The smallest prime for which all of these values of d are squares is $p = 15073$.
- Of the first million primes, there are only 1769 choices of p for which all of these values of d are squares.

To deal with these primes, we need a way of computing the Hilbert class polynomials of $\mathbb{Q}(\sqrt{-d})$.

Fortunately, we can do this without introducing any additional machinery. We will essentially generalize the computation used in the proof of Prop. 2.3.1 in [8]:

- Recall the maps:

$$j_2(a,b) = \frac{256a^2(a^2-3b)^2}{b^2(a^2-4b)} \qquad j_2'(a,b) = \frac{16^2(a^2+12b)^2}{b(a^2-4b)^2}$$

  The map $j_2(a,b)$ gives us the j-invariant of the curve:

$$y^2 = x(x^2+ax+b)$$

  and $j_2'(a,b)$ gives us the j-invariant of the isogenous curve. Now, if $E/\mathbb{C}$ has an isogeny of degree 2 $E \to E$, then there exists a model of E given by (a,b) such that $j_2(a,b) = j_2'(a,b)$. By solving the equation $j_2(a,b) = j_2'(a,b)$, Silverman obtains models of all elliptic curves $E/\mathbb{Q}$ with an endomorphism $E \to E$ of degree 2.
- To obtain models of all elliptic curves with an endomorphism $E \to E$ of degree ℓ, all we need is an analog of j_2, j_2' - and of course, we have such an analog.

For values of ℓ where $X_1(\ell)$ has genus 0, the maps $j_\ell(t), j_\ell'(t)$ are simply rational functions in t. We can set them equal to each other and obtain a single variable polynomial in t whose roots gives us models of elliptic curves with an isogeny of degree ℓ. We can then compute the minimal polynomial of the j-invariants of these curves to obtain Hilbert polynomials.

For example, setting $j_5(t) = j_5'(t)$, clearing denominators, and factoring, we obtain the condition:

$$\left(t^2+1\right)^2\left(t^4-36t^3+398t^2+36t+1\right)\left(t^4-22t^3-6t^2+22t+1\right)\cdots$$
$$\cdot\left(t^4-18t^3+200t^2+18t+1\right)\left(t^4-4t^3+46t^2+4t+1\right)=0$$

If $t^2+1=0$, then $j_5(t)=1728$, so we ignore that factor. Three of the quartic factors gives us elliptic curves with $j=(-2^5\cdot 3)^3, (2\cdot 3\cdot 11)^3, -2^15$; these j-invariants appear in [8], so we ignore them too. However, the roots of:

$$t^4-18t^3+200t^2+18t+1$$

give us elliptic curves with j-invariants:

$$j=320\left(884\sqrt{5}\pm 1975\right)$$

These j-invariants are not in $\mathbb{Q}$, so they represent a new isogeny class of elliptic curves with complex multiplication. Since $\mathbb{Q}[\sqrt{-5})$ has class number 2, and $\sqrt{-5}$ has norm 5, there must be a pair of elliptic curves defined over a quadratic extension of $\mathbb{Q}$ that have an isogeny of degree 5 to themselves, and since these j-values are the only irrational j-invariants, they must be the roots of the Hilbert class polynomial for $\mathbb{Q}(\sqrt{-5})$, and the Hilbert class function is:

$$H_5(j)=j^2-1264000j-681472000 \tag{H5}$$

Now, this example is interesting, but it does not help us find supersingular j-invariants in $\mathbb{F}_p$. The elliptic curves with these j-invariants are only supersingular if $\sqrt{-5}\notin\mathbb{F}_p$, but they are only defined over $\mathbb{F}_p$ if $\sqrt{5}\in\mathbb{F}_p$. Now, if $\sqrt{5}\in\mathbb{F}_p$ and $\sqrt{-5}\notin\mathbb{F}_p$, that means $\sqrt{-1}\notin\mathbb{F}_p$, so $j=1728$ is supersingular.

To ensure the Hilbert polynomial will have a root in $\mathbb{F}_p$, we should choose d so that $\mathbb{Q}(\sqrt{d})$ has odd class number. Now, we will compute $j_\ell(t), j'_\ell(t)$, for $\ell=4,6,8,10,12$ and keep a list of the minimal polynomials of the j-invariants we obtain along the way. We will be able to determine the related isogeny class by exhibiting values of d, and elements in $\mathbb{Q}(\sqrt{d})$ of the appropriate norm, that account for every new example we find.

4.1. $X_1(4)$. The map $X_1(4)\to\mathbb{A}^2$ is $t\mapsto(0,t)$ - i.e. the universal curve over $X_1(4)$ is:

$$y^2-ty=x^3-tx^2$$

The maps j_4, j'_4 are:

$$j_4(t)=\frac{\left(16t^2+16t+1\right)^3}{t^4(16t+1)} \tag{2}$$

$$j'_4(t)=-\frac{\left(256t^2-224t+1\right)^3}{t(16t+1)^4} \tag{3}$$

Setting these equal to each other and factoring, we obtain:

(4)

$$j_4(t) - j_4'(t) = \frac{(32t+1)\left(16t^2+t+1\right)\left(256t^2+16t+1\right)\left(256t^4+32t^3+753t^2+47t+1\right)}{t^4(16t+1)^4}$$

The j-invariants that we obtain from the solutions of $(32t{+}1)\left(16t^2+t+1\right)\left(256t^2+16t+1\right) = 0$ are $287496, 54000, -3375$ - we know about these already. However, the roots of:

$$\left(256t^4+32t^3+753t^2+47t+1\right)$$

give rise to j-invariants $\frac{-135}{2} \cdot \left(1415 \pm 637\sqrt{5}\right)$, which we haven't seen yet. Since $\frac{1+\sqrt{-15}}{2}$ has norm 4, and $\mathbb{Q}(\sqrt{-15})$ has class number 2, it follows that these j-invariants are the roots of the Hilbert class polynomial for $\mathbb{Q}(\sqrt{-d})$, and the Hilbert polynomial H_{15} is:

(H15)
$$H_{15}(j) = j^2 + 191025j - 121287375$$

4.2. $X_1(6)$**.** The map $X_1(6) \to \mathbb{A}^2$ is $t \mapsto (t, t+t^2)$, and:

$$j_6(t) = \frac{(3t+1)^3\left(3t^3+3t^2+9t+1\right)^3}{t^6(t+1)^3(9t+1)}$$

To obtain $j_6'(t)$, we use the involution β Composing these, we obtain:

$$j_6'(t) = \frac{(1-3t)^3\left(243t^3+405t^2+225t-1\right)^3}{t(t+1)^2(9t+1)^6}$$

We solve the equation $j_6(t) = j_6'(t)$, plug the solutions back into j_6 to obtain a list of j-invariants, and compute the minimal polynomials of those j-invariants.

We obtain two new minimal polynomials, one of degree 2 and one of degree 3. These must be the Hilbert polynomials for $\mathbb{Q}(\sqrt{-6}), \mathbb{Q}(\sqrt{-23})$, since these fields both contain elements of norm 6 ($\sqrt{-6}$, $\frac{1+\sqrt{-23}}{2}$, respectively) and they have class number 2, 3 respectively. The Hilbert polynomial for $\mathbb{Q}(\sqrt{-6})$ is:

(H6)
$$H_{-6}(j) = j^2 - 4834944j + 14670139392 = 0$$

and the Hilbert polynomial for $\mathbb{Q}(\sqrt{-23})$ is:

(H23)
$$H_{-23}(j) = j^3 + 3491750j^2 - 5151296875j + 12771880859375$$

4.3. $X_1(8)$**.** We obtain nothing new from $X_1(7)$, so we move on to $X_1(8)$. The map $X_1(8) \to \mathbb{A}^2$ is:

$$t \mapsto \left(\frac{(t-1)(2t-1)}{t}, (t-1)(2t-1)\right)$$

The involution $\beta : X_1(8) \to X_1(8)$:

$$\beta(t) = \frac{4t + \sqrt{2} - 2}{4(2t-1)}$$

Composing $j_8 \circ \beta$ gives us:

$$j_8'(t) = -\frac{\left(4096t^8 - 16384t^7 + 26624t^6 - 22528t^5 + 9600t^4 - 768t^3 - 864t^2 + 224t + 1\right)^3}{(t-1)t(2t-1)^2\left(8t^2 - 8t + 1\right)^8}$$

Now, we solve the equation $j_8(t) = j_8'(t)$, plug the roots back in, and compute the minimal polynomials. We find two new polynomials, one of degree 2 and one of degree 3. The polynomial of degree 3 must be the Hilbert polynomial for $\mathbb{Q}(\sqrt{-31})$, since that field has class number 3 and contains the element $\frac{1+\sqrt{-31}}{2}$ of norm 8:

$$j^3 + 39491307j^2 - 58682638134j + 1566028350940383 = 0$$

(H31)
$$H_{-31}(j) = j^3 + 39491307j^2 - 58682638134j + 1566028350940383$$

The other polynomial we obtain is:

$$j^2 - 52250000j + 12167000000$$

This roots of this polynomial give us j-invariants of curves which are 2-isogenous to the curve with complex multiplication by $\sqrt{-2}$.

4.4. $X_1(9)$**.** The map $i_9 : X_1(9) \to \mathbb{A}^2$ is:

(I9)
$$t \mapsto \left(t^2(t-1), t^2(t-1)\left(t^2 - t + 1\right)\right)$$

Thus:

(J9)
$$j_9(t) = \frac{\left(t^3 - 3t^2 + 1\right)^3\left(t^9 - 9t^8 + 27t^7 - 48t^6 + 54t^5 - 45t^4 + 27t^3 - 9t^2 + 1\right)^3}{(t-1)^9 t^9\left(t^2 - t + 1\right)^3\left(t^3 - 6t^2 + 3t + 1\right)}$$

We compute $j_9'(t)$ by computing 3-isogenies twice:

(J9')
$$j_9'(t) = \frac{\left(t^3 + 3t^2 - 6t + 1\right)^3\left(t^9 + 225t^8 - 855t^7 + 1866t^6 - 2844t^5 + 3123t^4 - 2265t^3 + 981t^2 - 234t + 1\right)^3}{(t-1)t\left(t^2 - t + 1\right)^3\left(t^3 - 6t^2 + 3t + 1\right)^9}$$

There are two new minimal polynomials, both of which have degree 2. One of them is the Hilbert polynomial of $\mathbb{Q}(\sqrt{-35})$, since $\frac{1+\sqrt{-35}}{2}$ has norm 9 and $\mathbb{Q}(\sqrt{-35})$ has class number 2:

(H35)
$$H_{-35}(t) = j^2 + 117964800j - 134217728000$$

The other quadratic polynomial corresponds to an elliptic curve which is isogenous to $j = 1728$ (check this).

4.5. $X_1(10)$**.** We obtain two new minimal polynomials, of degree 2, 4. The minimal polynomial of degree 2 must be the Hilbert polynomial for $\mathbb{Q}(\sqrt{-10})$, since that field has class number 2 and $\sqrt{-10}$ has norm 10:

$$H_{-10}(j) = j^2 - 425692800j + 9103145472000 \tag{H10}$$

The minimal polynomial of degree 4 must be the Hilbert polynomial for $\mathbb{Q}(\sqrt{-39})$, since the field has class number 4 and $\frac{1+\sqrt{-39}}{2}$ has norm 10.

(H39)

$H_{-39}(j) = j^4{+}331531596j^3{-}429878960946j^2{+}109873509788637459j{+}20919104368024767633$

4.6. $X_1(12)$**.** The map $i_{12} : X_1(12) \to \mathbb{A}^2$ is:

$$t \mapsto \left(\frac{(t-2)(t-1)\left(3t^2-6t+4\right)}{t^3}, \frac{(t-2)(t-1)\left(t^2-2t+2\right)\left(3t^2-6t+4\right)}{t^4}\right)$$

The involution $\beta : X_1(12) \to X_1(12)$ is:

$$t \mapsto \frac{t - \frac{1}{3}\left(3-\sqrt{3}\right)}{t-1}$$

Setting $j_{12}(t) = j_{12}(\beta(t))$ and clearing denominators, we obtain a polynomial in t whose roots encode the j-invariants of all curves with an isogeny $E \to E$ of degree 12.

For example, $\frac{1+\sqrt{-47}}{2}$ has norm 12 and the class number of $\mathbb{Q}(\sqrt{-47})$ is 5. The following quintic must be the Hilbert polynomial for $\mathbb{Q}(\sqrt{-47})$:

$$j^5 + 2257834125j^4 - 9987963828125j^3 + 5115161850595703125j^2 \cdots$$

$$\cdots - 14982472850828613281250j + 16042929600623870849609375 = 0$$

We also obtain:

$$20919104368024767633 + 109873509788637459j - 429878960946j^2 + 331531596j^3 + j^4$$

which must be the Hilbert polynomial for $\mathbb{Q}(\sqrt{-39})$, and corresponds to $\frac{3+\sqrt{-39}}{2}$.

There are two cubic factors, but these correspond to $\frac{5+\sqrt{-23}}{2}$ and $\frac{3+\sqrt{-31}}{2}$.

5. Algorithms

5.1. **Isogeny graphs for $\ell = 2, 3$.** In this section, we give an algorithm that takes as input a prime p, $\ell \in \{2, 3\}$, and a supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$, and returns:

(1) The complete set of supersingular j-invariants in $\mathbb{F}_{p^2}$.
(2) The supersingular isogeny graph for ℓ.

The basic structure of the algorithm can be described as follows:

(1) First, we find a single supersingular elliptic curve $E_0/\mathbb{F}_p$. Note that it doesn't matter which curve we start with, and it doesn't matter whether E_0 is defined over $\mathbb{F}_p$ or not - however, it is easier to search in $\mathbb{F}_p$, and it is always possible to find a supersingular curve $E_0/\mathbb{F}_p$. In the next step, we will assume that an explicit model for E_0 of the form:

$$y^2 = x^3 + fx + g \tag{5}$$

has been obtained. Note that such a model is easy to obtain, even if we only know the j-invariant of E_0:

- For $j(E_0) = 0$, we can use $f = 0, g = 1$.
- For $j(E_0) = 1728$, we can use $f = -1$, $g = 0$.
- For all other values of $j(E_0)$, we can use:

$$f = \frac{27j}{1728 - j}, \qquad g = \frac{54j}{1728 - j} \tag{6}$$

(2) Next, we look for a point of order ℓ on $E_0/\mathbb{F}_p$. *One advantage of taking $E_0/\mathbb{F}_p$, instead of over $\mathbb{F}_{p^2}$, is that we are guaranteed to find at least one point of order ℓ in $\mathbb{F}_p$. That makes this initial search considerably faster.*

(3) Once we have E_0 and a point $P_0 \in E_0(\mathbb{F}_p)$ of order ℓ, we find a "nice model" for (E, P_0). For both $\ell = 2, 3$, the nice model will be an equation for E given by a pair of parameters (a, b). The models are nice because:

- When we compute the isogenous curve $E/\langle P_0 \rangle$, the model we obtain will also be a nice model.
- If E is given by a nice model, it is very easy to find the other points of order ℓ needed to compute the isogeny graph.

(4) Once we have our nice model (a_0, b_0) for (E_0, P_0), we compute the other points $P_1, ..., P_\ell \in E_0(\mathbb{F}_{p^2})$ of order ℓ.

Note that to obtain these other torsion points, we simply need to find an ℓth root of a certain element $\mathbb{F}_{p^2}$ determined by (a_0, b_0)- the coordinates for the torsion points are readily computable once we have that ℓth root, and once we have the coordinates for $P_1, \ldots, P_\ell$, we can obtain all of the nice models $(a_1, b_1), \ldots, (a_\ell, b_\ell)$ needed to compute the isogeny graph.

(5) Once we have all of the nice models $(a_0, b_0), \ldots, (a_\ell, b_\ell)$ for E_0, we compute the coefficients of the nice models of the isogenous curves $(a'_0, b'_0), \ldots, (a'_\ell, b'_\ell)$.

Note that this step is determining all of the edges that are coming out of E_0 on the supersingular isogeny graph, so if we're interested in the isogeny graph, we record the edges.

(6) Finally, each of $(a'_0, b'_0), \ldots, (a'_\ell, b'_\ell)$ represents a supersingular elliptic curve, and at least one of those is guaranteed to be a supersingular elliptic curve that is not isomorphic to E_0.

We collect all the (a'_i, b'_i) that represent new curves, and repeat steps (4) and (5) for all of them, and do this until we are not obtaining any new elliptic curves.

There are only finitely many elliptic curves over $\mathbb{F}_{p^2}$, so this process will eventually terminate. Since all curves obtained in the algorithm are isogenous to E_0, and E_0 is supersingular, all of these curves are supersingular. Finally, since supersingular isogeny graphs are connected, we will obtain every supersingular curve in this way, in addition to obtaining the ℓ-isogeny graph itself.

We now present the algorithm in detail for $\ell = 2, 3$, so that we can explain what the nice models are, and how we use them to make the search for torsion points easier.

In both cases, we assume that step 1 has been completed, and we have a model for a supersingular curve $E_0/\mathbb{F}_p$ of the form 5.

5.1.1. *$\ell = 2$.* The algorithm is perfectly straightforward in this case. The one nontrivial part of the algorithm is going to be finding a square root.

(1) First, find a model for some supersingular $E_0/\mathbb{F}_p$.
(2) Finding a 2-torsion point on a model of the form 5 simply means finding a root of:

$$= x^3 + fx + g = 0$$

simply means finding a root of the cubic on the right hand side. For a supersingular E_0, with $f, g \in \mathbb{F}_p$, this cubic is guaranteed to have at least one root in $\mathbb{F}_p$, so we search in $\mathbb{F}_p$ for a root of $x^3 + fx + g = 0$. Once we find such a root, say x_0, we define $P_0 = (x_0, 0)$ and move on to the next step.

(3) To obtain a nice model, we do a change of variable
(4) To obtain the other torsion points, we solve the quadratic equation:

$$x^2 + a_0x + b_0 = 0$$

This step requires us to compute a square root $\rho = \sqrt{a_0^2 - 4b}$. Before moving on to the next step, we compute the nice models $(a_1, b_1), (a_2, b_2)$ that correspond to the two new 2-torsion points

(5) Once we have $(a_0, b_0), (a_1, b_1), (a_2, b_2)$, we compute $(a'_i, b'_i) = (-2a_i, a_i^2 - 4b_i)$ for $i = 0, 1, 2$.

(6) Finally, to decide whether (a'_i, b'_i) represents a new curve, we compute the j-invariant and compare it to the list of j-invariants that we've already found.

5.1.2. $\ell = 3$. We start by reviewing the criterion for determining whether a point on an elliptic has order 3.

Lemma 5.1. *Let K be a field of characteristic not equal to 2 or 3, let E/K be an elliptic curve given by an equation of the form:*

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

and let $P_0 = (x_0, y_0) \in E(K)$. Then P_0 is a point of order 3 if and only if

$$x_0^4 - 2a_4x_0^2 - 8a_6x_0 + (a_4^2 - 4a_2a_6) = 0$$

In particular, if $x_0 = 0$, then $P_0 = (0, y_0)$ is a point of order 3 if and only if $a_4^2 - 4a_2a_6 = 0$.

Proof. To check if P_0 is a point of order 3, we compute $x(2P_0)$ and set it equal to $x(P_0)$. Knowing that $x(2P_0) = x(P_0)$ allows us to deduce that $2P_0 = \pm P_0$. Furthermore, $2P_0 = P_0$ can only happen if P_0 is the identity; thus, if P_0 is a nonidentity point and $x(P_0) = x(2P_0)$, then $2P_0 = -P_0$ so P_0 is necessarily a point of order 3. This gives us the first equation.

Specializing to $x_0 = 0$, the criterion is equivalent to the vanishing of the constant term; so a point of the form $P_0 = (0, y_0)$ has order 3 if and only if $a_4^2 - 4a_2a_6$.

□

Lemma 5.2. *Let E/K be an elliptic curve and let $P \in E(K)$ be a point of order 3. If $j(E) \neq 0$, there exists an isomorphism $E \to E_{a,b}$, where $E_{a,b}/K$ is an elliptic curve given by an equation of the form:*

$$\text{(X3)} \qquad E_{a,b}: \quad y^2 = x^2 + a(x-b)^2 \quad (a, b \in K)$$

Furthermore, the isomorphism takes the point $P \in E(K)$ to the point $(0, b) \in E_{a,b}(K)$.

Proof. Since K does not have characteristic 2, we may assume E is given by an equation of the form:

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

After a change of variable $x \mapsto x + t$, we may assume $x(P_0) = 0$. By the previous lemma, the coefficients a_2, a_4, a_6 must satisfy $a_4^2 - 4a_2a_6 = 0$.

- Suppose $a_2 = 0$. Then $a_4^2 - 4a_2a_6 = a_4^2 = 0$, so $a_4 = 0$. Thus the equation for E has the form:

$$y^2 = x^3 + a_6$$

Any equation of this form has j-invariant equal to 0.
- Otherwise $a_2 \neq 0$. This means $a_2x^2 + a_4x + a_6$ is a quadratic polynomial, and the vanishing of $a_4^2 - 4a_2a_6$ encodes the fact that this polynomial is a square. Thus, we can factor the quadratic as:

$$a_2x^2 + a_4x + a_6 = a\left(x^2 + \frac{a_4}{a_2} + \frac{a_6}{a_2}\right) = a(x-b)^2$$

where $a = a_2$ and b is the root of the quadratic.

Thus the equation of E has the form:

$$y^2 = x^3 + a(x-b)^2 \tag{7}$$

□

There are two reasons we want to work with equations of the form X3:

- It is very easy to find the other points of order 3 if our equation has this form.
- It is very easy to describe the 3-isogenous curve using this equation - if E is described by an equation with coefficients (a, b), the isogenous curve will be given by a similar equation with coefficients $(-27a, 4a + 27b)$.

Now, the algorithm is going to work differently depending on $p \pmod 3$ - when $p \equiv 2 \pmod 3$, we have to be extra careful with the $j = 0$ curve, but we can avoid having to search for a point of order 3 on our first elliptic curve.

When $p \equiv 2 \pmod 3$:

- $j = 0$ is a supersingular j-invariant.
- There is one 3-isogeny from the $j = 0$ curve to itself, and there are three 3-isogenies from the $j = 0$ curve to the $j = -12288000$ curve.
- The $j = -12288000$ can be described by the following nice model:

$$E_1 : \quad y^2 = x^3 - 162(x+3)^2$$

Thus, we can jump to the loop in steps (4-6) of the algorithm for these primes. Furthermore, if () is a nonsquare, then () is supersingular and the polynomial () factors as: Thus, we can obtain a point of order 3 by solving a quadratic equation. Otherwise, we have to either use the quartic formula, or search for a root of ().

(1) First, find a model for some supersingular $E_0/\mathbb{F}_p$.

(2) Next, we need to find a 3-torsion point on:

$$E_0 : \quad y^2 = x^3 + fx + g$$

This means we need to find a root of:

$$3x^4 + 6fx^2 + 12gx - f^2 = 0$$

If $f, g \in \mathbb{F}_p$ and $p \equiv 2 \pmod 3$, this polynomial is guaranteed to have exactly 2 roots in $\mathbb{F}_p$, one of which gives rise to a 3-torsion point on $E_0(\mathbb{F}_q)$, and the other representing a 3-torsion point on $E_0^{-1}(\mathbb{F}_q)$.

We search $\mathbb{F}_p$ for a root x_0 of the quartic; once we find x_0, we have to determine whether $x_0^3 + fx_0 + g$ has a square root in $\mathbb{F}_p$ or not. If $x_0^3 + fx_0 + g$ is a square in $\mathbb{F}_p$, then we've found a 3-torsion point on $E_0(\mathbb{F}_p)$; otherwise, we have a 3-torsion point on $E_0^{-1}(\mathbb{F}_p)$. In the latter case, we can always replace E_0 with E_0^{-1} to avoid searching for the other root of the quartic in $\mathbb{F}_p$. *Note that we don't actually need to find a square root - we only need the x coordinate of the 3-torsion point, and we need to make sure we're working the correct model, which may be E^{-1} $x_0^3 + fx_0 + g$ is a nonsquare.*

(3) Once we find such a root, say x_0, we have to compute the nice model. In this case, we start by doing a change of variable so that x_0 is at 0. This give us an equation of the form:

$$y^2 = x^3 + c_0x^2 + c_1x + c_2$$

where:

Now, this equation initially seems more complicated than the one we started with - but as mentioned in: (CITE MATT DELONG PAPER)

once we've moved the x-coordinate of P_0 to 0, the condition that P_0 is a point of order 3 is encoded in the fact that the right-hand side can be factorized as:

$$y^2 = x^3 + a_0(x - b_0)^2$$

Obtaining a_0, b_0 from c_0, c_1, c_2 is completely straightforward - $a_0 = c_0$ and $b_0 =$

(4) Next, we need to obtain the other torsion points. This is where we need to compute cube roots, as we need to solve the equation:

$$x\left(12ab^2 - 12abx + 4ax^2 + 3x^3\right) = 0$$

The root $x = 0$ corresponds to the torsion point P_0 that we already have. The other three roots are obtained by solving:

$$12ab^2 - 12abx + 4ax^2 + 3x^3 = 0$$

Now, this cubic can be solved easily using the cubic formula, as long as we can compute cube roots easily. Specifically, if we can find a cube root:

$$\rho = \frac{2}{9}\sqrt[3]{-2a^2(4a+27b)}$$

then the roots of the cubic are ξ_1, ξ_2, ξ_3:

$$\begin{aligned} \xi_1 &= \frac{-4a}{9} + \rho + \frac{4a(4a+27b)}{81\rho} \\ \xi_2 &= \frac{-4a}{9} + \omega\rho + \frac{4a(4a+27b)}{81\omega\rho} \\ \xi_3 &= \frac{-4a}{9} + \omega^2\rho + \frac{4a(4a+27b)}{81\omega^2\rho} \end{aligned}$$

where $\omega \in \mathbb{F}_{p^2}$ is a primitive cube root of unity. Thus, we can obtain three additional nice models $(a_1, b_1), (a_2, b_2), a_3, b_3)$ corresponding to each of these points of order 3.

(5) Once we have $(a_0, b_0), (a_1, b_1), (a_2, b_2)$, we compute $(a_i', b_i') = (-27a_i, 4a_i + 27b_i)$ for $i = 0, 1, 2, 3$.

(6) Finally, to decide whether (a_i', b_i') represents a new curve, we compute the j-invariant and compare it to the list of j-invariants that we've already found.

5.2. Isogeny grahs for $\ell = 5, 7, 11, 13$.

5.3. Multiple Isogeny Graphs.

Given the following input:

- A prime $p > 3$.
- A primitive root $g \in \mathbb{F}_{p^2}\times$.
- An equation describing a supersingular curve $E_0/\mathbb{F}_{p^2}$.

the algorithm computes the following:

- The complete set of supersingular j-invariants.
- The ℓ-isogeny graph for all primes $\ell | \gcd(p^2 - 1, 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13)$.

in $\mathcal{O}(p^2)$ time.

(1) Compute the powers g^i for $i = 1, 2, .., p^2 - 1$, and keep a record of the discrete logarithms of every $\mathbb{F}_{p^2}^\times$ in a hash table. It is also helpful to make a hash table that records the powers of g, so that we can look them up in constant time in the future, rather than having to compute them again. This step requires us to compute $p^2 - 1$ products in $\mathbb{F}_{p^2}$, so it contributes $\mathcal{O}(p^2)$ to the overall complexity.

Note that once we've constructed these tables, we can do the following in constant time:

- Compute nth roots.

- Compute powers of g.
- Solve polynomials of degree 2, 3, 4.

(2) Compute the 2-isogeny graph using ().

This is fast - we have to solve $< \frac{p}{12}$ quadratics, and we can solve those in constant time using our hash table.

Note that we now also have the set of supersingular j-invariants.

(3) Compute the 3-isogeny graph.

- If $p \equiv 2 \pmod 3$, it is important to do the $j = 0$ curve first, as we did above.
- If $p \equiv 1 \pmod 3$, then $j = 0$ is not supersingular. On the one hand, this means we don't have to worry about supersingular curves which don't admit nice models; however, that also means we have to do some work to get started. To compute the 3-isogeny graph, we do the following:
  - First, find a point of order 3 in $E_0(\mathbb{F}_{p^2})$ (or $E_0^{-1}(\mathbb{F}_{p^2})$, if E_0 is defined over $\mathbb{F}_p$). We can do this by finding a root of the corresponding division polynomial, which has degree 4. This can be done in constant time using the quartic formula, or in $\mathcal{O}(p^2)$ time by simply searching for a root.
  - Next, find a "nice" model for E_0 using the 3-torsion point we just found, and use the algorithm.

(4)
- If $p \equiv \pm 1 \pmod 5$, we can compute the 5-isogeny graph over $\mathbb{F}_{p^2}$:
  - For each $t \in []$, compute $j_5(t)$.
  - If $j_5(t)$ is supersingular, compute $j_5'(t)$ and record the edge of the 5-isogeny graph.

  Note that this loop can stop as soon as we've found all of the edges we need.
- If $p \equiv 2 \pmod 5$, we can compute the graph if we iterate over $\mathbb{F}_{p^4}$ instead, but we're not including this case in the algorithm.

(5) (If $p \equiv \pm 1 \pmod 7$): For each t:

- Compute $f(t)$.
- Compute $j(f(t))$.
- If $j(f(t))$ is supersingular, compute $j'(f(t))$ and record the edge.

(6) (If $p \equiv \pm 1 \pmod{11}$):

THis is the most difficult part, becasue we do not have a fundamental domain.

(a) Construct a hash table that records which values of z we still need to check.

(b) For $z \in \mathbb{F}_{p^2} - \{0, 1\}$, we plug z_0 into the equation:

$$w^2 - w = z_0^3 - z_0^2$$

(c) Find the set of roots w_i of this quadratic in $\mathbb{F}_{p^2}$. If the quadratic has no roots, move on.

(d) Otherwise, we either have one point of order 2 with $z(P) = z$, or two points P_1, P_2 with $z(P_i) = z$. For each point we've found, we do the following:

- Compute the orbit of the point, and record the z-values of the points in the orbit.
- Compute the j-invariant of the curve associated to the point.
- If the j-invariant is supersingular, compute j' and record the edge.

(7) Finally, if $p \equiv \pm 1 \pmod{13}$, we do the following: for each $t \in$:

- Compute $f(t)$.
- Plug $f(t)$ into equation for $X_1(13)$.
- If the quadratic in w has a root, then we've found up to two points on $X_1(13)$, but they lie in the same α orbit, so we only need to use one of them. We compute j, and if supersingular, compute j' and record the edge.

References

[1] Houria Baaziz. Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points. 79(272):2371–2386, October 2010.

[2] Denis Charles and Kristin Lauter. Computing modular polynomials. *LMS J. Comput. Math.*, 8:195–204, 2005.

[3] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[4] Daeyeol Jeon. Automorphism groups of hyperelliptic modular curves. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 91(7), 2015.

[5] J.-F. Mestre. The method of graphs. Examples and applications. Class numbers and fundamental units of algebraic number fields, Proc. Int. Conf., Katata/Jap. 1986, 217-242 (1986)., 1986.

[6] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.

[7] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[8] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[9] Andrew V. Sutherland. Computing hilbert class polynomials with the chinese remainder theorem. *Math. Comput.*, 80:501–538, 2009.

[10] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.