SUPERSINGULAR ISOGENY GRAPHS FROM ALGEBRAIC MODULAR CURVES

NADIR HAJOUJI

Abstract. We describe algorithms for computing supersingular ℓ-isogeny graphs. The difficult step in these algorithms is finding all $\mathbb{F}_{p^2}$-points on an algebraic model of $X_0(\ell)$. We describe explicit models of $X_0(\ell)$, as well as algorithms for finding the $\mathbb{F}_{p^2}$ points of $X_0(\ell)$, for all primes $\ell \leq 13$. The algorithms we describe were used to compute all supersingular isogeny graphs for all pairs (p, ℓ) with $p \leq 4096$ and $\ell \leq 13$.

1. Introduction

Given a pair of primes p, ℓ, with $p \neq \ell$, we are interested in the following problems:

(1) Computing the set of supersingular j-invariants.
(2) Computing the supersingular ℓ-isogeny graphs.

There are already algorithms for computing these graphs, see e.g. [3, 7]. These algorithms work for all pairs p, ℓ, but they require one to find explicit generators of the ℓ-torsion subgroup, which requires solving polynomials of high degree. Our approach is more similar to the algorithm described in section 3.2 of [13]: we obtain all of the data we need by finding points on an appropriate modular curve that represent supersingular elliptic curves. However, [13] uses the modular curves $X_1(\ell)$, whereas we will be using the modular curves $X_0(\ell)$. This change is significant, as it will allow us to do all of our computations in $\mathbb{F}_{p^2}$: while supersingular curves $E/\mathbb{F}_{p^2}$ may fail to have *any* points of order ℓ defined over $\mathbb{F}_{p^2}$, we will show that the *subgroups* of order ℓ are always defined over $\mathbb{F}_{p^2}$. The main difficulty is obtaining models of the modular curves, together with formulas for the j-maps and formulas for isogenous curves.

In Section 2, we prove results about the field of definition of isogenies between supersingular elliptic curves. Next, we give compute algebraic models of $X_0(\ell)$ for $\ell = 5, 7, 11, 13$, by first obtaining a model of $X_1(\ell)$, and then constructing $X_0(\ell)$ as a quotient of $X_1(\ell)$ in Section 3 In Section 4, we describe explicit algorithms for computing isogeny graphs for all $\ell \leq 13$. Finally, in Section 5, we explain how to use our models of $X_0(\ell)$ to do computations related to the conjectures of Nakaya in [9].

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:

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

  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}.

[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.

- $x^3 + fx + g$ 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:

$$x^2 + p$$

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:

$$(x - p)^2$$

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

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 [15] or [10].

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 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2$ or it is congruent to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \pmod 2$. 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 [4], e.g. Furthermore, it is not hard to produce explicit examples of supersingular curves $E/\mathbb{F}_p$ for a fixed prime p. We discuss this further in Subsection ()

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 $a = 0 \pmod{\ell}$.

□

2.3. **Application: Computing Supersingular Isogeny Graphs.** When $p \equiv \pm 1 \pmod{\ell}$, we can find models for every supersingular j-invariant that have full ℓ-torsion over $\mathbb{F}_{p^2}$, so we can compute the supersingular isogeny graph over $\mathbb{F}_{p^2}$ in this case. Now, if $p \neq \pm 1 \pmod{\ell}$, then supersingular curves over $\mathbb{F}_{p^2}$ do not contain *points* of order ℓ - however, the *subgroups* of order ℓ will always be defined over $\mathbb{F}_{p^2}$! We've proven that Frobenius acts on supersingular elliptic curves as multiplication-by-$\pm[p]$. Now, this map does not fix torsion points, but it fixes cyclic subgroups setwise. Thus, any isogeny $E \to E'$ between supersingular elliptic curves with cyclic kernel is necessarily defined over $\mathbb{F}_{p^2}$.

Consequently, we can compute supersingular ℓ-isogeny graphs if we have the following:

- A single supersingular j-invariant $j_0 \in \mathbb{F}_{p^2}$.
- A model of the modular curve $X_0(\ell)$.
- Formulas $j_\ell, j'_\ell : X_0(\ell) \to X(1)$, where $j_\ell(P)$ is the j-invariant of the domain of the isogeny represented by P, and $j'_\ell(P)$ is the j-invariant of the codomain of the isogeny represented by P.

To obtain the ℓ-isogeny graph, including the complete set of supersingular j-invariants, we simply have to do the following:

(1) Compute the set $X_0(\ell)(\mathbb{F}_{p^2})$.
(2) For each $P \in X_0(\ell)(\mathbb{F}_{p^2})$, we compute and store the edge $(j_\ell(P), j'_\ell(P))$.
(3) We now know the complete ℓ-isogeny graph for ℓ - to obtain the supersingular isogeny graph, we simply compute the connected component of j_0.

Furthermore, once we've computed one isogeny graph this way, we know the complete set of supersingular j-invariants. To compute additional isogeny graphs, we can then use the following simpler algorithm:

(1) Compute the set $X_0(\ell)(\mathbb{F}_{p^2})$.
(2) For each $P \in X_0(\ell)(\mathbb{F}_{p^2})$, we compute $j_\ell(t)$. If $j_\ell(t)$ is supersingular, we compute $j'_\ell(P)$ and store the edge $(j_\ell(P), j'_\ell(P))$.

For general values of ℓ, the problem of computing all points on $X_0(\ell)$ can take $\mathcal{O}(p^4)$ time. However, for small values of ℓ, we can compute all $\mathbb{F}_{p^2}$ points on $X_0(\ell)$ in $\mathcal{O}(p^2)$, so the algorithm is straightforward as long as we can obtain the formulas required, and we can find a supersingular $j_0 \in \mathbb{F}_{p^2}$. We derive models of $X_0(\ell)$, together with formulas for the maps j_ℓ, j'_ℓ, in the next section.

3. Algebraic Models of Modular curves

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 $\mathbb{A}^2 = \operatorname{Spec} \mathbb{Z}[u, v]$ 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 $\mathcal{E}_{u,v} \times \operatorname{Spec} K$, 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 as a model for a plane curve $C_\ell \subset \mathbb{A}^2$ which is birational to $X_1(\ell)$. We will find maps

[3] See, e.g., Ex. 8.13 in [11].

$X_1(\ell) \to C_\ell$ 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 $i_\ell : X_1(\ell) \to \mathbb{A}^2$.

We can obtain maps $j_{\ell,1} : X_1(\ell) \to X(1)$ that give us the j-invariant of a point represented by a point on $X_1(\ell)$ by composing $X_1(\ell) \to \mathbb{A}^2$ with the j-invariant of $\mathcal{E}_{u,v}$. Furthermore, we can determine j-invariants of isogenous curves by applying Velu's formula to the elliptic surface over $X_1(\ell)$, and then computing the j-invariant of the elliptic surface we obtained.

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.

We will obtain models of $X_0(\ell)$ by taking the quotient of $X_1(\ell)$ by the group of automorphisms generated by the restriction of $\alpha_{\mathcal{E}}$ to $X_1(\ell)$.[4] We obtain the maps $j_\ell, j'_\ell : X_0(\ell) \to X(1)$ by finding maps on $X_0(\ell)$ that pull back to the correct function on $X_1(\ell)$.

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:

$$X_0(\ell) \to X_0(\ell) \qquad \tau \mapsto \frac{-1}{\ell\tau}$$

takes a point τ that represents an isogeny $E \to E'$ to the point that represents the dual isogeny $E' \to E$. We will obtain algebraic analogs of these involutions for the modular curves we obtain.

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

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

$$2P_0 = (v, uv) \qquad 3P_0 = (u, v-u)$$
$$-P_0 = (0, v) \qquad -2P_0 = (v, 0)$$

[4]Note that 2 is not a primitive element of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ for all values of ℓ we are considering, but it *is* a generator of $(\mathbb{Z}/\ell\mathbb{Z})^\times / \langle \pm 1 \rangle$ for $\ell = 5, 7, 11, 13$.

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 $j_{5,1} := j_{\mathcal{E}} \circ i_5$:

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

To obtain the j-invariant of the isogenous curve, we apply Velu's formula ([14]) on the entire family of elliptic curves 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:

$$j_{5,1}'(t) = \frac{\left(t^4 + 228t^3 + 494t^2 - 228t + 1\right)^3}{t\left(t^2 - 11t - 1\right)^5} \tag{J5.1'}$$

3.1.1. *Quotient.* To obtain the map $X_1(5) \to X_0(5)$, we need to find the automorphism of $X_1(5)$ that takes a point $t_1 \in X_1(5)$, that represents a pair (E,P), to the point $t_2 \in X_1(5)$ that represents $(E,2P)$. This is easy: the automorphism of $X_1(5)$ is $t \mapsto \frac{-1}{t}$, and so $X_0(5) = X_1(5)/\left\langle t \mapsto \frac{-1}{t}\right\rangle$. The function $t + \frac{-1}{t}$ is clearly invariant under this automorphism, so we use it to construct a quotient map $X_1(5) \to X_0(5)$:

$$q_5(t) = \frac{t^2 - 11t - 1}{t} \tag{Q5}$$

Note that the quotient map has been constructed to ensure the I_5 cusp gets sent to the point at infinity, and the I_1 cusp gets sent to the point 0 on $X_0(5)$.

To obtain the map $j_5 : X_0(5) \to X(1)$, we do the following:

- The poles of j_5 are at $0, \infty$ by construction: one can check that the map q_5 takes the cusps of $X_1(5)$ to $0, \infty$ on $X_0(5)$.
- We compute the zeros of $j_{5,1}$, and use the map q_5 to determine what the zeros of j_5 should be.
- Once we know the zeros and poles of j_5, the function is determined up to a scalar multiple. We can ensure we have the correct scalar by evaluating $j_{5,1}$ at a random point which is not a zero or pole.

The end result is:

$$j_{5,0}(t) = \frac{(t^2 + 10t + 5)^3}{t} \tag{J5.0}$$

One can check that $j_{5,1}(t) = j_{5,0} \circ q_5(t)$. Furthermore, note that $j'_{5,1}(t) = j_{5,0} \circ q_5(\frac{125}{t})$, so we no longer need to use Velu's formula.

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, and the modular curve $X_1(7)$ is the normalization of this curve. We write $i_7 : X_1(7) \to \mathbb{A}^2$ to denote the composition of the normalization map $X_1(7) \to C_7$ with the inclusion $C_7 \to \mathbb{A}^2$:

$$i_7(t)(t^2 - t, t^3 - t^2) \tag{I7}$$

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

$$y^2 + (1 + t - t^2)xy + t^2(1 - t)y = x^3 + t^2(1 - t)x^2 \tag{E7}$$

We compute $j_{7,1} = j_{\mathcal{E}} \circ i_7$:

$$j_{7,1}(t) = \frac{(t^2 - t + 1)^3 (t^6 - 11t^5 + 30t^4 - 15t^3 - 10t^2 + 5t + 1)^3}{t^7(t - 1)^7 (t^3 - 8t^2 + 5t + 1)} \tag{J7.1.1}$$

We can compute the formula for $j'_7(t)$ by applying Velu's formula to the universal elliptic curve, and computing the j-invariant of the result:

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

3.2.1. *Quotient.* To obtain a model of $X_0(7)$, we take the quotient of $X_1(7)$ by the automorphism:

$$\alpha_7(t) = \frac{1}{1-t} \tag{A7}$$

$t \mapsto \frac{1}{1-t}$. Finding a function invariant under this action is straightforward (e.g. take the sum of the orbit). We construct our quotient map $X_1(7) \to X_0(7)$ so that the I_7 singularity is at ∞ and the I_1 singularity is at 0:

$$q_7(t) = \frac{t^3 - 8t^2 + 5t + 1}{(1-t)t} \tag{Q7}$$

The map $j_7 : X_0(7) \to X(1)$ is:

$$j_{7,0}(t) = -\frac{(t^2 - 13t + 49)\,(t^2 - 5t + 1)^3}{t} \tag{J7.0}$$

The Fricke involution swaps the I_1, I_7 cusps of $X_0(7)$, so it has the form $t \mapsto \frac{a}{t}$ for some a. We can compute a by determining the j-invariant of the isogenous curve of a random point using the formulas for $X_1(7)$:

$$\beta_{7,0}(t) = \frac{49}{t} \tag{B7.0}$$

Thus:

$$j'_{7,0}(t) = -\frac{(t^2 - 245t + 2401)^3\,(t^2 - 13t + 49)}{t^7} \tag{J7.0.2}$$

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 $C_{11} \subset \mathbb{A}^2$. We obtained a nice model of $X_1(11)$, and a map $X_1(11) \to \mathbb{A}^2$, using methods described in [1]. The model for $X_1(11)$ is:

$$w^2 - w = z^3 - z^2 \tag{X11.1}$$

To compute j-invariants, we use the map $i_{11} : X_1(11) \to \mathbb{A}^2$:

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

3.3.1. *Quotient.* 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

$Aut(X_1(11)/X_0(11))$, so the quotient map $X_1(11) \to X_0(11)$ is an isogeny of degree 5, and can be computed using Velu's formula. The equation for $X_0(11)$ is:

(X11.0) $$y^2 - y = x^3 - x^2 - 10x - 20$$

The map $X_1(11) \to X_0(11)$ is:

(Q11) $q_{11}(z, w) =$

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

To obtain the map $j_{11,0}$, we compute the zeros and poles of $j_{11,1} = j_{\mathcal{E}} \circ i_{11}$, and use the map Q11 to determine the zeros and poles of $j_{11,0}$. This determines $j_{11,0}$ up to a scalar multiple. We then compute compute $j_{11,1}$ at a point that is not a zero or pole to determine the correct scalar.

The kernel of the isogeny coincides with the I_{11} locus, so $X_0(11)$ has an I_{11} fiber over the point at infinity. On the other hand, the I_1 fibers are mapped to the point $P = (16, 61)$ on $X_0(11)$. Thus, $j_{11,0}$ should have a pole of order 11 at infinity, and a pole of order 1 at $(16, 61)$.

Furthermore, $j_{11,0}$ has zeros of order 3 at the 4 points:

$$P_1 = \left(\sqrt{33} - \sqrt{2\sqrt{33} + 11} + 5, 3\sqrt{33} - 5\sqrt{2\sqrt{33} + 11} + 17\right)$$
$$P_2 = \left(\sqrt{33} + \sqrt{2\sqrt{33} + 11} + 5, 3\sqrt{33} + 5\sqrt{2\sqrt{33} + 11} + 17\right)$$
$$P_3 = \left(-\sqrt{33} + i\sqrt{2\sqrt{33} - 11} + 5, -3\sqrt{33} + 5i\sqrt{2\sqrt{33} - 11} + 17\right)$$
$$P_4 = \left(-\sqrt{33} - i\sqrt{2\sqrt{33} - 11} + 5, -3\sqrt{33} - 5i\sqrt{2\sqrt{33} - 11} + 17\right)$$

Note that $P_1 + P_2 + P_3 + P_4 = (5, 6)$, which is a point of order 5. Define $P_i' = P_i + (5, 6)$. Then $\sum P_i' = 0$, so we can find a function that vanishes on P_1', P_2', P_3', P_4':

$$32x^2 + 48x + 120y - 429$$

This allows us to obtain the function:

$$217 + 140x - 114x^2 + 12x^3 + x^4 - 32y + 40xy - 8x^2y$$

which has a zero of order 1 at the 4 points $P_1, .., P_4$, and a zero of order 4 at $(5, 6)$. To obtain the j-map, all we have to do is make sure we have the correct zeros and poles over the points

of order 5, which is much easier. The following function has the correct zeros and poles:

$$j_{11,0}(x,y) = \frac{\left(x^4+12x^3-8x^2y-114x^2+40xy+140x-32y+217\right)^3}{(-5x+y+19)\left(4x^2-xy-29x+4y+51\right)^2} \tag{J11.0}$$

Furthermore, $j_{11,0} \circ q_{11} = j_{\mathcal{E}} \circ i_{11}$ at points which are not zeros or poles,.

Now, this function has a pole at $(16, 61)$, because that point is a cusp of $X_0(11)$. However, we note that the numerator and denominator both vanish at the point $(5, 6)$, even though it is not a cusp. By finding points on $X_1(11)$ that lie over $(5, 6)$, we compute the j-invariant of the curve represented by $(5, 6)$ to be -121.

To compute the j-invariant of the isogenous curve, we just evaluate the j-invariant of $(16, 61) - P$, where the difference is computed using the group law. Explicitly, the image of a point (x, y) on $X_0(11)$ under this involution is given by:

$$(x,y) \mapsto \left(\frac{16x^2+214x+121y-260}{(x-16)^2}, \frac{61x^3+2759x^2+726xy-3730x+3025y-18020}{(x-16)^3}\right)$$

Note that $(16, 61) - (5, 6) = (16, -60)$; the j-invariant of the curve represented by $(16, -60)$ is $-11 \cdot 131^3$, so this tells us that the curves with $j = -11^2, -11 \cdot 131^3$ are related by an isogeny of degree 11 defined over $\mathbb{Q}$. Similarly, $(16, 61) - (5, -5) = (5, -5)$, so the curve represented by $(5, -5)$ has an isogeny of degree 11 to itself. Of course, this means $(5, -5)$ represents the elliptic curve over $\mathbb{Q}$ that has complex multiplication by $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$, which has j-invariant -2^{15}. In practice, it is easiest to just use these precomputed values to avoid having to compute analytic continuations.

3.4. $\ell = 13$**.** The curve $X_1(13)$ can be described by the following model [6]:

$$w^2 + wz^3 + wz^2 + w - z^2 - z = 0 \tag{X13}$$

To compute j-invariants on this curve, we use the map $i_{13} : X_1(13) \to \mathbb{A}^2$:

$$i_{13}(z,w) = \left(\frac{wz(wz-w-1)}{w+1}, \frac{wz(1-wz)(wz-w-1)}{w+1}\right) \tag{I13}$$

We define $j_{13,1} := j_{\mathcal{E}} \circ i_{13}$.

3.4.1. *Quotient Map.* 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 [6]. 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.

Explicit formulas for the generators of the automorphism group are computed in [6]. We only need the automorphism of order 6 to compute $X_0(13)$:

$$\alpha_{13}(z,w) = \left(\frac{-1}{1+z}, \frac{w-z}{z+z^2-w}\right) \tag{A13}$$

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:

$$q_{13} : X_1(13) \to X_0(13) \qquad q_{13}(z,w) = \frac{z^3+4z^2+z-1}{z(z+1)} \tag{Q13}$$

$$j_{13,0}(t) = -\frac{(t^2-5t+13)\left(t^4-7t^3+20t^2-19t+1\right)^3}{t} \tag{J13.0}$$

Finally, the Fricke involution on this model of $X_0(13)$ is given by:

$$\beta_{13}(t) = \frac{13}{t} \tag{B13.0}$$

We compose to obtain:

$$j'_{13,0}(t) = -\frac{(9t^2+3t+1)\left(5573t^4+61t^3+512t^2-231t+1\right)^3}{t(4t+1)^{13}} \tag{J13.0.2'}$$

4. Algorithms

In this section, we describe explicit algorithms for computing the supersingular isogeny graph for all $\ell \leq 13$.

We start by describing our algorithm for computing ℓ-isogeny graphs for $\ell = 2, 3$. For these values of ℓ, we essentially use an optimized version of the algorithm described in [3],[7].

- To use these algorithms, we need the ability to compute ℓth roots in $\mathbb{F}_{p^2}$, so we can solve polynomials of degree ℓ.
- The algorithm for $\ell = 2$ runs faster than every other algorithm. We will obtain the set of supersingular j-invariants by computing the 2-isogeny graph.
- Once we have the set of supersingular j-invariants, we can compute the remaining isogeny graphs by finding all points on $X_0(\ell)$ where the value of $j_{\ell,0}$ is supersingular.

4.1. $\ell = 2, 3$.

4.1.1. *Models for $\ell = 2, 3$.* We start by describing models we will use to describe pairs (E, P) where $P \in E(K)$ is a point of order $\ell \in \{2, 3\}$. See [11],[12] for more on the 2-torsion models, and [5] for more on the 3-torsion models.

Lemma 4.1. *Let K be a field of characteristic not equal to 2,3, and let (E, P) be a pair consisting of an elliptic curve E/K and a point $P \in E(K)$ of order $\ell \in \{2, 3\}$.*

- *If $\ell = 2$, there is a model for (E, P) of the form:*

$$y^2 = x(x^2 + ax + b) \qquad P = (0, 0) \tag{E2}$$

- *If $\ell = 3$ and $j(E) \neq 0$, there is a model for (E, P) of the form:*

$$y^2 = x^3 + a(x - b)^2 \qquad P = (0, b) \tag{E3}$$

Proof. We may assume that E is given by a Weierstrass equation of the form:

$$y^2 = x^3 + ax^2 + bx + c$$

Furthermore, applying a change of variable $x \mapsto x - x(P)$ if necessary, we may assume that $x(P) = 0$ and $y(P)^2 = c$. The point $(0, \sqrt{c})$ has order 2 if and only if $c = 0$; this proves the lemma for $\ell = 2$.

For $\ell = 3$, we have $P = (0, y_0) \in E(K)$ so we can write the equation for E as:

$$y^2 = x^3 + ax^2 + b_0x + y_0^2$$

for some $a, b_0 \in K$. Assume $a = 0$ and $(0, y_0)$ has order 3. A computation shows that this is only possible if $b_0 = 0$, so E has the form:

$$y^2 = x^3 + y_0^2$$

Note that this elliptic curve has j-invariant 0. Thus, if $j(E) \neq 0$, we can find an equation for E of the form:

$$y^2 = x^3 + ax^2 + b_0x + y_0 \quad (a \neq 0)$$

A computation shows that $(0, y_0)$ is a point of order 3 if and only if the quadratic:

$$ax^2 + b_0x + y_0$$

has a repeated root. Denoting that root by b, we see that the equation of E has the form:

$$y^2 = x^3 + a(x - b)^2$$

as claimed.

□

Now, given a pair of coefficients of this form, we will do two things:

- There are ℓ other pairs (a_i, b_i) that represent (E, P_i), where E is the elliptic curve represented by (a_0, b_0) and $P_i \neq P_0$ is a point of order ℓ. We can obtain these other pairs from (a_0, b_0), as long as we have the ability to compute ℓth roots in $\mathbb{F}_{p^2}$.
- We will obtain coefficients $(a_i,', b_i')$ for the isogenous curves.

Both of these steps are essentially accomplished by evaluating formulas.

To obtain the remaining pairs (a_i, b_i) from (a_0, b_0), we need to find the points (x_i, y_i) of order ℓ for which $x_0 \neq 0$. For $\ell = 2$, the points of order 2 are $(x_1, 0), (x_2, 0)$, where x_1, x_2 are the roots of the quadratic:

$$x^2 + a_0 x + b_0 = 0$$

For $\ell = 3$: the remaining points of order 3 can be obtained by solving the cubic:

$$3x^3 + 4a_0 x^2 - 12a_0 b_0 x + 12a_0 b_0^2$$

Note that this cubic can be solved using the cubic formula, as long as we can compute cube roots in $\mathbb{F}_{p^2}$. Specifically, if we can find:

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

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

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

where $\omega \in \mathbb{F}_{p^2}$ is a primitive cube root of unity. Now, once we've found all points of order ℓ, we obtain the coefficients (a_i, b_i) that represent (E_0, P_i) by a simple change of variable. Finally, once we have all pairs (a_i, b_i) for a given elliptic curve E_0, we compute new pairs of coefficients (a_i', b_i') that represent isogenous curves using the following formulas:

$$(a', b') = \begin{cases} (-2a, a^2 - 4b) & \text{if} \quad \ell = 2 \\ (-3a, 4a^3 + 27b) & \text{if} \quad \ell = 3 \end{cases}$$

Now, we use these formulas in Algorithm 1 to obtain the 2-isogeny and 3-isogeny graphs.

4.1.2. *Getting Started: The first model.* To get started, we need a pair (a, b) that represents a supersingular curve with a point of order $\ell \in \{2, 3\}$. We can obtain such a pair as long as we have a supersingular curve, and a point of order ℓ on that curve.

Algorithm 1 Supersingular Isogeny Graphs for $\ell \in \{2, 3\}$

Require: Coefficients (a, b) of a supersingular curve with ℓ-torsion.

```
Set Edges = {}
Set Models = {(a, b)}
Set J = {}.
while Models ≠ ∅ do
    Set NewModels = {}.
    for (a_0, b_0) ∈ Models do
        Compute j_ℓ(a_0, b_0)
        if j_ℓ(a_0, b_0) ∉ J then
            Add j_ℓ(a_0, b_0) to the set J.
            Compute the remaining pairs (a_i, b_i) for i ∈ {1, .., ℓ}.
            for i ∈ {0, 1, .., ℓ} do
                Compute (a'_i, b'_i).
                Add the pair (a'_i, b'_i) to NewModels.
            end for
        end if
    end for
    Set Models = NewModels.
end while
```

For $p \not\equiv 1 \pmod{12}$, at least one of $j = 0, 1728$ is supersingular, and so finding a supersingular curve is not difficult. When $p \equiv 1 \pmod{12}$, we have to work a little harder. 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 $\mathbb{Q}(\sqrt{-d})$. Now, while finding a nonsquare is easy, the problem of finding elliptic curves with complex multiplication can be difficult if the class number of $\mathbb{Q}(\sqrt{-d})$ is big. Fortunately, for most[5] primes, one of Heegner numbers is a nonsquare in $\mathbb{F}_p$, which means we can find an elliptic curve $E/\mathbb{Q}$ whose reduction mod p is guaranteed to be supersingular. Equations for these curves can be found in Appendix of [12].

If we can find a nonsquare $d \in \{-1, -2, -3, -7\}$, then the associated elliptic curve has a 2-torsion point over $\mathbb{Q}$. This makes it easier to run Algorithm 1 for $\ell = 2$. If all of

[5]The smallest prime for which all Heegner numbers are quadratic residues is 15073. Of the first million primes, there are only 1769 primes for which all Heegner numbers are quadratic residues.

these values of d are quadratic residues, we have to find a root of a cubic in $\mathbb{F}_p$ to start the algorithm.

On the other hand, only one of these curves has a point of order 3 over $\mathbb{Q}$, namely the curve with $j = 0$. If $p \equiv 2 \pmod 3$, the curve with $j = 0$ is supersingular, and has a point of order 3 defined over $\mathbb{Q}$. Of course. Now, while this is the *only* elliptic curve that does not admit a model of the form E3, we can do the first step of the algorithm in characteristic 0:

- The elliptic curve with $j = 0$ has an isogeny of degree 3 to itself, as well as three isogenies of degree 3 to the curve with $j = -12288000$.
- The curve with $j = -12288000$ has a model of the form E3:

$$y^2 = x^3 - 162(x+3)^2$$

Thus, we can start the algorithm with $(a, b) = (-162, 3)$ when $p \equiv 2 \pmod 3$.

Furthermore, while the curves associated to $d = -2, -11$ do not have a point of order 3 over $\mathbb{Q}$, we can obtain the points of order 3 by computing square roots. To use this algorithm for $\ell = 3$ and general p, we would need to find a root of a quartic in $\mathbb{F}_{p^2}$ as our first step.

4.2. $\ell \in \{5, 7, 11\}$**.** To compute the graph for $\ell \in \{5, 7, 13\}$, we use Algorithm 2. This algorithm assumes that we've already computed the set S_p of supersingular j-invariants. As long as we've already obtained this set, all we need is the formulas for $j_{\ell,0}$ that we obtained in the previous section (J5.0,J7.0.2,J13.0). Note that the cusps are at $0, \infty$, so we can evaluate $j_{\ell,0}(t)$ at any point in $\mathbb{F}_{p^2}$ without having to worry about dividing by 0.

Algorithm 2 Supersingular Isogeny Graphs for $\ell \in \{5, 7, 13\}$

Require: $S_p = \{j \in \mathbb{F}_{p^2} : j \text{ supersingular}\}$.
  Set Edges = {}
  for $t \in \mathbb{F}_{p^2}^\times$ **do**
    Compute $j_{\ell,0}(t)$
    if $j_{\ell,0}(t) \in S_p$ **then**
      Compute $j'_{\ell,0}(t)$.
      Record the edge $(j_{\ell,0}(t), j'_{\ell,0}(t))$.
    end if
  end for

4.2.1. *Warning.* We have to be careful when $p \not\equiv 1 \pmod{12}$: we might have multiple isogenies $E \to E'$ that are represented by a single point on $X_0(\ell)$ if $j(E) \in \{0, 1728\}$.

- If $j_{\ell,0}(t) = 0$ and $j'_{\ell,0}(t) \neq 0$, the edge $(0, j'_{\ell,0}(t))$ should be recorded 3 times.

- If $j_{\ell,0}(t) = 1728$ and $j'_{\ell,0}(t) \neq 0$, the edge $(1728, j'_{\ell,0}(t))$ should be recorded twice.

4.2.2. $\ell = 3$. We can also use this algorithm for $\ell = 3$ when $p \equiv 1 \pmod 3$ without needing to compute cube roots or solve a quartic polynomial. We can use:

$$j_3(b) = -\frac{256(6b+1)^3}{b^3(27b+4)} \tag{J3}$$

$$j'_3(b) = \frac{256(54b-1)^3}{b(27b+4)^3} \tag{J3.2}$$

as a substitute for $j_{\ell,0}, j'_{\ell,0}$

4.3. $\ell = 11$**.** For $\ell = 11$, we can use the same ideas, but the process is slightly messier because $X_0(11)$ has positive genus.

Algorithm 3 Supersingular Isogeny Graphs for $\ell = 11$

Require: $S_p = \{j \in \mathbb{F}_{p^2} : j \text{ supersingular}\}$.
  Define a set Edges $= \{\}$
  for $x_0 \in \mathbb{F}_{p^2} - \{5, 16\}$ **do**
    Find all points on $(x_0, y_0) \in X_0(11)(\mathbb{F}_{p^2})$.
    for $(x_0, y_0) \in X_0(11)(\mathbb{F}_{p^2})$ **do**
      Compute $j_{11,0}(x_0, y_0)$.
      if $j_{11,0}(x_0, y_0) \in S_p$ **then**
        Compute $j'_\ell(t)$.
        Record the edge $(j_{11,0}(t), j'_{11,0}(t))$.
      end if
    end for
  end for

As with $\ell = 5, 7, 13$, we have to be careful with $j = 0, 1728$. Furthermore, the formulas don't work for the noncuspidal points of order 5; we do these computations in characteristic 0.

5. Application: Nakaya's Conjectures

Finally, we note that the formulas we've obtained for computing supersingular isogeny graphs also be used to investigate the conjectures in [9]. For example, we can obtain an

algebraic model of $X_0(13)^+$ by taking the quotient of $X_0(13)$ by the Fricke involution $t \mapsto \frac{13}{t}$. We define $q_{13}^+ : X_0(13) \to X_0(13)^+$:

$$q_{13}^+(t) = -\left(t + \frac{13}{t}\right)$$

We will use the function $q_{13}^+(t)$ as a Hauptmodul for $X_0(13)^+$. Now, an easy computation shows that $j_{13}(t) + j'_{13}(t) = a_{13}(q_{13}^+(t))$ and $j_{13}(t) \cdot j'_{13}(t) = b_{13}(q_{13}^+(t))$, where:

$$\begin{aligned} a_{13}(y) = {} & y^{13} + 26y^{12} + 156y^{11} - 1508y^{10} - 21658y^9 - 39624y^8 + 612742y^7 + 3355976y^6 \\ & - 454779y^5 - 43741490y^4 - 95939974y^3 + 41335164y^2 + 291162600y + 174668400 \end{aligned}$$

$$b_{13}(y) = (y+5)^2 \left(y^4 + 254y^3 + 5077y^2 + 34092y + 75492\right)^3$$

Now, to compute the polynomials we need the polynomials $ss_p(X)$, whose roots are the supersingular j-invariants. We computed these $ss_p(X)$ and $ss_p^{(13*)}(X)$ for all p in the range $17 \leq p \leq 2048$.

- The roots of $ss_p^{(13*)}(X)$ lie in $\mathbb{F}_{p^2}$ for all p in this range. This provides further evidence that the answer to Question 1 is *yes*.
- We also verified that conjecture 5 is true for $N = 13$ and all p between 17 and 4096.

We also obtained algebraic analogs of the Hauptmoduls for $X_0(5)^+, X_0(7)^+$:

$$j_5^*(t) = \frac{t^2 + 22t + 125}{t} \tag{J5+}$$

$$j_7^*(t) = -\frac{t^2 - 13t + 49}{t} \tag{J7+}$$

These functions satisfy the relations:

$$j_{\ell,0}(t) + j'_{\ell,0}(t) = a_\ell(j_\ell^*(t))$$

$$j_{\ell,0}(t) j'_{\ell,0}(t) = b_\ell(j_\ell^*(t))$$

where a_ℓ, b_ℓ are the polynomials in Example 1 of [9].

6. Conclusion

6.1. **Implementation and tables.** Tables containing supersingular isogeny graphs (for $p \leq 512$) and adjacency matrices (for $p \leq 2048$) were computed by implementing the algorithms in this paper using Python.

The results and code can be found at `https://github.com/nhajouji/supsingecs`.

6.2. **Generalizations.** The algorithms that we have described for primes $\ell \leq 13$ can be extended a higher values of ℓ, without changing the overall complexity of the algorithm, as long as we can find all $\mathbb{F}_q$ points on a modular curve in $\mathcal{O}(q)$ time. For example, $X_0(\ell)$ has genus ≤ 2 for all primes $\ell \leq 37$. If one has a model of $X_0(\ell)$ as a hyperelliptic curve, as well as explicit formulas for the maps $j_{\ell,0} : X_0(\ell) \to X(1)$ and $\beta : X_0(\ell) \to X_0(\ell)$, then one can compute the ℓ-isogeny graph by adapting Algorithm 3

In fact, we can go beyond $\ell = 37$: if we can find a map $X_0(\ell) \to \mathbb{P}^1$ of degree $3, 4$, then we can find all points on $X_0(\ell)$ in $\mathcal{O}(q)$ time using the cubic/quartic formula. In other words, we can extend the algorithm to all primes ℓ where $X_0(\ell)$ has gonality ≤ 4.[6] This means we can extend the algorithm to:

$$\ell \in \{43, 67, 73, 103, 107\}$$

Note that $X_0(43)$ has gonality 3, and $X_0(\ell)$ has gonality 4 for the remaining values of ℓ [8].

We can also find points on bielliptic curves in $\mathcal{O}(q)$:

- First, find all points on the elliptic curve.
- Next, find all points on the double cover of the elliptic curves.

The curve $X_0(\ell)$ is bielliptic for the following prime values of ℓ [2]:

$$37, 53, 61, 79, 83, 89, 101, 131$$

We could, in theory, extend the algorithm even further: if we have a map $X_0(\ell) \to \mathbb{P}^1$ with the property that the corresponding field extension $K(X_0(\ell))/K((\mathbb{P}^1)$ is solvable, then we can in principle obtain the points on $X_0(\ell)$ in $\mathcal{O}(q)$, although it is not clear whether there are any values of ℓ for which this is true other than the values we've already listed.

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] Francesc Bars. Bielliptic modular curves. *Journal of Number Theory*, 76(1):154–165, May 1999.

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

[6] The idea of using gonality of the modular curve as a threshold appears in [13], but they use the modular curves $X_1(\ell)$ instead of $X_0(\ell)$. However, the values of ℓ for which $X_1(\ell)$ has gonality ≤ 4 are precisely the values of ℓ for which $X_0(\ell)$ has genus ≤ 2.

[4] 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.

[5] Matt Delong. A formula for the selmer group of a rational three-isogeny. *Acta Arithmetica*, 105:119–131, 1999.

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

[7] 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.

[8] Filip Najman and Petar Orlić. Gonality of the modular curve $x_0(n)$, 2022.

[9] Tomoaki Nakaya. The number of linear factors of supersingular polynomials and sporadic simple groups. *Journal of Number Theory*, 2018.

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

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

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

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

[14] J. Velu. Isogenies entre courbes elliptiques. *Comptes-Rendus de l'Academie des Sciences*, 273:238–241, 1971.

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