Exploring Kaneko's bound: On multi-edges, loops and the diameter of the supersingular ℓ-isogeny graph

Sebastiano Boscardin* Sebastian A. Spindler†

Abstract

We analyze Kaneko's bound to prove that, away from the j-invariant 0, edges of multiplicity at least three can occur in the supersingular ℓ-isogeny graph $\mathcal{G}_\ell(p)$ only if the base field's characteristic satisfies $p < 4\ell^3$. Further we prove a diameter bound for $\mathcal{G}_\ell(p)$, while also showing that most vertex pairs have a substantially smaller distance, in the directed case; this bound is then used in conjunction with Kaneko's bound to deduce that the distance of 0 and 1728 in $\mathcal{G}_\ell(p)$ is at least one fourth of the graph's diameter if $p \equiv 11 \bmod 12$. We also study other phenomena in $\mathcal{G}_\ell(p)$ with Kaneko's bound and provide data to demonstrate that the resulting bounds are optimal; for one of these bounds we investigate the connection between loop multiplicities in isogeny graphs and the factorization of the 'diagonal' classical modular polynomial $\Phi_\ell(X, X)$ in positive characteristic.

1 Introduction

The supersingular ℓ-isogeny graph is one of the fundamental objects in isogeny-based cryptography: Originally it was used to define one of the first isogeny-based primitives, the CGL hash function [CLG09]. Nowadays the hardness of finding a path between two of the graph's vertices is essential for many isogeny-based schemes such as SQIsign2D-West [Bas+25b], PRISM [Bas+25a] and the aforementioned CGL hash function, as other presumably hard problems such as the computation of the endomorphism ring of a supersingular elliptic curve or the problem of finding an isogeny between two supersingular elliptic curves are equivalent to the problem of path-finding under probabilistic polynomial time reductions (assuming the generalized Riemann hypothesis) [PW24; Wes22].

With the emergence of isogeny-based cryptography as a basis for post-quantum cryptography, it is hence natural that research on the structure of this isogeny graph has gained a lot of momentum in the last decade. For example, due to work of Pizer [Piz90] it has long been known that these graphs are Ramanujan graphs if they are undirected, but only recently in works such as [Bas+23] and [CL24] has this property been thoroughly analyzed and transferred to the general directed case.

While the Ramanujan property has a more global flavor, local properties of the graph have also garnered attention. Especially noteworthy are the vertices corresponding to the j-invariants 0 and 1728, which play a special role in the graph since the curves they represent have larger-than-usual automorphism groups. This has motivated thorough analysis both of the loops at these vertices [AAM19; OX19] and of their neighborhoods [LOX20].

On yet another note, the Ramanujan property also implies that the graph has a small diameter (in the undirected case) [Piz90; RM20] and that it has fast mixing times, i.e. that the endpoint distribution of a random walk looks close to uniform after a relatively small amount of steps [Bas+23; CL24]. Due to the latter property the graph cannot have too many multi-edges, but even more can be said: In the language of M-small curves for $M = \ell^2$, [LB20] shows that curves connected by double edges tend to cluster into 'valleys' such that different valleys are far apart in the graph, and [Arp+23] limits the total number of vertices at which double edges can occur to $2\ell \cdot (2\ell - 1)$.

A naturally related question is to analyze the occurrence of edges of multiplicity at least three in the supersingular ℓ-isogeny graph. Using a well-known bound of Kaneko [Kan89], [dH+24] points out that the existence of such triple edges at vertices of non-zero j-invariant is limited to field characteristics p that satisfy $p < 4\ell^4$, but the authors also use a computational approach in conjunction with resultant theory to prove that for primes $\ell \leq 13$ one can instead achieve the tighter bound $p < 4\ell^3$ on the characteristic.

*Eindhoven University of Technology, s.boscardin@tue.nl
†Research Institute CODE, University of the Bundeswehr Munich, s.spindler@unibw.de

Notably, however, this approach has two clear limitations: First, the computational nature of their proof only ever allows it to be extended to a finite list of primes ℓ. Moreover, even for the prime $\ell = 13$ it already takes both a lot of time and memory to verify the necessary computations since the resultants considered in the proof rapidly grow in size with increasing ℓ. Due to this reason the authors were left to conjecture that the tighter bound of $p < 4\ell^3$ might be true in general.

Our contributions. In this article we confirm this open conjecture of [dH+24]: We prove for any prime $\ell \in \mathbb{N}$ the tighter bound $p < 4\ell^3$ for when triple edges can exist (away from the vertex of j-invariant 0) in the supersingular ℓ-isogeny graph $\mathcal{G}_\ell(p)$. Our main tool will be Kaneko's bound [Kan89, Theorem 2'] (and a thorough analysis of its proof), with which we limit further phenomena in $\mathcal{G}_\ell(p)$ and provide tighter bounds in special cases, namely for loops and for multi-edges at $\mathbb{F}_p$-rational vertices, in Section 3. To close out this section and to give a complete picture, we discuss why the mentioned special phenomena never occur in the setting of ordinary elliptic curves.

In Section 4 we analyze (with Kaneko's bound) the distance of the two special vertices corresponding to the j-invariants 0 and 1728, improving on a more generally applicable bound of [LB20]. To relate this distance to the diameter of the supersingular ℓ-isogeny graph, we then fill what seems to be a gap in the literature by providing a rigorous proof of a diameter bound that holds even in the directed case. This bound in turn allows us to conclude that the distance between the j-invariants 0 and 1728 is at least one fourth of the graph's diameter. Lastly, we generalize and improve the bound of [Sar18, Theorem 1.5] to investigate how many vertex pairs have a distance close to the diameter.

To illustrate the tightness of the bounds obtained in the previously mentioned sections, we further contrast against each bound the respective ℓ-dependent maximal primes at which the analyzed special phenomenon occurs. We computed these primes with SageMath [Sage]; the interested reader can find the later mentioned SageMath scripts containing the raw data in this article's accompanying GitHub repository[1]. In the computation of the maximal primes for our result on multi-loops we used the connection between the multiplicity of loops and the factorization of the 'diagonal' classical modular polynomial $\Phi_\ell(X, X)$. As this connection seems to not be recorded in the literature for positive characteristics, we give a thorough proof and discuss an additional necessary requirement for this result in Section 5. Finally, we show that for ordinary curves this additional requirement can be loosened significantly, though it cannot be omitted entirely, in contrast to the previous results.

Related work. First, we want to mention the works [AAM19; LOX20; OX19] analyzing the behavior of and around the special j-invariants 0 and 1728 in the supersingular ℓ-isogeny graph, as well as the analysis of [dH+24, Theorem 9 & Remark 4], which initially motivated many of the questions addressed in this article. Interesting in its own right and crucial as a tool for our proofs, [Ban+19] investigates cycles in the supersingular ℓ-isogeny graph and the endomorphisms corresponding to such cycles. Beyond our tighter bound on triple edges, some of the results obtained via Kaneko's bound [Kan89, Theorem 2'] seem to be folklore, and we mainly collect them here for completeness and to demonstrate that the resulting bounds are already optimal. The results on the structure of ordinary isogeny graphs are completely classical (cf. [Sut13] for a nice introduction), and we mainly include them here for contrast to our previous results.

On the distance of 0 and 1728, it is important to mention [LB20, Theorem 1.3], which achieves a bound of $p < 4\ell^{2r}$ compared to our tighter bound of $p < 3\ell^{2r}$ (cf. Remark 6). For the diameter bound in the undirected case there is the classical work of Pizer [Piz90, Theorem 1] (see also [RM20, Theorem 2]) and more recent results such as [Arp+24, Corollary 9.2]. Other than the argument given in [Koh96, p. 90] (which results in an unpleasant cofactor) as well as the statistical analysis of [Arp+23, Section 6], however, the diameter of the directed isogeny graph seems to not have received much treatment in the literature yet, even though the Ramanujan property has been extended to this setting in [Bas+23, Theorem 3] and has been further studied in [CL24, Theorem 1.4]; the former reference also provides crucial insights for the proof of our diameter bound. In the undirected case [Sar18, Theorem 1.5] describes how many vertex pairs have a distance close to the diameter.

Regarding the multiplicity of loops and the factorization of the diagonal classical modular polynomial $\Phi_\ell(X, X)$, we would be remiss not to mention [Onu21], which has served as an inspiration for the reduction techniques used in our proofs. Further [Gha24] uses modified Hurwitz numbers and Brandt matrices to analyze when $\mathcal{G}_\ell(p)$ does not have any loops or multi-edges; this is somewhat orthogonal to our work as we do not restrict the existence of double edges or of simple loops.

[1] https://github.com/S17A05/KanekoExploration

2 Preliminaries

2.1 Isogenies over arbitrary fields

First we introduce the necessary notions for isogenies of elliptic curves; for a more thorough treatment we refer the interested reader to [Sil09] and [Was08].

Let k be a perfect field and let E_0, E_1 be elliptic curves over k. An *isogeny* $\varphi\colon E_0 \to E_1$ is a non-constant morphism of curves that induces a group morphism between the $\overline{k}$-rational points of E_0 and E_1; this group morphism is automatically surjective with finite kernel [Sil09, Theorems II.2.3 & III.4.10]. The *degree* $\deg(\varphi)$ of the isogeny φ is the degree of the finite field extension $\overline{k}(E_0)/\varphi^*\overline{k}(E_1)$, where the embedding $\varphi^*\colon \overline{k}(E_1) \hookrightarrow \overline{k}(E_0)$ of function fields is given by pre-composition with φ [Sil09, Sections II.2 & III.4]; to indicate that the degree of φ is equal to an integer $d \in \mathbb{N}$, we also refer to φ as a *d-isogeny*. When the induced field extension is separable, the isogeny φ is said to be *separable* and its degree is equal to the cardinality of its kernel $\ker(\varphi) \subseteq E_0(\overline{k})$ [Sil09, Theorem III.4.10]; note that the isogeny φ is always separable if its degree is not divisible by the characteristic of k. Finally, the isogeny φ is called *cyclic* if its kernel $\ker(\varphi)$ is a cyclic group.

A fundamental example of an isogeny is the *multiplication-by-m* map $[m]\colon E \to E$ for an integer $m \in \mathbb{Z} \setminus \{0\}$, which is the m^2-isogeny given by

$$[m](P) := \underbrace{P + \cdots + P}_{m \text{ times}}.$$

To any d-isogeny $\varphi\colon E_0 \to E_1$ we can associate its *dual* isogeny $\widehat{\varphi}\colon E_1 \to E_0$, which is the d-isogeny uniquely determined by the conditions $\widehat{\varphi} \circ \varphi = [d]$ (as maps on E_0) and $\varphi \circ \widehat{\varphi} = [d]$ (as maps on E_1) [Sil09, Section III.6][2]. Importantly, for two isogenies $\varphi\colon E_0 \to E_1$ and $\psi\colon E_1 \to E_2$ we have

$$\widehat{\widehat{\varphi}} = \varphi, \quad \widehat{\psi \circ \varphi} = \widehat{\varphi} \circ \widehat{\psi} \quad \text{and} \quad \deg(\psi \circ \varphi) = \deg(\psi) \cdot \deg(\varphi).$$

For completeness we also define $[0]$ to be the constant map $E_0 \to E_0$ sending every point of E_0 to the point at infinity, and we set $\deg([0]) := 0$ and $\widehat{[0]} := [0]$.

An isogeny $\varphi\colon E_0 \to E_1$ is called an *isomorphism* if $\deg(\varphi) = 1$, an *endomorphism* if $E_0 = E_1$, and an *automorphism* if it is both an isomorphism and an endomorphism. Note that there is an isomorphism between two elliptic curves E_0 and E_1 if and only if they have the same *j-invariant*, i.e. $j(E_0) = j(E_1)$; conversely, for any $j \in K$ we can find a curve defined over K whose j-invariant is j [Sil09, Proposition III.1.4].

In a slight abuse of language we also refer to the map $[0]\colon E \to E$ as an endomorphism; then the set $\mathrm{End}(E)$ of endomorphisms of E forms a ring under pointwise addition (using the group structure of E) and composition of functions. The multiplication maps $[n]$ realize the integers $\mathbb{Z}$ as a subring of $\mathrm{End}(E)$, i.e. $\mathrm{End}(E)$ is a ring of characteristic zero [Sil09, Proposition III.4.2], and we will sometimes omit the square brackets of these multiplication maps if they are clear from the context.

The (multiplicative) unit group of $\mathrm{End}(E)$ is precisely the group $\mathrm{Aut}(E)$ of automorphisms of E. The next result explains why the (curves of) j-invariants 0 and 1728 play a special role in the theory of isogenies:

Theorem 1 ([Sil09, Theorem III.10.1])**.** *Let k be a field and E an elliptic curve over k. Then we have $j(E) \notin \{0, 1728\}$ if and only if $\mathrm{Aut}(E) = \{\pm 1\}$ has order 2. If additionally $\mathrm{char}(k) \notin \{2, 3\}$, then we further have:*

(a) *If $j(E) = 0$, then $\mathrm{Aut}(E) = \langle -\omega \rangle$ where ω is a primitive third root of unity.*

(b) *If $j(E) = 1728$, then $\mathrm{Aut}(E) = \langle \iota \rangle$ where ι is a primitive fourth root of unity.*

The importance of these additional automorphisms is partially due to the following fact: Any separable isogeny is uniquely determined by its kernel up to post-composition by an isomorphism, and conversely any finite subgroup $H \leq E(\overline{k})$ is equal to the kernel of some separable isogeny with domain E [Sil09, Proposition III.4.12]. In view of this, we say that two isogenies $\varphi\colon E_0 \to E_1$ and $\psi\colon E_0 \to E_2$ are *equivalent* if there is an isomorphism $\sigma\colon E_1 \to E_2$ with $\sigma \circ \varphi = \psi$, i.e. if φ and ψ have the same kernel.

[2] In fact, either of these two equations already uniquely determines $\widehat{\varphi}$ due to the surjectivity of isogenies.

2.2 Isogenies over finite fields

From now on we will work with elliptic curves over finite fields $k = \mathbb{F}_q$ for some prime power $q = p^e$. For the following we assume the reader to be familiar with the basic concepts related to quadratic number fields and quaternion algebras. For the former the reader can find the necessary information in [Neu99, Chapter I] and [Cox13, Section 7]; for the latter we can recommend [GS06, Chapter 1] for a brief introduction and [Voi21] as a comprehensive reference. However, we also provide an introduction to quaternion algebras in Appendix A, where we define the standard involution, reduced trace and reduced norm using the notion of *pure* quaternions.

Motivated by the following lemma, we let $\widehat{-}$, nrd and trd denote the non-trivial Galois automorphism, the norm and the trace of a quadratic number field, or the standard involution, the reduced norm and the reduced trace of a quaternion algebra, depending on the context.

Lemma 2. Let K be a quadratic number field. Then K can be embedded into the quaternion $\mathbb{Q}$-algebra $\mathrm{Mat}_2(\mathbb{Q})$. Moreover, any $\mathbb{Q}$-algebra embedding $i\colon K \hookrightarrow \mathcal{B}$ of K into a quaternion $\mathbb{Q}$-algebra $\mathcal{B}$ maps the Galois conjugate of an element $\alpha \in K$ to the quaternion conjugate $\widehat{i(\alpha)}$. In particular, the (quadratic) trace and norm of elements in K coincides with the reduced trace and norm of their images under the embedding i.

Proof. Since K is a quadratic field, we find some integer $d \in \mathbb{Z}$ such that $K \cong \mathbb{Q}(\sqrt{d})$. Then we can embed K into $\mathrm{Mat}_2(\mathbb{Q})$ via

$$K \cong \mathbb{Q}(\sqrt{d}) \hookrightarrow \mathrm{Mat}_2(\mathbb{Q}),\ \sqrt{d} \mapsto \left(\begin{smallmatrix} 0 & 1 \\ d & 0 \end{smallmatrix}\right)$$

because the matrix on the right has trace 0 and determinant $-d$.

Now let $i\colon K \hookrightarrow \mathcal{B}$ be any $\mathbb{Q}$-algebra homomorphism, and note that it is injective since K has no non-trivial ideals. Then we see that the conjugation $\widehat{-}$ of $\mathcal{B}$ acts on $i(K)$ as a $\mathbb{Q}$-algebra automorphism of order 2, so the unique non-trivial element $\tau \in \mathrm{Gal}(K|\mathbb{Q})$ has to satisfy $\widehat{i(-)} = i \circ \tau$. As the quadratic norm resp. trace of $\alpha \in K$ are defined by $\alpha \cdot \tau(\alpha)$ resp. $\alpha + \tau(\alpha)$, the claim follows. □

The structure of the endomorphism ring of an elliptic curve over a finite field can be classified completely:

The structure of $\mathrm{End}(E)$ ([Sil09, Section III.9 & Theorem V.3.1])**.** *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then* $\mathrm{End}(E)$ *is an* order*, i.e. both a ($\mathbb{Z}$-)lattice and a subring*[3]*, of the $\mathbb{Q}$-algebra $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$. Moreover, exactly one of the following two cases occurs:*

Ord*:* $\mathrm{End}(E)$ *is an* imaginary quadratic order*, i.e.* $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$ *is an imaginary quadratic number field.*

Sup*:* $\mathrm{End}(E)$ *is a* quaternion order*, i.e.* $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$ *is a division quaternion $\mathbb{Q}$-algebra.*

In either case the involution $\widehat{-}$ on $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$ is given by $\mathbb{Q}$-linear extension of the isogeny dualization $\alpha \mapsto \widehat{\alpha}$. In particular, trd *is the $\mathbb{Q}$-linear extension of the endomorphism trace map $\alpha \mapsto \alpha + \widehat{\alpha} \in \mathbb{Z}$, and* nrd *is the $\mathbb{Q}$-quadratic extension of the degree map $\alpha \mapsto \deg(\alpha) \in \mathbb{N}_0$. Moreover, for any $\alpha \in \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$ we have*

$$4\,\mathrm{nrd}(\alpha) \geq \mathrm{trd}(\alpha)^2. \tag{1}$$

Proof of the inequality. We have $4\,\mathrm{nrd}(\alpha) - \mathrm{trd}(\alpha)^2 = (\alpha - \widehat{\alpha})(\widehat{\alpha} - \alpha) = \mathrm{nrd}(\alpha - \widehat{\alpha}) \geq 0$. □

This classification motivates the following definition:

Definition 1. An elliptic curve E over a finite field $\mathbb{F}_q$ is called *ordinary* if $\mathrm{End}(E)$ is commutative, and *supersingular* otherwise.

Since the curves of j-invariants 0 and 1728 play a special role due to their larger automorphism groups, we mention here in which cases they are supersingular:

Example 1 ([Sil09, Examples V.4.4-5])**.** Let E be an elliptic curve over a finite field $\mathbb{F}_q$.

1. If $j(E) = 1728$, then E is supersingular if and only if $p \not\equiv 1 \bmod 4$.
2. If $j(E) = 0$, then E is supersingular if and only if $p \not\equiv 1 \bmod 3$.

[3] Note that, once we know that $\mathrm{End}(E)$ is a lattice, flatness implies that it is a subring of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$.

We collect further important information about supersingular curves in the following result:

Theorem 3 ([Sil09, Theorems V.3.1 & V.4.1]). *Any supersingular elliptic curve E over a finite field $\mathbb{F}_q$ satisfies $j(E) \in \mathbb{F}_{p^2}$, i.e. it is isomorphic to a curve that is defined over $\mathbb{F}_{p^2}$. Moreover, the number n of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}_p}$ is given by $n = 1$ for $p \in \{2, 3\}$, and for $p \geq 5$ by*

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

The supersingular isogeny graph. We are now ready to define the central object of our study: Let ℓ and p be prime numbers with $\ell \neq p$. The *supersingular ℓ-isogeny graph* $\mathcal{G}_\ell(p)$ is the finite directed multigraph with

- vertices: A representative set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}_p}$.
- edges: Given two representatives E_0, E_1, the edges $E_0 \to E_1$ are given by the equivalence classes of ℓ-isogenies $E_0 \to E_1$.

This graph is almost undirected due to dualization; in particular, the distance function on $\mathcal{G}_\ell(p)$ is symmetric. However, if we have an isogeny $\psi\colon E_1 \to E_0$ and an automorphism $\rho \in \mathrm{Aut}(E_0)$, then the two equivalent isogenies ψ and $\rho \circ \psi$ dualize to the isogenies $\widehat{\psi}$ and $\widehat{\psi} \circ \rho^{-1}$, which may not be equivalent anymore. In view of Theorem 1, the following result explains why we obtain asymmetries exactly around the curves of j-invariants 0 and 1728. Its proof is implicit in the proof of [AAM19, Theorem 7], but we give a slightly different proof using the reduced trace of endomorphisms here.

Proposition 4. Let $p \geq 5$ be a prime, let $\varphi\colon E_0 \to E_1$ be an isogeny between elliptic curves over $\overline{\mathbb{F}_p}$ with $j(E_0) \neq j(E_1)$, and let $\sigma \in \mathrm{Aut}(E_0)$. Then φ and $\varphi \circ \sigma$ are equivalent if and only if $\sigma \in \{\pm 1\}$.

In particular, if $p \neq \ell$ are distinct primes and $\eta_\ell(E_0, E_1)$ is the number of equivalence classes of ℓ-isogenies $E_0 \to E_1$, then

$$\eta_\ell(E_0, E_1) \cdot \tfrac{|\mathrm{Aut}(E_1)|}{2} = \eta_\ell(E_1, E_0) \cdot \tfrac{|\mathrm{Aut}(E_0)|}{2}. \tag{2}$$

Proof. It is clear that $\pm\varphi$ is equivalent to φ. Conversely, assume that we have an automorphism $\sigma \in \mathrm{Aut}(E_0) \setminus \{\pm 1\}$. By Theorem 1 we then have two possible cases:

First, if $j(E_0) = 0 \neq j(E_1)$, then Theorem 1 shows that any $\rho \in \mathrm{Aut}(E_1)$ has order dividing 4 and thus satisfies $\mathrm{trd}(\rho) \in \{0, \pm 2\}$. Moreover, as the order of σ is 3 or 6, it satisfies $\mathrm{trd}(\sigma) \in \{\pm 1\}$. Thus we obtain

$$\mathrm{trd}(\widehat{\varphi} \circ \rho \circ \varphi) = \deg(\varphi) \cdot \mathrm{trd}(\rho) \neq \deg(\varphi) \cdot \mathrm{trd}(\sigma) = \mathrm{trd}(\deg(\varphi) \cdot \sigma) = \mathrm{trd}(\widehat{\varphi} \circ \varphi \circ \sigma),$$

i.e. $\rho \circ \varphi \neq \varphi \circ \sigma$ for any $\rho \in \mathrm{Aut}(E_1)$. Hence φ and $\varphi \circ \sigma$ are not equivalent.

If, on the other hand, $j(E_0) = 1728 \neq j(E_1)$, then any $\rho \in \mathrm{Aut}(E_1)$ has order dividing 6 by Theorem 1 and thus satisfies $\mathrm{trd}(\rho) \neq 0$. Furthermore, as the order of σ has to be 4 in this case, we have $\mathrm{trd}(\sigma) = 0$. By an analogous computation we obtain $\mathrm{trd}(\widehat{\varphi} \circ \rho \circ \varphi) \neq \mathrm{trd}(\widehat{\varphi} \circ \varphi \circ \sigma)$ and thus $\rho \circ \varphi \neq \varphi \circ \sigma$ for any $\rho \in \mathrm{Aut}(E_1)$, i.e. φ and $\varphi \circ \sigma$ are not equivalent. □

Because of the asymmetries around the vertices of j-invariants 0 and 1728, the works [AAM19], [OX19] and [LOX20] have analyzed the loops at and neighborhoods of vertices with these special j-invariants in $\mathcal{G}_\ell(p)$; we reproduce the bounds obtained in their articles here:

Theorem 5 ([AAM19, Theorems 10 & 12], [OX19]). *Let $p \neq \ell$ be distinct primes, and let E_{1728} resp. E_0 denote curves over $\overline{\mathbb{F}_p}$ with j-invariant $j(E_j) = j \in \{0, 1728\}$. Then the following holds:*

(a) *If E_{1728} is supersingular with at least* $\begin{cases} 1, & \ell \equiv 3 \mod 4 \\ 3, & \ell \equiv 1 \mod 4 \\ 2, & \ell = 2 \end{cases}$ *loops at E_{1728} in $\mathcal{G}_\ell(p)$, then $p < 4\ell$.*

(b) *If E_0 is supersingular with at least* $\begin{cases} 1, & \ell \equiv 2 \mod 3 \\ 3, & \ell \equiv 1 \mod 3 \\ 2, & \ell = 3 \end{cases}$ *loops at E_0 in $\mathcal{G}_\ell(p)$, then $p < 3\ell$.*

Theorem 6 ([LOX20, Theorem 2 & Section 5]). *Let $p \neq \ell$ be distinct primes. Then the following holds:*

(a) *If there are at least three non-equivalent ℓ-isogenies $E_{1728} \to E$ for supersingular curves E_{1728} and E over $\overline{\mathbb{F}_p}$ with $j(E_{1728}) = 1728 \neq j(E)$, then $p < 4\ell^2$.*

(b) *If there are at least four non-equivalent ℓ-isogenies $E_0 \to E$ for supersingular curves E_0 and E over $\overline{\mathbb{F}_p}$ with $j(E_0) = 0 \neq j(E)$, then $p < 3\ell^2$.*

The Ramanujan property. As equivalence classes of ℓ-isogenies correspond to order ℓ subgroups of an elliptic curve, the graph $\mathcal{G}_\ell(p)$ is $(\ell+1)$-(out-)regular, i.e. there are $\ell+1$ outgoing edges from any vertex E_0, since the ℓ-torsion subgroup of $E_0(\overline{\mathbb{F}_p})$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$ by [Sil09, Corollary III.6.4]. More importantly, the graph is connected due to having the *Ramanujan property*. To describe this property, recall that the (i,j)-th entry of the adjacency matrix A of $\mathcal{G}_\ell(p)$ is given by the number $\eta_\ell(E_i, E_j)$ of edges from the vertex E_i to the vertex E_j[4].

Theorem 7 ([Bas+23, Theorem 3]). *Let ℓ and p be prime numbers with $\ell \neq p$. Then the $(\ell+1)$-regular graph $\mathcal{G}_\ell(p)$ has the Ramanujan property. This means that its adjacency matrix A is diagonalizable with real eigenvalues, has the eigenvalue $\ell+1$ with multiplicity 1, and all other of its eigenvalues lie in the Hasse interval $[-2\sqrt{\ell}, 2\sqrt{\ell}]$. In particular, $\mathcal{G}_\ell(p)$ is connected.*

In view of Equation (2), the connectedness of $\mathcal{G}_\ell(p)$ immediately implies:

Corollary 8. $\mathcal{G}_\ell(p)$ is undirected (in the sense that $\eta_\ell(E_0, E_1) = \eta_\ell(E_1, E_0)$ for all pairs of vertices) if and only if $p \leq 7$ or $p \equiv 1 \bmod 12$.

Due to its Ramanujan property the graph $\mathcal{G}_\ell(p)$ also has fast mixing properties (cf. [Bas+23, Theorem 11] and [CL24, Proposition 1.12]), which makes it well-suited for cryptographic applications (see, for example, [CLG09, Section 4]). Moreover, in the undirected case it is well-known that the Ramanujan property implies that the *diameter* of $\mathcal{G}_\ell(p)$, i.e. the maximum of the lengths of shortest paths between any two vertices, grows at most logarithmically in the number n of vertices (cf. [Piz90, Theorem 1] and [RM20, Theorem 2]), and in Section 4 we will use the techniques of [Bas+23, Theorem 7] to obtain an analogous bound in the general directed case.

Constructing endomorphisms. In Section 3 we will often construct two non-commuting endomorphisms $\alpha, \beta \in \mathrm{End}(E)$ of a curve E satisfying $j(E) \notin \{0, 1728\}$ via suitable edges in $\mathcal{G}_\ell(p)$. For this approach, the following result will be crucial:

Proposition 9 ([Cos+19, Lemma 4.4]). Let $p \neq \ell$ be distinct primes and consider a collection of ℓ-isogenies $\varphi_i \colon E_{i-1} \to E_i, i \in \{1, \ldots, m\}$, of elliptic curves over $\overline{\mathbb{F}_p}$ such that for each $i \in \{1, \ldots, m-1\}$ the isogeny φ_{i+1} is not equivalent to $\widehat{\varphi}_i$. Then $\varphi_m \circ \cdots \circ \varphi_1$ is a cyclic ℓ^m-isogeny.

Note that, conversely, any ℓ^m-isogeny is a composition of m ℓ-isogenies by [Sil09, Corollary III.4.11]. Finally, the next result gives sufficient conditions for two endomorphisms to not commute:

Theorem 10 ([Ban+19, Theorem 4.10]). *Let $p \neq \ell$ be distinct primes, let E be a supersingular curve over $\overline{\mathbb{F}_p}$ with $j(E) \notin \{0, 1728\}$, and let $\alpha, \beta \in \mathrm{End}(E)$ be cyclic endomorphisms. Further assume the following:*

(1) *There are $1 \leq e \leq f \leq 2$ such that $\deg(\alpha) = \ell^e$ and $\deg(\beta) = \ell^f$.*

(2) *$\beta \notin \{\pm\alpha^{f/e}, \pm\widehat{\alpha}^{f/e}\}$.*

(3) *If $e = f = 1$, then $\beta \neq \pm\widehat{\beta}$.*

Then α and β do not commute.

Proof. Suppose for a contradiction that α and β do commute. Since β is cyclic and due to the technical assumption (3) that $\beta \neq \pm\widehat{\beta}$ if $\deg(\beta) = \ell = \deg(\alpha)$, we can apply [Ban+19, Theorem 4.10] (see also [Ban+19, Definition 4.3, Lemma 4.9]) to obtain $a, b \in \mathbb{N}$, a third endomorphism $\gamma \in \mathrm{End}(E)$ and automorphisms $u, v \in \mathrm{Aut}(E)$ such that $\alpha = u\gamma^a$ and $\beta \in \{v\gamma^b, v\widehat{\gamma}^b\}$. However, by assumption (1) and a degree comparison we then see that $b = a \cdot f/e$, and $\mathrm{Aut}(E) = \{\pm 1\}$ shows that

$$\beta \in \{v\gamma^b, v\widehat{\gamma}^b\} = \{v\gamma^{a\cdot f/e}, v\widehat{\gamma}^{a\cdot f/e}\} \subseteq \{\pm\alpha^{f/e}, \pm\widehat{\alpha}^{f/e}\}$$

in contradiction to assumption (2). □

[4] This is only well-defined after fixing a numbering of the vertices, but the desired properties of A are independent of the chosen numbering.

2.3 Discriminants and Kaneko's bound

To prepare our final tool, we introduce the necessary properties of *discriminants*; the interested reader can find further information on this topic in [Voi21, Chapter 15].

Fix a field K of characteristic $\mathrm{char}(K) \neq 2$ and let $\mathcal{B}$ be a quaternion K-algebra. For $\alpha_1, \dots, \alpha_n \in \mathcal{B}$ we write

$$d(\alpha_1, \dots, \alpha_n) := \det((\mathrm{trd}(\alpha_i \alpha_j))_{i,j=1,\dots,n}.$$

We note one straightforward, but nonetheless useful computational property of this quantity:

Lemma 11 ([Voi21, Lemma 15.2.5])**.** Let $\alpha_1, \dots, \alpha_n \in \mathcal{B}$, let $M = (m_{ij})_{i,j=1,\dots,n} \in \mathrm{Mat}_n(K)$ and let $\beta_i = \sum_{j=1}^n m_{ij}\alpha_j$. Then

$$d(\beta_1, \dots, \beta_n) = \det(M)^2 \cdot d(\alpha_1, \dots, \alpha_n)$$

The following trick is the crucial ingredient in the proof of Kaneko's bound [Kan89, Theorem 2']:

Proposition 12. Let $\alpha, \beta \in \mathcal{B}$ lie in the quaternion K-algebra $\mathcal{B}$ and set $\gamma := \left(\alpha - \frac{\mathrm{trd}(\alpha)}{2}\right)\left(\beta - \frac{\mathrm{trd}(\beta)}{2}\right)$. Then

$$\mathrm{trd}(\gamma)^2 - 4\,\mathrm{nrd}(\gamma) = \frac{(2\,\mathrm{trd}(\alpha\beta) - \mathrm{trd}(\alpha)\,\mathrm{trd}(\beta))^2 - D_\alpha D_\beta}{4}$$

with $D_\alpha := \mathrm{trd}(\alpha)^2 - 4\,\mathrm{nrd}(\alpha)$ and $D_\beta := \mathrm{trd}(\beta)^2 - 4\,\mathrm{nrd}(\beta)$, and further

$$d(1, \alpha, \beta, \alpha\beta) = -\left(\mathrm{trd}(\gamma)^2 - 4\,\mathrm{nrd}(\gamma)\right)^2.$$

Moreover, if $\mathcal{B}$ is a division K-algebra, then the following are equivalent:

(i) $1, \alpha, \beta, \alpha\beta$ are K-linearly independent.

(ii) α and β do not commute.

Proof. We provide the computational proofs of the formulas at the end of Appendix A, while the equivalence of (i) and (ii) is proven in Corollary 42 of Appendix A. □

Remark 1. As $(\alpha, \beta) \mapsto \mathrm{trd}(\alpha\beta)$ defines a non-degenerate bilinear form on $\mathcal{B}$ by [Voi21, Theorem 7.9.4], one can show that $d(\alpha_1, \dots, \alpha_n)$ is non-zero if and only if $\alpha_1, \dots, \alpha_n$ are K-linearly independent.

For the remainder of this exposition we focus on lattices in quaternion $\mathbb{Q}$-algebras. In view of Lemma 2, we note that the following also applies to lattices in quadratic number fields.

Definition 2. Let $\mathcal{B}$ be a quaternion $\mathbb{Q}$-algebra, let $L \subseteq \mathcal{B}$ be a lattice (necessarily of rank at most 4), and let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Z}$-basis of L. Then the *discriminant* of L is defined by

$$\mathrm{disc}(L) := d(\alpha_1, \dots, \alpha_n).$$

Remark 2. The above is well-defined by Lemma 11 since between any two bases $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_n$ of L we can find a base change matrix $M \in \mathrm{GL}_n(\mathbb{Z})$, which satisfies $\det(M) = \pm 1$.

Example 2. Let $\mathcal{B}$ be a quaternion $\mathbb{Q}$-algebra and let $\alpha \in \mathcal{B} \setminus \mathbb{Z}$ be an *integral* element, i.e. we have $\mathrm{trd}(\alpha), \mathrm{nrd}(\alpha) \in \mathbb{Z}$. Via the reduced characteristic polynomial of α we then see that the subring $\mathbb{Z}[\alpha] \subseteq \mathcal{B}$ is a lattice of rank 2 with basis $1, \alpha$, and due to the computational properties of the reduced trace (cf. Lemma 45) we obtain

$$\mathrm{disc}(\mathbb{Z}[\alpha]) = \det\begin{pmatrix} \mathrm{trd}(1) & \mathrm{trd}(\alpha) \\ \mathrm{trd}(\alpha) & \mathrm{trd}(\alpha^2) \end{pmatrix} = \det\begin{pmatrix} 2 & \mathrm{trd}(\alpha) \\ \mathrm{trd}(\alpha) & \mathrm{trd}(\alpha)^2 - 2\,\mathrm{nrd}(\alpha) \end{pmatrix} = \mathrm{trd}(\alpha)^2 - 4\,\mathrm{nrd}(\alpha).$$

Note that this coincides with the discriminant of the reduced characteristic polynomial of α.

Stacked bases theorem. *Let L be a lattice of rank n and let $F \subseteq L$ be a sublattice of the same rank. Then there is a basis $\alpha_1, \dots, \alpha_n$ of L and positive integers $k_1, \dots, k_n \in \mathbb{N}$ such that $k_1\alpha_1, \dots, k_n\alpha_n$ forms a basis of F. Moreover, for any such basis $\alpha_1, \dots, \alpha_n$ and positive integers $k_1, \dots, k_n \in \mathbb{N}$ we have*

$$k_1 \cdots k_n = [L : F].$$

Proof. The existence of the basis and corresponding positive integers is proven in [Bos18, Theorem 2.9.2]. Moreover, we notice that the special stacked form of the bases directly gives rise to an isomorphism $\mathbb{Z}/k_1\mathbb{Z} \times \cdots \times \mathbb{Z}/k_n\mathbb{Z} \cong L/F$ of Abelian groups, and the claim follows. □

Corollary 13. Let $\mathcal{B}$ be a quaternion $\mathbb{Q}$-algebra, and let $F \subseteq L \subseteq \mathcal{B}$ be two lattices in $\mathcal{B}$ of the same rank. Then

$$\operatorname{disc}(F) = [L : F]^2 \cdot \operatorname{disc}(L).$$

Proof. By the stacked bases theorem we find a basis $\alpha_1, \ldots, \alpha_n$ of L as well as $k_1, \ldots, k_n \in \mathbb{N}$ such $k_1\alpha_1, \ldots, k_n\alpha_n$ is a basis of F. Letting $M = \operatorname{diag}(k_1, \ldots, k_n)$, we can hence apply Lemma 11 to obtain

$$\operatorname{disc}(L) = d(k_1\alpha_1, \ldots, k_n\alpha_n) = \det(M)^2 d(\alpha_1, \ldots, \alpha_n) = (k_1 \cdots k_n)^2 \operatorname{disc}(L) = [L : F]^2 \cdot \operatorname{disc}(L).$$

□

The Deuring correspondence [Voi21, Sections 42.2-4] gives a strong connection between the theory of quaternion algebras (specifically quaternion orders) and endomorphism rings of supersingular elliptic curves, and it also relates (quaternion) fractional ideals to isogenies; for our purposes, the following partial result will be sufficient:

Theorem 14. *Let E be a supersingular elliptic curve over $\overline{\mathbb{F}_p}$. Then $\operatorname{End}(E)$ is a maximal quaternion order of $\mathbb{Q} \otimes_{\mathbb{Z}} \operatorname{End}(E)$, i.e. it is not properly contained in another order, and we have*

$$\operatorname{disc}(\operatorname{End}(E)) = -p^2.$$

Proof. The maximality as well as the absolute value $|\operatorname{disc}(\operatorname{End}(E)| = p^2$ are proven in [Voi21, Theorems 15.5.5 & 42.1.19][5], and the negative sign follows from Proposition 12 and Corollary 13 by choosing any two non-commuting endomorphisms. □

The main tool of this article will be Kaneko's bound (and its proof, as we will see later), which we phrase in the language of supersingular elliptic curves here:

Kaneko's bound ([Kan89, Theorem 2']). *Let p be a prime and let E be a supersingular elliptic curve over $\overline{\mathbb{F}_p}$. Further suppose that we have two endomorphisms $\alpha, \beta \in \operatorname{End}(E)$ that do not commute. Then we have*

$$4p \leq \operatorname{disc}(\mathbb{Z}[\alpha]) \cdot \operatorname{disc}(\mathbb{Z}[\beta]).$$

If additionally $\operatorname{disc}(\mathbb{Z}[\alpha]) = \operatorname{disc}(\mathbb{Z}[\beta])$, then we even have

$$p^2 \leq \operatorname{disc}(\mathbb{Z}[\alpha])^2.$$

Proof. By Theorem 14 the endomorphism ring $\operatorname{End}(E)$ is a maximal order in the quaternion $\mathbb{Q}$-algebra $\mathcal{B} := \mathbb{Q} \otimes_{\mathbb{Z}} \operatorname{End}(E)$, and this quaternion algebra is ramified exactly at p and ∞ since we have $\operatorname{disc}(\operatorname{End}(E)) = -p^2$. Moreover, the two quadratic orders $\mathbb{Z}[\alpha], \mathbb{Z}[\beta]$ embed into $\operatorname{End}(E)$, though these embeddings might not be optimal. However, we can simply pick quadratic superorders

$$\mathbb{Z}[\alpha] \subseteq \mathcal{O}_\alpha \subseteq \operatorname{End}(E) \supseteq \mathcal{O}_\beta \supseteq \mathbb{Z}[\beta]$$

that are inclusion-maximal among quadratic suborders of $\operatorname{End}(E)$ containing $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$, respectively. As the endomorphisms $\alpha \in \mathcal{O}_\alpha$ and $\beta \in \mathcal{O}_\beta$ do not commute, $\mathcal{O}_\alpha$ is different from $\mathcal{O}_\beta$. We can now apply Kaneko' bound [Kan89, Theorem 2'] in view of Corollary 13 to obtain

$$4p \leq \operatorname{disc}(\mathcal{O}_\alpha) \cdot \operatorname{disc}(\mathcal{O}_\beta) \leq \operatorname{disc}(\mathbb{Z}[\alpha]) \cdot \operatorname{disc}(\mathbb{Z}[\beta]).$$

Finally, when $\operatorname{disc}(\mathbb{Z}[\alpha]) = \operatorname{disc}(\mathbb{Z}[\beta])$, then Corollary 13 shows that $\operatorname{disc}(\mathcal{O}_\alpha)$ and $\operatorname{disc}(\mathcal{O}_\beta)$ differ by a rational square, so they define the same quadratic field $\mathbb{Q}\left(\sqrt{\operatorname{disc}(\mathcal{O}_\alpha)}\right) = \mathbb{Q}\left(\sqrt{\operatorname{disc}(\mathcal{O}_\beta)}\right)$. This allows us to apply the stronger variant of Kaneko's bound [Kan89, Theorem 2'] to deduce

$$p^2 \leq \operatorname{disc}(\mathcal{O}_\alpha) \cdot \operatorname{disc}(\mathcal{O}_\beta) \leq \operatorname{disc}(\mathbb{Z}[\alpha]) \cdot \operatorname{disc}(\mathbb{Z}[\beta]) = \operatorname{disc}(\mathbb{Z}[\alpha])^2,$$

where all throughout we have used that all discriminants of quadratic orders are negative due to Example 2, Equation (1) and Corollary 13. □

To stress the power of Kaneko's bound even beyond our upcoming results, we discuss in Appendix B how Theorems 5 and 6 on the loops at and neighborhoods of vertices of j-invariant 0 and 1728 in $\mathcal{G}_\ell(p)$ can be derived from this bound.

[5] Voight [Voi21, Definition 15.2.3 & Remark 15.2.4] takes the absolute value of our definition to be the discriminant.

3 Multi-edges and loops in ℓ-isogeny graphs

3.1 General bounds for multi-edges in $\mathcal{G}_\ell(p)$

We start with our improved bound on multi-edges: A vertex in $\mathcal{G}_\ell(p)$ of non-zero j-invariant can be the origin of three edges to the same target only if the characteristic satisfies $p < 4\ell^3$.

Theorem 15. *Let $p \neq \ell$ be distinct primes, let E_0, E_1 be supersingular curves over $\overline{\mathbb{F}_p}$ with $j(E_0) \neq 0$, and suppose that there are three non-equivalent ℓ-isogenies $\varphi_0, \varphi_1, \varphi_2 \colon E_0 \to E_1$. Then $p < 4\ell^3$.*

Proof. Due to Theorems 5(a) and 6(a) we may assume $j(E_0) \neq 1728$. Now define the endomorphisms

$$\beta := \widehat{\varphi_1} \circ \varphi_0 \in \mathrm{End}(E_0) \ni \widehat{\varphi_2} \circ \varphi_1 =: \alpha. \tag{3}$$

These two endomorphisms are cyclic by Proposition 9 and they have degree ℓ^2. Furthermore we cannot have $\beta = \pm\alpha$ or $\beta = \pm\widehat{\alpha}$: In the first case the cyclic kernel $\ker(\beta)$ would have to contain the two distinct cyclic groups $\ker(\varphi_0)$ and $\ker(\varphi_1)$ of order ℓ, and in the second case we would obtain $\varphi_0 = \pm\varphi_2$ in contradiction to the fact that φ_0 and φ_2 are not equivalent. With Theorem 10 we therefore conclude that α and β do not commute.

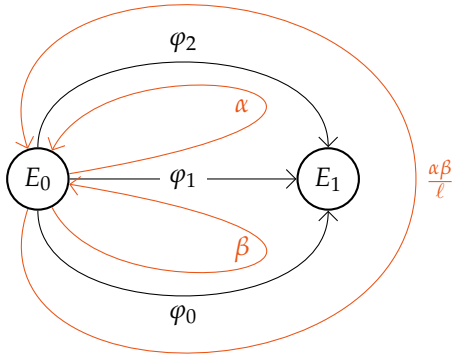


Figure 1: The construction of the endomorphisms α, β and the third endomorphism $\frac{\alpha\beta}{\ell}$.

For the remainder of this proof we follow the proof of Kaneko's bound given in [Kan89, Section 3] (which we already partially analyzed in Proposition 12), noting that our specific setting will allow us to gain a tighter bound. First we define the $\mathbb{Z}$-module

$$L := \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\alpha\beta \subseteq \mathrm{End}(E_0)$$

and the element

$$\gamma := \left(\alpha - \tfrac{\mathrm{trd}(\alpha)}{2}\right) \cdot \left(\beta - \tfrac{\mathrm{trd}(\beta)}{2}\right) \in \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E_0).$$

Then $(1, \alpha, \beta, \alpha\beta)$ is a basis of L by Proposition 12 since α and β do not commute. Moreover, by this result we have

$$\mathrm{disc}(L) = d(1, \alpha, \beta, \alpha\beta) = -\left(\mathrm{trd}(\gamma)^2 - 4\,\mathrm{nrd}(\gamma)\right)^2$$

and

$$D_\gamma := \mathrm{trd}(\gamma)^2 - 4\,\mathrm{nrd}(\gamma) = \frac{(2\,\mathrm{trd}(\alpha\beta) - \mathrm{trd}(\alpha)\,\mathrm{trd}(\beta))^2 - D_\alpha D_\beta}{4}$$

where we write $D_\alpha := \mathrm{trd}(\alpha)^2 - 4\,\mathrm{nrd}(\alpha) = \mathrm{disc}(\mathbb{Z}[\alpha])$ and $D_\beta := \mathrm{disc}(\mathbb{Z}[\beta])$ in view of Example 2. Now, crucially, we have

$$\alpha \circ \beta = \widehat{\varphi_2} \circ \varphi_1 \circ \widehat{\varphi_1} \circ \varphi_0 = \ell \cdot (\widehat{\varphi_2} \circ \varphi_0) \in \ell \cdot \mathrm{End}(E_0)$$

by construction, so we obtain the chain of rank four lattices

$$L \subseteq \underbrace{\mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\tfrac{\alpha\beta}{\ell}}_{=:F} \subseteq \mathrm{End}(E_0).$$

In view of the stacked bases theorem, Corollary 13 and Theorem 14 hence yield

$$-D_\gamma^2 = \operatorname{disc}(L) = [\operatorname{End}(E_0) : F]^2 \cdot [F : L]^2 \cdot \operatorname{disc}(\operatorname{End}(E_0)) = -[\operatorname{End}(E_0) : F]^2 \cdot \ell^2 \cdot p^2.$$

Therefore D_γ is a non-zero integer divisible by $\ell \cdot p$, and it is negative by Equation (1); Example 2 and Equation (1) thus allow us to deduce

$$\begin{aligned}
\ell \cdot p \leq -D_\gamma &= \frac{D_\alpha D_\beta - (2\operatorname{trd}(\alpha\beta) - \operatorname{trd}(\alpha)\operatorname{trd}(\beta))^2}{4} \\
&\leq \frac{D_\alpha D_\beta}{4} = \frac{1}{4} \cdot (-\operatorname{disc}(\mathbb{Z}[\alpha])) \cdot (-\operatorname{disc}(\mathbb{Z}[\beta])) \\
&= \frac{1}{4} \cdot \underbrace{\left(4\operatorname{nrd}(\alpha) - \operatorname{trd}(\alpha)^2\right)}_{\geq 0} \cdot \underbrace{\left(4\operatorname{nrd}(\beta) - \operatorname{trd}(\beta)^2\right)}_{\geq 0} \leq 4\operatorname{nrd}(\alpha)\operatorname{nrd}(\beta) = 4\ell^4.
\end{aligned}$$

Finally, dividing the above inequality by ℓ on both sides yields the bound $p \leq 4\ell^3$, which has to be a proper bound since $4\ell^3$ cannot be a prime. □

Remark 3. Using Kaneko's bound on p^2 for the case $\operatorname{disc}(\mathbb{Z}[\alpha]) = \operatorname{disc}(\mathbb{Z}[\beta])$ and being more precise in the above proof for the case $\operatorname{disc}(\mathbb{Z}[\alpha]) \neq \operatorname{disc}(\mathbb{Z}[\beta])$, one can directly derive the slightly stronger bound

$$p < 4\ell^3 - 5\ell.$$

For most of the remaining properties that we want to investigate in this section we can more directly apply our preliminary preparations. The following result will be our general blueprint:

Proposition 16. Let $p \neq \ell$ be distinct primes and let E_0 be a supersingular curve over $\overline{\mathbb{F}_p}$ with $j(E_0) \notin \{0, 1728\}$. Further suppose that we have two cyclic endomorphisms $\alpha, \beta \in \operatorname{End}(E_0)$ of degrees $\deg(\alpha) = \ell^e$ and $\deg(\beta) = \ell^2$ with $1 \leq e \leq 2$, and factor

$$\beta = \beta_2 \circ \beta_1 \quad \text{and} \quad \alpha = \alpha_1 \text{ or } \alpha = \alpha_2 \circ \alpha_1$$

into ℓ-isogenies according to the value of e. If β_1 is not equivalent to α_1 or $\widehat{\alpha_e}$, then we have

$$p < 4\ell^{2+e}$$

If moreover $e = 2$ and $\operatorname{trd}(\alpha) = \operatorname{trd}(\beta)$, then we even have $p < 4\ell^2$.

Proof. We first prove that α and β do not commute using Theorem 10. Suppose for a contradiction that $\beta = \pm\alpha^{2/e}$ or $\beta = \pm\widehat{\alpha}^{2/e}$. In the first case the cyclic kernel $\ker(\beta)$ would contain $\ker(\alpha_1)$, and in the second case it would contain $\ker(\widehat{\alpha_e})$. However, as it always contains the order ℓ subgroup $\ker(\beta_1)$, we would obtain $\ker(\beta_1) \in \{\ker(\alpha_1), \ker(\widehat{\alpha_e})\}$ (as the order of a subgroup in a cyclic group determines the subgroup uniquely), which contradicts our assumption. Therefore Theorem 10 shows that α and β do not commute, and with Kaneko's bound, Example 2 and Equation (1) we obtain

$$\begin{aligned}
4p &\leq (-\operatorname{disc}(\mathbb{Z}[\alpha]) \cdot (-\operatorname{disc}(\mathbb{Z}[\beta])) \\
&= (4\ell^e - \operatorname{trd}(\alpha)^2) \cdot (4\ell^2 - \operatorname{trd}(\beta)^2) \leq 16 \cdot \ell^{2+e}.
\end{aligned}$$

If moreover $e = 2$ and $\operatorname{trd}(\alpha) = \operatorname{trd}(\beta)$, then we have $\operatorname{disc}(\mathbb{Z}[\alpha]) = \operatorname{disc}(\mathbb{Z}[\beta])$. Hence the stronger version of Kaneko's bound and Equation (1) yield

$$p^2 \leq (-\operatorname{disc}(\mathbb{Z}[\alpha]))^2 = (4\ell^2 - \operatorname{trd}(\alpha)^2)^2 \leq (4\ell^2)^2$$

in this situation. Via division by 4 respectively by taking the square root we now obtain the claimed bound, noting that it has to be proper since $4 \cdot \ell^r$ cannot be a prime for $r \in \mathbb{N}$. □

One notable property of the special vertices 0 and 1728 is that they admit multi-edges to multiple neighbors in $\mathcal{G}_\ell(p)$. As the following result shows, for primes $p > 4\ell^4$ this property is exclusive to these two j-invariants. We note that, similarly to the same (looser) bound on the existence of triple edges, this result seems to be folklore; however, we still record it here for completeness.

Corollary 17. Let $p \neq \ell$ be distinct primes and let E_0, E_1, E_2 be supersingular curves over $\overline{\mathbb{F}_p}$ with $j(E_0) \notin \{0, 1728\}$ and $j(E_1) \neq j(E_2)$. Further suppose that there are two non-equivalent ℓ-isogenies $\varphi_1, \psi_1 \colon E_0 \to E_1$ and two non-equivalent ℓ-isogenies $\varphi_2, \psi_2 \colon E_0 \to E_2$. Then $p < 4\ell^4$.

Proof. We consider the two endomorphisms

$$\alpha_1 := \widehat{\psi_1} \circ \varphi_1 \in \mathrm{End}(E_0) \ni \widehat{\psi_2} \circ \varphi_2 =: \alpha_2,$$

which are cyclic of degree ℓ^2 by Proposition 9. If φ_2 was equivalent to φ_1 or to $\widehat{\widehat{\psi_1}} = \psi_1$, then the codomains E_2 of φ_2 and E_1 of $\{\varphi_1, \psi_1\}$ would have to be isomorphic, contradicting $j(E_1) \neq j(E_2)$. Therefore we can directly apply Proposition 16 to $(\alpha, \beta) = (\alpha_1, \alpha_2)$ with $e = 2$ to obtain $p < 4\ell^4$. □

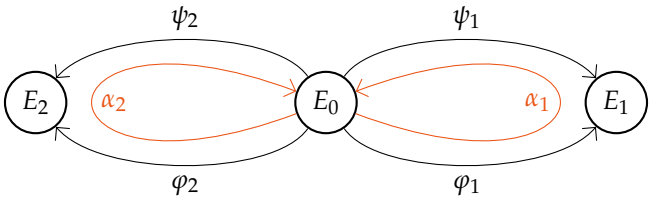
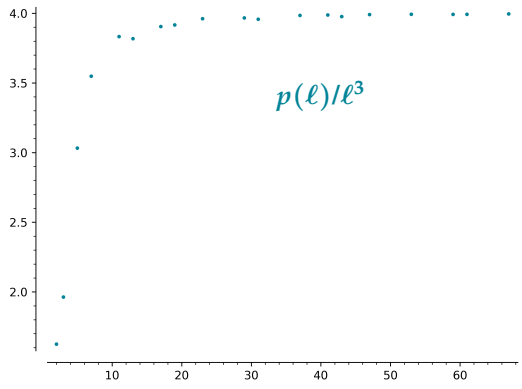
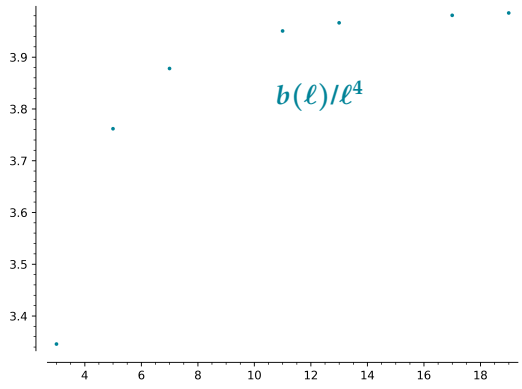


Figure 2: The endomorphisms α_1 and α_2 factor through non-isomorphic curves.

In Figure 3 we illustrate the tightness of the bounds of Theorem 15 and Corollary 17. To this end we computed for a prime ℓ the maximal prime $p(\ell) < 4\ell^3$ such that a triple edge originates from a vertex of non-zero j-invariant in $\mathcal{G}_\ell(p(\ell))$ respectively the maximal prime $b(\ell) < 4\ell^4$ such that two multi-edges originate from a vertex in $\mathcal{G}_\ell(b(\ell))$ whose j-invariant does not lie in $\{0, 1728\}$, and took the ratio relative to the ℓ-power ℓ^3 respectively ℓ^4; the corresponding data can be found in the files `generic_triple_primes.sage` and `double_double_primes.sage`.



(a) $p(\ell)/\ell^3$ (Theorem 15)



(b) $b(\ell)/\ell^4$ (Corollary 17)

Figure 3: Illustration of the tightness of the 'generic' bounds of Theorem 15 and Corollary 17.

3.2 Tighter bounds for loops in $\mathcal{G}_\ell(p)$

As indicated in Figure 3, the general bounds given by Theorem 15 and Corollary 17 are presumably very tight. However, there are two specializations of the previous settings that we will investigate in this article: For one, some of the edges could be loops, i.e. we could have $j(E_0) = j(E_1)$. For another, the multi-edges could lie at a vertex in $\mathbb{F}_p$, i.e. we could have $j(E_0) \in \mathbb{F}_p$ or $j(E_1) \in \mathbb{F}_p$. In this subsection we focus on the former situation.

First, the existence of triple loops in the supersingular ℓ-isogeny graph $\mathcal{G}_\ell(p)$ is subject to the following stronger bound on p:

Proposition 18. Let $p \neq \ell$ be distinct primes, let E_0 be a supersingular curve over $\overline{\mathbb{F}_p}$ and suppose that there are three non-equivalent $\alpha_0, \alpha_1, \alpha_2 \in \mathrm{End}(E_0)$ of degree $\deg(\alpha_i) = \ell$. Then $p < 4\ell^2$.

Proof. Due to Theorem 5 we may assume $j(E_0) \notin \{0, 1728\}$. Further we may assume that $\alpha_1 \neq \pm\widehat{\alpha_0}$ by switching α_1 and α_2 if necessary.

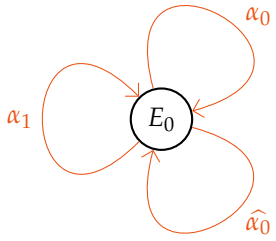


Figure 4: We can assume that α_1 is not equivalent to α_0 or $\widehat{\alpha_0}$.

Now suppose, for a proof by contradiction, that α_0 and α_1 commute. Then the prerequisites of Theorem 10 cannot be satisfied by $(\alpha, \beta) = (\alpha_0, \alpha_1)$ or $(\alpha, \beta) = (\alpha_1, \alpha_0)$, from which we deduce that $\alpha_0 = \pm\widehat{\alpha_0}$ and $\alpha_1 = \pm\widehat{\alpha_1}$. However, as the standard involution of a quaternion $\mathbb{Q}$-algebra fixes only the rational numbers and $\deg(\alpha_i) = \ell$ is not a square in $\mathbb{Q}$, we must have $\widehat{\alpha_i} = -\alpha_i$. Therefore

$$(\alpha_0 - \alpha_1)(\alpha_0 + \alpha_1) = \alpha_0^2 - \alpha_1\alpha_0 + \alpha_0\alpha_1 - \alpha_1^2 = -\widehat{\alpha_0}\alpha_0 + \widehat{\alpha_1}\alpha_1 = -\ell + \ell = 0,$$

i.e. $\alpha_0 = \pm\alpha_1$ in contradiction to the non-equivalence of α_0 and α_1.

We conclude that α_0 and α_1 do not commute, so Kaneko's bound and Equation (1) yield

$$4p \leq (-\operatorname{disc}(\mathbb{Z}[\alpha_0])) \cdot (-\operatorname{disc}(\mathbb{Z}[\alpha_1])) = (4\operatorname{nrd}(\alpha_0) - \operatorname{trd}(\alpha_0)^2) \cdot (4\operatorname{nrd}(\alpha_1) - \operatorname{trd}(\alpha_1)^2) \leq 16\ell^2.$$

Dividing by 4 finally results in the bound $p \leq 4\ell^2$, and this bound has to be proper since $4\ell^2$ cannot be a prime. □

Similarly, one might wonder if the bound of Corollary 17 can be tightened if one of the target curves is isomorphic to the domain curve, i.e. if we have two loops and a double edge to a different vertex in $\mathcal{G}_\ell(p)$. In fact, even the existence of one loop and a double edge is subject to a tighter bound, though we have to exclude the j-invariants 0 and 1728 as per usual.

Corollary 19. Let $p \neq \ell$ be distinct primes, let E_0, E_1 be supersingular curves over $\overline{\mathbb{F}_p}$ such that $j(E_0) \notin \{0, 1728\}$ and $j(E_0) \neq j(E_1)$, and suppose that there are two non-equivalent ℓ-isogenies $\varphi_0, \varphi_1 \colon E_0 \to E_1$ as well as one degree ℓ endomorphism $\alpha \in \mathrm{End}(E_0)$. Then $p < 4\ell^3$.

Proof. We consider the two endomorphisms α and $\beta := \widehat{\varphi_1} \circ \varphi_0 \in \mathrm{End}(E_0)$ of degree ℓ respectively ℓ^2, noting that these are both cyclic by Proposition 9. As in the proof of Corollary 17 we further see that φ_0 cannot be equivalent to α or $\widehat{\alpha}$ due to $j(E_0) \neq j(E_1)$. Therefore we can directly apply Proposition 16 with $e = 1$ to obtain $p < 4\ell^3$. □

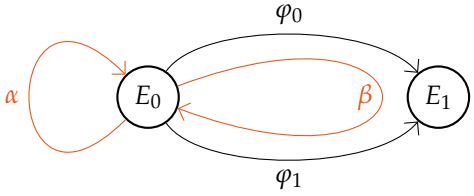
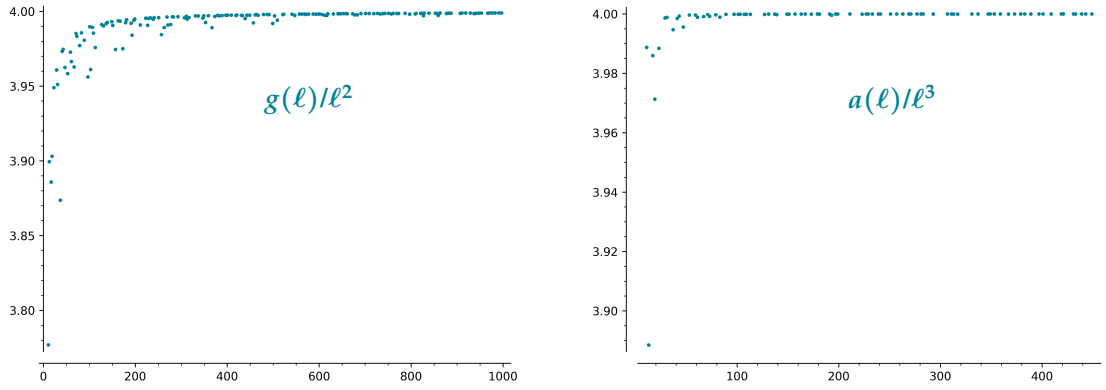


Figure 5: The endomorphisms α and β factor through non-isomorphic curves.

In Figure 6 we illustrate the tightness of the bounds of Proposition 18 and Corollary 19. To this end we computed for a prime ℓ the maximal prime $g(\ell) < 4\ell^2$ such that a triple loop exists in $\mathcal{G}_\ell(g(\ell))$ respectively the maximal prime $a(\ell) < 4\ell^3$ such that a loop and a multi-edge originate from a vertex in $\mathcal{G}_\ell(a(\ell))$ whose j-invariant does not lie in $\{0, 1728\}$, and took the ratio relative to the ℓ-power ℓ^2 respectively ℓ^3; we provide the corresponding data in the files `triple_loop_primes.sage` and `loop_double_primes.sage`.



(a) $g(\ell)/\ell^2$ (Proposition 18)

(b) $a(\ell)/\ell^3$ (Corollary 19)

Figure 6: Illustration of the tightness of the bounds on loops of Proposition 18 and Corollary 19.

3.3 Tighter bounds at $\mathbb{F}_p$-invariants in $\mathcal{G}_\ell(p)$

In this subsection we will look for tighter bounds if one of the vertices' j-invariants belongs not only to $\mathbb{F}_{p^2}$, but even to $\mathbb{F}_p$. For this we introduce some notions related to the Frobenius isogeny, the details on which can be found in [Sil09, Section II.2].

Let E be an elliptic curve over $\overline{\mathbb{F}_p}$ and let $q = p^e$ be a prime power. To E we can associate the q-conjugate curve $E^{(q)}$ by taking the coefficient-wise q-th power of a defining equation for E. This curve satisfies $j(E^{(q)}) = j(E)^q$, and we further have $E = E^{(q)}$ if and only if E is defined over $\mathbb{F}_q$.

Moreover, we have the *q-power Frobenius isogeny* $\pi\colon E \to E^{(q)}$ of degree q, which is defined by mapping a point of E to its coordinate-wise q-th power. If $\varphi\colon E_0 \to E_1$ is an isogeny between curves E_0, E_1 defined over $\mathbb{F}_q$, then we say that φ is *defined over* $\mathbb{F}_q$ if the q-power Frobenius endomorphisms $\pi_i \in \mathrm{End}(E_i)$ satisfy $\pi_1 \circ \varphi = \varphi \circ \pi_0$. Finally, we introduce the *q-Frobenius conjugate* of an isogeny (see also [Fus+25, Lemma 3.4]):

Lemma 20. Let E_0, E_1 be elliptic curves over $\overline{\mathbb{F}_p}$ and let $q = p^e$ be a prime power. For any separable[6] isogeny $\varphi\colon E_0 \to E_1$ there is a unique separable isogeny $\varphi^{(q)}\colon E_0^{(q)} \to E_1^{(q)}$ such that the q-power Frobenius isogenies $\pi_i\colon E_i \to E_i^{(q)}$ satisfy

$$\pi_1 \circ \varphi = \varphi^{(q)} \circ \pi_0.$$

Furthermore, the following holds:

(a) $\deg(\varphi) = \deg(\varphi^{(q)})$.

(b) If $E_0 = E_1$, then $\mathrm{trd}(\varphi) = \mathrm{trd}(\varphi^{(q)})$.

(c) $(\widehat{\varphi})^{(q)} = \widehat{\varphi^{(q)}}$.

(d) If $\psi\colon E_1 \to E_2$ is another separable isogeny, then $(\psi \circ \varphi)^{(q)} = \psi^{(q)} \circ \varphi^{(q)}$.

(e) If E_0 and E_1 are defined over $\mathbb{F}_q$, then φ is defined over $\mathbb{F}_q$ if and only if $\varphi^{(q)} = \varphi$.

[6] The result also holds for arbitrary isogenies, with the resulting isogeny $\varphi^{(q)}$ having the same inseparability degree as φ. In fact, by factoring φ according to [Sil09, Corollary II.2.12], the general case can be deduced directly from the separable case.

Proof. The uniqueness of $\varphi^{(q)}$ follows from the surjectivity of π_0, and its existence follows from [Sil09, Corollary II.2.12], noting that $\pi_1 \circ \varphi$ has inseparability degree q since φ is separable. Due to the multiplicativity of the degree we further have

$$q \deg(\varphi) = \deg(\pi_1) \deg(\varphi) = \deg(\pi_1 \circ \varphi) = \deg(\varphi^{(q)} \circ \pi_0) = \deg(\varphi^{(q)}) \deg(\pi_0) = q \deg(\varphi^{(q)})$$

and we obtain claim (a). In view of Lemma 45(c), claim (b) analogously follows from

$$q \operatorname{trd}(\varphi) = \deg(\widehat{\pi_0}) \operatorname{trd}(\varphi) = \operatorname{trd}(\pi_0 \varphi \widehat{\pi_0}) = \operatorname{trd}(\varphi^{(q)} \pi_0 \widehat{\pi_0}) = \operatorname{trd}(q \varphi^{(q)}) = q \operatorname{trd}(\varphi^{(q)}).$$

Next

$$(\widehat{\varphi})^{(q)} \circ \varphi^{(q)} \circ \pi_0 = (\widehat{\varphi})^{(q)} \circ \pi_1 \circ \varphi = \pi_0 \circ \widehat{\varphi} \circ \varphi = [\deg(\varphi)] \circ \pi_0,$$

so $(\widehat{\varphi})^{(q)} \circ \varphi^{(q)} = [\deg(\varphi)]$ by the surjectivity of π_0, and claim (a) shows that $(\widehat{\varphi})^{(q)}$ is dual to $\varphi^{(q)}$. Further, with the q-power Frobenius isogeny $\pi_2 \colon E_2 \to E_2^{(q)}$, claim (d) directly follows from

$$\pi_2 \circ \psi \circ \varphi = \psi^{(q)} \circ \pi_1 \circ \varphi = \psi^{(q)} \circ \varphi^{(q)} \circ \pi_0.$$

Finally, the uniqueness of $\varphi^{(q)}$ immediately yields claim (e).

□

Remark 4. If φ is given by a rational map (of coprime numerator and denominator), then we obtain a rational map (of coprime numerator and denominator) for $\varphi^{(q)}$ by raising all coefficients in the numerator and denominator to the q-th power, thus justifying the above notation. Moreover, since this process preserves the degrees of both the numerator and the denominator, we obtain an alternative proof of $\deg(\varphi) = \deg(\varphi^{(q)})$ (cf. [Was08, p.51]).

Remark 5. For any isogeny $\varphi \colon E_0 \to E_1$ we have $(\varphi^{(p)})^{(p)} = \varphi^{(p^2)}$. As both all the vertices and all the edges of $\mathcal{G}_\ell(p)$ can be represented by curves respectively isogenies defined over $\mathbb{F}_{p^2}$ due to [AAM19, Theorem 6], the p-Frobenius conjugation given by $E \mapsto E^{(p)}$ and $\varphi \mapsto \varphi^{(p)}$ hence induces an involution on the supersingular ℓ-isogeny graph $\mathcal{G}_\ell(p)$.

Now we focus on our second specialized setting, where we analyze the existence of multi-edges at a vertex with j-invariant in $\mathbb{F}_p$. Unsurprisingly we will have to make some exceptions for the special j-invariants 0 and 1728, for which an analysis complementing the following two results can be found in [LOX20, Theorem 2].

First, if the domain and target j-invariants do not belong to the same field, then even the existence of *two* non-equivalent ℓ-isogenies is subject to a stronger bound:

Corollary 21. Let $p \neq \ell$ be distinct primes, let E_0, E_1 be supersingular curves over $\overline{\mathbb{F}_p}$ and suppose that there are two non-equivalent ℓ-isogenies $\varphi_0, \varphi_1 \colon E_0 \to E_1$. Further assume one of the following:

i) $j(E_0) \in \mathbb{F}_p \setminus \{0, 1728\}$ and $j(E_1) \notin \mathbb{F}_p$, or

ii) $j(E_0) \notin \mathbb{F}_p$ and $j(E_1) \in \mathbb{F}_p$.

Then we have $p < 4\ell^2$.

Proof. First we reduce the proof of case ii) to case i): If $j(E_1) \in \{0, 1728\}$, then Theorem 1 and Equation (2) show that we have at least four non equivalent isogenies from E_1 to E_0 as we have $j(E_0) \notin \{0, 1728\}$, so Theorem 6 yields the claim. Otherwise we dualize to get two non-equivalent ℓ-isogenies $E_1 \to E_0$ with $j(E_0) \notin \mathbb{F}_p$ and $j(E_1) \in \mathbb{F}_p \setminus \{0, 1728\}$, i.e. we are in the situation of case i).

To prove the bound in case i), first note that $\operatorname{Aut}(E_1^{(p)}) = \{\pm 1\}$ by Theorem 1 since we have $j(E_1^{(p)}) = j(E_1)^p \notin \mathbb{F}_p$. Now Lemma 20 yields the ℓ-isogenies $\varphi_0^{(p)}, \varphi_1^{(p)} \colon E_0 \to E_1^{(p)}$, which are easily seen to be non-equivalent again. With this setup we consider the two endomorphisms

$$\alpha := \widehat{\varphi_0} \circ \varphi_1 \in \operatorname{End}(E_0) \ni \widehat{\varphi_0}^{(p)} \circ \varphi_1^{(p)} = \alpha^{(p)},$$

which are both cyclic of degree ℓ^2 by Proposition 9 since $\widehat{\varphi_0}^{(p)}$ is the dual of $\varphi_0^{(p)}$. Moreover, as in the proof of Corollary 17 we see that $\varphi_0^{(p)}$ is not equivalent to φ_1 or to $\widehat{\widehat{\varphi_0}} = \varphi_0$ since the target curves have the distinct j-invariants $j(E_1^{(p)}) = j(E_1)^p \neq j(E_1)$. Since α and $\alpha^{(p)}$ have the same reduced trace $\operatorname{trd}(\alpha) = \operatorname{trd}(\alpha^{(p)})$ by Lemma 20, we can therefore directly apply the stronger variant of Proposition 16 to obtain the bound $p < 4\ell^2$. □

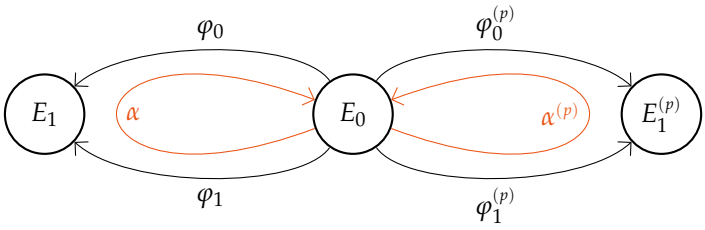


Figure 7: The endomorphisms α and $\alpha^{(p)}$ factor through non-isomorphic curves.

If on the other hand both j-invariants lie in $\mathbb{F}_p$, then the existence of a triple edge between the corresponding vertices is subject to the following stronger bound, assuming that 0 is not the j-invariant of the triple edge's origin:

Proposition 22. Let $p \neq \ell$ be distinct primes, let E_0, E_1 be supersingular curves defined over $\mathbb{F}_p$ and suppose that there are three non-equivalent ℓ-isogenies $\varphi_0, \varphi_1, \varphi_2 \colon E_0 \to E_1$. Further assume that $j(E_0) \in \mathbb{F}_p^\times$ and $j(E_1) \in \mathbb{F}_p$. Then we have $p < 4\ell^2$.

Proof. Due to Theorems 5(a) and 6(a) we may assume that $j(E_0) \notin \{0, 1728\}$. Moreover, due to Equation (2) and Theorem 6 we may assume $j(E_1) \notin \{0, 1728\}$.

Suppose first that φ_1 is not equivalent to $\varphi_1^{(p)}$. Without loss of generality we can further suppose that φ_1 is not equivalent to $\varphi_0^{(p)}$ by swapping φ_0 and φ_2 if necessary. In view of Lemma 20 we now consider the endomorphisms

$$\alpha := \widehat{\varphi_0} \circ \varphi_1 \in \mathrm{End}(E_0) \ni \widehat{\varphi_0}^{(p)} \circ \varphi_1^{(p)} = \alpha^{(p)}.$$

These endomorphisms are both cyclic of degree ℓ^2 by Proposition 9 since $\varphi_0^{(p)} \neq \pm\varphi_1^{(p)}$, and Lemma 20 yields $\mathrm{trd}(\alpha) = \mathrm{trd}(\alpha^{(p)})$.

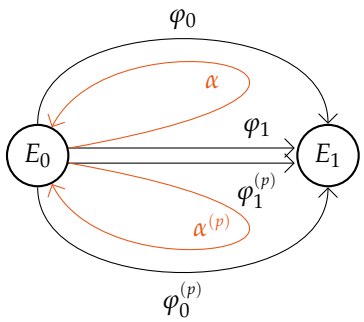


Figure 8: The endomorphisms α and $\alpha^{(p)}$ both factor through E_1.

As φ_1 is not equivalent to the starting edge $\varphi_1^{(p)}$ of $\alpha^{(p)}$ or the starting edge $\varphi_0^{(p)}$ of the dual of $\alpha^{(p)}$ by assumption, we can therefore apply the stronger variant of Proposition 16 to directly obtain the bound $p < 4\ell^2$.

On the other hand, suppose that φ_i is equivalent to $\varphi_i^{(p)}$ for every $i \in \{0, 1, 2\}$. Since we have $j(E_1) \notin \{0, 1728\}$, Theorem 1 shows that there are $\sigma_0, \sigma_1, \sigma_2 \in \{\pm 1\} = \mathrm{Aut}(E_1)$ such that

$$\varphi_i = \sigma_i \varphi_i^{(p)} \quad \text{for } i \in \{0, 1, 2\}.$$

By the pigeonhole principle there now exist two indices $i \neq j$ such that $\sigma_i \sigma_j = 1$, and with this we define the endomorphism $\alpha := \widehat{\varphi_i} \circ \varphi_j \in \mathrm{End}(E_0) \setminus \mathbb{Z}$. In view of Lemma 20 we obtain

$$\alpha^{(p)} = \widehat{\varphi_i}^{(p)} \circ \varphi_j^{(p)} = \widehat{\sigma_i \varphi_i} \circ \sigma_j \varphi_j = \sigma_i \sigma_j \cdot \widehat{\varphi_i} \circ \varphi_j = \alpha,$$

i.e. α is defined over $\mathbb{F}_p$. Now let $\mathrm{End}_{\mathbb{F}_p}(E_0) \subseteq \mathrm{End}(E_0)$ denote the subring of endomorphisms of E_0 that are defined over $\mathbb{F}_p$, and let $\pi \in \mathrm{End}_{\mathbb{F}_p}(E_0)$ denote the p-power Frobenius endomorphism of E_0.

By [DG16, p. 428] we then know that $\mathbb{Z}[\sqrt{-p}] \cong \mathbb{Z}[\pi] \subseteq \mathrm{End}_{\mathbb{F}_p}(E_0)$ is an inclusion of quadratic orders with relative index 1 or 2. In particular, with Corollary 13 and Example 2 we obtain

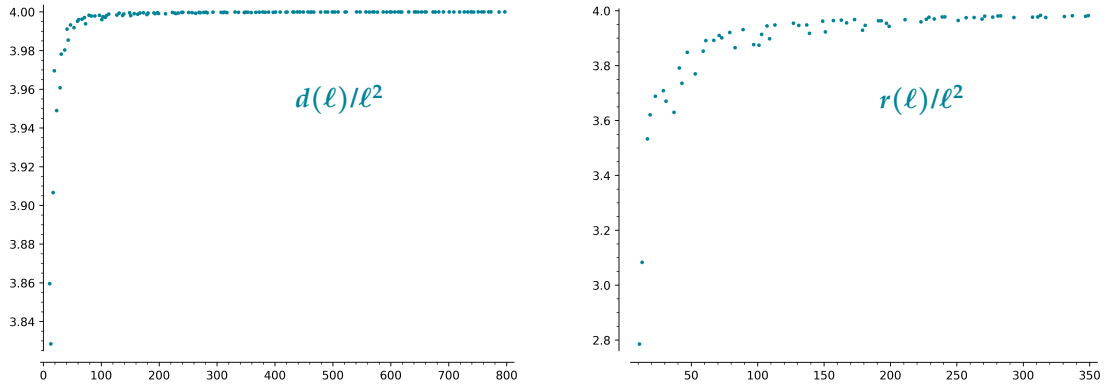
$$|\operatorname{disc}(\mathrm{End}_{\mathbb{F}_p}(E_0))| = \left[\mathrm{End}_{\mathbb{F}_p}(E_0) : \mathbb{Z}[\pi]\right]^{-2} \cdot |\operatorname{disc}(\mathbb{Z}[\pi])| \geq \tfrac{1}{4} \cdot (4\deg(\pi) - \operatorname{trd}(\pi)^2) = p.$$

Applying Corollary 13 to the inclusion $\mathbb{Z}[\alpha] \subseteq \mathrm{End}_{\mathbb{F}_p}(E_0)$ of quadratic orders, we therefore find

$$p \leq |\operatorname{disc}(\mathrm{End}_{\mathbb{F}_p}(E_0))| \leq |\operatorname{disc}(\mathbb{Z}[\alpha])| = 4\deg(\alpha) - \operatorname{trd}(\alpha)^2 \leq 4\ell^2$$

with Equation (1), proving that $p \leq 4\ell^2$ holds also in this second case. Finally, the obtained inequality $p \leq 4\ell^2$ has to be proper since $4\ell^2$ cannot be a prime. □

In Figure 9 we illustrate the tightness of the bounds of Corollary 21 and Proposition 22. To this end we computed for a prime ℓ the maximal prime $d(\ell) < 4\ell^2$ such that a double edge between a vertex of j-invariant in $\mathbb{F}_{d(\ell)} \setminus \{0, 1728\}$ and a vertex of j-invariant in $\mathbb{F}_{d(\ell)^2} \setminus \mathbb{F}_{d(\ell)}$ exists, respectively the maximal prime $r(\ell) < 4\ell^2$ such that a triple edge between two vertices of distinct j-invariants in $\mathbb{F}_{r(\ell)} \setminus \{0, 1728\}$ exists[7], and took the ratio relative to the ℓ-power ℓ^2; the corresponding data can be found in the files `different_field_primes.sage` and `rational_triple_primes.sage`.



(a) $d(\ell)/\ell^2$ (Corollary 21)

(b) $r(\ell)/\ell^2$ (Proposition 22)

Figure 9: Illustration of the tightness of the bounds for $\mathbb{F}_p$-rational invariants of Corollary 21 and Proposition 22.

3.4 Impossibility results for ordinary curves

Both in our techniques and in our results we have limited ourselves to supersingular elliptic curves until now. Therefore we discuss the previously analyzed phenomena in the context of (isogeny graphs of) ordinary elliptic curves in this subsection; more precisely, we explain why they can never occur for ordinary curves, irrespective of the relation between the characteristic p and the prime degree $\ell \neq p$. To discuss the structure of ordinary isogeny graphs, we first make the following definition:

Definition 3. Given distinct prime numbers $p \neq \ell$, the *full ℓ-isogeny graph* over $\overline{\mathbb{F}_p}$ is the infinite directed multigraph with

- vertices: A representative set of isomorphism classes of elliptic curves over $\overline{\mathbb{F}_p}$.
- edges: Given two representatives E_0, E_1, the edges $E_0 \to E_1$ are given by the equivalence classes of ℓ-isogenies $E_0 \to E_1$.

As we will always consider a fixed pair of primes (p, ℓ) that will be clear from the context, we also refer to the above graph simply as the *full isogeny graph*.

[7] We exclude $j = 1728$ and loops here as allowing these cases result in the maximal primes from Figures 14(a) and 6(a).

The supersingular ℓ-isogeny graph $\mathcal{G}_\ell(p)$ is the connected component of the full isogeny graph that contains all classes of supersingular curves over $\overline{\mathbb{F}_p}$, and we have discussed its structure in Section 2.2. In the following we recap the structure of the ordinary (connected) components of the full isogeny graph. These are known as *isogeny volcanoes* and were originally analyzed in [Koh96], though the volcanic terminology was only later introduced in [FM02]. For a thorough treatment we also recommend [Sut13].

To explain the volcanic structure of an ordinary component, we note the following result:

Lemma 23 ([Koh96, Proposition 21])**.** Let $p \neq \ell$ be distinct primes and let $\varphi\colon E_0 \to E_1$ be an ℓ-isogeny between ordinary elliptic curves E_0, E_1 over $\overline{\mathbb{F}_p}$. Then the image of the ring embedding

$$i\colon \operatorname{End}(E_1) \hookrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} \operatorname{End}(E_0),\ \psi \mapsto \tfrac{1}{\ell}\widehat{\varphi} \circ \psi \circ \varphi$$

does not depend on the choice of ℓ-isogeny φ. Moreover, exactly one of the following three cases occurs:

$\rightarrow$: The isogeny φ is *horizontal*, i.e. $\operatorname{End}(E_0) = i(\operatorname{End}(E_1))$.

$\downarrow$: The isogeny φ is *descending*, i.e. $i(\operatorname{End}(E_1)) \subseteq \operatorname{End}(E_0)$ of relative index ℓ.

$\uparrow$: The isogeny φ is *ascending*, i.e. $\operatorname{End}(E_0) \subseteq i(\operatorname{End}(E_1))$ of relative index ℓ.

The vertices of an ordinary (connected) component of the full isogeny graph can now be partitioned into levels $V_0, V_1, V_2, \ldots$ such that all vertices in one level V_i have the same endomorphism ring up to isomorphism, and such that the ℓ-adic valuation of this endomorphism ring's conductor is exactly i. Furthermore, the horizontal ℓ-isogenies give connections between vertices in the same level, descending isogenies give connections from curves of level V_i to curves of level V_{i+1} and ascending isogenies give connections from level V_i to level V_{i-1}. Notably, however, not all types of isogenies occur at every level: Horizontal isogenies only exist at level V_0, and in any level V_i with $i \geq 1$ any vertex has exactly one ascending and ℓ descending isogenies – this is exactly what motivates the volcanic terminology. The following result captures how many isogenies of each type occur at each vertex:

Theorem 24 ([Sut13, Theorem 7 & Remark 8])**.** *Let $p \neq \ell$ be distinct primes, let E be an ordinary elliptic curve over $\overline{\mathbb{F}_p}$ and let $\varphi_i\colon E \to E_i$, $i = 0, \ldots, \ell$, be representatives of the equivalence classes of ℓ-isogenies with domain E. Then the following holds:*

(a) *If $\operatorname{End}(E)$ is ℓ-maximal, i.e. if its conductor is not divisible by ℓ, then at most two[8] of the isogenies $\varphi_0, \ldots, \varphi_\ell$ are horizontal, and none are ascending.*

(b) *If the conductor of $\operatorname{End}(E)$ is divisible by ℓ, then exactly one of the isogenies $\varphi_0, \ldots, \varphi_\ell$ is ascending, and none are horizontal.*

(c) *The remaining isogenies at E are all descending. Moreover, they can be partitioned into sets of size $|\operatorname{Aut}(E)|/2$ according to the isomorphism class of their target curves.*

Even more can be said about the *rim* of the volcano, i.e. the level V_0: It is an (undirected) finite regular graph of degree at most 2, and the number of the vertices in it depends on the class group of the corresponding endomorphism ring (cf. [Sut13, Theorem 7]). For our purposes it suffices to understand the vertices in the rim in the case that $j(E) \in \{0, 1728\}$:

Lemma 25. Let $p \neq \ell$ be distinct primes and let E be an ordinary elliptic curve over $\overline{\mathbb{F}_p}$ such that $j(E) \in \{0, 1728\}$. Then E represents the unique vertex at level V_0 of its connected component.

Proof. Since E is ordinary, we must have $p \geq 5$. According to Theorem 1 we hence see that $\operatorname{End}(E)$ is the ring of integers of its fraction field, so E lies in level V_0 of its connected component. Moreover, any other curve E' in level V_0 (of the same connected component) would have an endomorphism ring isomorphic to $\operatorname{End}(E)$, but this already forces $j(E) = j(E')$ due to Theorem 1. □

[8] Depending on the splitting behavior of ℓ in the field of fractions of $\operatorname{End}(E)$.

Finally, we note here that the volcanoes in the full isogeny graph descend infinitely, i.e. they have infinitely many levels, since we consider all curves over $\overline{\mathbb{F}_p}$, not only over a finite field $\mathbb{F}_q$. In contrast to [FM02, Theorem 2.1] we also consider all ℓ-isogenies defined over $\overline{\mathbb{F}_p}$, not only over $\mathbb{F}_q$.

With this preparation we are ready to analyze our results in the setting of ordinary elliptic curves. Specifically, we show that the special phenomena that occurred for supersingular curves in small characteristics can never occur for ordinary curves:

Corollary 26. Let $p \neq \ell$ be distinct primes and let E_0, E_1, E_2 be ordinary elliptic curves over $\overline{\mathbb{F}_p}$. Then the following holds:

Thms. 5(b) & 6(b): If $j(E_0) = 0$, then there are at most three ℓ-isogenies $E_0 \to E_1$ and at most two ℓ-isogenies $E_0 \to E_0$ up to equivalence.

Thms. 5(a), 6(a) & 15: If $j(E_0) \neq 0$, then there are at most two ℓ-isogenies $E_0 \to E_1$ up to equivalence.

Cor. 17: If $j(E_0) \notin \{0, 1728\}$ and $j(E_1) \neq j(E_2)$, then there cannot be both two non-equivalent ℓ-isogenies $\varphi_1, \psi_1 \colon E_0 \to E_1$ and two non-equivalent ℓ-isogenies $\varphi_2, \psi_2 \colon E_0 \to E_2$.

Cor. 19: If $j(E_0) \notin \{0, 1728\}$ and $j(E_0) \neq j(E_1)$, then there cannot be both a degree ℓ endomorphism $\alpha \in \mathrm{End}(E_0)$ and two non-equivalent ℓ-isogenies $\varphi_0, \varphi_1 \colon E_0 \to E_1$.

Cor. 21: If $j(E_0) \notin \{0, 1728\}$ does not lie in the same field as $j(E_1)$, then there is at most one ℓ-isogeny $E_0 \to E_1$ up to equivalence.

Proof. The first two claims immediately follow from Theorems 24 and 1. The third and fourth claim follow from Theorem 24(a) since by assumption we can only have two non-equivalent ℓ-isogenies to the same curve if that curve lies in the same level, i.e. only if the isogenies are horizontal.

Lastly, if we have $j(E_1) \in \{0, 1728\}$ in the final claim, then the statement follows Lemma 25 and Theorem 24(b). Otherwise the situation is symmetric (cf. Equation (2) and Theorem 1), so we may assume that $j(E_0) \in \mathbb{F}_q$ and $j(E_1) \in \mathbb{F}_{q^r} \setminus \mathbb{F}_q$ for an $r \geq 2$. Now suppose that we have two non-equivalent ℓ-isogenies $\varphi_0, \varphi_1 \colon E_0 \to E_1$. Then Lemma 20 yields the two non-equivalent ℓ-isogenies $\varphi_0^{(q)}, \varphi_1^{(q)} \colon E_0 \to E_1^{(q)}$, and we further have $j(E_1^{(q)}) = j(E_1)^q \neq j(E_1)$ by assumption. Therefore the third claim above yields a contradiction. □

In preparation for Section 5 we close out this section by describing the loops at the vertices of j-invariants 0 and 1728 in slightly more detail. First, the following statement looks at degree ℓ endomorphisms as horizontal ℓ-isogenies in the more general context of *oriented* elliptic curves:

Lemma 27. Let $p \neq \ell$ be distinct primes, let E be an elliptic curve over $\overline{\mathbb{F}_p}$ and let $\mathcal{O} \subseteq \mathrm{End}(E)$ be a quadratic order. Then the following holds:

(a) If $\mathcal{O}$ is not ℓ-maximal, then it does not contain any endomorphism of degree ℓ.

(b) If $\mathcal{O}$ is ℓ-maximal, then it contains at most two non-equivalent degree ℓ endomorphisms, and their equivalence classes are represented by any pair of dual degree ℓ endomorphisms in $\mathcal{O}$.

Proof. Let K be the fraction field of $\mathcal{O}$, write $d_K = \mathrm{disc}(\mathcal{O}_K)$ and $\mathcal{O}_K = \mathbb{Z}[w_K]$ with $w_K = \frac{d_K + \sqrt{d_K}}{2}$. Then, for any $x, y \in \mathbb{Z}$, we have

$$\begin{aligned} \mathrm{nrd}(x + y w_K) &= \mathrm{nrd}\left(x + y\tfrac{d_K}{2} + y\tfrac{\sqrt{d_K}}{2}\right) \\ &= \left(x + y\tfrac{d_K}{2}\right)^2 - \left(y\tfrac{\sqrt{d_K}}{2}\right)^2 = x^2 + xyd_K + \tfrac{1}{4}(d_K^2 - d_K) \cdot y^2 \end{aligned} \tag{4}$$

where $\frac{1}{4}(d_K^2 - d_K)$ is an integer since $d_K \equiv 0, 1 \bmod 4$ due to Example 2.

Now recall that $\mathcal{O} = \mathbb{Z}[f w_K]$ for the conductor $f = [\mathcal{O}_K : \mathcal{O}]$ of $\mathcal{O}$ (see also the stacked bases theorem); hence if $\mathcal{O}$ is not ℓ-maximal and we have an element $x + y w_K \in \mathcal{O}$ with $x, y \in \mathbb{Z}$, then ℓ divides y. If such an element were to satisfy $\ell = \mathrm{nrd}(x + y w_K)$, then taking Equation (4) modulo ℓ would show that x^2 must be divisible by ℓ. Thus $x + y w_K \in \ell \mathcal{O}_K$ since ℓ is prime, and the multiplicativity of the norm forces the contradiction

$$\ell = \mathrm{nrd}(x + y w_K) \in \mathrm{nrd}(\ell \mathcal{O}_K) \subseteq \ell^2 \mathbb{Z},$$

which proves part (a).

On the other hand, if $\mathcal{O}$ is ℓ-maximal, then the ideal $\ell\mathcal{O}$ is prime to the conductor of $\mathcal{O}$ and hence admits a unique factorization into prime ideals of $\mathcal{O}$ by [Cox13, Exercise 7.26]. If we now have two endomorphisms $\alpha, \beta \in \mathcal{O}$ of degree ℓ, then (in the supersingular case due to Lemma 2) we get the factorization

$$\alpha\mathcal{O} \cdot \widehat{\alpha}\mathcal{O} = \ell\mathcal{O} = \beta\mathcal{O} \cdot \widehat{\beta}\mathcal{O}$$

into ideals of prime norm ℓ, which hence are prime ideals. Therefore uniqueness of the factorization shows that β is equivalent to α or $\widehat{\alpha}$, i.e. all equivalence classes of degree ℓ endomorphisms in $\mathcal{O}$ are represented by these two dual isogenies. □

The following result counts the number of loops at the vertices of j-invariant 0 and 1728 both in the ordinary case and for sufficiently large characteristic in the supersingular case:

Lemma 28. Let ℓ be a prime, let k be a field of characteristic $\mathrm{char}(k) \notin \{2, 3, \ell\}$, and let E be an elliptic curve over k of j-invariant $j \in \{0, 1728\}$. Further assume one of the following:

i) $\mathrm{End}(E)$ is a commutative ring, or

ii) $\mathrm{char}(k) = p > 4\ell$.

Then the number e_j of equivalence classes of degree ℓ endomorphisms of E is given by

$$e_{1728} = \begin{cases} 1, & \ell = 2 \\ 2, & \ell \equiv 1 \bmod 4 \\ 0, & \ell \equiv 3 \bmod 4 \end{cases} \quad \text{resp.} \quad e_0 = \begin{cases} 1, & \ell = 3 \\ 2, & \ell \equiv 1 \bmod 3 \\ 0, & \ell \equiv 2 \bmod 3 \end{cases}.$$

Proof. Let $\sigma \in \mathrm{Aut}(E)$ denote an automorphism of order 4 (if $j = 1728$) resp. 3 (if $j = 0$). The proof of Theorem 5 (see Appendix B) shows that for $\mathrm{char}(k) > 4\ell$ all endomorphisms of degree ℓ lie in the quadratic order $\mathbb{Z}[\sigma]$, and this is also true under assumption (i) because we then have $\mathrm{End}(E) = \mathbb{Z}[\sigma]$, as the latter is a maximal quadratic order. Since $\mathbb{Q}(\sigma)$ has class number one due to Theorem 1 (cf. [Neu99, p. 37]), we can compute the number of equivalence classes of degree ℓ endomorphisms by describing the splitting behavior of the ideal $\ell\mathbb{Z}[\sigma]$ into prime ideals.

On the one hand, if $j = 1728$, then $\sigma^2 = -1$ and we obtain from [Neu99, Theorem I.1.4] the claimed number of equivalence classes. On the other hand, if $j = 0$, then σ is a third primitive root of unity and we obtain from [Neu99, Corollary I.10.4] the claimed number of equivalence classes, except for $\ell = 2$. For $\ell = 2$ we still have $e_0 \leq 2$ due to Lemma 27(b), so there has to be a 2-isogeny $E \to E'$ to a curve of j-invariant $j(E') \neq 0$. However, by Equation (2) and Theorem 1 there then have to be at least three equivalence classes of 2-isogenies $E \to E'$. Hence these are all equivalence classes of 2-isogenies with domain E, and we obtain $e_0 = 0$. □

4 The distance between 0 and 1728 versus the diameter of $\mathcal{G}_\ell(p)$

In this section we want to analyze the distance between the vertices of the two special j-invariants 0 and 1728 in the full ℓ-isogeny graph, i.e. when two curves of these j-invariants are ℓ^r-isogenous over $\overline{\mathbb{F}_p}$ for distinct primes $p \neq \ell$ and $r \in \mathbb{N}$. We start with an application of Kaneko's bound, which gives a lower bound on said distance:

Proposition 29. Two curves E_0, E_{1728} of j-invariants $0, 1728 \in \mathbb{F}_p$ are isogenous if and only if they are both supersingular, i.e. if and only if $p \in \{2, 3\}$ or $p \equiv 11 \bmod 12$. Moreover, if they are ℓ^r-isogenous for a prime $\ell \neq p$ and $r \in \mathbb{N}$, then $p < 3\ell^{2r}$.

Proof. Due to $1728 \equiv 0 \bmod 6$ we may assume $p \geq 5$ without loss. Since the supersingular isogeny graph $\mathcal{G}_2(p)$ is connected by Theorem 7, we see that E_0 and E_{1728} are isogenous if they are both supersingular. Conversely, an isogeny $\phi\colon E_{1728} \to E_0$ would yield a $\mathbb{Q}$-algebra isomorphism

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E_0) \cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E_{1728})$$

induced by the conjugation $\mathrm{End}(E_0) \ni \psi \mapsto \frac{1}{\deg\phi} \cdot \widehat{\phi} \circ \psi \circ \phi$. In particular, both curves are either supersingular or both ordinary. By Theorem 1 we furthermore have the special automorphisms $\omega \in \mathrm{Aut}(E_0)$ of order 3 and $\iota \in \mathrm{Aut}(E_{1728})$ of order 4 that satisfy the equations

$$\omega^2 + \omega + 1 = 0 \quad \text{and} \quad \iota^2 + 1 = 0. \tag{5}$$

Hence the above would give an isomorphism $\mathbb{Q}(\sqrt{-3}) \cong \mathbb{Q}(\sqrt{-1})$ if both curves were ordinary and isogenous; as such an isomorphism does not exist, we deduce our first claim in view of Example 1.

Now suppose that we have an ℓ^r-isogeny $E_0 \to E_{1728}$ for an $r \in \mathbb{N}$, so that both curves are supersingular. Then we can also choose an ℓ^m-isogeny $\varphi\colon E_0 \to E_{1728}$ of minimal degree ℓ^m, where necessarily $m \leq r$. From this we obtain the two endomorphisms ω and $\widehat{\varphi} \circ \iota \circ \varphi$ of E_0, and the defining equations (5) imply

$$\begin{aligned} \deg(\omega) &= 1, & \deg(\widehat{\varphi} \circ \iota \circ \varphi) &= \deg(\varphi)^2 \deg(\iota) = \ell^{2m}, \\ \operatorname{trd}(\omega) &= -1, & \operatorname{trd}(\widehat{\varphi} \circ \iota \circ \varphi) &= \deg(\varphi) \cdot \operatorname{trd}(\iota) = 0. \end{aligned} \tag{6}$$

Next we factorize $\varphi = \varphi_m \circ \cdots \circ \varphi_1$ into ℓ-isogenies. Then the minimality of the degree ℓ^m of φ shows that no j-invariant occurs twice in the path described by φ; thus φ_{i+1} is not equivalent to $\widehat{\varphi}_i$ for any $i \in \{1, \ldots, m-1\}$, so φ is cyclic by Proposition 9.

In fact, even the composition $\widehat{\varphi} \circ \iota \circ \varphi$ is a cyclic isogeny. Indeed, as we have the factorization

$$\widehat{\varphi} \circ \iota \circ \varphi = \widehat{\varphi_1} \circ \cdots \circ (\widehat{\varphi_m} \circ \iota) \circ \varphi_m \circ \cdots \circ \varphi_1,$$

the previous argument shows that we only need to prove the non-equivalence of $\widehat{\varphi_m} \circ \iota$ and $\widehat{\varphi_m}$ to apply Proposition 9. However, by the minimality of m we know that $\varphi_m\colon E_{m-1} \to E_{1728}$ is not a loop in $\mathcal{G}_\ell(p)$. Thus $j(E_{m-1}) \neq j(E_{1728})$, so Proposition 4 yields the non-equivalence of $\widehat{\varphi_m} \circ \iota$ and $\widehat{\varphi_m}$.

Hence $\widehat{\varphi} \circ \iota \circ \varphi$ is cyclic by Proposition 9, and this implies that it does not commute with ω. In fact, assume to the contrary that these two endomorphisms commute. Then the cyclic kernel $\ker(\widehat{\varphi} \circ \iota \circ \varphi)$ contains the two subgroups $\ker(\varphi_1)$ and $\ker(\varphi_1 \circ \omega)$ of order ℓ, i.e. φ_1 and $\varphi_1 \circ \omega$ are equivalent. However, the minimality of m implies that the first isogeny $\varphi_1\colon E_0 \to E_1$ is not a loop in $\mathcal{G}_\ell(p)$. Thus $j(E_0) \neq j(E_1)$, so Proposition 4 shows that φ_1 and $\varphi_1 \circ \omega$ are not equivalent. We obtain a contradiction, i.e. $\widehat{\varphi} \circ \iota \circ \varphi$ and ω do not commute.

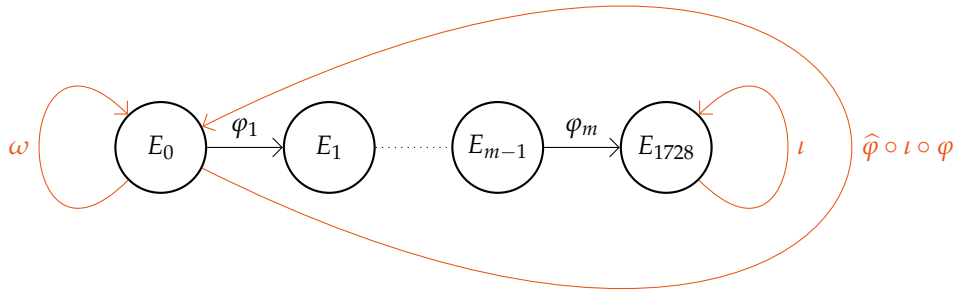


Figure 10: The endomorphisms ω and $\widehat{\varphi} \circ \iota \circ \varphi$ do not commute, where $\varphi = \varphi_m \circ \cdots \circ \varphi_1$.

Recalling the quantities computed in the Equations (6), Kaneko's bound now yields

$$\begin{aligned} 4p &\leq \operatorname{disc}(\mathbb{Z}[\widehat{\varphi} \circ \iota \circ \varphi]) \cdot \operatorname{disc}(\mathbb{Z}[\omega]) \\ &= \Big(\operatorname{trd}(\widehat{\varphi} \circ \iota \circ \varphi)^2 - 4 \cdot \deg(\widehat{\varphi} \circ \iota \circ \varphi)\Big) \cdot \Big(\operatorname{trd}(\omega)^2 - 4 \cdot \deg(\omega)\Big) \\ &= (0 - 4 \cdot \ell^{2m}) \cdot (1 - 4 \cdot 1) = 12\ell^{2m} \leq 12\ell^{2r}. \end{aligned}$$

Therefore $p \leq 3\ell^{2r}$, and this inequality has to be proper as $3\ell^{2r}$ cannot be a prime. □

Remark 6. For comparison, [LB20, Theorem 1.3] gives the looser bound $p \leq 4\ell^{2r}$ in our setting: Indeed, the j-invariants 0 and 1728 are 1-small due to Theorem 1 and have fundamental discriminants -3 respectively -4, so the mentioned result yields

$$\ell^r \geq d(0, 1728) \geq \tfrac{\sqrt{p}}{2}, \text{ i.e. } 4\ell^{2r} = (2\ell^r)^2 \geq p.$$

In Figure 11 we illustrate the tightness of the bound of Proposition 29; we provide the corresponding data in the file `special_path_primes.sage`.

Remark 7. For slightly above two thirds of the values m considered in Figure 11 the prime $s(m)$ is the largest prime below $3m^2$ in the equivalence class of 11 modulo 12. Contrastingly, $m = 269$ achieves the biggest number of primes congruent to 11 modulo 12 between $s(m) + 1$ and $3m^2$, namely 22.

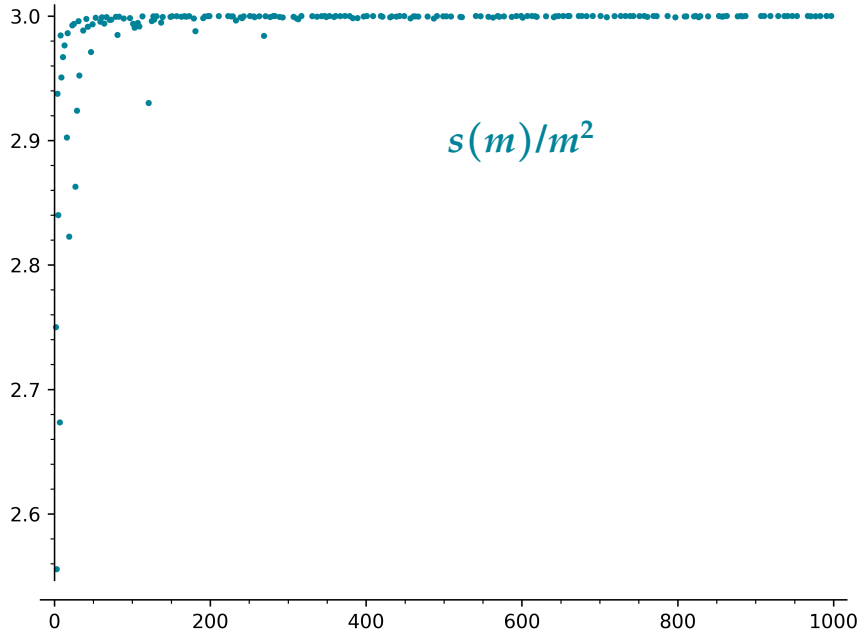


Figure 11: Plot of $s(m)/m^2$, where $s(m) < 3m^2$ is the maximal prime for which 0 and 1728 are isogenous as j-invariants in $\mathbb{F}_{s(m)}$ via a cyclic m-isogeny, for primes $m = \ell < 1000$ and non-prime prime powers $m = \ell^r < 400$.

As E_0 and E_{1728} can only be ℓ^r-isogenous if both lie in the connected graph $\mathcal{G}_\ell(p)$ by the above result, it is natural to search for a comparison between their distance and the diameter of $\mathcal{G}_\ell(p)$. Clearly this diameter is an upper bound for this distance, but we want to see if the diameter also leads to a lower bound. To this end we derive an explicit upper bound on said diameter, which will be a special case of the following more general bound that will find a second application later in this section.

Theorem 30. *Let $p \neq \ell$ be distinct primes with $p \geq 5$. Further let X and Y be two sets of vertices in $\mathcal{G}_\ell(p)$, and let $N \in \mathbb{N}_0$ such that there is no path of length at most N in $\mathcal{G}_\ell(p)$ between any $x \in X$ and $y \in Y$. Then*

$$N < 2\log_\ell\left(\frac{2}{\sqrt{c_X c_Y}} \cdot \frac{p-1}{12}\right),$$

where for any vertex set Z we write

$$c_Z := \begin{cases} |Z|, & 1728 \notin j(Z) \not\ni 0 \\ |Z| - \frac{1}{2}, & 1728 \in j(Z) \not\ni 0 \\ |Z| - \frac{2}{3}, & 1728 \notin j(Z) \ni 0 \\ |Z| - \frac{7}{6}, & 1728 \in j(Z) \ni 0 \end{cases}$$

Proof. We adapt our proof from [RM20, Theorem 2], which goes back to [VDH95, Theorem 2.3], while we account for the directed setting using the insights of [Bas+23, Section 3.1]. To this end, let $V = \{E_1, \ldots, E_n\}$ denote the vertex set of $\mathcal{G}_\ell(p)$ and consider the $|V|$-dimensional $\mathbb{C}$-vector space $\mathbb{C}^V$ spanned by V. On $\mathbb{C}^V$ we define an inner product via sesquilinear[9] extension of

$$\langle E_i, E_j \rangle := \frac{2}{|\operatorname{Aut}(E_j)|} \cdot \delta_{i,j} \tag{7}$$

where the Kronecker delta $\delta_{i,j}$ is 1 if $i = j$ and 0 otherwise. Due to Equation (2) we now know that the adjacency matrix A of $\mathcal{G}_\ell(p)$ is self-adjoint with respect to the above inner product when viewed as an operator on $\mathbb{C}^V$ via $w \mapsto A \cdot w$ (see also Remark 8 after this proof).

[9] Antilinear in the first, linear in the second component.

By the spectral theorem we can hence find an orthonormal basis $u_1, \dots, u_n$ of $\mathbb{C}^V$ by combining orthonormal bases of the eigenspaces of A. Furthermore, by the polynomial functional calculus for normal operators[10] we have

$$f(A) \cdot w = \sum_{t=1}^{n} f(\lambda_t) \langle u_t, w \rangle u_t \tag{8}$$

for any polynomial $f \in \mathbb{C}[\lambda]$ and any vector $w \in \mathbb{C}^V$, where λ_t is the eigenvalue of A corresponding to the eigenvector u_t.

We now identify a subset $Z \subseteq V$ with the corresponding sum vector $\sum_{z \in Z} z \in \mathbb{C}^V$, and Theorem 1 gives for any vertex sets $Z, Z' \subseteq V$ the equation

$$\langle Z, Z' \rangle = \langle Z', Z \rangle = \sum_{z_1 \in Z'} \sum_{z_2 \in Z} \langle z_1, z_2 \rangle = \sum_{z \in Z \cap Z'} \langle z, z \rangle = c_{Z \cap Z'}. \tag{9}$$

Importantly, the 'full' sum vector V generates the one-dimensional eigenspace corresponding to the eigenvalue $\ell + 1$ of A by Theorem 7, and due to Theorem 3 and Example 1 we have (see also [Hus04, Theorem 13.4.1])

$$\langle V, V \rangle = c_V = \frac{p-1}{12}; \tag{10}$$

for ease of notation we will thus assume $\lambda_1 = \ell + 1$ and $u_1 = V / \sqrt{c_V}$ in the following.

Now let $f \in \mathbb{C}[\lambda]$ be a polynomial of degree at most N. For any $x = E_i \in X$ and $y = E_j \in Y$ the (i,j)-th entry of $f(A)$ is zero by our assumption that there is no path of length at most N between x and y. This implies $\langle x, f(A)y \rangle = 0$, as the inner product gives the (i,j)-th entry of $f(A)$ up to rescaling by the factor $\frac{2}{|\operatorname{Aut}(E_i)|}$. Therefore

$$\langle X, f(A)Y \rangle = \sum_{x \in X} \sum_{y \in Y} \langle x, f(A)y \rangle = 0,$$

and Equation (8) further yields

$$0 = \langle X, f(A)Y \rangle = \sum_{t=1}^{n} f(\lambda_t) \langle u_t, Y \rangle \langle X, u_t \rangle.$$

Putting the term for $t = 1$ on the other side and taking the absolute value, we hence get

$$\left| f(\ell+1) \cdot \frac{\langle V, Y \rangle \langle X, V \rangle}{\langle V, V \rangle} \right| = \left| \sum_{t=2}^{n} f(\lambda_j) \langle u_t, Y \rangle \langle X, u_t \rangle \right| \leq \sup_{a \in [-2\sqrt{\ell}, 2\sqrt{\ell}]} |f(a)| \sum_{t=2}^{n} |\langle u_t, Y \rangle| \cdot |\langle X, u_t \rangle|$$

as the eigenvalues $\lambda_2, \dots, \lambda_n$ of A lie in the Hasse interval $[-2\sqrt{\ell}, 2\sqrt{\ell}]$ by Theorem 7. With the Cauchy–Schwarz inequality and Parseval's identity we furthermore have

$$\sum_{t=2}^{n} |\langle u_t, Y \rangle| \cdot |\langle X, u_t \rangle| \leq \sqrt{\sum_{t=2}^{n} |\langle u_t, Y \rangle|^2} \cdot \sqrt{\sum_{t=2}^{n} |\langle X, u_t \rangle|^2} \leq \sqrt{\langle Y, Y \rangle} \cdot \sqrt{\langle X, X \rangle} = \sqrt{c_Y} \cdot \sqrt{c_X}.$$

In view of Equation (9), we therefore obtain

$$\left| \frac{f(\ell+1)}{\langle V, V \rangle} \right| \leq \sup_{a \in [-2\sqrt{\ell}, 2\sqrt{\ell}]} |f(a)| \cdot \frac{\sqrt{c_Y}}{\langle V, Y \rangle} \cdot \frac{\sqrt{c_X}}{\langle X, V \rangle} = \frac{1}{\sqrt{c_X c_Y}} \cdot \sup_{a \in [-2\sqrt{\ell}, 2\sqrt{\ell}]} |f(a)|. \tag{11}$$

Now we consider the N-th Chebyshev polynomial $T_N \in \mathbb{C}[\lambda]$ of the first kind, which is uniquely determined[11] by the identity [MH02, Equation (1.49)]

$$T_N(\lambda) = \frac{1}{2} \left[(\lambda + \sqrt{\lambda^2 - 1})^N + (\lambda - \sqrt{\lambda^2 - 1})^N \right].$$

[10] Due to linearity it suffices to confirm the equation for any orthonormal basis eigenvector $w = u_t$, which is immediate.

[11] Explicitly, we have $T_0 = 1$, $T_1 = \lambda$ and $T_N = 2\lambda \cdot T_{N-1} - T_{N-2}$ for $N \geq 2$ (cf. [MH02, Equation (1.3a-b)]).

In particular, for $a \in [-1,1]$ we have $T_N(a) = \cos(N \cdot \arccos(a))$ (see [MH02, Equation (1.1)]), and thus $|T_N(a)| \leq 1$. This allows us to define

$$f(\lambda) \coloneqq T_N(\lambda/2\sqrt{\ell}), \text{ so that } |f(a)| \leq 1 \text{ for } a \in [-2\sqrt{\ell}, 2\sqrt{\ell}].$$

Using Equation (10), we now apply Equation (11) to this specific polynomial to get

$$\begin{aligned}
\frac{1}{\sqrt{c_X c_Y}} \cdot \frac{p-1}{12} &\geq |f(\ell+1)| = \left|T_N\left((\ell+1)/2\sqrt{\ell}\right)\right| \\
&= \frac{1}{2} \cdot \left[(\lambda + \sqrt{\lambda^2-1})^N + (\lambda - \sqrt{\lambda^2-1})^N\right] \\
&> \frac{1}{2} \cdot (\lambda + \sqrt{\lambda^2-1})^N = \frac{1}{2} \cdot \left(\frac{\ell+1+\sqrt{(\ell+1)^2-4\ell}}{2\sqrt{\ell}}\right)^N \\
&= \frac{1}{2} \cdot \left(\frac{\ell+1+\ell-1}{2\sqrt{\ell}}\right)^N = \frac{1}{2}\sqrt{\ell}^N = \frac{1}{2}\ell^{N/2}
\end{aligned}$$

where we briefly wrote $\lambda = (\ell+1)/2\sqrt{\ell} > 1$ for readability. Multiplying by 2, taking ℓ-base logarithms and then again multiplying by 2 thus leads to the desired bound. □

Remark 8. In [Bas+23, Section 3.1] the authors instead set $\langle E_i, E_j \rangle \coloneqq \frac{|\operatorname{Aut}(E_i)|}{2} \cdot \delta_{i,j}$ and state that A is self-adjoint with respect to this inner product as well, which is true when A is viewed as an operator via right multiplication $w \mapsto w \cdot A$. To use this fact in the proof of Theorem 30, one would hence instead have to look at the left eigenvector $\sum_{i=1}^{n} \frac{2}{|\operatorname{Aut}(E_i)|} E_i$ of A. The rest of the proof works analogously to the above, but one obtains the same bound with the same estimate in Equation (11).

Our diameter bound is now a simple application of Theorem 30:

Corollary 31. Let $p \neq \ell$ be primes with $p \neq 2$. Then the diameter of $\mathcal{G}_\ell(p)$ is at most $2\log_\ell\left(\frac{p-1}{\sqrt{6}}\right) + 1$.

Proof. Since the bound is non-negative for $p \geq 3$ and any $\ell \neq p$, we may assume that $\mathcal{G}_\ell(p)$ has positive diameter $d \in \mathbb{N}$; in particular, due to Theorem 3 we have $p \geq 5$. Now set $N \coloneqq d-1$, so that there are vertices x, y in $\mathcal{G}_\ell(p)$ with no path of length at most N between them. Then we can apply Theorem 30 to the singleton sets $X = \{x\}$ and $Y = \{y\}$: Due to $X \cap Y = \emptyset$ we have

$$c_X \cdot c_Y \geq \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{2}{3}\right) = \frac{1}{6}, \tag{12}$$

so our result gives the desired bound

$$d = N + 1 < 2\log_\ell\left(2\sqrt{6} \cdot \tfrac{p-1}{12}\right) + 1 = 2\log_\ell\left(\tfrac{p-1}{\sqrt{6}}\right) + 1.$$

□

Remark 9. As can be seen in Equation (12), the factor inside the logarithm of Corollary 31's bound can be improved if one knows that the vertices x and/or y are not of the special j-invariants 0 or 1728. For $\ell = 2$ one can also obtain the slightly tighter bound

$$d \leq 2\log_2\left(2\sqrt{2} \cdot \tfrac{p-1}{12}\right) + 2 = 2\log_2\left(\tfrac{p-1}{\sqrt{6}}\right) + (2 - \log_2(3))$$

from Theorem 30 by first walking one step from the curve of j-invariant 0 in $\mathcal{G}_2(p)$.

In the undirected case $p \equiv 1 \bmod 12$ (cf. Corollary 8) we lose the factor of $\sqrt{6}$ in Equation (11) completely, so

$$d \leq 2\log_\ell\left(\tfrac{p-1}{6}\right) + 1 = 2\log_\ell(n) + 2\log_\ell(2) + 1 \tag{13}$$

where $n = \frac{p-1}{12}$ is the number of vertices of $\mathcal{G}_\ell(p)$ by Theorem 3. In comparison, the classical bound due to Pizer [Piz90, Theorem 1] is given by $d \leq 2\log_\ell(n) + 2$ since $\mathcal{G}_\ell(p)$ is non-bipartite (cf. [Bas+23, Theorem 8]); this bound would be slightly better for $\ell \in \{2,3\}$, but worse as soon as $\ell \geq 5$.

Confusingly, however, Pizer's bound for bipartite graphs seems to coincide with the above bound for non-bipartite graphs, while conversely [RM20, Theorem 2] would give Pizer's bound for non-bipartite graphs in the bipartite setting (see also [VDH95, Section 4.1]). This suggests that either both of the above bounds are always satisfied, or that the two diameter bounds in [Piz90, Theorem 1] are assigned the wrong way around.

In conjunction with Proposition 29 we can now give a lower bound on the distance between the curves of j-invariants 0 and 1728 in $\mathcal{G}_\ell(p)$ in terms of the diameter of the graph.

Corollary 32. Let $p \neq \ell$ be distinct primes and assume that $p \equiv 11 \bmod 12$. Then the distance between the curves of j-invariants 0 and 1728 in $\mathcal{G}_\ell(p)$ is at least one fourth of the diameter of $\mathcal{G}_\ell(p)$.

Proof. Let $r \in \mathbb{N}$ be the distance between the curves of j-invariants 0 and 1728, so that $r > \frac{1}{2}\log_\ell(\frac{p}{3})$ due to Proposition 29. Further let $d \in \mathbb{N}$ denote the diameter of $\mathcal{G}_\ell(p)$ and note that we may assume $r < d$. Then the curves E_i and E_j in the proof of Corollary 31 satisfy $\{j(E_i), j(E_j)\} \neq \{0, 1728\}$, so Remark 9 gives the improved bound

$$d \leq 2\log_\ell\left(2\sqrt{3}\cdot\tfrac{p-1}{12}\right) + 1 < 2\log_\ell\left(\tfrac{p}{3}\right) + 1 < 4\cdot r + 1$$

and therefore $d \leq 4r$, i.e. $r \geq \frac{1}{4}d$, since $4r$ is an integer. □

Remark 10. Experimentally, the distance between 0 and 1728 seems to be much closer to d for most small pairs (p, ℓ), but the factor $\frac{1}{4}$ does not seem to be too loose for a general bound: For example, for $(p, \ell) = (1871, 5)$ the distance between 0 and 1728 is 2, whereas the diameter of $\mathcal{G}_5(1871)$ is 6.

For our second application, we mention the folklore statement that the diameter of $\mathcal{G}_\ell(p)$ is "essentially $\log(p)$" (see, for example, [DF+20, p. 55]). While the data of [Arp+23, Section 6]) suggests that for $\ell = 2$ all vertices have a distance approximately bounded by $\log(p)$, in the general case we can at least prove that almost all of the vertices have such a distance. To formalize this idea, we adapt the formulation of [Sar18, Theorem 1.5] to our setting:

Corollary 33. Let $p \neq \ell$ be distinct primes with $p \geq 5$, let $\epsilon > 0$ and fix an integer $N \in \mathbb{N}$ with

$$N > (1+\varepsilon)\log_\ell\left(\tfrac{p-1}{12}\right).$$

Further pick a vertex x of $\mathcal{G}_\ell(p)$ and let $V(x, N)$ denote the set of vertices in $\mathcal{G}_\ell(p)$ to which there is no path from x of length at most N in $\mathcal{G}_\ell(p)$. Then

$$|V(x,N)| \leq 2|\mathrm{Aut}(x)| \cdot \left(\frac{p-1}{12}\right)^{1-\epsilon} + \frac{7}{6}.$$

Remark 11. Let us explain how the above statement fits the idea that $\mathcal{G}_\ell(p)$ has "essentially $\log(p)$" diameter: By Theorem 3 we know that $\mathcal{G}_\ell(p)$ has $n \geq \frac{p-1}{12}$ vertices, so for $N > (1+\epsilon)\log_\ell\left(\frac{p-1}{12}\right)$ with $\epsilon > 0$ we get

$$\frac{|V(x,N)|}{n} \leq 2|\,\mathrm{Aut}(x)| \cdot \left(\frac{p-1}{12}\right)^{-\epsilon} + \frac{14}{p-1} \xrightarrow{p\to\infty} 0,$$

i.e. the number of vertices in $V(x, N)$ relative to the number of all vertices approaches 0 when p (equivalently, when n) goes to infinity.

Proof of Corollary 33. We apply Theorem 30 with $X := \{x\}$ and $Y := V(x, N)$. This gives

$$(1+\epsilon)\log_\ell\left(\tfrac{p-1}{12}\right) < N < 2\cdot\log_\ell\left(\tfrac{2}{\sqrt{c_X c_Y}}\cdot\tfrac{p-1}{12}\right),$$

and exponentiation with respect to base ℓ yields

$$\left(\frac{p-1}{12}\right)^{1+\epsilon} \leq \frac{4}{c_X c_Y}\cdot\left(\frac{p-1}{12}\right)^2.$$

Finally, we only need to rearrange for c_Y and use the bound $c_Y \geq |Y| - \frac{7}{6}$ (cf. Theorem 30) to obtain

$$|V(x,N)| = |Y| \leq c_Y + \frac{7}{6} \leq \frac{4}{c_X} \cdot \left(\frac{p-1}{12}\right)^{1-\epsilon} + \frac{7}{6} = 2|\operatorname{Aut}(x)| \cdot \left(\frac{p-1}{12}\right)^{1-\epsilon} + \frac{7}{6}.$$

□

Note that the involvement of the factor $|\operatorname{Aut}(x)|$ in the bound of Corollary 33 also has an intuitive explanation: Since the vertex x has approximately $c_{\{x\}}$ times as many neighbors as a vertex z with $\operatorname{Aut}(z) = \{\pm 1\}$, we expect to reach approximately $c_{\{x\}}^{-1} = |\operatorname{Aut}(x)|/|\{\pm 1\}|$ times as many vertices from x as we reach from z (on average) after a fixed number of steps. For essentially the same reason one needs the modified cardinalities c_Z in Theorem 30.

Remark 12. As in Remark 9 we note that we can obtain a (slightly) better bound if we know that Y does not contain a vertex of j-invariant 0 or 1728. In particular, in the undirected case $p \equiv 1 \bmod 12$ (cf. Corollary 8) we obtain the bound

$$|V(x,N)| \leq 4 \cdot \left(\frac{p-1}{12}\right)^{1-\epsilon} = 4 \cdot n^{1-\epsilon}. \tag{14}$$

To close out this section, let us mention that our bounds also extend to general (undirected) $(\ell+1)$-regular Ramanujan graphs with n vertices, where ℓ need not be prime, since we only need the isogeny-based machinery to handle the issue of directedness via the inner product (7). Explicitly, Theorem 30 turns into the bound

$$N < 2\log_\ell\left(\frac{2}{\sqrt{|X| \cdot |Y|}} \cdot n\right),$$

Equation (13) gives the diameter bound of [RM20, Theorem 2] if we replace $\lambda(X)$ by the Ramanujan bound $2\sqrt{\ell}$, and Equation (14) improves the bound from [Sar18, Theorem 1.5] by the factor $\frac{4}{(1+N)^2}$.

5 Counting loops in ℓ-isogeny graphs

To compute the data for Figure 6(a) on the existence of triple loops, we used a crucial trick for optimization, which we describe and justify in this section since it might be of independent interest.

First we recall the existence of the m-th classical modular polynomial $\Phi_m \in \mathbb{Z}[X,Y]$: Over any (perfect) field k of characteristic coprime to m it satisfies $\Phi_m(j_0, j_1) = 0$ for $j_0, j_1 \in k$ if and only if we can find elliptic curves E_0, E_1 over k with j-invariants $j(E_i) = j_i$ such that there exists a cyclic m-isogeny $\varphi\colon E_0 \to E_1$ [Sut13, Section 2.3]. Moreover, for $m = \ell$ a prime, the number of equivalence classes of ℓ-isogenies $E_0 \to E_1$ is given by the multiplicity of $j(E_1)$ as a root of $\Phi_\ell(j(E_0), Y)$ [AAM19, Section 2.4]. For reference, for primes $\ell < 1000$ and prime powers $m = \ell^r < 400$ these polynomials can be found in Sutherland's database of classical modular polynomials[12]; they were computed with the algorithms described in [BLS10, Section 6] and [BOS16, Algorithm 1.1].

To determine how many equivalence classes of degree ℓ endomorphisms $E \to E$ there are at each vertex E, one would expect to factor the 'diagonal' polynomial $\Phi_\ell(X,X) \in k[X]$, and then to compute for each of its roots $j_0 \in \bar{k}$ the multiplicity of j_0 as a root of the univariate polynomial $\Phi_\ell(j_0, Y)$. However, it is well-known that this second step is superfluous when $k = \mathbb{C}$, since then this multiplicity can already be read off from the factorization of $\Phi_\ell(X,X)$:

Theorem 34 ([Cox13, Theorem 13.4]). *Let ℓ be a prime and let $\mathcal{E}$ be an elliptic curve over $\mathbb{C}$. Then the number of equivalence classes of ℓ-isogenies $\mathcal{E} \to \mathcal{E}$ coincides with the multiplicity $\mu_\ell(j(\mathcal{E}); \mathbb{C})$ of $j(\mathcal{E})$ as a root of $\Phi_\ell(X,X) \in \mathbb{C}[X]$.*

Naturally, one might wonder to what extent this result translates to positive characteristic. The following example shows that it fails in general:

Example 3. For $p = 43$ and $\ell = 11$ the diagonal polynomial $\Phi_{11}(X,X)$ has a root of multiplicity 3 at $j_0 = 1728 = 8 \in \mathbb{F}_p$. However, the multiplicity of j_0 as a root of $\Phi_{11}(8,Y)$ is only 2.

[12] https://math.mit.edu/~drew/ClassicalModPolys.html

In the spirit of the previous section, the obstructions to this result are again limited to small characteristics relative to ℓ. Moreover, we at least always have an upper bound on the number of equivalence classes:

Theorem 35. *Let $p \neq \ell$ be distinct primes, let E be an elliptic curve over $\overline{\mathbb{F}_p}$ and let $\mu_\ell(j_0; \overline{\mathbb{F}_p})$ denote the multiplicity of $j_0 \in \overline{\mathbb{F}_p}$ as a root of $\Phi_\ell(X, X) \in \mathbb{F}_p[X]$. Then the following holds:*

(a) *There are at most $\mu_\ell(j(E); \overline{\mathbb{F}_p})$ equivalence classes of ℓ-isogenies $E \to E$.*

(b) *If $p > 4\ell$, then there are exactly $\mu_\ell(j(E); \overline{\mathbb{F}_p})$ equivalence classes of ℓ-isogenies $E \to E$.*

In fact, one can even prove the following strengthening of part (b) above:

Theorem 36. *Let $p \neq \ell$ be distinct primes. Then the following are equivalent:*

(i) *For any elliptic curve E over $\overline{\mathbb{F}_p}$ there are exactly $\mu_\ell(j(E); \overline{\mathbb{F}_p})$ equivalence classes of ℓ-isogenies $E \to E$.*

(ii) *The full ℓ-isogeny graph has exactly 2ℓ loops.*

(iii) *p does not divide $4\ell - t^2$ for any $t \in \mathbb{Z}$ with $t^2 < 4\ell$.*

The above results seem to be somewhat folklore, but complete proofs for them are hard to pinpoint in the literature. We therefore give proofs in this article using reductions of elliptic curves; for this we will recall the necessary facts, but refer the reader to [Lan87, Chapter 9] and [Sil09, Chapter VII] for the general definitions. Moreover, the proof of the stronger version (Theorem 36) is based on a 'global' counting argument using Hurwitz class numbers; as we later want to look at a single (ordinary) elliptic curve, we relay the proof of this stronger version to Appendix C, and only prove Theorem 35 via a 'local' argument here. To this end we recall Deuring's lifting theorem:

Deuring's lifting theorem ([Lan87, Theorem 13.5.14]). *For any elliptic curve E over $\overline{\mathbb{F}_p}$ and endomorphism $\overline{\alpha} \in \mathrm{End}(E)$ there exists a number field L, a prime $\mathfrak{P}$ of L above p and an elliptic curve $\mathcal{E}$ over L together with an endomorphism $\alpha \in \mathrm{End}(\mathcal{E})$ such that $\mathcal{E}$ has good reduction at $\mathfrak{P}$, the reduction of $\mathcal{E}$ modulo $\mathfrak{P}$ is isomorphic to E and the reduction of α modulo $\mathfrak{P}$ corresponds to $\overline{\alpha}$ under this isomorphism.*

Before we begin the proof, we further mention that for two curves $\mathcal{E}_1, \mathcal{E}_2$ defined over L with good reduction at $\mathfrak{P}$ and reductions E_1, E_2 we also obtain a reduction map $\mathrm{Hom}_L(\mathcal{E}_1, \mathcal{E}_2) \hookrightarrow \mathrm{Hom}(E_1, E_2)$ of isogenies $\mathcal{E}_1 \to \mathcal{E}_2$ defined over L[13]. This induced map is an injective group homomorphism compatible with dualization and composition of isogenies defined over L; in particular, it is a ring homomorphism if $E_1 = E_2$ and $\mathcal{E}_1 = \mathcal{E}_2$ (cf. [Lan87, Section 13.2] and [Sil94, Proposition II.4.4]).

Proof of Theorem 35. Clearly there is at least one equivalence class of ℓ-isogenies $E \to E$ if and only if $\mu_\ell(j(E); \overline{\mathbb{F}_p}) > 0$, so we may assume that this multiplicity is positive.

First we prove claim (a): Let $\overline{\alpha} \in \mathrm{End}(E)$ be of degree ℓ and apply Deuring's lifting theorem to obtain a number field L, a prime $\mathfrak{P}$ above p, an elliptic curve $\mathcal{E}$ over L and an $\alpha \in \mathrm{End}(\mathcal{E})$ such that $\mathcal{E}$ reduces to a curve isomorphic to E modulo $\mathfrak{P}$ and the reduction of α modulo $\mathfrak{P}$ corresponds to $\overline{\alpha}$ under this isomorphism. By enlarging L and picking a prime above $\mathfrak{P}$, we may further assume that L contains all roots $j_1, \dots, j_n$ of $\Phi_\ell(X, X)$ over $\mathbb{C}$. Then these roots are all elements of the ring of integers of L since $\Phi_\ell(X, X)$ has integer coefficients, and hence any elliptic curve over L with j-invariant j_i has potential good reduction at $\mathfrak{P}$ by [Sil09, Proposition VII.5.5].

By enlarging L once more, we may therefore assume that for any $i \in \{1, \dots, n\}$ we have an elliptic curve $\mathcal{E}_i$ over L with j-invariant $j(\mathcal{E}_i) = j_i$, good reduction at $\mathfrak{P}$ and such that all isogenies among $\mathcal{E}_1, \dots, \mathcal{E}_n$ (including endomorphisms) are defined over L[14]. Fixing an embedding $\mathcal{O}_L/\mathfrak{P} \hookrightarrow \overline{\mathbb{F}_p}$, we now get the factorization

$$\Phi_\ell(X, X) = \prod_{i=1}^{n} (X - j_i \bmod \mathfrak{P})^{\mu_\ell(j_i; \mathbb{C})}$$

in $\overline{\mathbb{F}_p}[X]$, and hence

$$\mu_\ell(j(E); \overline{\mathbb{F}_p}) = \sum_{i:\, j_i \bmod \mathfrak{P} = j(E)} \mu_\ell(j_i; \mathbb{C}). \tag{15}$$

[13] That is, invariant with respect to the action of the Galois group $\mathrm{Gal}(\overline{L}|L)$ on the set $\mathrm{Hom}(\mathcal{E}_1, \mathcal{E}_2)$ of isogenies $\mathcal{E}_1 \to \mathcal{E}_2$.

[14] For this last part we only need to replace L by a finite extension since $\mathrm{Hom}(\mathcal{E}_i, \mathcal{E}_m)$ is a lattice of rank at most 4 by [Sil09, Corollary III.7.5]; more precisely, from [Sil09, Corollary III.9.4] one can easily deduce that it has rank at most 2.

Furthermore, the lifted endomorphism α also has degree ℓ, and we thus find $j(\mathcal{E})$ among the different roots $j_1, \dots, j_n$ of $\Phi_\ell(X, X)$, i.e. we may without loss assume $\mathcal{E} = \mathcal{E}_i$ for some i. This proves that any degree ℓ endomorphism of E can be obtained via reduction of an endomorphism of degree ℓ at a curve (defined over L) whose j-invariant is a root of $\Phi_\ell(X, X)$ over $\mathbb{C}$.

Noting that equivalent endomorphisms stay equivalent after reduction, we hence see that reduction modulo $\mathfrak{P}$ induces a well-defined surjection

$$\Psi\colon \bigsqcup_{i\colon j_i \bmod \mathfrak{P} = j(E)} \left(\mathrm{Aut}(\mathcal{E}_i) \backslash^{\{\ell\text{-isogenies } \mathcal{E}_i \to \mathcal{E}_i\}} \right) \to \mathrm{Aut}(E) \backslash^{\{\ell\text{-isogenies } E \to E\}}$$

from the collection of all equivalence classes of ℓ-isogenies $\mathcal{E}_i \to \mathcal{E}_i$, where i ranges over all indices such that $j_i \bmod \mathfrak{P} = j(E)$, to the equivalence classes of ℓ-isogenies $E \to E$.

Moreover, for any elliptic curve $\mathcal{E}$ over $\mathbb{C}$ the number of equivalence classes of degree ℓ endomorphisms is equal to the multiplicity $\mu_\ell(j(\mathcal{E}); \mathbb{C})$ of $j(\mathcal{E})$ as a root of $\Phi_\ell(X, X)$ by Theorem 34; thus Equation (15) shows that the domain of Ψ has cardinality $\mu_\ell(j(E); \overline{\mathbb{F}_p})$, and the surjectivity of Ψ yields claim (a).

Now assume that $p > 4\ell$. In view of the previous arguments we want to show that the surjection Ψ is also injective. In preparation for this we first consider the edge case $j(E) = 0$ (resp. $j(E) = 1728$), where we argue that the reduction from the curve $\mathcal{E}_i$ with $j(\mathcal{E}_i) = 0$ (resp. with $j(\mathcal{E}_i) = 1728$) is already surjective on the degree ℓ equivalence classes. Indeed, by Lemma 28 we see that the number of equivalence classes coincides, so our assumption that $\mu_\ell(j(E); \overline{\mathbb{F}_p}) > 0$ shows that there is an i with $j(\mathcal{E}_i) = 0$ (resp. $j(\mathcal{E}_i) = 1728$). Moreover, there is at least one equivalence class on E that can be lifted to an equivalence class on $\mathcal{E}_i$, namely the reduction of an equivalence class on $\mathcal{E}_i$. As the equivalence classes on both curves are represented by an ℓ-isogeny and its dual by Lemma 27, the compatibility of the reduction with dualization therefore implies that all equivalence classes on E can be obtained via reduction from $\mathcal{E}_i$.

Now suppose that we have two equivalent ℓ-isogenies $\overline{\alpha_0}, \overline{\alpha_1} \in \mathrm{End}(E)$ and corresponding lifts $\alpha_0 \in \mathrm{End}(\mathcal{E}_i)$ and $\alpha_1 \in \mathrm{End}(\mathcal{E}_m)$ for some indices $i, m \in \{1, \dots, n\}$, where we may choose i such that $j(\mathcal{E}_i) \in \{0, 1728\}$ if $j(E) \in \{0, 1728\}$ according to the previously established surjectivity; to show that Ψ is injective, we have to prove that $i = m$ and that α_0 and α_1 are equivalent.

By our assumption on i we see that reduction induces an isomorphism $\mathrm{Aut}(\mathcal{E}_i) \cong \mathrm{Aut}(E)$ by Theorem 1, so we can also lift the automorphism $\overline{\sigma} \in \mathrm{End}(E)$ with $\overline{\alpha_1} = \overline{\sigma} \circ \overline{\alpha_0}$ to an automorphism $\sigma \in \mathrm{Aut}(\mathcal{E}_i)$, and hence we may replace α_0 by the equivalent $\sigma \circ \alpha_0$ to assume that α_0 and α_1 are lifts of the same endomorphism $\overline{\alpha_1} =: \overline{\alpha}$ to $\mathcal{E}_i$ and $\mathcal{E}_m$. In particular, the reduction maps induce isomorphisms

$$\mathbb{Z}[\alpha_0] \cong \mathbb{Z}[\overline{\alpha}] \cong \mathbb{Z}[\alpha_1].$$

The discriminant of $\mathbb{Z}[\alpha_j] \cong \mathbb{Z}[\overline{\alpha}]$ is of the form $t^2 - 4\ell < 0$ for some $t \in \mathbb{Z}$ by Example 2 and Equation (1), so our assumption $p > 4\ell$ shows that $\mathrm{disc}(\mathbb{Z}[\alpha_0]) = \mathrm{disc}(\mathbb{Z}[\alpha_1])$ is not divisible by p.

In particular, the conductors of these quadratic orders are also not divisible by p due to Corollary 13, and [Onu21, Lemma 3.1] shows that the inclusion of $\mathbb{Z}[\overline{\alpha}] \subseteq \mathrm{End}(E)$ is optimal, i.e. $\mathrm{End}(E)$ does not contain a proper quadratic superorder of $\mathbb{Z}[\overline{\alpha}]$. As the reduction modulo $\mathfrak{P}$ induces quadratic embeddings $\mathrm{End}(\mathcal{E}_i), \mathrm{End}(\mathcal{E}_m) \hookrightarrow \mathrm{End}(E_0)$ that map $\mathbb{Z}[\alpha_j]$ to $\mathbb{Z}[\overline{\alpha}]$, we therefore deduce that α_0 and α_1 already generate their respective endomorphism rings, i.e.

$$\mathrm{End}(\mathcal{E}_i) = \mathbb{Z}[\alpha_0] \cong \mathbb{Z}[\overline{\alpha}] \cong \mathbb{Z}[\alpha_1] = \mathrm{End}(\mathcal{E}_m).$$

The transitivity of the classical group action of the class group $\mathfrak{Cl}(\mathbb{Z}[\overline{\alpha}])$ on isomorphism classes of elliptic curves over $\mathbb{C}$ with endomorphism rings isomorphic to $\mathbb{Z}[\overline{\alpha}]$ (cf. [Sil94, Proposition II.1.2(b)], which generalizes to non-maximal orders) hence shows that we can find an ideal class $[\mathfrak{a}]$, represented by an ideal $\mathfrak{a}$ of norm coprime to p due to [Cox13, Corollary 7.17]), such that $[\mathfrak{a}] \cdot \mathcal{E}_i \cong \mathcal{E}_m$, and we thus obtain an isogeny $\varphi\colon \mathcal{E}_i \to \mathcal{E}_m$ of degree coprime to p such that

$$\alpha_1 \circ \varphi = \varphi \circ \alpha_0. \tag{16}$$

Reduction modulo $\mathfrak{P}$ now yields an endomorphism $\overline{\varphi} \in \mathrm{End}(E)$ that is separable since its degree is coprime to p. Furthermore $\overline{\varphi}$ commutes with $\overline{\alpha}$ due to Equation (16), and in view of Proposition 12 the maximality of $\mathbb{Z}[\overline{\alpha}]$ in $\mathrm{End}(E)$ yields $\overline{\varphi} \in \mathbb{Z}[\overline{\alpha}]$.

The isogeny $\overline{\varphi}$ is separable with kernel

$$\ker(\overline{\varphi}) = \bigcap_{\beta \in \mathfrak{a}} \ker(\beta)$$

and $\mathfrak{a}$ is of norm coprime to p. Hence any $\beta \in \mathfrak{a}$ is separable with $\ker(\beta) \supseteq \ker(\overline{\varphi})$, so it factors through $\overline{\varphi}$ by [Sil09, Proposition III.4.12]; due to the maximality of $\mathbb{Z}[\overline{\alpha}]$, $\overline{\varphi}$ thus generates an ideal of $\mathbb{Z}[\overline{\alpha}]$ that contains $\mathfrak{a}$, and a comparison of ideal norms shows that $\mathfrak{a} = \overline{\varphi}\mathbb{Z}[\overline{\alpha}]$ is a principal ideal[15].

Since the classical class group action is free (see again [Sil94, Proposition II.1.2(b)]), we deduce that $[\mathfrak{a}] \cdot \mathcal{E}_i \cong \mathcal{E}_m$ is isomorphic to $\mathcal{E}_i$, and from this we obtain $j_m = j_i$, i.e. $i = m$. As the two lifts $\alpha_0, \alpha_1 \in \mathrm{End}(\mathcal{E}_i)$ lift the same endomorphism, the injectivity of the reduction now implies $\alpha_0 = \alpha_1$ (which shows that our original lifts were equivalent via the lifted automorphism σ), and this proves the injectivity of Ψ. □

We note an interesting consequence of our prior bound on loops:

Corollary 37. Let p, ℓ be primes with $p > 4\ell^2$ and let E be an elliptic curve over $\overline{\mathbb{F}_p}$ such that there is a degree ℓ endomorphism $\varphi \in \mathrm{End}(E)$. Further let L be a number field, let $\mathfrak{P}$ be a prime ideal of L and fix an embedding $\mathcal{O}_L/\mathfrak{P} \hookrightarrow \overline{\mathbb{F}_p}$. Then, up to isomorphism, at most one of the elliptic curves over L whose reduction modulo $\mathfrak{P}$ is (isomorphic to) E admits an endomorphism of degree ℓ.

Proof. By Proposition 18 we know that there are at most two equivalence classes of degree ℓ endomorphisms $E \to E$. Moreover, the proof of this bound shows that any degree ℓ endomorphism must commute with φ; due to Proposition 12 they hence must lie in a common quadratic order, and Lemma 27 shows that these equivalence classes can be represented by φ and $\widehat{\varphi}$. If we now have an elliptic curve $\mathcal{E}$ over L that reduces to E modulo $\mathfrak{P}$ and that admits a lift of a degree ℓ endomorphisms of E, then it also admits a lift of the dual of this isogeny, namely the dual of the original lift. After a sufficient enlargement of L, the bijectivitity of the reduction map Ψ constructed in the proof of Theorem 35 thus shows that no other curve over L with reduction E modulo $\mathfrak{P}$ can admit an endomorphism of degree ℓ unless it is isomorphic to $\mathcal{E}$. □

Note that the diagonal modular polynomial $\Phi_\ell(X, X)$ is of degree 2ℓ with leading coefficient -1 by [Cox13, Theorem 11.18(iv)] and the Kronecker congruence relation [Cox13, Theorem 11.18(v)]; from Theorem 35(a) we hence immediately obtain:

Corollary 38. Let $p \neq \ell$ be distinct primes. Then there are at most 2ℓ loops in the full isogeny graph. In particular, there are at most 2ℓ loops in the supersingular ℓ-isogeny graph $\mathcal{G}_\ell(p)$.

In contrast to the previous impossibility results of Section 3.4, we cannot forgo a bound on the characteristic in Theorem 35(b) if E is an ordinary curve:

Example 4. Consider $p = 13$ and $\ell = 127$. Then the j-invariant $j_0 = 0 \in \mathbb{F}_p$ belongs to an ordinary curve by Example 1 and $\Phi_{127}(X, X)$ has a root of multiplicity 10 at j_0, but the multiplicity of 0 as a root of $\Phi_{127}(0, Y)$ is 2 by Lemma 28.

However, we can decrease the size of the lower bound significantly for ordinary curves, as we will show now. We need one intermediate result:

Lemma 39. Let p be a prime and let E be an ordinary elliptic curve over $\overline{\mathbb{F}_p}$. Then the discriminant $\mathrm{disc}(\mathrm{End}(E))$ of the endomorphism ring $\mathrm{End}(E)$ is a non-zero quadratic residue modulo p.

Proof. E can be defined over $\mathbb{F}_q$ for some power q of p, and we thus have the q-power Frobenius endomorphism $\pi_q \in \mathrm{End}(E)$. As E is ordinary, π_q cannot be self-dual by [Sil09, Theorem V.3.1], so $\mathbb{Z}[\pi_q] \subseteq \mathrm{End}(E)$ is a quadratic order. Hence Corollary 13 and Example 2 yield

$$\mathrm{disc}(\mathrm{End}(E)) \cdot [\mathrm{End}(E) : \mathbb{Z}[\pi_q]]^2 = \mathrm{disc}(\mathbb{Z}[\pi_q]) = \mathrm{trd}(\pi_q)^2 - 4q \equiv \mathrm{trd}(\pi_q)^2 \not\equiv 0 \mod p$$

where we know that $\mathrm{trd}(\pi_q)^2$ is not divisible by p due to [Was08, Proposition 4.31] as E is ordinary. Therefore $\mathrm{disc}(\mathrm{End}(E))$ is a non-zero quadratic residue modulo p. □

[15] This is a proof that the action of $\mathfrak{Cl}(\mathbb{Z}[\overline{\alpha}])$ on curves over $\overline{\mathbb{F}_p}$ oriented by $\mathbb{Z}[\overline{\alpha}]$ is free; see also [Onu21, Theorem 3.4].

The following result strengthens Theorem 35(b) for ordinary curves by giving a smaller lower bound. If we are allowed to exclude the j-invariants 0 and 1728, e.g. because Lemma 28 already gives the number of equivalence classes of degree ℓ endomorphisms at them, then we can obtain an even smaller lower bound:

Proposition 40. Let $p \neq \ell$ be distinct primes, let E be an ordinary curve over $\overline{\mathbb{F}_p}$ and let $\mu_\ell(j_0; \overline{\mathbb{F}_p})$ denote the multiplicity of $j_0 \in \overline{\mathbb{F}_p}$ as a root of $\Phi_\ell(X, X)$. Further assume one of the following:

i) $p > \sqrt{\frac{4}{3}\ell}$,

ii) $p > \sqrt{\ell}$ and $j(E) \neq 0$, or

iii) $p > \sqrt{\frac{4}{7}\ell}$ and $j(E) \notin \{0, 1728\}$.

Then there are exactly $\mu_\ell(j(E); \overline{\mathbb{F}_p})$ equivalence classes of ℓ-isogenies $E \to E$.

Proof. Let us recall where we needed the assumption $p > 4\ell$ in the proof of Theorem 35(b): Firstly, we needed it to have a precise understanding of the equivalence classes at vertices of j-invariants $j = 0$ and $j = 1728$ according to Lemma 28, but for ordinary curves we do not need this restriction due to the same referenced result. Secondly, we needed it to argue that for $\overline{\alpha} \in \mathrm{End}(E)$ of degree ℓ the prime p cannot divide the discriminant $\mathrm{disc}(\mathbb{Z}[\overline{\alpha}])$.

Hence suppose for a contradiction that there is an $\alpha \in \mathrm{End}(E)$ of degree ℓ such that p divides $\mathrm{disc}(\mathbb{Z}[\alpha])$. Then $\alpha \notin \mathbb{Z}$ since ℓ is not a square in $\mathbb{Z}$, so Lemma 39 and Corollary 13 show that p has to divide $\mathrm{disc}(\mathbb{Z}[\alpha])$ with even multiplicity. This allows us to find a $d \in \mathbb{N}$ such that

$$4\ell \geq 4\ell - \mathrm{trd}(\alpha)^2 = -\mathrm{disc}(\mathbb{Z}[\alpha]) = d \cdot p^2 > d \cdot \tfrac{4}{7}\ell = \tfrac{d}{7} \cdot 4\ell$$

and we deduce $d \in \{1, 2, 3, 4, 5, 6\}$. Moreover, Corollary 13 gives

$$-[\mathrm{End}(E) : \mathbb{Z}[\alpha]]^2 \cdot \mathrm{disc}(\mathrm{End}(E)) = -\mathrm{disc}(\mathbb{Z}[\alpha]) = d \cdot p^2,$$

and p does not divide $\mathrm{disc}(\mathrm{End}(E))$ by Lemma 39. With any $\beta \in \mathrm{End}(E)$ such that $\mathrm{End}(E) = \mathbb{Z}[\beta]$ we further obtain

$$-\mathrm{disc}(\mathrm{End}(E)) = 4\deg(\beta) - \mathrm{trd}(\beta)^2 \equiv -\mathrm{trd}(\beta)^2 \equiv 0, 3 \mod 4$$

from Example 2. As only $d = 4$ is not squarefree, the above forces $d \in \{3, 4\}$ and $\mathrm{disc}(\mathrm{End}(E)) = -d$.

Now first assume that $d = 4$, which is only possible in case iii) due to the smaller lower bound. Then $\mathrm{disc}(\mathrm{End}(E)) = -4$ shows that $\mathrm{End}(E)$ is (isomorphic to) the maximal order $\mathbb{Z}[\sqrt{-1}]$ in the quadratic field $\mathbb{Q}(\sqrt{-1})$, so E has an automorphism of order 4. Thus Theorem 1 forces $j(E) = 1728$, which is impossible in case iii).

Finally, assume that $d = 3$, which is not possible in case i) due to the larger lower bound. Then $\mathrm{disc}(\mathrm{End}(E)) = -3$ shows that $\mathrm{End}(E)$ is (isomorphic to) the maximal order in the quadratic field $\mathbb{Q}(\sqrt{-3})$. Since this order is of the form $\mathbb{Z}[\omega]$ for a third root of unity, E has an automorphism of order 3 and Theorem 1 forces $j(E) = 0$, which is impossible in the last two cases.

Therefore p cannot divide the discriminant $\mathrm{disc}(\mathbb{Z}[\alpha])$, and repeating the proof of Theorem 35(b) gives the desired claim. □

To close out the analysis of this section, we give examples of j-invariants of ordinary curves to indicate that the above bounds of Proposition 40 are optimal:

Example 5.

1. In Example 4 we have seen that $j = 0 \in \mathbb{F}_{13}$ has multiplicity 10 as a root of $\Phi_{127}(X, X)$, but multiplicity 2 as a root of $\Phi_{127}(0, Y)$. Note that $\sqrt{\frac{4}{3} \cdot 127} \approx 13.01 > 13$.
2. For $\ell = 293$ and $p = 17$ the j-invariant $j = 1728 = 11 \in \mathbb{F}_p$ has multiplicity 18 as a root of $\Phi_{293}(X, X)$, but multiplicity 2 as a root of $\Phi_{293}(11, Y)$ by Lemma 28. Further $\sqrt{293} \approx 17.12 > 17$.
3. For $\ell = 7$ and $p = 2$ the j-invariant $1 \in \mathbb{F}_p$ has multiplicity 2 as a root of $\Phi_7(X, X)$, but multiplicity 1 as a root of $\Phi_7(1, Y)$. Note that $\sqrt{\frac{4}{7} \cdot 7} = \sqrt{4} = 2$.

Remark 13. In the above notation the case $d = 7$ can only occur for $p = 2$, which can be seen by considering the equation

$$4\ell = \mathrm{trd}(\alpha)^2 + 7 \cdot p^2$$

modulo 8 for odd primes ℓ and p. Therefore the bound in case iii) of Proposition 40 can be improved to $p > \sqrt{\frac{1}{2}\ell}$ if one restricts to odd characteristics; here $\ell = 19$ and $p = 3$ with $\sqrt{\frac{1}{2} \cdot 19} \approx 3.08 > 3$ and the j-invariant $j = 2 \in \mathbb{F}_p$, whose multiplicity as a root of $\Phi_{19}(X, X)$ is 6, show that $d = 8$ can occur (since the next possibility would be $d = 11$, but $\sqrt{\frac{4}{11} \cdot 19} < 3$). This indicates that we cannot optimize the bound further with the above method, and experiments support this claim: There are many pairs (p, ℓ) with $\sqrt{\frac{4}{11}\ell} < p < \sqrt{\frac{1}{2}\ell}$ for which a j-invariant $j_0 \notin \{0, 1728\}$ of an ordinary curve with less than $\mu_\ell(j_0; \overline{\mathbb{F}_p})$ loops of degree ℓ exists. In fact, to guarantee the existence of such a j-invariant it suffices to find (p, ℓ) satisfying the above bounds and such that $\ell - 2p^2$ is a square. Put differently, one needs to find pairs (p, t) where p is an odd prime and $t \in \mathbb{N}$ is an integer with $t < \frac{\sqrt{3}}{2}p$ such that $t^2 + 2p^2$ is a prime. Large scale experiments suggest that such pairs occur infinitely often; in fact, for any odd prime $p \leq 2^{22}$ there is always at least one t satisfying the above conditions. Moreover, the conjectured asymptotic formula [HL23, Conjecture F] (applied with $a = 1$, $b = 0$, $c = 2p^2$ and $n = \frac{11}{4}p^2$) indicates that for sufficiently large p we can always find a suitable t.

6 Conclusion

In this article we proved the tighter bound $p < 4\ell^3$ for the existence of triple edges at vertices of non-zero j-invariant in $\mathcal{G}_\ell(p)$. Further we analyzed vertex distances in the graph, which lead us to a general diameter bound that is provably non-tight for almost all vertex pairs. Moreover, we also showed that the distance of the special vertices of j-invariants 0 and 1728 (in the case $p \equiv 11 \bmod 12$) is always at least one fourth of the graph's diameter. Finally, we limited the existence of other special phenomena in $\mathcal{G}_\ell(p)$ and demonstrated the tightness of the related bounds with experimental data; our computations also lead us to an extensive study of the multiplicities of loops in $\mathcal{G}_\ell(p)$, and we were able to establish a precise understanding of when these multiplicities coincide with the root multiplicities of the 'diagonal' classical modular polynomial $\Phi_\ell(X, X)$ in positive characteristics.

An interesting remaining question on our bounds is the search for abstract tightness proofs of the form

If the bound is satisfied and [additional condition], *then the analyzed phenomenon is guaranteed to occur*

that might also yield general lower bounds on the respective maximal primes at which these phenomena occur. Take Proposition 29 for example: Due to the first part of this result we see that the additional condition would have to include $p \equiv 11 \bmod 12$, but Remark 7 shows that this condition alone is not sufficient. In fact, even conditions on the values of the Jacobi symbols between $\pm p$ and $\pm \ell^n$ do not yield sufficient conditions for the occurrence of a cyclic ℓ^n-isogeny $0 \to 1728$.

Another open problem is to improve the diameter bound of Corollary 31, which is generally not tight: Small-scale experiments suggest that the factor 2 in front of the logarithm can be replaced by $\frac{3}{2}$, or possibly even by $\frac{4}{3}$. Note that any such improvement would also improve the lower bound given in Corollary 32, so Remark 10 implies that the cofactor $\frac{4}{3}$ would be close to optimal.

Acknowledgments. The authors would like to thank Jonathan Komada Eriksen and Maria Corte-Real Santos for interesting discussions around Sections 3 and 4 as well as for organizing the 2025 Isogeny Club Brainstorm Sessions in Madrid, which sparked this collaboration. Further we want to thank Marc Houben for helpful pointers for Theorem 35, and Lorenz Panny and Sina Schaeffler for helpful input regarding Remark 13.

References

[AAM19] G. Adj, O. Ahmadi, and A. Menezes. "On isogeny graphs of supersingular elliptic curves over finite fields". In: *Finite Fields and Their Applications* 55 (2019), pp. 268–283. ISSN: 1071-5797.

[Arp+23] S. Arpin et al. "Adventures in Supersingularland". In: *Experimental Mathematics* 32(2) (2023), pp. 241–268.

[Arp+24] S. Arpin et al. "Orientations and Cycles in Supersingular Isogeny Graphs". In: *Research Directions in Number Theory: Women in Numbers V*. Ed. by A. Bucur, W. Ho, and R. Scheidler. Springer, Cham, 2024, pp. 25–86. ISBN: 978-3-031-51677-1.

[Ban+19] E. Bank, C. Camacho-Navarro, K. Eisenträger, T. Morrison, and J. Park. "Cycles in the Supersingular ℓ-Isogeny Graph and Corresponding Endomorphisms". In: *Research Directions in Number Theory. Women in Numbers IV*. Ed. by J. S. Balakrishnan, A. Folsom, M. Lalín, and M. Manes. Vol. 19. Association for Women in Mathematics Series. Springer, Cham, 2019, pp. 41–66.

[Bas+25a] A. Basso et al. "PRISM: Simple and Compact Identification and Signatures from Large Prime Degree Isogenies". In: *Public-Key Cryptography – PKC 2025*. Ed. by T. Jager and J. Pan. Springer, Cham, 2025, pp. 300–332. ISBN: 978-3-031-91826-1.

[Bas+25b] A. Basso et al. "SQIsign2D–West: The Fast, the Small, and the Safer". In: *Advances in Cryptology – ASIACRYPT 2024*. Ed. by K.-M. Chung and Y. Sasaki. Springer, Singapore, 2025, pp. 339–370. ISBN: 978-981-96-0891-1.

[Bas+23] A. Basso et al. "Supersingular Curves You Can Trust". In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by C. Hazay and M. Stam. Springer, Cham, 2023, pp. 405–437. ISBN: 978-3-031-30617-4.

[Bos18] S. Bosch. *Algebra. From the Viewpoint of Galois Theory*. Birkhäuser Advanced Texts Basler Lehrbücher. Birkhäuser Cham, 2018. ISBN: 978-3-319-95177-5.

[BLS10] R. Bröker, K. E. Lauter, and A. V. Sutherland. "Modular polynomials via isogeny volcanoes". In: *Mathematics of Computation* 81 (2010), pp. 1201–1231.

[BOS16] J. H. Bruinier, K. Ono, and A. V. Sutherland. "Class polynomials for nonholomorphic modular functions". In: *Journal of Number Theory* 161 (2016). Special Issue on Applications of Automorphic Forms in Number Theory and Combinatorics, pp. 204–229. ISSN: 0022-314X.

[CLG09] D. X. Charles, K. E. Lauter, and E. Z. Goren. "Cryptographic Hash Functions from Expander Graphs". In: *Journal of Cryptology* 22(1) (2009), pp. 93–113.

[CL24] G. Codogni and G. Lido. *Spectral Theory of Isogeny Graphs*. July 2024. arXiv: 2308.13913 [math.NT].

[Cos+19] A. Costache, B. Feigon, K. Lauter, M. Massierer, and A. Puskás. "Ramanujan Graphs in Cryptography". In: *Research Directions in Number Theory. Women in Numbers IV*. Ed. by J. S. Balakrishnan, A. Folsom, M. Lalín, and M. Manes. Vol. 19. Association for Women in Mathematics Series. Springer, Cham, 2019, pp. 1–40.

[Cox13] D. A. Cox. *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication*. 2nd edition. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. John Wiley & Sons, 2013.

[DF+20] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski. "SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies". In: *Advances in Cryptology – ASIACRYPT 2020*. Ed. by S. Moriai and H. Wang. Springer, Cham, 2020, pp. 64–93. ISBN: 978-3-030-64837-4.

[DG16] C. Delfs and S. D. Galbraith. "Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$". In: *Designs, Codes and Cryptography. An International Journal* 78(2) (Feb. 2016), pp. 425–440.

[dH+24] T. den Hollander, S. Kleine, M. Mula, D. Slamanig, and S. A. Spindler. *More Efficient Isogeny Proofs of Knowledge via Canonical Modular Polynomials*. Cryptology ePrint Archive, Paper 2024/1738. 2024. To appear at CRYPTO 2025.

[Eic55] M. Eichler. "Zur Zahlentheorie der Quaternion-Algebren". In: *Journal für die reine und angewandte Mathematik* 195 (1955), pp. 127–151.

[FM02] M. Fouquet and F. Morain. "Isogeny Volcanoes and the SEA Algorithm". In: *Algorithmic Number Theory. 5th International Symposium, ANTS-V, Sydney, Australia, July 7-12, 2002. Proceedings*. Ed. by C. Fieker and D. R. Kohel. Lecture Notes in Computer Science 2369. Springer Berlin Heidelberg, Aug. 2002, pp. 276–291.

[Fus+25] J. Fuselier, A. Iezzi, M. Kozek, T. Morrison, and C. Namoijam. "Computing supersingular endomorphism rings using inseparable endomorphisms". In: *Journal of Algebra* 668 (2025), pp. 145–189. ISSN: 0021-8693.

[Gha24] W. Ghantous. "Loops, multi-edges and collisions in supersingular isogeny graphs". In: *Advances in Mathematics of Communications* 18(4) (2024), pp. 935–955.

[GS06] P. Gille and T. Szamuely. *Central Simple Algebras and Galois Cohomology*. 1st edition. Cambridge Studies in Advanced Mathematics 101. Cambridge University Press, Cambridge, 2006. ISBN: 978-0-521-86103-8.

[Gro87] B. H. Gross. "Heights and the Special Values of L-series". In: *Number Theory: Proceedings of the 1985 Montreal Conference held June 17-29, 1985. Canadian Mathematical Society Conference Proceedings*. Ed. by J. Labute and H. Kisilevsky. Vol. 7. American Mathematical Society, 1987, pp. 115–187.

[HL23] G. H. Hardy and J. E. Littlewood. "Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes". In: *Acta Mathematica* 44 (1923), pp. 1–70.

[Hur85] A. Hurwitz. "Ueber Relationen zwischen Classenanzahlen binärer quadratischer Formen von negativer Determinante". In: *Mathematische Annalen* 25(2) (June 1885), pp. 157–196.

[Hus04] D. Husemöller. *Elliptic Curves*. 2nd edition. Graduate Texts in Mathematics 111. Springer New York, NY, 2004. ISBN: 978-0-387-95490-5.

[Kan89] M. Kaneko. "Supersingular j-invariants as singular moduli mod p". In: *Osaka Journal of Mathematics* 26(4) (Dec. 1989), pp. 849–855.

[Koh96] D. Kohel. "Endomorphism rings of elliptic curves over finite fields". https://www.i2m.univ-amu.fr/perso/david.kohel/pub/thesis.pdf. PhD thesis. University of California, Berkeley, 1996.

[Lan87] S. Lang. *Elliptic Functions*. Graduate Texts in Mathematics 112. Springer New York, NY, 1987. ISBN: 9780387965086.

[LOX20] S. Li, Y. Ouyang, and Z. Xu. "Neighborhood of the supersingular elliptic curve isogeny graph at $j = 0$ and 1728". In: *Finite Fields and Their Applications* 61 (2020), p. 101600. ISSN: 1071-5797.

[LB20] J. Love and D. Boneh. "Supersingular curves with small noninteger endomorphisms". In: *ANTS XIV: Proceedings of the Fourteenth Algorithmic Number Theory Symposium*. Vol. 4. Open Book Series. Mathematical Sciences Publishers, 2020, pp. 7–22.

[MH02] J. C. Mason and D. C. Handscomb. *Chebyshev Polynomials*. Chapman and Hall/CRC, Boca Raton, FL, 2002. ISBN: 978-0-429-19138-1.

[Neu99] J. Neukirch. *Algebraic Number Theory*. Trans. by N. Schappacher. Grundlehren der mathematischen Wissenschaften 322. Springer Berlin Heidelberg, 1999.

[Onu21] H. Onuki. "On oriented supersingular elliptic curves". In: *Finite Fields and Their Applications* 69 (2021), p. 101777. ISSN: 1071-5797.

[OX19] Y. Ouyang and Z. Xu. "Loops of isogeny graphs of supersingular elliptic curves at j = 0". In: *Finite Fields and Their Applications* 58 (2019), pp. 174–176. ISSN: 1071-5797.

[PW24] A. Page and B. Wesolowski. "The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent". In: *Advances in Cryptology – EUROCRYPT 2024*. Ed. by M. Joye and G. Leander. Springer, Cham, 2024, pp. 388–417. ISBN: 978-3-031-58751-1.

[Piz90] A. K. Pizer. "Ramanujan graphs and Hecke operators". English. In: *Bull. Am. Math. Soc., New Ser.* 23(1) (1990), pp. 127–137. ISSN: 0273-0979.

[RM20] M. Ram Murty. "Ramanujan Graphs: An Introduction". In: *Indian Journal of Discrete Mathematics* 6(2) (2020), pp. 91–127.

[Sage] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.6)*. https://www.sagemath.org. 2025.

[Sar18] N. T. Sardari. "Diameter of Ramanujan Graphs and Random Cayley Graphs". In: *Combinatorica* 39 (2018), pp. 427–446.

[Sil94] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 151. Springer New York, 1994.

[Sil09] J. H. Silverman. *The Arithmetic of Elliptic Curves*. English. 2nd edition. Graduate Texts in Mathematics 106. Springer New York, NY, 2009. ISBN: 978-0-387-09493-9.

[Sut13] A. V. Sutherland. "Isogeny volcanoes". In: *ANTS X. Proceedings of the Tenth Algorithmic Number Theory Symposium*. Ed. by E. W. Howe and K. S. Kedlaya. Vol. 1. The Open Book Series. Mathematical Sciences Publishers, Nov. 2013, pp. 507–530.

[VDH95] E. R. Van Dam and W. H. Haemers. "Eigenvalues and the Diameter of Graphs". In: *Linear and Multilinear Algebra* 39 (1995), pp. 33–44.

[Voi21] J. Voight. *Quaternion Algebras*. Graduate Texts in Mathematics 288. Springer, Cham, 2021. ISBN: 978-3-030-56692-0.

[Was08] L. C. Washington. *Elliptic Curves. Number Theory and Cryptography*. English. 2nd edition. Chapman and Hall/CRC, Boca Raton, FL, 2008. ISBN: 978-1-4200-7146-7.

[Wes22] B. Wesolowski. "The supersingular isogeny path and endomorphism ring problems are equivalent". In: *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*. 2022, pp. 1100–1111.

A A basis- and extension-free introduction to quaternion algebras

For any field K of characteristic $\mathrm{char}(K) \neq 2$ and $n \in \mathbb{N}$ we write $\mathrm{Mat}_n(K)$ for the K-algebra of $n \times n$-matrices. A four-dimensional K-algebra $\mathcal{B}$ is called a *quaternion algebra* if it is *central*, i.e. $K \subseteq \mathcal{B}$ is the center of $\mathcal{B}$, and further satisfies one of the following two properties[16]:

i) $\mathcal{B}$ is a *division* algebra, i.e. every non-zero element has a multiplicative left inverse[17], or

ii) $\mathcal{B}$ is *split*, i.e. it is isomorphic to $\mathrm{Mat}_2(K)$ as a K-algebra.

We first note the following important facts:

Lemma 41. Let $\mathcal{B}$ be a finite-dimensional K-algebra. Then the following holds:

(a) Any $\alpha \in \mathcal{B}$ satisfies a non-trivial polynomial equation over K.

(b) If $\mathcal{B}$ is a division algebra, then $K[\alpha] \subseteq \mathcal{B}$ is a field.

(c) If $\mathcal{B}$ is a quaternion algebra, then any $\alpha \in \mathcal{B}$ satisfies a quadratic polynomial equation over K.

Proof. For claim (a) we see that the set $\{\alpha^n \mid n \in \mathbb{N}_0\} \subseteq \mathcal{B}$ is K-linearly dependent since $\mathcal{B}$ is finite-dimensional, and from this we immediately obtain a non-trivial polynomial equation for α over K. Next suppose that $\mathcal{B}$ is a division algebra and let $\beta \in K[\alpha] \setminus \{0\}$. Choosing a non-trivial equation of minimal degree for β according to part (a), we get a polynomial $P \in K[X]$ with $P(0) \neq 0$ such that $P(\beta) = 0$. Multiplying through with the inverse of β (in $\mathcal{B}$) yields

$$\beta^{-1} = -P(0)^{-1} \cdot (P(\beta) - P(0)) \cdot \beta^{-1} = -P(0)^{-1} \cdot \left(\frac{P - P(0)}{X}\right)(\beta) \in K[\beta] \subseteq K[\alpha].$$

Thus $K[\alpha]$ is a commutative K-subalgebra closed under inversion of non-zero elements, so it is a field. Finally, if $\mathcal{B}$ is split, then the Cayley–Hamilton theorem immediately implies that any $\alpha \in \mathcal{B}$ satisfies a quadratic polynomial equation. Thus we may assume that $\mathcal{B}$ is division, so that $K[\alpha]$ is a field by part (b). Since $\mathcal{B}$ is central, we now deduce that $\mathcal{B}$ is at least two-dimensional as a vector space over $K[\alpha]$. However, since $\mathcal{B}$ is four-dimensional over K, this shows that $K[\alpha]$ has dimension at most two over K, and the claim follows. □

While we will work without bases in the following, we note the following simple criterion for finding a basis of a division quaternion K-algebra:

Corollary 42. Let $\mathcal{B}$ be a division quaternion K-algebra and let $\alpha, \beta \in \mathcal{B}$. Then the four quaternions $1, \alpha, \beta, \alpha\beta$ are K-linearly independent if and only if α and β do not commute.

Proof. If α and β do not commute, then we have $\alpha \notin K$ and $\beta \notin K[\alpha]$. Now $K[\alpha] \subseteq \mathcal{B}$ is a field due to Lemma 41(b), and we see that 1 and β are $K[\alpha]$-linearly independent. Put differently, the quaternions $1, \alpha, \beta$ and $\alpha\beta$ are K-linearly independent. Conversely, this implies that $1, \alpha, \beta$ and $\alpha\beta$ generate the non-commutative K-algebra $\mathcal{B}$ over K, so at least one pair of generators cannot commute, and this is easily seen to be equivalent to α and β not commuting. □

Example 6. The assumption that $\mathcal{B}$ is division is necessary for Corollary 42, as can be seen by taking any two non-commuting upper triangular matrices $\alpha, \beta \in \mathrm{Mat}_2(K)$, e.g.

$$\alpha = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

The following notion gives a nice way to define the (reduced) trace and norm of $\mathcal{B}$ both without choosing a basis and without extending to a splitting field, as hinted at in [GS06, Remark 1.1.4].

Definition 4. A quaternion $\alpha \in \mathcal{B}$ is called *pure* if $\alpha^2 \in K$ and $\alpha \notin K^\times$. We denote the set of pure quaternions in $\mathcal{B}$ by $\mathcal{B}_0$.

[16] Implicitly Wedderburn's theorem [GS06, Theorem 2.1.3] is used here to classify four-dimensional central *simple* algebras.

[17] Since $\mathcal{B}$ is finite-dimensional, the existence of a multiplicative right inverse, which then has to coincide with the left inverse, follows immediately.

Example 7. For $\mathcal{B} = \mathrm{Mat}_2(K)$ the pure quaternions $\mathcal{B}_0$ are precisely the matrices of trace 0. In particular, they form a K-linear subspace of $\mathcal{B}$. Moreover, from the expression

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \frac{a+d}{2} & 0 \\ 0 & \frac{a+d}{2} \end{pmatrix} + \begin{pmatrix} \frac{a-d}{2} & b \\ c & \frac{d-a}{2} \end{pmatrix}$$

we directly read off the decomposition $\mathcal{B} = K \oplus \mathcal{B}_0$.

In fact, the observations from Example 7 all hold for general quaternion K-algebras:

Proposition 43. Let $\mathcal{B}$ be a quaternion K-algebra. Then the subset $\mathcal{B}_0 \subseteq \mathcal{B}$ of pure quaternions is a three-dimensional K-subspace that satisfies $\mathcal{B} = K \oplus \mathcal{B}_0$.

Proof. If $\mathcal{B}$ is split, then we can use any K-algebra isomorphism between $\mathcal{B}$ and $\mathrm{Mat}_2(K)$ to derive the claim from Example 7 since such an isomorphism preserves the set of pure quaternions; therefore we will assume that $\mathcal{B}$ is division for the remainder of this proof.

Clearly we have $K \cap \mathcal{B}_0 = \{0\}$. Next we let $\alpha \in \mathcal{B}$ and use Lemma 41 to find a polynomial $X^2 + cX + d \in K[X]$ of which α is a root. We may assume $\alpha \notin K$, so that this quadratic polynomial is irreducible (since $\mathcal{B}$ is division), which implies that its discriminant $c^2 - 4d \in K$ is not a square. With this setup we define $\alpha_0 := \alpha + \frac{c}{2}$ and obtain

$$\alpha_0^2 = \alpha^2 + c\alpha + \tfrac{c}{4}^2 = -d + \tfrac{c^2}{4} = \tfrac{1}{4}(c^2 - 4d) \in K$$

As $c^2 - 4d$ is not a square, we deduce that α_0 cannot be an element of K, and thus $\alpha_0 \in \mathcal{B}_0$ gives

$$\alpha = -\tfrac{c}{2} + \alpha_0 \in K + \mathcal{B}_0.$$

Finally, we only have to prove that $\mathcal{B}_0$ is a K-subspace of $\mathcal{B}$. To this end let $\lambda \in K$ and $\alpha, \beta \in \mathcal{B}_0$. Then we clearly have $(\lambda\alpha)^2 = \lambda^2\alpha^2 \in K$ and $\lambda\alpha \notin K^\times$, so $\lambda\alpha \in \mathcal{B}_0$. To show that we also have $\alpha + \beta \in \mathcal{B}_0$, we may assume $\alpha \neq 0$ and distinguish two cases:

$\beta \in K[\alpha]$: Writing $\beta = c + d\alpha$ with $c, d \in K$, we get

$$K \ni \beta^2 = (c + d\alpha)^2 = c^2 + 2cd\alpha + d^2\alpha^2 \in 2cd\alpha + K$$

and hence $2cd\alpha \in K$. Due to $\alpha \notin K$ this forces $cd = 0$, and if $d = 0$ we also necessarily have $c = 0$ since $\beta \notin K^\times$. Thus $c = 0$ either way, so $\beta = d\alpha$ and $\alpha + \beta = (d+1)\alpha \in \mathcal{B}_0$.

$\beta \notin K[\alpha]$: Immediately we see that our assumption implies $\alpha + \beta \notin K$. Furthermore the same argument as in Corollary 42 shows that the quaternions 1, α, β, and $\alpha\beta$ are K-linearly independent, i.e.

$$\mathcal{B} = K \oplus K\alpha \oplus K\beta \oplus K\alpha\beta.$$

Now the element $\gamma := \alpha\beta + \beta\alpha$ commutes with α and β since $\alpha^2, \beta^2 \in K$, so the above decomposition shows that γ lies in the center K of $\mathcal{B}$. Therefore

$$(\alpha + \beta)^2 = \alpha^2 + \alpha\beta + \beta\alpha + \beta^2 = \alpha^2 + \gamma + \beta^2 \in K,$$

and we obtain $\alpha + \beta \in \mathcal{B}_0$ as required.

□

The above decomposition $\mathcal{B} = K \oplus \mathcal{B}_0$ gives rise to a K-linear involution map

$$\widehat{-} : \mathcal{B} \to \mathcal{B},\ \alpha = \lambda + \alpha_0 \mapsto \lambda - \alpha_0 =: \widehat{\alpha}$$

called the *standard involution* of $\mathcal{B}$. It satisfies the following properties for any $\alpha, \beta \in \mathcal{B}$:

(a) $\widehat{\alpha}\alpha = \alpha\widehat{\alpha} \in K$.

(b) $\widehat{\alpha\beta} = \widehat{\beta} \cdot \widehat{\alpha}$.

Proof. Only property (b) is not immediate, and via basic algebra we see that it suffices to prove the claim for pure quaternions $\alpha, \beta \in \mathcal{B}_0$. Here we have $\widehat{\beta}\widehat{\alpha} = (-\beta)(-\alpha) = \beta\alpha$ and further

$$K \ni (\alpha+\beta)^2 = \alpha^2 + \beta^2 + \alpha\beta + \beta\alpha \in \alpha\beta + \beta\alpha + K,$$

i.e. $\alpha\beta + \beta\alpha \in K$. Moreover, we compute

$$K \ni (\alpha\beta+\beta\alpha)^2 - 4\alpha^2\beta^2 = (\alpha\beta)^2 + \alpha\beta\beta\alpha - 2\alpha\beta\beta\alpha + \beta\alpha\alpha\beta - 2\beta\alpha\alpha\beta + (\beta\alpha)^2 = (\alpha\beta-\beta\alpha)^2 \tag{17}$$

where we used multiple times that $\alpha^2, \beta^2 \in K$ are central. This gives us the sum decomposition

$$2\alpha\beta = (\alpha\beta+\beta\alpha) + (\alpha\beta-\beta\alpha). \tag{18}$$

If in this decomposition we would have $(\alpha\beta-\beta\alpha) \in K^\times$, then we would immediately use $\alpha^2 \in K$ to derive a contradiction from

$$2(\alpha\beta-\beta\alpha)\alpha = (\alpha\beta-\beta\alpha)\alpha + \alpha(\alpha\beta-\beta\alpha) = -\beta\alpha^2 + \alpha^2\beta = 0.$$

Therefore we have $(\alpha\beta-\beta\alpha) \notin K^\times$, i.e. this is a pure quaternion due to Equation (17). Equation (18) hence gives the decomposition of $2\alpha\beta$ according to $\mathcal{B} = K \oplus \mathcal{B}_0$. We thus deduce

$$2\widehat{\alpha\beta} = \widehat{2\alpha\beta} = (\alpha\beta+\beta\alpha) - (\alpha\beta-\beta\alpha) = 2\beta\alpha = 2\widehat{\beta}\widehat{\alpha},$$

from the definition of the involution, and division by 2 finally yields the claim. □

The standard involution now yields the multiplicative *reduced norm* map nrd and the K-linear *reduced trace* map trd given by

$$\mathrm{nrd}\colon \mathcal{B} \to K,\ \alpha \mapsto \widehat{\alpha}\alpha \quad \text{and} \quad \mathrm{trd}\colon \mathcal{B} \to K,\ \alpha \mapsto \alpha + \widehat{\alpha}.$$

Using the multiplicativity of the reduced norm map, the following properties are all immediate:

Lemma 44. Let $\mathcal{B}$ be a quaternion K-algebra and let $\alpha \in \mathcal{B}$. Then the following holds:

(a) $\mathrm{trd}(\alpha) = \mathrm{trd}(\widehat{\alpha})$ and $\mathrm{nrd}(\alpha) = \mathrm{nrd}(\widehat{\alpha})$.

(b) α is a root of its *reduced characteristic polynomial* $X^2 - \mathrm{trd}(\alpha)X + \mathrm{nrd}(\alpha) \in K[X]$.

(c) $\mathcal{B}_0$ is the kernel of the reduced trace map trd.

(d) α is invertible if and only if $\mathrm{nrd}(\alpha) \neq 0$.

Finally, we give some basic, but nonetheless important formulas for the reduced trace:

Lemma 45. Let $\mathcal{B}$ be a quaternion K-algebra and let $\alpha, \beta \in \mathcal{B}$. Then the following holds:

(a) $\mathrm{trd}(\alpha^2) = \mathrm{trd}(\alpha)^2 - 2\cdot\mathrm{nrd}(\alpha)$.

(b) $\mathrm{trd}(\alpha\beta) = \mathrm{trd}(\beta\alpha)$.

(c) $\mathrm{trd}(\widehat{\alpha}\beta\alpha) = \mathrm{nrd}(\alpha)\,\mathrm{trd}(\beta)$.

(d) $\mathrm{trd}(\alpha\beta\alpha) = \mathrm{trd}(\alpha)\,\mathrm{trd}(\alpha\beta) - \mathrm{nrd}(\alpha)\,\mathrm{trd}(\beta)$.

Proof. Claim (a) is a direct consequence of the linearity of the reduced trace and the fact that α is a root of its reduced characteristic polynomial by Lemma 44(b). Next, via direct calculation and the linearity of the reduced trace one reduces claim (b) to the case where $\alpha, \beta \in \mathcal{B}_0$, and here it immediately follows from $\widehat{\beta}\widehat{\alpha} = \beta\alpha$. For claim (c) we in turn use claim (b) and the linearity of the trace to get

$$\mathrm{trd}(\widehat{\alpha}\beta\alpha) = \mathrm{trd}(\alpha\widehat{\alpha}\beta) = \mathrm{trd}(\mathrm{nrd}(\alpha)\beta) = \mathrm{nrd}(\alpha)\,\mathrm{trd}(\beta).$$

Lastly, for claim (d) we use claims (b), (c) and the linearity of trd to obtain

$$\mathrm{trd}(\alpha\beta\alpha) = \mathrm{trd}\left(\alpha\beta\alpha + \widehat{\alpha}\beta\alpha - \widehat{\alpha}\beta\alpha\right) = \mathrm{trd}\left(\mathrm{trd}(\alpha)\beta\alpha\right) - \mathrm{trd}(\widehat{\alpha}\beta\alpha) = \mathrm{trd}(\alpha)\,\mathrm{trd}(\alpha\beta) - \mathrm{nrd}(\alpha)\,\mathrm{trd}(\beta).$$

□

The computations for Proposition 12. To close out this section, we provide the computations for the proof of Proposition 12. Recall that we define

$$\gamma := \left(\alpha - \tfrac{\mathrm{trd}(\alpha)}{2}\right)\left(\beta - \tfrac{\mathrm{trd}(\beta)}{2}\right) \in \mathcal{B},$$

and for readability we set

$$s := \mathrm{trd}(\alpha\beta),\ t_\alpha := \mathrm{trd}(\alpha),\ t_\beta := \mathrm{trd}(\beta),\ n_\alpha := \mathrm{nrd}(\alpha),\ n_\beta := \mathrm{nrd}(\beta).$$

Now we first compute

$$\begin{aligned}\mathrm{trd}(\gamma) &= \mathrm{trd}(\alpha\beta) - \tfrac{\mathrm{trd}(\alpha)}{2}\mathrm{trd}(\beta) - \tfrac{\mathrm{trd}(\beta)}{2}\mathrm{trd}(\alpha) + \tfrac{\mathrm{trd}(\alpha)}{2}\tfrac{\mathrm{trd}(\beta)}{2}\mathrm{trd}(1)\\ &= s - \tfrac{1}{2}t_\alpha t_\beta - \tfrac{1}{2}t_\beta t_\alpha + \tfrac{t_a t_\beta}{4}\cdot 2\\ &= s - \tfrac{1}{2}t_\alpha t_\beta\end{aligned}$$

and

$$\begin{aligned}\mathrm{nrd}(\gamma) &= \mathrm{nrd}\left(\alpha - \tfrac{\mathrm{trd}(\alpha)}{2}\right)\cdot \mathrm{nrd}\left(\beta - \tfrac{\mathrm{trd}(\beta)}{2}\right)\\ &= \left(\alpha - \tfrac{\mathrm{trd}(\alpha)}{2}\right)\left(\widehat{\alpha} - \tfrac{\mathrm{trd}(\alpha)}{2}\right)\cdot\left(\beta - \tfrac{\mathrm{trd}(\beta)}{2}\right)\left(\widehat{\beta} - \tfrac{\mathrm{trd}(\beta)}{2}\right)\\ &= \left(\mathrm{nrd}(\alpha) - \tfrac{\mathrm{trd}(\alpha)}{2}(\alpha+\widehat{\alpha}) + \tfrac{\mathrm{trd}(\alpha)^2}{4}\right)\left(\mathrm{nrd}(\beta) - \tfrac{\mathrm{trd}(\beta)}{2}(\beta+\widehat{\beta}) + \tfrac{\mathrm{trd}(\beta)^2}{4}\right)\\ &= \left(n_\alpha - \tfrac{t_\alpha^2}{2} + \tfrac{t_\alpha^2}{4}\right)\cdot\left(n_\beta - \tfrac{t_\beta^2}{2} + \tfrac{t_\alpha^2}{4}\right)\\ &= \left(n_\alpha - \tfrac{t_\alpha^2}{4}\right)\left(n_\beta - \tfrac{t_\beta^2}{4}\right),\end{aligned}$$

so that

$$4\cdot\left(\mathrm{trd}(\gamma)^2 - 4\,\mathrm{nrd}(\gamma)\right) = (2s - t_\alpha t_\beta)^2 - \underbrace{(4n_\alpha - t_\alpha^2)}_{=-D_\alpha}\cdot\underbrace{(4n_\beta - t_\beta^2)}_{=-D_\beta}$$

as desired. Next we use the computational properties of the reduced trace (Lemma 45) to see that

$$\begin{pmatrix}\mathrm{trd}(1) & \mathrm{trd}(\alpha) & \mathrm{trd}(\beta) & \mathrm{trd}(\alpha\beta)\\ \mathrm{trd}(\alpha) & \mathrm{trd}(\alpha^2) & \mathrm{trd}(\alpha\beta) & \mathrm{trd}(\alpha^2\beta)\\ \mathrm{trd}(\beta) & \mathrm{trd}(\beta\alpha) & \mathrm{trd}(\beta^2) & \mathrm{trd}(\beta\alpha\beta)\\ \mathrm{trd}(\alpha\beta) & \mathrm{trd}(\alpha\beta\alpha) & \mathrm{trd}(\alpha\beta^2) & \mathrm{trd}((\alpha\beta)^2)\end{pmatrix} = \begin{pmatrix}2 & t_\alpha & t_\beta & s\\ t_\alpha & t_\alpha^2 - 2n_\alpha & s & t_\alpha\cdot s - n_\alpha\cdot t_\beta\\ t_\beta & s & t_\beta^2 - 2n_\beta & t_\beta\cdot s - n_\beta\cdot t_\alpha\\ s & t_\alpha\cdot s - n_\alpha\cdot t_\beta & t_\beta\cdot s - n_\beta\cdot t_\alpha & s^2 - 2n_\alpha n_\beta\end{pmatrix},$$

and a direct computation shows that the determinant of this matrix M is given by

$$\begin{aligned}\det(M) &= -\left(st_\alpha t_\beta - t_\beta^2 n_\alpha - t_\alpha^2 n_\beta - s^2 + 4n_\alpha n_\beta\right)^2\\ &= -\left(s^2 - st_\alpha t_\beta + t_\beta^2 n_\alpha + t_\alpha^2 n_\beta - 4n_\alpha n_\beta\right)^2\\ &= -\left(s^2 - st_\alpha t_\beta + (\tfrac{1}{4}t_\alpha^2 t_\beta^2 - \tfrac{1}{4}t_\alpha^2 t_\beta^2) + t_\beta^2 n_\alpha + t_\alpha^2 n_\beta - 4n_\alpha n_\beta\right)^2\\ &= -\left((s - \tfrac{1}{2}t_\alpha t_\beta)^2 - (\tfrac{1}{4}t_\alpha^2 t_\beta^2 - t_\alpha^2 n_\beta - t_\beta^2 n_\alpha + 4n_\alpha n_\beta)\right)^2\\ &= -\left(\frac{(2s - t_\alpha t_\beta)^2 - (4n_\alpha - t_\alpha^2)(4n_\beta - t_\beta^2)}{4}\right)^2\\ &= -\left(\mathrm{trd}(\gamma)^2 - 4\,\mathrm{nrd}(\gamma)\right)^2.\end{aligned}$$

□

B Reproving prior results with Kaneko's bound

In this section we use Kaneko's bound to obtain the bounds proven in [AAM19, Theorem 10 & 12], [OX19] and [LOX20, Theorem 2 & Section 5]. First we prove the loop bounds from [AAM19], while simultaneously getting the improved bound from [OX19] for free. In fact, in [AAM19, Theorem 10] the authors already use an argument very close to what we need to do, only with their weaker Kaneko-type bound [AAM19, Lemma 9] – for this reason we present here only the modified steps. We recall the statement as given in Section 2.2:

Theorem 5. *Let $p \neq \ell$ be distinct primes, and let E_{1728} resp. E_0 denote curves over $\overline{\mathbb{F}_p}$ with j-invariant $j(E_j) = j \in \{0, 1728\}$. Then the following holds:*

(a) *If E_{1728} is supersingular with at least* $\begin{cases} 1, & \ell \equiv 3 \bmod 4 \\ 3, & \ell \equiv 1 \bmod 4 \\ 2, & \ell = 2 \end{cases}$ *loops at E_{1728} in $\mathcal{G}_\ell(p)$, then $p < 4\ell$.*

(b) *If E_0 is supersingular with at least* $\begin{cases} 1, & \ell \equiv 2 \bmod 3 \\ 3, & \ell \equiv 1 \bmod 3 \\ 2, & \ell = 3 \end{cases}$ *loops at E_0 in $\mathcal{G}_\ell(p)$, then $p < 3\ell$.*

Proof. As in the proof of [AAM19, Section 5.2] we handle the case $\ell = 2$ for $j = 1728$ and $\ell = 2, 3$ for $j = 0$ manually via inspection of the classical modular polynomials Φ_2 and Φ_3. Then, for the first claim we find, as in the proof of [AAM19, Theorem 10], a supersingular curve E_{1728} with j-invariant $j(E_{1728}) = 1728$, an automorphism $\iota \in \mathrm{Aut}(E_{1728})$ of order 4 and a degree ℓ endomorphism $\alpha \in \mathrm{End}(E_{1728})$ that does not lie in the quadratic subfield $\mathbb{Q}(\iota) \subseteq \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E_{1728}) =: \mathcal{B}$ of the quaternion $\mathbb{Q}$-algebra $\mathcal{B}$. Therefore $\{1, \alpha\}$ generate $\mathcal{B}$ as a $\mathbb{Q}(\iota)$-vector space, and with Proposition 12 we deduce that α and ι cannot commute. From the reduced characteristic equation $\iota^2 + 1 = 0$ we further obtain

$$\mathrm{disc}(\mathbb{Z}[\iota]) = \mathrm{trd}(\iota)^2 - 4\deg(\iota) = 0^2 - 4 \cdot 1 = -4, \tag{19}$$

and, in view of Equation (1), Kaneko's bound hence yields

$$4p \leq (-\mathrm{disc}(\mathbb{Z}[\iota]))(-\mathrm{disc}(\mathbb{Z}[\alpha])) = 4 \cdot (4\deg(\alpha) - \mathrm{trd}(\alpha)^2) \leq 16\ell.$$

By the same methods we find for the second claim a supersingular curve E_0 with j-invariant $j(E_0) = 0$, an automorphism $\omega \in \mathrm{Aut}(E_0)$ of order 3 and an endomorphism $\alpha \in \mathrm{End}(E_0)$ of degree ℓ that does not lie in $\mathbb{Q}(\omega)$. However, now the reduced characteristic equation $\omega^2 + \omega + 1 = 0$ gives

$$\mathrm{disc}(\mathbb{Z}[\omega]) = \mathrm{trd}(\omega)^2 - 4\deg(\omega) = (-1)^2 - 4 \cdot 1 = -3, \tag{20}$$

and with Kaneko's bound we arrive at

$$4p \leq (-\mathrm{disc}(\mathbb{Z}[\omega]))(-\mathrm{disc}(\mathbb{Z}[\alpha])) = 3 \cdot (4\deg(\alpha) - \mathrm{trd}(\alpha)^2) \leq 12\ell.$$

In either case we obtain the claimed bound via division by 4, and these bounds have to be proper since 3ℓ and 4ℓ cannot be primes. □

Next we use Kaneko's bound to prove the bounds from [LOX20]. In contrast to the previous result, the authors instead use an ideal-theoretic approach in their article[18], so we give a complete alternative proof here. We again recall the statement as given in Section 2.2:

Theorem 6. *Let $p \neq \ell$ be distinct primes. Then the following holds:*

(a) *If there are at least three non-equivalent ℓ-isogenies $E_{1728} \to E$ for supersingular curves E_{1728} and E over $\overline{\mathbb{F}_p}$ with $j(E_{1728}) = 1728 \neq j(E)$, then $p < 4\ell^2$.*

(b) *If there are at least four non-equivalent ℓ-isogenies $E_0 \to E$ for supersingular curves E_0 and E over $\overline{\mathbb{F}_p}$ with $j(E_0) = 0 \neq j(E)$, then $p < 3\ell^2$.*

[18] This approach allows them to give a more precise description of the neighborhoods of 0 and 1728, which can alternatively be deduced from the structure of the $\mathbb{F}_p$-rational supersingular isogeny graph (cf. [DG16, Theorem 2.7]).

Proof. As before we note that we have the special automorphisms $\iota \in \mathrm{Aut}(E_{1728})$ and $\omega \in \mathrm{Aut}(E_0)$ of order 4 respectively 3. In the first setting we have three non-equivalent ℓ-isogenies $E_{1728} \to E$, so we can always find two ℓ-isogenies $\varphi_0, \varphi_1 \colon E_{1728} \to E$ such that φ_0 is not equivalent to φ_1 or $\varphi_1 \circ \iota$. Now define the endomorphism

$$\alpha := \widehat{\varphi_0} \circ \varphi_1 \in \mathrm{End}(E_{1728})$$

of degree ℓ^2, which is cyclic by Proposition 9 as φ_0 is not equivalent to φ_1 or $\varphi_1 \circ \iota$. Moreover, α does not commute with ι, since otherwise the cyclic group $\ker(\alpha)$ would have to contain the two distinct order ℓ groups $\ker(\varphi_1)$ and $\ker(\varphi_1 \circ \iota)$. In view of Equation (19), Kaneko's bound therefore yields

$$4p \leq (-\operatorname{disc}(\mathbb{Z}[\iota])) \cdot (-\operatorname{disc}(\mathbb{Z}[\alpha])) = 4 \cdot (4\deg(\alpha) - \operatorname{trd}(\alpha)^2) \leq 16\ell^2.$$

Analogously we find in the second setting two ℓ-isogenies $\varphi_0, \varphi_1 \colon E_0 \to E$ such that φ_0 is not equivalent to φ_1, $\varphi_1 \circ \omega$ or $\varphi_1 \circ \omega^2$. By the same construction we then get a cyclic $\alpha \in \mathrm{End}(E_0)$ of degree ℓ^2 that does not commute with ω, and with Equation (20) Kaneko's bound yields

$$4p \leq (-\operatorname{disc}(\mathbb{Z}[\omega])) \cdot (-\operatorname{disc}(\mathbb{Z}[\alpha])) = 3 \cdot (4\deg(\alpha) - \operatorname{trd}(\alpha)^2) \leq 12\ell^2.$$

Dividing by 4 hence gives the claimed bound in either case, and this bound has to be proper since $3\ell^2$ and $4\ell^2$ cannot be primes.

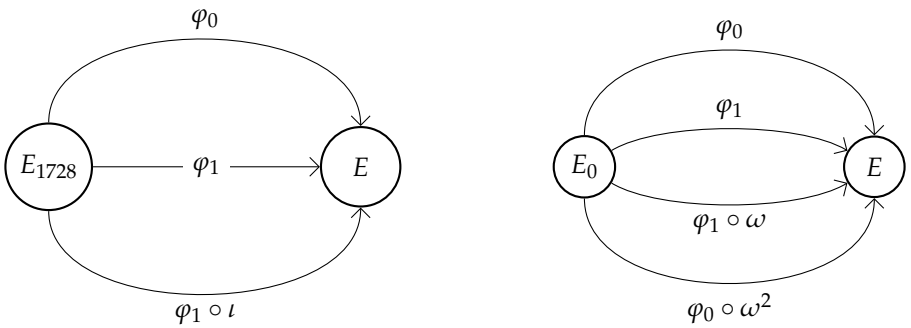
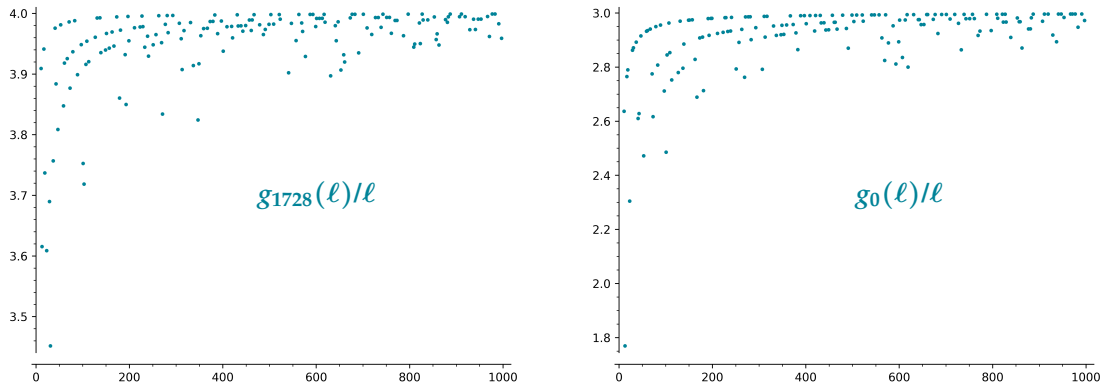


Figure 12: φ_0 is not equivalent to φ_1 and $\varphi_1 \circ \iota$ resp. to φ_1, $\varphi_1 \circ \omega$ and $\varphi_1 \circ \omega^2$.

□

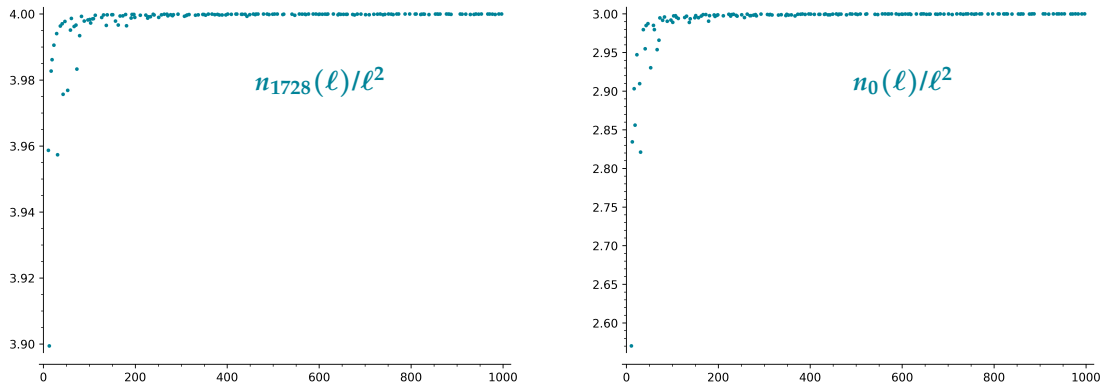
In Figure 13 we illustrate the tightness of the bound of Theorem 5; the corresponding data, which extends the data from [AAM19, Table 1], can be found in the files `special_loop_1728_primes.sage` and `special_loop_0_primes.sage`.



(a) $j = 1728$ (b) $j = 0$

Figure 13: Plots of $g_j(\ell)/\ell$, where $g_j(\ell)$ is the maximal prime for which there exists at least as many non-equivalent endomorphisms of degree ℓ at j (considered in the finite field with $g_j(\ell)$ elements) as in the prerequisites of Theorem 5, for $j \in \{0, 1728\}$ and primes $10 < \ell < 1000$.

In Figure 14 we illustrate the tightness of the bound of Theorem 6; we provide the corresponding data, which extends the data from [LOX20, Table 1], in the files `special_neigh_1728_primes.sage` and `special_neigh_0_primes.sage`.



(a) $j = 1728$ (b) $j = 0$

Figure 14: Plots of $n_j(\ell)/\ell^2$, where $n_j(\ell)$ is the maximal prime for which there exist at least three respectively four non-equivalent ℓ-isogenies $E_j \to E$ with $j(E) \neq j(E_j) = j$, for $j \in \{0, 1728\}$ and primes $10 < \ell < 1000$.

C Loop counting via Hurwitz class numbers

In this section we prove Theorem 36, which strengthens Theorem 35, via Hurwitz class numbers. We briefly recall the statement here:

Theorem 36. *Let $p \neq \ell$ be distinct primes. Then the following are equivalent:*

(i) *For any elliptic curve E over $\overline{\mathbb{F}_p}$ there are exactly $\mu_\ell(j(E); \overline{\mathbb{F}_p})$ equivalence classes of ℓ-isogenies $E \to E$.*

(ii) *The full ℓ-isogeny graph has exactly 2ℓ loops.*

(iii) *p does not divide $4\ell - t^2$ for any $t \in \mathbb{Z}$ with $t^2 < 4\ell$.*

To work towards the proof, we first use the reduction technique to characterize which imaginary quadratic orders occur as endomorphism rings of ordinary elliptic curves; the following gives a converse to Lemma 39 for odd primes:

Proposition 46. Let $\mathcal{O}$ be an imaginary quadratic order and let p be an odd prime. If $\operatorname{disc}(\mathcal{O})$ is a non-zero quadratic residue modulo p, i.e. $\left(\frac{\operatorname{disc}(\mathcal{O})}{p}\right) = 1$ in Legendre symbol notation, then $\mathcal{O}$ is isomorphic to the endomorphism ring of an ordinary elliptic curve over $\overline{\mathbb{F}_p}$.

Proof. Fixing an embedding of $\mathcal{O}$ into $\mathbb{C}$, it is immediate that $\mathcal{O} = \{\alpha \in \mathbb{C} : \alpha\mathcal{O} \subseteq \mathcal{O}\}$, and according to [Sil09, Theorem VI.5.3] we thus find an elliptic curve $\mathcal{E}$ over $\mathbb{C}$ such that $\operatorname{End}(\mathcal{E}) \cong \mathcal{O}$. The j-invariant $j(\mathcal{E})$ of $\mathcal{E}$ hence is an algebraic integer by [Sil94, Theorem II.6.1], so $\mathcal{E}$ is defined over a number field L and has potential good reduction over any prime $\mathfrak{P}$ of L lying above p by [Sil09, Proposition VII.5.5]. Hence we may enlarge L and pick a prime above $\mathfrak{P}$ to assume that $\mathcal{E}$ has good reduction at $\mathfrak{P}$. Due to our assumption we now see that p does not divide the conductor of $\mathcal{O}$ and that p splits in the (quadratic) fraction field K of $\mathcal{O}$ by [Neu99, Proposition I.8.3] since $X^2 - \operatorname{disc}(\mathcal{O})$ splits into two distinct linear factors modulo p. Therefore [Lan87, Theorem 13.4.12] shows that the reduction E of $\mathcal{E}$ modulo $\mathfrak{P}$ is ordinary, and that the reduction of endomorphisms induces an isomorphism $\operatorname{End}(E) \cong \operatorname{End}(\mathcal{E}) \cong \mathcal{O}$. □

Let us briefly recall that an imaginary quadratic order is uniquely determined by its discriminant up to isomorphism. Indeed, $\mathcal{O}$ is a quadratic order in $K = \mathbb{Q}(\sqrt{\operatorname{disc}(\mathcal{O})})$, and in view of the stacked bases theorem we have $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ where $\mathcal{O}_K \subseteq K$ is the ring of integers of K and $f = [\mathcal{O}_K : \mathcal{O}]$ is the conductor of $\mathcal{O}$ (see also [Cox13, Lemma 7.2]), which can be computed from $\operatorname{disc}(\mathcal{O}) = f^2 \operatorname{disc}(\mathcal{O}_K)$ according to Corollary 13.

For an imaginary quadratic order $\mathcal{O}$ of discriminant $d = \operatorname{disc}(\mathcal{O})$ we now set

$$h(d) := |\mathfrak{Cl}(\mathcal{O})| \text{ and } u(d) := \frac{|\mathcal{O}^\times|}{2} = \begin{cases} 1, & d \neq -3, -4 \\ 2, & d = -4 \\ 3, & d = -3 \end{cases}$$

to be the size of its class group and half the size of its (multiplicative) unit group, respectively.

Definition 5. Let $D \in \mathbb{N}$. Then the D-th *Hurwitz class number* $H(D)$ is defined by

$$H(D) := \sum_{df^2 = -D} \frac{h(d)}{u(d)}$$

where the sum runs over all discriminants d and $f \in \mathbb{N}$ with $df^2 = -D$.

The following well-known identity will help us in the final step of our proof:

Proposition 47 ([Hur85, p. 164])**.** Let ℓ be a prime. Then

$$\sum_{t \in \mathbb{Z} \colon t^2 < 4\ell} H(4\ell - t^2) = 2\ell.$$

Proof of Theorem 36. As $\Phi_\ell(X, X) \in \mathbb{F}_p[X]$ has degree 2ℓ, we have

$$\sum_{j \in \overline{\mathbb{F}_p}} \mu_\ell(j; \overline{\mathbb{F}_p}) = 2\ell,$$

and in view of Theorem 35(a) this immediately yields the equivalence of (i) and (ii). To prove the equivalence of (ii) and (iii), we closely follow the proof of [Gro87, Proposition 1.9]:

First assume that p does not divide $4\ell - t^2$ for any $t \in \mathbb{Z}$ with $t^2 < 4\ell$, and note that this implies $p \neq 2$. For each $j \in \overline{\mathbb{F}_p}$ we let E_j denote a curve of j-invariant j; due to Equation (1), the number s of loops in the full isogeny graph is then given by

$$\begin{aligned} s &= \sum_{j \in \overline{\mathbb{F}_p}} |\{\alpha \in \operatorname{End}(E_j) \colon \deg(\alpha) = \ell\}| \cdot |\operatorname{Aut}(E_j)|^{-1} \\ &= \sum_{j \in \overline{\mathbb{F}_p}} \sum_{\substack{t \in \mathbb{Z} \\ t^2 < 4\ell}} |\{\alpha \in \operatorname{End}(E_j) \colon \operatorname{trd}(\alpha) = t, \deg(\alpha) = \ell\}| \cdot |\operatorname{Aut}(E_j)|^{-1} \end{aligned} \tag{21}$$

where only finitely many summands are non-zero; to simplify notation we write

$$A_j(t, \ell) := \{\alpha \in \operatorname{End}(E_j) \colon \operatorname{trd}(\alpha) = t, \deg(\alpha) = \ell\}.$$

Now let $t \in \mathbb{Z}$ with $t^2 < 4\ell$. Any $\alpha \in A_j(t, \ell)$ corresponds to an embedding $\mathcal{O}_{t^2 - 4\ell} \hookrightarrow \operatorname{End}(E_j)$ of a (fixed) imaginary quadratic order of discriminant $D = t^2 - 4\ell$, and any such embedding can be extended uniquely to an embedding of the quadratic imaginary order $\mathcal{O}_d$ above $\mathcal{O}_D$ of a discriminant d satisfying $d \cdot f^2 = t^2 - 4\ell$ for some $f \in \mathbb{N}$. Moreover, $\operatorname{Aut}(E_j)$ acts on such embeddings via conjugation, and this group action descends to $\operatorname{Aut}(E_j)/\{\pm 1\}$ since conjugation by ± 1 is trivial. The stabilizer of an embedding under this action is trivial unless the order itself has discriminant $d = -3$ resp. $d = -4$ (in which case necessarily $j = 0$ resp. $j = 1728$), and then it contains $3 = u(-3)$ respectively $2 = u(-4)$ elements, namely the whole group $\operatorname{Aut}(E_j)/\{\pm 1\}$; put differently, the stabilizer always contains exactly $u(d)$ elements. Writing $h_j(d)$ for the number of optimal embeddings of $\mathcal{O}_d$ up to conjugation, the orbit equation for group actions [Bos18, Proposition 5.1.7] thus yields

$$|A_j(t, \ell)| = \sum_{df^2 = t^2 - 4\ell} h_j(d) \cdot \frac{|\operatorname{Aut}(E_j)/\{\pm 1\}|}{u(d)} = \frac{|\operatorname{Aut}(E_j)|}{2} \cdot \sum_{df^2 = t^2 - 4\ell} \frac{h_j(d)}{u(d)}.$$

Returning to Equation (21) and rearranging the sum, we therefore obtain

$$s = \sum_{j \in \overline{\mathbb{F}_p}} \sum_{\substack{t \in \mathbb{Z} \\ t^2 < 4\ell}} \sum_{df^2 = t^2 - 4\ell} \frac{h_j(d)}{2u(d)} = \sum_{\substack{t \in \mathbb{Z} \\ t^2 < 4\ell}} \sum_{df^2 = t^2 - 4\ell} \frac{1}{2u(d)} \sum_{j \in \overline{\mathbb{F}_p}} h_j(d). \tag{22}$$

In the next step we will focus on the inner sum of the right hand side of Equation (22): To this end we decompose $\overline{\mathbb{F}_p} = \mathbb{J}_{\text{ord}} \sqcup \mathbb{J}_{\text{sup}}$ into j-invariants belonging to ordinary and to supersingular curves. Then, as stated in [Gro87, Equation (1.12)], Eichler [Eic55, Satz 10] proved that

$$\sum_{j \in \mathbb{J}_{\text{sup}}} h_j(d) = \begin{cases} \left(1 - \left(\frac{d}{p}\right)\right) h(d), & d \neq p^2 \cdot d' \\ 0, & d = p^2 \cdot d' \end{cases} \tag{23}$$

where $\left(\frac{d}{p}\right)$ denotes the Legendre symbol. Thus we only need to compute the sum over the $\mathbb{J}_{\text{ord}}$, which allows us to ignore conjugation of embeddings since the corresponding endomorphism rings will be commutative. As p does not divide d by assumption, we now distinguish two cases:

$\left(\frac{d}{p}\right) = -1$: In this case there is no ordinary elliptic curve over $\overline{\mathbb{F}_p}$ with endomorphism ring of discriminant d by Lemma 39, so there cannot be any optimal embedding of $\mathcal{O}_d$ into any $\text{End}(E_j)$, i.e.

$$\sum_{j \in \mathbb{J}_{\text{ord}}} h_j(d) = 0 = \left(1 + \left(\frac{d}{p}\right)\right) h(d).$$

$\left(\frac{d}{p}\right) = 1$: In this case there is an ordinary elliptic curve over $\overline{\mathbb{F}_p}$ with endomorphism ring of discriminant d by Proposition 46. Moreover, for each such curve there are exactly 2 such optimal embeddings of $\mathcal{O}_d$. In fact, we first get a second embedding by post-composing with the dualization map (equivalently by pre-composing with the unique non-trivial element of $\text{Gal}(\mathbb{Q}(\sqrt{d})|\mathbb{Q})$). Further, any two embeddings i_1, i_2 have the same image and thus induce an automorphism $i_2^{-1} \circ i_1$ on $\mathcal{O}_d$; this automorphism corresponds via $\mathbb{Q}$-linear extension to a unique element of $\text{Gal}(\mathbb{Q}(\sqrt{d})|\mathbb{Q})$, so the above two embeddings are indeed all embeddings. Finally, the simply transitive action of the class group $\mathfrak{Cl}(\mathcal{O}_d)$ on the ordinary curves over $\overline{\mathbb{F}_q}$ with endomorphism ring isomorphic to $\mathcal{O}_d$ (cf. [Sut13, Section 2.8]), together with the fact that there is at least one such curve, shows that there are exactly $|\mathfrak{Cl}(\mathcal{O}_d)| = h(d)$ such curves (up to isomorphism). Hence we obtain

$$\sum_{j \in \mathbb{J}_{\text{ord}}} h_j(d) = 2 \cdot h(d) = \left(1 + \left(\frac{d}{p}\right)\right) h(d).$$

Altogether the sum over $\mathbb{J}_{\text{ord}}$ is equal to $(1 + (\frac{d}{p})) \cdot h(d)$, and due to $p \nmid d$ Equation (23) yields

$$\sum_{j \in \overline{\mathbb{F}_p}} h_j(d) = \sum_{j \in \mathbb{J}_{\text{ord}}} h_j(d) + \sum_{j \in \mathbb{J}_{\text{sup}}} h_j(d) = \left(1 + \left(\frac{d}{p}\right)\right) h(d) + \left(1 - \left(\frac{d}{p}\right)\right) h(d) = 2h(d).$$

With this identity and Proposition 47 we return to Equation (22) to finally deduce

$$s = \sum_{\substack{t \in \mathbb{Z} \\ t^2 < 4\ell}} \sum_{df^2 = t^2 - 4\ell} \frac{2h(d)}{2u(d)} = \sum_{\substack{t \in \mathbb{Z} \\ t^2 < 4\ell}} H(4\ell - t^2) = 2\ell.$$

Conversely suppose that p divides $D = 4\ell - t^2$. Then the above formulas still hold for all d with $p \nmid d$ (at least if p is odd), but they do not hold for any d with $p \mid d$. In fact, for such a d we have no ordinary elliptic curve with an optimal embedding $\mathcal{O}_d \hookrightarrow \text{End}(E)$ by Lemma 39. Moreover, Equation (23) still holds true, where for $p = 2$ the symbol $\left(\frac{d}{p}\right)$ has to be interpreted as $-1, 0, 1$ according to whether p is inert, ramified or completely split in $\mathbb{Q}(\sqrt{d})$ (cf. [Eic55, Equation (9)]); as we assume that p divides d, we therefore obtain

$$\sum_{j \in \mathbb{J}_{\text{ord}}} h_j(d) + \sum_{j \in \mathbb{J}_{\text{sup}}} h_j(d) \leq 0 + h(d) < 2h(d).$$

By assumption we can always find a d with $p \mid d$, namely $d = D$ (with conductor $f = 1$), so summing over all d shows

$$s < \sum_{\substack{t \in \mathbb{Z} \\ t^2 < 4\ell}} \sum_{df^2 = t^2 - 4\ell} \frac{2h(d)}{2u(d)} = 2\ell;$$

here we note that this inequality also holds for $p = 2$, since we will always have at most $2h(d')$ ordinary curves over $\overline{\mathbb{F}_2}$ (up to isomorphism) with endomorphism ring of a given discriminant d'. □