Geometry and Arithmetic in the Moduli of Pairs of Elliptic Curves

by

Yu Fu

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Mathematics

at the
University of Wisconsin-Madison
2023

Date of Final Oral Exam: 05/11/2023
The dissertation is approved by the following members of the Final Oral Committee:

Professor Jordan Ellenberg, Professor, Mathematics
Professor Ananth Shankar, Assistant Professor, Mathematics
Professor Tonghai Yang, Professor, Mathematics
Professor Dima Arinkin, Professor, Mathematics

Geometry and Arithmetic in the Moduli of Pairs of Elliptic Curves

Yu Fu

Abstract

This thesis explores two kinds of questions on the moduli spaces of pairs of elliptic curves over number fields and finite fields. The first question is about rational points in a family of pairs of elliptic curves over number fields. Given a family of products of elliptic curves over a rational curve over a number field K, we give a bound for the number of special fibers of height at most B such that the two factors are isogenous. We prove an upper bound that depends on K, the family, and the height B. Moreover, if we slightly change the definition of the height of the parametrizing family, we prove a uniform bound that depends only on the degree of the family, K and the height B.

The second question is about the size of isogeny classes of non-simple abelian surfaces over finite fields. Let $A = E \times E_{ss}$ be an abelian surface over a finite field $\mathbb{F}_q$, where E is an ordinary elliptic curve and E_{ss} is a supersingular elliptic curve. We give a lower bound on the size of isomorphism classes of principally polarized abelian surfaces defined over $\mathbb{F}_{q^n}$ that are $\overline{\mathbb{F}}_q$-isogenous to A by studying classification of certain kind of finite group schemes.

Dedication

To my parents.

Acknowledgements

I would like to, first and foremost, thank my Ph.D. advisers, Jordan Ellenberg and Ananth Shankar, for introducing me to the beautiful topic of arithmetic geometry, for guiding me through the way of discovery, excitement, occasional despair, then utter relief, surprise, and eventual awe of the beauty. Also, I want to thank them for suggesting I work on these problems - this thesis wouldn't exist without them.

I would like to thank the rest of my thesis committee members: Dima Arinkin and Tonghai Yang. I am immensely grateful to Tonghai Yang for his love and passion for every student and his numerous math and life advice during the past few years. He performs as a good role model of being a math professor and an excellent philanthropist.

I thank all my colleagues and friends over the past few years. In addition, I thank all the people for and discussing mathematics and sharing ideas with me, especially Asvin, Qiao, Ruofan, Sun Woo, Tejasi, Tian and Ziquan. I am grateful for their time and kindness.

Thanks to my friends Di, Junyi, Mingrui, Jingying, and many others for your unconditional love and support. I couldn't survive without your company during the pandemic.

I am grateful to everyone for being with me when I was on the tough job market last fall, especially Pam (Miao), Jingying and Sun Woo for their enormous help and emotional support. I couldn't get such a fantastic job without you.

I thank the academic staff at the math department of the University of Wisconsin-Madison for their support over the past few years, especially Bobby and Kathie, for their generous help.

A special thanks to Shasha, who passed away nine years ago. You inspired me to be a mathematician when I was a high school student. Rest in peace, and I will make your dream come true.

I thank my family, especially my parents, for always being supportive and for encouraging me to be myself. This thesis is dedicated to them.

Contents

Chapter 1

Introduction

The exuberant arithmetic properties of elliptic curves have been brought to mathematicians' attention for more than 150 years. In this report, we explore two directions in the moduli aspect of elliptic curves, with main results shown in Subsction 1.1 and 1.2.

This thesis has three chapters, including the present one. Chapter 2 talks about the first direction, and Chapter 3 about the second.

1.1 Families of isogenous elliptic curves ordered by heights

Let k be a field. Let $X \to S$ be a family of algebraic varieties over k, where S is irreducible, and let X_η be the generic fiber of this family. People care about what properties of X_η extend to other fibers and how we can measure the size of specializations such that a specific property does not extend. For example, the Hilbert Irreducibility Theorem says that for a Galois covering $X \to \mathbb{P}^n$ over a number field K, for most of the rational points $t \in \mathbb{P}^n(K)$ the specializations over t generate a Galois extension with Galois group G. Moreover, the size of the complement set, which can be considered as locus of *'exceptional'* points, can be bounded as in [23].

In [10], Ellenberg, Elsholtz, Hall, and Kowalski studied families of Jacobians of hyperelliptic curves defined over number fields by affine equations

$$y^2 = f(x)(x-t),\ t \in \mathbf{A}^1,$$

with the assumption that the generic fiber is geometrically simple. They proved that the number of geometrically non-simple fibers in this family, with the height of the parametrizer $t \leq B$, is bounded above by a constant $C(f)$ depending on f. Moreover, they obtained an effective bound using the analytic method that depends on the primes dividing the discriminant of $f(x)$ and the genus of the family.

In this paper, we study families of pairs of elliptic curves defined over a rational curve over a number field K. To be precise, let C be a rational curve over K isomorphic to $\mathbb{P}^1$ which parametrizes a one-dimensional family of pairs of elliptic curves and let (E_t, E'_t) be the generic fiber of this family over $K(t)$, with the assumption that there exists no isogeny between E_t and E'_t. We prove an upper bound for the number of specializations of (E_t, E'_t) such that the two factors are isogenous, with the assumption that the height of the parameter $t \leq B$. The method relies on constructions of explicit covers of $X(1) \times X(1)$ and results in dimension growth conjecture, as proven in [6]. Moreover, by a proper choice of definition of the height of t, this uniform upper bound depends only on the degree and the height of the parameter. The independence of our bound is an exciting aspect for possible further applications.

To discuss the results, we first fix the general setting and terminology (see section §2 for more details). Define ι to be the map from C to $\mathbb{P}^3$ which is a composition of a finite map via the j-invariant, followed by the Segre embedding:

$$\iota : C \to X(1) \times X(1) \to \mathbb{P}^1 \times \mathbb{P}^1 \hookrightarrow \mathbb{P}^3. \tag{1.1.1}$$

To be precise, the map ι sends t to

$$(E_t, E'_t) \mapsto (j(E_t), j(E'_t)) \mapsto (j(E_t)j(E'_t); j(E_t); j(E'_t); 1).$$

Degrees and heights are computed with respect to this fixed embedding. We prove the following theorem:

Theorem 1.1.1. *Let K be a number field of degree d_K. let C be a rational curve over K isomorphic to $\mathbb{P}^1$ which parametrizes a one-dimensional family of pairs of elliptic curves (E, E'). Let (E_t, E'_t) be the generic fiber of this family over $K(t)$, and suppose* *that there exists no $\overline{K(t)}$-isogeny between E_t and E'_t. Let $d = \deg \iota^*\mathcal{O}_{\mathbb{P}^3}(1)$ be the degree of the parameter family C defined with respect to ι. Let $H(\iota)$ be the height of ι defined by the projective height of the coefficients of the defining polynomials of $j(E_t)$ and $j(E'_t)$. Let $H : C(K) \to \mathbb{R}$ be the projective height defined over K. Define $S(B)$ to be the set*

$$S(B) = \{t \in C(K) | H(t) \leq B, \text{ there is an } \overline{\mathbb{Q}}\text{-isogeny between } E_t \text{ and } E'_t\}.$$

There is an absolute constant M such that for any $B \geq M$, we have

$$|S(B)| \lesssim_K d^{4+\epsilon}(\log H(\iota) + \log B)^6.$$

Definition 1.1.2. For a point $P_t \in C$ parametrized by $t \in K$, define the height $H(P_t)$ to be the projective height of $\iota(P_t) \in \mathbb{P}^3$.

Note that in Theorem 3.1.1, $H(t)$ is the height of t as an element of K. If we change the definition of the height from $H(t)$ to $H(P_t)$ and assume that $H(P_t) \leq B$, then we get an *uniform* bound on the number of points t such that E_t and E'_t are geometrically isogenous. Moreover, this uniform bound only depends on K, the height B, and the degree of the family.

Theorem 1.1.3. *Assume the same hypothesis as in Theorem 3.1.1. Let $S'(B)$ be the set*

$$S'(B) = \{t \in C(K) | H(P_t) \leq B, \text{ there is an } \overline{\mathbb{Q}}\text{-isogeny between } E_t \text{ and } E'_t\}.$$

Then we have

$$|S'(B)| \lesssim_K d^4(\log B)^6.$$

1.2 Isogeny Classes of Non-Simple Abelian Surfaces over Finite Fields

Many fundamental problems on Shimura varieties pertain to the behavior of isogeny classes, for example, the Hecke orbit conjecture and specific questions related to unlikely intersections. In [24, Theorem 4.1], Shankar and Tsimerman proved an asymptotic formula for the size of the isogeny class of ordinary elliptic curves over finite fields. As an application, they proved the existence of a hypersurface in the moduli space $X(1)^{270}$, which intersects every isogeny class.

A few common strategies exist to obtain asymptotic formulas for the size of isogeny classes of abelian varieties over finite fields. In particular, when the abelian variety is ordinary and simple, the inspiring work of Deligne [8] explicitly classified such abelian varieties over finite fields. Using the classification, one can get bounds for the isogeny classes of ordinary abelian varieties, for example, [24, Theorem 3.3]. A handful of studies in this flavor have been performed in more general settings. For example, one may refer to [18] when the abelian variety is almost-ordinary and geometrically simple and to [4] for a setting of Hilbert modular varieties. All of the results above depend on the existence of canonical lifting and classification of abelian varieties over finite fields.

A second way of doing this is to interpret isogeny classes in terms of orbital integrals. For example, in [2], Achter and Cunningham proved an explicit formula for the size of the isogeny class of a Hilbert-Blumenthal abelian variety over a finite field. They express the size of the isogeny class as a product of local orbital integrals on $GL(2)$ and then evaluate all the relevant orbital integrals. See also [1] where Achter and Williams proved that for a particular class of simple, ordinary abelian surfaces over $\mathbb{F}_q$ given by a q-weil polynomial f, the number of principally polarized abelian surfaces over $\mathbb{F}_q$ with Weil polynomial f could be calculated by an infinite product of local factors which can be calculated by method of orbital integrals.

Throughout this article, (A, λ_A) is a principally polarized non-simple abelian surface defined over $\mathbb{F}_q$, with the polarization given by λ_A. Moreover, we assume that A has the form $A = E \times E_{ss}$, where E is an ordinary elliptic curve and E_{ss} is a supersingular elliptic curve. The endomorphism algebra $\mathrm{End}^\circ(A)$ is non-commutative, and there is no canonical lifting of A. Therefore, we cannot interpret the question as estimating the size of class groups by using the classification of abelian varieties over finite fields. Instead, we measure the size of the isogeny class of A defined over $\mathbb{F}_q$ and describe how this cardinality is affected by the base change to finite extensions of $\mathbb{F}_q$ by using group-theoretical methods.

Before introducing the main theorem, we introduce some notations. Let $I(q^n, A)$ be the set of principally polarized abelian varieties defined over $\mathbb{F}_{q^n}$ that are isogenous to A over $\overline{\mathbb{F}}_q$. Let $N(q^n, A)$ denote the cardinality of $I(q^n, A)$. By interpreting the question as a classification of finite subgroup schemes, we obtain a lower bound on the number of principally polarized abelian varieties over $\mathbb{F}_{q^n}$ that is isogenous to A over $\overline{\mathbb{F}}_q$. Our main result is the following.

Theorem 1.2.1. *Let (A, λ_A) be a principally polarized abelian variety over $\mathbb{F}_q$ such that $A = E \times E_{ss}$. Let K be the quadratic number field such that $K = \mathrm{End}^\circ(E)$. Let n be an integer such that for all prime ℓ ramified in $\mathcal{O}_K$, $(n, \ell) \neq 1$. Then*

$$N(q^n, A) \gg q^{n+o(1)}.$$

Also, we provide a different approach to count the size of isogeny classes of ordinary elliptic curves over finite fields, which upper bound is known by Lenstra [14, Proposition 1.19] and Shankar-Tsimerman [24, Theorem 3.3].

Theorem 1.2.2. *Let E be an elliptic curve defined over $\mathbb{F}_q$. For a positive density set of n, we have*

$$N(q^n, E) = (q^n)^{1/2+o(1)}.$$

There is a general conjecture regarding the size of the isogeny class of abelian varieties over finite fields. Let $N(W)$ be the open Newton stratum of $\mathcal{A}_g$ consisting of all abelian varieties whose Newton polygon is W and let A be a principally polarized abelian variety in $\mathcal{A}_g$. Recall that the *central leaf* through A consists of all abelian varieties in $N(W)$ whose p-divisible group is isomorphic to $A[p^\infty]$. The *isogeny leaf* through A is a maximal irreducible subscheme of $\mathcal{A}_g$ consisting of abelian varieties A' in $N(W)$ such that A' is isogenous to A through an isogeny whose kernel is an iteration extension of the group scheme α_p. Let $\dim(CL)$ be the dimension of the central leaf through A and let $\dim(IL)$ be the dimension of the isogeny leaf through A.

Conjecture 1.2.3. *We have*

$$N(q^n, A) = q^{n(\frac{\dim(CL)}{2} + \dim(IL)) + o(1)}.$$

All the previous results we state above satisfy the Conjecture 3.1.3. When A is a non-simple abelian surface, it is easy to see that the dimension of the central leaf through A is 2, by the formula of lattice-point count by Shankar and Tsimerman [24, Section 5.2]. The dimension of the isogeny leaf through A is 0. Therefore the conjecture is true in this case.

Chapter 2

Families of isogenous elliptic curves ordered by height

2.1 Introduction

Let k be a field. Let $X \to S$ be a family of algebraic varieties over k, where S is irreducible, and let X_η be the generic fiber of this family. People care about what properties of X_η extend to other fibers and how we can measure the size of specializations such that a specific property does not extend. For example, the Hilbert Irreducibility Theorem says that for a Galois covering $X \to \mathbb{P}^n$ over a number field K, for most of the rational points $t \in \mathbb{P}^n(K)$ the specializations over t generate a Galois extension with Galois group G. Moreover, the size of the complement set, which can be considered as locus of *'exceptional'* points, can be bounded as in [23].

In [10], Ellenberg, Elsholtz, Hall, and Kowalski studied families of Jacobians of hyperelliptic curves defined over number fields by affine equations

$$y^2 = f(x)(x-t), \ t \in \mathbf{A}^1,$$

with the assumption that the generic fiber is geometrically simple. They proved that the number of geometrically non-simple fibers in this family, with the height of the parametrizer $t \leq B$, is bounded above by a constant $C(f)$ depending on f. Moreover, they obtained an effective bound using the analytic method that depends on the primes dividing the discriminant of $f(x)$ and the genus of the family.

In this paper, we study families of pairs of elliptic curves defined over a rational curve over a number field K. To be precise, let C be a rational curve over K isomorphic to $\mathbb{P}^1$ which parametrizes a one-dimensional family of pairs of elliptic curves and let (E_t, E'_t) be the generic fiber of this family over $K(t)$, with the assumption that there exists no isogeny between E_t and E'_t. We prove an upper bound for the number of specializations of (E_t, E'_t) such that the two factors are isogenous, with the assumption that the height of the parameter $t \leq B$. The method relies on constructions of explicit covers of $X(1) \times X(1)$ and results in dimension growth conjecture, as proven in [6]. Moreover, this uniform upper bound depends only on the degree and height of the parameter. The independence of our bound is an exciting aspect for possible further applications.

To discuss the results, we first fix the general setting and terminology (see section §2 for more details). Define ι to be the map from C to $\mathbb{P}^3$ which is a composition of a finite map via the j-invariant, followed by the Segre embedding:

$$\iota : C \to X(1) \times X(1) \to \mathbb{P}^1 \times \mathbb{P}^1 \hookrightarrow \mathbb{P}^3. \tag{2.1.1}$$

To be precise, the map ι sends t to

$$(E_t, E'_t) \mapsto (j(E_t), j(E'_t)) \mapsto (j(E_t)j(E'_t); j(E_t); j(E'_t); 1).$$

Degrees and heights are computed with respect to this fixed embedding. We prove the following theorem:

Theorem 2.1.1. *Let K be a number field of degree d_K. let C be a rational curve over K isomorphic to $\mathbb{P}^1$ which parametrizes a one-dimensional family of pairs of elliptic curves (E, E'). Let (E_t, E'_t) be the generic fiber of this family over $K(t)$, and suppose that there exists no $\overline{K(t)}$-isogeny between E_t and E'_t. Let $d = \deg \iota^* \mathcal{O}_{\mathbb{P}^3}(1)$ be the degree of the parameter family C defined with respect to ι. Let $H(\iota)$ be the height of ι defined by the projective height of the coefficients of the defining polynomials of $j(E_t)$ and $j(E'_t)$.*

Let $H : C(K) \to \mathbb{R}$ be the projective height defined over K. Define $S(B)$ to be the set

$$S(B) = \{t \in C(K) | H(t) \leq B, \text{ there is an } \overline{\mathbb{Q}}\text{-isogeny between } E_t \text{ and } E'_t\}.$$

There is an absolute constant M such that for any $B \geq M$, we have

$$|S(B)| \lesssim_K d^{4+\epsilon}(\log H(\iota) + \log B)^6.$$

Definition 2.1.2. For a point $P_t \in C$ parametrized by $t \in K$, define the height $H(P_t)$ to be the projective height of $\iota(P_t) \in \mathbb{P}^3$.

Note that in Theorem 3.1.1, $H(t)$ is the height of t as an element of K. If we change the definition of the height from $H(t)$ to $H(P_t)$ and assume that $H(P_t) \leq B$, then we get an *uniform* bound on the number of points t such that E_t and E'_t are geometrically isogenous. Moreover, this uniform bound only depends on K, the height B, and the degree of the family.

Theorem 2.1.3. *Assume the same hypothesis as in Theorem 3.1.1. Let $S'(B)$ be the set*

$$S'(B) = \{t \in C(K) | H(P_t) \leq B, \text{ there is an } \overline{\mathbb{Q}}\text{-isogeny between } E_t \text{ and } E'_t\}.$$

Then we have

$$|S'(B)| \lesssim_K d^4(\log B)^6.$$

Relations with Unlikely Intersections

Although Theorem 2.1.1 indicates the sparsity of isogeny between elliptic curves in a family, one should emphasize that this is not an unlikely intersection problem on its own. There are infinitely many $t \in \overline{\mathbb{Q}}$ such that E_t and E'_t are isogenous! However, since we are working over a fixed number field K, this number has to be finite. Nevertheless, one may consider questions in more generalized settings.

Let S be a GSpin Shimura variety and denote by $\{Z_i\}_i$ a sequence of special divisors on S. Let $C \hookrightarrow S$ be a curve whose generic fiber has *maximal monodromy.*

Definition 2.1.4. Define the set $Z(C)$ to be the intersection of C with the infinite union of the special divisors

$$Z(C) = C \cap \bigcup_i Z_i.$$

If C is a curve over $\mathbb{C}$, then the set $Z(C)$ is infinite, which is a classical result dating back to the 1980s. In the work [15], Maulik, Shankar, and Tang proved a similar result for curves C over $\overline{\mathbb{F}}_p$. The result also holds if $C = \operatorname{Spec} \mathcal{O}_K$ where K is a number field, as proved by Shankar-Shankar-Tang-Tayou in [25].

Since $X(1) \times X(1)$ is a GSpin Shimura variety, one can take the special divisors to be $Z_n = Y_0(n)$, which parametrizes n-isogenous pairs of elliptic curves. Our Theorem 2.1.3 can be reformulated as follows:

Theorem 2.1.5. *Let K be a number field of degree d_K. Let $C \in X(1) \times X(1)$ be a rational curve defined over K parametrizing a family of non-isotrivial and generically non-isogenous elliptic curves. Let d be the projective degree of C defined by ι. For a positive integer B define the set $Z(C;B)$ to be the set of K-valued points on C such that*

$$Z(C;B) = \{x \in Z(C) \mid H(\iota(x)) \leq B\}.$$

We have

$$|Z(C;B)| \lesssim_K d^4 (\log B)^6.$$

The discussion above suggests the following question (which we do not claim to know the answer to):

Question: Suppose C is a curve defined over $\overline{\mathbb{Q}}$ and let $Z(C;B)$ denote the set of $\overline{\mathbb{Q}}$-valued points in $Z(C)$ whose absolute height is bounded above by B. One may ask if $Z(C;B)$ is finite. If this is the case, can we get an upper bound in terms of the bounded height B?

Non-simple abelian varieties in a family

Theorem 3.1.1 can be considered as a generalization of the results from Ellenberg, Elsholtz, Hall, and Kowalski. In work in progress, we hope to generalize their main results [10, Theorem A, Theorem B] to any family of abelian varieties parametrized by an irreducible rational curve. To be explicit, let $X \in \mathcal{A}_g/\mathbb{Q}$ be a curve that parametrizes a 1-dimensional family of abelian varieties where we denote by A_x the fiber of this family over $x \in X$. Let d be the projective degree of X. We aim to obtain a uniform bound for the number of $x \in X(\mathbb{Q})$ such that A_x is geometrically non-simple, using a method similar to what we use in this article. By contrast, all upper bounds for the number of non-simple fibers studied in previous literature depend on X, and a uniform upper bound that does not depend on X would follow inexplicitly from Lang's conjecture via the result of Caporaso-Harris-Mazur [5], as explained in [10].

Organization of the paper. In §2, we recall the notion of heights on projective spaces, Hecke correspondence, the modular diagonal quotient surfaces, and some results on the dimension growth conjectures, which we will use later. In §3, we interpret the counting problem into counting rational points on projective curves with certain level structures and construct 'nice' Galois covers that capture the information of being isogenous. In §4, we construct certain projective embeddings with respect to the covers in §3, such that the dimension growth conjecture applies. In §5, we give an upper bound on the change of heights between covers so that one can bound the height of the lifting points. Finally, we prove Theorem 3.1.1 and Theorem 2.1.3 in §6.

2.2 Preliminaries

This section introduces the notations, definitions, and geometric objects for future use. Also, we recall some results in arithmetic geometry, primarily a result of the dimension growth conjectures, that play an essential role in our proofs.

Let C be a rational curve over K isomorphic to $\mathbb{P}^1$ parametrizing a one-dimensional family of pairs of elliptic curves, and let (E_t, E_t') be the generic fiber of this family over $K(t)$, with the assumption that there exists no isogeny between E_t and E_t'. Without loss of generality, one may write E_t and E_t' in the Weierstrass form

$$E_t : y^2 = x^3 + f(t)x + g(t) \tag{2.2.1}$$

$$E_t' : y^2 = x^3 + f'(t)x + g'(t) \tag{2.2.2}$$

where $f(t)$, $g(t)$, $f'(t)$ and $g'(t)$ are rational functions over K. Therefore, the j-invariants of E_t and E_t', denoted by $j(E_t)$ and $j(E')$, are also rational functions.

2.1. **Heights of points.** For a rational point $a \in K$, define the height $H(a)$ of a to be

$$H(a) := \prod_{v \in M_K} \max\{1, |a|_v\}^{\frac{n_v}{[K:\mathbb{Q}]}}$$

where $n_v = [K_v : \mathbb{Q}_v]$.

The height of a K-rational point $P \in \mathbb{P}^n$ with homogeneous coordinates $P = (x_0, \cdots, x_n)$ is defined to be

$$H(P) = \prod_{v \in M_K} \max\{|x_0|_v, \cdots, |x_n|_v\}^{\frac{n_v}{[K:\mathbb{Q}]}}$$

where $n_v = [K_v : \mathbb{Q}_v]$. Recall that we define ι to be the map obtained via the j-invariant and via the Segre embedding in $\mathbb{P}^3$, see (2.1.1).

Recall the definition of $H(P_t)$ in Definition 2.1.2. The following lemma indicates that

$$H(P_t) = H(j(E_t))H(j(E_t')).$$

Lemma 2.2.1. *Let σ_n be the Segre embedding of n-copies of $\mathbb{P}^1$*

$$\sigma_n \colon \underbrace{\mathbb{P}^1 \times \mathbb{P}^1 \times \ldots \times \mathbb{P}^1}_{n\text{-}times} \hookrightarrow \mathbb{P}^{2^n - 1}$$

such that for a point $(x_1, \cdots, x_n) \in \mathbb{P}^1 \times \cdots \times \mathbb{P}^1$

$$\sigma_n(x_1, \cdots, x_n) = (\prod_{1 \le i \le n} x_i, \prod_{i_1 < i_2 < \cdots < i_{n-1}} x_{i_1} \cdots x_{i_{n-1}}, \ldots, x_1, \ldots, x_n, 1).$$

Let $H(.)$ be the projective height defined above. We have

$$H(\sigma_n(x_1, \cdots, x_n)) = H(x_1) \cdots H(x_n).$$

Proof. By definition of the projective height,

$$H(\sigma_n(x_1, \cdots, x_n)) = \prod_{v \in M_K} \max\{|\prod_{1 \leq i \leq n} x_i|_v, \cdots, |x_1|_v, \cdots, |x_n|_v, 1\}^{\frac{n_v}{[K:\mathbb{Q}]}}$$

and

$$H(x_1) \cdots H(x_n) = \prod_{v \in M_K} \{\max\{1, |x_1|_v\} \cdots \max\{1, |x_n|_v\}\}^{\frac{n_v}{[K:\mathbb{Q}]}}.$$

A direct observation shows that for each $v \in M_K$,

$$\max\{|\prod_{1 \leq i \leq n} x_i|_v, \cdots, |x_1|_v, \cdots, |x_n|_v, 1\} = \max\{1, |x_1|_v\} \cdots \max\{1, |x_n|_v\}.$$

□

2.2. **The modular diagonal quotient surfaces.** Later in this article, we will define the modular surface $X_{\tilde{H}_\Delta}(m)$ (see (2.3.1)) that lies in a special family, called the *modular diagonal quotient surfaces*, which arise naturally as the (coarse) moduli space to the moduli problem that classifies isomorphisms between mod m Galois representations attached to pairs of elliptic curves E/K.

The modular curve $X(m)$ is a Galois cover of $X(1)$ with Galois group

$$G = SL_2(\mathbb{Z}/m\mathbb{Z})/\{\pm 1\}.$$

Let ϵ be an element in $(\mathbb{Z}/m\mathbb{Z})^\times$. Let α_ϵ be the automorphism of G defined by conjugation with $Q_\epsilon = \left(\begin{smallmatrix} \epsilon & 0 \\ 0 & 1 \end{smallmatrix}\right)$, i.e. $\alpha_\epsilon(g) = Q_\epsilon g Q_\epsilon^{-1}$. The product surface $X(m) \times X(m)$ carries an action of the twisted diagonal subgroup of $SL_2(\mathbb{Z}/m\mathbb{Z}) \times SL_2(\mathbb{Z}/m\mathbb{Z})$ defined by

$$\alpha_\epsilon : \Delta_\epsilon = \{(g, \alpha_\epsilon(g)) : g \in G\}.$$

Definition 2.2.2. The twisted diagonal quotient surface defined by α_ϵ is the quotient surface $X_\epsilon := \Delta_\epsilon \backslash X(m) \times X(m)$ obtained by the action of Δ_ϵ.

X_ϵ can be viewed as the moduli space of the triple (E_1, E_2, Q), where

$$Q : E_1[p] \overset{\sim}{\to} E_2[p]$$

multiplies the Weil pairing by ϵ.

The modular diagonal quotient surfaces and their modular interpretation are widely used in studying Mazur's question[16] [11], Frey's conjecture[**Fre97**], and so on.

2.3. **Uniform bound for points of bounded height on curves.**

Let X be an irreducible projective curve defined over a number field K with a degree d embedding into $\mathbb{P}^n$. Denote by $N(X,B)$ the set of K-rational points on $X \subseteq \mathbb{P}^n$ of projective heights at most B. Heath-Brown proved a uniform bound for rational points on a curve X with bounded height in [13, Theorem 5], which addresses that

$$N(X,B) \leq O_\epsilon(B^{2/d+\epsilon}).$$

The result on irreducible projective curves with the removal of the term B^ϵ without needing $\log B$ was proved by Walsh in [28], using a combination of the determinant method based on the p-adic approximation introduced by Heath-Brown [13] with the method due to Ellenberg and Venkatesh in [9]. The uniform upper bound on $N(X,B)$ with an explicit term of polynomial growth depends on d was proved by Castryck, Cluckers, Dittmann, and Nguyen [6]:

Theorem 2.2.3. *[6, Theorem 2] Given $n \geq 1$, there exists a constant $c = c(n)$ such that for all $d > 0$ and all integral projective curves $X \in \mathbb{P}^n_{\mathbb{Q}}$ of degree d and all $B \geq 1$ one has*

$$|N(X,B)| \leq cd^4B^{2/d}.$$

A year later, Paredes and Sasyk [19] extended the work of Castryck, Cluckers, Dittmann, and Nguyen to give uniform estimates for the number of rational points of bounded height on projective varieties defined over global fields. More precisely, they proved the following extension of [6, Theorem 2] to global fields.

Theorem 2.2.4. *[19, Theorem 1.8] Let K be a global field of degree d_K. Let H be the absolute projective multiplicative height. For any integral projective curve $C \subseteq \mathbb{P}^N_K$ of degree d it holds*

$$|\{\boldsymbol{x} \in C(K) : H(\boldsymbol{x}) \leq B\}| \lesssim_{K,N} \begin{cases} d^4 B^{\frac{2d_K}{d}} & \textit{if } K \textit{ is a number field,} \\ d^8 B^{\frac{2d_K}{d}} & \textit{if } K \textit{ is a function field.} \end{cases}$$

We will discuss this result in section §6, where we apply it.

2.3 Construct Galois Covering with Level Structures

In this section, we construct 'nice' Galois coverings of $X(1) \times X(1)$ with level structures. To be precise, for a large enough rational prime m, these are quotients of $X(m) \times X(m)$ by certain kinds of subgroups of $SL_2(\mathbb{Z}/m\mathbb{Z}) \times SL_2(\mathbb{Z}/m\mathbb{Z})$, with the property that one can lift a point $t \in S(B)$ to one of the quotients. In other words, the Galois coverings capture points that parametrize isogenous pairs (E_t, E_t') in the family. The main theorem in this section is Lemma 2.3.11.

We assume that m is a rational prime such that $m \geq M' = \max\{17, M_1\}$ for some absolute integer M_1 defined in Theorem 2.3.4. Also we want m to be a prime between $2(\log(d+1) + \log H(\iota) + \log B)^{\frac{1}{2}}$ and $4(\log(d+1) + \log H(\iota) + \log B)^{\frac{1}{2}}$ once we fix B, which we will make precise in §6. This condition implies that we need to assume $4(\log(d+1) + \log H(\iota) + \log B)^{\frac{1}{2}} \geq M'$ and thus we can always assume B is greater than the absolute integer $M = e^{(\frac{M'}{4})^2}$ to make everything go through. Let $X(m) \times X(m)$ be the surface parametrizing 4-tuples (E, E', ϕ, ϕ'), where E_t and E_t' are elliptic curves and ϕ, ϕ' are m-level structures, i.e.

$$\phi : E[m] \to (\mathbb{Z}/m\mathbb{Z})^2, \phi' : E'[m] \to (\mathbb{Z}/m\mathbb{Z})^2$$

are isomorphisms of group schemes preserving the Weil pairing. Let H be a subgroup of $SL_2(\mathbb{Z}/m\mathbb{Z}) \times SL_2(\mathbb{Z}/m\mathbb{Z})$ and define X_H to be the quotient

$$X_H := (X(m) \times X(m))/H. \tag{2.3.1}$$

p-torsion monodromy representations and the lifting criterion. Let E be an elliptic curve over a number field K and let p be a prime. Denote by

$$\rho_{E,p} : G_K \to \mathrm{Aut}(E[p])$$

the p-torsion Galois representation associated to the p-torsion points $E[p]$ of the elliptic curve E. It is a standard fact that the elliptic curve E/K admits an isogeny of degree p defined over K if and only if the image $\rho_{E,p}\left(G_K\right)$ is contained in a Borel subgroup of $\mathrm{Aut}(E[p])$. If E/K and E'/K are related by an isogeny over K of degree coprime to p, then this isogeny induces a G_K-module isomorphism $E[p] \simeq E'[p]$, which identifies the images $\rho_{E,p}\left(G_K\right)$ and $\rho_{E',p}(G_K)$ up to change of basis. See [21] for an explicit description of the images of p-torsion Galois representations attached to the product of two isogenous elliptic curves with an isogeny of degree p.

Definition 2.3.1. Define H_Δ to be the image of the diagonal map

$$\Delta : SL_2(\mathbb{Z}/m\mathbb{Z}) \to SL_2(\mathbb{Z}/m\mathbb{Z}) \times SL_2(\mathbb{Z}/m\mathbb{Z}).$$

We will prove, in Proposition 2.3.7, that there exists an isogeny $\phi_t : E_t \to E'_t$ defined over $\overline{\mathbb{Q}}$ if and only if the monodromy of the p-torsion Galois representation on $E_t[p] \times E'_t[p]$ is contained in a group $\tilde{H}_\Delta$, which contains H_Δ as an index 2 subgroup for all but finitely many p.

Remark 2.3.2. It is a classical result that for elliptic curves defined over a number field K, there are finitely many j-invariants with complex multiplication in K. Denote this number by $C(K)$. We need to bound the number of points P_t on C whose j-invariant lies in this set. There are at most $C(K)^2$ points $P_t \in C$ such that $\iota(P_t) = (j(E_t), j(E'_t))$ contains CM j-invariants. Therefore in our setting, we can discard them and focus on pairs of elliptic curves without complex multiplication.

Lemma 2.3.3. *Let E_1 and E_2 be two elliptic curves without complex multiplication over a number field K. If there exists an isogeny $\phi : E_1 \to E_2$ defined over K then the p-torsion Galois representation of $E_1 \times E_2$*

$$\mathrm{Gal}(\bar{K}/K) \to GL_2(\mathbb{F}_p) \times GL_2(\mathbb{F}_p)$$

has image conjugate to H_Δ for primes p not dividing the degree of ϕ.

Proof. First, by Serre's open image theorem, the p-torsionGalois representation of each factor

$$\mathrm{Gal}(\bar{K}) \to GL_2(\mathbb{F}_p)$$

is surjective for all large enough primes p.

Suppose E_1/K and E_2/K are related by an isogeny over K of degree d, then for all primes $p \nmid d$ this isogeny induces a G_K-module isomorphism from $E_1[p]$ to $E_2[p]$, which identifies the images $\rho_{E_1,p}(G_K)$ and $\rho_{E_2,p}(G_K)$. The lemma follows.

□

Note that Lemma 2.3.3 is a result of pairs of elliptic curves over number fields. Later in the proof of Proposition 2.4.9, we need to use the result over the function field $K(t)$ that classifies elliptic curves up to isogeny by their p-torsion Galois representations. We present a beautiful theorem by Bakker and Tsimerman [3, Theorem 1].

Theorem 2.3.4. *Let k be an algebraically closed field of characteristic 0. For any $N > 0$, there exists $M_N > 0$ such that for any prime $p > M_N$ and any smooth quasi-projective curve U of gonality $n < N$, non-isotrivial elliptic curves $\mathcal{E}$ over U are classified up to isogeny by their p-torsion local system $\mathcal{E}[p]$.*

Definition 2.3.5. Let $\tilde{H}_\Delta$ be the maximal subgroup of $SL_2(\mathbb{Z}/m\mathbb{Z}) \times SL_2(\mathbb{Z}/m\mathbb{Z})$ that contains H_Δ as an index 2 subgroup.

The following lemma, together with the fact that if F is a field with more than 5 elements then the only proper normal subgroup of $SL_2(F)$ is the group $\{\pm 1\}$, proves that $\tilde{H}_\Delta$ is the unique proper subgroup of $SL_2(\mathbb{Z}/m\mathbb{Z}) \times SL_2(\mathbb{Z}/m\mathbb{Z})$ that contains H_Δ as an index 2 subgroup.

Lemma 2.3.6. *Let A be a group and let $G = A \times A$. Define $\Delta = \{(a,a) \mid a \in A\}$ as the diagonal subgroup of G. If $\Delta \leq H \leq G$ then there exists a normal subgroup N of A such that $H = \{(g,h) \in G \mid gh^{-1} \in N\}$.*

Proof. Let $N = \{h \in A \mid (h,1) \in H\}$ be a subgroup of G. We claim that N is the desired normal subgroup. Indeed, for any $a \in A$ and $(h,1) \in H$, we have $(aha^{-1},1) = (a,a)(h,1)(a^{-1},a^{-1}) \in H$, therefore N is a normal subgroup of A.

For any $a, a' \in A$, we have $(aa'^{-1}, 1)(a', a') = (a, a')$. Therefore $(a, a') \in H$ is and only if $(aa'^{-1}, 1) \in H$, if and only if $aa'^{-1} \in A$ by the definition of A. □

Proposition 2.3.7. *Let E_1 and E_2 be elliptic curves without complex multiplication over $\mathbb{Q}$. There exists an isogeny $\phi : E_1 \to E_2$ defined over $\overline{\mathbb{Q}}$ if and only if the p-torsion Galois representation*

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}_p) \times GL_2(\mathbb{F}_p)$$

has image contained $\tilde{H}_\Delta$, for all primes p not dividing the degree of ϕ.

Proof. We need the following lemma:

Lemma 2.3.8. *Let E_1, E_2 be elliptic curves without complex multiplication defined over a number field K. If E_1 and E_2 are isogenous over $\overline{\mathbb{Q}}$ then there exists a quadratic twist of E_2 that is isogenous to E_1 over K.*

Suppose there exists an isogeny $\varphi : E_1 \to E_2$ over $\overline{\mathbb{Q}}$ then by Lemma 2.3.8 and Lemma 2.3.3, there is a quadratic extension L/K such that G_L has diagonal image in $GL_2(\mathbb{F}_p) \times GL_2(\mathbb{F}_p)$. Therefore the image of G_K is contained in a subgroup of $GL_2(\mathbb{F}_p) \times GL_2(\mathbb{F}_p)$ which contains H_Δ as an index 2 subgroup. For the other direction, we take the preimage of the H_Δ, which can be written in the form G_F for some number field F, that is quadratic over K. By Proposition 2.19, there is an isogeny $\varphi : E_1 \to E_2$ defined over F which completes the proof.

□

Proof of Lemma 2.3.8. Let $\varphi : E_1 \to E_2$ be an isogeny over $\overline{\mathbb{Q}}$ and $G_{\overline{Q}/K} = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. For every $g \in G_{\overline{Q}/K}$, $\varphi^g = [\alpha(g)] \circ \varphi$ is another isogeny $E_1 \to E_2$ of the same degree as φ. Here we define $\alpha : G_{\overline{Q}/K} \to \mathbb{R}$ be a character on $G_{\overline{Q}/K}$. Since for all elliptic curves without complex multiplication over $\overline{\mathbb{Q}}$, there exists a cyclic isogeny $\varphi : E_1 \to E_2$ up to sign and all other isogenies ψ from E_1 to E_2 can be written as $\psi = \varphi \circ [m]$ for some integer m, we have $\alpha(g) = \pm 1$. Hence $\alpha(g)$ is a quadratic character and there exists $d \in K^*$ such that $\alpha(g) = g(\sqrt{d})/\sqrt{d}$. Thus the quadratic twist of E_2 by d is the desired twist.

□

Definition 2.3.9. Let $H_\mathrm{p} := H_1 \times H_2$, where H_1 and H_2 (possibly $H_1 = H_2$) are maximal parabolic subgroups of $SL_2(\mathbb{Z}/m\mathbb{Z})$.

Remark 2.3.10. All maximal parabolic subgroups of $SL_2(\mathbb{Z}/m\mathbb{Z})$ are in the same conjugacy class. Therefore the covers constructed in this way are all isomorphic to each other. If $t \in S(B)$ lifts to one, it lifts to all.

Lemma 2.3.11. *Any rational point $t \in S(B)$ for some B admits a lifting to one of the congruence covers: $X_{\tilde{H}_\Delta}(K)$ or $X_{H_p}(K)$.*

Proof. By the argument above, when there is a K-isogeny of degree $m \nmid d$, it induces a G_K-isomorphism $E_t[m] \simeq E'_t[m]$ which implies an isomorphism of the mod m Galois images, up to a change of basis given by conjugating by an element $(1, g) \in SL_2(\mathbb{Z}/m\mathbb{Z})$. Applying Proposition 2.3.7, we get the conclusion that if m does not divide the degree of the isogeny, the Galois image lies in $\tilde{H}_\Delta$. As for the rest of the lemma, when $d = m$, we have the Galois image of the m-torsion monodromy representation of both E_1 and E_2 contained in a Borel subgroup of $SL_2(\mathbb{Z}/m\mathbb{Z})$. Since any Borel subgroup is maximal parabolic in $SL_2(\mathbb{Z}/m\mathbb{Z})$, this proves lemma 2.3.11. □

2.4 Geometric Interpretation and Projective Embeddings

In this section, we explore the geometric interpretation of the question and construct projective embeddings, which allow us to transform the question into counting rational points with bounded height in projective spaces.

Definition 2.4.1. Let H be a subgroup of $SL_2(\mathbb{Z}/m\mathbb{Z}) \times SL_2(\mathbb{Z}/m\mathbb{Z})$ such that H is either $\tilde{H}_\Delta$ or H_p. Define C_H to be the lifting of C to the modular surface $X_H := X(m) \times X(m)/H$, which is given by the pullback of the following diagram.

$$\begin{tikzcd} C_H \arrow[r] \arrow[d] & X_H \arrow[d] \\ C \arrow[r] & X(1) \times X(1) \end{tikzcd}$$

2.4.1 The curve C_H is integral

In order to apply the result by Paredes and Sasyk, we need to prove that the lifting C_H of C is integral for large enough m. We need the following Goursat's lemma:

Lemma 2.4.2. *[12, Theorem 5.5.1] Let G and H be groups, and let K be a subdirect product of G and H; that is, $K \leq G \times H$, and $\pi_G(K) = G, \pi_H(K) = H$, where π_G and π_K are the projections onto the first and second factor, respectively from $G \times H$. Let $N_1 = K \cap \ker(\pi_G)$ and $N_2 = K \cap \ker(\pi_H)$. Then N_2 can be identified with a normal subgroup N_G of G, N_1 can be identified with a normal subgroup N_H of H, and the image of K in $G/N_G \times H/N_H$ is the graph of an isomorphism $G/N_G \cong H/N_H$.*

Proof. See [12, Theorem 5.5.1].

□

Also, we prove the following proposition:

Proposition 2.4.3. *For all $m \geq 17$, the Galois image of the p-torsion monodromy representation of $E_t[m]$ and $E_t'[m]$ in the generic fiber is $SL_2(\mathbb{Z}/m\mathbb{Z})$.*

Proof. Suppose the Galois image of the m-torsion monodromy representation is some proper subgroup G of $SL_2(\mathbb{Z}/m\mathbb{Z})$. Then we have a dominant map $f : C \to X(m)/G$. Since the genus of C is zero, this implies that the genus of the modular curve $X(m)/G$ is zero.

Let $\mathcal{N}(m)$ be the quantity such that

$$\mathcal{N}(m) := \min\{\text{genus}(X(m)/G) \mid G \subsetneq SL_2(\mathbb{Z}/m\mathbb{Z}),\ G \text{ maximal}\}.$$

Cojocaru and Hall proved the genus formula for $X(m)/G$ for all possible maximal subgroup G of $SL_2(\mathbb{Z}/m\mathbb{Z})$, which is summarized in a table [7, Table 2.1]. Moreover, they proved that

$$\mathcal{N}(m) = \frac{1}{12}\left[m - (6 + 3\mathrm{e}_2 + 4\mathrm{e}_3)\right] > 0$$

for $m \geq 17$. The proposition follows. □

Now we are ready to prove that C_H is irreducible. This follows as a consequence of Proposition 2.4.3:

Lemma 2.4.4. *For each choice of H, the curve C_H is integral.*

Proof. We have the covering map $q_{\tilde{U}} : \tilde{U} \to U$ where U is the connected dense open subset of C parametrizing smooth points. Later in the proof of Proposition 2.4.9, we showed that the Galois image of the m-torsion monodromy representation of $\pi_1(U)$ is the full group $SL_2(\mathbb{Z}/m\mathbb{Z}) \times SL_2(\mathbb{Z}/m\mathbb{Z})$, by using Proposition 2.4.3 and Lemma 2.4.2. Therefore the monodromy of $\pi_1(U)$ acts transitively on the right cosets $SL_2(\mathbb{Z}/m\mathbb{Z}) \times SL_2(\mathbb{Z}/m\mathbb{Z})/H$, which implies that the cover C_H is connected for both $H = \tilde{H}_\Delta$ and $H = H_{\mathrm{p}}$. The lemma follows by the fact that the quotient space of a connected space is connected.

□

2.4.2 Construct projective embeddings

In this subsection, we give an explicit construction of projective embeddings of C_H, denoted by ι_H. We make the following diagram commute for each case's choice of $N \in \mathbb{Z}$. Here the rational map $\mathbb{P}^N \dashrightarrow \mathbb{P}^3$ is a projection of coordinates of $\mathbb{P}^N$.

$$\begin{tikzcd} C_H \arrow[r, hook, "\iota_H"] \arrow[d, "q"'] & \mathbb{P}^N \arrow[d, dotted] \\ C \arrow[r, hook] & \mathbb{P}^3. \end{tikzcd} \tag{2.4.1}$$

Case I: The modular diagonal quotient surfaces.

Recall the definition of the modular diagonal quotient surfaces in §2.4. In our case where $\epsilon = 1$, $X_{H_\Delta}(m)(K)$ has the moduli interpretation that it is the set of isomorphism classes of triples (E_1, E_2, ψ), where E_1, E_2 are elliptic curves over K and $\psi : E_1[m] \overset{\sim}{\to} E_2[m]$ is an isomorphism of the m-torsion subgroups of the elliptic curves which preserves the Weil pairing. Let t be a rational point of $C(K)$ such that there exists a point $(E_t, E'_t, \psi : E_t[m] \overset{\sim}{\to} E'_t[m])$ which is a point of $X_{H_\Delta}(m)(K)$. One may notice that it is not obvious that $C_{\tilde{H}_\Delta}$ is connected, and we will address this point in Lemma 2.4.4.

We now define some functions on $C_{\tilde{H}_\Delta}$ in order to apply the result from [6] and to bound the number of points on $C_{\tilde{H}_\Delta}$.

For a fixed $t \in K$, there is a list of elliptic curves isogenous to E_t through cyclic isogenies of degree m given by the list of cyclic subgroups of $E_t[m]$, say

$$E_{t,1}, \cdots, E_{t,m+1}.$$

Similarly we have a list of m-cyclic subgroups of $E'_t[m]$ parametrizing the m-cyclic isogenies of E'_t, with the corresponding list of elliptic curves isogenous to E'_t:

$$E'_{t,1}, \cdots, E'_{t,m+1}.$$

Remark 2.4.5. These isogenies will most likely *not* be defined over K unless $E_t[m]$ or $E'_t[m]$ has a rational cyclic subgroup. Even then, most of them will not be defined over K.

For each point (E_t, E'_t, ψ) on $\tilde{C}$, we have $m+1$ cyclic subgroups of $E_t[m]$ and $m+1$ cyclic subgroups of $E'_t[m]$ which can be placed in natural bijection with each other under ψ. We can re-order the lists for E'_t such that $E_{t,1}$ is in correspondence with $E'_{t,1}$ and so on.

Definition 2.4.6. Let F be a function defined on $X_{\tilde{H}_\Delta}$ given by

$$F(E_t, E'_t, \psi) = j(E_{t,1})j(E'_{t,1}) + \cdots + j(E_{t,m+1})j(E'_{t,m+1}).$$

Lemma 2.4.7. *F is defined over $\mathbb{Q}$. Moreover, F is an element of the function field $\mathbb{Q}(X_{\tilde{H}_\Delta})$.*

Proof. For any $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $t \in \overline{\mathbb{Q}}$, denote by (t, ψ) one of the preimages on $X_{\tilde{H}_\Delta}$.

$$F((t,\psi)^g) = \Sigma_{i=1}^{m+1} j(E_{t^g,i})j(E'_{t^g,i}) = \Sigma_{i=1}^{m+1}(j(E_{t,i})j(E'_{t,i}))^g.$$

The second equality holds since $\psi^g = \psi$ and for an arbitrary $1 \leq i \leq m+1$, there is a unique k such that

$$(j(E_{t,i}))^g = j(E_{t,k})$$

and once we fix i, it is also true that

$$(j(E'_{t,i}))^g = j(E'_{t,k})$$

for the same k.

□

Definition 2.4.8. Define $\iota'_{\tilde{H}_\Delta} : C_{\tilde{H}_\Delta} \to \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ to be the function given by

$$\iota'_{\tilde{H}_\Delta}((E_t, E'_t, \psi)) = (F(E_t, E'_t, \psi), j(E_t), j(E'_t)).$$

Proposition 2.4.9. *For $m \geq 17$, $\iota'_{\tilde{H}_\Delta}$ is generically an embedding of $C_{\tilde{H}_\Delta}$ into $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$. This is equivalent to saying that the subfield $M \subset K(C_{\tilde{H}_\Delta})$ generated by $j(E_t)$, $j(E'_t)$ and F is the whole function field.*

The proof of Proposition 2.4.9 splits into two parts. The first part is to show that M is not contained in $K(C)$. The second part is to show there is no intermediate extension between $K(C)$ and $K(C_{\tilde{H}_\Delta})$, so that $K(C) \subseteq M \subseteq K(C_{\tilde{H}_\Delta})$ and $M \neq K(C)$ implies $M = K(C_{\tilde{H}_\Delta})$.

First, we present some representation theoretical lemma which we will use later. Let G be a finite group and let V and V' be permutation representations of G of the same dimension, such that G acts 2-transitively on some finite sets by V and V'. It is a standard fact that the corresponding representation V(resp. V') is the direct sum of the trivial representation and an irreducible representation whose coordinates sum to 0. Denote the irreducible representation by V_0(resp. V'_0). We prove that if $v \in V$, $v' \in V'$ such that $\langle v, v' \rangle = \langle v, (v')^g \rangle$ for any $g \in G$, then either v or v' is fixed by G. We first prove the following lemma.

Lemma 2.4.10. *If $v \in V$ (resp. $v' \in V'$) is not in the trivial representation generated by $[1, \cdots, 1]^T$, the set $\{v - v^g\}$(resp. $\{v' - (v')^g\}$), as g ranges over G, span the space of all vectors in V_0(resp. V'_0).*

Proof. Let W_v(resp. W'_v) be the subspace Span$\{v - v^g\}$(resp. Span$\{(v') - (v')^g\}$) as g ranges over G. We claim that W_v is a sub-representation of V_0, the irreducible representation of the permutation representation given by the condition that the sum of the coordinates equals 0. Indeed, for any $v \in W_v$, $\sigma, \tau \in G$, one have

$$(v - v^\sigma)^\tau = v^\tau - v^{\sigma\tau} = (v - v^{\sigma\tau}) - (v - v^\tau).$$

The lemma follows from the face that V_0(resp. V'_0) is irreducible. □

Lemma 2.4.11. *If $v \in V$, $v' \in V'$ such that $\langle v, v' \rangle = \langle v, (v')^g \rangle$ for any $g \in G$, then either v or v' is fixed by G.*

Proof. If $\langle v, v' \rangle = \langle v, (v')^g \rangle$ for all $g \in G$, then

$$\langle v, (v') - (v')^\gamma \rangle = 0$$

for all $g \in G$.

If $W_{v'} = 0$, then $v' = (v')^g$ for any $g \in G$ thus v' is fixed by G. If $W_{v'} \neq 0$, by lemma 2.4.10, $v' - (v')^g$ span the space V'_0 which is the orthogonal complement of the trivial representation. Therefore

$$v \in W_{v'}^\perp = \mathbb{C}\langle [1, \cdots, 1]^T \rangle,$$

thus fixed by G.

□

Now we apply Lemma 2.4.11 to the case where $G = SL_2(\mathbb{Z}/m\mathbb{Z})$ and where V and V' are $m+1$ dimensional representations of $SL_2(\mathbb{Z}/m\mathbb{Z})$ spanned by vectors v_t and v'_t respectively, as t ranges over C. For $t \in C$ such that E_t and E'_t are both non-singular, define v_t and v'_t by

$$v_t = (j(E_{t,1}), \cdots, j(E_{t,m+1})) \tag{2.4.2}$$

$$v'_t = (j(E'_{t,1}), \cdots, j(E'_{t,m+1})). \tag{2.4.3}$$

It is easy to see that V and V' are permutation representations of $SL_2(\mathbb{Z}/m\mathbb{Z})$ by its transitive action on the basis.

Recall the definition of F in 2.4.6. We may also write F as an inner product:

$$F(E_t, E'_t, \psi) = \langle v_t, v'_t \rangle = j(E_{t,1})j(E'_{t,1}) + \cdots + j(E_{t,m+1})j(E'_{t,m+1}).$$

Note that F is defined on $C_{\tilde{H}_\Delta}$ by restriction, but $SL_2(\mathbb{Z}/m\mathbb{Z}) \times SL_2(\mathbb{Z}/m\mathbb{Z})$ does not act on $C_{\tilde{H}_\Delta}$. By Lemma 2.4.4 $C_{\tilde{H}_\Delta}$ is connected, we define C' as the Galois closure of $C_{\tilde{H}_\Delta}$ over C. This is equivalent to saying that C' is the pullback of C all the way to $X(m) \times X(m)$, see diagram 2.4.4. Therefore the pullback of F to $X(m) \times X(m)$ is a function on C' with $F^\sigma = F$ for all $\sigma \in \tilde{H}_\Delta$. We prove that F is not defined on C.

$$\begin{tikzcd}
C' \arrow[r, hook] \arrow[d] & X(m) \times X(m) \arrow[d] \\
C_{\tilde{H}_\Delta} \arrow[r, hook] \arrow[d] & X(m) \times X(m)/\tilde{H}_\Delta \arrow[d] \\
C \arrow[r, hook] & X(1) \times X(1).
\end{tikzcd} \tag{2.4.4}$$

Lemma 2.4.12. *F is not defined on C.*

Proof. For each $\gamma \in SL_2(\mathbb{Z}/m\mathbb{Z})$, the action of γ on F is given by

$$F(E_t, E'_t, \psi)^\gamma = \langle v_t, (v'_t)^\gamma \rangle.$$

If F is defined on C, then for every $\gamma \in SL_2(\mathbb{Z}/m\mathbb{Z})$ we have $F^\gamma = F$ therefore $\langle v_t, v'_t \rangle = \langle v_t, (v'_t)^\gamma \rangle$. By Lemma 2.4.11, either v_t or v'_t is fixed by $SL_2(\mathbb{Z}/m\mathbb{Z})$. But this implies either

$$j(E_{t,1}) = \cdots = j(E_{t,m+1})$$

or

$$j(E'_{t,1}) = \cdots = j(E'_{t,m+1}).$$

Since there exists $t \in C$ such that E_t and E'_t are both non-CM elliptic curves, this cannot happen. Therefore F cannot be defined on C.

□

Now we are ready to prove the generic injectivity of ι'_{H_Δ}. We show no intermediate cover exists between $\tilde{C}$ and C by an argument using monodromy.

Proof of Proposition 2.4.9. By lemma 2.4.11, we have the argument that F is not defined on C.

Recall that $C_{\tilde{H}_\Delta}$ is defined to be the cover of C constructed by pulling back $C \to X(1) \times X(1)$ in the previous context. Let $U \subset C$ be the dense open locus parametrizing smooth points, i.e., pairs of genuine elliptic curves. The étale fundamental group $\pi_1(U)$ is a quotient of the absolute Galois group of $K(t)$, which acts on the m-torsion of the generic fiber, say $E_t[m]$ and $E'_t[m]$, in the usual Galois way. Proposition 2.4.3 asserts that for $m \geq 17$, the map

$$\rho_m : \pi_1(U) \to SL_2(\mathbb{Z}/m\mathbb{Z}) \times SL_2(\mathbb{Z}/m\mathbb{Z})$$

is surjective on each of the two factors. Therefore the reduction map

$$\bar{\rho}_m : \pi_1(U) \to PSL_2(\mathbb{Z}/m\mathbb{Z}) \times PSL_2(\mathbb{Z}/m\mathbb{Z})$$

is surjective on each factor. For $m \geq 5$, the projective special linear group $PSL_2(\mathbb{Z}/m\mathbb{Z}) = SL_2(\mathbb{Z}/m\mathbb{Z})/\{\pm 1\}$ is simple. By assumption, the generic fiber E_t and E'_t of the family are not isogenous. Therefore by the work of Bakker and Tsimerman [3, Theorem 1], there exists an absolute constant M_1 such that for any prime $m > M_1$, the image of ρ_m on each of the factors is non-isomorphic. Hence the inequivalence condition in Lemma 2.4.2 is satisfied. Lemma 2.4.2 leads to the conclusion that the Galois image of the m-torsion monodromy representation of $\pi_1(U)$ is full in $PSL_2(\mathbb{Z}/m\mathbb{Z}) \times PSL_2(\mathbb{Z}/m\mathbb{Z})$.

We prove that there is no intermediate cover between $C_{\tilde{H}_\Delta}$ and C. Suppose there is a curve X such that

$$C_{\tilde{H}_\Delta} \to X \to C$$

with all maps of degrees greater than 1. Since the connected covering space of C is in bijection with the subgroups of $\pi_1(C)$, X corresponds to a proper subgroup H' strictly containing $\tilde{H}_\Delta$. However, $\tilde{H}_\Delta$ is a maximal subgroup of $PSL_2(\mathbb{Z}/m\mathbb{Z}) \times PSL_2(\mathbb{Z}/m\mathbb{Z})$, which implies that X is isomorphic to $C_{\tilde{H}_\Delta}$, contradiction. Therefore $C_{\tilde{H}_\Delta}$ is birational to its image under $\iota'_{\tilde{H}_\Delta}$, which proves the proposition. □

We have constructed a generic embedding $\iota'_{\tilde{H}_\Delta}$ of $C_{\tilde{H}_\Delta}$ into a product of projective lines from the argument above. Composing with the Segre embedding, we get a generic embedding of $C_{\tilde{H}_\Delta}$ into $\mathbb{P}^7$, denoted by $\iota_{\tilde{H}_\Delta}$.

$$\iota_{\tilde{H}_\Delta} : C_{\tilde{H}_\Delta} \hookrightarrow \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \hookrightarrow \mathbb{P}^7.$$

One notice that $\iota_{\tilde{H}_\Delta}$ fits into the diagram 2.4.1 at the beginning of this chapter, with $N = 7$.

Case II: the maximal parabolic quotient surfaces. When $H = H_{\mathrm{p}}$ which is a product of maximal parabolic subgroups, the quotient $X(m) \times X(m)/H$ is isomorphic to $X_0(m) \times X_0(m)$. The corresponding projective embedding $\iota_{H_{\mathrm{p}}}$ can be constructed in the context of Hecke correspondence of level $SL_2(\mathbb{Z}/m\mathbb{Z})$ followed by the Segre embedding, as following:

$$\iota_{H_{\mathrm{p}}} : X_0(m) \times X_0(m) \hookrightarrow \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \hookrightarrow \mathbb{P}^{15}. \tag{2.4.5}$$

To be explicit, for a point $\tilde{P}_t = (E_t, \tilde{E}_t, E'_t, \tilde{E}'_t)$ that lifts $P_t = (E_t, E'_t)$, where E_t and $\tilde{E}_t$ are linked by a cyclic isogeny of degree m and same for E'_t and $\tilde{E}'_t$, one may write $\iota_{H_{\mathrm{p}}}$ as

$$\begin{aligned}\iota_{H_{\mathrm{p}}} : (E_t, \tilde{E}_t, E'_t, \tilde{E}'_t) &\mapsto j(E_t) \times j(\tilde{E}_t) \times j(E'_t) \times j(\tilde{E}'_t) \\ &\mapsto (j(E_t)j(\tilde{E}_t)j(E'_t)j(\tilde{E}'_t); \cdots ; j(E_t); j(\tilde{E}_t); j(E'_t); j(\tilde{E}'_t); 1).\end{aligned}$$

In this case, we choose $N = 15$ in diagram 2.4.1.

2.5 Bound for the Change of Heights

In this section, we give an upper bound on the height of a point in $C_H(K)$ lying over a point $P_t \in C(K)$, in terms of the height $H(t)$ and the level m. The main theorem of this section is Proposition 2.5.4.

5.1. **Hecke correspondence and modular polynomials.** Modular polynomials of elliptic curves, the so-called 'elliptic modular polynomials,' are the most common and simplest examples of modular equations. For a positive integer m, the classical modular polynomial Φ_m is the minimal polynomial of $j(mz)$ over $\mathbb{C}(j)$. In other words we have $\Phi_m(j(mz), j(z)) = 0$. The bivariate polynomial $\Phi_m(X, Y)$ is symmetric of degree $\psi(m) = m\prod_{p|m}(1 + p^{-1})$ in both variables, and its coefficients grow super-exponentially in m. The modular curve $Y_0(m)$ is birational to its image in $\mathbb{P}^1 \times \mathbb{P}^1$ with Φ_m an equation for this image. The graph of Φ_m describes the Hecke correspondence such that there exists a cyclic isogeny of degree m between projections onto each copy of $\mathbb{P}^1$.

For elliptic curves E_1 and E_2 linked with a cyclic isogeny of order m, we aim to find an upper bound for the height $H(j(E_1))$, in terms of $H(j(E_2))$ and the coefficients of Φ_m. This has been worked out by Pazuki in [20].

Theorem 2.5.1. *[20, Theorem 1.1] Let $\varphi : E_1 \to E_2$ be a $\overline{\mathbb{Q}}$-isogeny between two elliptic curves defined over $\overline{\mathbb{Q}}$. Let j_1 and j_2 be the respective j-invariants. Then one has*

$$|h(j_1) - h(j_2)| \leq 9.204 + 12 \log \deg \varphi$$

where $h(.)$ denotes the absolute logarithmic Weil height.

Theorem 2.5.1 leads to the following corollary:

Corollary 2.5.2. *Let $\varphi : E_1 \to E_2$ be a $\overline{\mathbb{Q}}$-isogeny between two elliptic curves defined over $\overline{\mathbb{Q}}$ which is cyclic of degree m. Let j_1 and j_2 be the respective j-invariants. Then one has*

$$H(j_1) < Am^{12}H(j_2)$$

for some absolute constant A. Here $H(.)$ denotes the projective height.

5.2. **Bounding change of heights.** We prove an upper bound on the product of heights, which we will use later.

Lemma 2.5.3. *Let d be the projective degree of C under the embedding ι, see (2.1.1). Let $H(\iota)$ be the height of ι defined by the height of the coefficients of the defining polynomials of $j(E_t)$ and $j(E'_t)$. Then for every $t \in K$ with $H(t) \leq B$, we have*

$$H(P_t) \leq (d+1)H(\iota)B^d.$$

Proof. By Lemma 2.2.1 we have

$$H(P_t) = H(j(E_t))H(j(E'_t)).$$

The lemma then follows from [26, VIII, Theorem 5.6] , which asserts that when there is a map of degree d between two projective spaces, say

$$F : \mathbb{P}^m \to \mathbb{P}^M,$$

then for all points $P \in P^m(\overline{\mathbb{Q}})$ there are positive constant C_1 and C_2 depending on F such that

$$C_1 H(P)^d \leq H(F(P)) \leq C_2 H(P)^d.$$

Write $F = [f_0, \cdots, f_M]$ using homogeneous polynomials f_i having no common zeros. Let $H(F)$ be the height of F defined by the height of the coefficients of f_i. The constant C_1 and C_2 can be explicitly calculated in terms of M, m and $H(F)$. Especially, we can let $C_1 = \binom{m+d}{m}H(F)$. The lemma follows from the assumption that $F = \iota$, $m = 1$ and $M = 3$.

□

By Lemma 2.3.11, for our choice of $m \in \mathbb{Z}$, a rational point $t \in C(K)$ with $t \in S(B)$ for some B lifts to a rational point on one of the covers $C_{\tilde{H}_\Delta} \subset X_{\tilde{H}_\Delta}$ or $C_{H_{\mathrm{p}}} \subset X_{H_{\mathrm{p}}}$. We have the following proposition:

Proposition 2.5.4. *Fix $m \in \mathbb{N}$. Let $t \in K$ be a rational point such that $t \in S(B)$ for some B. Let P_t denote the point on C parametrized by t, and denote by $\tilde{P}_t$ a lifting of P_t to one of the covers C_H in Lemma 2.3.11. Let $H(\iota_H(\tilde{P}_t))$ denote the projective height of $\tilde{P}_t$ with respect to ι_H.*

If $H = \tilde{H}_\Delta$*, then*

$$H(\iota_H(\tilde{P}_t)) \leq (m+1)m^{24(m+1)}A^{2(m+1)}((d+1)H(\iota))^{m+2}B^{d(m+2)}.$$

If $H = H_{\mathrm{p}}$*, then*

$$H(\iota_H(\tilde{P}_t)) \leq m^{24}(d+1)^2 H(\iota)^2 B^{2d}.$$

Proof. **Case 1:** P_t **lifts to** $\tilde{C}_{\tilde{H}_\Delta}(K)$

As noted above, passing to the quotient $C_{\tilde{H}_\Delta}$ we have $\iota_{\tilde{H}_\Delta}$ embeds $C_{\tilde{H}_\Delta}$ into $\mathbb{P}^7$ by composing $\iota'_{\tilde{H}_\Delta}$ with the Segre embedding. A point $\tilde{P}_t = (E_t, E'_t, \psi : E_t[m] \overset{\sim}{\to} E'_t[m])$ that is a lift of $P_t = (E_t, E'_t)$ embedded into $\mathbb{P}^7$ as following:

$$(E_t, E'_t, \psi) \to F \times j(E_t) \times j(E'_t) \hookrightarrow [Fj(E_t)j(E'_t), Fj(E_t), Fj(E'_t), \cdots, 1].$$

Since our ultimate goal is to count rational points parametrized by $t \in K$, we need a formula relating the height of $\iota_H(\tilde{P}_t)$ with heights of F, $j(E_t)$ and $j(E'_t)$. By Lemma 2.2.1, we have

$$H(\iota_H(\tilde{P}_t)) = H(F)H(j(E_t))H(j(E'_t)). \tag{2.5.1}$$

Let i be an integer between 1 and $m+1$ such that

$$H(j(E_{t,i})j(E'_{t,i})) = \max_{1 \leq k \leq m+1} H(j(E_{t,k})j(E'_{t,k})).$$

By Definition 2.4.6 and Corollary 2.5.2 and Lemma 2.5.3, together with the fact that for any $\alpha, \beta, \alpha_1 \cdots \alpha_r \in \overline{\mathbb{Q}}$,

$$H(\alpha\beta) \leq H(\alpha)H(\beta)$$

and

$$H(\alpha_1 + \cdots \alpha_r) \leq rH(\alpha_1) \cdots H(\alpha_r),$$

we have

$$\begin{aligned} H(F) &= H(j(E_{t,1})j(E'_{t,1}) + \cdots + j(E_{t,m+1})j(E'_{t,m+1})) && (2.5.2)\\ &\le (m+1)H(j(E_{t,i}))^{m+1}H(j(E'_{t,i}))^{m+1} && (2.5.3)\\ &\le (m+1)m^{24(m+1)}A^{2(m+1)}H(j(E_t))^{m+1}H(j(E'_t))^{m+1} && (2.5.4)\\ &\le (m+1)m^{24(m+1)}A^{2(m+1)}((d+1)H(\iota))^{m+1}B^{d(m+1)}. && (2.5.5)\end{aligned}$$

The constant A comes from Corollary 2.5.2, and the first part of the lemma follows from (2.5.1).

Case 2: P_t lifts to one of the maximal parabolic quotient surfaces

Recall the definition of H_{p} (2.3.9) and $\iota_{H_{\mathrm{p}}}$ (2.4.5). As in the previous case, Lemma 2.2.1 implies that

$$H(\iota_{H_{\mathrm{p}}}(\tilde{P}_t)) = H(j(E_t))H(j(\tilde{E}_t))H(j(E'_t))H(j(\tilde{E}'_t))$$

By Corollary 2.5.2 and Lemma 2.5.3, where $\tilde{E}_t$ is m-isogenous to E_t and $\tilde{E}'_t$ is m-isogenous to E'_t, we have

$$H(\iota_{H_{\mathrm{p}}}(\tilde{P}_t)) \ll m^{24}(d+1)^2H(\iota)^2B^{2d}.$$

□

2.6 Proof of the Main Theorems

2.6.1 Proof of Theorem 3.1.1

The previous sections show that for a rational point P_t on C, we have two types of possible liftings to some modular surfaces with m-level structures. Accordingly, we divide the proof of Theorem 3.1.1 into two parts and analyze each part's contribution to $|S(B)|$. We make optimization of m in terms of the height B of t as.

Case 1: Contributions from modular diagonal quotient surfaces.

Recall that we have the following commutative diagram:

$$\begin{tikzcd}
C_{\tilde{H}_\Delta} \arrow[r, hook, "\iota'_{\tilde{H}_\Delta}"] \arrow[d, "q"'] & \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \arrow[r, hook, "\text{Segre}"] \arrow[d] & \mathbb{P}^7 \\
C \arrow[r, hook] & \mathbb{P}^1 \times \mathbb{P}^1 \arrow[r, hook] & \mathbb{P}^3
\end{tikzcd}$$

Let $\iota_{\tilde{H}_\Delta}$ be the composition of $\iota'_{\tilde{H}_\Delta}$ with the Segre embedding. In order to apply Theorem 2.2.4, we bound the degree of $\iota_{\tilde{H}_\Delta}$, which depends on m and the projective degree of C.

Let $\deg_{C_{\tilde{H}_\Delta}}(F)$ be the degree of F as a function on $C_{\tilde{H}_\Delta}$. The degree of the function $\iota'_{\tilde{H}_\Delta}$ on $C_{\tilde{H}_\Delta}$ can be viewed as a tridegree, which we denote by $(\deg_{C_{\tilde{H}_\Delta}}(F), e, e')$. When we pass to $\mathbb{P}^7$ by compose with the Segre embedding, we have

$$\iota_{\tilde{H}_\Delta} = \deg(F) + e + e'.$$

Here e denotes the degree of the function $j(E_t)$ on $C_{\tilde{H}_\Delta}$ and e' is the degree of $j(E'_t)$ on $C_{\tilde{H}_\Delta}$. Let α be the degree of the cover q and let d_E be the degree of the j-invariant map $C \to \mathbb{P}^1$. Therefore $e = \alpha d_E$. Similarly, we have $e' = \alpha d_{E'}$. Therefore

$$\deg(\iota_{\tilde{H}_\Delta}) > e + e' = \alpha(d_E + d_{E'}) = \alpha d.$$

The degree of q is equal to the index of $\tilde{H}_\Delta$ inside the Galois group $G = SL_2(\mathbb{Z}/m\mathbb{Z}) \times SL_2(\mathbb{Z}/m\mathbb{Z})$. We have

$$\alpha = [G : \tilde{H}_\Delta] = m^3(1 - \frac{1}{m^2}) = m(m+1)(m-1).$$

Therefore

$$\deg(\iota_{\tilde{H}_\Delta}) \geq m(m+1)(m-1)d.$$

In order to get an upper bound of $\deg(\iota_{\tilde{H}_\Delta})$, we need an upper bound for the degree of F over $C_{\tilde{H}_\Delta}$. Recall from diagram 2.4.4, C' is the Galois closure of $C_{\tilde{H}_\Delta}$ over C and the function F is defined to be

$$F = j(E_{t,1})j(E'_{t,1}) + \cdots + j(E_{t,m+1})j(E'_{t,m+1}).$$

The individual terms $j(E_{t,i})$ and $j(E'_{t,i})$ are defined on C', instead of on $C_{\tilde{H}_\Delta}$. A point on C' is a product of triples $(E_t, P, G) \times (E'_t, P', G')$, where P(resp. P') is a point of $E_t[m]$(resp. $E'_t[m]$) and G(resp. G') is a cyclic subgroup of $E_t[m]$(resp. $E'_t[m]$). Fix a j-invariant x, the degree of $j(E_{t,i})$(resp. $j(E'_{t,i})$) is the number of points on C' such that $j(E_t/G) = x$. As long as E_t and E'_t) is not CM, there are $m+1$ j-invariants which are m-isogenous to x and there are d_E points on C mapping to each of those $(m+1)$ j-invariants. Hence the degree $\deg_C(j(E_{t,i}))$(resp. $\deg_C(j(E'_{t,i}))$) for each $1 \le i \le m+1$ is $(m+1)d_E$(resp. $(m+1)d_{E'}$).

The argument above, together with the fact that if f and g are functions on a curve X then

$$\deg(f+g) \le \deg(f) + \deg(g)$$

and

$$\deg(fg) \le \deg(f) + \deg(g),$$

yields that

$$\deg_{C_{\tilde{H}_\Delta}}(F) \le \deg_{C'}(F) \le (m+1)^2 d.$$

Hence we get an upper bound on the degree of $\iota_{\tilde{H}_\Delta}$ which is

$$\deg(\iota_{\tilde{H}_\Delta}) \le (m(m+1)(m-1) + (m+1)^2)d.$$

We can write the argument in the paragraph above in a lemma:

Lemma 2.6.1.

$$m(m+1)(m-1)d \le \deg(\iota_{\tilde{H}_\Delta}) \le (m(m+1)(m-1) + (m+1)^2)d.$$

Let S_{B,m,H_Δ} be the set of rational points on $C_{\tilde{H}_\Delta}(K)$ which are liftings of P_t for some $t \in S(B)$. Recall that we prove an upper bound for the heights of points in S_{B,m,H_Δ} in Proposition 2.5.4. Theorem 2.2.4 ([19, Theorem 1.8]) then applies, along with Lemma

2.4.4 and Lemma 2.6.1, yielding

$$S_{B,m,H_\Delta} \lesssim_K ((\alpha+(m+1)^2)d)^4((m+1)m^{24(m+1)}A^{2(m+1)}((d+1)H(\iota))^{m+2}B^{d(m+2)})^{\frac{2d_K}{\alpha d}} \tag{2.6.1}$$

$$\lesssim_K ((m^2+1)(m+1)d)^4((m+1)m^{24(m+1)}A^{2(m+1)}((d+1)H(\iota))^{m+2}B^{d(m+2)})^{\frac{2d_K}{m(m-1)(m+1)d}} \tag{2.6.2}$$

$$\lesssim_K (m^3d)^4(m+1)^{\frac{2d_K}{m(m-1)(m+1)d}}A^{\frac{4d_K}{m(m-1)d}}m^{\frac{48d_K}{m(m-1)d}}((d+1)H(\iota)B)^{\frac{2d_K(m+2)}{m(m-1)(m+1)}} \tag{2.6.3}$$

The terms in (2.6.3) other than $(m^3d)^4$ are bounded above by an absolute constant. The argument requires optimizations on the choice of m, which we will prove in the following lemma.

Lemma 2.6.2. *Recall that m is a prime between $2(\log(d+1)+\log H(\iota)+\log B)^{\frac{1}{2}}$ and $4(\log(d+1)+\log H(\iota)+\log B)^{\frac{1}{2}}$. There is an absolute constant A_0 such that*

$$(m+1)^{\frac{2d_K}{m(m-1)(m+1)d}}A^{\frac{4d_K}{m(m-1)d}}m^{\frac{48d_K}{m(m-1)d}}((d+1)H(\iota)B)^{\frac{2d_K(m+2)}{m(m-1)(m+1)}} \leq A_0.$$

Proof. Once we write

$$(m+1)^{\frac{2d_K}{m(m-1)(m+1)d}}$$

as

$$e^{(\frac{2d_K}{m(m-1)(m+1)d})\log(m+1)},$$

it is easy to see that for $m \geq 2$ we have

$$(m+1)^{\frac{2d_K}{m(m-1)(m+1)d}} \ll e^{\frac{2d_K}{d}} \leq e^{2d_K}.$$

This is because $\frac{\log(m+1)}{m(m-1)(m+1)}$ is bounded above by 1. A similar argument shows that

$$m^{\frac{48d_K}{m(m-1)d}} \ll e^{\frac{48d_K}{d}} \leq e^{48d_K}$$

which also contributes as a constant independent of m and d.

It is left to consider $((d+1)H(\iota)B)^{\frac{2d_K(m+2)}{m(m-1)(m+1)}}$ which plays an important role in the optimization process. We make the optimization by choosing suitable m in terms of B, d, and $H(\iota)$. The following inequalities, together with Proposition 2.4.3, allows one to take m to be any prime between $2(\log(d+1)+\log H(\iota)+\log B)^{\frac{1}{2}}$ and $4(\log(d+1)+\log H(\iota)+\log B)^{\frac{1}{2}}$, so that

$$\begin{aligned}
((d+1)H(\iota)B)^{\frac{2d_K(m+2)}{m(m-1)(m+1)}} &= e^{\frac{2d_K(m+2)}{m(m-1)(m+1)}}(\log(d+1)+\log H(\iota)+\log B) \\
&= e^{\frac{2d_K(\log(d+1)+\log H(\iota)+\log B)}{(m-1)(m+1)}} \cdot e^{\frac{4d_K(\log(d+1)+\log H(\iota)+\log B)}{m(m-1)(m+1)}} \\
&\le e^{N_1 d_K} \cdot e^{N_2 d_K}
\end{aligned}$$

where $\frac{2(\log(d+1)+\log H(\iota)+\log B)}{(m-1)(m+1)d}$ and $\frac{4(\log(d+1)+\log H(\iota)+\log B)}{m(m-1)(m+1)d}$ are bounded above by some absolute constant N_1 and N_2.

□

We have the following proposition as a conclusion of the case.

Proposition 2.6.3. *The number of points in $|S(B)|$ that comes from the modular diagonal quotient surface is bounded up by*

$$\begin{aligned}
S_{B,m,H_\Delta} &\lesssim_K d^4((\log(d+1)+\log H(\iota)+\log B))^6 \\
&\lesssim_K d^{4+\epsilon}(\log H(\iota)+\log B)^6.
\end{aligned}$$

Proof. The proposition follows from the inequality (2.6.3) and Lemma 2.6.2. □

Case 2: Contributions from maximal parabolic quotient surfaces. Recall that in this case, we have the following commutative diagram.

$$\begin{tikzcd}
C_{H_{\mathrm{p}}} \arrow[r, hook, "\iota'_{H_{\mathrm{p}}}"] \arrow[d, "q"'] & \mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^1 \arrow[r, hook, "\text{Segre}"] \arrow[d] & \mathbb{P}^{15} \\
C \arrow[r, hook] & \mathbb{P}^1\times\mathbb{P}^1 \arrow[r, hook] & \mathbb{P}^3
\end{tikzcd}$$

The degree of the covering space q, denoted by β, is equal to the index of H_{p} inside the Galois group G, similar to the previous case. The index of H_{p} as a product of maximal parabolic subgroups is equal to

$$\beta = [G : H_{\mathrm{p}}] = \frac{1}{4}(m+1)^2.$$

One notice that the degree of $\iota_{H_{\mathrm{p}}}$ satisfies $\deg(\iota_{H_{\mathrm{p}}}) = \beta d$. Let $S_{B,m,H_{\mathrm{p}}}$ be the number of rational points in $C_{H_{\mathrm{p}}}(K)$ that lift P_t for some $t \in S(B)$. Applying Proposition 2.5.4 and Theorem 2.2.3, we get the following inequality

$$S_{B,m,H_{\mathrm{p}}} \lesssim_K ((m+1)^2 d)^4 (m^{24}(d+1)^2 H(\iota)^2 B^{2d})^{\frac{8d_K}{(m+1)^2 d}}$$

which allows us to make the same optimization as in case 1. By taking

$$m \sim (\log B + \log(d+1) + \log H(\iota))^{\frac{1}{2}},$$

we get an upper bound of the total contribution to $|S(B)|$ from the maximal parabolic surfaces:

Proposition 2.6.4.

$$\begin{aligned} S_{B,m,H_{\mathrm{p}}} &\lesssim_K d^4 (\log B + \log(d+1) + \log H(\iota))^4 \\ &\lesssim_K d^{4+\epsilon} (\log B + \log H(\iota))^4. \end{aligned}$$

Proof of Theorem 3.1.1. It is easy to see that the contribution from case 1 dominates that of case 2. Theorem 3.1.1 then follows from Proposition 2.6.3 and 2.6.4.

□

2.6.2 Proof of Theorem 2.1.3

Recall that in Theorem 3.1.1, $H(t)$ is defined as the height of t as an element of K. Instead, if we calculate the height of t as the height of a point on $X(1) \times X(1)$, which we have been calling $H(P_t)$. Assume that $H(P_t) \leq B$. In this section, we prove an *uniform* bound on the number of points t such that E_t and E'_t are geometrically isogenous, which only depends on K, B, and the *degree* of the parametrize family.

We need a slightly modified version of Proposition 2.5.4, which we state as a corollary.

Corollary 2.6.5. *Fix $m \in \mathbb{N}$. Let $t \in K$ be a rational point such that $t \in S(B)$ for some B. Let P_t denote the point on C parametrized by t, and denote by $\tilde{P}_t$ a lifting of P_t to one of the covers C_H in Lemma 2.3.11. Let $H(\iota_H(\tilde{P}_t))$ denote the projective height of $\tilde{P}_t$ with respect to ι_H.*

If $H = \tilde{H}_\Delta$, then

$$H(\iota_H(\tilde{P}_t)) \leq (m+1)m^{24(m+1)}A^{2(m+1)}B^{(m+2)}.$$

If $H = H_{\mathrm{p}}$, then

$$H(\iota_H(\tilde{P}_t)) \leq m^{24}B^2.$$

Proof. The proof is the same as Proposition 2.5.4, except that we have

$$H(j(E_t))H(j(E'_t)) \leq B$$

instead of Lemma 2.5.3. □

Proof of Theorem 2.1.3. Let $S'_{B,m,H}$ be the set of rational points on $C_H(K)$ which are preimages of P_t for some $t \in S'(B)$. A similar argument to the proof of Theorem 3.1.1 yields

$$\begin{aligned} S'_{B,m,\tilde{H}_\Delta} &\lesssim_K ((\alpha + (m+1)^2)d)^4((m+1)m^{24(m+1)}A^{2(m+1)}B)^{(m+2)\frac{2d_K}{\alpha d}} && (2.6.4)\\ &\lesssim_K ((m^2+1)(m+1)d)^4((m+1)m^{24(m+1)}A^{2(m+1)}B^{(m+2)})^{\frac{2d_K}{m(m-1)(m+1)d}} && (2.6.5)\\ &\lesssim_K (m^3d)^4(m+1)^{\frac{2d_K}{m(m-1)(m+1)d}}A^{\frac{4d_K}{m(m-1)d}}m^{\frac{48d_K}{m(m-1)d}}B^{\frac{2d_K(m+2)}{m(m-1)(m+1)d}} && (2.6.6)\end{aligned}$$

when $H = \tilde{H}_\Delta$, and

$$S'_{B,m,H_{\mathrm{p}}} \lesssim_K ((m+1)^2d)^4(m^{24}B^2)^{\frac{8d_K}{(m+1)^2d}}. \tag{2.6.7}$$

We choose m to be a prime between $2(\log B)^{\frac{1}{2}}$ and $4(\log B)^{\frac{1}{2}}$ as to control the growth of the B-power factors in both 2.6.6 and 2.6.7, such that

$$\begin{aligned} B^{\frac{2d_K(m+2)}{m(m-1)(m+1)d}} &= e^{\frac{2d_K(m+2)}{m(m-1)(m+1)d}\log B}\\ &= e^{\frac{2d_K(\log B)}{(m-1)(m+1)}} \cdot e^{\frac{4d_K(\log B)}{m(m-1)(m+1)}}\\ &\leq e^{N'_1 d_K} \cdot e^{N'_2 d_K}\end{aligned}$$

and

$$B^{\frac{16d_K}{(m+1)^2d}} = e^{\frac{16d_K}{(m+1)^2d}\log B} \leq e^{N_3'd_K}$$

for some absolute constant N_1', N_2' and N_3'. □

Chapter 3

Isogeny classes of non-simple abelian surfaces over finite fields

3.1 Introduction

Many fundamental problems on Shimura varieties pertain to the behavior of isogeny classes, for example, the Hecke orbit conjecture and specific questions related to unlikely intersections. In [24, Theorem 4.1], Shankar and Tsimerman proved an asymptotic formula for the size of the isogeny class of ordinary elliptic curves over finite fields. As an application, they proved the existence of a hypersurface in the moduli space $X(1)^{270}$, which intersects every isogeny class.

A few common strategies exist to obtain asymptotic formulas for the size of isogeny classes of abelian varieties over finite fields. In particular, when the abelian variety is ordinary and simple, the inspiring work of Deligne [8] explicitly classified such abelian varieties over finite fields. Using the classification, one can get bounds for the isogeny classes of ordinary abelian varieties, for example, [24, Theorem 3.3]. A handful of studies in this flavor have been performed in more general settings. For example, one may refer to [18] when the abelian variety is almost-ordinary and geometrically simple and to [4] for a setting of Hilbert modular varieties. All of the results above depend on the existence of canonical lifting and classification of abelian varieties over finite fields.

A second way of doing this is to interpret isogeny classes in terms of orbital integrals. For example, in [2], Achter and Cunningham proved an explicit formula for the size of the isogeny class of a Hilbert-Blumenthal abelian variety over a finite field. They express the size of the isogeny class as a product of local orbital integrals on $GL(2)$ and then evaluate all the relevant orbital integrals. See also [1] where Achter and Williams proved that for a particular class of simple, ordinary abelian surfaces over $\mathbb{F}_q$ given by a q-weil polynomial f, the number of principally polarized abelian surfaces over $\mathbb{F}_q$ with Weil polynomial f could be calculated by an infinite product of local factors which can be calculated by method of orbital integrals.

Throughout this article, let (A, λ_A) be a principally polarized non-simple abelian surface defined over $\mathbb{F}_q$, with the polarization given by λ_A. Moreover, assume that A has the form $A = E \times E_{ss}$, where E is an ordinary elliptic curve and E_{ss} is a supersingular elliptic curve. The endomorphism algebra $\mathrm{End}^\circ(A)$ is non-commutative, and there is no canonical lifting of A. Therefore, we cannot interpret the question as estimating the size of class groups by using the classification of abelian varieties over finite fields. Instead, we measure the size of the isogeny class of A defined over $\mathbb{F}_q$ and describe how this cardinality is affected by the base change to finite extensions of $\mathbb{F}_q$ by using group-theoretical methods.

Before introducing the main theorem, we introduce some notations. Let $I(q^n, A)$ be the set of principally polarized abelian varieties defined over $\mathbb{F}_{q^n}$ that are isogenous to A over $\overline{\mathbb{F}}_q$. Let $N(q^n, A)$ denote the cardinality of $I(q^n, A)$. By interpreting the question as a classification of finite subgroup schemes, we obtain a lower bound on the number of principally polarized abelian varieties over $\mathbb{F}_{q^n}$ that is isogenous to A over $\overline{\mathbb{F}}_q$. Our main result is the following.

Theorem 3.1.1. *Let (A, λ_A) be a principally polarized abelian variety over $\mathbb{F}_q$ such that $A = E \times E_{ss}$. Let K be the quadratic number field such that $K = \mathrm{End}^\circ(E)$. Let n be an integer such that for all prime ℓ ramified in $\mathcal{O}_K$, $(n, \ell) \neq 1$. Then*

$$N(q^n, A) \gg q^{n+o(1)}.$$

Also, we provide a different approach to count the size of isogeny classes of ordinary elliptic curves over finite fields, which upper bound is known by Lenstra [14, Proposition 1.19] and Shankar-Tsimerman [24, Theorem 3.3].

Theorem 3.1.2. *Let E be an elliptic curve defined over $\mathbb{F}_q$. For a positive density set of n, we have*

$$N(q^n, E) = (q^n)^{1/2+o(1)}.$$

There is a general conjecture regarding the size of the isogeny class of abelian varieties over finite fields. Let $N(W)$ be the open Newton stratum of $\mathcal{A}_g$ consisting of all abelian varieties whose Newton polygon is W and let A be a principally polarized abelian variety in $\mathcal{A}_g$. Recall that the *central leaf* through A consists of all abelian varieties in $N(W)$ whose p-divisible group is isomorphic to $A[p^\infty]$. The *isogeny leaf* through A is a maximal irreducible subscheme of $\mathcal{A}_g$ consisting of abelian varieties A' in $N(W)$ such that A' is isogenous to A through an isogeny whose kernel is an iteration extension of the group scheme α_p. Let $\dim(CL)$ be the dimension of the central leaf through A and let $\dim(IL)$ be the dimension of the isogeny leaf through A.

Conjecture 3.1.3. *We have*

$$N(q^n, A) = q^{n(\frac{\dim(CL)}{2}+\dim(IL))+o(1)}.$$

All the previous results we state above satisfy the Conjecture 3.1.3. When A is a non-simple abelian surface, it is easy to see that the dimension of the central leaf through A is 2, by the formula of lattice-point count by Shankar and Tsimerman [24, Section 5.2]. The dimension of the isogeny leaf through A is 0. Therefore the conjecture is true in this case.

3.2 The Isogeny Classes and Maximal Isotropic Subgroups

A classical way to construct abelian varieties isogenous to a fixed abelian variety A is to take quotients of A by finite subgroup schemes. A theorem of Mumford [17, II.7 Theorem

4] addresses that one can construct isogenies from finite subgroups of an abelian variety and vice versa.

Theorem 3.2.1. *[17, II.7 Theorem 4] Let X be an abelian variety. There is a one-to-one correspondence between the two sets of objects:*

(a) finite subgroups $K \in X$,

(b) separable isogenies $f : X \to Y$, where two isogenies $f_1 : X \to Y_1$, $f_2 : X \to Y_2$ are considered equal if there is an isomorphism $h : Y_1 \to Y_2$ such that $f_2 = h \circ f_1$, which is set up by $K = \ker(f)$, and $Y = X/K$.

The maximal isotropic subgroups. In order to count the number of abelian varieties isogenous to A, a natural way is to look at all its finite subgroups $G \subset A$. Let $A[m]$ be the m-torsion subgroup of A . when $p \nmid m$, $A[m] = (\mathbb{Z}/m\mathbb{Z})^4$. Without loss of generality, let m be a prime integer. Recall that for a symplectic F-vector space V equipped with the symplectuc bilinear form $\omega : V \times V \to F$, a subspace H is called *isotropic* if for any $h_1, h_2 \in H$, $\omega(h_1, h_2) = 0$. It is a standard fact that for a symplectic vector space of dimension $2g$, each of the maximal isotropic subspaces is of dimension g.

Definition 3.2.2. Let (A, λ_A) be a principally polarized abelian surface, and ℓ be a prime such that $\ell \nmid p$. Define the *(ℓ^m, ℓ^m)-isogeny* to be any isogeny $f : A \to B$ whose kernel is a maximal isoptopic subgroup of $A[\ell^m]$, with respect to the Weil paring induced by the polarization λ_A.

We claim that for an (ℓ^m, ℓ^m)-isogeny $f : A \to B$, there is a unique principal polarization on B, denoted by λ_B, such that $f^*\lambda_B = \ell^m \times \lambda_A$. This is a consequence of Grothendieck's descent, and we omit the proof here. See [22, Proposition 2.4.7] for detailed proof. This fact allows us to compute a lower bound of $N(q^n, A)$ first by counting the number of maximal isotropic subgroups of A that are defined over F_{q^n}, then by computing the number of the subgroups that give the same quotient up to isomorphism.

Lemma 3.2.3. *For $l \nmid p$, there are*

$$\ell^{3m} + \ell^{3m-1} + \ell^{3m-2} + l^{3m-3}$$

maximal isotropic subgroups of $A[\ell^m]$ with respect to the principal polarization λ_A.

Proof. Without loss of generality, one can assume that λ_A is given by the matrix

$$\lambda_A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}$$

up to a proper choice of basis for the ℓ-adic Tate module $T_\ell A$. Then the corresponding symplectic form is $\psi(x, y) = x^T M y$. It is easy to see that any cyclic group H of order ℓ^m, we call it *isotropic line*, is an isotropic subgroup. Any maximal isotropic subgroup has the form $(\mathbb{Z}/\ell^m\mathbb{Z})^2$. These can be viewed as the *isotropic planes* inside $A[\ell^m]$. Let $H^\perp$ denote the orthogonal complement of H. A direct computation shows that

$$H \subset H^\perp, dim(H^\perp) = 3.$$

Since any maximal isotropic subgroup has dimension two, the number of isotropic planes containing H is the number of lines in $H^\perp/H$ counts to $\ell^m + \ell^{m-1}$. The number of lines L in $A[\ell^m]$ is $\ell^{3m} + \ell^{3m-1} + \ell^{3m-2} + \ell^{3m-3}$ and any maximal isotropic plane contains $\ell^m + \ell^{m-1}$ lines. The result follows. □

We introduce a criterion by Waterhouse [29, Proposition 3.6], which enables us to rule out maximal isotropic subgroups that give the same quotient variety up to isomorphism. We investigate the ℓ-power subgroups of A, where $\ell \nmid p$. Let $H_1, H_2 \cong (\mathbb{Z}/\ell^m\mathbb{Z})^2$ be isotropic planes in $A[\ell^m]$.

Definition 3.2.4. H_1 is equivalent to H_2 if they define the same quotient up to isomorphism

$$A/H_1 \cong A/H_2.$$

Theorem 3.2.5. *[29, Proposition 3.6] Let G_1 and G_2 be two finite subgroups of A, not necessarily étale. Then $A/G_1 \cong A/G_2$ if and only if for some isogeny $\rho \in \mathrm{End}(A)$ and some non-zero $N \in \mathbb{Z}$, $\rho^{-1}(G_1) = [N]^{-1}G_2$.*

Proof. See [29, Proposition 3.6]. We include the proof here for completeness.

Suppose $A/G_1 \simeq A/G_2$. Then we have $\varphi_i : A \to B$ with $\ker \varphi_i = G_i, i = 1, 2$. For N_1 large (e.g., $N_1 = \operatorname{rank} G_1$), we have $[N_1]^{-1}G_2 \supseteq G_1$. Now $[N_1]^{-1}G_2 = \ker(N_1\varphi_2)$, so by the definition of quotient there is a $\sigma : B \to B$ such that $\sigma\varphi_1 = N_1\varphi_2$. For N_2 large enough there is a $\rho : A \to A$ with $\varphi_1\rho = [N_2]\sigma\varphi_1$ (choose an i_A and look at the two lattices in E). Thus $\varphi_1\rho = N_1N_2\varphi_2$. Set $N = N_1N_2$, then

$$\rho^{-1}(G_1) = \ker(\varphi_1\rho) = \ker([N]\varphi_2) = [N]^{-1}G_2.$$

Conversely, $A \xrightarrow{\rho} A \to A/G_1$ shows that

$$A/G_1 \simeq A/\rho^{-1}(G_1);$$

likewise

$$A/G_2 \simeq A/[N]^{-1}G_2,$$

so the condition is sufficient.

□

3.3 Counting inequivalent maximal isotropic planes

In this section, we prove a lower bound for the number of inequivalent maximal isotropic planes. The main result is Proposition 3.3.3 and Proposition 3.3.5. For any prime $\ell \nmid p$, fix a basis $\{e_1, e_2, f_1, f_2\}$ for $T_\ell A$, such that for $i, j = 1, 2$, $\omega(e_i, f_j) = 1$ only when $i \neq j$. For the rest of the paper, H will denote a maximal isotropic subgroup of $A[\ell^m]$.

Let $\phi : A \to B$ be an isogeny defined over $\mathbb{F}_{q^n}$. Since there is no isogeny between ordinary and supersingular elliptic curves, the endomorphism ring decomposes as $\operatorname{End}(A) = \operatorname{End}(E) \times \operatorname{End}(E_{ss})$. Therefore there is a decomposition of ϕ into ordinary and supersingular part, namely $\phi = \phi_{\text{ord}} \times \phi_{\text{ss}}$, accordingly a decomposition of the kernel: $\ker(\phi) = K_{\text{ord}} \times K_{ss}$, where $K_{\text{ord}} \subset E$ and $K_{ss} \subset E_{ss}$. We have the following theorems on the number of endomorphisms of elliptic curves over finite fields whose kernel is cyclic:

Proposition 3.3.1. *Let E be an ordinary elliptic curve defined over F_{q^n}. For any positive integer d, the number of endomorphisms in* $\operatorname{End}(E)$ *with cyclic kernel $\mathbb{Z}/d\mathbb{Z}$ is* *bounded up by $O(d^\epsilon)$.*

Proof. Let $K = \mathrm{End}^\circ(E)$, E is ordinary implies that K is a quadratic number field. Let $\mathcal{O}_K$ denote the ring of integers of K. Assume that d has prime decomposition $d = p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_s^{f_s} d_1$, such that p_i splits in $\mathcal{O}_K$, q_j inert in $\mathcal{O}_K$ and every prime factor of d_i, namely the ramified prime, divides D. The number of endomorphisms in $\mathrm{End}(E)$ with cyclic kernel $\mathbb{Z}/\ell^m\mathbb{Z}$ is the number of elements in $\mathcal{O}_K$ with norm ℓ^k. Therefore it is $(e_1+1)\cdots(e_r+1)$ if all f_j, $1 \le j \le s$ are even, or zero otherwise. The divisor bound is $O(d^\epsilon)$, which is a standard fact. □

Proposition 3.3.2. *Let E_{ss} be a supersingular elliptic curve defined over F_{q^n}. For $\ell \nmid D$ where D is the determinant of the norm form on End(E_{ss}), there are $O(\ell^m)$ endomorphisms whose kernel is the cyclic group $\mathbb{Z}/\ell^m\mathbb{Z}$.*

Proof. Let E_{ss} be a supersingular elliptic curve defined over F_{q^n} with characteristic p, then $O_{E_{ss}} = \mathrm{End}(E_{ss})$ is a maximal order in the quaternion algebra ramified exactly at p and ∞. Endomorphism with kernel a cyclic subgroup of order m, i.e., of degree m, are elements in $O_{E_{ss}}$ with norm m. For a quaternion algebra $F = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$ where $\alpha^2 = a, \beta^2 = b, a < 0, b < 0, \beta\alpha = -\alpha\beta$, $x = x_0 + x_1\alpha + x_2\beta + x_3\alpha\beta \in F$, the norm $N(x) = x\bar{x} = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$ is a quaternion quadratic form. The question boils down to counting the number of representations

$$r(n) = r_N(n) = \#\{x \in \mathbb{Z}^4, x = (x_0, x_1, x_2, x_3); N(x) = n\}$$

This can be solved making use of the theta series

$$\vartheta(z) = \sum_{\alpha \in \mathbb{Z}^4} e(zN(\alpha)) = \sum_{n \ge 0} r(n)e(nz)$$

where $e(z) = e^{2\pi i z}$, which is a generating series for $r(n)$. $\vartheta(z)$ satisfy

$$\vartheta(\frac{az+b}{cz+d}) = \chi(\gamma)(cz+d)^{m/2}\vartheta(z)$$

where $\gamma \in SL_2(\mathbb{Z})$ and therefore is a modular form of weight $m/2$. So it can be written as the sum of an Eisenstein series

$$E(z) = \sum_{n\geq 0} \rho(n)e(nz), \rho(0) = 1$$

and a cusp form

$$f(z) = \vartheta(z) - E(z) = \sum_{n\geq 1} a(n)e(nz).$$

Thus we can write $r(n) = \rho(n) + a(n)$ and then bound it from above by estimating the Fourier coefficient $a(n)$ of the cusp form and estimating $\rho(n)$ gives a bound from below. In our case where $m = 4$, assume that $\ell \nmid D$. We have $\frac{m}{2} - 1 = 1$ such that

$$\rho(n) \gg n.$$

One way to get a nontrivial upper bound for $a(n)$ is to use the Rankin-Selberg method. For even m, Deligne[Del73] proved that $a(n) \ll n^{\frac{m}{4}-\frac{1}{2}+\epsilon}$. In our case, it turns out to be

$$a(n) \ll n^{\frac{1}{2}}.$$

Putting together, we get

$$r(\ell^m) \gg \ell^m.$$

Since E_{ss} is simple, every non-zero endomorphism is an isogeny, and we have

$$\ell^m + \ell^{m-1} = O(\ell^m)$$

cyclic subgroups of order ℓ^m in $E_{ss}[\ell^m] = \mathbb{Z}/\ell^m\mathbb{Z} \times \mathbb{Z}/\ell^m\mathbb{Z}$. Thus

$$r(n) = r_N(n) = O(\ell^m).$$

□

There are two types of maximal isotropic planes in $A[\ell^m]$ we take into concern with respect to our choice of basis:

- **Type 1:** H is a product $H_1 \times H_2$ where $H_1 \in E$, $H_2 \in E_{ss}$.
- **Type 2:** H cannot be written as a product $H_1 \times H_2$ where $H_1 \leq E$, $H_2 \leq E_{ss}$.

3.3.1 H is of product type

In the case where H is of type 1, we write $H = \langle ae_1 + be_2, cf_1 + df_2\rangle$, where $a, b, c, d \in \mathbb{Z}/\ell^m\mathbb{Z}$. Here $\{e_1, e_2, f_1, f_2\}$ denote a basis of $A[\ell^m]$. We claim that:

Proposition 3.3.3. *Let N_1 be the number of inequivalent maximal isotropic planes of type 1. We have*

$$N_1 \asymp \ell^m$$

Proof. For an elliptic curve, either ordinary or supersingular, there are $O(\ell^m)$ cyclic subgroups of the order less than or equal to ℓ^m. Therefore, there are $O(\ell^{2m})$ such kind of H in total. Let H_1 and $H_1^{'}$ be cyclic subgroups(isotropic lines) of $E[\ell^m]$. By Theorem 3.2.5, $A/H_1 \cong A/H_1^{'}$ if and only if there exists $\phi \in \mathrm{End}(E)$, $N \in \mathbb{Z}$ such that $\phi^{-1}H_1^{'} = [N]^{-1}H_1$. For such possible ϕ that has prime-to-ℓ kernel, we have $N \nmid \ell$, $N^{-1}H_1 = (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/\ell^m\mathbb{Z})$. Since $\mathrm{Ker}(N) \subset \mathrm{Ker}(\phi)$, ϕ factors through the multiplication by N map as $\phi = i \circ N$ where $i \in \mathrm{Aut}(E)$. But for an ordinary elliptic curve, there are only finitely many units in $\mathrm{End}(E)$, thus the possible choices of ϕ.

The same argument also works for ϕ has ℓ-power kernel. Indeed, for positive integer k, we have $[\ell^k]^{-1}H_1 = (\mathbb{Z}/\ell^k\mathbb{Z}) \times (\mathbb{Z}/\ell^{k+m}\mathbb{Z})$ and the possible choices of $\mathrm{Ker}(\phi)$ are $(\mathbb{Z}/\ell^{k+i}\mathbb{Z}) \times (\mathbb{Z}/\ell^{k-i}\mathbb{Z})$ for $0 \le i \le m$. Proposition 3.3.1 implies that the number of inequivalent isotropic lines $H_1 \subset E$ is $O(l^{m-\epsilon})$.

We assumed that H_2 comes from the supersingular elliptic curve E_{ss}. Since the number of supersingular elliptic curves up to $\bar{\mathbb{F}}_q$-isomorphism is finite, for instance, see [26, V.4 Theorem 4.1]. we have finitely many inequivalent $H_2 \in E_{ss}$. Putting these arguments together, we proved that the number of such inequivalent H of type 1 is asymptotically ℓ^m.

□

3.3.2 H is not a product

In the second case, we assume that H is not a product of ordinary and supersingular subgroups. To be explicit, we write $H = \langle e_1 + af_1 + bf_2, e_2 + cf_1 + df_2\rangle$, with the assumption that

$$det(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = -1.$$

By Lemma 3.2.3 and Proposition 3.3.3, the total number of the maximal isotropic plane in the non-product form is $O(\ell^{3m})$.

Fix an H in this form. We count the number of all isotropic planes H' that is equivalent to H. By work of Waterhouse [29],

$$\phi^{-1}H' = [N]^{-1}H$$

for some $\phi \in \mathrm{End}(A)$ and some positive integer N. Before proving Proposition 3.3.5, we introduce the following lemma.

For any $\phi \in \mathrm{End}(A)$, we can write $\phi = \phi_{\mathrm{ord}} \times \phi_{\mathrm{ss}}$. As a consequence, the kernel of ϕ decomposes as $\mathrm{Ker}(\phi) = K_{\mathrm{ord}} \times K_{\mathrm{ss}}$. Therefore, to bound the number of endomorphisms ϕ once we fix N, we need to bound the number of possible ϕ_{ord} and ϕ_{ss} separately. By Proposition 3.3.1, the number of endomorphisms of an ordinary elliptic curve with a fixed degree d is $O\left(d^{\epsilon}\right)$. Therefore, we only have to determine how many possible choices of K_{ss} we can have under the assumption of H.

Lemma 3.3.4. *Assume that H is of Type 2, and take $N = \ell^m$. Then there are at most $O(\ell^m)$ supersingular endomorphisms which we denote by ϕ_{ss}, such that*

$$\phi_{ss} = \ell^a \circ \phi_{cyc},$$

for some $0 \leq a \leq m$, and there exists an endomorphism $\phi = \phi_{\mathrm{ord}} \times \phi_{ss}$, such that

$$\phi^{-1}H' = [N]^{-1}H.$$

Moreover, ϕ_{cyc} is cyclic of order at most ℓ^m.

Proof. First of all, we prove that the degree of ϕ_{cyc} is at most ℓ^m. This is equivalent to the statement that we cannot have an element

$$\alpha \in [\ell^m]^{-1}H \cap E_{\mathrm{ss}}$$

whose order is greater than or equals to ℓ^{m+1}. We prove this by contradiction. Suppose such an element exists and call it $|x|$. Since $|x| \geq \ell^{m+1}$, $\ell^m \circ (x)$ is nontrivial. By definition we have $\ell^m \circ (x) \in H$ and $\ell^m \circ (x) \in E_{\mathrm{ss}}$. Therefore

$$\ell^m \circ (x) \in [\ell^m]^{-1} H \cap E_{\mathrm{ss}}.$$

Since H has the form $H = \langle e_1 + af_1 + bf_2, e_2 + cf_1 + df_2 \rangle$, one gets to the conclusion that $E_{\mathrm{ss}} \cap H = \{\mathrm{id}\}$. Hence the contradiction.

By Proposition 3.3.2, we conclude that there are at most $O(\ell^m)$ such ϕ_{cyc}, hence at most $O(\ell^m)$ such ϕ_{ss}.

□

Proposition 3.3.5. *Let N_2 be the number of inequivalent maximal isotropic planes of type 2. We have*

$$N_2 >> \ell^{2m-\epsilon}$$

Proof. For a fixed H, getting a lower bound of the number of inequivalent isotropic planes is equivalent to getting an upper bound of the maximal isotropic planes which are equivalent to H. We do this by bounding the number of endomorphisms $\phi \in \mathrm{End}(A)$ such that $\phi \circ [N]^{-1} H$ is a maximal isotropic plane for each fixed N, as N goes through the set of positive integers.

First, suppose that $\ell \nmid N$. In this case, the pullback of an isotropic plane under ϕ has the form

$$\phi^{-1}(H) \simeq (\mathbb{Z}/\ell^m\mathbb{Z})^2 \times \ker(\phi).$$

On the other hand, we have

$$[N]^{-1} H \simeq (\mathbb{Z}/\ell^m\mathbb{Z})^2 \times (\mathbb{Z}/N\mathbb{Z})^4.$$

By Theorem 3.2.5, $\mathrm{Ker}(\phi) \simeq (\mathbb{Z}/N\mathbb{Z})^4$. Therefore we have $\phi = i \circ N$, where $i \in \mathrm{Aut}(A)$ is an automorphism. Taking for granted the fact that principally polarized abelian varieties have finitely many automorphisms which are independent of n, we get finitely many H' that is equivalent to H where $H' = \phi(\circ [N]^{-1} H)$ is a maximal isotropic plane inside $A[\ell^m]$.

When $l \mid N$, $k \geq 1$. We may write $N = N_0 \cdot \ell^a$ for some $a \geq 1$, where N_0 is coprime to ℓ. Then

$$[N]^{-1}H \simeq (\mathbb{Z}/\ell^a\mathbb{Z})^2 \times (\mathbb{Z}/\ell^{m+a}\mathbb{Z})^2 \times (\mathbb{Z}/N_0\mathbb{Z})^4.$$

Therefore

$$\mathrm{Ker}(\phi) \simeq (\mathbb{Z}/N_0\mathbb{Z})^4 \times G_\ell,$$

where G_ℓ is some ℓ-power subgroup which we will specify later. Therefore ϕ can be written as a decomposition

$$\phi = i \circ N_0 \circ \phi_l$$

where ϕ_ℓ is an ℓ-power isogeny with kernel G_ℓ.

So without loss of generality, we can assume that $N = \ell^k$ for some $k \geq 1$ and prove the following subcases depending on the power of ℓ.

If $k < m$, we have

$$[\ell^k]^{-1}H = (\mathbb{Z}/\ell^k\mathbb{Z})^2 \times (\mathbb{Z}/\ell^{k+m}\mathbb{Z})^2.$$

Let $A \subset [\ell^k]^{-1}H$ be a subgroup such that

$$[\ell^k]^{-1}H/A \simeq (\mathbb{Z}/\ell^m\mathbb{Z})^2.$$

Then

$$A \simeq (\mathbb{Z}/\ell^k\mathbb{Z})^2 \times (\mathbb{Z}/\ell^{k+i}\mathbb{Z}) \times (\mathbb{Z}/\ell^{k-i}\mathbb{Z})$$

for some $0 \leq i \leq m$. Hence the possible choices of $\mathrm{Ker}(\phi)$ have the above form.

For $k = m$, we have

$$[\ell^m]^{-1}H = (\mathbb{Z}/\ell^m\mathbb{Z})^2 \times (\mathbb{Z}/\ell^{m+m}\mathbb{Z})^2.$$

Similarly we have the possible choices for $\mathrm{Ker}(\phi)$ are subgroups in the following form

$$(\mathbb{Z}/\ell^{m+i}\mathbb{Z}) \times (\mathbb{Z}/\ell^{m-i}\mathbb{Z}) \times (\mathbb{Z}/\ell^{m+j}\mathbb{Z}) \times (\mathbb{Z}/\ell^{m-j}\mathbb{Z})$$

for $0 \leq i \leq m$ and $0 \leq j \leq m$.

For $k > m$, the possible choices for $\mathrm{Ker}(\phi)$ are

$$(\mathbb{Z}/\ell^{k+i}\mathbb{Z}) \times (\mathbb{Z}/\ell^{k+j}\mathbb{Z}) \times (\mathbb{Z}/\ell^{k+m-n}\mathbb{Z}) \times (\mathbb{Z}/\ell^{k+m-w}\mathbb{Z})$$

where $i, j, n, w \geq 0$ and $i + j + n + w = 2m$.

However, since $\mathbb{Z}/\ell^{k-m}\mathbb{Z}$ is a common factor, this implies $\mathrm{Ker}(\phi)$ contains $\ker([\ell^{k-m}]) = (\mathbb{Z}/\ell^{k-m}\mathbb{Z})^4$. Therefore ϕ factors through the multiplication by ℓ^{k-m} map, we are returning to the case where $k = m$.

Now we can bound the number of endomorphisms and the number of maximal isotropic planes equivalent to a given H. Proposition 3.3.1 asserts that the number of endomorphisms of an ordinary elliptic curve with a fixed degree d is $O\left(d^{\epsilon}\right)$ and Lemma 3.3.4 states that there are at most $O(\ell^m)$ supersingular endomorphisms that serve as the supersingular part of ϕ. An upper bound of the maximal isotropic planes isomorphic to a fixed H is $O(\ell^{m+\epsilon})$. Therefore the total number of inequivalent maximal isotropic planes of type 2 in $A[\ell^m]$ is

$$O(\ell^{2m-\epsilon}) = O(\ell^{3m})/O(\ell^{m+\epsilon})).$$

□

Remark 3.3.6. We note that improving the bound without the ϵ term is plausible.

Corollary 3.3.7. *Let $\ell_1, \cdots, \ell_n$ be n primes different from p and let $m_1, \cdots, m_n$ be positive integers. Let N_0 be the total number of inequivalent maximal isotropic planes. We have*

$$N_0 >> (\ell_1^{m_1} \cdots \ell_n^{m_n})^{2-\epsilon}$$

Proof. The proof is a generalization of Proposition 3.3.5 proof. Since the majority of the inequivalent maximal isotropic planes come from products of isotropic planes of Type 2 as ℓ varies, we fix a subgroup G

$$G \simeq (\mathbb{Z}/\ell_1^{m_1}\mathbb{Z})^2 \times \cdots \times (\mathbb{Z}/\ell_n^{m_n}\mathbb{Z})^2$$

such that for each ℓ_i, $1 \leq i \leq n$, $(\mathbb{Z}/\ell_1^{m_1})^2$ is an isotropic plane of Type 2. Let $\{e_1^1, e_2^1, f_1^1, f_2^1\}, \cdots, \{e_1^n, e_2^n, f_1^n, f_2^n\}$ be a basis for $T_{\ell_1}(A), \cdots, T_{\ell_n}(A)$, respectively.

We count the maximal number of maximal isotropic planes G' that is equivalent to G. By Theorem 3.2.5, G and G' are equivalent if there is $\phi \in \operatorname{End}(A)$ and non-zero positive integer N such that $\phi^{-1}G' = [N]^{-1}G$. We split the argument into different cases based on the choice of N.

Case I: N is coprime to $\ell_1, \cdots, \ell_n$.

If N is coprime to $\ell_1 \cdots \ell_n$,

$$[N]^{-1}H = (\mathbb{Z}/N\mathbb{Z})^4 \times (\mathbb{Z}/\ell_1^{m_1})^2\mathbb{Z} \times \cdots \times (\mathbb{Z}/\ell_n^{m_n}\mathbb{Z})^2.$$

Therefore we have $\phi = i \circ N$, where $i \in \operatorname{Aut}(A)$ is an automorphism. Taking for granted the fact that principally polarized abelian varieties have finitely many automorphisms, we get finitely many H' that is equivalent to H under the assumption that $H' = \phi \circ [N]^{-1}H$.

Case II: $N = \ell_{j_1}^{m_{j_1}} \cdots \ell_{j_k}^{m_{j_k}}$ for some $0 < k \leq n$ and $1 \leq j_1 < \cdots < j_k \leq n$.

Similar to Proposition 3.3.5, if N is not coprime to some of the $\{\ell_1, \cdots, \ell_n\}$, we may restrain ourselves on this case, for the same reason as explained in the proof of Proposition 3.3.5.

The pullback of G under $\ell_{j_1}^{m_{j_1}} \cdots \ell_{j_k}^{m_{j_k}}$ is isomorphic to

$$(\mathbb{Z}/\ell_{j_1}^{m_{j_1}}\mathbb{Z})^2 \times \cdots \times (\mathbb{Z}/\ell_{j_k}^{m_{j_k}}\mathbb{Z})^2 \times (\mathbb{Z}/\ell_{j_1}^{2m_{j_1}}\mathbb{Z})^2 \times \cdots \times (\mathbb{Z}/\ell_{j_k}^{2m_{j_k}}\mathbb{Z})^2 \times \prod_{j \neq j_1, \cdots, j_k} (\mathbb{Z}/\ell_j^{m_j}\mathbb{Z})^2.$$

Recall that for each $1 \leq i \leq n$ we assume that

$$G_i := (\mathbb{Z}/\ell_i^{m_i}\mathbb{Z})^2 = \langle e_1^i + a_i f_1^i + b_i f_2^i, e_2^i + c_i f_1^i + d_i f_2^i \rangle,$$

with the assumption that

$$\det(\begin{bmatrix} a_i & b_i \\ c_i & d_i \end{bmatrix}) = -1.$$

Similar to the proof of Lemma 3.3.4, an endomorphism ϕ that satisfies the Waterhouse's criterion can be realized as an endomorphism with kernel $\operatorname{Ker}(\phi) = K_{\text{ord}} \times K_{\text{ss}}$. Moreover, we can factor out the ℓ-power scalar multiple from each part and consider those supersingular endomorphisms whose kernels are cyclic subgroups. We claim that the supersingular part K_{ss} contains a cyclic subgroup of order at most $\ell_{j_1}^{m_{j_1}} \cdots \ell_{j_k}^{m_{j_k}}$. Suppose this is not the case, i.e., there is an element $x \in [\ell_{j_1}^{m_{j_1}} \cdots \ell_{j_k}^{m_{j_k}}]^{-1} H \cap E_{\mathrm{ss}}$ with order $|x| \geq \ell_{j_1}^{m_{j_1}} \cdots \ell_{j_k}^{m_{j_k}}$, then

$$\ell_{j_1}^{m_{j_1}} \cdots \ell_{j_k}^{m_{j_k}} \circ (x) \in \prod_i G_i \cap E_{\mathrm{ss}}$$

is nontrivial. By definition of G_i for each $1 \leq i \leq n$, the intersection $\prod_i G_i \cap E_{\mathrm{ss}}$ is trivial. Therefore the claim follows.

By Proposition 3.3.2, there are at most $\ell_{j_1}^{m_{j_1}} \cdots \ell_{j_k}^{m_{j_k}}$ such K_{ss}. For the ordinary component, Proposition 3.3.1 implies that there are at most $(\ell_{j_1}^{m_{j_1}} \cdots \ell_{j_k}^{m_{j_k}})^{2\epsilon}$ many possible choices for K_{ord}. We conclude that there are at most $(\ell_{j_1}^{m_{j_1}} \cdots \ell_{j_k}^{m_{j_k}})^{2-\epsilon}$ maximal isotropic planes G' that are equivalent to a given G. The result follows. □

3.4 Proof of the Theorems

3.4.1 Semisimplicity assumption on the Frobenius action

Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with $\mathrm{End}^\circ(E) = K$ and let π be the Frobenius endomorphism. Here K is the quadratic imaginary field generated by π: $K = \mathbb{Q}(\pi)$. We fix a basis $\{e_1, e_2\}$ of $T_\ell(E)$. The characteristic polynomial χ_π is the unique polynomial such that for every n prime to p, the characteristic polynomial of the action of the Frobenius π on $E[n]$ is χ_π mod n. Let Δ_{π^n} be the discriminant of π^n. The characteristic polynomial is a quadratic polynomial

$$\chi_{\pi^n} = x^2 - tx + q^n.$$

We have $\Delta_{\pi^n} = t^2 - 4q^n$.

Remark 3.4.1. For an degree n extension F_{q^n}, the Frobenius of $E_{\mathbb{F}_{q^n}}$ is π^n.

An isogeny $\phi\colon E \to E'$ whose kernel is a cyclic subgroup of E can be understood by looking at the Frobenius action on the torsion subgroups. If ϕ is defined over $\mathbb{F}_{q^n}$, then

$\ker \phi$ is stabilized by the Frobenius action. For $\ell \neq p$, the number of ℓ-power isogenies defined over $\mathbb{F}_{q^n}$ is determined by the action of π^n on ℓ-power torsions. Moreover, the action of Frobenius can be realized as a 2×2 matrix with coefficients in $\mathbb{Z}/\ell^m\mathbb{Z}$.

Now we state the semisimplicity assumption on the Frobenius action, which helps us narrow down cases that we should focus on.

Recall that our goal is to compute the number of ℓ-power isogenies from E that is defined over $\mathbb{F}_{q^n}$, as ℓ goes through all prime integers. The semisimplicity of the Frobenius action depends on whether ℓ is ramified in $\mathcal{O}_K$ or not:

⋆ If ℓ is unramified in $\mathcal{O}_K$, then π^n is semisimple modulo ℓ^m for all $m \geq 1$. We prove the following lemma:

Lemma 3.4.2. *Let m be the maximal number such that $\Delta_{\pi^n} \equiv 0$ mod ℓ^{2m}, then*

$$\pi^n \equiv \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \text{ mod } \ell^m.$$

Proof. Let λ_1 and λ_2 be the eigenvalues of χ_{π^n}. We have

$$\Delta_{\pi^n} = (\lambda_1 - \lambda_2)^2$$

and ℓ^{2m} divides Δ_{π^n}. Therefore $\ell^m \mid (\lambda_1 - \lambda_2)$.

Since ℓ is unramified in $\mathcal{O}_K$, the action of π^n is semisimple modulo ℓ^m. Work on the setting over $\mathbb{Z}_\ell$, if $\lambda_1, \lambda_2 \in \mathbb{Z}_\ell$ we are done. Otherwise, $\lambda_1, \lambda_2 \in \mathcal{O}_\ell$ where $\mathcal{O}_\ell$ is unramified of degree 2. We now prove that λ_1, λ_2 mod ℓ^m are in $\mathbb{Z}/\ell^m\mathbb{Z}$. By the semisimplicity assumption, the action of π^n is diagonalizable over $\mathcal{O}_\ell/\ell^m\mathcal{O}_\ell$ for any $m \geq 1$. This is equivalent to say there exists $X \in \mathrm{GL}_2(\mathcal{O}_\ell/\ell^m\mathcal{O}_\ell)$ such that

$$\pi^n = X \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} X^{-1} \text{ mod } \ell^m.$$

But we proved that $\lambda_1 \equiv \lambda_2$ mod ℓ^m. Therefore

$$\pi^n = XX^{-1} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_1 \end{bmatrix} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_1 \end{bmatrix} \text{ mod } \ell^m.$$

Since $\pi^n \bmod \ell^m \in \mathrm{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z})$, the lemma follows. □

- $\star$ If ℓ is ramified in $\mathcal{O}_K$, then it is possible that the Frobenius action π^n is not semisimple. But Recall that we assumed on n such that for ℓ ramified in $\mathcal{O}_K$, $(n, \ell) \neq 1$. This implies for all such $\ell \mid \Delta_K$, the power of ℓ dividing Δ_{π^n} is bounded independent of n. Therefore we have the following corollary:

Corollary 3.4.3. *Let n be an integer such that for all prime $\ell \mid \Delta_K$, $(n, \ell) = 1$. Let S be the set of all primes that divides Δ_K. Then the number of ℓ-power isogenies where $\ell \in S$ is bounded independent of n. In other words, this number does not grow with n.*

We make the table of classification of the Frobenius action under the semisimplicity assumption as follows:

(a). Assume ℓ, m, n such that $\chi_{\pi^n} \bmod \ell^m$ is irreducible modulo ℓ^m. In this case π^n acts on $E[\ell^m]$ as a distortion map. I.e., no subgroups $\mathbb{Z}/\ell^m\mathbb{Z}$ is stabilized by π^n. Therefore E has no ℓ^m-isogenies defined over $\mathbb{F}_{q^n}$.

(b.1). Assume ℓ, m, n such that π^n is diagonalizable mod ℓ^m. Moreover, χ_{π^n} has distinct eigenvalues λ and μ modulo ℓ^m. In this case, the Frobenius acts on $E[\ell^m]$ as a matrix conjugates to $\begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}$ and there are two isogenies of degree ℓ^m from E which are defined over $\mathbb{F}_{q^n}$, given by E modulo cyclic subgroups generated by the two eigenvectors of λ and μ respectively.

(b.2). Assume ℓ, m, n such that π^n is diagonalizable mod ℓ^m. Moreover, the Frobenius χ_{π^n} modulo ℓ^m has one eigenvalue λ of multiplicity two. In this case, the Frobenius acts on $E[\ell^m]$ as a scalar multiple by $\begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$ and every ℓ^m subgroup is stable under π^n. Therefore, there are $\ell^m + \ell^{m-1} + \cdots + 1$ ℓ-power isogenies of degree less than or equal to ℓ^m from E which are defined over $\mathbb{F}_{q^n}$.

(b.3). Assume ℓ, m, n such that π^n is diagonalizable mod ℓ^m. Assume that χ_{π^n} has distinct eigenvalues λ and μ modulo ℓ^m but eigenvalues are congruent modulo

ℓ^r for some $1 < r < m$. In this case, the Frobenius acts on $E[\ell^r]$ as a matrix conjugates to $\begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$ and there are $\ell^r + \ell^{r-1} + \cdots + 1$ ℓ-power isogenies of degree less than or equal to ℓ^m from E which are defined over $\mathbb{F}_{q^n}$.

3.4.2 Horizontal isogenies

As one may notice, there are a lot of prime power isogenies of E that are indeed endomorphisms of E. By the theory of complex multiplications, the number of such isogenies is bounded by the class number of $\mathcal{O}_K$, see Theorem 3.4.6. We give information about when such isogenies arise and use the information to bound the total number of isogenies defined over $\mathbb{F}_{q^n}$.

We use the classification of the Frobenius action on the ℓ-torsion subgroups to compute each case's horizontal prime power isogenies.

Definition 3.4.4. Let $f\colon E \to E'$ be an isogeny of degree ℓ^m. We say f is *horizontal* if $\mathrm{End}(E) = \mathrm{End}(E')$.

Let $\mathfrak{a}$ be an invertible ideal in $\mathrm{End}(E)$. Define the $\mathfrak{a}$-torsion subgroup of E as

$$E[\mathfrak{a}] := \left\{P \in E\left(\overline{\mathbb{F}}_q\right) \mid \sigma(P) = 0 \text{ for all } \sigma \in \mathfrak{a}\right\}.$$

Let $\phi_{\mathfrak{a}}$ be an isogeny whose kernel is $E[\mathfrak{a}]$. Then the codomain $E/E[\mathfrak{a}]$ is a well-defined elliptic curve. The isogeny $\phi_{\mathfrak{a}}$ is horizontal, and its degree equals the ideal norm of $\mathfrak{a}$. We denote by $\mathfrak{a} \cdot E$ for the isomorphism class of the image of $\phi_{\mathfrak{a}}$.

Lemma 3.4.5. *Let E_{q^n} be an ordinary elliptic curve over $\mathbb{F}_{q^n}$ with the Frobenius action by π^n. Let $H(\ell^m)$ denote the number of horizontal ℓ^m-isogenies.*

$$H(\ell^m) = \begin{cases} 0, & \text{if } \pi^n \text{ is irreducible} \\ 1, & \text{if } \pi^n \text{ is diagonalizable with one eigenvalue modulo } \ell^m \\ 2, & \text{if } \pi^n \text{ is diagonalizable with two eigenvalues modulo } \ell^m \end{cases}.$$

Proof. If Δ_{π^n} is not a square modulo ℓ^m, we are in case (a) where no subgroup of order ℓ^m is stabilized by the action of π^n. Therefore no ℓ^m-isogeny is defined over $\mathbb{F}_{q^n}$.

Suppose π^n is diagonalizable with one eigenvalue modulo ℓ^m. In that case, we are in case (b.2) (and (b.3)), and there is one horizontal isogeny given by $\mathfrak{a} = (\pi^n - \lambda, \ell^m)$ with norm ℓ^m. Moreover, $\phi_{\mathfrak{a}}$ is self-dual.

If π^n is diagonalizable with two eigenvalues modulo ℓ^m, we are in case (b.1). There are two torsion subgroups of order ℓ^m, generated by the eigenvector of λ and μ, respectively. The two horizontal isogenies are given by the ideals $\mathfrak{a} = (\pi^n - \lambda, \ell^m)$ and $\hat{\mathfrak{a}} = (\pi^n - \mu, \ell^m)$. Furthermore, $\mathfrak{a}\hat{\mathfrak{a}} = (\ell^m)$ implying that $\mathfrak{a}$ and $\hat{\mathfrak{a}}$ are the inverse of one another in the class group, thus $\phi_{\hat{\mathfrak{a}}}$ is the dual isogeny of $\phi_{\mathfrak{a}}$.

□

Recall that for an elliptic curve E with CM by an order $\mathcal{O}$, horizontal ℓ-isogenies correspond to the CM action of an invertible $\mathcal{O}$-ideal of norm ℓ. Moreover, let $\mathrm{Ell}_q(\mathcal{O})$ be the set

$$\mathrm{Ell}_q\left(\mathcal{O}\right) := \left\{E/\mathbb{F}_q : \mathrm{End}(E) \simeq \mathcal{O}\right\}.$$

Because elliptic curves in $\mathrm{Ell}_q(\mathcal{O})$ are connected exclusively by horizontal cyclic isogenies, the theory of complex multiplication tells us:

Theorem 3.4.6. *Let E be an elliptic curve with endomorphism ring $\mathcal{O}$. Then the set of horizontal isogenies forms a principal homogeneous space under the class group of $\mathcal{O}$. To be precise, assume the set is non-empty. Then it is a principal homogeneous space for the class group $\mathcal{C}\ell(\mathcal{O})$, under the action*

$$\mathcal{C}\ell(\mathcal{O}) \times \mathrm{Ell}_q(\mathcal{O}) \longrightarrow \mathrm{Ell}_q(\mathcal{O}), \tag{3.4.1}$$

$$(\mathfrak{a}, E) \longmapsto \mathfrak{a} \cdot E \tag{3.4.2}$$

with cardinality equal to the class number $h(\mathcal{O})$.

Proof. See for example [27, Chapter II].

□

3.4.3 Proof of Theorem 3.1.2

Fix an ordinary elliptic curve E over $\mathbb{F}_q$ as in the previous context. Assume $\mathrm{End}(E) = \mathcal{O}$. We compute the size of $I(q^n, E)$, which can be interpreted as the number of certain cyclic subgroups. We consider two kinds of subgroups; one is that the subgroups are the kernel of some horizontal isogenies, and the other is where the subgroups define non-horizontal isogenies.

Let $\{\ell_i\}$, $1 \leq i \leq k$ be the set of prime divisors of Δ_{π^n} which are unramified in $\mathcal{O}_K$. For each i, let m_i be the *maximal* integer such that $\ell^{2m} \mid \Delta_{\pi^n}$. By Lemma 3.4.2, the n-Frobenius action is diagonalizable and The classification $(b.2)$ tells us that every ℓ^j-subgroup, $1 \leq j \leq m$ is defined over F_{q^n}. For ordinary elliptic curves, $\Delta_{\pi^n} \neq 0$, so only finitely many primes divide Δ_{π^n}.

Lemma 3.4.7. *We have*

$$N(q^n, E) \asymp (\prod_{i=1}^{k} \ell_i^{m_i})^{1-\epsilon}.$$

Proof. Denote by $\mathrm{Ell}_{q,\mathrm{as/ds}}(\mathcal{O})$ the isomorphism classes of elliptic curves that admit an ascending/descending isogeny to E. Thus

$$N(q^n, E) = |\,\mathrm{Ell}_{q,\mathrm{as/ds}}(\mathcal{O})| + |\,\mathrm{Ell}_q(\mathcal{O})|.$$

Since we have the assumptions on n, by Lemma 3.4.2, π^n is diagonalizable modulo any power of $\ell_1, \cdots, \ell_k$, and by Corollary 3.4.3, the number of ramified prime-power isogenies does not grow with n. Thus we only have to consider isogenies from cases where the Frobenius action is diagonal, i.e., the number of isogenies grows with n. By Theorem 3.4.6, the number of horizontal isogenies $|\,\mathrm{Ell}_q(\mathcal{O})| = h(\mathcal{O})$ is a fixed number once we fix E.

The number of non-horizontal isogenies is roughly the number of cyclic subgroups of order less than or equal to $\ell_1^{m_1} \cdots \ell_k^{m_k}$, up to minus $h(\mathcal{O})$. This is because Lemma 3.4.5 implies that if $\Delta_{\pi^n} \equiv 0 \bmod \ell^m$, there is always a horizontal ℓ-power isogeny, and Theorem 3.4.6 tells us there are at most $h(\mathcal{O})$ horizontal isogenies come from this form. By Theorem 3.2.5, For any cyclic subgroup G of $\mathbb{Z}/\ell_1^{m_1} \cdots \ell_k^{m_k}\mathbb{Z}$, there are at most

$(\ell_1^{m_1}\cdots\ell_k^{m_k})^\epsilon$ cyclic subgroups that give quotient curves isomorphic to E/G. Therefore

$$N(q^n,E)=\prod_{i=1}^{k}(\ell_i^{m_i}+\ell_i^{m_i-1}+\cdots+\ell)/(\ell_1^{m_1}\cdots\ell_k^{m_k})^\epsilon \tag{3.4.3}$$

$$\asymp(\ell_1^{m_1}\cdots\ell_k^{m_k})^{1-\epsilon} \tag{3.4.4}$$

□

Proof of Theorem 3.1.2. Lemma 3.4.7 asserts that we can write $N(q^n,E)$ as a product of $\ell_1^{m_1},\cdots,\ell_k^{m_k}$; on the other hand, for large n, the product well approximates the square root of Δ_{π^n}:

$$\prod_{i=1}^{k}\ell_i^{m_i}\asymp\Delta_{\pi^n}^{\frac{1}{2}}\asymp q^{\frac{n}{2}}.$$

The theorem follows.

□

3.4.4 Proof of Theorem 3.1.1

Proof of Theorem 3.1.1. Let $A=E\times E_{ss}$ be an abelian surface defined over $\mathbb{F}_q$, with the assumption that E is the same ordinary elliptic curve as in the previous section. The Frobenius π_A^n acts on the ℓ-adic Tate modules of A by a conjugacy to

$$\left(\begin{array}{c|cc} \pi^n & \multicolumn{2}{c}{0} \\ \hline & q^{n/2} & 0 \\ 0 & & \\ & 0 & q^{n/2} \end{array}\right)$$

where π^n is the Frobenius of E over $\mathbb{F}_{q^n}$. For the set of prime divisors of Δ_{π^n} which are unramified in $\mathcal{O}_K$ and positive integers n such that $(n,\ell)\neq 1$, we want to count the number of inequivalent maximal isotropic planes defined over $\mathbb{F}_{q^n}$. By definition of m_i, for each $1\leq i\leq k$, π_A^n acts as a scalar on $A[\ell_i^{m_i}]$.

Corollary 3.3.7 together with the equality

$$\prod_{i=1}^{k}\ell_i^{m_i}\asymp q^{\frac{n}{2}}$$

indicate that for a positive density set of n, we have

$$N(q^n, A) \gg ((\ell_1^{m_1} \cdots \ell_k^{m_k})^{2-\epsilon}) = q^{n+\epsilon}$$

for some $\epsilon > 0$.

□

Bibliography

[1] Jeffrey Achter and Cassie Williams. “Local Heuristics and an Exact Formula for Abelian Surfaces Over Finite Fields”. In: *Canadian Mathematical Bulletin* 58 (Mar. 2014).

[2] Jeffrey D. Achter and Clifton L.R. Cunningham. “Isogeny Classes of Hilbert–Blumenthal Abelian Varieties over Finite Fields”. In: *Journal of Number Theory* 92.2 (2002), pp. 272–303.

[3] Benjamin Bakker and Jacob Tsimerman. “p-torsion monodromy representations of elliptic curves over geometric function fields”. In: *Annals of Mathematics* 184.3 (2016), pp. 709–744.

[4] Tejasi Bhatnagar and Yu Fu. *Classification of some abelian varieties with real multiplication over finite fields.* Preprint.

[5] Lucia Caporaso, Joe Harris, and Barry Mazur. “Uniformity of rational points”. In: *J. Amer. Math. Soc.* 10.1 (1997), pp. 1–35.

[6] Wouter Castryck et al. “The dimension growth conjecture, polynomial in the degree and without logarithmic factors”. In: *Algebra & Number Theory* 14.8 (2020), pp. 2261 –2294.

[7] Alina Carmen Cojocaru and Chris Hall. “Uniform results for Serre’s theorem for elliptic curves”. In: *International Mathematics Research Notices* 2005.50 (2005), pp. 3065–3080.

[8] Pierre Deligne. “Variétés abéliennes ordinaires sur un corps fini”. In: *Inventiones mathematicae* 8.3 (1969), pp. 238–243.

[9] J. Ellenberg and A. Venkatesh. “On uniform bounds for rational points on non-rational curves”. In: *International Mathematics Research Notices* 2005.35 (2005), pp. 2163–2181.

[10] Jordan S. Ellenberg et al. “Non-simple abelian varieties in a family: geometric and analytic approaches”. In: *Journal of the London Mathematical Society* 80.1 (2009), pp. 135–154.

[11] E. S. Halberstadt and Alain Kraus. “On the modular curves YE(7)”. In: *Math. Comput.* 69 (2000), pp. 1193–1206.

[12] M. Hall. *The Theory of Groups*. Dover Books on Mathematics. Dover Publications, 2018.

[13] D. R. Heath-Brown. “The Density of Rational Points on Curves and Surfaces”. In: *Annals of Mathematics* 155.2 (2002), pp. 553–598.

[14] H. W. Lenstra. “Factoring Integers with Elliptic Curves”. In: *Annals of Mathematics* 126.3 (1987), pp. 649–673.

[15] Davesh Maulik, Ananth N. Shankar, and Yunqing Tang. “Picard ranks of K3 surfaces over function fields and the Hecke orbit conjecture”. In: *Inventiones Mathematicae* 228.3 (2022), pp. 1075–1143.

[16] B. Mazur and D. Goldfeld. “Rational isogenies of prime degree”. In: *Inventiones mathematicae* 44.2 (1978), pp. 129–162.

[17] David Mumford. *Abelian varieties.* English. Vol. 5. Tata Inst. Fundam. Res., Stud. Math. London: Oxford University Press, 1970.

[18] Abhishek Oswal and Ananth N. Shankar. “Almost ordinary abelian varieties over finite fields”. In: *Journal of the London Mathematical Society* 101.3 (2020), pp. 923–937.

[19] Marcelo Paredes and Román Sasyk. “Uniform bounds for the number of rational points on varieties over global fields”. In: *Algebra & Number Theory* 16.8 (2022), pp. 1941–2000.

[20] Fabien Pazuki. “Modular invariants and isogenies”. In: *International Journal of Number Theory* 15.03 (2019), pp. 569–584.

[21] A Reverter and N Vila. “Galois representations attached to the product of two elliptic curves”. In: *The Rocky Mountain Journal of Mathematics* 30.3 (2000), pp. 1121–1127.

[22] Damien Robert. “Fonctions thêta et applications à la cryptographie”. Theses. Université Henri Poincaré - Nancy I, July 2010.

[23] Jean-Pierre Serre. *Lectures on the Mordell-Weil Theorem.* Aspects of Mathematics. Vieweg+Teubner Verlag Wiesbaden, 1989.

[24] Ananth N. Shankar and Jacob Tsimerman. “Unlikey Intersections In Finite Characteristic”. In: *Forum of Mathematics, Sigma* 6 (2018), e13.

[25] Ananth N. Shankar et al. “Exceptional jumps of Picard ranks of reductions of K3 surfaces over number fields”. In: *Forum of Mathematics, Pi* 10 (2022).

[26] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics. Springer New York, 2009.

[27] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* 1994.

[28] Miguel N. Walsh. “Bounded Rational Points on Curves”. In: *International Mathematics Research Notices* 2015.14 (2014), pp. 5644–5658.

[29] William C. Waterhouse. “Abelian varieties over finite fields”. en. In: *Annales scientifiques de l’École Normale Supérieure* Ser. 4, 2.4 (1969), pp. 521–560.