A Uniform Version of a Finiteness Conjecture for Elliptic Curves with Complex Multiplication

By

Abbey M. Bourdon

Faculty Advisor: Christopher Rasmussen,

Assistant Professor of Mathematics

Wesleyan University

Middletown, CT

May 2014

A Dissertation in Mathematics

submitted in partial fulfillment of the

requirements for the degree of Doctor of Philosophy

Abstract

Let A be an abelian variety defined over a number field F. For a prime number ℓ, we consider the field extension of F generated by the ℓ-powered torsion points of A. According to a conjecture made by Rasmussen and Tamagawa, if we require this field to be both a pro-ℓ extension of $F(\mu_{\ell^\infty})$ and unramified away from ℓ, examples are quite rare. Indeed, it is expected that for a fixed dimension and field of definition, there exists such an abelian variety for only a finite number of primes.

We prove a uniform version of the conjecture in the case where the abelian varieties are elliptic curves with complex multiplication. In addition, we provide explicit bounds in cases where the number field has degree less than or equal to 100.

Acknowledgements

I am very grateful to my advisor, Chris Rasmussen, for suggesting the problem and for his guidance and support throughout the preparation of this work. I also very much appreciate the helpful comments of my committee members, Wai Kiu Chan and David Pollack.

Finally, I would like to extend a special thanks to my parents, without whom this would not have been possible.

Contents

Notation

- μ_ℓ denotes the group of ℓth roots of unity in $\bar{\mathbb{Q}}$, and $\mu_{\ell^\infty} = \cup_{n\geq 1}\mu_{\ell^n}$.
- For an abelian variety A defined over a field F, we denote the extension of F generated by the ℓ-torsion points of A by $F(A[\ell])$. The field $F(A[\ell^\infty])$ is generated over F by the ℓ-powered torsion points of A
- If F is a number field, d_F is the absolute discriminant of $F/\mathbb{Q}$. We denote the ring of integers of F by $\mathcal{O}_F$, and $\mathcal{O}_F^\times$ is its group of units.
- w_F denotes the number of distinct roots of unity in a number field F.
- If $\mathfrak{a}$ is an integral ideal in the number field F, we denote the norm of $\mathfrak{a}$ by $\mathcal{N}(\mathfrak{a})$. In other words, $\mathcal{N}(\mathfrak{a}) = [\mathcal{O}_F : \mathfrak{a}]$.
- If $\mathcal{O}$ is an order in an imaginary quadratic field K, then $h(\mathcal{O})$ denotes the cardinality of the ideal class group of $\mathcal{O}$. In particular, $h(\mathcal{O}_K) = h_K$, the class number of K.
- F_s denotes the separable closure of a field F.
- $\left(\frac{a}{\ell}\right)$ is the Kronecker symbol.

1 Introduction

1.1 Ihara's Question

One of the current guiding problems in number theory is to describe the structure of the absolute Galois group, $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. While partial solutions exist—such as the complete description of all abelian extensions of $\mathbb{Q}$ provided by class field theory—the general problem has thus far eluded any direct approach. Instead, we may seek to understand $G_{\mathbb{Q}}$ by examining its action on other objects. These so-called Galois representations arise naturally in a wide variety of ways and are associated to objects ranging from modular forms to points on abelian varieties. However, there is one example which appears particularly promising, in that it encodes all the structure of $G_{\mathbb{Q}}$ and more: the action of $G_{\mathbb{Q}}$ on the outer automorphism group of the algebraic fundamental group of $\mathbb{P}^1_{\bar{\mathbb{Q}}} \setminus \{0, 1, \infty\}$.

For our purposes we may define the algebraic fundamental group of a connected scheme X as $\pi_1(X) := \varprojlim \mathrm{Aut}_X(X_i)$, where $\{X_i\}$ is the collection of all finite étale Galois covers $f_i : X_i \to X$ and $\mathrm{Aut}_X(X_i)$ is the group of automorphisms of X_i compatible with f_i. This is reminiscent of how we may view the topological fundamental group as the group of deck transformations of the universal cover, and indeed for any scheme of finite type over $\mathbb{C}$ we find $\pi_1(X)$ is isomorphic to the profinite completion of the topological fundamental group of $X(\mathbb{C})$. If X is quasi-compact and geometrically integral over a field F and $\bar{X}$ denotes its base change to the separable closure of F, we may relate the fundamental groups of X and $\bar{X}$ via the following exact sequence (for a

proof, see for example Prop. 5.6.1 in [42]):

$$1 \to \pi_1(\bar{X}) \to \pi_1(X) \to \mathrm{Gal}(F_s/F) \to 1. \ ^{1}$$

Conjugation by a lift of an element in $\mathrm{Gal}(F_s/F)$ then defines a natural representation separable closure of F, we may relate the fundamental groups of X and $\bar{X}$ via the following exact sequence (for a proof, see for example Prop. 5.6.1 in [42]):

$$\Phi\colon \mathrm{Gal}(F_s/F) \to \mathrm{Out}(\pi_1(\bar{X})),$$

often referred to as the "outer Galois representation."

In the case where $X = \mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$, we have the following key result of Belyĭ:

Theorem 1 (Belyĭ, [5])**.** *The outer Galois representation*

$$\Phi\colon G_{\mathbb{Q}} \to \mathrm{Out}(\pi_1(\mathbb{P}^1_{\bar{\mathbb{Q}}} \setminus \{0, 1, \infty\}))$$

is injective.

Thus to explain the structure of $G_{\mathbb{Q}}$, it will suffice to understand the structure of $\mathrm{Out}(\pi_1(\bar{X}))$. As the topological fundamental group of the complex manifold corresponding to $\bar{X}$ is a free group on two generators, F_2, in essence we find all of the mystery of $G_{\mathbb{Q}}$ is contained in $\mathrm{Out}(\hat{F}_2)$.

Although this result is promising, using the structure of $\mathrm{Out}(\pi_1(\bar{X}))$ as a means of explaining $G_{\mathbb{Q}}$ has proved quite difficult. One line of investigation that stems from work of Drinfel'd [12] and Ihara [17], [18] studies a lift

$$\Phi\colon G_{\mathbb{Q}} \to \mathrm{Aut}(\pi_1(\mathbb{P}^1_{\bar{\mathbb{Q}}} \setminus \{0, 1, \infty\}))$$

to achieve the containment of $G_{\mathbb{Q}}$ in a subgroup of $\mathrm{Aut}(\pi_1(\bar{X}))$ known as the profinite Grothendieck-Teichmüller group, $\widehat{GT}$.[2] It is an open question whether or not $G_{\mathbb{Q}}$ is actually isomorphic to $\widehat{GT}$, and describing the relationship between $G_{\mathbb{Q}}$ and $\widehat{GT}$ is

[1] Some texts refer to $\pi_1(X)$ as the arithmetic or étale fundamental group of X and $\pi_1(\bar{X})$ as the geometric fundamental group of X, though this terminology is not standardized.

[2] While the definition of $\widehat{GT}$ is beyond the scope of this text, we direct the interested reader to a survey article of Schneps [34].

currently an active area of research. (See, for example, recent work by Hatcher, Lochak, Nakamura, and Schneps in [14] and [24].)

Another approach to studying Φ, championed by Ihara in the 1980s, is to fix a prime number ℓ and consider the associated representation involving the pro-ℓ fundamental group of $\bar{X}$. Since $\pi_1^\ell(\bar{X})$ is the maximal pro-ℓ quotient of $\pi_1(\bar{X})$, it is a characteristic quotient of $\pi_1(\bar{X})$, and we may define $\Phi_\ell \colon G_F \to \mathrm{Out}(\pi_1^\ell(\bar{X}))$ via the following commutative diagram:

$$\begin{array}{ccc} G_F & \xrightarrow{\Phi} & \mathrm{Out}(\pi_1(\bar{X})) \\ & \searrow^{\Phi_\ell} & \downarrow \\ & & \mathrm{Out}(\pi_1^\ell(\bar{X})) \end{array}$$

While the hope is that Φ_ℓ will prove more manageable to study than Φ, the cost of this simplification is a loss of injectivity. Describing the fixed field of the kernel of Φ_ℓ, which we will denote $\text{山}(\mathbb{Q}, \ell)$,[3] is thus a natural first step. We know from Ihara's 1986 paper [16] that $\text{山}(\mathbb{Q}, \ell)$ is a pro-ℓ extension of $\mathbb{Q}(\mu_{\ell^\infty})$ unramified away from ℓ, but it is still an open question, first posed by Ihara, to determine whether $\text{山}(\mathbb{Q}, \ell)$ is the *maximal* such extension. A conjecture of Deligne gives some evidence for an affirmative answer for odd regular primes ℓ, as shown by Sharifi in [36], but all other attempts to determine maximality have identified explicit subfields of $\text{山}(\mathbb{Q}, \ell)$ arising naturally from geometric objects such as Fermat curves and principal modular curves.

As an example, we will describe possible subfields of $\text{山}(\mathbb{Q}, \ell)$ arising from abelian varieties. For an abelian variety A defined over $\mathbb{Q}$ and a rational prime ℓ, we let $\mathbb{Q}(A[\ell])$ denote the field extension of $\mathbb{Q}$ generated by ℓ torsion points of A and $\mathbb{Q}(A[\ell^\infty])$ the field extension generated by ℓ-powered torsion points of A. We recall $\mathbb{Q}(A[\ell^\infty])$ is a pro-ℓ extension of $\mathbb{Q}(A[\ell])$, and by Serre and Tate in [35] we know that this extension is unramified away from ℓ when A has good reduction away from ℓ. Thus for any A with

[3]The kanji 山 is read *san*. Motivation for this notation is discussed in [32].

1. $\mathbb{Q}(A[\ell])/\mathbb{Q}(\mu_\ell)$ an extension of ℓ-powered degree, and

2. good reduction away from ℓ,

the field $\mathbb{Q}(A[\ell^\infty])$ is a pro-ℓ extension of $\mathbb{Q}(\mu_{\ell^\infty})$ unramified away from ℓ. In this case $\mathbb{Q}(A[\ell^\infty])$ can either provide an explicit example of a subfield of $Ш(\mathbb{Q}, \ell)$ or else a negative answer to Ihara's question.

Many explicit fields constructed in this way have been shown to be subfields of $Ш(\mathbb{Q}, \ell)$. For example, we have the following results for an elliptic curve $E/\mathbb{Q}$:

Theorem 2 (Rasmussen, [30])**.** *If E has good reduction away from 2, the field $\mathbb{Q}(E[2^\infty])$ is contained in $Ш(\mathbb{Q}, 2)$.*

Theorem 3 (Papanikolas, Rasmussen, [28])**.** *If E has good reduction away from 3, the field $\mathbb{Q}(E[3^\infty])$ is contained in $Ш(\mathbb{Q}, 3)$.*

Theorem 4 (Rasmussen, Tamagawa, [33])**.** *If E has complex multiplication by $\mathbb{Q}(\sqrt{-\ell})$ and good reduction away from a rational prime ℓ, the field $\mathbb{Q}(E[\ell^\infty])$ is a subfield of $Ш(\mathbb{Q}, \ell)$.*

It is interesting to note that for elliptic curves over $\mathbb{Q}$ with $\mathbb{Q}(E[\ell^\infty])$ a pro-ℓ extension of $\mathbb{Q}(\mu_{\ell^\infty})$ unramified away from ℓ, there are only two isogeny classes that do not fall under one of the three theorems stated above: 121a and 121c.[4] As Rasmussen and Tamagawa remark in [33], it is possible that the torsion point fields associated to these curves provide a negative answer to Ihara's question and consequently a counterexample to Deligne's conjecture mentioned above. For more on these two exceptions, see [31].

1.2 Finiteness Conjecture

Abelian varieties with torsion point fields that provide test cases for Ihara's question—namely, those satisfying properties (1) and (2) above—are actually quite rare. For

[4]This is Cremona's notation. See [9].

example, in the case of elliptic curves over $\mathbb{Q}$, Rasmussen and Tamagawa show in [33] there are only 50 $\mathbb{Q}$-isomorphism classes with the desired properties, even as we allow ℓ to vary over all the primes. In particular, there are no such examples for $\ell > 163$. This phenomenon appears to hold if we consider both higher-dimensional abelian varieties and abelian varieties defined over arbitrary number fields. Explaining this observation is the goal of Rasmussen and Tamagawa's joint works [33] and [32], and the scarcity of such abelian varieties is the topic of their finiteness conjecture.

More precisely, let $\mathscr{A}(F, g, \ell)$ be the set of F-isomorphism classes of abelian varieties A/F of dimension g for which $F(A[\ell^\infty])$ is both a pro-ℓ extension of $F(\mu_{\ell^\infty})$ and unramified away from ℓ. We will use $\mathscr{A}(F, g)$ to denote the disjoint union of the $\mathscr{A}(F, g, \ell)$ over the set of all primes ℓ, i.e., $\mathscr{A}(F, g) := \{([A], \ell) : [A] \in \mathscr{A}(F, g, \ell)\}$. Then we may state the Rasmussen-Tamagawa finiteness conjecture as follows:

Conjecture 1 (Rasmussen, Tamagawa, [33])**.** *Let F be a number field and $g > 0$. The set $\mathscr{A}(F, g)$ is finite. Thus there exists a constant $C(F, g)$ for which $\mathscr{A}(F, g, \ell) = \varnothing$ when $\ell > C(F, g)$.*

Several cases of Conjecture 1 have been established. In the same 2008 paper, Rasmussen and Tamagawa prove that curves in $\mathscr{A}(F, 1)$ possess an F-rational ℓ-isogeny, and if $F = \mathbb{Q}$ there are only a limited number of primes for which this can occur by a celebrated result of Mazur ([21]). A theorem of Momose [23] extends Mazur's result to almost all quadratic fields. This yields:

Theorem 5 (Rasmussen, Tamagawa, [33])**.** *If F is a number field of degree 1 or 2 that is not an imaginary quadratic field of class number one, then the set $\mathscr{A}(F, 1)$ is finite. Moreover, $C(\mathbb{Q}, 1) = 163$.*

In fact, $C(\mathbb{Q}, 1) = 163$ is the best possible bound, as Rasmussen and Tamagawa give an example of an elliptic curve defined over $\mathbb{Q}$ with $\mathbb{Q}(E[163^\infty])$ a pro-163 extension of $\mathbb{Q}(\mu_{163})$.

Other partial proofs of the conjecture have been found under additional assumptions on the abelian varieties in question. For example, Ozeki determined that for ℓ sufficiently large, the ℓ-adic Galois representation that would be associated to $A \in \mathscr{A}(F, g, \ell)$ cannot exist if A has everywhere semistable reduction. This implies the following theorem, where $\mathscr{A}(F, g, \ell)_{st}$ denotes the set of F-isomorphism classes of abelian varieties in $\mathscr{A}(F, g, \ell)$ with semistable reduction.[5]

Theorem 6 (Ozeki, [25]). *Let F be a number field of degree n and discriminant d_F. Then $\mathscr{A}(F, g, \ell)_{st}$ is empty if:*

1. *$\ell \nmid d_F$ and $\ell > 2^{\delta_1}\binom{2g}{g}$, where $\delta_1 := 2ng + 1$;*
2. *n is odd and $\ell > 2^{\delta_2}\binom{2g}{g}$, where $\delta_2 := 2n^2g + 1$.*

In a subsequent paper, Ozeki was able to prove the non-existence of certain abelian varieties with abelian ℓ-adic Galois representation, implying the following case of Conjecture 1:

Theorem 7 (Ozeki, [26]). *The set of F-isomorphism classes of abelian varieties in $\mathscr{A}(F, g, \ell)$ which have complex multiplication over F is empty for any prime ℓ large enough.*

The strongest evidence for Conjecture 1 to date appears in a new paper by Rasmussen and Tamagawa, [32], in which they prove that the Generalized Riemann Hypothesis implies the conjecture.

Theorem 8 (Rasmussen, Tamagawa [32]). *Let F be a number field with Galois closure $\tilde{F}$ over $\mathbb{Q}$, and let $g > 0$. For all $\ell \gg 0$, assume the Generalized Riemann Hypothesis holds for the Dedekind zeta functions of number fields of the form $L\tilde{F}$, where L is a subfield of $\mathbb{Q}(\mu_\ell)$. Then $\mathscr{A}(F, g)$ is finite.*

[5] In [32], Rasmussen and Tamagawa offer another proof of Conjecture 1 in the case of abelian varieties with semistable reduction. Although the paper appeared later, their result existed earlier and their approach motivated Ozeki's work.

The surprising connection is made through a character $\chi(m_{\mathbb{Q}})$ constructed from the mod-ℓ Galois representation associated to an abelian variety from $\mathscr{A}(F,g)$. Given GRH, for large enough ℓ there exists a rational prime $p < \frac{\ell}{4g}$ and $\mathfrak{p} \mid p$ in F such that $\chi(m_{\mathbb{Q}})$ is trivial on a Frobenius element associated to $\mathfrak{p}$. However, by an argument inspired by Mazur's result on isogenies of elliptic curves ([21]), Rasmussen and Tamagawa conclude that $\chi(m_{\mathbb{Q}})$ does not vanish on such small primes.

In addition, they have the following unconditional cases obtained from examining the special fiber of a Néron model of the abelian varieties in question:

Theorem 9 (Rasmussen, Tamagawa [32])**.** *Let F be a number field of degree n. Then $\mathscr{A}(F,g)$ is finite in the following cases:*

1. *$n = 1$ and $g = 2, 3$*
2. *$n = 2, 3$ and $g = 1$*
3. *$F/\mathbb{Q}$ is a Galois extension of exponent 3 and $g = 1$.*

Other versions of the conjecture have appeared. Arai has explored the conjecture in the context of QM-abelian surfaces (see [2]), and in [27] Ozeki and Taguchi have a generalization of the conjecture which extends the result of Ozeki for semistable abelian varieties. However, the version of the conjecture most relevant for our purposes appears in a more recent work of Rasmussen and Tamagawa. It tells us that in fact we may expect the bound C to be uniform in the degree of $F/\mathbb{Q}$.

Conjecture 2 (Rasmussen, Tamagawa, [32])**.** *Let F be a number field and $g > 0$. There exists a constant C depending only on g and the degree of $F/\mathbb{Q}$ for which $\mathscr{A}(F,g,\ell) = \varnothing$ when $\ell > C$.*

As with the conditional proof of Conjecture 1, in certain cases the Generalized Riemann Hypothesis implies even this stronger conjecture:

Theorem 10 (Rasmussen, Tamagawa [32])**.** *Assume the Generalized Riemann Hypothesis. Then Conjecture 2 holds for any g and any F of odd degree.*

Unconditionally, we have the following:

Theorem 11 (Rasmussen, Tamagawa [32])**.** *Conjecture 2 holds in the case where $g = 1$ and F has degree 3.*

1.3 New Results

Despite this progress, Conjecture 2 is known unconditionally only in the case where $g = 1$ and $[F : \mathbb{Q}] = 1$ or 3. Moreover, aside from the case when $F = \mathbb{Q}$, any known bounds are likely far from optimal. In this thesis, we prove a result stronger than Conjecture 2 for elliptic curves with complex multiplication, and we give improved bounds for number fields of degree $1 < n \leq 100$. Specifically, we have the following theorem:

Theorem 12. *Let F be a number field with $[F : \mathbb{Q}] = n$. There exists a constant $C = C(n)$ depending only on n with the following property: If there exists a CM elliptic curve E/F with $F(E[\ell^\infty])$ a pro-ℓ extension of $F(\mu_\ell)$ for some rational prime ℓ, then $\ell \leq C$.*

We record the consequences of this theorem for Conjectures 1 and 2. Let $\mathscr{A}^{\mathrm{CM}}(F, g, \ell)$ be the subset of $\mathscr{A}(F, g, \ell)$ consisting of abelian varieties with complex multiplication, and define $\mathscr{A}^{\mathrm{CM}}(F, g) := \{([A], \ell) : [A] \in \mathscr{A}^{\mathrm{CM}}(F, g, \ell)\}$. Then as a direct consequence of Theorem 12, we have the following corollaries:

Corollary 1. *Let F be a number field with $[F : \mathbb{Q}] = n$. There exists a constant $C = C(n)$ depending only on n such that $\mathscr{A}^{\mathrm{CM}}(F, 1, \ell) = \varnothing$ if $\ell > C$.*

Corollary 2. *$\mathscr{A}^{\mathrm{CM}}(F, 1)$ is finite.*

Note that the bound of Theorem 12 is achieved even as we relax the ramification requirement, thereby allowing the inclusion of elliptic curves with bad reduction at primes other than ℓ. However, without the ramification requirement, we cannot guarantee (nor should we expect) a finiteness result as in Corollary 2. In addition, for the purposes of

comparison with Ozeki's result, it is important to emphasize that the theorem holds for elliptic curves with "potential CM," i.e., those elliptic curves with complex multiplication over $\bar{F}$.

The following table illustrates the computed bounds $C(n)$ for CM elliptic curves defined over a number field F of degree $n \leq 7$:

n	$C(n)$
1, 2	163
3, 4	907
5, 6	2683
7	5923

Generating these bounds depends on having an explicit list of the imaginary quadratic fields with a given class number, which currently exists for class numbers up to 100 (see [44]). In theory, our method will generate an explicit bound for CM elliptic curves defined over a number field F of any degree.

2 Elliptic Curves

2.1 Preliminaries

An elliptic curve E defined over a number field F is a curve in projective space that corresponds to solutions of a Weierstrass equation of the form

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \qquad a, b \in F$$

with **discriminant** $\Delta := -16(4a^3 + 27b^2) \neq 0$. The discriminant condition ensures the corresponding geometric object is nonsingular (with no cusps or self-intersections) and guarantees the curve will have genus one. For an equation of this form, $[0 : 1 : 0]$ is the only point on the curve with $Z = 0$, so we may instead consider the affine equation

$$y^2 = x^3 + ax + b,$$

and just remember there is an extra point $\mathscr{O} = [0 : 1 : 0]$ "at infinity."

The rich mathematical structure of elliptic curves comes from the fact that we may define a binary operation on the points of E so that they form an abelian group with identity $\mathscr{O}$. To add two points P and Q on E, we first find the line l_1 passing through P and Q. (If $P = Q$, we take l_1 to be the tangent line to the curve at P.) By a classical theorem of Bézout, l_1 will intersect our curve in exactly three points, counting multiplicity. We will call the third point of intersection R. Next, we find a second line, l_2, passing through R and $\mathscr{O}$, our point at infinity. The line l_2 intersects our curve at R, $\mathscr{O}$, and a third point. That third point of intersection is $P + Q$. We illustrate the

group law in Figure 1, which shows the graph of the real solutions of the elliptic curve corresponding to $y^2 = x^3 - 3x + 3$.

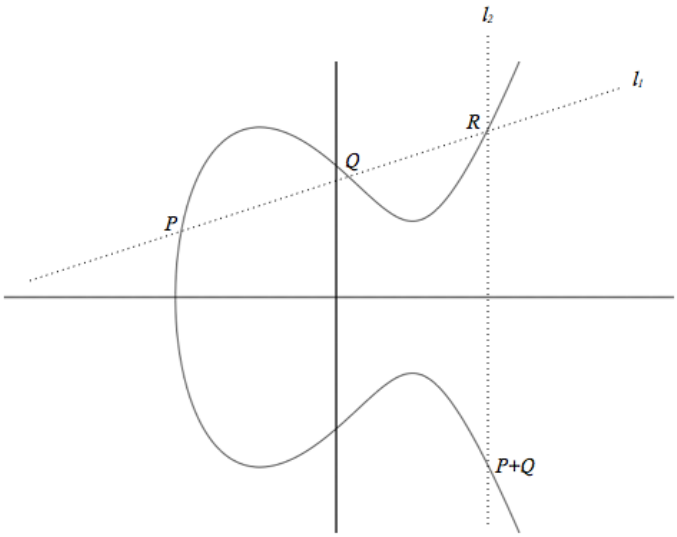


Figure 1

A morphism $\varphi : E_1 \to E_2$ of elliptic curves is a map locally defined by polynomials. That is:

Definition 1. Let E_1 and E_2 be defined over a number field F. If $\varphi : E_1 \to E_2$ is a **morphism** from E_1 to E_2, then for every $P \in E_1$ there exists a neighborhood U of P such that

$$\varphi|_U(P) = [f_0(P) : f_1(P) : f_2(P)]$$

for homogeneous $f_i \in \bar{F}[x_0, x_1, x_2]$ of the same degree. For an extension L/F, we say the morphism is L**-rational** or **defined over** L if $f_i \in L[x_0, x_1, x_2]$ for all P.

Note that a morphism need not respect the underlying group structure of our elliptic curves. Thus when we discuss maps between elliptic curves, we often require the following additional constraint:

Definition 2. An **isogeny** from E_1 to E_2 is a morphism φ from E_1 to E_2 such that $\varphi(\mathcal{O}) = \mathcal{O}$. The curves E_1 and E_2 are **isogenous** if φ is non-constant.

An isogeny of elliptic curves is in fact a group homomorphism:

Proposition 1. *Let φ be an isogeny from E_1 to E_2. Then $\varphi(P+Q) = \varphi(P) + \varphi(Q)$ for $P, Q \in E_1$.*

Proof. See Theorem III.4.8 in [40]. □

An important invariant for an isogeny is its degree, which in general is equal to the degree of the extension of function fields induced by the isogeny. However, in the case of elliptic curves over number fields we may define it as follows:

Definition 3. Let $\varphi : E_1 \to E_2$ be an isogeny. Then the **degree** of φ is the size of its kernel, i.e., $\deg(\varphi) := \#\varphi^{-1}(\mathscr{O})$.

If we say E possesses an n-isogeny for a positive integer n, we mean there exists an isogeny φ from E to another elliptic curve E' such that φ has degree n.

Before giving an example, we must introduce some notation. For a positive integer n and a point P on E, let $[n]P := P + P + \cdots + P$, or P added to itself n times. If n is a negative integer, let $[n]P := [-n](-P)$. Finally, $[0]P := \mathscr{O}$.

Example 1: For an integer n, we have the multiplication-by-n isogeny

$$[n] : E \to E, \qquad P \mapsto [n]P.$$

This is an isogeny of degree n^2. (See Theorem 6.2 in [40].)

There are two invariants associated to an elliptic curve E which we may obtain easily from its equation. One is the discriminant, Δ, which we have already defined. This value encodes information about how an elliptic curve behaves when reduced modulo a prime. Loosely, we say an elliptic curve has good reduction at a prime $\mathfrak{p} \in F$ if the equation we obtain by reducing the coefficients of our equation modulo $\mathfrak{p}$ is an elliptic curve over the corresponding finite field. More specifically, to determine the reduction type at $\mathfrak{p}$, we view the equation for E as defining a curve over the completion $F_{\mathfrak{p}}$. Considered over this local field, E has an equation called the minimal model with coefficients in the ring

of integers and a discriminant with minimal valuation (see Chapter 7 of [40] for details). Then if we let $\mathbb{F}_\mathfrak{p}$ denote the residue field of $F_\mathfrak{p}$, we have:

Definition 4. An elliptic curve E defined over a number field F has **good reduction** at a prime $\mathfrak{p} \in F$ if the minimal model for E with respect to $\mathfrak{p}$ defines a nonsingular curve over $\mathbb{F}_\mathfrak{p}$ when its coefficients are reduced modulo $\mathfrak{p}$. If the curve over $\mathbb{F}_\mathfrak{p}$ is singular, we say E has **bad reduction** at $\mathfrak{p}$.

From this definition, we may deduce the following:

Proposition 2. If $\mathfrak{p} \nmid \Delta$, then E has good reduction at $\mathfrak{p}$.[1]

Another invariant of E we may obtain directly from its Weierstrass equation is the j-invariant. For a curve with equation $y^2 = x^3 + ax + b$, we define the **j-invariant**:

$$j_E := -1728\frac{(4a)^3}{\Delta}.$$

This value characterizes the isomorphism class of E and also provides a kind of minimal field of definition for our elliptic curve:

Proposition 3. *1. Two elliptic curves are isomorphic over $\bar{F}$ if and only if they have the same j-invariant.*

2. Let E/F be an elliptic curve with j-invariant j_E. Then there exists an elliptic curve E' defined over $\mathbb{Q}(j_E)$ with j-invariant j_E.

Proof. See Proposition III.1.4 in [40]. □

It is important to note, however, that E' and E may not be isomorphic over F. That is, the isomorphism may not be defined by polynomials with coefficients in F.

[1] The complete reduction information for E is encoded in another invariant known as the conductor. See p. 256 of [40] for details.

2.2 Torsion Point Fields

As above, let E be an elliptic curve defined over a number field F.

Definition 5. The **n-torsion subgroup** is the subgroup of all points with order dividing n, denoted by $E[n]$. In other words, $E[n] := \{P \in E : [n]P = \mathscr{O}\}$.

Unlike with an arbitrary group, we are guaranteed the existence of n-torsion points for every positive integer n. In fact, we know the structure of the n-torsion subgroup explicitly:

Theorem 13. *Let E be an elliptic curve defined over a number field F. Then for any positive integer n,*

$$E[n] \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

Proof. See Corollary III.6.4 in [40]. □

For the purposes of this thesis, we are most interested in the field extensions generated by the coordinates of n-torsion points of our elliptic curve. If E is an elliptic curve defined over a number field F, we define this extension by $F(E[n]) := F(x, y : (x, y) \in E[n])$.

Example 2: Let E be the elliptic curve corresponding to the equation $y^2 = x^3 + 1$. One can check that

$$E[2] = \left\{\mathscr{O}, (-1, 0), \left(\frac{1+\sqrt{-3}}{2}, 0\right), \left(\frac{1-\sqrt{-3}}{2}, 0\right)\right\}.$$

Thus $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{-3})$.

Of course, once we consider torsion point fields for larger integers m, explicitly calculating the coordinates for m-torsion points becomes infeasible and we must rely on more general theory to obtain results.

Torsion point fields possess a number of interesting arithmetic properties, and the fact that they arise from a geometric object makes them all the more compelling. For example, we have the following classical results. In each we assume E is an elliptic curve defined over a number field F.

Proposition 4. *For a positive integer n, the extension $F(E[n])/F$ is a Galois extension of F containing the n-th roots of unity, i.e., $\mu_n \subset F(E[n])$.*

Proof. See the discussion on page 30 of [1] and Corollary III.8.1.1 in [40]. □

Theorem 14 (Criterion of Néron-Ogg-Shafarevich)**.** *Let ℓ be a prime number. If E has good reduction away from a prime $\mathfrak{p} \in F$ lying above ℓ, then $F(E[\ell])/F$ is unramified away from $\mathfrak{p}$.*

Proof. See Theorem VII.7.1 in [40]. □

2.3 Mod-n Galois Representation

Let E be an elliptic curve defined over a number field F, and let n be a positive integer. The Galois group $G_F := \mathrm{Gal}(\bar{F}/F)$ acts naturally on the points of E via their coordinates. That is, for $\sigma \in G_F$, we have $\sigma \cdot (x, y) := (\sigma(x), \sigma(y))$ for $(x, y) \in E$ and $\sigma \cdot \mathscr{O} := \mathscr{O}$. This Galois action is compatible with the group law of our elliptic curve, since for $P, Q \in E$, the coordinates of $P + Q$ are rational functions in the coordinates of P and Q with coefficients in F. Thus $\sigma(P + Q) = \sigma(P) + \sigma(Q)$, and it follows that σ sends n-torsion points to n-torsion points. This gives a G_F-action on $E[n]$, which is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2 by Theorem 13, and a choice of basis for $E[n]$ yields

$$\rho_{E,n} : G_F \to \mathrm{Aut}(E[n]) \cong GL_2(\mathbb{Z}/n\mathbb{Z}).$$

We call $\rho_{E,n}$ the **mod-n Galois representation** associated to E.

Example 3: Let $E : y^2 = x^3 + 1$ as above. Then $P_1 = (-1, 0), P_2 = \left(\frac{1+\sqrt{-3}}{2}, 0\right), P_3 = \left(\frac{1-\sqrt{-3}}{2}, 0\right)$ are the nontrivial points of $E[2]$. Note $P_1 + P_2 = P_3$, so we may take $\{P_1, P_2\}$

to be a basis for $E[2]$. If $\sigma' \in \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ is complex conjugation, $\sigma'(P_1) = P_1$ and $\sigma'(P_2) = P_3$. Thus

$$\rho_{E,2}(\sigma') = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

The kernel of $\rho_{E,n}$ is precisely $\mathrm{Gal}(\bar{F}/F(E[n]))$, which means $\rho_{E,n}$ induces an injection

$$\rho_{E,n} : \mathrm{Gal}(F(E[n])/F) \hookrightarrow GL_2(\mathbb{Z}/n\mathbb{Z}).$$

Thus $\mathrm{Gal}(F(E[n])/F)$ can be identified as a subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$, providing us with one tool for studying n-torsion point fields. For example, it is now immediate that the order of $\mathrm{Gal}(F(E[n])/F)$ divides $\#GL_2(\mathbb{Z}/n\mathbb{Z})$. Another implication is that results on torsion point fields of elliptic curves can have consequences for the mod-n Galois representation, as is the case with our main result.

One computationally useful property of the mod-n Galois representation stems from its connection to the cyclotomic character mod n, which we will denote by χ. Recall $\chi : G_F \to (\mathbb{Z}/n\mathbb{Z})^\times$ is defined by Galois action on a primitive n-th root of unity. That is, if ζ_n is a primitive n-th root of unity and $\sigma \in G_F$, then $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$.

Proposition 5. *Let χ be the mod n cyclotomic character. Then $det(\rho_{E,n}) = \chi$.*

The proof of this proposition relies on the Weil pairing, which is a map $e_n : E[n] \times E[n] \to \mu_n$. While we direct the interested reader to section III.8 of [40] for the formal definition of e_n, we note here some of its useful properties.

Proposition 6. *The Weil pairing e_n is:*

1. *Bilinear:*

   $e_n(P_1 + P_2, Q) = e_n(P_1, Q) + e_n(P_2, Q)$

   $e_n(P, Q_1 + Q_2) = e_n(P, Q_1) + e_n(P, Q_2)$

2. *Alternating:*

   $e_n(P, P) = 1$

3. *Nondegenerate:*

   If $e_n(P,Q) = 1$ *for all* $P \in E[n]$*, then* $Q = \mathscr{O}$*.*

4. *Galois invariant:*

   For $\sigma \in G_F$*,* $\sigma(e_n(P,Q)) = e_n(\sigma(P), \sigma(Q))$*.*

Proof. See Proposition III.8.1 in [40]. □

In addition, e_n sends a basis of $E[n]$ to a primitive n-th root of unity:

Lemma 1. *Let* $\{P,Q\}$ *be a basis of* $E[n]$*. Then* $e_n(P,Q) = \zeta_n$*, a primitive* n*-th root of unity.*

Proof. Suppose $e_n(P,Q) = \zeta \in \mu_n$ of order d. For an arbitrary $S \in E[n]$, $S = aP + bQ$. Then

$$\begin{aligned} e_n(S, dQ) &= e_n(aP + bQ, dQ) \\ &= e_n(aP, dQ)e_n(bQ, dQ) \\ &= e_n(P,Q)^{da} e_n(Q,Q)^{db} \\ &= \zeta^{da} 1^{db} \\ &= 1. \end{aligned}$$

As S is arbitrary and the Weil pairing is nondegenerate, $dQ = \mathscr{O}$. Thus n divides d, and it follows that $n = d$. □

Proof of Proposition 5. Let $\sigma \in G_F$. With respect to a basis $\{P,Q\}$ of $E[n]$,

$$\rho_{E,n}(\sigma) = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

for some $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$. As the Weil pairing is Galois invariant, it follows that:

$$\begin{aligned} \sigma(\zeta_n) &= \sigma(e_n(P,Q)) \\ &= e_n(\sigma(P), \sigma(Q)) \end{aligned}$$

$$
\begin{aligned}
&= e_n(aP + cQ, bP + dQ) \\
&= e_n(aP, bP)e_n(aP, dQ)e_n(cQ, bP)e_n(cQ, dQ) \\
&= e_n(P, P)^{ab}e_n(P, Q)^{ad}e_n(Q, P)^{bc}e_n(Q, Q)^{cd} \\
&= 1 \cdot e_n(P, Q)^{ad}e_n(Q, P)^{bc} \cdot 1 \\
&= e_n(P, Q)^{ad}(e_n(P, Q)^{-1})^{bc} \\
&= e_n(P, Q)^{ad-bc} \\
&= \zeta_n^{ad-bc}.
\end{aligned}
$$

Since $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$, we have our result. □

We close with a connection between mod-n Galois representations and maps between elliptic curves which is relevant for our main result:

Proposition 7. *Let E be an elliptic curve defined over a number field F, and let ℓ be a rational prime. Then E possesses an F-rational ℓ-isogeny if and only if $\rho_{E,\ell}$ is upper triangular with respect to some basis.*

Proof. Suppose E possesses an F-rational ℓ-isogeny, $\varphi : E \to E'$. By definition, the kernel of φ is a group of order ℓ. Let P be a generator of this cyclic group. Since φ is defined over F, it is locally defined by polynomials in $F[x_0, x_1, x_2]$. Then for $\sigma \in G_F$, we have $\varphi(\sigma(P)) = \sigma(\varphi(P)) = \sigma(\mathcal{O}) = \mathcal{O}$. Thus $\sigma(P) \in \ker(\varphi) = \langle P \rangle$, and $\langle P \rangle$ is fixed as a set by $\sigma \in G_F$. It follows that for a basis $\{P, Q\}$ for some $Q \in E[\ell]$, the representation $\rho_{E,\ell}$ is upper triangular.

Conversely, suppose $\rho_{E,\ell}$ is upper triangular with respect to the basis $\{P, Q\}$. Then $\langle P \rangle$ is a cyclic subgroup of order ℓ fixed as a group by G_F. Then E has an F-rational ℓ-isogeny by Proposition III.4.12 and Remark III.4.13.2 in [40]. □

3 Class Field Theory

3.1 Preliminaries

Though this theory exists in much more generality, here we restrict our attention to the case where K is an imaginary quadratic field so we may take a **modulus** $\mathfrak{m}$ to be simply an integral ideal of $\mathcal{O}_K$. Then relative to $\mathfrak{m} = \prod \mathfrak{p}^{m(\mathfrak{p})}$, we define the following two subsets:

$$I_K(\mathfrak{m}) = \text{the set of all fractional ideals of } K \text{ relatively prime to } \mathfrak{m},$$

$$P_K(\mathfrak{m}) = \{(\alpha) : \alpha \in K^\times, \mathrm{ord}_\mathfrak{p}(\alpha - 1) \geq m(\mathfrak{p}) \text{ for all } \mathfrak{p} \text{ dividing } \mathfrak{m}\}.$$

The set $P_K(\mathfrak{m})$ is a subgroup of $I_K(\mathfrak{m})$, and the quotient $I_K(\mathfrak{m})/P_K(\mathfrak{m})$ is called the **$\mathfrak{m}$-ray class group** of K. This generalizes the notion of the ideal class group, and we recover its definition in the case where $\mathfrak{m} = 1$.

For an abelian extension L of K, let $\mathfrak{m}$ be an integral ideal of $\mathcal{O}_K$ divisible by every prime ideal which is ramified in L/K. Then the **Artin map**,

$$\Phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K),$$

is induced by sending each $\mathfrak{p} \in I_K(\mathfrak{m})$ to the Frobenius automorphism $\left(\frac{L/K}{\mathfrak{p}}\right)$. With this definition, we may now recall one of the major results of class field theory:

Theorem 15 (Existence Theorem)**.** *Let $\mathfrak{m}$ be a modulus of K, and let H be a group such that*

$$P_K(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m}).$$

There is a unique abelian extension L/K unramified away from primes dividing $\mathfrak{m}$ such that $\ker(\Phi_{L/K,\mathfrak{m}}) = H$.

Proof. See Theorem 9.16 of Chapter V in [19]. □

In fact, every such abelian extension of K can be obtained in this way. See Theorem 5.7 of Chapter V in [19] for details.

3.2 Ray Class Fields

Let K be an imaginary quadratic field, and let $\mathfrak{m}$ be an integral ideal of K. Then by Theorem 15, we may make the following definition:

Definition 6. The **ray class field** of K with modulus $\mathfrak{m}$ is the unique abelian extension $K_\mathfrak{m}/K$ such that $\ker(\Phi_{K_\mathfrak{m}/K,\mathfrak{m}}) = P_K(\mathfrak{m})$.

Since the Artin map is surjective (Theorem 5.7 in Chapter V of [19]), it follows from the definition that $\mathrm{Gal}(K_\mathfrak{m}/K) \cong I_K(\mathfrak{m})/P_K(\mathfrak{m})$, the $\mathfrak{m}$-ray class group. As with the ideal class group, the $\mathfrak{m}$-ray class group is finite, and we have the following explicit formula for its cardinality.

Proposition 8. *Let $\mathfrak{m}$ be an integral ideal in a number field K. The order of the ray class group modulo $\mathfrak{m}$, and thus the degree of the extension $K_\mathfrak{m}/K$, is given by:*

$$h_\mathfrak{m} = h_K \cdot [U : U_\mathfrak{m}]^{-1} \cdot \mathcal{N}(\mathfrak{m}) \cdot \textstyle\prod_{\mathfrak{p}|\mathfrak{m}} \left(1 - \mathcal{N}(\mathfrak{p})^{-1}\right)$$

where

$$\begin{aligned} h_K &= \textit{class number of } K \\ U &= \mathcal{O}_K^\times \\ U_\mathfrak{m} &= \{\alpha \in U : \mathrm{ord}_\mathfrak{p}(\alpha - 1) \geq m(\mathfrak{p}) \textit{ for all } \mathfrak{p} \textit{ dividing } \mathfrak{m}\}. \end{aligned}$$

Proof. See Corollary 3.2.4 in [7]. Note we have restricted to the case where our modulus is an integral ideal. □

In the special case $\mathfrak{m} = \ell\mathcal{O}_K$, we obtain:

Corollary 3. *Let ℓ be a prime and $\mathfrak{m}$ be the modulus $\ell\mathcal{O}_K$ in a quadratic field K. Then:*

1. *If ℓ is ramified in K, $h_\mathfrak{m} = h_K \cdot [U : U_\mathfrak{m}]^{-1} \cdot \ell \cdot (\ell - 1)$.*
2. *If ℓ splits in K, $h_\mathfrak{m} = h_K \cdot [U : U_\mathfrak{m}]^{-1} \cdot (\ell - 1) \cdot (\ell - 1)$.*
3. *If ℓ is inert in K, $h_\mathfrak{m} = h_K \cdot [U : U_\mathfrak{m}]^{-1} \cdot (\ell + 1) \cdot (\ell - 1)$.*

Proof. We prove each case separately:

· Suppose ℓ is ramified in K. Then $\ell\mathcal{O}_K = \mathfrak{p}^2$, and since $\mathcal{N}(\mathfrak{p}) = \ell$,

$$\mathcal{N}(\mathfrak{p}^2) \cdot (1 - \mathcal{N}(\mathfrak{p})^{-1}) = \ell^2 \left(1 - \tfrac{1}{\ell}\right) = \ell(\ell - 1).$$

· Suppose ℓ splits in K. Then $\ell\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, and since $\mathcal{N}(\mathfrak{p}_i) = \ell$ for $i = 1, 2$,

$$\mathcal{N}(\mathfrak{p}_1\mathfrak{p}_2) \cdot (1 - \mathcal{N}(\mathfrak{p}_1)^{-1}) \cdot (1 - \mathcal{N}(\mathfrak{p}_2)^{-1}) = \ell^2 \left(1 - \tfrac{1}{\ell}\right)\left(1 - \tfrac{1}{\ell}\right) = (\ell - 1)^2.$$

· Suppose ℓ is inert in K. Then $\ell\mathcal{O}_K = \mathfrak{p}$, and since $\mathcal{N}(\mathfrak{p}) = \ell^2$,

$$\mathcal{N}(\mathfrak{p}) \cdot (1 - \mathcal{N}(\mathfrak{p})^{-1}) = \ell^2 \left(1 - \tfrac{1}{\ell^2}\right) = \ell^2 - 1. \qquad \square$$

Finally, we have the following additional definition which helps characterizes subfields of ray class fields:

Definition 7. The **conductor** of an abelian extension L/K, denoted $\mathfrak{f}(L/K)$, is the greatest common divisor of all moduli $\mathfrak{m}$ such that $L \subset K_\mathfrak{m}$.

Given the restricted ramification found in ray class fields, it is not surprising that the conductor is related to the behavior of primes in L/K. More precisely, we have:

Proposition 9. *Suppose L is an abelian extension of K of conductor $\mathfrak{f}(L/K)$. A prime of ideal of K ramifies in L if and only if it divides $\mathfrak{f}(L/K)$.*

Proof. See Theorem 12.7 in Chapter V, §6 of [19]. $\square$

3.3 Ring Class Fields

For an imaginary quadratic field K and a positive integer f, let H_f be the subgroup of $I_K(f\mathcal{O}_K)$ generated by the set

$$\{(\alpha) : \alpha \in \mathcal{O}_K, \alpha \equiv a \bmod f\mathcal{O}_K \text{ where } a \in \mathbb{Z}, (a, f) = 1\}.$$

Then $P_K(f\mathcal{O}_K) \subset H_f \subset I_K(f\mathcal{O}_K)$, and we may define the following by Theorem 15:

Definition 8. The **ring class field** of K with conductor f is the unique abelian extension K_f/K such that $\ker(\Phi_{K_f/K, f\mathcal{O}_K}) = H_f$.

The group $\mathrm{Gal}(K_f/F)$ is isomorphic to the ideal class group of the order $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ (see Proposition 7.22 in [8]). Thus we have an explicit formula for the cardinality of $[K_f : K]$:

Proposition 10.

$$[K_f : K] = h(\mathcal{O}_f) = \frac{h(\mathcal{O}_K)f}{[\mathcal{O}_K^\times : \mathcal{O}_f^\times]} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right).$$

Proof. See Theorem 7.24 in [8]. □

4 Elliptic Curves with Complex Multiplication

4.1 Preliminaries

We may obtain explicit constructions of ray class fields and ring class fields using a certain class of elliptic curves; namely, those possessing complex multiplication. These are the elliptic curves with "more endomorphisms than expected," a notion we will now make more precise.

Definition 9. Let E be an elliptic curve defined over a number field F. The **endomorphism ring** of E, denoted $\mathrm{End}(E)$, is the set of isogenies from E to E that are defined over $\bar{F}$. This can be given the structure of a ring with the following definitions:

$$(\varphi + \psi)(P) = \varphi(P) + \psi(P),$$

$$(\varphi\psi)(P) = \varphi(\psi(P)),$$

for $\varphi, \psi \in \mathrm{End}(E)$ and $P \in E$.

For most elliptic curves, the only endomorphisms are the multiplication-by-n maps of Example 1. In other words, for these curves $\mathbb{Z} \cong \mathrm{End}(E)$ under the map $n \mapsto [n]$. If there are not any additional endomorphisms, the elliptic curve is said to have complex multiplication:

Definition 10. Let E be an elliptic curve defined over a number field F. We say E has **complex multiplication**, or **CM**, if $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$. In this case, $\mathrm{End}(E)$ is isomorphic to an order in an imaginary quadratic field K called the **CM field** of E. (See VI.5.5 of [40].)

Example 4: The elliptic curve E defined by $y^2 = x^3 + 1$ has CM by the maximal order in $\mathbb{Q}(\sqrt{-3})$. For example, the map

$$(x, y) \mapsto \left(\frac{-1+\sqrt{-3}}{2}x, y\right)$$

defines an isogeny from E to E that is not a multiplication-by-n map.

Although an elliptic curve may have CM by an arbitrary order, often we may restrict to the case where E has CM by the maximal order in an imaginary quadratic field K, the full ring of integers $\mathscr{O}_K$. Specifically, we have the following result:

Proposition 11. *Let E be an elliptic curve defined over a number field F with CM by the order $\mathcal{O}_f$ in an imaginary quadratic field K. There exists an F-rational isogeny $\varphi : E \to E'$ where E' is defined over F and has CM by $\mathscr{O}_K$. Moreover, φ is cyclic of degree f.*

Proof. See Proposition 25 in [6]. □

4.2 CM Elliptic Curves and Class Field Theory

If E has CM by the maximal order in K, then the ray class field of K with modulus $N\mathcal{O}_K$ can be generated from the N-torsion points of E. This construction involves the use of the Weber function, which we will now define. To streamline notation, we will assume E has an equation of the form

$$y^2 = 4x^3 - g_2x - g_3.$$

We do not lose anything by making this assumption as an elliptic curve defined over a number field F will be isomorphic over F to a curve having an equation of this form.

Definition 11. Let E be an elliptic curve defined by $y^2 = 4x^3 - g_2x - g_3$. The **Weber function** $\mathfrak{h}$ on E is

$$\mathfrak{h}(x,y) = \begin{cases} \frac{g_2g_3}{\Delta}x \text{ if } j_E \neq 0, 1728, \\ \frac{g_2^2}{\Delta}x^2 \text{ if } j_E = 1728, \\ \frac{g_3}{\Delta}x^3 \text{ if } j_E = 0, \end{cases}$$

where j_E is the j-invariant of E and $\Delta = g_2^3 - 27g_3^2$.

We then obtain an explicit description of the ray class field from the following theorem, the roots of which can be traced back to the work of Hasse in [13]:

Theorem 2. *Let E be an elliptic curve defined over $K(j_E)$ with $\mathrm{End}(E) \cong \mathcal{O}_K$ for some imaginary quadratic field K. Let $\mathfrak{h}$ be the Weber function on E. Then $K(j_E, \mathfrak{h}(E[N]))$ is the ray class field of K with modulus $N\mathcal{O}_K$.*

Proof. See, for example, Theorem 2 in [20, p.126]. □

Note that the Weber function is model independent. That is, if $\varphi\colon E \to E'$ is an $\bar{F}$-isomorphism and $\mathfrak{h}_E$, $\mathfrak{h}_{E'}$ the Weber functions of E and E', respectively, we have $\mathfrak{h}_E = \mathfrak{h}_{E'} \circ \varphi$. (See [37, p.107].) This allows us to extend the result of Theorem 2 to include elliptic curves defined over an arbitrary number field F.

Corollary 4. *Let E be an elliptic curve defined over a number field F with $\mathrm{End}(E) \cong \mathcal{O}_K$ for some imaginary quadratic field K. Then $K(j_E, \mathfrak{h}(E[N]))$ is the ray class field of K with modulus $N\mathcal{O}_K$.*

Proof. Let E be an elliptic curve defined over a number field F with $\mathrm{End}(E) \cong \mathcal{O}_K$. E is isomorphic over $\mathbb{C}$ to an elliptic curve E' defined over $K(j_E)$ by Proposition 3. If we let φ denote the isomorphism from E to E', the model independence of the Weber function gives $\mathfrak{h}_E(E[N]) = \mathfrak{h}_{E'}(\varphi(E[N])) = \mathfrak{h}_{E'}(E'[N])$. By Theorem 2, $K(j_{E'}, \mathfrak{h}_{E'}(E'[N])) = K(j_E, \mathfrak{h}_E(E[N]))$ is the ray class field of K modulo $N\mathcal{O}_K$, as desired. □

While building ray class fields takes a bit of work—in particular, one must obtain the coordinates of certain torsion points of the elliptic curve—the method for constructing ring class fields is almost immediate. We need only compute the j-invariant of our CM elliptic curve:

Theorem 16. *Let E be an elliptic curve defined over a number field F with $\mathrm{End}(E) \cong \mathcal{O}_f$ in an imaginary quadratic field K. Then $K(j_E)$ is the ring class field of K with conductor f.*

Proof. See Theorem 11.1 in [8]. □

In fact we can so construct all ring class fields of an imaginary quadratic field K. See Chapter 3 in [8] for details.

4.3 Torsion Point Fields of CM Elliptic Curves

Let ℓ be a rational prime. Recall that for an arbitrary elliptic curve, the mod-ℓ Galois representation is an injective homomorphism $\mathrm{Gal}(F(E[\ell])/F) \hookrightarrow \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$. As a consequence, $[F(E[\ell]) : F]$ must divide $\#\mathrm{GL}_2(\mathbb{F}_\ell)$. However, if E has CM by the ring of integers in an imaginary quadratic field K, the representation $\rho_{E,\ell}$ gives an injection from $\mathrm{Gal}(F(E[\ell])/FK)$ to the group of $\mathcal{O}_K/\ell\mathcal{O}_K$-module automorphisms of $E[\ell]$. Since $\mathrm{Aut}_{\mathcal{O}_K/\ell\mathcal{O}_K}(E[\ell]) \cong (\mathcal{O}_K/\ell\mathcal{O}_K)^\times$, this provides us with more refined divisibility conditions:

Proposition 12. *Let E be an elliptic curve with CM by $\mathcal{O}_K$ in K. Then for an odd prime ℓ:*

1. *If $\left(\frac{d_K}{\ell}\right) = 1$, then $[F(E[\ell]) : F] \mid 2(\ell-1)^2$.*
2. *If $\left(\frac{d_K}{\ell}\right) = -1$, then $[F(E[\ell]) : F] \mid 2(\ell^2-1)$.*
3. *If $\left(\frac{d_K}{\ell}\right) = 0$, then $[F(E[\ell]) : F] \mid 2(\ell^2-\ell)$.*

Proof. See, for example, Corollary 17 of [6] or the proof of Theorem 2.3 in [39]. □

In addition, we have the following relationship between the CM field of E its torsion point fields:

Lemma 2. *For a number field F, let E/F be an elliptic curve with CM by the maximal order in an imaginary quadratic field K. Suppose ℓ is an odd prime. Then $K \subset F(E[\ell])$, and $F(E[\ell])/FK$ is an abelian extension.*

Proof. See discussion on p. 12 and Lemma 15 in [6].[1] □

[1] Note the ramification requirement that appears in the assumptions of Lemma 15 is not used in the proof.

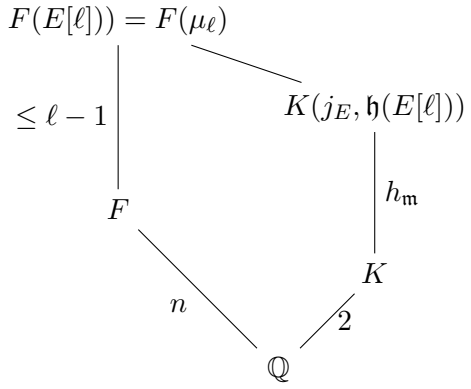
5 Proof of Main Result

From the divisibility conditions of Proposition 12, we see that it is only possible for an odd prime ℓ to divide the degree of $F(E[\ell])/F$ when ℓ divides d_K. This is a fact we are able to exploit:

Lemma 3. *Suppose E is an elliptic curve defined over a number field F with complex multiplication by $\mathcal{O}_K$ in K. Suppose ℓ is prime and $\ell > \frac{w_K}{2}n+1$, where n is the degree of $F/\mathbb{Q}$. If $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ, then ℓ must divide d_K.*

Proof. Let $[F(E[\ell]) : F(\mu_\ell)]$ be a power of ℓ, and suppose ℓ is an odd prime which does not divide d_K. Since $\ell \neq 2$, Proposition 12 forces $F(E[\ell]) = F(\mu_\ell)$. We will show this is a contradiction unless $\ell \leq \frac{w_K}{2}n + 1$.

By Lemma 2, $K \subset F(E[\ell])$. Thus $F(E[\ell])$ also contains $K(j_E, \mathfrak{h}(E[\ell]))$, the ray class field of K modulo $\mathfrak{m} = \ell\mathcal{O}_K$ by Corollary 4. This gives us the following diagram of fields:



From Corollary 3, if ℓ splits in K then

$$\begin{aligned} h_{\mathfrak{m}} &= h_K \cdot [U : U_{\mathfrak{m}}]^{-1} \cdot (\ell - 1) \cdot (\ell - 1) \\ &\geq 1 \cdot \frac{1}{w_K} \cdot (\ell - 1) \cdot (\ell - 1). \end{aligned}$$

Similarly, if ℓ is inert in K,

$$h_{\mathfrak{m}} \geq 1 \cdot \frac{1}{w_K} \cdot (\ell + 1) \cdot (\ell - 1).$$

In either case, $h_{\mathfrak{m}} \geq \dfrac{1}{w_K} \cdot (\ell - 1)^2$. But

$$2 \cdot \frac{1}{w_K} \cdot (\ell - 1)^2 > n \cdot (\ell - 1)$$

whenever $\ell > \dfrac{w_K}{2} n + 1$. In other words, $F(E[\ell]) \neq F(\mu_\ell)$ for $\ell > \dfrac{w_K}{2} n + 1$. □

In fact, the same result holds for elliptic curves with CM by an arbitrary order. We begin with a necessary lemma.

Lemma 4. *Let E, E' be elliptic curves defined over a number field F. If there exists an F-rational n-isogeny $\varphi : E \to E'$, then $F(E[m]) = F(E'[m])$ for any m with $(m, n) = 1$.*

Proof. Since φ is a group homomorphism, it restricts to a homomorphism $\tilde{\varphi} : E[m] \to E'[m]$. The kernel of $\tilde{\varphi}$ is a subgroup of the kernel of φ, so $\#\ker(\tilde{\varphi}) \mid n$. However, $\ker(\tilde{\varphi})$ is also a subgroup of $E[m]$, a group of order m^2. Since $(m, n) = 1$, it follows $\ker(\tilde{\varphi}) = 1$ and $\tilde{\varphi}$ defines an injection, $E[m] \hookrightarrow E'[m]$. As these both have size m^2 by Theorem 13, it is in fact an isomorphism. Then the fact that φ is defined over F gives

$$F(E'[m]) = F(\varphi(E[m])) \subset F(E[m]).$$

To get the reverse containment, we consider $\hat{\varphi} : E' \to E$, the dual isogeny to φ. (See III.6 in [40] for the definition and properties of $\hat{\varphi}$.) Since $\deg(\hat{\varphi}) = \deg(\varphi)$, we may replace φ with $\hat{\varphi}$ in the argument above to find $\hat{\varphi}$ induces an isomorphism from $E'[m]$

to $E[m]$. Since φ, E, and E' are defined over F, by Theorem 7.8.1 in [10] $\hat{\varphi}$ is defined over F, and

$$F(E[m]) = F(\hat{\varphi}(E'[m])) \subset F(E'[m]). \qquad \square$$

Proposition 13. *Suppose E is an elliptic curve defined over a number field F with complex multiplication by an order in K. Suppose ℓ is prime and $\ell > \frac{w_K}{2}n + 1$, where n is the degree of $F/\mathbb{Q}$. If $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ, then ℓ must divide d_K.*

Proof. Suppose E has CM by the order $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ in K. Then by Proposition 11 there exists an F-rational isogeny $\varphi\colon E \to E'$ where E' is defined over F and has CM by $\mathcal{O}_K$. Since φ is of degree f, we need only to show that f and ℓ are relatively prime. Then $F(E[\ell]) = F(E'[\ell])$ by the previous lemma, and the result will follow from Lemma 3.

Let $f = p_1^{a_1} \cdots p_r^{a_r}$ be the prime factorization of f, with $p_1 < p_2 < \ldots < p_r$. By Proposition 10, the class number of $\mathcal{O}_f$ satisfies:

$$h(\mathcal{O}_f) = \frac{h(\mathcal{O}_K)p_1^{a_1-1} \cdots p_r^{a_r-1}}{[\mathcal{O}_K^\times : \mathcal{O}_f^\times]} \prod_{i=1}^{r} \left(p_i - \left(\frac{d_K}{p_i}\right)\right).$$

Since $|\mathcal{O}_K^\times| = w_K$ and $|\mathcal{O}_f^\times| \geq 2$,

$$\begin{aligned} h(\mathcal{O}_f) &\geq \frac{h(\mathcal{O}_K)p_1^{a_1-1} \cdots p_r^{a_r-1}}{w_K/2} \prod_{i=1}^{r} \left(p_i - \left(\frac{d_K}{p_i}\right)\right) \\ &\geq \frac{2}{w_K}\left(p_r - \left(\frac{d_K}{p_r}\right)\right) \\ &\geq \frac{2}{w_K}\left(p_r - 1\right). \end{aligned}$$

We may obtain an upper bound on $h(\mathcal{O}_f)$ by recalling that $K(j_E)$ is the ring class field of K of the order $\mathcal{O}_f$ (Theorem 16). Thus $[K(j_E) : K] = h(\mathcal{O}_f)$. Since $j_E \in F$, a number field of degree n, we also have $[K(j_E) : K] \leq n$. It follows that $h(\mathcal{O}_f) \leq n$. Combining this with the inequality above, we find $p_r \leq \frac{w_K}{2}n + 1$. Since $\ell > \frac{w_K}{2}n + 1$, this is enough to conclude ℓ and f are relatively prime, as desired. $\square$

If n is odd we can extend the result to all odd primes:

Corollary 5. *Suppose E is an elliptic curve defined over a number field F with complex multiplication by an order in K. Suppose the degree of $F/\mathbb{Q}$ is odd, and let ℓ be an odd prime number. If $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ, then ℓ must divide d_K.*

Proof. Suppose $\ell \nmid d_K$, and assume for the sake of contradiction that $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ. By Lemma 2, $K = \mathbb{Q}(\sqrt{D}) \subset F(E[\ell])$. In fact, $K \subseteq F(\mu_\ell)$, for otherwise $F(\mu_\ell)(\sqrt{D})$ would be a proper extension of $F(\mu_\ell)$ contained in $F(E[\ell])$ and 2 would divide $[F(E[\ell]) : F(\mu_\ell)]$. However, since $\ell \nmid d_K$, we know $K \nsubseteq \mathbb{Q}(\mu_\ell)$. Thus $\mathbb{Q}(\mu_\ell)(\sqrt{D})$ is a proper extension of $\mathbb{Q}(\mu_\ell)$ contained in $F(\mu_\ell)$. Since $[F(\mu_\ell) : \mathbb{Q}(\mu_\ell)] = [F : \mathbb{Q}(\mu_\ell) \cap F]$, this forces $2 \mid [F : \mathbb{Q}(\mu_\ell) \cap F]$, which is a contradiction. □

We are now ready to prove our main result:

Theorem 12. *Let F be a number field with $[F : \mathbb{Q}] = n$. There exists a constant $C = C(n)$ depending only on n with the following property: If there exists a CM elliptic curve E/F with $F(E[\ell^\infty])$ a pro-ℓ extension of $F(\mu_\ell)$ for some rational prime ℓ, then $\ell \leq C$.*

Proof. Suppose there exists a CM-elliptic curve E/F with $F(E[\ell^\infty])$ a pro-ℓ extension of $F(\mu_\ell)$. Thus $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ. Since $w_K \leq 6$ for an imaginary quadratic field K, the previous proposition shows $\ell \leq 3n + 1$ or $\ell \mid d_K$ where K is the CM-field of E. However, since $h(\mathcal{O}_K)$ divides $h(\mathcal{O}_f) = [K(j_E) : K] \leq n$, it follows that K has class number less than or equal to n. As there are only a finite number of such K, proved by Heilbronn in [15], the result follows. □

It is clear that obtaining an explicit bound depends only on knowing the imaginary quadratic fields with a given class number, i.e., it depends on having a solution to the Gauss class number problem for imaginary quadratic fields. For class numbers up through 7 and odd class numbers up to 23, complete lists of the corresponding fields exist (see [4] for a history of the many mathematicians involved in the early work on

this problem and for a list of imaginary quadratic fields with odd class number up to 23; see [41], [3], [43] for lists of imaginary quadratic fields of class number 2, 4, and 6, respectively). More recent work by Watkins in [44] gives a solution for class numbers up to 100. To illustrate how these results may be used, we have compiled a table of bounds for elliptic curves defined over a number field F of degree n where $n \leq 7$:

n	$C(n)$
1, 2	163
3, 4	907
5, 6	2683
7	5923

We justify the claimed bounds. Suppose there exists a CM-elliptic curve E/F with $F(E[\ell^\infty])$ a pro-ℓ extension of $F(\mu_\ell)$. Then $[F(E[\ell]) : F(\mu_\ell)]$ is ℓ-powered, and by Proposition 13, we know $\ell \leq \frac{w_K}{2}n + 1 \leq 3n + 1$ or ℓ divides d_K where K is the CM field of E. As mentioned in the proof of Theorem 12, the class number of K is less than or equal to n, so we need only consult the lists of the discriminants of imaginary quadratic fields satisfying this constraint. A check of the possible primes dividing those discriminants yields the bounds above. Since Rasmussen and Tamagawa in [33] find an example of a CM-elliptic curve defined over $\mathbb{Q}$ with $\mathbb{Q}(E[163^\infty])$ a pro-163 extension of $\mathbb{Q}(\mu_{163})$, we see that in fact 163 is the best possible bound for $n = 1$ and $n = 2$.

We may also achieve a rough bound when F has degree up to 100. In Table 4 from [44], Watkins records the largest fundamental discriminant (in absolute value) for each class number up to 100. This is sufficient to generate additional bounds. For example, we know the largest fundamental discriminant in Watkins's table, 2383747, occurs when K has class number 98. Hence the largest possible prime dividing any discriminant is 2383739, so $C(n) \leq 2383739$ for all $n \leq 100$.

6 Additional Applications

6.1 Rationality

Determining when $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ will in fact establish when there exists a non-trivial ℓ-torsion point with coordinates in $F(\mu_\ell)$:

Lemma 5. *Suppose E is an elliptic curve defined over a number field F. Then E has a non-trivial ℓ-torsion point rational over $F(\mu_\ell)$ if and only if $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ.*

Proof. Suppose $P \in E[\ell]$ is rational over $F(\mu_\ell)$. Then we can choose a basis $\{P, Q\}$ of $E[\ell]$ for which the mod-ℓ Galois representation yields

$$\mathrm{Gal}(F(E[\ell])/F(\mu_\ell)) \subseteq \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{F}_\ell \right\}.$$

Indeed, the determinant of this matrix will equal the cyclotomic character by Proposition 5, which is trivial in this extension. It follows that $\mathrm{Gal}(F(E[\ell])/F(\mu_\ell))$ has size 1 or ℓ. The other direction is a result of the Orbit-Stabilizer Theorem, but we can also see it as an immediate consequence of Lemma 6 below. □

Thus Proposition 13 implies that for CM elliptic curves, points with prime order ℓ that is large relative to the degree of F will only have coordinates in $F(\mu_\ell)$ if ℓ divides the discriminant of the CM field K. Our main result may be reformulated as follows:

Theorem 12'. *Let F be a number field with $[F : \mathbb{Q}] = n$. There exists a constant*

$C = C(n)$ depending only on n with the following property: If there exists a CM elliptic curve E/F with a nontrivial ℓ-torsion point defined over $F(\mu_\ell)$ for some rational prime ℓ, then $\ell \leq C$.

To put this result in context, we briefly record the known rationality results to which Theorem 12' may be compared. We start with Merel's uniform boundedness theorem, which gives one of the most celebrated results on rationality of torsion points of elliptic curves (not necessarily with CM). In particular, his work implies the following theorem:

Theorem 17 (Merel, [22])**.** *Suppose F is a number field and L is an extension of F, where $[L : \mathbb{Q}] = n$. If there exists an elliptic curve E/F with a non-trivial ℓ-torsion point defined over L for some rational prime ℓ, then $\ell \leq P(n)$, a constant which depends only on n.*

Note that by restricting to CM elliptic curves and to a specific extension of F, namely $L = F(\mu_\ell)$, we are able to find a bound depending only on the degree of F. Furthermore, current explicit and theoretical bounds for $P(n)$ are too big to rule out the possibility of an ℓ-torsion point rational over $F(\mu_\ell)$.

Other work considers the rationality question specifically for CM elliptic curves. For example, we have the following result of Silverberg, which is a corollary to a more general result on abelian varieties. Here, φ denotes Euler's totient function.

Theorem 18 (Silverberg, [38])**.** *Suppose E is an elliptic curve defined over a number field F of degree n, E has CM by an order $\mathcal{O}$ in an imaginary quadratic field K, and P is an N-torsion point defined over F. Let μ denote the number of roots of unity in $\mathcal{O}$. Then:*

1. *$\varphi(N) \leq \mu n \leq 6n$.*
2. *If $K \subseteq F$ then $\varphi(N) \leq \mu n/2 \leq 3n$.*
3. *$N \ll n \log\log n$.*

Since the degree of $F(\mu_\ell)$ is at least $\ell - 1$, these inequalities do not provide information concerning nontrivial rational ℓ-torsion points. A recent paper by Clark, Cook, and Stankewicz ([6]) refines both the bounds of Silverberg cited above and the related bounds given by Prasad and Yoganada in [29]. In addition, they give conditions that arise from the examination of the modular curve $X_1(\ell)$. Though the results are much more general in nature, they do not imply the present result over the specific field $F(\mu_\ell)$.

6.2 Mod-ℓ Galois Representation

If $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ, this partially determines the form of the Galois representation attached to E. Recall $\rho_{E,\ell} : G_F \to GL_2(\mathbb{F}_\ell)$ is the mod-ℓ Galois representation, and χ denotes the cyclotomic character mod ℓ. Then for $\delta = [\mathbb{F}_\ell^\times : \chi(G_F)]$, we have the following result of Rasmussen and Tamagawa:

Lemma 6 (Rasmussen, Tamagawa, [33])**.** *Suppose E is an elliptic curve defined over a number field F where $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ. Then there exists a basis of $E[\ell]$ with respect to which*

$$\rho_{E,\ell}(G_F) = \begin{bmatrix} \chi^{i_1} & * \\ 0 & \chi^{i_2} \end{bmatrix}.$$

Furthermore, i_1, i_2 may be chosen to be nonnegative integers less than $\frac{\ell-1}{\delta}$.

Proof. A version of this appears as Lemma 3 in [33], and a more general version appears in [32]. Note that although the result in [32] is stated for abelian varieties A/F where $F(A[\ell^\infty])$ is both a pro-ℓ extension of $F(\mu_\ell)$ and unramified away from ℓ, the ramification requirement is not used in the proof. □

In this context, Proposition 13 is perhaps more useful than our main result. If our goal is to identify elliptic curves with the "nice" Galois representation depicted above, we now know that for CM elliptic curves, primes large relative to the degree of F must divide the discriminant of our CM field K.

7 Closing Remarks

Although finding the conditions necessary for $[F(E[\ell]) : F(\mu_\ell)]$ to be a power of ℓ was enough to prove the uniform bound in Theorem 12, it is desirable to discover sufficient conditions as well, particularly given the applications to rationality and the Galois representation attached to E. Unfortunately, the converse of Proposition 13 does not hold. As a counterexample, consider the elliptic curve defined by the equation

$$y^2 = x^3 - 595x + 5586$$

at the prime $\ell = 7$. This curve has CM by an order in $K = \mathbb{Q}(\sqrt{-7})$, so ℓ divides d_K and $\ell > 3 \cdot 1 + 1$. By Lemma 4 in [11], $\sqrt{7}$ is contained in $\mathbb{Q}(E[\ell])$. Since $\sqrt{7}$ is not contained in $\mathbb{Q}(\mu_\ell)$, we find that $\mathbb{Q}(\mu_\ell)(\sqrt{7})$ gives a degree 2 extension of $\mathbb{Q}(\mu_\ell)$ inside of $\mathbb{Q}(E[\ell])$. In other words, 2 divides $[F(E[\ell]) : F(\mu_\ell)]$ and so the desired extension is not a power of ℓ.

For at least some number fields, however, adding the assumption that the elliptic curve has good reduction away from ℓ gives us the desired condition. For example, we have the following additional result for elliptic curves over $\mathbb{Q}$:

Proposition 14. *Suppose E is an elliptic curve over $\mathbb{Q}$ with CM by an order in an imaginary quadratic field K. Let $\ell > 3$ be a prime number. If $\ell \mid d_K$ and E has good reduction away from ℓ, then $[\mathbb{Q}(E[\ell]) : \mathbb{Q}(\mu_\ell)]$ is a power of ℓ.*

Proof. Suppose E has CM by the order $\mathcal{O}_f = \mathbb{Z} + f\mathcal{O}_K$ in K. Then by Proposition 11 there exists a $\mathbb{Q}$-rational f-isogeny $\varphi\colon E \to E'$ where E' is defined over $\mathbb{Q}$ and

has CM by $\mathcal{O}_K$. If $(f, \ell) = 1$, Lemma 4 shows $\mathbb{Q}(E[\ell]) = \mathbb{Q}(E'[\ell])$. However, this is immediate as $\ell > 3$ and $f \leq 3$. Indeed, since $j_E \in \mathbb{Q}$, it follows from Theorem 16 that $[K(j_E) : K] = h(\mathcal{O}_f) = 1$; the only orders with class number 1 have conductor 1, 2, or 3.

From now on we will assume E has CM by $\mathcal{O}_K$. By Lemma 2 and Theorem 14, $\mathbb{Q}(E[\ell])$ is an abelian extension of K that is unramified away from ℓ. Thus the conductor of $\mathbb{Q}(E[\ell])/K$ is of the form $\mathfrak{p}^r$, where $\mathfrak{p}$ is the prime of K above ℓ, and $\mathbb{Q}(E[\ell])$ is contained in the ray class field of K with modulus $\mathfrak{p}^r$. (See Proposition 9.) The result will be a consequence of the formula for the order of a ray class group given in Proposition 8.

Since $h(\mathcal{O}_f) = 1$, the class number of K is 1. By assumption $\ell \mid d_K$ and $\ell \neq 2, 3$, so K is of the form $\mathbb{Q}(\sqrt{-\ell})$ where $\ell \in \{7, 11, 19, 43, 67, 163\}$. Furthermore, since $\ell \equiv 3 \pmod 4$, $K \subset \mathbb{Q}(\mu_\ell)$. Thus we have the following containment of fields, where $K_{\mathfrak{p}^r}$ is the ray class field of K with modulus $\mathfrak{p}^r$:

$$\begin{array}{c} K_{\mathfrak{p}^r} \\ | \\ \mathbb{Q}(E[\ell]) \\ | \\ \mathbb{Q}(\mu_\ell) \\ {\scriptstyle \frac{\ell-1}{2}} \; | \\ K \end{array}$$

Using the formula for the order of a ray class group of modulus $\mathfrak{p}^r$ given in Proposition 8, we find an expression for $[K_{\mathfrak{p}^r} : K]$. Note $\mathcal{O}_K^\times = \{1, -1\}$.

$$\begin{aligned} h_{\mathfrak{p}^r} &= h_K \cdot [U : U_{\mathfrak{p}^r}]^{-1} \cdot \mathcal{N}(\mathfrak{p}^r) \cdot \left(1 - \mathcal{N}(\mathfrak{p})^{-1}\right) \\ &= 1 \cdot \frac{1}{2} \cdot \mathcal{N}(\mathfrak{p})^r \cdot \left(1 - \mathcal{N}(\mathfrak{p})^{-1}\right) \\ &= \frac{1}{2} \cdot \ell^r \cdot \left(1 - \frac{1}{\ell}\right) \end{aligned}$$

$$= \frac{1}{2} \cdot \ell^{r-1} \cdot (\ell - 1).$$

Let $\alpha = [\mathbb{Q}(E[\ell]) : \mathbb{Q}(\mu_\ell)]$. By the containment of fields above we see

$$\frac{\ell - 1}{2} \cdot \alpha \mid \frac{1}{2} \cdot \ell^{r-1} \cdot (\ell - 1).$$

This implies $\alpha \mid \ell^{r-1}$, as desired. □

Generalizing this approach has proved to be problematic. For an elliptic curve defined over an arbitrary number field F, one must consider a ray class field of $K(j_E)$, which in general will not be equal to K. The fact that we may have an infinite number of units in the ring of integers of $K(j_E)$ makes it much more difficult to gain anything useful from the formula of Proposition 8.

In fact, there is some evidence that for CM elliptic curves defined over a number field $F \neq \mathbb{Q}$, it may be more difficult to come by examples for which $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ. At least for elliptic curves defined over the field $F = \mathbb{Q}(j_E)$,[1] stronger conditions must be met, as we see in the following additional result:

Proposition 15. *Suppose E is an elliptic curve defined over $F = \mathbb{Q}(j_E)$ with CM by the maximal order in an imaginary quadratic field K. If $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ for some odd prime ℓ, then:*

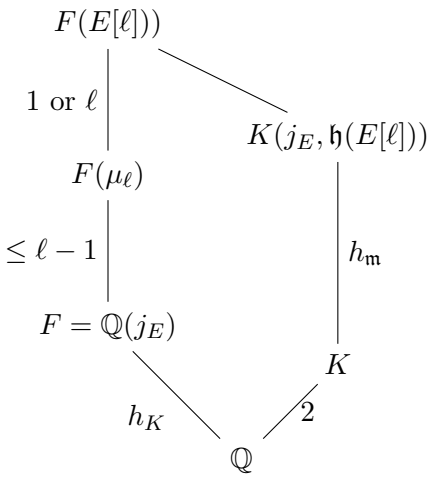
1. *$F(E[\ell])/K$ is a Galois extension.*
2. *Each elliptic curve with CM by $\mathcal{O}_K$ is isomorphic over $\bar{F}$ to an elliptic curve E' with $F(E'[\ell]) = F(E[\ell])$.*

If $F = \mathbb{Q}$, these conditions are met trivially.

Proof. Let E be as in the proposition statement, and suppose $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ. Then $F(E[\ell]) = K_{\ell\mathcal{O}_K}$, the ray class field of K with modulus $\ell\mathcal{O}_K$, as we

[1] Recall $\mathbb{Q}(j_E)$ may be thought of as a type of minimal field of definition by Proposition 3.

now show. Note $K_{\ell\mathcal{O}_K} \subset F(E[\ell])$ by Lemma 2 and Corollary 4. Since $[\mathbb{Q}(j_E) : \mathbb{Q}] = h_K$ (see, for example, Theorem 4.3 in [39]), we have the following diagram of fields:



As $\ell \neq 2$, the formula of Corollary 3 gives

$$h_{\mathfrak{m}} = h_K \cdot \frac{1}{2} \cdot (\ell - 1) \cdot \gamma,$$

where γ is ℓ, $\ell-1$, or $\ell+1$, depending on the behavior of ℓ in K. If $[F(E[\ell]) : F(\mu_\ell)] = 1$, then the inclusion of fields would force $[F(\mu_\ell) : F] > \ell - 1$. Thus $[F(E[\ell]) : F(\mu_\ell)] = \ell$. But then γ must equal ℓ, and by the inclusion of fields

$$2 \cdot h_K \cdot \frac{1}{2} \cdot (\ell - 1) \cdot \ell \;\Big|\; h_K \cdot [F(\mu_\ell) : F] \cdot \ell.$$

From this we may conclude $[F(\mu_\ell) : F] = \ell-1$ and $F(E[\ell]) = K_{\ell\mathcal{O}_K}$. It is now immediate that $F(E[\ell])$ is a Galois extension of K.

Let E_1 be an elliptic curve with CM by $\mathcal{O}_K$. By Theorem 4.3 in [39], the j-invariants of elliptic curves with $\mathcal{O}_K$-CM are Galois conjugate, so there exists $\sigma \in \mathrm{Gal}(K(j_E)/K)$ such that $\sigma(j_E) = j_{E_1}$. Furthermore, if we consider the curve E^σ obtained by allowing σ to act on the coefficients of the defining equation for E, we find $j_{E^\sigma} = j_{E_1}$. By Proposition 3, we will be done if we can establish $F(E[\ell]) = F(E^\sigma[\ell])$ when $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ.

Suppose $[F(E[\ell]) : F(\mu_\ell)]$ is a power of ℓ. Then by part 1, $F(E[\ell])$ is a Galois extension of K. Let $\tilde{\sigma} \in \mathrm{Gal}(F(E[\ell])/K)$ such that $\tilde{\sigma}|_{K(j_E)} = \sigma$, and let $F' = \mathbb{Q}(j_{E^\sigma})$. By the definition of the group law of an elliptic curve,

$$\tilde{\sigma}(F(E[\ell])) = F'(E^\sigma[\ell]).$$

But $\tilde{\sigma}(F(E[\ell])) = F(E[\ell])$ since $F(E[\ell])/K$ is Galois, and we have our claim. $\square$

Note

Sections of this dissertation have appeared previously in the paper *A Uniform Version of a Finiteness Conjecture for CM Elliptic Curves* of the same author available at `http://arxiv.org/abs/1305.5241`.

Bibliography

[1] Clemens Adelmann, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics, vol. 1761, Springer-Verlag, Berlin, 2001. MR 1836119 (2002g:11151)

[2] Keisuke Arai, *On the Rasmussen-Tamagawa conjecture for QM-abelian surfaces*, preprint, submitted (http://arxiv.org/abs/1211.0599).

[3] Steven Arno, *The imaginary quadratic fields of class number* 4, Acta Arith. **60** (1992), no. 4, 321–334.

[4] Steven Arno, M. Robinson, and Ferrell Wheeler, *Imaginary quadratic fields with small odd class number*, Acta Arithmetica **83** (1998), no. 4, 295–330 (eng).

[5] G. V. Belyĭ, *On galois extensions of a maximal cyclotomic field*, Math. USSR-Izv. **14** (1980), no. 2, 247–256.

[6] Pete L. Clark, Brian Cook, and James Stankewicz, *Torsion points on elliptic curves with complex multiplication*, Int. J. Number Theory **9** (2013), 447–479.

[7] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000.

[8] David A. Cox, *Primes of the form* $x^2 + ny^2$, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1989, Fermat, class field theory and complex multiplication.

[9] John Cremona, *Elliptic curve data*, `http://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html`, 2014.

[10] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR 2112196 (2006f:11045)

[11] Luis Dieulefait, Enrique González-Jiménez, and Jorge Jiménez Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication*, Proc. Amer. Math. Soc. **139** (2011), no. 6, 1961–1969.

[12] V. G. Drinfel′d, *On quasitriangular quasi-Hopf algebras and on a group that is closely connected with* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Algebra i Analiz **2** (1990), no. 4, 149–181. MR 1080203 (92f:16047)

[13] Helmut Hasse, *Neue begrndung der komplexen multiplikation. erster teil: Einordnung in die allgemeine klassenkrpertheorie.*, Journal fr die reine und angewandte Mathematik **157** (1927), 115–139 (ger).

[14] Allen Hatcher, Pierre Lochak, and Leila Schneps, *On the Teichmüller tower of mapping class groups*, J. Reine Angew. Math. **521** (2000), 1–24. MR 1752293 (2001h:57018)

[15] Hans Heilbronn, *On the class-number in imaginary quadratic fields*, The Quarterly Journal of Mathematics **os-5** (1934), no. 1, 150–160.

[16] Yasutaka Ihara, *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. (2) **123** (1986), no. 1, 43–106. MR 825839 (87c:11055)

[17] ———, *Braids, Galois groups, and some arithmetic functions*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), Math. Soc. Japan, Tokyo, 1991, pp. 99–120. MR 1159208 (95c:11073)

[18] ———, *On the embedding of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *into* $\widehat{\mathrm{GT}}$, The Grothendieck theory of dessins d'enfants (Luminy, 1993), London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994, With an appendix: the action of the absolute Galois group on the moduli space of spheres with four marked points by Michel Emsalem and Pierre Lochak, pp. 289–321. MR 1305402 (96b:14014)

[19] Gerald J. Janusz, *Algebraic number fields*, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996.

[20] Serge Lang, *Elliptic functions*, second ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987, With an appendix by J. Tate.

[21] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR 482230 (80h:14022)

[22] Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449. MR 1369424 (96i:11057)

[23] Fumiyuki Momose, *Isogenies of prime degree over number fields*, Compositio Math. **97** (1995), no. 3, 329–348. MR 1353278 (97f:11039)

[24] Hiroaki Nakamura and Leila Schneps, *On a subgroup of the grothendieck-teichmller group acting on the tower of profinite teichmller modular groups*, Inventiones mathematicae **141** (2000), no. 3, 503–560 (English).

[25] Yoshiyasu Ozeki, *Non-existence of certain galois representations with a uniform tame inertia weight*, Int. Math. Res. Not. **2011** (2011), no. 11, 2377–2395.

[26] ———, *Non-existence of some cm abelian varieties with certain prime power torsion*, Tohoku. Math. J. **65** (2013), no. 3, 357–371.

[27] Yoshiyasu Ozeki and Yuichiro Taguchi, *On congruences of Galois representations of number fields*, preprint, submitted (http://arxiv.org/abs/1306.0321).

[28] Matthew Papanikolas and Christopher Rasmussen, *On the torsion of Jacobians of principal modular curves of level* 3^n, Arch. Math. (Basel) **88** (2007), no. 1, 19–28.

[29] Dipendra Prasad and C. S. Yogananda, *Bounding the torsion in CM elliptic curves*, C. R. Math. Acad. Sci. Soc. R. Can. **23** (2001), no. 1, 1–5. MR 1816457 (2002j:11057)

[30] C. Rasmussen, *On the fields of 2-power torsion of certain elliptic curves*, Math. Res. Lett. **11** (2004), no. 4, 529–538.

[31] Christopher Rasmussen, *On elliptic curves of conductor* 11^2 *and an open question of Ihara*, Algebraic number theory and related topics 2007, RIMS Kôkyûroku Bessatsu, B12, Res. Inst. Math. Sci. (RIMS), Kyoto, 2009, pp. 101–113. MR 2605776 (2012a:14056)

[32] Christopher Rasmussen and Akio Tamagawa, *Arithmetic of abelian varieties with constrained torsion*, preprint, submitted (http://arxiv.org/abs/1302.1477).

[33] ———, *A finiteness conjecture on abelian varieties with constrained prime power torsion*, Math. Res. Lett. **15** (2008), no. 6, 1223–1231.

[34] Leila Schneps, *The Grothendieck-Teichmüller group* $\widehat{\mathrm{GT}}$*: a survey*, Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, pp. 183–203. MR 1483118 (99a:14043)

[35] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR 0236190 (38 #4488)

[36] Romyar T. Sharifi, *Relationships between conjectures on the structure of pro-p Galois groups unramified outside p*, Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, RI, 2002, pp. 275–284. MR 1935409 (2004c:11204)

[37] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971, Kanô Memorial Lectures, No. 1.

[38] A. Silverberg, *Points of finite order on abelian varieties*, p-adic methods in number theory and algebraic geometry, Contemp. Math., vol. 133, Amer. Math. Soc., Providence, RI, 1992, pp. 175–193. MR 1183978 (93h:11058)

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

[40] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094 (2010i:11005)

[41] H. M. Stark, *On complex quadratic fields wth class-number two*, Math. Comp. **29** (1975), 289–302, Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday.

[42] Tamás Szamuely, *Galois groups and fundamental groups*, Cambridge Studies in Advanced Mathematics, vol. 117, Cambridge University Press, Cambridge, 2009. MR 2548205 (2011b:14064)

[43] Christian Wagner, *Class number* 5*,* 6 *and* 7, Math. Comp. **65** (1996), no. 214, 785–800.

[44] Mark Watkins, *Class numbers of imaginary quadratic fields*, Math. Comp. **73** (2004), no. 246, 907–938 (electronic).