SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Classification of Elliptic Curves with ℓ-Torsion over Finite Fields

av

Johanna Tano

2026 - No K5

Classification of Elliptic Curves with ℓ-Torsion over Finite Fields

Johanna Tano

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Sjoerd Wijnand de Vries

2026

Abstract

We develop theory and algorithms for the classification of elliptic curves over finite fields. Using geometric and arithmetic invariants, we study Weierstrass equations up to isomorphism, and for ordinary curves we show that the ℓ-adic height of the endomorphism ring relative to Frobenius determines the rank of the rational ℓ-torsion subgroup. We interpret this description through the theory of isogeny volcanoes, obtaining both structural insight and an efficient algorithm for computing this rank without point-finding methods. We can then count $\mathbb{F}_q$-rational points of order ℓ up to isomorphism by classifying their orbits under automorphisms. As an application, we compute traces of Hecke operators, recovering known values up to an explicit correction term.

Abstract

Vi utvecklar teori och algoritmer för klassificering av elliptiska kurvor över ändliga kroppar. Med hjälp av geometriska och aritmetiska egenskaper studerar vi Weierstrassekvationer upp till isomorfi, och för ordinära kurvor visar vi att den ℓ-adiska höjden av endomorfismringen relativt Frobenius avgör rangen hos den rationella ℓ-torsionsgruppen. Vi tolkar våra resultat genom teorin om isogenivulkaner, vilket ger både ökad strukturell insikt samt en effektiv algoritm för att beräkna denna rang utan punktsökningsmetoder. Vi kan därefter räkna $\mathbb{F}_q$-rationella punkter av ordning ℓ upp till isomorfi genom att klassificera deras banor under automorfismer. Som en tillämpning beräknar vi spår av Heckeoperatorer och återfår kända värden upp till en explicit korrektionsterm.

Contents

1 Introduction **7**

2 Preliminaries **8**

3 Classification of Curves **10**
3.1 Geometric Invariant 10
3.2 Isomorphism Classes 11
3.3 Enumerate Curves over $\mathbb{F}_q$ 14
3.3.1 Algorithm 14

4 Invariants Governed by Frobenius **15**
4.1 The Endomorphism Ring 15
4.2 Number of Rational Points 17
4.3 Isogeny Classes 18
4.4 Number Field Embedding 19

5 Arithmetic Approach to ℓ-Torsion Subgroups **22**
5.1 Probing Ideals In The Endomorphism Ring 23
5.2 The ℓ-adic Height of Number Field Order 24
5.3 Frobenius Stable ℓ-Isogenies 27
5.4 Visualizing Isogeny Volcanoes 28
5.5 Compute Rank of $E[\ell](\mathbb{F}_q)$ 30
5.5.1 Algorithm 31

6 Classification of ℓ-Torsion Points **32**
6.1 Fixed Points And Automorphism Orbits 33
6.2 Determine Size of $\mathcal{P}_\ell(\mathbb{F}_q)$ 34
6.2.1 Algorithm 37

7 An Application to Modular Forms **38**
7.1 Trace of Hecke Operator 38

8 End Note **40**

1 INTRODUCTION

In this paper, we develop theory and algorithms for the classification of elliptic curves over finite fields, with emphasis on their rational prime torsion structure. We aim for a complete enumeration over the entire field of definition: given a finite field of size q and a prime ℓ, our end goal is to be able to count distinct pairs (E, P) up to isomorphism, where E is an elliptic curve defined over $\mathbb{F}_q$ and P is a rational point of order ℓ. Motivated both by the desire for our algorithms to scale efficiently in q and ℓ, and by the pursuit of a deeper structural understanding of how arithmetic invariants, in particular Frobenius, govern the rational points, we intentionally adopt a strict number-theoretic approach to some aspects of the classification problem.

Chapter 2 provides a short introduction to finite fields and preliminaries on elliptic curves. Chapter 3 develops the geometric classification of curves by their j-invariant, ending with an algorithm that enumerates all curve equations up to isomorphism defined over $\mathbb{F}_q$. Chapter 4 turns to the arithmetic side, introducing the endomorphism ring of a curve and isogeny classes, an indexing of curves by another invariant: the trace of Frobenius. We also introduce additional number-theoretical background needed in the following chapter.

In Chapter 5, we shift focus to the structure of rational points, with the goal of determining the size of the rational ℓ-torsion subgroup. Avoiding computationally expensive point-finding methods, we study the endomorphism ring of a curve and kernels of ℓ-isogenies, to probe this problem from a more computationally feasible perspective. We show that for our classification task, it is enough to know whether the endomorphism ring of a curve lies above a certain threshold relative to ℓ within a larger number field governed by Frobenius. This leads us to an existing algorithm for computing the endomorphism ring, and to the theory of isogeny volcanoes, which we draw on as inspiration both to develop instructive visualizations as well as for the design of our final algorithm.

Once the number of ℓ-torsion points on each curve is known, it remains to determine how these points behave under the action of automorphisms, which includes looking more closely at the structure of some individual point geometry. We then end Chapter 6 with the final algorithm to count equivalent pairs (E, P) over $\mathbb{F}_q$. Finally, in Chapter 7, as an application and verification of our algorithms, we compute the trace of Hecke operators on modular forms where we are able to get consistent results up to an error term comparing with known data.

2 PRELIMINARIES

Finite Fields

We denote by $\mathbb{F}_q$ the finite field with q elements, where $q = p^n$ for p prime and n positive integer. The multiplicative group $\mathbb{F}_q^\times$ is cyclic of order $q-1$. We will use the following basic property of subgroups of cyclic groups.

Lemma 2.1. *Let g be a generator of $\mathbb{F}_q^\times$, then the subgroup of n-th powers is given by*

$$(\mathbb{F}_q^\times)^n = \{x^n : x \in \mathbb{F}_q^\times\} = \langle g^{\gcd(n,q-1)} \rangle, \qquad \#(\mathbb{F}_q^\times)^n = \frac{q-1}{\gcd(n,q-1)},$$

and the quotient group $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^n$ has index $[\mathbb{F}_q^\times : (\mathbb{F}_q^\times)^n] = \gcd(n, q-1)$.

Proof. See, e.g., [5, Chapter 2.3 and 3]. □

Elliptic Curves

Geometric Definition

An elliptic curve E/K over a field with $\mathrm{char}(K) \neq 2, 3$ can be defined by an equation

$$E\colon y^2 = x^3 + Ax + B, \quad A, B \in K,$$

with non-vanishing discriminant $\Delta = 4A^3 + 27B^2 \neq 0$. This is called the short **Weierstrass** form. In particular, the pair $(A, B) = (0, 0)$ is excluded, and at most one of A, B is zero. We denote by $E(\overline{K})$ the set of affine solutions $(x, y) \in \overline{K} \times \overline{K}$ to the equation together with a distinguished point at infinity $\{\infty\}$, and the K-rational subset as $E(K)$.

Remark 2.2. *Since we work throughout in $\mathrm{char}(K) \neq 2, 3$, we may identify a curve E with its coefficient pair (A, B), and shall write $E_{A,B}$ when need to emphasize this.*

Abelian Group of Points

The unique feature of elliptic curves is that the points $E(\overline{K})$ carries a natural abelian group structure, where addition is defined geometrically by the so called chord-tangent rule. Over a finite field, this makes $E(\mathbb{F}_q)$ into a finite abelian group, and by the structure theorem, we know that it is isomorphic to a direct sum of cyclic groups

$$E(\mathbb{F}_q) \cong \bigoplus_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}, \qquad d_i \mid d_{i+1}.$$

By this description $E(\mathbb{F}_q)$ has d_1^r points of order dividing d_1. However, for any integer n, the n-torsion subgroup over $\overline{\mathbb{F}}_q$ is known to be isomorphic to either $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$,

$\mathbb{Z}/n\mathbb{Z}$ or $\{\infty\}$ [12, Theorem III.6.1]. In particular, the d_1^r points of order dividing d_1 in $E(\mathbb{F}_q)$ must be contained in such torsion subgroup, yielding $r \leq 2$ and $E(\mathbb{F}_q)$ is either trivial, cyclic or bicyclic, and the only possible group structures over $\mathbb{F}_q$ are

$$E(\mathbb{F}_q) \cong \{\infty\} \quad \text{or} \quad E(\mathbb{F}_q) \cong \mathbb{Z}_n \quad \text{or} \quad E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

for some integer $n \geq 1$, or for some integers $n_1, n_2 \geq 1$ with $n_1 \mid n_2$ [18, Theorem 4.1].

Maps Between Curves

A morphism $\varphi : E \to E'$ between curves is a map on $E(\overline{K})$, which on affine points can be written as $\varphi(x, y) = (R(x), yS(x))$, where $R(x) = p(x)/q(x)$ and $S(x)$ are rational functions with $p(x), q(x) \in K[x]$. We say that φ is defined over K when its coefficients lie in K.

An **isogeny** $\phi : E \to E'$ is a morphism that also satisfies $\phi(\infty) = \infty$. If such a map exists, the curves are said to be **isogenous**. An important property is that every isogeny is also a group homomorphism preserving the group structure. The **degree** of an isogeny is $\deg(\phi) := \max(\deg p(x), \deg q(x))$. An isogeny is **separable** if $R'(x) \neq 0$, and **inseparable** otherwise. Since addition of a curve is defined geometrically, we denote by $[n]$ repeated addition of a point P n times.

For any isogeny $\phi : E \to E'$ of degree m, there exists a unique isogeny $\hat{\phi} : E' \to E$, called the **dual isogeny**, satisfying

$$\hat{\phi} \circ \phi = [m] \text{ on } E \quad \text{and} \quad \phi \circ \hat{\phi} = [m] \text{ on } E'.$$

Further important properties of the dual we will be using throughout is

i Additivity: $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$,
ii Self-duality for integer isogenies: $\widehat{[m]} = [m]$ with $\deg[m] = m^2$,
iii Preserves degree: $\deg \hat{\varphi} = \deg \varphi$.

Every non-constant isogeny has finite kernel, and if an isogeny $\phi : E \to E'$ is separable, then we can determine the size of its kernel as

$$\deg(\phi) = \#\ker(\phi), \quad \ker(\phi) \subseteq E(\overline{K}). \tag{1}$$

The set of isogenies between elliptic curves E and E' is denoted by $\mathrm{Hom}_{\overline{K}}(E, E')$. If we also treat the zero map defined as $[0]P = \infty$ as an isogeny of degree 0, we can make this set into an abelian group under pointwise addition, with the zero map $[0]$ as the identity. We denote by $\mathrm{Hom}_K(E, E')$ the subset of isogenies defined over K. For proofs and more details on curve morphisms, isogenies and properties of the dual, see e.g. [12, Chapter III] and [18, Chapter 3].

3 CLASSIFICATION OF CURVES

Our first goal is to study some pure geometrical properties of curves, namely the coefficient pair (A, B), and how it give rise to certain invariants and special types of curves, leading up to classifying unique curves up to equivalence over a base field.

3.1 Geometric Invariant

A natural invariant of a Weierstrass equation is the **j-invariant**. For a curve E with coefficients (A, B), it is defined as

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}. \tag{2}$$

Special values arises when one coefficient is zero, giving $j \in \{0, 1728\}$. These curves admit extra symmetry and therefore often requires separate treatment. The j-invariant is directly tied to the equivalence of curves, and we begin by study the set of coefficients corresponding to a fixed j-invariant.

Definition 3.1. *Denote by*

$$\mathcal{W}_j(\mathbb{F}_q) = \{(A, B) \in \mathbb{F}_q^2 : 4A^3 + 27B^2 \neq 0,\ j(E_{A,B}) = j\}$$

the set of short Weierstrass coefficients over $\mathbb{F}_q$ with j-invariant j.

Lemma 3.2. *For every $j \in \mathbb{F}_q$, there exists an elliptic curve $E/\mathbb{F}_q$ such that $j(E) = j$. In particular, the coefficient pair (A, B) may be chosen as $(0, 1)$ if $j = 0$, as $(1, 0)$ if $j = 1728$, and as $\left(\frac{3j}{1728-j}, \frac{2j}{1728-j}\right)$ otherwise.*

The next proposition shows how every pair in $\mathcal{W}_j(\mathbb{F}_q)$ can be generated by starting from a fixed pair (A, B), for example as in Lemma 3.2, and applying a simple transformation.

Proposition 3.3. *Fix one pair $(A, B) \in \mathcal{W}_j(\mathbb{F}_q)$, and define $\Psi_{A,B} : \mathbb{F}_q^\times \to \mathcal{W}_j(\mathbb{F}_q)$ by*

$$\Psi_{A,B}(u) = \begin{cases} (0, uB), & \text{if } j = 0, \\ (uA, 0), & \text{if } j = 1728, \\ (u^2A, u^3B), & \text{if } j \notin \{0, 1728\}. \end{cases}$$

Then $\Psi_{A,B}$ is well-defined and bijective.

Proof. A direct computation shows that $\mathrm{Im}(\Psi_{A,B}) \subseteq \mathcal{W}_j(\mathbb{F}_q)$ so the map is well-defined. We now aim to show it is surjective. Let $(A', B') \in \mathcal{W}_j(\mathbb{F}_q)$. First note that $\mathrm{char}(\mathbb{F}_q) \neq$

$2, 3$, so the constants 4, 27, and $1728 = 2^6 \cdot 3^3$ in Equation 2 are units in $\mathbb{F}_q$, so

$$j(E_{A',B'}) = 0 \iff A' = 0, \qquad j(E_{A',B'}) = 1728 \iff B' = 0.$$

This implies that distinct pairs in $\mathcal{W}_j(\mathbb{F}_q)$ for $j \in \{0, 1728\}$ must have their non-zero coefficient differ by some element $u \in \mathbb{F}_q^\times$, hence the claim follows. For $j \notin \{0, 1728\}$, we need to find an $u \in \mathbb{F}_q^\times$ such that $\Psi_{(A,B)}(u) = (A', B')$. Using the given assumption $j(E_{A,B}) = j(E_{A',B'})$ and Equation 2 we know that the coefficients satisfy $(A'A^{-1})^3 = (B'B^{-1})^2$. Let $A'A^{-1} = \alpha$ and $B'B^{-1} = \beta$ for some $\alpha, \beta \in \mathbb{F}_q^\times$, then

$$\alpha^3 = \beta^2 \quad \text{and} \quad A' = \alpha A, \quad B' = \beta B.$$

Now set $u = \beta\alpha^{-1}$, then $\Psi_{(A,B)}(u) = (\alpha A, \beta B) = (A', B')$, and we conclude $\Psi_{A,B}$ surjective. To prove injectivity, suppose $\Psi_{A,B}(u) = \Psi_{A,B}(v)$. If $j \in \{0, 1728\}$, then immediately $u = v$. If $j \notin \{0, 1728\}$, then $u^2 = v^2$ and $u^3 = v^3$, hence $(uv^{-1})^2 = 1$ and $(uv^{-1})^3 = 1$, which implies $uv^{-1} = 1$, so $u = v$, yielding $\Psi_{A,B}$ injective as claimed. □

3.2 Isomorphism Classes

We are now ready to define the equivalence of curves in terms of isomorphism classes, using the definitions and results from the previous section.

Definition 3.4. *Denote the set of isomorphism classes of elliptic curves over $\mathbb{F}_q$ by*

$$\mathcal{E}(\mathbb{F}_q) = \{E : E/\mathbb{F}_q\}/\sim,$$

where $E \sim E'$ if and only if there exists a non-zero element $u \in \mathbb{F}_q$ such that the coefficients satisfy

$$A' = u^4 A \quad \textit{and} \quad B' = u^6 B.$$

*The curves E and E' are then said to be **isomorphic** over $\mathbb{F}_q$, and we write $E \cong_{\mathbb{F}_q} E'$.*

We immediately have the following necessary condition for isomorphic curves, following directly from the definition of j-invariant and isomorphism.

Corollary 3.5. *If $E \cong_{\mathbb{F}_q} E'$ then $j(E) = j(E')$.*

Definition 3.6. *For $j \in \mathbb{F}_q$, define*

$$e_j = \begin{cases} 6, & \textit{if } j = 0, \\ 4, & \textit{if } j = 1728, \\ 2, & \textit{otherwise.} \end{cases}$$

Corollary 3.7. *An **automorphism** of E is an isomorphism $E \to E$. The automorphism group of E over $\mathbb{F}_q$ is*

$$\mathrm{Aut}_{\mathbb{F}_q}(E) \cong \mu_{e_j}(\mathbb{F}_q) = \{u \in \mathbb{F}_q^\times : u^{e_j} = 1\},$$

where $\mu_{e_j}(\mathbb{F}_q)$ is the group of e_j-th roots of unity in $\mathbb{F}_q^\times$ and has size $\gcd(e_j, q-1)$.

Proof. It follows directly from Definition 3.4 requiring $(A, B) = (u^4 A, u^6 B)$. For more details of the isomorphism see [12, Corollary III.10.2]. □

Corollary 3.8. *Let $\Psi_{A,B}$ be defined as in Proposition 3.3. Then $E \cong_{\mathbb{F}_q} E'$ if and only if $\Psi_{A,B}(w) = (A', B')$ for some $w \in (\mathbb{F}_q^\times)^{e_j}$.*

Proof. From Definition 3.4, $E \cong_{\mathbb{F}_q} E'$ if and only if $(A', B') = (u^4 A, u^6 B)$ for some $u \in \mathbb{F}_q^\times$. Rewriting this in terms of e_j gives

$$(u^4 A, u^6 B) = \begin{cases} (0, u^{e_j} B), & \text{if } j = 0, \\ (u^{e_j} A, 0), & \text{if } j = 1728, \\ ((u^{e_j})^2 A, (u^{e_j})^3 B), & \text{if } j \notin \{0, 1728\}. \end{cases}$$

Set $w := u^{e_j}$, clearly $w \in (\mathbb{F}_q^\times)^{e_j}$ and we can write $(A', B') = \Psi_{A,B}(w)$. □

Corollary 3.9. *Two elliptic curves are isomorphic over $\overline{\mathbb{F}}_q$ if and only if they have the same j-invariant.*

Proof. The forward direction follows from Corollary 3.5. For the converse, suppose $j(E) = j(E')$. By Corollary 3.8, it suffices to show that $(A', B') = \Psi_{A,B}(w)$ for some $w \in (\overline{\mathbb{F}}_q^\times)^{e_j}$. By assumption, we know $(A', B') \in \mathcal{W}_{j(E)}(\overline{\mathbb{F}}_q)$ and so $(A', B') = \Psi_{A,B}(u)$ for some $u \in \overline{\mathbb{F}}_q^\times$. But since $\overline{\mathbb{F}}_q$ is algebraically closed, the map $x \mapsto x^{e_j}$ is surjective on $\overline{\mathbb{F}}_q^\times$, and there exists $w \in \overline{\mathbb{F}}_q^\times$ such that $u = w^{e_j}$, which proves the claim. □

Twists and Symmetry

We note that the equivalence in Corollary 3.9 only holds over the algebraic closure. In general, the map $x \mapsto x^{e_j}$ is not surjective on $\mathbb{F}_q^\times$ and hence the converse direction fails. However, since curves sharing the same j-invariant eventually become isomorphic over some extension of $\mathbb{F}_q$, we are motivated to partition $\mathcal{E}(\mathbb{F}_q)$ into subsets indexed by j.

Definition 3.10. *Denote the set of isomorphism classes of elliptic curves over $\mathbb{F}_q$ with a fixed j-invariant by*

$$\mathcal{E}_j(\mathbb{F}_q) = \{E : E/\mathbb{F}_q \text{ elliptic curve with } j(E) = j\}/\sim,$$

where $E \sim E'$ if and only if $E \cong_{\mathbb{F}_q} E'$. Following the standard terminology in the literature, we refer to the distinct isomorphism classes in this set as ***twists****.*

Proposition 3.11. *Let e_j depend on j as in Definition 3.6. Then the set of twists for a fixed j-invariant is in bijection with the quotient group*

$$\mathcal{E}_j(\mathbb{F}_q) \cong \mathbb{F}_q^\times / (\mathbb{F}_q^\times)^{e_j}.$$

Proof. Fix $(A, B) \in \mathcal{W}_j(\mathbb{F}_q)$. By Proposition 3.3, the map $\Psi_{A,B} : \mathbb{F}_q^\times \to \mathcal{W}_j(\mathbb{F}_q)$ is a bijection. Let g be a generator of $\mathbb{F}_q^\times$. Then every coefficient pair in $\mathcal{W}_j(\mathbb{F}_q)$ can be written, and hence identified uniquely by g^k in $\mathbb{F}_q^\times$ as

$$\Psi_{A,B}(g^k) \qquad \text{for some } k \in \{0, 1, \ldots, q-2\}.$$

By Corollary 3.8 we get $\mathbb{F}_q$-isomorphic curves if and only if their coefficients differ by an element of $(\mathbb{F}_q^\times)^{e_j}$. Thus

$$E_{\Psi_{A,B}(g^m)} \cong_{\mathbb{F}_q} E_{\Psi_{A,B}(g^n)} \iff g^{n-m} \in (\mathbb{F}_q^\times)^{e_j}.$$

From Lemma 2.1, the e_j-th power subgroup of $\mathbb{F}_q^\times$ is given by $(\mathbb{F}_q^\times)^{e_j} = \langle g^d \rangle$ with $d = \gcd(e_j, q-1)$, hence $g^{n-m} \in (\mathbb{F}_q^\times)^{e_j}$ if and only if $n \equiv m \mod d$, and we can construct the bijection as

$$g^i(\mathbb{F}_q^\times)^{e_j} \longmapsto [E_{\Psi_{A,B}(g^i)}] \in \mathcal{E}_j(\mathbb{F}_q), \qquad i = 0, 1, \ldots, d-1.$$

□

For $j \notin \{0, 1728\}$, the set $\mathcal{E}_j(\mathbb{F}_q)$ always contains exactly two twists, commonly referred to as **quadratic twists**, due to the fact that they become isomorphic over the quadratic extension $\mathbb{F}_{q^2}$. To see this, if $E \ncong_{\mathbb{F}_q} E'$, then by Corollary 3.8 we have $(A', B') = \Psi_{A,B}(u)$ for some nonsquare $u \in \mathbb{F}_q^\times$. Passing to the extension, by [8, Proposition 7.1.2], the equation $w^2 = u$ has a solution in $\mathbb{F}_{q^2}$ if and only if $u^{(q^2-1)/2} = 1$, but since $u \in \mathbb{F}_q^\times$, we have $u^{(q^2-1)/2} = u^{(q-1)(q+1)/2} = 1$, and $(A', B') = \Psi_{A,B}(w^2)$ yielding $E \cong_{\mathbb{F}_{q^2}} E'$.

Remark 3.12. *By Lemma 2.1, the number of twists in $\mathcal{E}_j(\mathbb{F}_q)$ is $[\mathbb{F}_q^\times : (\mathbb{F}_q^\times)^{e_j}] = \gcd(e_j, q-1)$, which is also the size of $\mathrm{Aut}_{\mathbb{F}_q}(E)$. Equivalently, a curve admitting more symmetry will, if the base field contains the necessary roots of unity, obtain a larger automorphism group. This in turn results in shorter isomorphism orbits under $\Psi_{A,B}$, and hence more non-isomorphic twists over $\mathbb{F}_q$.*

Theorem 3.13. *The set of distinct curves up to isomorphism defined over $\mathbb{F}_q$ is*

$$\mathcal{E}(\mathbb{F}_q) \;=\; \bigsqcup_{j\in\mathbb{F}_q} \mathcal{E}_j(\mathbb{F}_q),$$

where the total number of isomorphism classes is given by

$$\#\mathcal{E}(\mathbb{F}_q) \;=\; 2(q-2) + \gcd(4, q-1) + \gcd(6, q-1).$$

Proof. Using Proposition 3.11 and Lemma 3.2 we get the total number of distinct elliptic curves by summing over the size of the twist sets for each $j \in \mathbb{F}_q$ as

$$\sum_{j\in\mathbb{F}_q} [\mathbb{F}_q^\times : (\mathbb{F}_q^\times)^{e_j}] \;=\; [\mathbb{F}_q^\times : (\mathbb{F}_q^\times)^2](q-2) \;+\; [\mathbb{F}_q^\times : (\mathbb{F}_q^\times)^4] \;+\; [\mathbb{F}_q^\times : (\mathbb{F}_q^\times)^6].$$

By Lemma 2.1, each index equals $\gcd(e_j, q-1)$, and noting that q is odd, we have $\gcd(2, q-1) = 2$ and the desired formula follows. □

3.3 Enumerate Curves over $\mathbb{F}_q$

We close this section with an algorithm that returns one coefficient pair for each $\mathbb{F}_q$-isomorphism class in $\mathcal{E}(\mathbb{F}_q)$.

3.3.1 Algorithm

Algorithm 1 Enumerates all elliptic curves over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism.

```
1:  function EnumCurves(q)
2:      g ← generator of F_q^×
3:      E ← [ ]                                   ▷ initialize empty list
4:      for j ∈ F_q do
5:          (A, B) ← Weierstrass coefficients for j        ▷ see Lemma 3.2
6:          for i = 0, 1, ..., gcd(e_j, q − 1) − 1 do      ▷ e_j as in Definition 3.6
7:              Append Ψ_{A,B}(g^i) to E                   ▷ see Proposition 3.3
8:          end for
9:      end for
10:     return E
11: end function
```

4 INVARIANTS GOVERNED BY FROBENIUS

While the j-invariant gives a geometric classification, over finite fields the Frobenius endomorphism provides a second fundamental invariant. It governs the structure of $\mathbb{F}_q$-rational points and leads us to another indexing of curves. It also connects elliptic curves to their associated number fields and endomorphism rings, which will be central in Chapter 5.

4.1 The Endomorphism Ring

An **endomorphism** is an isogeny from a curve to itself. We denote by

$$\mathrm{End}_{\overline{\mathbb{F}}_q}(E) := \mathrm{Hom}_{\overline{\mathbb{F}}_q}(E, E)$$

the set of all such endomorphisms. This set inherits the abelian group structure described in Chapter 2, but we can now also define multiplication as composition of maps, and it becomes a ring. To simplify notation, we write $\mathrm{End}(E) := \mathrm{End}_{\overline{\mathbb{F}}_q}(E)$.

A fundamental class of endomorphisms comes from the abelian group structure on points. Since the group law is given by rational functions, repeated addition yields a natural embedding $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$, $n \mapsto [n]$, where $[n]$ denotes multiplication by n [18, Theorem 3.6]. In particular, the endomorphism ring is unital, and by [12, Proposition 4.2] it has characteristic 0 and no zero divisors. In most cases $\mathrm{End}(E)$ is also commutative, and curves are said to be **ordinary** if so, and **supersingular** otherwise [11, Definition 3.3]. In this paper we restrict the theory developed around endomorphism rings to those of ordinary curves. In either case, we note that the embedding $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ must land in the center to preserve the abelian group structure of $\mathrm{End}(E)$. An endomorphism also has its dual in the same ring, and we add two useful definitions.

Definition 4.1. *For an endomorphism $\varphi \in \mathrm{End}(E)$, define the **trace** and **norm** by*

$$\mathrm{Tr}(\varphi) := \varphi + \hat{\varphi} \in \mathbb{Z} \subseteq \mathrm{End}(E) \qquad \textit{and} \qquad \mathrm{N}(\varphi) := \hat{\varphi} \circ \varphi = \deg(\varphi) \in \mathbb{Z} \subseteq \mathrm{End}(E),$$

The fact that the norm is an integer is immediate from definition of degree. The fact that the trace lands in $\mathbb{Z}$ is due to the next lemma, derived from Proposition [12, p. III.8.6]

Lemma 4.2. *For any $\alpha \in \mathrm{End}(E)$, we have*

$$\mathrm{Tr}(\alpha) = 1 + \deg \alpha - \deg(1 - \alpha) \in \mathbb{Z}.$$

Proof. Using properties of the dual isogeny, we compute

$$\begin{aligned}\deg(1-\alpha) &= (1-\alpha)\widehat{(1-\alpha)} = (1-\alpha)(1-\hat{\alpha}) \\ &= 1-\alpha-\hat{\alpha}+\alpha\hat{\alpha} = 1-(\alpha+\hat{\alpha})+\deg(\alpha) \\ &= 1-\mathrm{Tr}(\alpha)+\deg(\alpha).\end{aligned}$$

Rearranging yields the result. □

We further note that an automorphism $\sigma \in \mathrm{End}_{\mathbb{F}_q}(E)$ must satisfy $\deg(\sigma) = 1$, and $\sigma \circ \hat{\sigma} = [1]$, so $\mathrm{Aut}_{\mathbb{F}_q}(E)$ may be identified with the subgroup of units in $\mathrm{End}_{\mathbb{F}_q}(E)$.

Definition 4.3. *Let $E/\mathbb{F}_q$ be an elliptic curve. The q-th* ***Frobenius endomorphism*** *$\pi_q : E \to E$ is defined as*

$$\pi_q(x,y) = (x^q, y^q), \quad \pi_q(\infty) = \infty.$$

Remark 4.4. *We will omit the subscript q when the context is clear, and simply write π for the Frobenius endomorphism.*

Proposition 4.5. *The Frobenius endomorphism π satisfies the quadratic relation*

$$\pi^2 - t\pi + q = 0 \in \mathrm{End}(E), \qquad \textit{where } t := \mathrm{tr}(\pi) \textit{ and } q := \mathrm{N}(\pi).$$

Proof. We start by noting that $\mathrm{N}(\pi) = \deg(\pi) = q$ by definition of degree of an isogeny. Then the identity follows from a simple verification

$$\pi^2 - \mathrm{tr}(\pi)\cdot\pi + \mathrm{N}(\pi) = \pi^2 - (\pi+\hat{\pi})\pi + \hat{\pi}\pi = \pi^2 - \pi^2 - \hat{\pi}\pi + \hat{\pi}\pi = 0.$$

□

Frobenius and the base field

A key property of the q-th Frobenius endomorphism is that $x^q = x$ for all $x \in \mathbb{F}_q$. In fact, an element $u \in \overline{\mathbb{F}}_q$ belongs to $\mathbb{F}_q$ if and only if it is fixed by Frobenius. This gives an alternative description of the $\mathbb{F}_q$-rational endomorphisms: an endomorphism $\varphi \in \mathrm{End}(E)$ is defined over $\mathbb{F}_q$ if and only if it commutes with Frobenius, that is

$$\mathrm{End}_{\mathbb{F}_q}(E) = \{\varphi \in \mathrm{End}(E) \mid \varphi \circ \pi = \pi \circ \varphi\}.$$

For ordinary curves, however, we already know $\mathrm{End}(E)$ is commutative, hence this applies to all endomorphisms yielding the following result, see [11, 19, Theorem 4.3, Theorem 7.2].

Lemma 4.6. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve. Then $\mathrm{End}_{\mathbb{F}_q}(E) = \mathrm{End}_{\overline{\mathbb{F}}_q}(E)$.*

In particular we deduce the following

Corollary 4.7. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve, then* $\mathrm{End}(E) \cong \mathrm{End}(E')$ *for any $E' \in \mathcal{E}_j(E)(\mathbb{F}_q)$.*

Special j-Invariants and Supersingularity

By Proposition 3.7, the automorphism group of E is determined by which roots of unity lie in $\mathbb{F}_q^\times$. However, by Lemma 4.6, the endomorphism ring and hence the subgroup of units does not change for an ordinary curve over any extension field. This forces a curve with $j(E) \in \{0, 1728\}$ to be supersingular if and only if $\mathbb{F}_p$ does not contain the required roots of unity [11, Chapter 3], and we can directly state a result on the automorphism group of ordinary curves.

Lemma 4.8. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve. Then*

$$\mathrm{Aut}_{\mathbb{F}_q}(E) \cong \begin{cases} \mu_4 & \text{if } j(E) = 1728, \\ \mu_6 & \text{if } j(E) = 0, \\ \mu_2 & \text{otherwise.} \end{cases}$$

For any elliptic curve, there is another characterization of supersingularity in terms of the trace of Frobenius, for proof see [18, Proposition 4.31].

Lemma 4.9. *Let $E/\mathbb{F}_q$ be an elliptic curve, then E is supersingular if and only if* $\mathrm{tr}(\pi) \equiv 0 \pmod{p}$ *where $p = \mathrm{char}(\mathbb{F}_q)$.*

4.2 Number of Rational Points

Using Frobenius, we also obtain the following characterizations of the rational points.

Definition 4.10. *For an elliptic curve $E/\mathbb{F}_q$, we identify the set of rational points as*

$$E(\mathbb{F}_q) = \left\{ P \in E(\overline{\mathbb{F}}_q) \;\middle|\; \pi(P) = P \right\}.$$

Proposition 4.11. *Let $E/\mathbb{F}_q$ be an elliptic curve with Frobenius endomorphism π and trace of Frobenius $t = \mathrm{tr}(\pi)$. Then the number of $\mathbb{F}_q$-rational points is given by*

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

Proof. From Definition 4.10, we deduce $E(\mathbb{F}_q) = \ker(\pi - 1)$, and from [18, Proposition 2.29] we know the endomorphism $\pi - 1$ is separable, allowing us to write $\#E(\mathbb{F}_q) =$

$\#\ker(\pi - 1) = \deg(\pi - 1)$, hence applying Lemma 4.2 and rearranging gives

$$\#E(\mathbb{F}_q) = \deg(\pi - 1) = 1 + \deg(\pi) - \mathrm{tr}(\pi) = q + 1 - t.$$

For more details on the relationship between the trace of Frobenius and the number of $\mathbb{F}_q$-rational points, see, for example, [12, 18, Theorem V.2.3.1, Ch 4.3]. □

Remark 4.12. *We note the identity* $(\pi - 1)\widehat{(\pi - 1)} = \deg(\pi - 1) = q + 1 - t$.

We now state a classical result on the upper bound of the number for rational points, for proof we refer to [18, Theorem 4.2].

Lemma 4.13 (Hasse's Theorem)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve with trace of Frobenius t. Then $|t| \leq 2\sqrt{q}$, or equivalently, $|(q + 1 - \#E(\mathbb{F}_q))| \leq 2\sqrt{q}$.*

Remark 4.14. *If $E/\mathbb{F}_q$ is ordinary, then the inequality in Lemma 4.13 is strict. Indeed, equality $|t| = 2\sqrt{q}$ would imply $p \mid t$, which is impossible by Lemma 4.9.*

4.3 Isogeny Classes

By Tate [15, Theorem 1], two elliptic curves over $\mathbb{F}_q$ are isogenous if and only if they have the same number of $\mathbb{F}_q$-rational points, which motivates the following classification.

Definition 4.15. *We define an* ***isogeny class*** *as the set of isomorphism classes of elliptic curves over $\mathbb{F}_q$ sharing the same trace of Frobenius t*

$$\mathcal{I}_t(\mathbb{F}_q) := \{E/\mathbb{F}_q \mid \#E(\mathbb{F}_q) = q + 1 - t\}/\sim,$$

where $E \sim E'$ if and only if $E \cong_{\mathbb{F}_q} E'$. Equivalently, all curves isogenous to one another over $\mathbb{F}_q$.

Remark 4.16. *By Lemma 4.9 we may classify an entire class $\mathcal{I}_t(\mathbb{F}_q)$ as ordinary or supersingular, since it only depends on t.*

It turns out that membership in $\mathcal{E}_j(\mathbb{F}_q)$ and $\mathcal{I}_t(\mathbb{F}_q)$ together identifies the isomorphism class of an ordinary elliptic curve over $\mathbb{F}_q$. In other words, distinct twists sharing the same j-invariant are distinguished precisely by the trace t. The following result will not be proven, but we state it here and refer to [4, Proposition 14.19] for proof.

Lemma 4.17. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve. Then $E \cong_{\mathbb{F}_q} E'$ if and only if $E' \in \mathcal{E}_{j(E)}(\mathbb{F}_q)$ and $E' \in \mathcal{I}_{t(E)}(\mathbb{F}_q)$.*

4.4 Number Field Embedding

By Proposition 4.5, Frobenius satisfies a monic quadratic polynomial $p_\pi(X) = X^2 - tX + q \in \mathbb{Z}[X]$, so π is an algebraic integer and generates the subring $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$. For ordinary curves, Remark 4.14 gives $t^2 < 4q$, so the discriminant $D_\pi = t^2 - 4q$ is negative and the induced number field $\mathbb{Z}[\pi] \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\pi)$ is imaginary quadratic. In fact, for $E/\mathbb{F}_q$ ordinary, it is a known result, see [18, Theorem 10.6], that $\mathrm{End}(E)$ is always an order in an imaginary quadratic field, and as we shall see in the next section, the arithmetic of these orders yield understanding into how Frobenius acts on ℓ-torsion.

For this, we first need to introduce some algebraic number theory, which we summarize in Definition 4.18 and refer to e.g. [8, 5, Chapter 13, Chapter 7.1] for proofs. We also refer to [18, 9, 16, Chapter 10, Chapter 4, Theorem 3.19] for its direct application to endomorphism rings of elliptic curves.

Definition 4.18. *An **imaginary quadratic field** is a number field of the form $K = \mathbb{Q}(\sqrt{-d})$ for some squarefree positive integer d. The ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\omega_K]$, where*

$$\omega_K = \begin{cases} (1+\sqrt{-d})/2 & \text{if } d \equiv 3 \pmod 4, \\ \sqrt{-d} & \text{if } d \equiv 1, 2 \pmod 4. \end{cases} \tag{3}$$

*This is a free $\mathbb{Z}$-module of rank 2, with $\mathbb{Z}$-basis $\{1, \omega_K\}$. An **order** in K is a subring $\mathcal{O} \subseteq \mathcal{O}_K$ of finite index. In the quadratic case, every order has the form*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K,$$

*where $f = [\mathcal{O}_K : \mathcal{O}]$ is called the **conductor**, and the order satisfies $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = K$. Denote by D_K the fundamental discriminant of the field K, where $D_K = -d$ if $d \equiv 3 \pmod 4$, and $D_K = -4d$ when $d \equiv 1, 2 \pmod 4$, then any order has discriminant $D = f^2 D_K$.*

From the definitions above, we make some remarks: we always have $f_K = [\mathcal{O}_K : \mathcal{O}_K] = 1$, and $\mathcal{O}_K$ is the maximal order. Moreover, we get $K = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ for some imaginary quadratric field K, but then $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subset K$, and we initially concluded $\mathbb{Z}[\pi] \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\pi)$, so we must have $K = \mathbb{Q}(\pi)$. Further, let $E/\mathbb{F}_q$ be ordinary and denote by $\mathcal{O}_E$ its order. Then we always have

$$\mathbb{Z}[\pi] \subseteq \mathcal{O}_E \subseteq \mathcal{O}_K,$$

with $f_E \mid f_\pi$, since by the tower law

$$f_\pi = [\mathcal{O}_K : \mathbb{Z}[\pi]] = [\mathcal{O}_K : \mathcal{O}_E][\mathcal{O}_E : \mathbb{Z}[\pi]] = f_E \cdot [\mathcal{O}_E : \mathbb{Z}[\pi]].$$

In fact, every divisor of f_π determines a conductor and hence an order, and each such

order corresponds to at least one curve. The following is due to Waterhouse [19, Theorem 4.2].

Lemma 4.19. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with Frobenius endomorphism π. Then every order $\mathcal{O}$ satisfying $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ corresponds to the endomorphism ring of some curve in the isogeny class $\mathcal{I}_t(\mathbb{F}_q)$.*

Using the $\mathbb{Z}$-basis of $\mathcal{O}_K$ as in Definition 4.18, we can write $\pi = a_\pi + f_\pi \omega_K$ with $a_\pi \in \mathbb{Z}$. Rearranging this, we recover the basis element $\omega_K = \frac{\pi - a_\pi}{f_\pi}$ which is another algebraic integer, in particular, must correspond to an endomorphism for some curve in the maximal order by Lemma 4.19, hence we can use Definition 4.1 to get

$$\mathrm{Tr}(\omega_K) = \frac{t - 2a_\pi}{f_\pi} \in \mathbb{Z}, \qquad \mathrm{N}(\omega_K) = \frac{a_\pi^2 - t a_\pi + q}{f_\pi^2} \in \mathbb{Z}. \tag{4}$$

We deduce the following congruences.

Proposition 4.20. *Let f_π be the conductor of $\mathbb{Z}[\pi]$ in $\mathcal{O}_K$, and write $\pi = a_\pi + f_\pi \omega_K$ in the $\mathbb{Z}$-basis $\{1, \omega_K\}$ of $\mathcal{O}_K$. Then $a_\pi \in \mathbb{Z}$ and satisfies*

$$t \equiv 2a_\pi \pmod{f_\pi} \quad \textit{and} \quad q \equiv a_\pi^2 \pmod{f_\pi}.$$

Proof. Equation 4 immediately yields $t \equiv 2a_\pi \pmod{f_\pi}$, and $q \equiv t a_\pi - a_\pi^2 \pmod{f_\pi^2}$, which also holds modulo f_π, and hence $q \equiv 2a_\pi^2 - a_\pi^2 = a_\pi^2 \pmod{f_\pi}$. □

Remark 4.21. *To simplify notation, we write αR for the ideal generated by (α) in the ring R. Thus, if $(a - b) \subseteq (\alpha) \subseteq R$, then $a \equiv b \mod \alpha R$.*

Corollary 4.22. *By Proposition 4.20, it follows from the definition of $t := \pi + \hat{\pi}$ and $q := \pi\hat{\pi}$ that the Frobenius endomorphism and its dual are always congruent to the same integer a_π modulo $f_\pi \mathcal{O}_K$.*

Quadratic Twists

Proposition 4.23. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with Frobenius π. Then the quadratic twist E' of E has Frobenius $\pi' = -\pi$.*

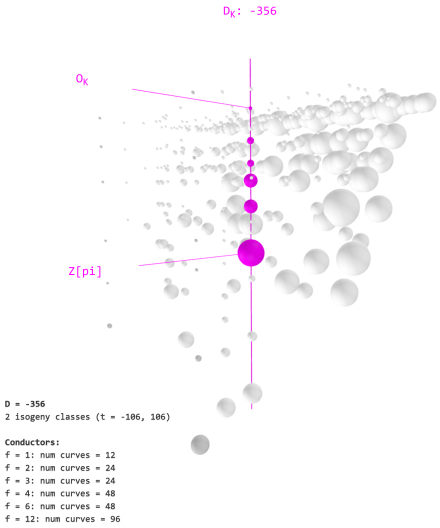
Proof. Since E' is the quadratic twist of E, the curves become isomorphic over $\mathbb{F}_{q^2}$. For ordinary curves, the endomorphism ring depends only on the j-invariant, so we may identify $\mathrm{End}(E) \cong \mathrm{End}(E') \cong \mathcal{O}_E$. In particular, we may view the Frobenius endomorphisms π and π' as algebraic integers in $\mathcal{O}_E$. Since E and E' are isomorphic over $\mathbb{F}_{q^2}$, their q^2-Frobenius endomorphisms agree, so $\pi^2 = (\pi')^2$, and we must have $\pi' = \pm\pi$. Now, E and E' share the same j-invariant and hence both belong to $\mathcal{E}_{j(E)}(\mathbb{F}_q)$.

If $\pi' = \pi$, their traces of Frobenius would agree and they would also belong to the same isogeny class $\mathcal{I}_{t(E)}(\mathbb{F}_q)$, which by Lemma 4.17 would imply $E \cong_{\mathbb{F}_q} E'$, contradicting the assumption that they are non-isomorphic over $\mathbb{F}_q$. We conclude $\pi' \neq \pi$, yielding $\pi' = -\pi$. □

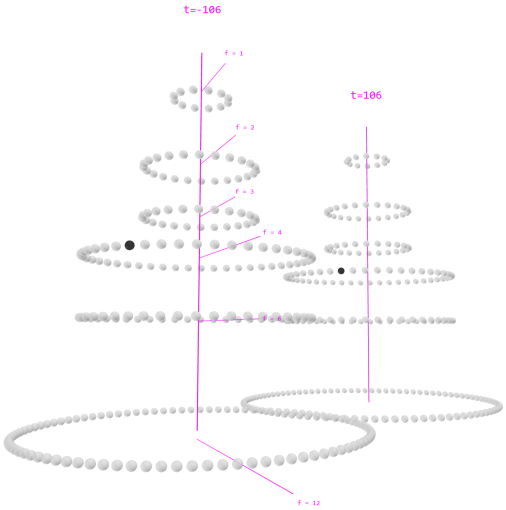
Corollary 4.24. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with trace t. Then the quadratic twist E' of E has trace $t' = -t$.*

Proof. By Proposition 4.23, we have $\mathrm{tr}(\pi') = \mathrm{tr}(-\pi) = -(\pi + \hat{\pi}) = -t$. □

We summarize our new invariants. Let $E/\mathbb{F}_q$ be ordinary with trace t, then the pair (D_K, f_π) is an invariant shared by all curves in $\mathcal{I}_{\pm t}(\mathbb{F}_q)$. Moreover, by Corollary 4.7 we deduce that the pair (D_K, f_E) must be constant on $\mathcal{E}_j(\mathbb{F}_q)$. In particular, the ambient number field, and hence the fundamental discriminant D_K, is an invariant shared by $\mathcal{I}_{\pm t}(\mathbb{F}_q)$ and $\mathcal{E}_j(\mathbb{F}_q)$ and does not change over any extension. The following visualizations are made based on data generated by our classification algorithms, see [14]. They illustrate the distribution of number fields over $\mathbb{F}_q$, as well as how curves can be partitioned by (j, t) within such fields.



(a) White dots represents all orders occurring as endomorphism rings over $\mathbb{F}_{5^6}$, displayed by (D_K, f, D_π). Pink vertical line shows a single number field, $D_K = -356$, and the suborders between $\mathcal{O}_K$ and $\mathbb{Z}[\pi]$.



(b) Field with $D_K = -356$ and $f_\pi = 12$. White dots represents distinct curves in $\mathcal{I}_{\pm 106}(\mathbb{F}_{5^6})$ displayed on different conductor levels. Black dots represent two quadratic twists in $\mathcal{E}_j(\mathbb{F}_{5^6})$, confirming shared invariant $f_E = f'_E = 4$ but different isogeny class, illustrating the twist symmetry.

Special j-Invariants yield Special Number Fields

By Lemma 4.8, ordinary curves with $j(E) = 1728$ have $\mathrm{Aut}(E) \cong \mu_4$, while those with $j(E) = 0$ have $\mathrm{Aut}(E) \cong \mu_6$. Let i be a primitive fourth root of unity and ζ a

primitive cube root of unity. Then $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta]$ must occur as subrings of $\mathcal{O}_E$, since these are the only imaginary quadratic integer rings with more units than $\mu_2 = \{\pm 1\}$ [5, Chapter 7.1], giving the following inclusions

$$\mathbb{Z}[i] \subseteq \mathcal{O}_E \quad \text{if } j = 1728, \qquad \mathbb{Z}[\zeta] \subseteq \mathcal{O}_E \quad \text{if } j = 0.$$

Lemma 4.25. *Let $E/\mathbb{F}_q$ be ordinary with $j(E) \in \{0, 1728\}$. Then $\mathcal{O}_E = \mathcal{O}_K$.*

Proof. Comparing discriminants, we see that $D_K^i = D_i = -4$ and $D_K^\zeta = D_\zeta = -3$. Equivalently, $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta]$ both have conductor 1, and therefore they are maximal orders. The result then follows from the stated inclusions above. □

5 ARITHMETIC APPROACH TO ℓ-TORSION SUBGROUPS

In this section, our goal is to determine how much of the ℓ-torsion of an elliptic curve is $\mathbb{F}_q$-rational. We study how the size of this subgroup depends on our classification parameters, and derive necessary conditions on these for algorithmic efficiency. For this approach, we must assume that E is ordinary and that $\ell \neq \mathrm{char}(\mathbb{F}_q)$ is prime. For ordinary curves there is no need for distinction between $\mathbb{F}_q$-rational endomorphism rings so we simply write $\mathrm{End}(E)$ in this section.

We begin by examining the full ℓ-torsion subgroup over $\overline{\mathbb{F}}_q$, viewing $E(\overline{\mathbb{F}}_q)$ as a module over the endomorphism ring, the ℓ-torsion subgroup of E, denoted by $E[\ell]$, consists of all points in the algebraic closure $\overline{\mathbb{F}}_q$ that are annihilated by $[\ell]$, and we write

$$E[\ell] = \{P \in E(\overline{\mathbb{F}}_q) \mid [\ell]P = \infty\} = \ker(\ell).$$

Since $[\ell]$ is separable, we have $\deg(\ell) = \#\ker(\ell) = \ell^2$, so the ℓ-torsion subgroup $E[\ell] \subseteq E(\overline{\mathbb{F}}_q)$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$.

Proposition 5.1. *Let $E/\mathbb{F}_q$ be ordinary and let $\ell \neq \mathrm{char}(\mathbb{F}_q)$ be prime. Then $E[\ell]$ is a 2-dimensional $\mathbb{F}_\ell$-vector space, and $E[\ell](\mathbb{F}_q)$ is its Frobenius-fixed subspace. Define*

$$\mathrm{rank}_\ell(E/\mathbb{F}_q) := \dim_{\mathbb{F}_\ell} E[\ell](\mathbb{F}_q) \in \{0, 1, 2\}.$$

The number of cyclic subgroups of order ℓ contained in $E[\ell](\mathbb{F}_q)$ is 0, 1, or $\ell + 1$ corresponding to $\mathrm{rank}_\ell(E/\mathbb{F}_q) = 0$, 1, or 2, respectively.

5.1 Probing Ideals In The Endomorphism Ring

Throughout, let $E/\mathbb{F}_q$ be ordinary, let π denote the Frobenius endomorphism and let $t := \mathrm{Tr}(\pi)$ denote the trace.

Definition 5.2. *We define the $\mathbb{F}_q$-rational ℓ-torsion subgroup as*

$$E[\ell](\mathbb{F}_q) = E(\mathbb{F}_q) \cap E[\ell] = \ker(\pi - 1) \cap \ker(\ell).$$

The intersection of these ideals thus governs the ℓ-rank, and we begin by stating criteria based on ideal containment. We first need the following lemma. For proof see [12, Corollary 4.11].

Lemma 5.3. *Let $\phi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ be nonconstant isogenies, with ϕ separable. If $\ker\phi \subseteq \ker\psi$, then there exists a unique isogeny $\lambda : E_2 \to E_3$ such that*

$$\psi = \lambda \circ \phi$$

Theorem 5.4. *The following is an equivalent criterion for full ℓ-rank on E*

$$(\pi - 1) \subseteq (\ell) \text{ in } \mathrm{End}(E) \quad \iff \quad E[\ell] \subseteq E(\mathbb{F}_q).$$

Proof. Assume $(\pi - 1) \subseteq (\ell)$ in $\mathrm{End}(E)$, then we can write $\pi - 1 = \alpha \circ [\ell]$ for some $\alpha \in \mathrm{End}(E)$, and it follows that for any $P \in \ker(\ell)$, we have $P \in \ker(\pi - 1)$, hence $E[\ell] \subseteq E(\mathbb{F}_q)$. Conversely, suppose $E[\ell] \subseteq E(\mathbb{F}_q)$, and so $\ker(\ell) \subseteq \ker(\pi - 1)$. Since $\ell \neq \mathrm{char}(\mathbb{F}_q)$, we know ℓ is separable, and we can use Corollary 5.3 which guarantees the existence of a unique isogeny λ such that $\pi - 1 = \lambda \circ [\ell]$, and hence $(\pi - 1) \subseteq (\ell)$ in $\mathrm{End}(E)$. □

Corollary 5.5. *We restate the equivalence in Theorem 5.4 as*

$$\pi \equiv 1 \mod \ell\,\mathrm{End}(E) \quad \iff \quad \mathrm{rank}_\ell(E/\mathbb{F}_q) = 2.$$

Proposition 5.6. *The following is an equivalent criterion for nonzero ℓ-rank on E*

$$(\pi - 1)(\hat{\pi} - 1) \subseteq (\ell) \text{ in } \mathrm{End}(E) \quad \iff \quad E[\ell] \cap E(\mathbb{F}_q) \neq \{0\}.$$

Proof. By Remark 4.12 and Proposition 4.11, the first statement is equivalent to $\ell \mid (\pi - 1)(\hat{\pi} - 1) = \#E(\mathbb{F}_q)$. The second statement $E[\ell] \cap E(\mathbb{F}_q) \neq \{0\}$ means that $E(\mathbb{F}_q)$ contains a nontrivial point of order ℓ, but since $E(\mathbb{F}_q)$ is a finite abelian group, this is equivalent to ℓ dividing its order, as claimed. □

Corollary 5.7. $\ell \mid q + 1 - t \implies (\pi - 1)(\pi - q) \equiv 0 \mod \ell\,\mathrm{End}(E)$.

Proof. If $\ell \mid q+1-t$, then $q+1 \equiv \pi+\hat{\pi} \mod \ell\,\mathrm{End}(E)$ so rearranging gives $\hat{\pi}-1 \equiv q-\pi$

mod $\ell \operatorname{End}(E)$. From assumption, we also have $\ell \mid (\pi-1)(\hat{\pi}-1)$, hence $(\pi-1)(q-\pi) \equiv 0$ mod $\ell \operatorname{End}(E)$ and $(1-)(\pi-1)(\pi-q) \equiv 0 \equiv (\pi-1)(\pi-q) \mod \ell \operatorname{End}(E)$. □

By Corollary 5.5, we need $\pi \equiv 1 \mod \ell \operatorname{End}(E)$ for full rank, but since integers are self-dual, we also get $\hat{\pi} \equiv 1 \mod \ell \operatorname{End}(E)$, yielding $q \equiv \pi\hat{\pi} \equiv 1 \pmod{\ell}$ as a necessary criterion for full rank. We summarize our initial results as follows.

Proposition 5.8. *The ℓ-rank of E is governed by q and t as*

1. $\ell \nmid q+1-t \iff \operatorname{rank}_\ell(E/\mathbb{F}_q) = 0$.
2. $\ell \mid q+1-t \implies (\pi-1)(\pi-q) \equiv 0 \mod \ell \operatorname{End}(E)$ *and either*
   - (a) $\ell \nmid q-1$ *then* $\operatorname{rank}_\ell(E/\mathbb{F}_q) = 1$,
   - (b) $\ell \mid q-1$ *then* $(\pi-1)^2 \equiv 0 \mod \ell \operatorname{End}(E)$, *and either*
     - i. $\pi \not\equiv 1 \mod \ell \operatorname{End}(E)$ *then* $\operatorname{rank}_\ell(E/\mathbb{F}_q) = 1$,
     - ii. $\pi \equiv 1 \mod \ell \operatorname{End}(E)$ *then* $\operatorname{rank}_\ell(E/\mathbb{F}_q) = 2$.

From q and t alone, we cannot distinguish between cases 2.b.i and 2.b.ii. For that, we must examine the endomorphism ring and the isogeny class of E more closely. However, we conclude this first part with the following necessary criterion on q for full ℓ-rank, applying uniformly to all curves over $\mathbb{F}_q$.

Corollary 5.9. *If $\ell \nmid (q-1)$, then $\operatorname{rank}_\ell(E/\mathbb{F}_q) < 2$ for all $E \in \mathcal{E}(\mathbb{F}_q)$.*

5.2 The ℓ-adic Height of Number Field Order

Recall that the endomorphism ring of a curve can be described as an order $\mathcal{O}_E$ in the imaginary quadratic field $K = \mathbb{Q}(\pi)$, and where all curves in $\mathcal{I}_t(\mathbb{F}_q)$ satisfy $\mathbb{Z}[\pi] \subseteq \mathcal{O}_E \subseteq \mathcal{O}_K$. By Proposition 5.4, we want π to act as the identity modulo $\ell\mathcal{O}_E$. A necessary condition is thus for π to act as an integer modulo $\ell\mathcal{O}_K$. By Corollary 4.22, we know this is always true modulo $f_\pi\mathcal{O}_K$, and will now deduce when it also holds modulo $\ell\mathcal{O}_K$.

Lemma 5.10. *Let f_π be the conductor of $\mathbb{Z}[\pi]$ in $\mathcal{O}_K$. Then*

$$\ell \mid f_\pi \iff \pi \equiv n \mod \ell\mathcal{O}_K \text{ for some } n \in \mathbb{Z}.$$

Proof. Assume $\ell \mid f_\pi$. Then the congruences in Proposition 4.20 also holds modulo $\ell\mathcal{O}_K$ and we conclude $\pi \equiv a_\pi$ with $a_\pi \in \mathbb{Z}$. Conversely, if $\pi \equiv n \mod \ell\mathcal{O}_K$, then using the $\mathbb{Z}$-basis $\{1, \omega_K\}$ for $\mathcal{O}_K$ from Proposition 4.20, we may write

$$\pi = a_\pi + f_\pi\omega_K = n + \ell(x + y\omega_K) = (n + x\ell) + y\ell\omega_K$$

for some $x, y \in \mathbb{Z}$. Comparing coefficients for ω_K yields $\ell \mid f_\pi$. □

Corollary 5.11. *Let a_π be as in Proposition 4.20. If $\pi \equiv n \mod \ell\mathcal{O}_K$ for some $n \in \mathbb{Z}$, then $n \equiv a_\pi \mod \ell$.*

Proof. From the converse proof of Lemma 5.10, comparing the integer coefficients yields $a_\pi \equiv n \mod \ell$. □

We conclude that $\ell \mid f_\pi$ is a necessary condition for π to act as an integer modulo $\ell\mathcal{O}_K$, in which case we have the congruences $\pi \equiv \hat{\pi} \equiv a_\pi$ and $q = \pi\hat{\pi} \equiv a_\pi^2$. We now narrow down when this integer can take the identity values.

Proposition 5.12. *Let f_π be the conductor of $\mathbb{Z}[\pi]$ in $\mathcal{O}_K$. Then*

$$\ell \mid f_\pi \text{ and } \ell \mid q-1 \iff \pi \equiv \pm 1 \mod \ell\mathcal{O}_K.$$

Proof. By Lemma 5.10 and Corollary 5.11, the condition $\ell \mid f_\pi$ is equivalent to $\pi \equiv \hat{\pi} \equiv a_\pi \mod \ell\mathcal{O}_K$ for some integer a_π. If in addition $\ell \mid q-1$, then $q = a_\pi^2 \equiv 1 \mod \ell$, so $a_\pi \equiv \pm 1 \mod \ell$, and therefore the full statement is equivalent to $\pi \equiv \pm 1 \mod \ell\mathcal{O}_K$. □

Corollary 5.13. *If $\ell \nmid f_\pi$, then $\operatorname{rank}_\ell(E/\mathbb{F}_q) < 2$ for all $E \in \mathcal{I}_{\pm t}(\mathbb{F}_q)$.*

Proof. If $\pi \not\equiv 1 \mod \ell\mathcal{O}_K$, then no curve with trace t can have full ℓ-rank. If also $\pi \not\equiv -1 \mod \ell\mathcal{O}_K$, then by Proposition 4.23 the Frobenius endomorphism of a quadratic twist satisfies $\pi' = -\pi$, so $\pi' \not\equiv 1 \mod \ell\mathcal{O}_K$ as well. Hence no curve in $\mathcal{I}_{-t}(\mathbb{F}_q)$ can have full ℓ-rank either. □

We now show that replacing the condition $\ell \mid q-1$ with $\ell \mid q+1-t$ selects the isogeny class in which full rank occurs.

Proposition 5.14. *Let f_π be the conductor of $\mathbb{Z}[\pi]$ in $\mathcal{O}_K$. Then*

$$\ell \mid f_\pi \text{ and } \ell \mid q+1-t \iff \pi \equiv 1 \mod \ell\mathcal{O}_K.$$

Proof. Again, if $\ell \mid f_\pi$, then π acts as the integer a_π modulo $\ell\mathcal{O}_K$. Adding the condition $\ell \mid q+1-t$ gives $\ell \mid a_\pi^2 + 1 - 2a_\pi = (a_\pi - 1)^2$, and since ℓ is prime, this implies $a_\pi \equiv 1 \mod \ell$. Therefore $\pi \equiv 1 \mod \ell\mathcal{O}_K$. □

Corollary 5.15. *If $\ell \mid f_\pi$ and $\ell \mid q+1-t$ then there exists $E \in \mathcal{I}_t(\mathbb{F}_q)$ such that $\operatorname{rank}_\ell(E/\mathbb{F}_q) = 2$.*

Proof. From Proposition 4.19 there exists at least one curve with $\mathcal{O}_E = \mathcal{O}_K$. □

Having established necessary criteria on f_π governing whether full ℓ-rank is possible in an isogeny class, we actually have all we need to determine the ℓ-rank for curves with

j-invariant 0 or 1728.

Proposition 5.16. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with $j(E) \in \{0, 1728\}$. Then*

$$\operatorname{rank}_\ell(E/\mathbb{F}_q) = \begin{cases} 0 & \text{if } \ell \nmid \#E(\mathbb{F}_q), \\ 1 & \text{if } \ell \mid \#E(\mathbb{F}_q), \text{ and } \ell \nmid f_\pi \\ 2 & \text{if } \ell \mid \#E(\mathbb{F}_q), \text{ and } \ell \mid f_\pi. \end{cases}$$

Proof. First two cases follows directly from Proposition 5.8 and Corollary 5.13. Full rank follows from Proposition 5.14 as $\mathcal{O}_E = \mathcal{O}_K$ by Lemma 4.25. □

For all other ordinary curves, the ℓ-rank is determined by how $\mathcal{O}_E$ sits between $\mathbb{Z}[\pi]$ and $\mathcal{O}_K$, and in particular by the ℓ-divisibility of f_E compared to f_π. We first need the following definition.

Definition 5.17. *The ℓ-adic valuation $v_\ell(n)$ of an integer n is the largest integer k such that $\ell^k \mid n$.*

Theorem 5.18. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve. Let f_π be the conductor of the Frobenius endomorphism π, and let f_E be the conductor of the endomorphism ring $\mathcal{O}_E$. Then the following are equivalent*

i $\ell \mid q + 1 - t$, *and* $v_\ell(f_E) < v_\ell(f_\pi)$,
ii $E[\ell] \subset E(\mathbb{F}_q)$.

Proof. By Proposition 4.20 we are allowed to write $\pi = a_\pi + f_\pi \omega_K$ as an element of $\mathcal{O}_K$. By integer factorization, and since $f_E \mid f_\pi$, we can write $f_\pi = n\ell^k$ where $\gcd(\ell, n) = 1$ with $0 \leq k$, and $f_E = m\ell^e$ with $\gcd(\ell, m) = 1$, $m \mid n$ and $0 \leq e \leq k$. Now note that $v_\ell(f_E) < v_\ell(f_\pi)$ implies $\ell \mid f_\pi$ so by Proposition 5.14 we have $\ell \mid (a_\pi - 1)$, and (i) is equivalent to

$$\pi - 1 = a_\pi - 1 + f_\pi \omega_K \in \ell\mathbb{Z} + n\ell^k \omega_K \in \ell(\mathbb{Z} + n\ell^{k-1}\omega_K) =: \ell\mathcal{O}$$

for some order $\mathcal{O}$ with conductor $n\ell^{k-1}$. By assumption, $e < k$, hence $m\ell^e = f_E \mid n\ell^{k-1}$ since $m \mid n$, and so $\mathcal{O} \subseteq \mathcal{O}_E$, and (i) is equivalent to $\pi - 1 \in \ell\mathcal{O}_E$. By Theorem 5.4, this is again equivalent to (ii). □

It now remains to deduce how we can determine the relationship between the ℓ-adic valuations of f_E and f_π for curves in isogeny classes, as this is not trivially given by our classification so far. For this, we shall exploit the structure of ℓ-isogenies.

5.3 Frobenius Stable ℓ-Isogenies

Definition 5.19. *Let $E, E' \in \mathcal{I}_t(\mathbb{F}_q)$. An ℓ-isogeny $\phi_\ell : E \to E'$ satisfies*

$$\deg(\phi_\ell) = \ell \qquad \textit{and} \qquad \ker(\phi_\ell) \subseteq E[\ell],$$

thus, kernels of ℓ-isogenies are precisely the cyclic subgroups of $E[\ell]$.

The Modular Polynomial

The **classical modular polynomial** $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$ parametrizes these isogenies between ordinary elliptic curves, and can be written over $\overline{\mathbb{F}}_q$ as [18, Theorem 12.5]

$$\Phi_\ell(j(E), Y) = \prod_{i=1}^{\ell+1} (Y - j(E/\mathcal{K}_i)),$$

where $\mathcal{K}_i$ are the kernels of the distinct ℓ-isogenies from E, so the roots are precisely the j-invariants of the codomains. Over $\mathbb{F}_q$, the roots of $\Phi_\ell(j(E), Y)$ correspond to those ℓ-isogenies that are defined over $\mathbb{F}_q$. Equivalently, they reflect how many order-ℓ subgroups of $E[\ell]$ are Frobenius-stable. This does not yet imply the kernel is pointwise fixed by Frobenius, and hence contained in $E[\ell](\mathbb{F}_q)$ as defined in Proposition 5.1. For this, we also need conditions on q and t as described in Proposition 5.8.

The key point for us is that factoring the modular polynomial actually reveals the ℓ-adic position of the endomorphism order, which allows us to reconstruct f_E. Efficient algorithms for extracting this information were initiated by Kohel [9] and further developed in works such as [2, 13, 7, 10]. We shall now give a brief overview of the theory behind these algorithms, as it aligns directly with our arithmetic approach to determining the ℓ-rank.

Isogeny Volcanoes

An isogeny class can be organized into an isogeny graph whose vertices are j-invariants and whose edges are ℓ-isogenies. These graphs have a particular structure, named **isogeny volcanos** by Fouquet and Morain [6]. The vertices are arranged by ℓ-adic height into levels, where edges are classified by their direction: an edge going from E to E' is horizontal if $f_{E'} = f_E$, descending if $f_{E'} = \ell f_E$, and ascending if $f_{E'} = f_E/\ell$. Formally, we have the following definition.

Definition 5.20. *The total height of an ℓ-volcano is $v_\ell(f_\pi)$. The height of a curve is*

$$h_\ell(E) := v_\ell(f_\pi) - v_\ell(f_E),$$

*where curves with $h_\ell(E) = 0$ lie on the **floor**, and those with $h_\ell(E) = v_\ell(f_\pi)$ lie on the **surface**.*

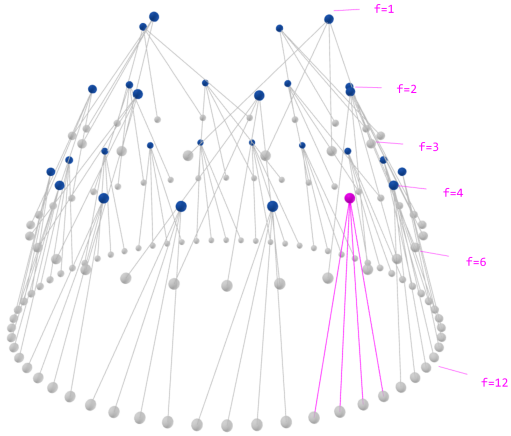
By [13, Theorem 7], if the volcano has nonzero height, then vertices on the floor have exactly one ascending edge, whereas vertices lying strictly above the floor have total degree $\ell + 1$. Horizontal edges occur only on the surface, and any vertex has at most 2 such edges. In other words, the local information given by the number of edges can be used to orient a global position in the graph. This is precisely what the existing algorithms for computing f_E exploit: starting at a curve E, one follows outgoing edges until the floor is located, and from the number of levels traversed one recovers the exact height $h_\ell(E)$. Repeating this for each prime divisor of f_π then reconstructs f_E.

5.4 Visualizing Isogeny Volcanoes

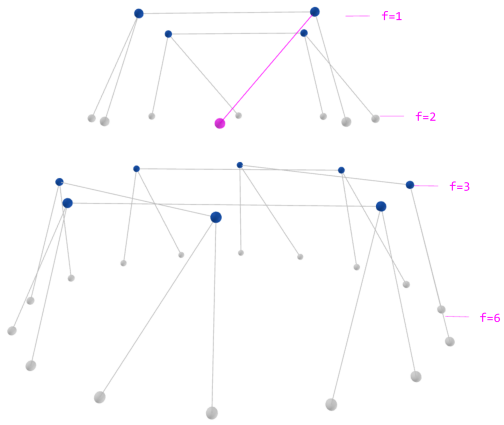
For a given isogeny class $\mathcal{I}_t(\mathbb{F}_q)$, we construct a graph whose vertices are curves organized by conductor index in the tower between $\mathbb{Z}[\pi]$ and $\mathcal{O}_K$. By Lemma 4.17, distinct curves in $E \in \mathcal{I}_t(\mathbb{F}_q)$ may be identified by j-invariant, so we can use the algorithm of [10] (as implemented in [SageMath]) to compute f_E and then assign each curve a unique vertex v_j at corresponding conductor level. For each prime $\ell \mid q + 1 - t$, edges (j, j') are then added for every root j' of $\Phi_\ell(j(E), Y)$ over $\mathbb{F}_q$. Recall that these edges corresponds to the number of Frobenius-stable cyclic subgroups of $E[\ell]$, while now, by construction, we also know that $\ell \mid q+1-t$, hence all vertices are forced to be in case 2 of Proposition 5.8. The degree of a vertex, by standard linear algebra, now directly distinguishes the remaining subcases.

Degree	mod ℓ End(E)	Case	rank$_\ell$
2	$(\pi - 1)(\pi - q) \equiv 0$	2.a	1
1	$(\pi - 1)^2 \equiv 0$	2.b.i	1
$\ell + 1$	$(\pi - 1) \equiv 0$	2.b.ii	2

As we organize our graph by the true conductor level rather than the theoretical volcano levels, we instead indicate the ℓ-adic volcano structure by a color scheme: vertices lying strictly above the ℓ-adic floor are colored blue, and those on the floor are colored white.



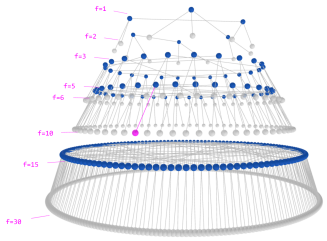
(a) 3-volcano of height 1 in isogeny class $\mathcal{I}_{98}(\mathbb{F}_{11^4})$ with $f_\pi = 12$. Highlighted curve with $f_E = 4$ yields $h_\ell(E) > 0$ and $\ell + 1$ edges



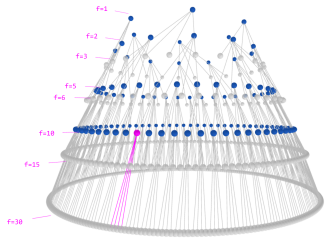
(b) 2-volcano of height 1 in isogeny class $\mathcal{I}_{-22}(\mathbb{F}_{5^4})$ with $f_\pi = 6$. Highlighted curve with $f_E = 2$ yields $h_\ell(E) = 0$ and only one edge

Figure 2: Isogeny Volcanoes

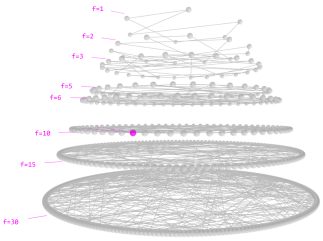
Counting the edges in Figures 2, we see that indeed, a white vertex on the floor has exactly one ascending edge, while a blue vertex above the floor has $\ell + 1$ edges. Importantly, the edge count confirms Theorem 5.18, which restated in volcano language says: for an ℓ-volcano corresponding to an isogeny class satisfying $\ell \mid q + 1 - t$, full ℓ-rank occurs if and only if the curve lies strictly above the floor, i.e. $h_\ell(E) > 0$.



(a) 2-volcano of height 1. Curves with $f_E \in \{2, 6, 10, 30\}$ lies on the floor, and curves with $f_E \in \{1, 3, 5, 15\}$ on surface. Highlighted j-invariant with $f_E = 10$ has one ascending edge.



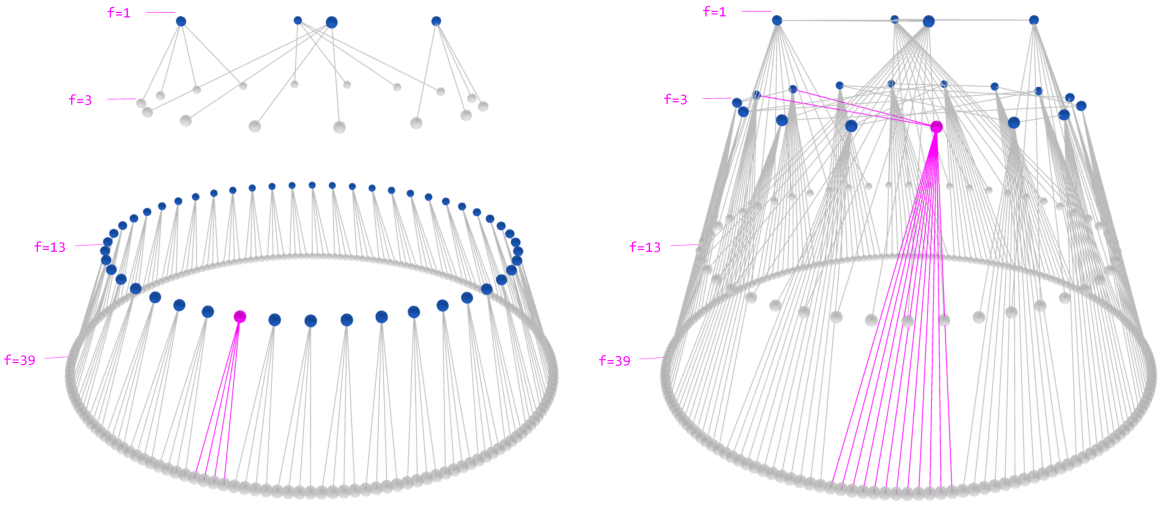
(b) 3-volcano of height 1. Curves with $f_E \in \{3, 6, 15, 30\}$ lies on the floor, and curves with $f_E \in \{1, 2, 5, 10\}$ on surface. Highlighted j-invariant with $f_E = 10$ has $3 + 1$ descending edges.



(c) 11-volcano of height 0, floor and surface coincide, and $h_\ell(E) = 0$ for all curves. Highlighted j-invariant with $f_E = 10$, has two horizontal edges and no vertical edges.

Figure 3: Fixed isogeny class $\mathcal{I}_{-234}(\mathbb{F}_{117649})$ in number field with discriminant $D_K = -472$ and $f_\pi = 30$ showing different ℓ-volcano structures. Highlighted in pink one selected curve with $f_E = 10$.

We note that for different primes, the same curve may lie on the floor for one volcano and on the surface for another. We also note that the indexing of the volcano levels and the conductor levels does not follow the same hierarchy: white dots on the floor may appear above blue dots on the surface, precisely because the volcano height is relative to ℓ. Further, Figure 3c recovers the case $\ell \nmid f_\pi$, which we now in this language refer to as the volcano having no height, the floor coincides with the surface, and all edges are horizontal. In particular, the degree is at most 2 for any vertex, hence no curve in this isogeny class can have full ℓ-rank, in agreement with Corollary 5.13.



(a) 3-volcano. Highlighted curve with $f_E = 13$ on the surface has 4 descending edges and no horizontal edges.

(b) 13-volcano. Highlighted curve with $f_E = 3$ on the surface has 12 descending edges and 2 horizontal, yielding in total 14 edges.

Figure 4: Isogeny Volcanoes in $\mathcal{I}_{-1081}(\mathbb{F}_{5^8})$ with $D_K = -259$ and $f_\pi = 39$.

5.5 Compute Rank of $E[\ell](\mathbb{F}_q)$

As we have now seen, for the purpose of determining the ℓ-rank it suffices to decide whether E lies on the ℓ-adic floor or strictly above it. This can be done with a single evaluation of Φ_ℓ, namely by checking whether $\Phi_\ell(j(E), Y)$ has $\ell+1$ roots over $\mathbb{F}_q$ (equivalently, strictly more than 2). Still, motivated by the algorithm used to compute the full conductor, we introduce a reduced variant that avoids the overhead of determining the exact height of the order and instead records more binary information in the *prime conductor* f_E^*. Formally, let

$$h_\ell^*(E) = \begin{cases} 1 & \text{if } \Phi_\ell(j(E), Y) \text{ has } \ell+1 \text{ roots over } \mathbb{F}_q \\ 0 & \text{otherwise,} \end{cases} \tag{5}$$

then define

$$f_E^* = \prod_{\ell \mid f_\pi} \ell^{v_\ell(f_\pi)(1-h_\ell^*(E))}. \tag{6}$$

We see that by this construction, $h_\ell^*(E) > 0$ precisely when $h_\ell(E) > 0$.

5.5.1 Algorithm

We suggest to precompute the prime conductor as an invariant shared by a curve and its quadratic twist, and only later resolve the twist ambiguity via the trace-dependent condition. Concretely, for curves with $j(E) \in \{0, 1728\}$, we set $f_E^* = 1$. For all other curves in $\mathcal{E}_j(\mathbb{F}_q)$, we compute f_E^* by factoring Φ_ℓ only for primes ℓ that satisfy the necessary conditions of Proposition 5.12. This construction accounts for the possibility that either the curve or its quadratic twist lies in an isogeny class admitting full rank. In every other case, when these conditions fail, we simply set $f_E^* = 1$ for all curves in $\mathcal{E}_j(\mathbb{F}_q)$.

Having computed the prime conductor in this way, the correctness of the ℓ-rank algorithm below follows directly from Theorem 5.18 and the construction of f_E^*.

Algorithm 2 Compute the prime conductor f_E^* of an ordinary elliptic curve $E/\mathbb{F}_q$

function AboveFloor(E, ℓ)
  $\Phi(Y) \leftarrow \Phi_\ell\big(j(E), Y\big) \in \mathbb{F}_q[Y]$
  $r \leftarrow \#\{\text{roots of } \Phi(Y) \text{ in } \mathbb{F}_q\}$ ▷ counted with multiplicity
  return $r > 2$
end function
function PrimeConductor(E, f_π)
  if $j(E) \in \{0, 1728\}$ **then** ▷ always at maximal order, so $f_E^* = 1$
    return 1
  end if
  $f_E^* \leftarrow 1$
  for each prime power $\ell^e \parallel f_\pi$ **do**
    if $\ell \nmid q - 1$ **then**
      $f_E^* \leftarrow f_E^* \cdot \ell^e$ ▷ Split case, only horizontal, floor equals surface
    else
      $h \leftarrow e$ if AboveFloor(E, ℓ) else 0
      $f_E^* \leftarrow f_E^* \cdot \ell^{e-h}$
    end if
  end for
  return f_E^*
end function

Algorithm 3 Compute ℓ-torsion rank of an ordinary elliptic curve $E/\mathbb{F}_q$, $\ell \neq \operatorname{char} \mathbb{F}_q$.

function EllTorsionRank(E, q, ℓ)
  let $t \leftarrow E.t$ ▷ precomputed by e.g Schoof's algorithm in SageMath
  let $f_E^* \leftarrow E.f_E^*$ ▷ precomputed by Algorithm 2
  let $f_\pi \leftarrow \sqrt{(t^2 - 4q)/D_K}$ ▷ see Definition 4.18
  if $\ell \nmid q + 1 - t$ **then**
    return 0
  else
    return 2 if $\ell \mid f_\pi / f_E^*$ else 1
  end if
end function

Remark 5.21. *The design of this algorithm separates computation into layers based on our classification parameters, aiming at flexibility and efficiency when varying these. The trace t is computed once per j and q, and the modular polynomial $\Phi_\ell(X, Y)$ can be precomputed and cached once per ℓ [3, Theorem 1]. Then only for (q, t, ℓ) satisfying the conditions as stated in Corollary 5.15, the cost reduces to specializing $\Phi_\ell(j, Y)$, at $O(\ell^2)$ [3, Lemma 4.5], and finding roots over $\mathbb{F}_q$, at $O(\ell \log q)$ [17, Corollary 14.16], giving a total cost of $O(\ell^2 + \ell \log q)$ to compute the prime conductor per such tuple. This separation of information by parameter makes the algorithm flexible when varying ℓ, and also admits further optimization if one fixes a base field and varies n for q^n, as the prime conductor could be cached for j invariants over lower extensions. By contrast, naive point finding would yield $O(\ell^3 \log q)$ [18, Theorem 3.6] for all curves in $\mathcal{E}(\mathbb{F}_q)$, with no pre-filtering or shared computations.*

6 CLASSIFICATION OF ℓ-TORSION POINTS

Having developed theory to compute the size of prime torsion subgroups, we now look deeper into the internal structure of such subgroups, aiming to classify individual points up to $\mathbb{F}_q$-isomorphism. That is, we wish to determine unique pairs (E, P) with $E/\mathbb{F}_q$ and P a point of order ℓ. We begin by defining the equivalence on these pairs.

Definition 6.1. *Two pairs (E_1, P_1) and (E_2, P_2) are called $\mathbb{F}_q$-equivalent if there exists an isomorphism $\psi : E_1 \to E_2$ defined over $\mathbb{F}_q$ such that $\psi(P_1) = P_2$.*

It is clear that (E_1, P_1) and (E_2, P_2) are not equivalent if E_1 and E_2 are not isomorphic, in other words, non-equivalent classes of $\mathcal{E}(\mathbb{F}_q)$ always yields non-equivalent pairs. Hence, we obtain the $\mathbb{F}_q$-isomorphism classes of (E, P) by picking distinct representative curves E from $\mathcal{E}(\mathbb{F}_q)$ and identify the unique ℓ-torsion points as distinct orbits

under of automorphisms. Formally, we have the following definition

Definition 6.2. *For a fixed elliptic curve $E/\mathbb{F}_q$, let $X = E[\ell](\mathbb{F}_q) \setminus \{\infty\}$. We define the set of unique ℓ-torsion points on this curve as*

$$\mathcal{P}_\ell(E) = X/\sim,$$

where $P_1 \sim P_2$ if there exists $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(E)$ such that $P_2 = \sigma(P_1)$. We define

$$\mathcal{P}_\ell(\mathbb{F}_q) = \bigsqcup_{E \in \mathcal{E}(\mathbb{F}_q)} \mathcal{P}_\ell(E)$$

to be the set of all unique ℓ-torsion points over $\mathbb{F}_q$ up to isomorphism.

Remark 6.3. *If we also allow $\ell = 1$ we can identify $X = \{\infty\}$ and hence $\mathcal{P}_1(\mathbb{F}_q) \cong \mathcal{E}(\mathbb{F}_q)$.*

Our main goal is to determine the size of $\mathcal{P}_\ell(\mathbb{F}_q)$, and as we already know the size of $\mathcal{E}(\mathbb{F}_q)$, the rest of this section will be devoted to deriving explicit counting formulas for $\#\mathcal{P}_\ell(E)$ for each curve E.

6.1 Fixed Points And Automorphism Orbits

To determine the size of $\mathcal{P}_\ell(E)$ for a given curve E, we need to determine the number of distinct orbits under the action of $\mathrm{Aut}_{\mathbb{F}_q}(E)$ on the set $X = E[\ell](\mathbb{F}_q) \setminus \{\infty\}$. For this task we use a well-known formula from standard group theory.

Lemma 6.4 (Burnside's Lemma)**.** *Let G be a finite group acting on a finite set X. Then the number of distinct orbits under the action of G is given by*

$$\#(X/G) = \frac{1}{\#G} \sum_{g \in G} \#\,\mathrm{Fix}(g),$$

where $\mathrm{Fix}(g) = \{x \in X : g \cdot x = x\}$ denotes the set of elements fixed by g.

In order to use this lemma, we need to know the number of fixed points under the action of each automorphism, which for $\ell > 3$ turns out to be a trivial task.

Proposition 6.5. *Let $E/\mathbb{F}_q$ with characteristic $p > 3$. Let $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(E)$ be a non-identity automorphism. If $P \in E[\ell](\mathbb{F}_q) \setminus \{\infty\}$ satisfies $\sigma(P) = P$, then $\ell \in \{2, 3\}$.*

Proof. A point $P \in E[\ell]$ is fixed by an automorphism σ if and only if $P \in \ker(\sigma - 1)$. We now aim to show that the size of this kernel, hence the order of any point lying in it, is limited. Noting that $\deg(\sigma) = 1$, and $\hat{\sigma} \circ \sigma = \sigma \circ \hat{\sigma} = 1$ implying $\hat{\sigma}$ is just σ^{-1},

applying Lemma 4.2 we obtain

$$\deg(\sigma - 1) = 1 + \deg(\sigma) - \operatorname{tr}(\sigma) = 2 - \operatorname{tr}(\sigma) = 2 - (\sigma + \sigma^{-1}) = \deg(\sigma^{-1} - 1),$$

so it suffices to compute the degree of this kernel for one representative of each pair $\{\sigma, \sigma^{-1}\}$. We consider each automorphism group case by case.

Case $\operatorname{Aut}_{\mathbb{F}_q}(E) \cong \mu_2$ The non-identity automorphism is -1, with trace $\operatorname{tr}(-1) = -1 + (-1) = -2$. We compute $\deg(-1 - 1) = 2 - (-2) = 4$, and so $\deg(\sigma - 1) = 4$ for all non-identity $\sigma \in \mu_2$.

Case $\operatorname{Aut}_{\mathbb{F}_q}(E) \cong \mu_4$ The group is generated by i, where $\mu_4 \setminus \mu_2 = \{i, i^{-1}\}$. Noting that $i^{-1} = -i$, we get $\operatorname{tr}(i) = i + (-i) = 0$, and $\deg(i - 1) = 2 - 0 = 2$. Hence $\deg(\sigma - 1) \in \{2, 4\}$ for all non-identity $\sigma \in \mu_4$.

Case $\operatorname{Aut}_{\mathbb{F}_q}(E) \cong \mu_6$ The group is generated by $-\zeta^2$, where $\zeta^2 + \zeta + 1 = 0$. The set $\mu_6 \setminus \mu_2$ consists of the cube roots $\{\zeta, \zeta^2\}$ and primitive 6th roots $\{-\zeta, -\zeta^2\}$. We compute

$$\begin{aligned} \operatorname{tr}(\zeta) = \zeta + \zeta^2 = -1 &\implies \deg(\zeta - 1) = 2 - (-1) = 3, \\ \operatorname{tr}(-\zeta) = -\zeta - \zeta^2 = 1 &\implies \deg(-\zeta - 1) = 2 - 1 = 1, \end{aligned}$$

yielding $\deg(\sigma - 1) \in \{1, 3, 4\}$ for all non-identity $\sigma \in \mu_6$.

Summarizing, we find $\deg(\sigma - 1) \in \{1, 2, 3, 4\}$. Since $\operatorname{char}(\mathbb{F}_q) > 3$, none of these degrees are divisible by p, implying the isogenies $(\sigma - 1)$ are separable, so we know

$$\#\ker(\sigma - 1) \in \{1, 2, 3, 4\}.$$

By Lagrange's Theorem, the order of any point $P \in \ker(\sigma - 1) \cap \ker(\ell)$ must divide $\#\ker(\sigma - 1)$ and ℓ, thus, if σ fixes a non trivial point $P \in E[\ell]$, then $\ell \in \{2, 3\}$. Since $E[\ell](\mathbb{F}_q) \subseteq E[\ell](\overline{\mathbb{F}}_q)$, the same holds for points defined over $\mathbb{F}_q$. □

6.2 Determine Size of $\mathcal{P}_\ell(\mathbb{F}_q)$

Theorem 6.6. *Let $E/\mathbb{F}_q$ be an elliptic curve, let $\ell > 3$ be prime with $\ell \neq \operatorname{char}(\mathbb{F}_q)$, and let $r = \dim_{\mathbb{F}_\ell} E[\ell](\mathbb{F}_q)$. Then*

$$\#\mathcal{P}_\ell(E) = \frac{\ell^r - 1}{\#\operatorname{Aut}_{\mathbb{F}_q}(E)}.$$

Proof. By Proposition 6.7, only the identity fixes points of order ℓ, which trivially fixes all of them. Applying Burnside's Lemma 6.4 to $\ell^r - 1$ points of order ℓ in $E[\ell](\mathbb{F}_q)$ directly yields the result. □

For $\ell \in \{2, 3\}$ we need to consider both the size of the automorphism group as well as the curve equation to determine the number of fixed points for each non-identity automorphism. As this will get less trivial, we first summarize the results from the proof of Proposition 6.5 into the following Corollary.

Corollary 6.7. *For a non-identity automorphism $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(E)$, the number of non-trivial fixed points $\#\ker(\sigma - 1) - 1$ in $E(\overline{\mathbb{F}}_q)$ is*

$$\#\ker(\sigma - 1) - 1 = \begin{cases} 3, & \text{if } \sigma \in \{-1\}, \\ 1, & \text{if } \sigma \in \{i, -i\}, \\ 2, & \text{if } \sigma \in \{\zeta, \zeta^2\}, \\ 0, & \text{if } \sigma \in \{-\zeta, -\zeta^2\}. \end{cases}$$

Fixed Points of Order 3

Proposition 6.8. *Let $E/\mathbb{F}_q$ be an elliptic curve with $r = \dim_{\mathbb{F}_3} E[3](\mathbb{F}_q)$, where $3 \neq \mathrm{char}(\mathbb{F}_q)$. Define*

$$\mathrm{F}_\zeta := \begin{cases} 4, & \text{if } j(E) = 0, \text{ and } 6 \mid q - 1, \text{ and } B \text{ is a square } \in \mathbb{F}_q, \\ 0, & \text{otherwise,} \end{cases}$$

then

$$\#\mathcal{P}_3(E) = \frac{(3^r - 1) + \mathrm{F}_\zeta}{\#\,\mathrm{Aut}_{\mathbb{F}_q}(E)}.$$

Proof. First, consider the case where $j(E) \neq 0$ or $6 \nmid q - 1$, so $\mathrm{F}_\zeta = 0$. In this case, $\mathrm{Aut}_{\mathbb{F}_q}(E)$ is isomorphic to μ_2 or μ_4. By Corollary 6.7, no non-identity automorphism fixes points of order 3. Burnside's Lemma yields

$$\#\mathcal{P}_3(E) = \frac{\#\,\mathrm{Fix}(\mathrm{id})}{\#\,\mathrm{Aut}_{\mathbb{F}_q}(E)} = \frac{3^r - 1}{\#\,\mathrm{Aut}_{\mathbb{F}_q}(E)}.$$

Now consider $j(E) = 0$ and $6 \mid q - 1$, implying $\mathrm{Aut}_{\mathbb{F}_q}(E) \cong \mu_6$. Again, using Corollary 6.7 we know that the automorphisms ζ and ζ^2 can fix points of order 3, and each fixes exactly 2 in the algebraic closure. Explicitly, the action of these automorphisms on points is given by

$$\zeta \cdot (x, y) = (\zeta x, y), \quad \zeta^2 \cdot (x, y) = (\zeta^2 x, y).$$

Since $\zeta, \zeta^2 \neq 1$, and we require $\zeta^2 x = \zeta x = x$, the only solution is $x = 0$. Recall that for any curve $j(E) = 0$ we have $A = 0$, substituting into the curve equation $y^2 = x^3 + B$ yields $y^2 = B$. Hence, the extra fixed points in this case are $(0, \pm\sqrt{B})$, which exist in

$E[3](\mathbb{F}_q)$ if and only if B is a square in $\mathbb{F}_q$. We get

$$\#\mathcal{P}_3(E) = \frac{\#\operatorname{Fix}(\mathrm{id}) + \#\operatorname{Fix}(\zeta) + \#\operatorname{Fix}(\zeta^2)}{\#\operatorname{Aut}_{\mathbb{F}_q}(E)} = \frac{(3^r-1)+4}{\#\operatorname{Aut}_{\mathbb{F}_q}(E)}.$$

If B is not a square, $\#\operatorname{Fix}(\zeta) + \#\operatorname{Fix}(\zeta^2) = 0 = \mathrm{F}_\zeta$, and we can write

$$\#\mathcal{P}_3(E) = \frac{(3^r-1)+\mathrm{F}_\zeta}{\#\operatorname{Aut}_{\mathbb{F}_q}(E)}$$

covering both cases as stated. □

Fixed Points of Order 2

Proposition 6.9. *Let $E/\mathbb{F}_q$ be an elliptic curve with $r = \dim_{\mathbb{F}_2} E[2](\mathbb{F}_q)$, where $2 \neq \operatorname{char}(\mathbb{F}_q)$. Then*

$$\#\mathcal{P}_2(E) = \begin{cases} 1, & \text{if } j(E)=0, \text{ and } 6 \mid q-1, \text{ and } B \text{ is a cube } \in \mathbb{F}_q, \\ 2^{r-1}, & \text{if } j(E)=1728, \text{ and } 4 \mid q-1, \\ 2^r-1, & \text{otherwise,} \end{cases}$$

Proof. We begin by showing that all points of order 2 are fixed by inversion, and that they all satisfy $P = (x, 0)$. We have $-1 \cdot (x, y) = (x, -y)$, a point is therefore fixed by -1 if and only if $y = 0$, further, since $-P = P$, this implies $2P = \mathcal{O}$. Thus $\operatorname{Fix}(-1) = E[2](\mathbb{F}_q)$. We now proceed by cases on the size of the automorphism group.

Case $\operatorname{Aut}_{\mathbb{F}_q}(E) \cong \mu_2$. Burnside's Lemma gives directly

$$\#\mathcal{P}_2(E) = \frac{\#\operatorname{Fix}(\mathrm{id}) + \#\operatorname{Fix}(-1)}{\#\operatorname{Aut}_{\mathbb{F}_q}(E)} = \frac{2(2^r-1)}{2} = 2^r - 1.$$

Case $j = 1728$, $4 \mid q-1$, so $\operatorname{Aut}_{\mathbb{F}_q}(E) \cong \mu_4$. By Corollary 6.7, i and $-i$ each fix exactly 1 point of order 2. Since $B = 0$, the curve is $y^2 = x(x^2 + A)$, so $P_0 = (0, 0) \in E[2](\mathbb{F}_q)$ is fixed by every automorphism and necessarily also by i and $-i$. Counting P_0 as its own orbit and applying Burnside to the remaining $2^r - 2$ points yields

$$\#\mathcal{P}_2(E) = \frac{\#\operatorname{Aut}_{\mathbb{F}_q}(E) + \#\operatorname{Fix}(\mathrm{id}) - 1 + \#\operatorname{Fix}(-1) - 1}{\#\operatorname{Aut}_{\mathbb{F}_q}(E)} = \frac{4 + 2(2^r-2)}{4} = 2^{r-1}.$$

Case $j = 0$, $6 \mid q-1$, so $\operatorname{Aut}_{\mathbb{F}_q}(E) \cong \mu_6$. By Corollary 6.7, no automorphism in $\mu_6 \setminus \{1, -1\}$ fixes a point of order 2, so

$$\#\mathcal{P}_2(E) = \frac{\#\operatorname{Fix}(\mathrm{id}) + \#\operatorname{Fix}(-1)}{\#\operatorname{Aut}_{\mathbb{F}_q}(E)} = \frac{2(2^r-1)}{6}.$$

Since $A = 0$, the 2-torsion condition $y = 0$ reduces to $x^3 = -B$. As $\zeta \in \mu_6 \subseteq \mathbb{F}_q$, the three roots $-\sqrt[3]{B}$, $-\zeta\sqrt[3]{B}$, $-\zeta^2\sqrt[3]{B}$ all lie in $\mathbb{F}_q$ if and only if B is a cube in $\mathbb{F}_q$, resulting in $r = 2$, or $r = 0$. The orbit count is therefore $\frac{2(2^2-1)}{6} = 1$ if B is a cube, and $2^0 - 1 = 0$ otherwise. □

6.2.1 Algorithm

We are now ready to present our final algorithm to compute $\#\mathcal{P}_\ell(\mathbb{F}_q)$ for any prime $\ell \neq \mathrm{char}(\mathbb{F}_q)$. The algorithm is a direct implementation of the counting formulas derived in this section, relying on the previously developed algorithms.

Algorithm 4 Count Number of Points of order ℓ over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism.

function CountOrbits(E, ℓ, r)
  $a \leftarrow \#\operatorname{Aut}_{\mathbb{F}_q}(E)$ ▷ Size of automorphism group over $\mathbb{F}_q$
  $r \leftarrow$ EllTorsionRank(E, q, ℓ) ▷ See Algorithm 3
  return 0 if $r = 0$ ▷ Early exit if no points of order ℓ
  if $\ell = 2$ **then**
    return 1 if B is a cube in $\mathbb{F}_q$ and $a = 6$ else 2^{r-1} if $a = 4$ else $2^r - 1$
  else if $\ell = 3$ **then**
    $B \leftarrow$ coefficient in Weierstrass equation of E
    $\mathrm{F}_\zeta \leftarrow 4$ if B is a square in $\mathbb{F}_q$ and $a = 6$ else 0
    return $(3^r - 1 + \mathrm{F}_\zeta)/a$
  else
    return $(\ell^r - 1)/a$
  end if
end function
function CountEllTorsionPoints(q, ℓ)
  $\mathcal{E} \leftarrow$ EnumCurves(q) ▷ See Algorithm 1
  $N \leftarrow 0$
  for each $E \in \mathcal{E}$ **do**
    $N \leftarrow N +$ CountOrbits(E, ℓ)
  end for
  return N
end function

Remark 6.10. *For supersingular curves, we compute the ℓ-torsion rank using either explicit point enumeration or by inspecting the abelian group invariants of $E(\mathbb{F}_q)$, both methods directly available in SageMath. For more details see [14].*

7 AN APPLICATION TO MODULAR FORMS

Elliptic curves are deeply connected to modular forms, the goal of this section is not to introduce any new theory, but simply to test our algorithms against known data.

7.1 Trace of Hecke Operator

Hecke operators are linear operators acting on a space of modular forms. In [1, Theorem 2.1], the trace of this action is expressed as a weighted sum over pairs (E, P), precisely the objects we have classified. The formula as stated in the paper is

$$\mathrm{Tr}(T_p \mid S_{k+2}(\Gamma_1(N))) = -\,\mathrm{Eis}(\Gamma_1(N), k) - \sum_{[(E,P)]\in Y_1(N)(\mathbb{F}_q)} \frac{h_k(\pi_E, \hat{\pi}_E)}{\#\,\mathrm{Aut}_{\mathbb{F}_q}(E, P)}.$$

The left-hand side exist as recorded data and can be found in the database [LMFDB]. In the weighted sum on the right hand side, h_k is a known symmetric polynomial evaluated at the Frobenius endomorphism π_E and its dual $\hat{\pi}_E$, which means we are able to compute the right-hand side up to the term Eis. We rewrite the sum in our notation as

$$\sum_{E\in\mathcal{E}(\mathbb{F}_q)} h_k(\pi_E, \hat{\pi}_E) \sum_{P\in\mathcal{P}_\ell(E)} \frac{1}{\#\,\mathrm{Stab}(P)}.$$

By the orbit-stabilizer theorem [5, Chapter 4.1, Proposition 2], we have $\#\,\mathrm{Stab}(P) = \#\,\mathrm{Aut}_{\mathbb{F}_q}(E)/\#P_\ell(E)$. Hence the un-weighted contribution to the sum from a representative curve is

$$\sum_{P\in\mathcal{P}_\ell(E)} \frac{1}{\#\,\mathrm{Stab}(P)} = \sum_{P\in\mathcal{P}_\ell(E)} \frac{\#P_\ell(E)}{\#\,\mathrm{Aut}_{\mathbb{F}_q}(E)} = \frac{1}{\#\,\mathrm{Aut}_{\mathbb{F}_q}(E)} \sum_{P\in\mathcal{P}_\ell(E)} \#P_\ell(E).$$

By the class equation [5, Chapter 4.1, Theorem 7], the right sum is just the total number of points of order ℓ in $E[\ell](\mathbb{F}_q)$. Hence, let $r = \mathrm{rank}_\ell(E/\mathbb{F}_q)$, then the trace formula simplifies to

$$\mathrm{Tr}(T_p \mid S_{k+2}(\Gamma_1(\ell))) = -\,\mathrm{Eis}(\Gamma_1(\ell), k) - \sum_{E\in\mathcal{E}(\mathbb{F}_q)} \frac{h_k(\pi_E, \hat{\pi}_E)\cdot(\ell^r - 1)}{\#\,\mathrm{Aut}_{\mathbb{F}_q}(E)}.$$

Results

Noting that the left hand side of the equation is $k+2$, we compute the sum, and compare our results with values obtained from [LMFDB] for $(\ell, k+2)$ over several primes p. Since we are not able to compute the $\mathrm{Eis}(\Gamma_1(\ell), k)$ term directly, we instead tabulate the difference Diff = Computed − LMFDB in the tables below, in order to examine

whether the differences exhibit a consistent pattern, indicating correct computation.

	$k+2=8$					$k+2=10$				
	a_7 $\equiv 2$	a_{11} $\equiv 1$	a_{13} $\equiv 3$	a_{17} $\equiv 2$	a_{19} $\equiv -1$	a_7 $\equiv 2$	a_{11} $\equiv 1$	a_{13} $\equiv 3$	a_{17} $\equiv 2$	a_{19} $\equiv -1$
Computed	-1742	-8936	7404	-39592	26544	5944	87748	-912	907664	-1942136
LMFDB	-1744	-8940	7402	-39594	26540	5942	87744	-914	907662	-1942140
Diff	2	4	2	2	4	2	4	2	2	4

Table 1: level $\ell = 5$, weights $k \in \{8, 10\}$

	$k+2=8$					$k+2=10$				
	a_5 $\equiv 5$	a_{11} $\equiv 4$	a_{13} $\equiv -1$	a_{17} $\equiv 3$	a_{19} $\equiv 5$	a_5 $\equiv 5$	a_{11} $\equiv 4$	a_{13} $\equiv -1$	a_{17} $\equiv 3$	a_{19} $\equiv 5$
Computed	-3	1251	-4964	-71835	46435	852	74088	-365982	877458	-718692
LMFDB	-6	1248	-4970	-71838	46432	849	74085	-365988	877455	-718695
Diff	3	3	6	3	3	3	3	6	3	3

Table 2: level $\ell = 7$, weights $k \in \{8, 10\}$

	$k+2=8$				$k+2=9$			
	a_{23} $\equiv 1$	a_{41} $\equiv 8$	a_{43} $\equiv -1$	a_{47} $\equiv 3$	a_{23} $\equiv 1$	a_{41} $\equiv 8$	a_{43} $\equiv -1$	a_{47} $\equiv 3$
Computed	-96795	1936575	3857880	-2529095	856065	-13192695	0	21702765
LMFDB	-96805	1936570	3857870	-2529100	856055	-13192700	0	21702760
Diff	10	5	10	5	10	5	0	5

Table 3: Level $\ell = 11$, weights $k + 2 \in \{8, 9\}$.

Studying the tables above, we observe that for a fixed pair $(\ell, k > 0)$, the difference, hence the assumed $\mathrm{Eis}(\Gamma_1(\ell), k)$ contribution, lies in $\{0, n, 2n\}$ for $n = (\ell - 1)/2$. In fact, the observed results suggest that

$$\mathrm{Eis}(\Gamma_1(\ell), k) \stackrel{?}{=} n(1 + \mathrm{sgn}(p, l)^k)$$

with

$$\mathrm{sgn}(p, l) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{l} \\ -1 & \text{if } p \equiv -1 \pmod{l} \\ 0 & \text{otherwise.} \end{cases}$$

We interpret the consistent pattern of discrepancy in our results, observed across a large number of parameters, as validating our algorithms, in particular for computing the rank, and hence the number of points of order ℓ in $E[\ell](\mathbb{F}_q)$. For further details and additional results, see [14].

8 END NOTE

Elliptic curves are rich mathematical objects that can be studied from a wide range of perspectives, and classifying them, as we have seen in this paper, draws on tools spanning geometry and group theory to algebraic number theory, all ending in an application to modular forms. Knowing this, we have deliberately tried to keep the theory as conceptually clean as possible in each section, for example, while the ℓ-torsion and the action of Frobenius on the subgroups $E[\ell]$ are well suited to be studied by linear algebra, or more generally the set of rational points via group theory, we chose a full ring-theoretic approach, as it fits more naturally with the isogeny volcano framework, which in our opinion yields a better understanding of how Frobenius interacts with geometry and what governs the structure of $\mathbb{F}_q$-rational points. In particular allowing for making it visually apparent how the parameters (q, ℓ, j, t) govern the torsion structure, rather than reducing the study to matrices and abelian group invariants of individual curves.

The current computational bottleneck is the enumeration of j-invariants over $\mathbb{F}_q$ and the computation of the trace t of Frobenius for each such curve. Nevertheless, we are able to run the algorithms efficiently in the range $q < 10^6$ and $\ell < 100$. For substantially larger values, more efficient methods for curve enumeration may be needed; we briefly describe some possible directions below.

Future Work

During the work of this thesis, and motivated by the deep number-theoretic connections of elliptic curves, we also explored even more pure arithmetic approaches to the counting problem of (E, P), and saw that there are indeed theories closely related to the direction we pursued that may achieve this. As we saw in the Hecke application, we did not need to use the geometry of the curve equation. Further, for our visualizations and volcano graphs, if one enumerates only the possible traces t, and hence the possible number fields and orders, there exist methods to compute the j-invariant for a given order and trace. One may therefore start from the other end, and, if the geometry is not important, only knowing the tuple (q, ℓ, j, t) is in principle enough to study the structure of an isogeny class and the associated number field. Hence, for certain applications, one may be able to avoid explicit curve enumeration and repeated trace computations entirely. Some of these ideas were tested experimentally and implemented in Python/SageMath, and are available in the source code [14]. However, these methods diverge from the classification of actual curves and go beyond the theoretical framework developed in this thesis, instead, it would be of great interest to explore in future work, both from a computational and theoretical perspective.

REFERENCES

[1] Jonas Bergström and Sjoerd de Vries. **Periodicity of traces of Hecke operators modulo prime powers**. 2026. arXiv: 2601.03029 [math.NT]. URL: https://arxiv.org/abs/2601.03029.

[2] Gaetan Bisson and Andrew V. Sutherland. "Computing the Endomorphism Ring of an Ordinary Elliptic Curve over a Finite Field". In: **Journal of Number Theory** 113 (2011), pp. 815–831. DOI: 10.1016/j.jnt.2009.11.003. URL: https://arxiv.org/abs/0902.4670.

[3] Reinier Broker, Kristin Lauter, and Andrew V. Sutherland. "Modular polynomials via isogeny volcanoes". In: **Mathematics of Computation** 81.278 (July 14, 2011), pp. 1201–1231. ISSN: 0025-5718, 1088-6842. DOI: 10.1090/S0025-5718-2011-02508-1. arXiv: 1001.0402[math]. URL: http://arxiv.org/abs/1001.0402 (visited on 02/25/2026).

[4] David A. Cox. **Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication**. John Wiley & Sons, Inc., 1989. ISBN: 0-471-50654-0.

[5] David S. Dummit and Richard M. Foote. **Abstract Algebra**. 3rd. Wiley, 2003. ISBN: 978-0471433347.

[6] Mireille Fouquet and François Morain. "Isogeny Volcanoes and the SEA Algorithm". In: **Algorithmic Number Theory**. Ed. by Claus Fieker and David R. Kohel. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 276–291. ISBN: 978-3-540-45455-7.

[7] Sorina Ionica and Antoine Joux. **Pairing the Volcano**. 2011. arXiv: 1110.3602 [math.AG]. URL: https://arxiv.org/abs/1110.3602.

[8] Kenneth Ireland and Michael Rosen. **A Classical Introduction to Modern Number Theory**. Vol. 84. Springer, 1990.

[9] David R. Kohel. "Endomorphism rings of elliptic curves over finite fields". In: 1996. URL: https://api.semanticscholar.org/CorpusID:122855991.

[LMFDB] The LMFDB Collaboration. **The L-functions and modular forms database**. https://www.lmfdb.org. [Online; accessed 17 March 2026]. 2026.

[10] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. "ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$". In: **Forum of Mathematics, Sigma** 10 (2022), e62. ISSN: 2050-5094. DOI: 10.1017/fms.2022.38. arXiv: 2106.11141[math]. URL: http://arxiv.org/abs/2106.11141 (visited on 02/25/2026).

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

[11] René Schoof. "Nonsingular plane cubic curves over finite fields". In: **Journal of Combinatorial Theory, Series A** 46.2 (1987), pp. 183–211. ISSN: 0097-3165. DOI: 10.1016/0097-3165(87)90003-3. URL: https://www.sciencedirect.com/science/article/pii/0097316587900033.

[12] Joseph H Silverman. **The Arithmetic of Elliptic Curves**. Graduate texts in mathematics. Dordrecht: Springer, 2009. DOI: 10.1007/978-0-387-09494-6. URL: https://cds.cern.ch/record/1338326.

[13] Andrew V. Sutherland. **Isogeny volcanoes**. Version v3, 7 May 2013. 2013. arXiv: 1208.5370 [math.NT]. URL: https://arxiv.org/abs/1208.5370.

[14] Johanna Tano. **Source Code for Classification of Elliptic Curves with ℓ-Torsion over Finite Fields**. 2026. URL: https://github.com/johannatano/bsc-thesis-ell-curves-2026.

[15] John Tate. "Endomorphisms of abelian varieties over finite fields". In: **Inventiones Mathematicae** 2.2 (Apr. 1966), pp. 134–144. ISSN: 0020-9910, 1432-1297. DOI: 10.1007/BF01404549. URL: http://link.springer.com/10.1007/BF01404549 (visited on 02/27/2026).

[16] Nicholas George Triantafillou. **Isogeny Volcanoes**. URL: https://ngtriant.github.io/notes/volcanoes.pdf.

[17] Joachim Von Zur Gathen and Jürgen Gerhard. **Modern Computer Algebra**. 3rd ed. Cambridge University Press, Apr. 25, 2013. ISBN: 978-1-107-03903-2 978-1-139-85606-5. DOI: 10.1017/CBO9781139856065. URL: https://www.cambridge.org/core/product/identifier/9781139856065/type/book (visited on 03/03/2026).

[18] Lawrence C. Washington. **Elliptic Curves: Number Theory and Cryptography**. 2nd. Chapman & Hall/CRC, 2008. ISBN: 9781420071466.

[19] William C Waterhouse. "Abelian varieties over finite fields". In: ().