Math. Res. Lett.
Volume 22, Number 2, 403–416, 2015

A uniform version of a finiteness conjecture for CM elliptic curves

Abbey Bourdon

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 these fields 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.

1. Introduction

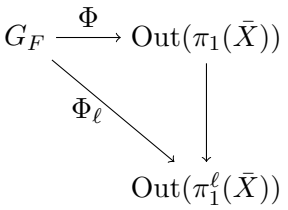
Galois representations are an indispensable tool for analyzing the structure of the absolute Galois group of a number field F. One example of considerable interest comes from the fact that $G_F := \mathrm{Gal}(\bar{F}/F)$ acts (up to inner automorphism) on the algebraic fundamental group of the projective line minus three points. More precisely, if we let $X = \mathbb{P}^1_F \setminus \{0, 1, \infty\}$ and $\bar{X} = X \otimes_F \bar{F}$, we may relate $\pi_1(X)$ and $\pi_1(\bar{X})$ through the following exact sequence:

$$1 \to \pi_1(\bar{X}) \to \pi_1(X) \to G_F \to 1.$$

From this we construct the natural representation

$$\Phi\colon G_F \to \mathrm{Out}(\pi_1(\bar{X})).$$

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



The fixed field of the kernel of Φ_ℓ, which we will denote $Ш(F,\ell)$, is a large subfield of $\bar{F}$ that as of yet is not entirely understood. We know from Ihara's 1986 paper [10] that $Ш(F,\ell)$ is a pro-ℓ extension of $F(\mu_{\ell^\infty})$ unramified away from ℓ, but it is still an open question, first posed by Ihara in the case where $F=\mathbb{Q}$, to determine whether $Ш(F,\ell)$ is the *maximal* such extension.

Subfields arising from geometric objects have helped to shed light on the structure of $Ш(F,\ell)$. For example, by the work of Rasmussen, Papanikolas, and Tamagawa in [15], [14], and [17], we know that if E is an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathbb{Q}(\sqrt{-\ell})$ and good reduction away from ℓ, the field $\mathbb{Q}(E[\ell^\infty])$ is a subfield of $Ш(\mathbb{Q},\ell)$. However, a finiteness conjecture made by Rasmussen and Tamagawa in [17] implies such examples arising from abelian varieties are quite rare. As this conjecture motivates our work, we pause to introduce some notation and formalize its statement.

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. *Let F be a number field and $g>0$. The set $\mathscr{A}(F,g)$ is finite.*

This implies that, for a fixed F and g, there exists a constant C for which $\mathscr{A}(F,g,\ell)=\varnothing$ when $\ell > C$. One may ask whether stronger behavior should be expected for the bound C, and indeed the following uniform (meaning uniform in the degree of $F/\mathbb{Q}$) conjecture appears in [16, Conj. 2]:

Conjecture 2. *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 $\ell > C$.*

In [17], Rasmussen and Tamagawa prove Conjecture 1 in the cases where $g=1$ and $[F:\mathbb{Q}]=1$ or 2, excluding the 9 imaginary quadratic fields of class

number one. In addition, they find a complete list of $\mathbb{Q}$-isogeny classes in $\mathscr{A}(\mathbb{Q},1)$, showing that $\mathscr{A}(\mathbb{Q},1,\ell)$ is empty if $\ell > 163$. Later work by Ozeki in [13] proves Conjecture 1 for abelian varieties with complex multiplication defined over a number field containing the CM field, and Arai has explored the conjecture in the context of QM-abelian surfaces (see [1]).

More recently in [16], Rasmussen and Tamagawa prove that the Generalized Riemann Hypothesis implies Conjecture 1, and they give unconditional proofs in several new cases where the degree of F is restricted and $g \leq 3$. (In particular, they resolve the conjecture in the case where F is an imaginary quadratic field of class number one and $g = 1$.) In addition, they prove a slightly stronger version of Conjecture 2 under the Generalized Riemann Hypothesis for any g and any F of odd degree.

Despite this progress, Conjecture 2 is known unconditionally only in the case where $g = 1$ and $[F : \mathbb{Q}] = 1$ or 3 (see [17], [16]). Moreover, aside from the case when $F = \mathbb{Q}$, any known bounds are likely far from optimal. In this article, 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 1. *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 1, 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 1 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.

A discussion of computed bounds is included at the end of Section 3.

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, i.e., by those points with order ℓ^r for some $r \in \mathbb{Z}^+$.
- 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 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, $\mathcal{N}(\mathfrak{a}) = [\mathcal{O}_F : \mathfrak{a}]$.
- $\left(\frac{a}{\ell}\right)$ is the Kronecker symbol.

2. Background on ray class fields and elliptic curves

We first recall the definition of the $\mathfrak{m}$-ray class group. Though the theory exists in more generality, here we restrict our attention to the case where K is an imaginary quadratic field so we may take $\mathfrak{m}$ to be an integral ideal of $\mathcal{O}_K$. Then relative to $\mathfrak{m} = \prod \mathfrak{p}^{m(\mathfrak{p})}$, we define the following two subsets:

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

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

Note $P_K(\mathfrak{m})$ is a subgroup of $I_K(\mathfrak{m})$, and the quotient $I_K(\mathfrak{m})/P_K(\mathfrak{m})$ is the $\mathfrak{m}$-ray class group of K. As with the ideal class group, whose definition we recover when $\mathfrak{m} = 1$, the $\mathfrak{m}$-ray class group is finite. In fact, we have the following explicit formula for its cardinality:

Proposition 1. *Let $\mathfrak{m}$ be an integral ideal in a number field K. The order of the ray class group modulo $\mathfrak{m}$ is given by:*

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

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 [5]. 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, $h_{\mathfrak{m}} = h_K \cdot [U : U_{\mathfrak{m}}]^{-1} \cdot (\ell + 1) \cdot (\ell - 1)$.

Just as the ideal class group gives the Galois group of the Hilbert class field, in general the $\mathfrak{m}$-ray class group gives the Galois group of an abelian extension of K called the ray class field of K with modulus $\mathfrak{m}$, denoted by $K_{\mathfrak{m}}$. Ramification in the extension $K_{\mathfrak{m}}/K$ is restricted to primes dividing $\mathfrak{m}$, and the primes that split completely are precisely the primes in $P_K(\mathfrak{m})$. The fact that a unique $K_{\mathfrak{m}}$ exists for any ideal $\mathfrak{m}$ of $\mathcal{O}_K$ is a consequence of the Existence Theorem of Class Field Theory, and we direct the interested reader to Chapter 5 of [11] for details.

We can construct the ray class fields of an imaginary quadratic field K using torsion points of elliptic curves possessing complex multiplication. Recall that if E/F is an elliptic curve, we say E has complex multiplication, or CM, if its ring of $\bar{F}$-endomorphisms is strictly larger than $\mathbb{Z}$. In this case, $\mathrm{End}(E) \otimes \mathbb{Q}$ is isomorphic to an imaginary quadratic field K, and $\mathrm{End}(E)$ is isomorphic to an order in that field. 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, as we will now explain.

Since $\mathrm{char}(F) \neq 2$ or 3, E is isomorphic over F to a curve having an equation of the form $y^2 = 4x^3 - g_2x - g_3$, with $g_2, g_3 \in F$. The Weber function $\mathfrak{h}$ on E is defined as follows, where j_E is the j-invariant of E and

$\Delta = g_2^3 - 27g_3^2$:

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

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 [8]:

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 [12, 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 [18, 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 $K(j_E)$. (See [19, p.105].) 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. □

3. Proof of main result

For an arbitrary elliptic curve, the mod-ℓ Galois representation is an injective homomorphism $\mathrm{Gal}(F(E[\ell])/F) \to \mathrm{GL}_2(\mathbb{F}_\ell)$. As a consequence, $[F(E[\ell]) : F]$ must divide $\#\mathrm{GL}_2(\mathbb{F}_\ell)$. However, if E has CM, much more is known:

Proposition 2. *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* $[F(E[\ell]) : F] \mid 2(\ell^2-\ell)$.

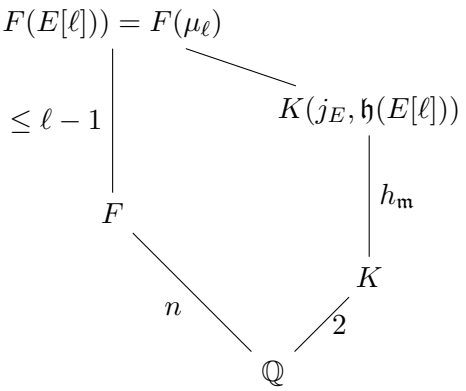
Proof. See, for example, Corollary 17 of [4]. □

From these conditions, 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 1. *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 2 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 15 in [4], $K \subset F(E[\ell])$. Thus $F(E[\ell])$ also contains $K(j_E, \mathfrak{h}(E[\ell]))$, the ray class field of K modulo $\mathfrak{m} = \ell\mathcal{O}_K$. 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, $h_{\mathfrak{m}} \geq \frac{1}{w_K} \cdot (\ell-1)^2$. But

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

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

In fact, the same result holds for elliptic curves with CM by an arbitrary order:

Proposition 3. *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 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 cyclic of degree f (Proposition 25 in [4]), we need only to show that f and ℓ are relatively prime. This will ensure the induced map $\varphi\colon E[\ell] \to E'[\ell]$ is in fact an isomorphism, and since the isomorphism is defined over F, we will have $F(E[\ell]) = F(E'[\ell])$. The result will then be a consequence of the previous lemma.

Let $f = p_1^{a_1} \cdots p_r^{a_r}$ be the prime factorization of f, with $p_1 < p_2 < \cdots < p_r$. As shown in [6, p.146], 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 $|\mathcal{O}_f^\times| \geq 2$,

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

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 $\mathcal{O}_f$ (see [6, p.220]). Thus $[K(j_E) : K] = \#\mathrm{cl}(\mathcal{O}_f)$, and $h(\mathcal{O}_f) \leq n$. 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. □

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 15 in [4], $K = \mathbb{Q}(\sqrt{D}) \subset F(E[\ell])$. 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 1. *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 $\#\mathrm{cl}(\mathcal{O}_f) = [K(j_E) : K] \leq n$, 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 [9], 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 [3] 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 [20], [2], [21] for lists of imaginary quadratic fields of class number 2, 4, and 6, respectively). More recent work by Watkins in [22] 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 a power of ℓ, and by Proposition 3, 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 1, 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 [17] 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 Watkins paper [22], he 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 $n \leq 100$.

4. 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 this paper, it is desirable to discover sufficient conditions as well. As discussed in the introduction, elliptic curves possessing this characteristic help us better understand $Ш(F, \ell)$, provided they also have good reduction away from ℓ. Here, we present two additional applications.

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

Lemma 2. *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 [17], and a more general version appears in [16]. Note that although the result in [16] 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. □

Knowing the sufficient conditions for $[F(E[\ell]) : F(\mu_\ell)]$ to be a power of ℓ would also establish when there exist ℓ-torsion points rational over $F(\mu_\ell)$:

Lemma 3. *Suppose E is an elliptic curve defined over a number field F. 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 $E[\ell]$, yielding $\mathrm{Gal}(F(E[\ell])/F(\mu_\ell)) \cong \left\langle \left[\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right] \right\rangle$, where $b \in \mathbb{F}_\ell$. (Recall the determinant of this matrix will equal the cyclotomic character, which is trivial in this extension.) But this group 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 2. □

Unfortunately, the converse of Proposition 3 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 [7], $\sqrt{7}$ 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.

Acknowledgements

The author is grateful to her advisor, Chris Rasmussen, for suggesting the problem and for his guidance in preparing this paper. The author would also like to thank Akio Tamagawa for his helpful comment on the Weber function, as well as Ravi Ramakrishna and James Stankewicz for their remarks on a draft of this paper. Finally, the author appreciates the comments and suggestions made by the referee.

References

[1] Keisuke Arai. *On the Rasmussen-Tamagawa conjecture for QM-abelian surfaces.* RIMS Kôkyûroku Bessatsu B44, Res. Inst. Math. Sci. (RIMS), Kyoto, 2013.

[2] Steven Arno, *The imaginary quadratic fields of class number* 4. Acta Arith., **60**(4):321–334, 1992.

[3] Steven Arno, M. Robinson and Ferrell Wheeler, *Imaginary quadratic fields with small odd class number.* Acta Arithmetica, **83**(4):295–330, 1998.

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

[5] Henri Cohen, *Advanced topics in computational number theory*, volume 193 of "Graduate Texts in Mathematics". Springer-Verlag, New York, 2000.

[6] David A. Cox, *Primes of the form* $x^2 + ny^2$. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989.

[7] 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**(6):1961–1969, 2011.

[8] Helmut Hasse, *Neue begründung der komplexen multiplikation. erster teil: Einordnung in die allgemeine klassenkörpertheorie.* Journal für die reine und angewandte Mathematik, **157**:115–139, 1927.

[9] Hans Heilbronn, *On the class-number in imaginary quadratic fields.* The Quarterly Journal of Mathematics, os-**5**(1):150–160, 1934.

[10] Yasutaka Ihara, *Profinite braid groups, Galois representations and complex multiplications.* Ann. of Math. (2), **123**(1):43–106, 1986.

[11] Gerald J. Janusz, *Algebraic number fields*, volume 7 of "Graduate Studies in Mathematics". American Mathematical Society, Providence, RI, second edition, 1996.

[12] Serge Lang, *Elliptic functions*, volume 112 of "Graduate Texts in Mathematics". Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[13] Yoshiyasu Ozeki, *Non-existence of certain CM abelian varieties with prime power torsion.* Tohoku Math. J. (2), **65**(3):357–371, 2013.

[14] Matthew Papanikolas and Christopher Rasmussen, *On the torsion of Jacobians of principal modular curves of level* 3^n. Arch. Math. (Basel), **88**(1):19–28, 2007.

[15] C. Rasmussen, *On the fields of 2-power torsion of certain elliptic curves.* Math. Res. Lett., **11**(4):529–538, 2004.

[16] Christopher Rasmussen and Akio Tamagawa, *Arithmetic of abelian varieties with constrained torsion.* Preprint, submitted, `arXiv:1302.1477`.

[17] Christopher Rasmussen and Akio Tamagawa, *A finiteness conjecture on abelian varieties with constrained prime power torsion.* Math. Res. Lett., **15**(6):1223–1231, 2008.

[18] 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.

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

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

[21] Christian Wagner, *Class number* 5, 6 *and* 7. Math. Comp., **65**(214):785–800, 1996.

[22] Mark Watkins, *Class numbers of imaginary quadratic fields.* Math. Comp., **73**(246):907–938 (electronic), 2004.

Department of Mathematics, University of Georgia
Athens, GA 30602-7403, USA
E-mail address: abourdon@uga.edu

Received May 23, 2013