Lifted Elliptic Curve Isogeny Graphs

Honours Project

Shai Levin
sbl57@uclive.ac.nz

September 2021

Acknowledgements

Foremost, I would like to thank my supervisor Prof. Felipe Voloch for providing this motivating research topic, and for his limitless support and guidance in the drafting of this project.

Contents

0 Introduction

The rise of quantum computing has led to the search for cryptographic primitives which are not vulnerable to quantum-based attacks. One of leading approaches to constructing quantum resistant cryptographic protocols is by using random walks on isogeny graphs. Loosely stated, isogeny graphs are formed with elliptic curves as vertices, and isogenies between them as edges. Computing isogenies between elliptic curves is believed to be a strong cryptographic primitive. The security of most of these protocols, such as CSIDH [1], is loosely based on the hardness of the following problem:

(Path Finding in Isogeny Graphs) *Given the supersingular ℓ-isogeny graph over a finite field, and two random j-invariants of elliptic curves $j(E)$, $j(E')$, find a path in the isogeny graph joining them.*

In the case of CSIDH, the $\mathbb{F}_p$ *restricted supersingular isogeny graph* is used. Several variations on this path problem exist. For instance, SIDH[2], is based on a more constrained problem. Due to the reliance on this path problem, a great deal of importance lies in characterising the random walks on isogeny graphs. We shall see later that the hardness of this problem is closely related to the fact that the supersingular isogeny graph is Ramanujan.

As a consequence, isogeny graphs, and their relatives, are of great interest to the cryptographer. It may be useful to introduce additional complexity to these graphs. Herein lies the novel result of this project: extending the structure of isogeny graphs. Inspired by the *full level structure* described by Roda[3], we introduce three different levels of structure, and discuss their properties. It turns out that they form *covering graphs*, or *lifts* of the base isogeny graph. We deduce their connectivity, shape and size.

Aimed at a broader audience, this project provides all the basic definitions required to understand elliptic curves and their isogenies. The study of elliptic curves intersects the vast disciplines of combinatorics, number theory, and algebraic geometry. As a consequence, many of the topics discussed may be familiar to the reader. The challenge arises from understanding the sum of their parts.

The first section introduces the category of elliptic curves: a mathematical object which admits both a geometric and arithmetic structure. Morphisms between elliptic curves are known as isogenies, and are special in that they preserve both group structure and geometry. Some properties are discussed purely to aid understanding, and others for the direct application in later sections.

In the second section, we describe two well known isogeny graphs - isogeny volcanoes and the supersingular isogeny graph over finite fields. We include a section on expander graphs - an important property exhibited by the supersingular isogeny graph.

The final section comprises the novel work of the project. In it we learn some interesting properties of the added structure to isogeny graphs. Sage[4] was used to generate these graphs, with some examples and sample code included.

0.1 Prerequisites and Notation

The reader is assumed to be versed with fundamental topics in abstract algebra as taught in [5]. In addition, the group structure of elliptic curves utilises the properties of the projective space, so some knowledge in projective geometry is recommended. Background of the projective geometry applied to elliptic curves can be found in [6, appendix A]. Lastly the project deals with the properties of isogeny and modified isogeny graphs, so some elementary graph theory knowledge will be expected. The field of elliptic curves is rife with results from algebraic number theory and geometry. These subjects are well beyond the scope of the project, and would require substantially more background to include. As such, some theorems will be stated without motivation.

In general, we use K to refer to an arbitrary (perfect) field. For finite fields in particular, we refer to a field of order q as $\mathbb{F}_q$. Many of the statements in this paper do not include cases of fields of characteristic two or three. As such, results exclusive to fields of these characteristic will be omitted.

1 Elliptic Curves

The term *elliptic curves* originates from the study of the arc-length integrals of an ellipse. This work lead to the computation of so-called *elliptic functions* over the complex projective plane. Elliptic curves have been studied for well over a century, and the content of this field of mathematics is incredibly vast.

This section provides introductory knowledge to the field of elliptic curves. Many proofs are left out of this chapter but are referenced for completeness. There are analogous methods to describe elliptic curves by means of formalisms in algebraic geometry see Silverman's books [7] for an in depth introduction to elliptic curves and isogenies, or [6] as a beginner suitable option.

Definition 1 (Algebraic closure)**.** Given a field K, the *algebraic closure* of K, denoted as $\bar{K}$, is the algebraic field extension of K that is *algebraically closed.* That is, every non-constant polynomial in $\bar{K}[x]$ has a root in $\bar{K}$.

Definition 2 (Projective Space)**.** Given the set of points

$$(x_0, ..., x_n) \in \bar{K}^{n+1}$$

over a base field K, such that $x_0, ..., x_n$ are not all zero, the projective n-space, $\mathbb{P}^n$, is defined as the set of equivalence classes of the equivalence relation

$$(x_0, ..., x_n) \sim (y_0, .., y_n)$$

if there exists a $\rho \in \bar{K}^\times$ such that $x_i = \rho y_i$ for all i. *Simply* put, an equivalence class corresponds to all scalar multiples of a tuple, are denoted with square brackets as $[x_0, ..., x_n]$.

Definition 3 (Elliptic curve)**.** An elliptic curve is a non-singular, projective algebraic curve of genus one, which contains a base point $\mathcal{O}$, over a field K.

Given a cubic algebraic curve $\mathcal{C}$:

(i) $\mathcal{C}$ is *projective* if it is defined as the set of solutions to a degree three polynomial equation in three variables

$$\phi(X, Y, Z) = 0$$

in $\mathbb{P}^2$. From now, we will relax our notation by dehomogenising our equations, referring to an elliptic curve in 2 variables in affine coordinates x and y and including the point $\mathcal{O} = [0, 1, 0]$ on the line $Z = 0$.

(ii) $\mathcal{C}$ is *non-singular* if it does not contain a singular point. A point $P \in \mathcal{C}$ is *singular if and only if*

$$\frac{\partial \phi}{\partial X}(P) = \frac{\partial \phi}{\partial Y}(P) = \frac{\partial \phi}{\partial Z}(P) = 0.$$

$\mathcal{C}$ is an elliptic curve if it satisfies (i) and (ii). Any algebraic curve is genus one if it is bi-rationally isomorphic to non-singular cubic curves in $\mathbb{P}^2$.

We refer to the notion of isomorphism of elliptic curves as that of bi-rational equivalence. That is, two curves E_1 and E_2 are said to be isomorphic if there exists a bijective rational map between them.

Definition 4. An elliptic curve E is said to be *defined over a field* K, if the coefficients of the elliptic curve are in K, and it forms the base field of the projective plane E lies in. Given $\phi(x, y)$ is a dehomogenised equation of E,

$$E(K) = \{(x, y) \in K^2 : \phi(x, y) = 0\} \cup \{\mathcal{O}\}.$$

We call these the *rational points* of E over K.

1.1 Weierstrass Equation and j-invariant

In order to classify our elliptic curves, we use a useful result from Silverman [7, p.45].

Theorem 1 (Weierstrass equation)**.** *Every elliptic curve defined over K, where $char(K) \neq 2, 3$; is isomorphic to a curve of Weierstrass form, given in affine form by the equation*

$$y^2 = x^3 + Ax + B$$

plus a single point $\mathcal{O} = [0, 1, 0]$ on the projective line $Z = 0$ at infinity. Associated to this equation is the discriminant (Δ) and j-invariant (j):

$$\Delta = -16(4A^3 + 27B^2) \neq 0 \qquad \textit{and} \qquad j = -1728\frac{(4A)^3}{\Delta}$$

Proof. The proof relies on a homography - a change in coordinates - which maps an arbitrary rational point $\mathcal{P}$ to the point at infinity. See [7, p.42]. □

Remark. If we wish, we can extend the definition of Weierstrass normal form to fields of characteristic 2 and 3. See [7, Chap. III]

When dealing with equations, from now on, we will work with elliptic curves in Weierstrass form.

1.2 Isomorphisms and Automorphisms

Proposition 1. *(a) Two elliptic curves are isomorphic over $\bar{K}$ if and only if they have the same j-invariant*

(b) For $j \in \bar{K}$, there exists an elliptic curve defined over $K(j)$ whose j-invariant is j.

Proof. See [7, III, Prop 1.4]. □

Proposition 2 (Twists)**.** *Let E, E' be the elliptic curves defined over K where*

$$E : y^2 = x^3 + Ax + B \quad \textit{and} \quad E' : y^2 = x^3 + A'x + B'.$$

Then E and E' are isomorphic over K if and only if $A' = u^4A$ and $B' = u^6B$, for some $u \in K^\times$. The isomorphism is precisely the map

$$(x, y) \to (u^2x, u^3y)$$

Remark. If $u \notin K$ but $u^2 \in K$, we say that E' is the *quadratic twist* of E by u^2. That is, it is isomorphic over the extension field $K(u)$.

The two propositions above allows us to classify the isomorphism classes of elliptic curves by means of j-invariants. In fact, we do not need a very large field extension to find isomorphisms between curves with equal j-invariants. The *j-invariant* will play an important part in the construction of our isogeny graphs.

Proposition 3. *Let E_1 and E_2 be elliptic curves over a field K, and $j(E_1) = j(E_2)$. Then they are isomorphic over an extension of K of degree at most 6. If $j(E_1), j(E_2) \neq 0, 1728$; then they are isomorphic over an extension of degree at most 2.*

Proof. See [8, Thm 14.14]. □

A brief discussion of the automorphism group of elliptic curves is relevant to this project, as we wish to identify points of elliptic curves unique up to automorphism. Fortunately, while the endomorphism rings of elliptic curves in Weierstrass form can be challenging to determine, the automorphism group is far simpler.

Theorem 2. *Let E/K be an elliptic curve. Then, for char$(K) \neq 2, 3$;*

$$\#Aut(G) = \begin{cases} 6 & \textit{if } j(E) = 0 \\ 4 & \textit{if } j(E) = 1728 \\ 2 & \textit{otherwise} \end{cases}$$

Moreover, the automorphisms of E for $j(E) \neq 0, 1728$ are precisely

$$(x, y) \to (x, y) \quad \textit{and} \quad (x, y) \to (x, -y)$$

Proof. See [7, III, Thm. 10.1] for a complete proof. To see the two explicit maps above are the only automorphisms in the third case, consider

$$E : y^2 = x^3 + Ax + B.$$

Every automorphism will be of the form

$$(x, y) \to (u^2x, u^3y) \quad \text{for some } u \in K^\times$$

where $u^4A = A$ and $u^6B = B$. If $j(E) \neq 0, 1728$; then the only possibilities are $u = \pm 1$. □

1.3 Group Law

By defining elliptic curves over a projective plane, we are able to utilise Bezout's theorem [9] to construct a operation which forms a group on the curves.

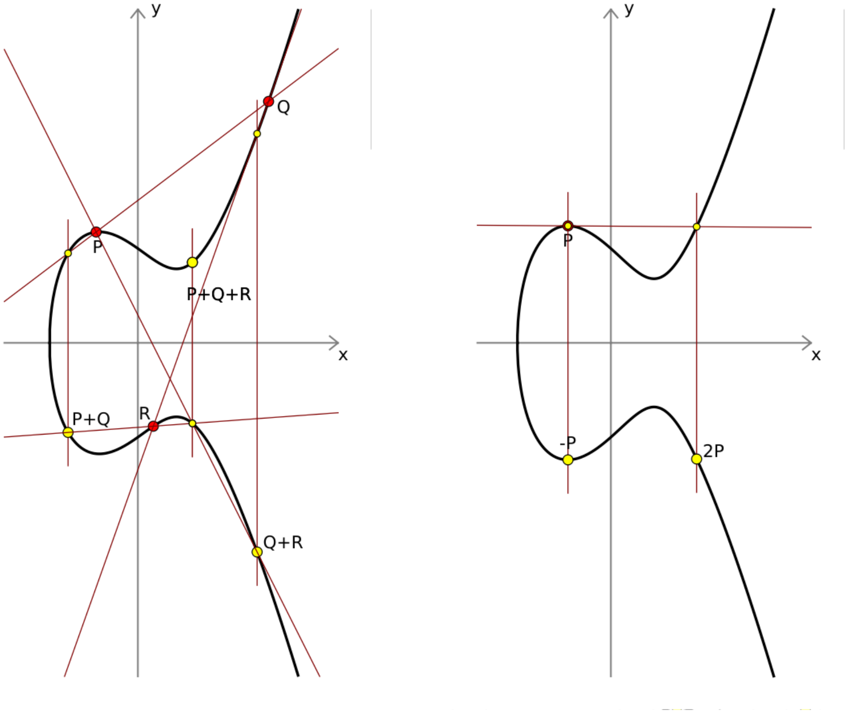

Figure 1: The group law on $Y^2 = X^3 - 4X + 8$ [10]

Theorem 3. *(Bezout's Theorem) Let X and Y be two distinct projective plane curves with degrees x and y, with no common component. Then $X \cap Y$ consists of xy points, including multiplicities.*

Bezout's theorem guarantees that any line which meets an elliptic curve will meet it precisely three times (where we count intersections at tangents twice). We need this for our group operation

Definition 5 (Geometric Group Operation)**.** For an elliptic curve E/K, we define the binary operation $\oplus : E \times E \to E$, given points $A, B \in E$:

- Let L be the line through A and B. If $A = B$, take L to be the tangent of E at A. Let C be the third point of intersection of L with E.
- Now let M be the line through C and $\mathcal{O}$. We denote the third point of intersection of M with E as $A \oplus B$

Surprisingly, this operation on the points of an elliptic curve forms an abelian group.

Proposition 4. *The composition law stated above has the following properties:*

Identity: *$P \oplus \mathcal{O} = P$ for all $P \in E$.*

Commutativity: *$P \oplus Q = Q \oplus P$ for all $P, Q \in E$.*

Inverse: *For all $P \in E$ there exists $P^{-1} \in E$ such that:*

$$P \oplus P^{-1} = \mathcal{O}.$$

Associativity: *For $P, Q, R \in E$, we have:*

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

Hence, $(E, \oplus)$ forms an abelian group with identity $\mathcal{O}$. Moreover $E(K) < E/K$.

Proof. See [7, III, Prop. 2.2] □

We will commonly refer to this group operation as +. See Appendix A for the explicit algorithm for computing the group law. We define the *multiplication-by-m map* the natural way, where, for $P \in E$:

$$[m]P = \underbrace{P + P + ... + P}_{\text{m times}}.$$

1.4 Supersingular and Ordinary Elliptic Curves

Definition 6. Given an elliptic curve E/K, $m \in \mathbb{Z}$, $m \neq 0$, the *m-torsion subgroup of E*, denoted as $E[m]$, is the set of points of E of order dividing m. That is,

$$E[m] = \{P \in E : [m]P = 0\}.$$

Proposition 5. *Let E be an elliptic curve over $\bar{K}$, then:*

1. *$E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$ if $char(\bar{K}) \nmid m$. If m is prime, $E[m]$ contains $m+1$ distinct cyclic groups of order m.*

2. *If $p = char(\bar{K})$, then:*

$$E[p^i] \simeq \begin{cases} \mathbb{Z}/p^i\mathbb{Z} & \text{for any } i \geq 0, \text{ or} \\ \{\mathcal{O}\} & \text{for any } i \geq 0. \end{cases}$$

Proof. See [7, III, Cor. 6.4] □

Proposition 5.2 allows us to characterise elliptic curves into two important classes. For a field of non zero characteristic p, if $E[p] \simeq \mathcal{O}$, we say E is *supersingular*. In the other case, we say E is *ordinary*. In many aspects these two classes of elliptic curve behave fundamentally differently.

We shall now briefly state a property of the endomorphism rings of ordinary elliptic curves. Ordinary and supersingular elliptic curves may also be characterised by their endomorphism rings. A peculiar behaviour of supersingular curves is that they have unusually large endomorphism rings, which we see in their isogeny graphs.

Theorem 4. *Let E/K be an elliptic curve. We say an elliptic curve E has complex multiplication if $End(E)$ is larger than $\mathbb{Z}$. We define the endomorphism algebra on E to be $End^0(E) = End(E) \otimes \mathbb{Q}$. then, if E has complex multiplication, one of the following hold:*

(i) $End^0(E)$ is isomorphic to imaginary quadratic field, in which case E is ordinary, or

(ii) $End^0(E)$ is isomorphic to a quaternion algebra, and E is supersingular.

Over a field of positive characteristic, E always has complex multiplication.

Proof. See [8, Thm 13.17, 14.8, 14.18]. □

1.5 Isogenies

Isogenies are morphisms between elliptic curves which preserve the group structure. Isogenies are a fundamental to the study of elliptic curves.

Definition 7. Let E_1 and E_2 be elliptic curves. An *isogeny* is morphism

$$\phi : E_1 \to E_2$$

which has a finite kernel. We say E_1 and E_2 are *isogenous* if there exists a nontrivial isogeny between them. We will see in section 2 that this in fact forms an equivalence relation.

Theorem 5. *An isogeny is a group homomorphism from $E(K)$ to $E'(K)$ that is surjective over the algebraic closure $K = \bar{K}$.*

Proof. See [7, III, Thm. 4.8] □

Since isogenies are group homomorphisms with finite kernels, we obtain the following corollaries directly.

Corollary 1. *Let $\phi : E \to E'$ be a nontrivial isogeny. Then* $\ker \phi$ *is a finite subgroup of E. We call an isogeny cyclic if the kernel is cyclic.*

Corollary 2. *Let H, G be cyclic subgroups of an elliptic curve E/K such that $|H| \neq |G| \neq char(K)$. Suppose there is an isogeny $\phi : E \to E'$ such that* $\ker \phi = G$. *Then $|\phi(H)| = |H|$.*

Now, the *Frobenius map* is a particularly important isogeny.

Definition 8 (Frobenius map)**.** Let E/K be an elliptic curve, where $p \neq 0$ is the characteristic of K. Let $q = p^r$ for some $r \in \mathbb{Z}$. The map $\pi : E \to E$ where

$$\phi(x, y) = (x^q, y^q) \qquad \text{for all } (x, y) \in E.$$

is an isogeny called the *q-th power Frobenius map.* Suppose $K = \mathbb{F}_q$. Then, by Fermat's Little Theorem, it fixes the points of $E(\mathbb{F}_q)$.

We now introduce the important notions of the *degree* and *separability* of an isogeny. In order to avoid cumbersome algebraic geometry, we shall characterise degree and separability using a result shown in Sutherland's course notes.

Proposition 6. *Let $\phi : E \to E'$ be an isogeny over a field K of characteristic $p \neq 0$. Then, for some $r \in \mathbb{Z}^+$, ϕ is a composition of an isogeny $\phi' : E \to E'$ and the p^r-th power Frobenius isogeny π of maximal r such that*

$$\phi = \phi' \circ \pi$$

Proof. The proof for non-even characteristics is given in [8, Cor. 6.4]. □

Corollary 3. *Let $\phi : E \to E'$, $\psi : E' \to E''$ be isogenies. Then*

$$\deg(\psi \circ \phi) = \deg \phi \cdot \deg \psi$$

Definition 9 (Separability, Degree [11, Defn. 26])**.** Let $\phi : E_1 \to E_2$ be an isogeny. By Proposition 6, we have that $\phi = \phi' \circ \pi$ for an isogeny ϕ' and a p^r-Frobenius isogeny, π.

(i) ϕ is said to be separable *if and only if* π is the identity map. If ϕ is separable, then

$$\deg \phi = \deg \phi' = \# \ker \phi$$

(ii) ϕ is said to be purely inseparable *if and only if* ϕ' is the identity map and $r > 0$. If ϕ is purely inseparable, then

$$\deg \phi = \deg \pi = p^r$$

(iii) Otherwise ϕ is said to be inseparable, and

$$\deg \phi = \deg \phi \cdot \deg \pi = \# \ker \phi \cdot p^r$$

(iv) If $\deg \phi = n$, ϕ is an *n-isogeny*; and E_1, E_2 are said to be *n-isogenous.*

(v) The isogenies of degree 1 are isomorphisms and are said to be both purely inseparable and separable.

Theorem 6. *Let E be an elliptic curve over an algebraically closed field, and G a finite subgroup of E. Then there exists, up to composition with an isomorphism, a unique elliptic curve E' and separable isogeny*

$$\phi : E \to E' \qquad \textit{such that} \qquad \ker \phi = G.$$

We refer to the image as the quotient $E/\ker \phi$

When constructing isogenies and isogeny graphs, we focus on separable isogenies, due to the two statements above. Separable isogenies are entirely determined by their kernel. So there is a one-to-one correspondence between the subgroups of elliptic curves, and their isogenies. A fundamental result of Vélu gives us the explicit formulas for calculating the isogeny and the image curve, given any subgroup of an elliptic curve. The details are described in appendix C. Now, based off the theorem above and the structure of torsion groups, we state the following lemma:

Lemma 1. *Let $E/\bar{K}$ be an elliptic curve. Let $\ell \neq char(\bar{K})$. Then, up to isomorphism, there are $\ell + 1$ isogenies of degree ℓ from E.*

We conclude the section on isogenies with a result of the duality of isogenies.

Theorem 7 (Dual Isogeny Theorem)**.** *Let $\phi : E_1 \to E_2$ be a nontrivial isogeny of degree m. Then there exists a unique isogeny*

$$\hat{\phi} : E_2 \to E_1 \qquad \textit{where} \qquad \hat{\phi} \circ \phi = [m]_{E_1}.$$

$\hat{\phi}$ is called the dual isogeny of ϕ. It satisfies natural properties of duality:

1. $\hat{\phi}$ has degree m

2. $\widehat{\phi \circ \psi} = \hat{\phi} \circ \hat{\psi}$ and $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$ for any isogeny $\psi : E_2 \to E_3$

3. $\hat{\hat{\phi}} = \phi$

4. For all $m \in \mathbb{Z}$,

$$\widehat{[m]} = [m] \qquad \textit{and} \qquad \deg[m] = m^2.$$

Proof. The proof is lengthy due to dealing with inseparable cases. See [7, III, Thm 6.1] □

1.6 Elliptic Curves over Finite Fields

We will conclude this section with some important theorems of the rational points of elliptic curves over finite fields. When dealing with computation in elliptic curves, we are primarily interested in the finite field case.

Theorem 8. *Let E be an elliptic curve defined over $\mathbb{F}_q$ where $q = p^i$. Then*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

for some $m, n \in \mathbb{Z}^+$ where $m|n$ and $p \nmid m$

Proof. See [8, Cor. 7.4] □

Theorem 9. *(Hasse) Let $E/\mathbb{F}_q$ be an elliptic curve defined over a finite field of order q. Then*

$$\#E(\mathbb{F}_q) = q + 1 - \epsilon \quad \textit{where} \quad |\epsilon| \leq 2\sqrt{q}.$$

ϵ is known as the trace of the q-th power Frobenius map, π_E. It satisfies the equation:

$$\pi_E^2 - \epsilon\pi_E + q = 0$$

Proof. See [7, V, Thm. 1.1]. □

Corollary 4. *Let $E/\mathbb{F}_p$ be an elliptic curve, for a prime p. Then E is supersingular if and only if $\#E(\mathbb{F}_p) = p + 1$*

Proposition 7. *Let E be a supersingular elliptic curve over a field K of prime characteristic, p. Then $j(E)$ is in $\mathbb{F}_{p^2}$.*

Proof. See [8, Thm. 14.16] □

These theorems greatly help us in our construction of isogeny graphs, as discussed in the next section. Knowing all supersingular curves lie within $\mathbb{F}_{p^2}$ allows us to efficiently find the complete set of supersingular curves over the full algebraic closure without having to look over larger field extensions.

Lastly, perhaps the most crucial tool in dealing with isogenies of elliptic curves over finite fields. Below is a corollary of the well known theorem of Tate. However, the main theorem is omitted as it would require some exposition into algebraic number theory.

Theorem 10 (Corollary of Tate Isogeny Theorem)**.** *Elliptic curves $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$ are isogenous if and only if*

$$\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q).$$

The theorem above implies that ordinary curves will never be isogenous to supersingular curves, as they have different numbers of points.

1.7 The Modular Polynomial

Definition 10. For a prime ℓ, we define $\Phi_\ell : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ as the modular polynomial. The modular polynomial is a algebraic curve that is symmetric in x, y. The roots of $\Phi_\ell(j(E), x)$ determine the j-invariants of ℓ-isogenous neighbours to an elliptic curve E.

Example. The modular polynomial for $\ell = 2$ is given below:

$$\begin{aligned}\Phi_2(x, y) = {} & x^3 + y^3 - x^2y^2 + 1488x^2y + 1488xy^2 - 162000x^2 - 162000y^2 \\ & +40773375xy + 8748000000x + 8748000000y - 157464000000000\end{aligned}$$

The modular polynomial is derived from the larger theory of modular curves. Constructing these modular curves will not be detailed in this project. What is relevant is that, assuming the generalised Riemann hypothesis, finding the modular polynomial for a given prime ℓ can be done in polynomial time, and the coefficients for small primes are widely available.[12][13].

Theorem 11. *Elliptic curves E, E' are ℓ-isogenous if and only if*

$$\Phi_\ell(j(E), j(E')) = 0,$$

where E, E' may be defined over any base field.

Proof. See [14, 2.3] □

2 Isogeny graphs

In this section we will discuss isogeny graphs. These are graphs with isomorphism classes of elliptic curves as vertices, and isogenies as edges. There are several flavours of isogeny graph. We will focus on graphs with fixed degree isogenies, over finite sets of elliptic curves. These include supersingular isogeny graphs, and *isogeny volcanoes*; a name coined by Fouquet and Morain in [15]. We begin by informally defining a general isogeny graph.

Definition 11 (Isogeny graph)**.** An *isogeny graph* is a graph whose vertices are j-invariants corresponding to isomorphism classes of elliptic curves, and isogenies representing edges between them.

Remark. By the dual isogeny theorem, we may define our edges as undirected.

Elliptic curves being *isogenous* form an equivalence relation. Clearly being isogenous is reflexive and transitive. It is also symmetric by the Dual Isogeny Theorem. So a natural question is, how do we characterise the equivalence classes of this relation? That is, the connected components of isogeny graphs. We have derived some helpful tools along the way to answer this question.

- We know that the cardinality of the rational points of elliptic curves over finite fields are equal if and only if they are isogenous.

- We have two ways to compute whether or not elliptic curves are ℓ-isogenous, for a fixed ℓ. We may use modular polynomials, or if we want explicit isogenies, Vélu's formulas.

2.1 ℓ-isogeny Graphs

We are interested in isogeny graphs for a fixed, prime degree ℓ. Provided $\ell \neq p$ for a field characteristic p, isogenies of prime degree are necessarily separable. We shall now, formally define the ℓ-isogeny graph:

Definition 12 ([14, Defn. 3])**.** For a field K, and a prime $\ell \neq char(K)$, we define the ℓ-isogeny (multi-)graph $G_\ell(K) = (\mathbf{V}, \mathbf{E})$ to have vertex set $\mathbf{V} = K$, and directed (multi-)set E,

$$\mathbf{E} = \{(j_1, j_2) \in K^2 : \Phi_\ell(j_1, j_2) = 0\}$$

Where each edge of $\mathbf{E}$ has multiplicity equal to the multiplicity of the roots $(Y - j_2)$ of $\Phi_\ell(j_1, Y)$.

Remark. This graph may be viewed as undirected if we delete the vertices 0 and 1728. We introduce one caveat. For the simplicity of proofs in this project, we will break convention and say that in the undirected graphs, loops only increase a vertices degree by 1.

We know, from proposition 1, that each element of K will correspond to a j-invariant of an elliptic curve over K. So the vertex set will consist of all elliptic curves over K. By Tate's isogeny theorem, $G_\ell(K)$ will consist of ordinary and supersingular components.

Let us consider some properties of the supersingular components:

- *By proposition 7, if $char(K) = p$, then the supersingular components of K will lie in $G_\ell(\mathbb{F}_{p^2})$.*

- *By lemma 1, the supersingular components of $G_\ell(\mathbb{F}_{p^2})$ are $\ell + 1$-regular graphs.* If E is supersingular, it will have $\ell + 1$ isogenous neighbours. Thus the degree of $j(E) \geq \ell + 1$.

We shall note vertex degree of vertices on the ℓ-isogeny graph as $\deg_{G_\ell(\mathbb{F}_{p^2})}(j(E))$. Over $\mathbb{F}_{p^2}$, this will always be $\ell + 1$.

It turns out that the supersingular components are connected. Moreover, they form Ramanujan graphs, a class of graph with special connectivity properties.

Theorem 12. *The subgraph of $G_\ell(\mathbb{F}_{p^2})$, formed by vertices of supersingular j-invariants, is connected. Moreover, if $12|p-1$, it is a Ramanujan graph.* [14, 2.5]

From now on, we shall call this graph the *supersingular ℓ-isogeny graph.*

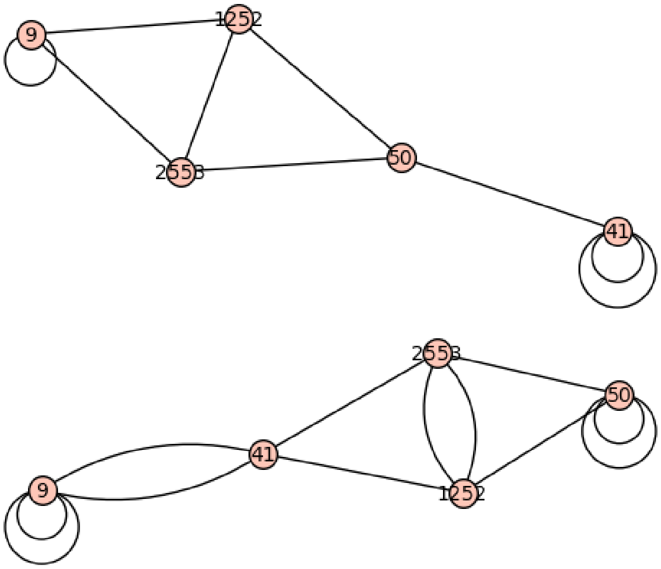

Figure 2: The supersingular 2-isogeny and 3-isogeny graphs of $\mathbb{F}_{61^2}$.

2.2 Expander and Ramanujan Graphs

Now, we shall digress on the special properties of the supersingular ℓ-isogeny graph. We are interested in broader class of graphs known as *expander graphs*. All connected graphs are expanders, but in loose terms, the best expander graphs are those with small degree that remain strongly connected. We shall briefly go over the definitions and properties of these graphs, obtained from a survey of Hoory et al [16]. Expanders may be defined in a number of ways. We will define the expansion ratio, and then briefly the algebraic properties of expanders.

Definition 13 (Expansion Ratio)**.** Let G be an undirected, d-regular graph. Let $(S, \bar{S})$ denote a vertex cut of G, and $E(S, \bar{S})$ to be the set of edges connecting the two vertex sets. We denote the *expansion ratio* of G as

$$h(G) = \min_{\{S \subseteq V(G), |S| \leq \frac{|V(G)|}{2}\}} \frac{|E(S, \bar{S})|}{|S|}$$

Typically the expansion ratio is considered over a family of d-regular graphs. We fix d and want a bound for $h(G)$ for any n. In practice, $h(G)$ is hard to compute, so expanders are typically characterised with spectral graph theory.

Definition 14 (Graph Spectrum)**.** Let G be a graph on n vertices. We define $A = A(G)$ to be the *adjacency matrix* of G, an $n \times n$ matrix whose (u, v) entry is the number of edges between u and v. Since A is symmetric, and real, it has n real eigenvalues, denoted as λ_i where

$$d \geq \lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n \geq -d.$$

These eigenvalues are known as the *spectrum* of G, and are studied in spectral graph theory. Here are some properties we can determine from the spectrum of a graph G:

- G is connected if and only if $\lambda_1 > \lambda_2$
- G is bipartite if and only if $\lambda_1 = -\lambda_n$
- If G is d-regular, then $\lambda_1 = d$.

It is clear here that the connectivity of a graph depends closely on λ_2.

Definition 15 (Expander Graph, Spectral Gap)**.** A connected, d-regular graph is an expander graph, with spectrum $\lambda_1 \geq ... \geq \lambda_n$. We define the *spectral gap* as $d - \lambda_2$. The spectral gap provides an estimation of the expansion ratio, because of the following bound [16, Thm. 2.4]:

$$\frac{1}{2}(d - \lambda_2) \leq h(G) \leq \sqrt{2d(d - \lambda_2)}$$

An important property of expander graphs is given below.

Lemma 2 (Expander Mixing Lemma)**.** *Let G be a d-regular graph with n vertices, then for all $S, T \subseteq V(G)$:*

$$|E(S,T)| - \frac{d|S||T|}{n} \leq \lambda(G)\sqrt{|S||T|}$$
$$\textit{where} \quad \lambda(G) = max(|\lambda_2|, ..., |\lambda_n|)$$

The left hand side of this equation measures the deviation between two quantities: $|E(S,T)|$, the number of edges between the two vertex sets; and the expected number of edges between S and T in a random graph of edge density d/n. In layman's terms, this lemma implies the following:

- *Edges of an expander graph are evenly distributed in the graph.*

- *The distribution of end vertices of random walks quickly converge to a uniform distribution. If a graph has n vertices, it converges in $O(\log n)$ steps.*

Proof. See [16, Lemma 2.5] □

Why do we care about this property for isogeny graphs? Consider a naive protocol which constructs random walks of a fixed length, starting at a fixed (public) vertex v, along a graph G to a (secret) vertex w. Now, suppose an attacker wanted to guess the endpoint of the random walk. For each vertex u in G, the attacker calculates the probability of ending a walk at u. If this probability distribution is not uniform, he may pick the vertices of highest probability first. This, in practice, means the attacker may need to make fewer guesses than if the distribution was uniform.

Note that the smaller our value of $\lambda(G)$, the better *mixing* properties G has. Stated below is a lower bound for $\lambda(G)$:

Theorem 13 (Alon-Boppana)**.** *A d-regular graph on n vertices satisfies:*

$$\lambda(G) \geq 2\sqrt{d-1} - o_n(1).$$

where $o_n(1) \to 0$ as $n \to \infty$ for a fixed d.

There is a particular class of expander graph that exhibits a tight upper bound for $\lambda(G)$.

Definition 16 (Ramanujan Graph)**.** An d-regular expander graph is a *Ramanujan graph* if

$$\lambda(G) \leq 2\sqrt{d-1}.$$

This is almost the tightest possible bound for $\lambda(G)$ and as a consequence, Ramanujan graphs are essentially optimal expander graphs. In general, they are very difficult to construct, but have a wide variety of application in error-correction codes, network reliability, and cryptography.

The fact that supersingular isogeny graphs are Ramanujan is a big motivating factor to their study of applications. In some sense, it motivates the hardness of the isogeny path-finding problem.

2.3 Isogeny Volcanoes

We shall now look at the the ordinary components of the ℓ-isogeny graph. It turns out the ordinary components form a class of graph known as *volcanoes*.

The mathematics of navigating the volcanoes of the ℓ-isogeny graph would require an entire section on its own. See [14] for an introductory survey on this topic. We shall pull some results and discuss the general structure of these volcanoes in this section.

A volcano graph is named such because of its resemblance to a geological volcano. We define an ℓ-volcano as follows [14, Defn. 1]:

Definition 17. (Volcano Graph) A *ℓ-volcano* is a (simple), connected graph whose vertices may be partitioned into *levels* $V_0, ..., V_d$ such that the following hold:

(i) The subgraph V_0 is either a single vertex with loops, or a simple cycle. We call V_0 the *crater rim*.

(ii) For $i > 0$, each vertex in V_i has exactly one neighbour in the level V_{i-1}.

(iii) For all $v \in V_i$, $i \neq d$, $\deg(v) = \ell + 1$. The vertices on the V_d, denoted as the *floor* of V, have degree 1.

That is, if we disregard parallel edges and loops, V consists of a cycle with isomorphic balanced trees rooted at each vertex. We say that V has depth d. We may also have infinite volcanoes, with unbounded depth.

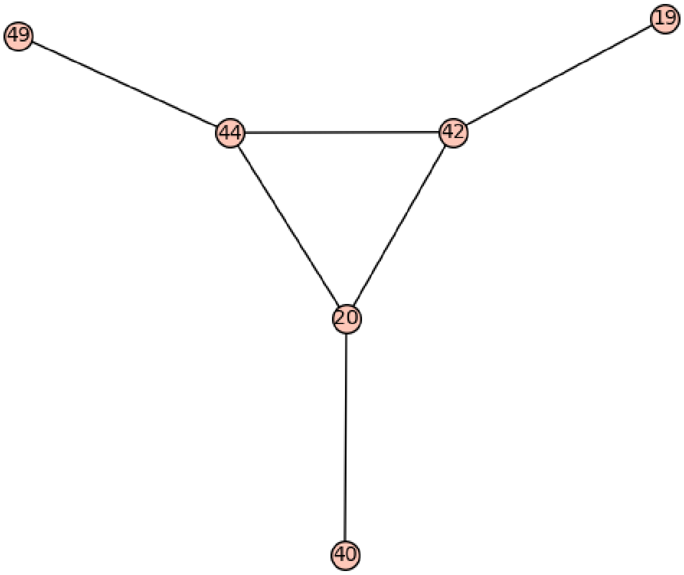

Figure 3: The ordinary component of $G_2(\mathbb{F}_{59})$ containing $j = 44$.

We digress briefly, by looking at a manner of categorising isogenies between ordinary elliptic curves by looking at endomorphism rings. Our goal is to characterise different 3 forms of isogenies, namely, *ascending, descending, and vertical* isogenies.

Theorem 14 ([8, Thm. 23.3])**.** *Let $\phi : E \to E'$ be an ℓ-isogeny over K. Then $End^0(E) \simeq End^0(E')$ and if E, E' are ordinary, then we say $End(E) = \mathcal{O}$ and $End(E') = \mathcal{O}'$ are orders in the imaginary quadratic field $End^0(E)$. One of the following hold:*

(i) $[\mathcal{O} : \mathcal{O}'] = \ell$, and say that ϕ is descending.

(ii) $[\mathcal{O}' : \mathcal{O}] = \ell$, and we say that ϕ is ascending.

(iii) $\mathcal{O} = \mathcal{O}'$ and we say that ϕ is horizontal.

These isogenies are named so for good reason. A theorem of Kohel, from [14], states that the ordinary components not containing $j = 0, 1728$ of the ℓ-isogeny graph are in fact ℓ-volcanoes.

Theorem 15 (Kohel)**.** *Let V be an ordinary component of $G_\ell(\mathbb{F}_q)$, not containing 0 or 1728. Then V is an ℓ-volcano of depth d such that the following hold:*

(i) Each curve E, $j(E) \in V_i$ has the same endomorphism ring $\mathcal{O}_i$.

(ii) *The vertex-induced subgraph on* V_0 *has degree* 0*,* 1 *or* 2*. If the degree of* $V_0 = 0$*, then* $|V_0| = 1$*.*

(iii) $[\mathcal{O}_i : \mathcal{O}_{i+1}] = \ell$ *for* $0 \leq i \leq d$

In layman's terms, Kohel's theorem formalises the symmetry of isogenies from curves at the same level on the volcano, and that the structure of an ordinary component of the ℓ-isogeny graph forms a volcano. We traverse the volcano with descending, ascending and horizontal isogenies. Further results of Kohel's theorem give us efficient, although unwieldy, ways to compute the depth and size of the crater rim of a volcano, which are omitted as they would require extensive exposition.

Almost all isogeny based cryptographic protocols use the supersingular components of the isogeny graphs. The reason is twofold. Curiously, there is little known about the characterisation of random walks on the isogeny volcanoes.Secondly, methods to compute supersingular elliptic curve isogenies currently exist[17], but we do not know of fast enough methods for the ordinary case to be of cryptographic use.

3 Isogeny graphs with Gamma structure

The imposed Gamma structure is derived from level structure described in [3]. The following section will discuss some lesser forms of structure we can impose, and their properties.

3.1 Defining the Gamma Structure

We start by introducing Given a set of elliptic curves over K, we choose two primes ℓ, m, such that $l \neq m \neq char(K)$. We then consider our traditional ℓ-isogeny graph, and impose additional structure on it.

In defining the graphs described in this section, we need to be careful with the automorphism groups of the elliptic curves we work with. For the purpose of proofs, and definitions below, we want to exclude the *degenerate* elliptic curves of j-invariants 0 and 1728. In practice, we do this by picking our prime characteristic carefully. If we work over supersingular curves, we pick a field of characteristic p such that $12 \mid p - 1$. For ordinary curves, we pick a characteristic such that $12 \nmid p - 1$. This guarantees the exclusion of these j-invariants.

In practice, the method of generating the graphs is as follows. We start with a set of elliptic curves over a field of characteristic described above. We then extend that field until we satisfy both of these conditions:

1. All elliptic curves of the same j-invariant are isomorphic i.e. there are no quadratic twists.
2. For each elliptic curve E, the full m-torsion group lies in the field. That is, there are $m + 1$ cyclic groups of order m in $E(K)$.

Over a finite field, and for a small prime m, finding a suitable field extension is easy to do.

Definition 18 (Gamma 0 construction)**.** For a set of elliptic curves $\mathcal{E}$ over K, we define the ℓ-$\Gamma_0(m)$ graph $(\mathbf{V}, \mathbf{E})$ as follows:

$$\mathbf{V}^* = \{(E, \langle g\rangle) : g \in E[m], E \in \mathcal{E},\ \text{and } g \neq \mathcal{O}\}$$

Where $\mathbf{V}$ is a quotient of $\mathbf{V}^*$. That is, the **vertices** of the graph is the pairs (E, G) where E is an elliptic curve in $\mathcal{E}$, and G is a cyclic subgroup of E of order m.

$$\mathbf{E} = \{((E, G), (E', G')) : \exists\phi : E \to E', \phi \text{ is an } \ell\text{-isogeny}, \phi(G) = G'\}$$

That is, each **edge** $((E, G), (E', G'))$ of the graph corresponds to an isogeny $\phi : E \to E'$ of degree ℓ such that the image of G through ϕ is G'.

Isomorphic curves are included twice, which is not what we want. We will resolve this by quotienting out the problem vertices with equivalence relations. We define equivalence up to isomorphism in the usual way, where vertices

$$(E, G) \sim (E', G')$$

if there is an isomorphism from E to E' that maps G to G'. We then quotient the vertex set. So we let

$$\mathbf{V} = \mathbf{V}^*/\sim.$$

Definition 19 (Gamma 1 construction)**.** The ℓ-$\Gamma_1(m)$ graph $(\mathbf{V}, \mathbf{E})$ is defined for a set of elliptic curves $\mathcal{E}$ over K is defined as follows:

$$\mathbf{V}^* = \{(E, x) : x \in E[m], E \in \mathcal{E}/\simeq,\ \text{and } x \neq \mathcal{O}\}$$

So, the **vertices** are the pairs (E, x) where E is an elliptic curve in the quotient set $\mathcal{E}/\simeq$, and x is a point of E of order m.

$$\mathbf{E} = \{((E, x), (E', y)) : \exists \phi : E \to E', \phi \text{ is an } \ell\text{-isogeny, and } \phi(x) = y\}$$

We have a **directed** edge from (E, x) to (E', y) if the curves are ℓ-isogenous and that isogeny maps x to y up to isomorphism.

Again, we use a similar equivalence relation. We say vertices $(E, A) \dot{\sim} (E', A')$ if there is an isomorphism from E to E' mapping A to A'. Now we let

$$\mathbf{V} = \mathbf{V}^*/\dot{\sim}$$

Remark (1). In the case of the Gamma 1 graph, in order to keep each vertex unique, we need to map each point to its inverse. For a curve E/K and a point $a \in E$, consider (E, a) and $(E, -a)$. Since E/K is abelian, the inverse map is an automorphism. Conveniently, the equivalence relation takes care of this for us.

Remark (2). We define the curves over a base field, but if $K = \mathbb{F}_p$, we will work over $\mathbb{F}_{p^2}$, to allow compatible quadratic twists.

The level structure described in [3] is included below. It is in some sense the most restricted of all the graphs. For canonical reasons, we let $N = m$.

Definition 20 (Full level structure)**.** For distinct primes $m, \ell \neq char(K)$, restricted to a set of elliptic curves $\mathcal{E}$ over K, we define the level ℓ-$\Gamma(m)$ structure as the graph $(\mathbf{V}, \mathbf{E})$ where:

$$\mathbf{V}^* = \{(E, \alpha) \ : \ E \in \mathcal{E}, \alpha : (\mathbb{Z}/m\mathbb{Z})^2 \to E[m]\}$$

Such that α is an isomorphism onto the m-torsion subgroup of each curve.

$$\mathbf{E} = \{((E, \alpha), (E', \beta)) : \exists \phi : E \to E', \ \phi \text{ is an } \ell\text{-isogeny}, \phi \circ \alpha = \beta\}$$

We apply an equivalence relation again, which guarantees each isomorphism class in $\mathcal{E}$ has a unique representative E. Let $(E, \alpha) \bar{\sim} (E', \beta)$ if there is an isomorphism $\phi : E \to E'$ such that $\phi \circ \alpha = \beta$, then let

$$\mathbf{V} = \mathbf{V}^*/\bar{\sim}.$$

Remark. An equivalent definition of this would be to fix a presentation $\langle A, B \rangle$ of $E[m]$ for each vertex.

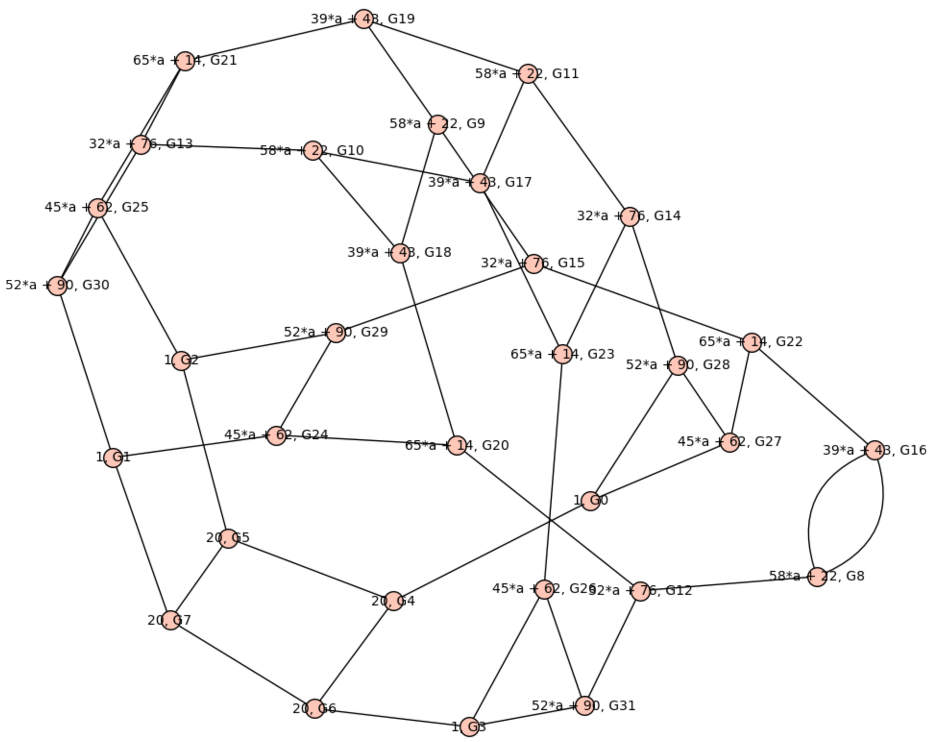

Figure 4: The supersingular 2-$\Gamma_0(3)$ graph over $\mathbb{F}_{97^2}$

Turning our attention to the first two graphs, it may not be clear why the Gamma 0 may be represented as *undirected* edges, while Gamma 1 case needs *directed* edges. We will prove this below. Noting that an undirected graph is equivalent to a directed graph if every outward edge has a dual inward edge.

Proposition 8. *(Edge Duality of Gamma 0) Given vertices (E_1, G_1) and (E_2, G_2) in ℓ-$\Gamma_0(m)$, let $\phi : E_1 \to E_2$ be an isogeny where $\phi(G_1) = G_2$, then the dual of ϕ, $\hat{\phi}$ satisfies:*

$$\hat{\phi}(G_2) = G_1.$$

Proof. Consider $\hat{\phi} \circ \phi$. By the dual isogeny theorem, it is $[\ell]_{E_1}$. So

$$\begin{aligned}\hat{\phi}(G_2) &= \hat{\phi} \circ \phi(G_1)\\ &= [\ell](G_1)\end{aligned}$$

Since G_1 is a cyclic group of order m, let $G_1 = \langle g_1 \rangle$ for some generator g_1. Now

$$\begin{aligned}[\ell](\langle g_1 \rangle) &= \{\ell \cdot i \cdot g_1 : 0 \leq i \leq m - 1\}\\ &= \langle \ell \cdot g_1 \rangle\end{aligned}$$

Since $\gcd(\ell, m) = 1$ we have that $[\ell]g_1$ is also generator of G_1, hence $[\ell](G_1) = G_1$. That is,

$$\hat{\phi}(G_2) = [\ell](G_1) = G_1.$$

□

Proposition 8 guarantees we can traverse each direction of an edge in the Gamma 0 graph. So we may define it as an undirected graph.

Proposition 9. *(Edge Duality of Gamma 1) Given a directed edge from (E_1, P_1) to (E_2, P_2) of ℓ-$\Gamma_1(m)$, let $\phi : E_1 \to E_2$ be the isogeny such that $\phi(P_1) = P_2$. If $m|\ell^2 - 1$, then there exists a dual reverse edge from (E_2, P_2) to (E_1, P_1).*

Proof. Suppose $m|\ell^2 - 1$. Since l, m are prime, we have that

$$\ell = mk - 1 \quad \text{or} \quad \ell = mk + 1 \quad \text{for some } k \in \mathbb{Z}$$

Now by the Dual Isogeny theorem, there exists a dual of ϕ, namely $\hat{\phi}$ such that $\hat{\phi} \circ \phi = [\ell]_{E_1}$. So

$$\phi(P_1) = P_2 \quad \text{and} \quad \hat{\phi}(P_2) = \ell \cdot P_1.$$

But, by definition, P_1 has order m. So either

$$\begin{aligned} \ell \cdot P_1 &= (mk + 1) \cdot P_1 \\ &= mk \cdot P_1 + P_1 \\ &= \mathcal{O} + P_1 \\ &= P_1 \end{aligned} \tag{1}$$

or

$$\begin{aligned} \ell \cdot P_1 &= (mk - 1) \cdot P_1 \\ &= mk \cdot P_1 - P_1 \\ &= \mathcal{O} - P_1 \\ &= -P_1. \end{aligned} \tag{2}$$

In case (1), our reverse edge is precisely $\hat{\phi}$. If case (2), we may compose $\hat{\phi}$ with the automorphism $[-1]$ to obtain our dual reverse edge, as in the diagram below.

$$\begin{tikzcd}
P_1 \arrow[r, "\phi"] & P_2 \arrow[dl, "\hat{\phi}"] \\
-P_1 \arrow[u, "{[-1]}"] &
\end{tikzcd}$$

□

So, if $m|\ell^2 - 1$, then we may represent the Gamma 1 graph as an undirected graph by identifying each pair of directed edges with an edge.

Corollary 5 (Gamma Equivalence)**.** *Let $\ell = 2$, $m = 3$. Then*

$$\ell\text{-}\Gamma_0(m) \simeq \ell\text{-}\Gamma_1(m)$$

Proof. Let $\rho : V(\ell\text{-}\Gamma_0(m)) \to V(\ell\text{-}\Gamma_1(m))$ be a map between vertex sets where

$$\rho(E_1, \langle P \rangle) = (E_1, P).$$

We know that

$$\langle P \rangle = \{\mathcal{O}, P, -P\}.$$

Now, ρ is well defined, since our image of two choices of generator are identified to the same vertex (by automorphism). ρ is also onto since every point of order m of E is a generator of a cyclic group in E. Similarly, ρ is also injective.

Now, suppose $(E_1, \langle P_1 \rangle)$ and $(E_2, \langle P_2 \rangle)$ are adjacent vertices in $\ell\text{-}\Gamma_0(m)$. Then there exists a $\phi : E_1 \to E_2$ such that $\phi(\langle P_1 \rangle) = \langle P_2 \rangle$. Since P_2 and $-P_2$ are the only elements in the image of $\langle P_1 \rangle$ of order 3, we have that $\phi(P_1) = \pm P_2$. If we compose ϕ with an automorphism, we obtain that (E_1, P_1) and (E_2, P_2) are adjacent in $\ell\text{-}\Gamma_1(m)$.

Lastly, suppose (E_1, P_1) and (E_2, P_2) are adjacent vertices in $\ell\text{-}\Gamma_1(m)$. Let $\phi : E_1 \to E_2$ where $\phi(P_1) = P_2$. Then clearly $\phi(\langle P_1 \rangle) = \langle P_2 \rangle$, and $(E_1, \langle P_1 \rangle)$ and $(E_2, \langle P_2 \rangle)$ are adjacent vertices in $\ell\text{-}\Gamma_0(m)$.

Thus ρ is a graph isomorphism and $\ell\text{-}\Gamma_0(m) \simeq \ell\text{-}\Gamma_1(m)$. □

Remark. In general, for $m > 3$, ρ will not be well defined. Consider $\rho(E, G)$ for some $(E, G) \in \ell\text{-}\Gamma_0(m)$. G has $m - 1$ generators, so by the pigeonhole principle, if $m > 3$, there is some generators of G, say g_1 and g_2 such that $g_1 \neq \pm g_2$. Now (E, g_1) and (E, g_2) are two distinct vertices in $\ell\text{-}\Gamma_1(m)$.

3.2 Connectivity and Other Properties

The following question is a fundamental to this project. *Suppose we start with components of an ℓ-isogeny graph: either an isogeny volcano, or the supersingular component over a finite field. Choose an m. What is the structure and connectivity of the resulting Gamma 0 and Gamma 1 graph?*

We shall consider the cases of supersingular isogeny graph, and ordinary volcanoes. Well, we start with some elementary proofs on the sizes of the vertex sets and graph degree.

Lemma 3. *Let k be the number of vertices in a ℓ-isogeny graph component over $\bar{K}$, then, over the elliptic curves in that component,*

(i) ℓ-$\Gamma_0(m)$ will have $k \cdot (m+1)$ vertices and

(ii) if $m > 2$, ℓ-$\Gamma_1(m)$ will have $\frac{k(m^2-1)}{2}$ vertices.

(iii) if $m > 2$, ℓ-$\Gamma(m)$ will have $\frac{k(m^2-1)(m^2-m)}{2}$

Proof. For (i), we know the m-torsion subgroup contains precisely $m+1$ cyclic groups of order m over $\bar{K}$. So for each elliptic curve E, we have $m+1$ vertices of the form (E, G_i). We also know each j-invariant is represented by a unique elliptic curve, suppose otherwise. Then, suppose E is such a representative, and let

$$\{(E, G_0), (E, G_1), ..., (E, G_m), (E', H)\} \subseteq V(\ell\text{-}\Gamma_0(m)),$$

where E, E' are isomorphic but no isomorphism exists between them mapping H to some G_i. Let $\phi : E' \to E$ be such an isomorphism. Then by definition,

$$(\phi(E'), \phi(G')) = (E, \phi(G')) \in V(\ell\text{-}\Gamma_0(m)).$$

So E has at least $m+2$ points of order m. A contradiction. So E is unique.

For (ii), we simply count the generators of each group in (i), and identify each point with its inverse. For all odd primes m, each generator has a non-self-inverse. There are $m-1$ generators, so that is $\frac{m-1}{2}$ points up to automorphism. Multiply this by the cardinality of (i) to obtain our result of (ii).

For (iii), we simply count the number of linearly independent elements of $\mathbb{Z}/m\mathbb{Z}^2$, and divide by the number of automorphisms between them. $\square$

Remark. For completeness, this proof also shows that there is a unique elliptic curve representing each j-invariant.

We define vertex degree in the usual way. When dealing with the equations, we shall include parallel edges, but in the representations of our graphs, we shall ignore them. However, calculating edge multiplicity is straightforward in practice.

Lemma 4. *For a field K, and an elliptic curve E/K, let*

$$\begin{aligned} j(E) &\in V(G_\ell(K)), \\ (E,G) &\in V(\ell\text{-}\Gamma_0(m)), \\ (E,P) &\in V(\ell\text{-}\Gamma_1(m)) \\ (E,\alpha) &\in V(\ell\text{-}\Gamma(m)) \end{aligned}$$

Then the degrees

$$\begin{aligned} \deg_{G_\ell(K)}(j(E)) &= \deg_{\ell\text{-}\Gamma_0(m)}(E,G) && \text{(i)} \\ &= \operatorname{outdeg}_{\ell\text{-}\Gamma_1(m)}(E,P). && \text{(ii)} \\ &= \operatorname{outdeg}_{\ell\text{-}\Gamma(m)}(E,\alpha) && \text{(iii)} \end{aligned}$$

Moreover, the neighbourhoods of these vertices are in bijection.

Proof. Let us count the (outward) edges of an $j(E)$ by the isogenies they represent, let

$$I = \{\phi_1, \phi_2, ..., \phi_n\}$$

where $\phi_i : E \to E_i$ for each isogeny from E to some neighbour E_i. We know that $|I| = \deg_{G_\ell(K)}(j(E))$.

For (i), consider a vertex $(E,G) \in V(\ell\text{-}\Gamma_0(m))$ for some G. For each $\phi_i \in I$, we have that (E_i) has a subgroup $G_i = \phi_i(G)$ of order m. Hence

$$((E,G),(E_i,G_i)) \in E(\ell\text{-}\Gamma_0(m))$$

So $\deg_{\ell\text{-}\Gamma_0(m)}(E,G) \geq \deg_{G_\ell(K)}(j(E))$. Clearly equality holds, since we constructed our edges based on the isogenies in I. Part (ii) and (iii) follow a similar argument. □

In fact, have more than equality of degree. The *local structure* of vertices in our Gamma graph is in bijection with the vertices in the ℓ-isogeny graph.

This motivates the notion of adding *structure* to our original graph. In fact, consider applying an equivalence relation $(E, X) \sim (E, Y)$. Where X, Y can either be groups or points, depending on which Gamma graph we choose. Its quotient graph is isomorphic to the ℓ-isogeny graph. We can also map ℓ-$\Gamma_1(m)$ to ℓ-$\Gamma_0(m)$ by identifying points on curves to the cyclic groups they lie in. It turns out this 'special' map is in fact a covering map:

Definition 21 (Covering Graph)**.** A graph C is a covering graph of a graph G if there is a *covering* map f from the vertex set of C to the vertex set of G such that f is surjective and *local* isomorphism. That is, the neighbours of a vertex v in C are in bijection with the neighbours of $f(v)$ in G.

A graph C is said to be an *n-lift* of G if for each vertex v of G, $f^{-1}(v)$ has exactly n elements.

Theorem 16. *(i) ℓ-$\Gamma_0(m)$ is an $(m+1)$-lift of $G_\ell(K)$.*

(ii) ℓ-$\Gamma_1(m)$ is an $(\frac{m-1}{2})$-lift of ℓ-$\Gamma_0(m)$, and a $(\frac{m^2-1}{2})$-lift of $G_\ell(K)$.

Proof. For (i), let the covering map be $f : V(\ell\text{-}\Gamma_0(m)) \to V(G_\ell(K))$ such that $f(E, G) = j(E)$. By Lemma 3 and 4, we have that f is surjective, mapping $m+1$ vertices to one, and locally isomorphic. Part (ii) follows a similar process for a covering map $f' : \ell\text{-}\Gamma_1(m) \to \ell\text{-}\Gamma_0(m)$. Since covering maps are closed under composition, the second statement follows. □

Remark. We have assumed that K is a large enough field to include the all $m+1$ cyclic groups of order m.

Covering graphs are a well-studied topic in algebraic graph theory. We can now exploit the covering property of our Gamma graphs to determine some properties. We shall start with isogeny volcanoes.

Lemma 5. *If X is a covering graph of Y with covering map f, and Y' is a vertex-induced subgraph of Y, then the vertex-induced subgraph of X, $f^{-1}(Y')$, covers Y'.*

Lemma 6 (Covering Partitions)**.** *Let X be a covering graph of Y, with a covering map f, and let A, B be (vertex-induced) subgraphs of Y partitioning the vertices of Y. Then $f^{-1}(A)$ and $f^{-1}(B)$ partition the vertices of X.*

Proof. Since X covers Y, let A' and B' be the maximal (vertex-induced) subgraphs of X that cover A and B respectively. That is,

$$A' = f^{-1}(A) \quad \text{and} \quad B' = f^{-1}(B).$$

Since f is onto, and $V(f(A') \cup f(B')) = V(A \cup B) = V(Y)$, it follows that $V(X) = A' \cup B'$. Now suppose there is a vertex $v \in A' \cap B'$, then $f(v) \in A \cap B$. A contradiction, since A and B are disjoint. So $f^{-1}(A)$ and $f^{-1}(B)$ partition X. □

Lemma 7 (Covering Gluing Lemma)**.** *Let X and Y be graphs, and A, B be (vertex-induced) subgraphs that partition the vertices of X. Let $f : X \to Y$ be a surjective map. f is a local isomorphism and X covers Y if and only if A and B are covering graphs of the vertex-induced subgraphs $f(A)$ and $f(B)$ of Y and for all $v \in V$, $f(v)$ is a locally isomorphic to v where V is the set of vertices:*

$$\begin{aligned} V = \{v \in A : (v, w) \in E(X) \textit{ for some } w \in B\} \cup \\ \{w \in B : (w, v) \in E(X) \textit{ for some } v \in A\} \end{aligned}$$

*That is, V is the set vertices of A and B adjacent to a vertex in the opposite partition. We will call the **joining set** of A and B.*

Proof. For the if direction, for each vertex $v \in (A - V) \cup (B - V)$, $f(v)$ is locally isomorphic to v, since we have not added or removed any edges between these vertices. The vertices that increase in degree are precisely the vertices in V. If there exists a vertex $v \in V$ not locally isomorphic to $f(v)$, f cannot be locally isomorphic over X, we have a contradiction. The converse is trivial. □

Lemma 8. *If X is a covering graph of Y, and Y is a tree, then X is a disjoint union of copies of Y. If Y is a forest, then X is a union of copies of Y.*

Proof. See [18, Lemma 6.8.3] for the tree case. If Y is a forest, for each tree T in Y, there is a covering subgraph of X that is a union of copies of T. It follows that X is a union of copies of Y. □

Isogeny volcanoes are *almost* trees. The lemmas above give us the bulk of the work for the following theorem.

Theorem 17. *Let V be a volcano graph, and Y a covering graph of V. Then Y is a union of volcano components. Moreover:*

(i) The crater rim of each component in Y is a cycle of length a multiple of the crater rim of V.

(ii) For each volcano $W \in Y$, the forest, $W - W_0$ is a union of copies of the forest of $V - V_0$, where each tree is isomorphic.

Proof. Let $f : Y \to V$ be such a covering map. If Y covers V, then every component of Y covers V. Let W be a component of Y. We will show W is a volcano.

V_0 is an n-cycle for some n. This implies $f^{-1}(V_0)$ is a union of copies of cycles of length a multiple of n. Call it A.

$V - V_0$ is a forest, say, of nm components, with each $v \in V_1$ corresponding to a unique root of a tree. Consider the preimage, $f^{-1}(V - V_0)$. By Lemma 8, $f^{-1}(V - V_0)$ is a union of copies of $V - V_0$. Call it B, and the roots $B' = f^{-1}(V_1)$

We return to W. V_0 and $V - V_0$ partition the vertices of V. Therefore, $f^{-1}(V_0)|_W$ and $f^{-1}(V - V_0)|_W$ partition the vertex set of W. So A and B are two disjoint subgraphs of W. What edges are missing in the union of these disjoint subgraphs of W? By the gluing lemma, only the edges between vertices of the joining set, $f^{-1}(V_0 \cup V_1)$, will change. Since each vertex on V_0 has an edge to m unique tree roots in V_1, it follows that each vertex in A has an edge to a m unique vertices B'. Since every tree in B is isomorphic, the representation of W is independent of our choice of vertex in B'. Thus W is a volcano. □

Corollary 6. *The ℓ-$\Gamma_1(m)$ and ℓ-$\Gamma_0(m)$ graphs over the elliptic curves in a finite isogeny volcano are unions of volcanoes.*

In general, the volcanoes of the Gamma graphs are not connected. Investigation into what determines the cycle lengths of the crater rims is needed, which would also tell us the number of components.

Now let us look at the Gamma graphs over the supersingular elliptic curves of a given field. The supersingular Gamma graphs may not even be connected at all. A characterisation of the components of the full level m graph has been proven by Roda.

Lemma 9. *(Connectivity of supersingular full level m) Let (E, α), (E', β) be vertices in ℓ-$\Gamma(m)$ over $\bar{\mathbb{F}}_q$. Then (E, α) and (E', β) are connected if and only if*

$$\det \alpha\beta^{-1} \in \langle \ell \rangle \subseteq (\mathbb{Z}/m\mathbb{Z})^*$$

Proof. See [3, Section 3.3] □

Using Roda's lemma, we may prove the connectivity of the Gamma 1 graph.

Theorem 18. *The supersingular ℓ-$\Gamma_1(m)$ and ℓ-$\Gamma_0(m)$ graphs are connected.*

Proof. We prove the Gamma 1 case. Let E, E' be two supersingular elliptic curves over K, and $P \in E(K)$. Since E, E' are connected in the supersingular ℓ-isogeny graph, we know that for all $P' \in E[m]\backslash\{\mathcal{O}\}$ there exists an ℓ^i-isogeny $\psi : E \to E'$ such that $\psi(P) = P'$ for some $P' \in E'[m]\backslash\{\mathcal{O}\}$.

What remains is to show that for any elliptic curve E, given distinct $P, P' \in E[m]\backslash\{\mathcal{O}\}$, there exists an isogeny $\phi : E \to E$ of degree a power of ℓ, that maps P to P'. Since m is prime, we view $E[m]$ as a 2 dimensional vector space over $\mathbb{Z}/m\mathbb{Z}$. Let $\alpha : (\mathbb{Z}/m\mathbb{Z})^2 \to E[m]$ be an isomorphism such that $\alpha(1,0) = P$ and $\alpha(0,1) = Q$ for some nontrivial $Q \in E[m]$ linearly independent from P. We want to guarantee another isomorphism that satisfies lemma 9. Let

$$P' = aP + bQ \tag{1}$$

$$Q' = cP + dQ \tag{2}$$

$$1 = ad - bc \tag{3}$$

for some $a, b, c, d \in \mathbb{Z}$. Note that a and b are fixed by α, and Q' is linearly independent from P' by equation (3). Now let $\beta : (\mathbb{Z}/m\mathbb{Z})^2 \to E[m]$ be an isomorphism such that $\beta(1,0) = P'$ and $\beta(0,1) = Q'$. Using the system of equations above, we solve for $\alpha\beta^{-1}$:

$$\alpha\beta^{-1} = \begin{pmatrix} x(P) & y(P) \\ x(Q) & y(Q) \end{pmatrix} \begin{pmatrix} x(P') & y(P') \\ x(Q') & y(Q') \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\implies \det \alpha\beta^{-1} = \frac{1}{ad - bc} = 1.$$

Hence, there exists an isogeny ϕ mapping α to β. Moreover, we have that

$$\phi \circ \alpha = \beta$$

$$\implies \phi(\alpha(1,0)) = \beta(1,0)$$

$$\implies \phi(P) = P'$$

Hence (E, P) and (E, P') are always connected in Gamma 1. It follows that any two vertices (E_1, P_1) and (E_2, P_2) are connected.

$$(E_1, P_1) \xrightarrow{\psi} (E_2, \psi(P_1)) \xrightarrow{\phi} (E_2, P_2)$$

As a clear consequence, the supersingular Gamma 0 graph is also connected. □

Now, we know that the base supersingular ℓ-isogeny graph is Ramanujan. If the supersingular Gamma graphs are connected, are they also Ramanujan?

Open Problem 1. *Starting with the set of supersingular elliptic curves, is the ℓ-$\Gamma_0(m)$, ℓ-$\Gamma_1(m)$, or ℓ-$\Gamma(m)$ graphs Ramanujan?*

3.3 Application: Families of Ramanujan Graphs

We return to the discussion of Ramanujan graphs. In their applications, we are interested in answering this question, stated more generally:

Open Problem 2. *Let Y be a graph, and X be a connected n-lift of Y. If Y is Ramanujan, then X Ramanujan.*

See [19] for a paper encompassing this work. [20] suggest that a typical n-lift of a Ramanujan graph is *nearly* Ramanujan. However, proving this strong statement in general would give us a method to construct infinite families of Ramanujan graphs. Unfortunately, answering this problem would imply a solution to the well known open problem below:

Open Problem 3. *There exists infinitely many d-regular, non-bipartite Ramanujan graphs for every $d \geq 3$.*

The open problem has been proven for $d = q + 1$ where q is a prime power[21]. Suppose we could prove our special case, Open Problem 1. Curiously, this could provide an alternative for infinite d-regular Ramanujan graphs if $d = \ell + 1$. Consider the following construction.

(Infinite family of d-regular Ramanujan graphs) *Fix $\ell = d - 1$. Start with the set of supersingular curves and work over the full algebraic closure of a field of characteristic p. Now, for each possible m, if ℓ-$\Gamma_0(m)$ is Ramanujan, then this defines an infinite class of d-regular Ramanujan graphs.*

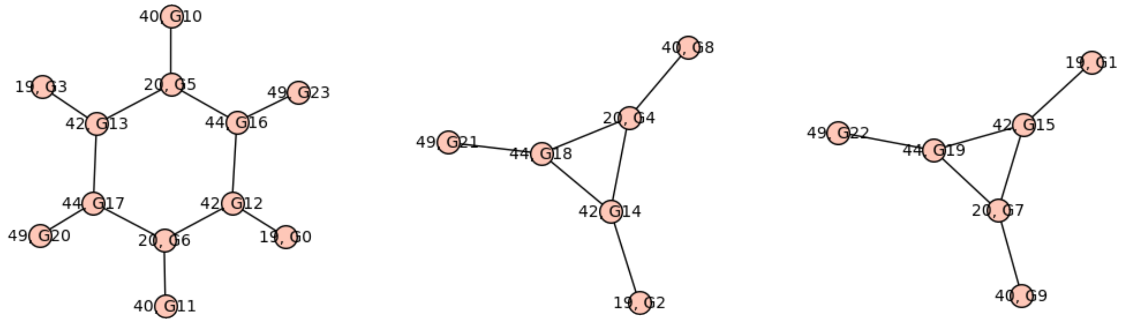

Figure 5: 2-$\Gamma_0(3)$ graph over $\mathbb{F}_{59}$ of ordinary component containing $j = 44$

Of course, this only works for prime ℓ, but some work could be done to extend our definitions to allow for prime power ℓ. One might also like to consider relating the Lubotzsky construction to the Gamma graphs, and the full level structure. A thesis of Roda has performed some establishing work on this [3].

Cryptographic hash functions have been constructed on supersingular isogeny graphs relying on their Ramanujan property. In particular, they on fast mixing in walks of the graph providing pseudo-randomness. Proving these lifted supersingular isogeny graphs are Ramanujan would be the first step to showing that it may be possible to devise secure hash functions with them.

3.4 Examples

Now we shall walk through some examples. We start with the ordinary component of the 2-isogeny graph over $\mathbb{F}_{59}$, as seen in Fig. 3. Note how our original crater rim of the volcano was a 3-cycle of j-invariants 20, 42, 44. Now let us consider the Gamma 0 graph, 2-$\Gamma_0(3)$ over the same field, depicted in Fig. 5. For convenience, we have labelled vertices by j-invariant, and indexed the subgroups. We can see that the curves split into 3 components. They retain their volcano structure, but 2 have crater rims which are 3 cycles, and 1 has a 6-cycle crater rim.

If we look at the isogenies from the rim to its adjacent vertex in V_1, note how it will always map a cyclic group to a unique cyclic group - so the volcano structure is preserved. If we look at the crater rim, depending on which cyclic group we fix, we may have to traverse around the crater rim in the original volcano more than once to return to our start vertex. For instance, the path from $(20, G_5)$ to $(42, G_{12})$ consists of 3 edges, and a cycle back to itself requires 6 edges.

See Fig. 4 for the supersingular Gamma 0 isogeny graph over $\mathbb{F}_{97^2}$ for $\ell = 2, m = 3$. Strangely, it appears to have some geometric structure, with two symmetric planar components. We know the gamma graphs are always $(\ell + 1)$-regular, if we count loops as directed edges. Some testing with small primes did not yield any counterexamples to being connected or Ramanujan.

3.5 Graph Generation

A challenge posed in this project was designing efficient algorithms for generating these graphs. Given we can find an l-isogeny graph efficiently, we need to be able to find the Gamma graphs efficiently. If we could exclusively use the modular polynomial for a given ℓ and m, constructing such graphs would be straightforward. Unfortunately, in general, it is likely that computing explicit isogenies is necessary.
However, in a special case of Gamma 0 graphs, a novel method can be used, using only the modular polynomial. Consider the following diagram:

$$\begin{tikzcd}
E_1 \arrow[r, "\phi"] \arrow[d, "\psi'"] & E_3 \arrow[d, "\psi"] \\
E_2 \arrow[r, "\phi'"] & E_4
\end{tikzcd} \tag{✡}$$

Where E_1, E_2, E_3, E_4 are elliptic curves, not necessarily distinct, and ϕ, ϕ' are isogenies of degree m, and ψ, ψ' are isogenies of degree l. We will see below that the existence of this commutative diagram implies that

$$((E_1, \ker \phi), (E_2, \ker \phi'))$$

is in the edge set of l-$\Gamma_0(m)$. Furthermore, there is a one-to-one correspondence between edges in l-$\Gamma_0(m)$ and (✡). So to finding the edges of l-$\Gamma_0(m)$ is equivalent to finding these 'rectangles' in the l-isogeny and m-isogeny graphs.

Proposition 10. *The commutative diagram (✡) exists if and only if there is an edge*

$$((E_1, \ker \phi), (E_2, \ker \phi'))$$

in the l-$\Gamma_0(m)$ graph.

Proof. Let (V, E) be the l-$\Gamma_0(m)$ graph. Suppose we have (✡). ϕ and ϕ' are cyclic isogenies. Since they are cyclic, their kernels are cyclic subgroups of order m. So $(E_1, \ker\phi), (E_2, \ker\phi') \in V$. Now suppose:

$$\exists x \in \ker\phi, \psi'(x) \notin \ker\phi$$

$$\implies \psi' \circ \phi'(x) \neq \mathcal{O}$$

So $\psi \circ \phi$ and $\psi' \circ \phi$ map to the same image curve, and, up to isomorphism:

$$\mathcal{O} = \psi(\mathcal{O}) = \psi \circ \phi(x) = \phi' \circ \psi'(x) \neq \mathcal{O}$$

A contradiction, hence

$$\psi'(\ker\phi) = \ker\phi'$$

Now suppose we have $((E_1, G_1), (E_2, G_2)) \in E$. Let ψ' be the isogeny between E_1 and E_2 where $\psi'(G_1) = G_2$. Now G_1, G_2 uniquely determine isogenies of degree m ϕ, ϕ' such that:

$$\phi : E_1 \to X \text{ and } \phi' : E_2 \to Y$$

Consider the isogeny $\psi : X \to Z$ with kernel $\phi(\ker\psi')$. We know:

$$\psi'(\ker\phi) = \ker\phi' \tag{1}$$
$$\phi(\ker\psi') = \ker\psi \tag{2}$$

If $P \in \ker\psi' \oplus \ker\phi$, by (1):

$$\begin{aligned} &\phi(P) \in \phi(\ker\psi') = \ker\psi \\ \Rightarrow \quad &\psi(\phi(P)) = \mathcal{O} \end{aligned} \tag{3}$$

Similarly, by (2):

$$\begin{aligned} &\psi'(P) \in \phi'(\ker\phi) = \ker\phi' \\ \Rightarrow \quad &\phi'(\psi'(P)) = \mathcal{O} \end{aligned} \tag{4}$$

So, by (3) & (4), $\ker\psi' \oplus \ker\phi \subseteq \ker\psi \circ \phi$ and $\ker\psi' \oplus \ker\phi \subseteq \ker\phi' \circ \psi'$ but

$$\begin{aligned} &|\ker\psi' \oplus \ker\phi| = |\ker\psi \circ \phi| = |\ker\phi' \circ \psi'| = lm \\ \Rightarrow \quad &\ker\psi \circ \phi = \ker\phi' \circ \psi' \end{aligned} \tag{5}$$

So the image curve Z of $\psi \circ \phi$ is equal to the image curve Y of $\phi' \circ \psi'$, hence we have the construction (✡). □

Warning. Note that this guarantees the *existence* of such an edge. However, there are many situations which make constructing graphs with this method infeasible. For instance, suppose E_1, E_2, E_3, E_4 are isogenous elliptic curves over K based on the diagram below:

$$\begin{tikzcd}
E_1 \arrow[r, bend left, "\phi_1"] \arrow[r, bend right, "\phi_2"] \arrow[d, "\psi'"] & E_3 \arrow[d, "\psi"] \\
E_2 \arrow[r, bend left, "\phi_1'"] \arrow[r, bend right, "\phi_2'"] & E_4
\end{tikzcd}$$

Where $\phi_1, \phi_2, \phi_1', \phi_2'$ are m-isogenies, and ψ, psi' are ℓ-isogenies. Using the proposition above, we know that either

$$\psi'(\ker \phi_1) = \ker \phi_1' \quad \text{or} \quad \psi'(\ker \phi_1) = \ker \phi_2'$$

But we cannot guarantee which edge is in the Gamma 0 graph without constructing the explicit isogenies and determining where each kernel maps to.

If there is no parallel edges in the m-isogeny graph - that is, every m-isogeny from one elliptic curve to another is unique - then we may use Proposition 10 to generate the l-$\Gamma_0(m)$ graph using the algorithm stated in appendix B. It is worth noting the diagram (✡) is precisely the commutative diagram employed by SIDH (see Appendix D).

Now, for the Gamma 1 graph generation, a more naive method was used. In general, we need the explicit isogenies in order to determine where a point will get mapped to. This equates to finding subgroups of order 2 and 3, and constructing isogenies between a class of curves, checking by composing with isomorphisms. Some speed up would be desirable. See appendix E for the implementations. Some speed up is achieved through the modular polynomial.

Appendix A Explicit Weierstrass Group Law

The method of computation using the group law on an elliptic curve is given below:

Definition 22 (Explicit Weierstrass Group Law)**.** Given a elliptic curve in Weierstrass form $E : y^2 = x^3 + Ax + B$, let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ where $P_1, P_2 \in E$, $P_1, P_2 \neq \mathcal{O}$:

1. If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 \oplus P_2 = \mathcal{O}$
2. Otherwise, set
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P_1 = P_2 \end{cases}$$
3. Then $P_1 \oplus P_2 = (x_3, y_3)$. Where
$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = -\lambda x^3 - y_1 + \lambda x_1$$

The case where $P_1 = P_2$ is known as the duplication formula.

Appendix B Generating Gamma 0 Graph

Note that this algorithm works only if there are no parallel edges as described in the graph generation section. Some alterations are needed to guarantee the correct graph generation as in the sage code in Appendix E.

Algorithm 1: Generating l-$\Gamma_0(m)$

```
Input: $l$-isogeny digraph $L$, $m$-isogeny digraph $M$
Output: $l$-$\Gamma_0(m)$ digraph $X$
Set $X$ to empty digraph
Set $K$ to empty set // Kernels of $m$-isogenies

for $(A, B)$ in edge set of $M$ do
    Compute isogeny kernel $\alpha$ of $(A, B)$, add to K
    Add $(A, \alpha)$ to vertex set of $X$
for pairs $(A, B), (C, D)$ in edge set of $L$ do
    if (A,C) and (B,D) or (A,D) and (B,C) in edge set of $M$ then
        Retrieve isogeny kernels $\alpha, \beta$ of edges in $M$ from $K$
        Add edge $((A, \alpha), (B, \beta))$ to edge set of $X$
```

Appendix C Vélu's Formulas

Vélu's formula gives us a computational method to find the equations for an isogeny for a given kernel. For ease of notation, for a point P on an elliptic curve, we use $x(P)$ and $y(P)$ to refer to the x and y coordinates of the point.

Theorem 19 (Vélu). *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over K. Let G be a finite subgroup of $E(\bar{K})$. Then $\phi : E \to E/G$ is a separable isogeny that has equation*

$$\phi(P) = \left(x(P) + \sum_{Q \in G \setminus \{\mathcal{O}\}} \big(x(P+Q) - x(Q) \big), y(P) + \sum_{Q \in G \setminus \{\mathcal{O}\}} \big(y(P+Q) - y(Q) \big) \right)$$

and the image of ϕ can be written as $y^2 = x^3 + A'x = B'$, where

$$A' = A - 5 \sum_{Q \in G \setminus \{\mathcal{O}\}} \big(3x(Q)^2 + A \big)$$

$$B' = B - 7 \sum_{Q \in G \setminus \{\mathcal{O}\}} \big(5x(Q)^3 + 3Ax(Q) + 2B \big)$$

Appendix D SIDH

By adding structure to our isogeny graphs, we play isogenies of two fixed prime degrees off each other. This is similar in many aspects to the protocol of *Supersingular isogeny Diffie-Hellman (SIDH)* key exchange, [2]. This key exchange protocol is a promising candidate in post-quantum cryptography, due to its similarity to the classic Diffie Hellman key exchange. SIDH offers small key sizes and perfect forward secrecy. In this appendix we will briefly discuss the SIDH protocol.

D.1 SIDH Protocol

The general idea involves finding walks on the ℓ and m supersingular isogeny graphs over $\mathbb{F}_{p^2}$, and computing the end vertex curve. This works because of the following commutative diagram:

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[d, "\psi"] & E/\langle A \rangle \arrow[d, "\psi'"] \\ E/\langle B \rangle \arrow[r, "\phi'"] & E/\langle A, B \rangle \end{tikzcd} \tag{1}$$

Where A, B are torsion points of an elliptic curve E.

Now, suppose Alice and Bob wish to compute a shared key over a public channel via SIDH protocol. We start with the following shared parameters:

- Distinct, small primes ℓ and m. Typically $\ell = 2$, $m = 3$

- A prime of the form $p = \ell^{e_\ell} \cdot m^{e_m} \cdot f \pm 1$. Where f is a scaling factor and coprime to ℓ, m.

- A starting supersingular elliptic curve $E/\mathbb{F}_p^2$

- Fixed points $P, Q, R, S \in E(\mathbb{F}_p^2)$ where P, Q have order ℓ^{e_ℓ} and R, S have order m^{e_m}.

Alice chooses her base, ℓ and completes the steps:

1. Alice generates two random integers $a, b < \ell^{e_\ell}$ and computes

$$A := a \cdot P + b \cdot Q.$$

2. Using Velu's formulas, she constructs an isogeny $\phi_\ell : E \to E/\langle A \rangle$. This is her private key

3. Alice then computes $E/\langle A \rangle$, $\phi_\ell(R)$ and $\phi_\ell(S)$; which she sends to Bob.

Bob completes the same steps for m, resulting in a private key ϕ_m and shares $E/\langle B \rangle$, $\phi_m(P)$ and $\phi_m(Q)$ with Alice. With this Alice continues:

4. Alice computes

$$K := a(\phi_m(P)) + b(\phi_m(Q))$$

4. She uses K to generate an isogeny

$$\phi' : E/\langle B \rangle \to E/\langle A, B \rangle$$

4. She computes the Weierstrass equation of $E/\langle A, B \rangle$

Bob follows a similar process, reaching the same isogenous curve of E, and computing its j-invariant. This acts as the shared key.

Appendix E Sage Code

The graphs discussed in this paper have been constructed using Sage[4] code. Below is the code used to construct Gamma 0 graph.

```
# Final Working Version of Gamma 0
# Auth: Shai Levin
import itertools

def neighbour(n, j1, j2, K):
  #RETURNS TRUE & MULTIPLICITY IF j2,j2 are neighbours
  F = PolynomialRing(K, 'x').gen()
  PHI = sage.modular.ssmod.ssmod.Phi_polys(n,F,j1)
  z = PHI.roots(multiplicities=True)
  for root, mult in z:
    if root == j2:
      return True, mult
  return False, 0

def Find_SS_Set ( p, K ):
  #Return SS set of curves over K
  SS = []
  for x in range(p):
    for y in range(p):
      if EllipticCurve(K,j=K(x+c*y)).is_supersingular():
        SS.append(x+c*y)
  return SS

def Find_Component(p,l):
  # find the component of isogenous elliptic curves with l
                                 elements
  Ord = []
  for x in range(p):
    for y in range(p):
      C = EllipticCurve(K,j=K(x+c*y))
      if C.cardinality() == l or C.quadratic_twist().
                                     cardinality() == l:
        Ord.append(x+c*y)
  return Ord

def Gen_Graph( p, K, ell1, ell2 ):
  SS = Find_SS_Set(p,K)
  #E_1 = EllipticCurve(K,[0, 33, 0,25,0])
  #SS = Find_Component(p,E_1.cardinality())
  SS_pairs = [(j1, j2) for j1 in SS for j2 in SS]
```

```
ell1_edges = set()
for (j1, j2) in SS_pairs:
  neigh1, mult1 = neighbour(ell1, j1,j2,K)
  if neigh1:
    ell1_edges.add(frozenset([j1,j2]))
vertex_set = set()
for j1 in SS:
  E = EllipticCurve(K, j=j1)
  for ell2_tors in E(0).division_points(ell2):
    if ell2_tors != E(0):
      vertex_set.add((j1, frozenset([ell2_tors,-ell2_tors,
                                     E(0)])))
      #set consists of group els
D = Graph(loops=True, multiedges=True)
D.add_vertices(vertex_set)
for (j1, g1),(j2,g2) in itertools.
                                combinations_with_replacement
                                (vertex_set, 2):
  if frozenset([j1,j2]) in ell1_edges and ((D.degree((j1,g1
                                  )) <= (ell1+1)) or j1 ==
                                  j2):
    E_1 = EllipticCurve(K, j=j1)
    isogenies = [EllipticCurveIsogeny(E_1, ell1_tors) for
                                    ell1_tors in E_1(0).
                                    division_points(ell1)]
    for isogeny in isogenies:
      if isogeny.codomain().j_invariant() == j2 \
      and isogeny.degree() == ell1:
        isom = isogeny.codomain().isomorphism_to(
                                        EllipticCurve(K,j=j2
                                        ))
        pipe = {isom(isogeny(point)) for point in g1}
        if pipe == g2:
          D.add_edge((j1,g1),(j2,g2))
          if g1 == g2 and j1 == j2:
            #stops duplication of loops, should only be 1
                                            loop
            break
i = 0
#tidy up vertex labelling
for j_inv, group in sorted(D.vertices()):
  D.relabel({(j_inv, group): "{}, G{}".format(GF(p^2,’a’)(
                                  j_inv), i)})
  i += 1
#lambda for determining ramanujan
```

```
  lambg = max([abs(lamb) for lamb in D.spectrum()[1:]])
  if lambg <= float(2*sqrt(ell1)):
    print("Graph is Ramanujan!")
  else:
    print("Graph is NOT Ramanujan")
  #check size of vertex set is correct
  print(len(SS)*(ell2+1), len(vertex_set))
  D.show(figsize=(10,5), iterations=1000000)
  # lots of iterations makes prettier graphs, reduce for
                                speed

p = 61
k = 4
K.<a> = GF(p^k,'a')
if k != 1:
  c = K.gen()**(((p**k)-1)/((p**2)-1)) # point of order |K|/2
else:
  c = 0


 Gen_Graph(p,K,2,3)
```

[10] [4]

References

[1] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, "CSIDH: An Efficient Post-Quantum Commutative Group Action," in *Advances in Cryptology – ASIACRYPT 2018*, T. Peyrin and S. Galbraith, Eds. Cham: Springer International Publishing, 2018, pp. 395–427.

[2] D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in *Post-Quantum Cryptography*, B.-Y. Yang, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

[3] M. Roda, "Supersingular isogeny graphs with level n structure and path problems on ordinary isogeny graphs," Master's thesis, McGill University, 2019.

[4] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2021, https://www.sagemath.org.

[5] J. Gallian, *Contemporary abstract algebra.* Cengage Learning, 2016.

[6] J. H. Silverman and J. T. Tate, *Rational points on elliptic curves.* Springer, 1992, vol. 9.

[7] J. H. Silverman, *The arithmetic of elliptic curves.* Springer, 2009, vol. 106.

[8] A. V. Sutherland, "Graduate Course on Elliptic Curves," MIT, 2019. [Online]. Available: https://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2019/index.htm

[9] R. Hartshorne, *Algebraic Geometry*, ser. Graduate Texts in Mathematics. New York, NY: Springer New York, 1977, vol. 52. [Online]. Available: http://link.springer.com/10.1007/978-1-4757-3849-0

[10] S. Kebekus, "Elliptic Curve Plotter," for group law diagrams. [Online]. Available: https://kebekus.gitlab.io/ellipticcurve/

[11] L. De Feo, "Graph Theory Meets Cryptography - course notes," Wurzburg, Germany, 2019.

[12] R. Broker, K. Lauter, and A. V. Sutherland, "Modular polynomials via isogeny volcanoes," *Mathematics of Computation*, vol. 81, no. 278, Jul. 2011, arXiv: 1001.0402. [Online]. Available: http://arxiv.org/abs/1001.0402

[13] A. Sutherland, "Modular polynomial coefficients," source of modular polynomial coefficients. [Online]. Available: https://math.mit.edu/~drew/ClassicalModPolys.html

[14] A. V. Sutherland, "Isogeny volcanoes," *The Open Book Series*, vol. 1, no. 1, pp. 507–530, Nov. 2013, arXiv: 1208.5370. [Online]. Available: http://arxiv.org/abs/1208.5370

[15] M. Fouquet and F. Morain, "Isogeny volcanoes and the sea algorithm," in *Proceedings of the 5th International Symposium on Algorithmic Number Theory*, ser. ANTS-V. Berlin, Heidelberg: Springer-Verlag, 2002, p. 276–291.

[16] S. Hoory, N. Linial, and A. Wigderson, “Expander graphs and their applications,” *Bulletin of the American Mathematical Society*, vol. 43, no. 04, pp. 439–562, Aug. 2006. [Online]. Available: http://www.ams.org/journal-getitem?pii=S0273-0979-06-01126-8

[17] C. Delfs and S. Galbraith, “Computing isogenies between supersingular elliptic curves over F_p,” *Designs, Codes and Cryptography*, vol. 78, Oct. 2013.

[18] C. D. Godsil and G. Royle, *Algebraic graph theory*, nachdr. ed., ser. Graduate texts in mathematics. New York Berlin Heidelberg: Springer, 2004, no. 207.

[19] C. Hall, D. Puder, and W. F. Sawin, “Ramanujan Coverings of Graphs,” *Advances in Mathematics*, vol. 323, pp. 367–410, Jan. 2018, arXiv: 1506.02335. [Online]. Available: http://arxiv.org/abs/1506.02335

[20] E. Lubetzky, B. Sudakov, and V. Vu, “Spectra of lifted Ramanujan graphs,” *Advances in Mathematics*, vol. 227, no. 4, pp. 1612–1645, Jul. 2011. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0001870811001010

[21] A. Lubotzky, R. Phillips, and P. Sarnak, “Ramanujan graphs,” *Combinatorica*, vol. 8, no. 3, pp. 261–277, Sep. 1988. [Online]. Available: https://doi.org/10.1007/BF02126799