Math. Res. Lett. **15** (2008), *no.* 6, 1223–1231

A FINITENESS CONJECTURE ON ABELIAN VARIETIES WITH CONSTRAINED PRIME POWER TORSION

Christopher Rasmussen and Akio Tamagawa

Abstract. The pro-ℓ Galois representation attached to the arithmetic fundamental group of a curve influences heavily the arithmetic of its branched 'ℓ-covers.' In many cases, the ℓ-power torsion on the Jacobian of such a cover is fixed by the kernel of this representation, giving explicit information about this kernel. Motivated by the relative scarcity of interesting examples for ℓ-covers of the projective line minus three points, the authors formulate a conjecture to quantify this scarcity. A proof for certain genus one cases is given, and an exact set of curves satisfying the required arithmetic conditions in the base case is determined.

0. Introduction and Motivation

Fix a prime ℓ, and an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$, the field of rational numbers. Let $\boldsymbol{\mu}_N$ denote the group of Nth roots of unity in $\bar{\mathbb{Q}}$, and let $\Lambda_\ell \subset \bar{\mathbb{Q}}$ denote the maximal pro-ℓ extension of $\mathbb{Q}(\boldsymbol{\mu}_\ell)$, unramified away from ℓ. Let $\mathbb{P}^1_{01\infty} := \mathbb{P}^1_{\bar{\mathbb{Q}}} \smallsetminus \{0, 1, \infty\}$. There is a natural outer Galois representation on the pro-ℓ algebraic fundamental group of $\mathbb{P}^1_{01\infty}$,

$$\rho_\ell \colon G_{\mathbb{Q}} \longrightarrow \mathrm{Out}\big(\pi_1^\ell(\mathbb{P}^1_{01\infty})\big).$$

Let Ω_ℓ denote the fixed field of the kernel of ρ_ℓ. Ihara, in [5], noticed that Ω_ℓ is a subfield of Λ_ℓ. Further, Anderson and Ihara showed, in [1], that Ω_ℓ is an infinite nonabelian extension of $\mathbb{Q}(\boldsymbol{\mu}_{\ell^\infty})$, and gave a beautiful description of Ω_ℓ: it is generated over $\mathbb{Q}$ by the ramification sets of certain genus 0 coverings of $\mathbb{P}^1$.

It is an open problem, first posed by Ihara in the 1980s, to describe the difference between the fields Ω_ℓ and Λ_ℓ, or even to decide whether or not the two are equal. There is a line of investigation for this question, which proceeds roughly as follows. Let k be a subfield of Ω_ℓ, and let C be a complete nonsingular curve over k, with good reduction away from ℓ. Let A_C denote the Jacobian of C, and let $k_C := \mathbb{Q}(A_C[\ell^\infty])$, the field generated by the ℓ-power torsion of A_C. If $k(A_C[\ell]) \subset \Lambda_\ell$, it follows from the results of Serre and Tate [11] that k_C is a subfield of Λ_ℓ.

Suppose the curve C admits the structure of a *geometric ℓ-cover* of $\mathbb{P}^1_{01\infty}$, that is, there exists a morphism $f \colon C \to \mathbb{P}^1$ defined over k such that the Galois closure of $f \otimes \bar{\mathbb{Q}}$ is branched only over $\{0, 1, \infty\}$ and has ℓ-power degree. In this situation, there is a known sufficient condition on f which implies that k_C lies inside of Ω_ℓ. This is a

Received by the editors October 25, 2007.

2000 *Mathematics Subject Classification.* 11G05, 11G15, 11F80, 14H30.

The first author dedicates this work to the memory of his grandmother, Mary Dorothy Rasmussen, who passed away on January 7, 2008.

This work was partly supported by NSF grant #0134259 and JSPS KAKENHI 15740009, 18540027 and 19·07028.

result of Anderson and Ihara [1], who proved "Ω_ℓ-rationality" for the ℓ-power torsion of Jacobians for several families of curves, e.g., Fermat curves of ℓ-power level and principal modular curves of level 2^n ($\ell = 2$). Using the same approach, analogous results have been proven for elliptic curves over $\mathbb{Q}$ when $\ell \leq 3$ [10], [9] and for principal modular curves of level 3^n ($\ell = 3$) [9].

Intuitively, the constraints on the abelian variety A_C are quite strong. Ignoring the geometric requirement, even the arithmetic restraints are quite powerful. Because Λ_ℓ ramifies only over ℓ, A_C must have good reduction away from ℓ. By Faltings' proof of the Shafarevich Conjecture for abelian varieties, [4, Satz 6], for a fixed number field k, a fixed positive integer g and a fixed prime ℓ, there are only finitely many abelian varieties A/k of dimension g (up to k-isomorphism) satisfying $k(A[\ell^\infty]) \subset \Lambda_\ell$. However, this understates the situation considerably. The purpose of this article is to suggest that such finiteness results hold *even as ℓ varies over all primes*, and prove such a result in the 'base case' $k = \mathbb{Q}, g = 1$. We extend this result (still with $g = 1$) to all but finitely many quadratic number fields.

In §1, we give the necessary material to state the conjecture precisely. In §2, we prove a lemma on the structure of the Galois representation on the ℓ-torsion of such an abelian variety. In §3, we give the proof, by interpreting the lemma in the case of elliptic curves. Proving finiteness independent of the prime ℓ relies on the deep result of Mazur (and extensions by Momose) characterizing the non-cuspidal rational points of modular curves. In §4, we compute explicitly the finite set of elliptic curves $E/\mathbb{Q}$ satisfying the $\mathbb{Q}(E[\ell^\infty]) \subset \Lambda_\ell$. In §5, we demonstrate the stronger containment $\mathbb{Q}(E[\ell^\infty]) \subseteq \Omega_\ell$ holds for almost all of these elliptic curves.

1. Statement of Conjecture and Results

Let K be a number field. For any prime ℓ, let $\tilde{K}_\ell$ denote the maximal pro-ℓ extension of $K(\boldsymbol{\mu}_\ell)$ which is unramified away from ℓ (for example, if $K = \mathbb{Q}$, then $\tilde{K}_\ell = \Lambda_\ell$). For any number field K and any integer $g \geq 0$, let $\mathscr{A}(K, g, \ell)$ denote the set of K-isomorphism classes of abelian varieties A/K, of dimension g, which satisfy

$$K(A[\ell^\infty]) \subseteq \tilde{K}_\ell.$$

For fixed K and g, define also the set

$$\mathscr{A}(K, g) := \big\{([A], \ell) : [A] \in \mathscr{A}(K, g, \ell)\big\}.$$

Again, it follows from the finiteness theorems on abelian varieties with prescribed reduction type that the sets $\mathscr{A}(K, g, \ell)$ must be finite. However, it is not clear a priori why the set $\mathscr{A}(K, g)$ should be finite – that is, why should one expect $\mathscr{A}(K, g, \ell) = \varnothing$ for all ℓ sufficiently large? As we will show in §2, the Galois structure of the ℓ-torsion of such an abelian variety is constrained in such a way to make the appearance of large ℓ quite unlikely.

Conjecture 1. *Let K be a number field and let $g \geq 0$. Then the set $\mathscr{A}(K, g)$ is finite.*

In evidence of the conjecture, we will demonstrate the following.

Theorem 2. *The set $\mathscr{A}(\mathbb{Q}, 1)$ is finite. That is, there are only finitely many pairs $([E], \ell)$ of $\mathbb{Q}$-isomorphism classes of elliptic curves E over $\mathbb{Q}$ and primes ℓ for which $\mathbb{Q}(E[\ell^\infty]) \subseteq \Lambda_\ell$.*

Specifically, if $([E], \ell) \in \mathscr{A}(\mathbb{Q}, 1)$, then $\ell \leq 163$. In fact, we determine exactly the set $\mathscr{A}(\mathbb{Q}, 1)$ in this paper. One can deduce quickly from the Riemann-Hurwitz formula that a genus 1 curve can admit the structure of a geometric ℓ-cover of $\mathbb{P}^1_{01\infty}$ only if $\ell \leq 3$. Hence, there exist curves $C/\mathbb{Q}$ which do not admit the structure of a geometric ℓ-cover of $\mathbb{P}^1_{01\infty}$, but whose Jacobians satisfy $\mathbb{Q}(A_C[\ell^\infty]) \subseteq \Lambda_\ell$. In fact, most of the curves in $\mathscr{A}(\mathbb{Q}, 1)$ also satisfy $\mathbb{Q}(A_C[\ell^\infty]) \subseteq \Omega_\ell$. To the authors' knowledge, these are the first explicit examples of curves which have this property, but which do not admit the structure of a geometric ℓ-cover of $\mathbb{P}^1_{01\infty}$.

By using the results of Momose, we extend Theorem 2 to prove finiteness for $\mathscr{A}(K, 1)$ for almost all quadratic extensions $K/\mathbb{Q}$. A precise statement is given in §3.

2. Lemma on Galois Action

Consider the tower of fields $\mathbb{Q} \subset \mathbb{Q}(\boldsymbol{\mu}_\ell) \subset \Lambda_\ell$, corresponding to the exact sequence

$$1 \longrightarrow \mathrm{Gal}\,(\Lambda_\ell/\mathbb{Q}(\boldsymbol{\mu}_\ell)) \longrightarrow \mathrm{Gal}\,(\Lambda_\ell/\mathbb{Q}) \longrightarrow \mathrm{Gal}\,(\mathbb{Q}(\boldsymbol{\mu}_\ell)/\mathbb{Q}) \longrightarrow 1 \quad . \tag{1}$$

The purpose of this section is to show that when the group in the middle of the above sequence acts on a finite dimensional $\mathbb{F}_\ell$-vector space (e.g., the ℓ-torsion of an abelian variety), the action is highly constrained.

In this section, let G be a group with a normal pro-ℓ subgroup N, such that the quotient $\Delta = G/N$ is isomorphic to $\mathbb{F}_\ell^\times$. Because N is pro-ℓ, it has trivial image under any character $\psi\colon G \to \mathbb{F}_\ell^\times$. Hence, there is always an induced character $\bar{\psi}\colon \Delta \to \mathbb{F}_\ell^\times$. Let $\chi\colon G \to \mathbb{F}_\ell^\times$ be a character such that the induced character $\bar{\chi}$ is an isomorphism. Finally, let V be a finite dimensional $\mathbb{F}_\ell$-vector space of dimension d on which G acts continuously.

Lemma 3. *The vector space V admits a filtration*

$$\{0\} = V_0 \subset V_1 \subset \cdots \subset V_{d-1} \subset V_d = V$$

such that each V_i has dimension i and is fixed (as a set) by G. Further, for each $1 \leq i \leq d$, G-action on the space V_i/V_{i-1} is given by $g \cdot \bar{v} = \chi(g)^{k_i} \cdot \bar{v}$ for some $k_i \in \mathbb{Z}$, $0 \leq k_i \leq \ell - 2$.

Remarks. Choose an ordered basis $\{v_1, v_2, \ldots, v_d\}$ of V with each $v_i \in V_i \smallsetminus V_{i-1}$. The lemma implies that with respect to this basis, the action of G has the upper-triangular form

$$\begin{pmatrix} \chi^{k_1} & * & \cdots & * \\ & \chi^{k_2} & \cdots & * \\ & & \ddots & \vdots \\ & & & \chi^{k_d} \end{pmatrix}.$$

In the following sections, we will specialize to the case where $G = \mathrm{Gal}(\Lambda_\ell/\mathbb{Q})$, $N = \mathrm{Gal}(\Lambda_\ell/\mathbb{Q}(\boldsymbol{\mu}_\ell))$, χ is the ℓ-cyclotomic character mod ℓ, and $V = A[\ell]$ for some abelian variety A. However, the lemma needs none of these additional assumptions.

Proof of Lemma 3. The proof will proceed by induction on d. The $d = 1$ case is trivial – G must act via a power of χ. So assume the result holds for $\mathbb{F}_\ell$-vector spaces of dimension $d - 1$, and let V be an $\mathbb{F}_\ell$-vector space of dimension d.

Consider the action of N on V, which necessarily factors through some finite ℓ-group N_0. Hence, the N-orbits of V must all have order a power of ℓ and so the subspace V^N of fixed points is non-trivial ($V^N = \{0\}$ implies ℓ divides $|V| - 1$, which is impossible). Further, because N is normal in G, we have that V^N is G-stable, and so a well-defined action of Δ on V^N is induced. More explicitly, for any $\delta \in \Delta$, choose a lift $g \in G$, and define $\delta \cdot v = g \cdot v$. The action is well-defined, because two lifts differ by an element $n \in N$, which fixes all $v \in V^N$.

Now, suppose $\Delta = \langle \delta \rangle$. Fix a basis for V^N, and let $\rho\colon \Delta \to GL(V^N)$ be the associated representation. Because $\delta^{\ell-1} = e$, we know that the matrix $A = \rho(\delta)$ satisfies $A^{\ell-1} = I$. Consequently, the minimal polynomial for A splits completely over $\mathbb{F}_\ell$, and so A has an eigenvector w with some eigenvalue $\lambda \in \mathbb{F}_\ell^\times$. Choose $0 \le k_1 \le \ell - 2$ so that $\bar{\chi}^{k_1}(\delta) = \lambda$. Hence, Δ fixes the subspace $W = \langle w \rangle$, and acts via $\bar{\chi}^{k_1}$ on W: $\delta^i \cdot w = \lambda^i w = \bar{\chi}^{k_1}(\delta^i) w$.

Since $W \subseteq V^N$, χ^{k_1} actually gives the action of G on W, and so W is G-stable. Hence, there is an induced G-action on the quotient space $V' = V/W$, which has dimension $d - 1$. By the induction hypothesis, there is a filtration

$$\{0\} = V_0' \subset V_1' \subset \cdots \subset V_{d-1}' = V' \tag{2}$$

such that G acts on each quotient V_i'/V_{i-1}' via $\chi^{k_i'}$. Let $\pi\colon V \to V'$ be the natural projection, and define $V_0 = \{0\}$, $V_i := \pi^{-1}(V_{i-1}')$. Because W is G-stable, π is G-equivariant. In particular, V_i is G-stable.

We know G acts via a power of χ on $V_1 = W$. Let $i \ge 2$. Then, for any $g \in G$, $v \in V_i$, we see that

$$\begin{aligned} \pi(g \cdot v) &= g \cdot \pi(v) \\ &= \chi^{k_{i-1}'}(g) \cdot \pi(v) + v' \qquad\qquad v' \in V_{i-2}' \\ &= \pi\left(\chi^{k_{i-1}'}(g) \cdot v + v^*\right), \end{aligned} \tag{3}$$

where $v^* \in V_{i-1}$ is such that $\pi(v^*) = v'$. Hence, there exists $w \in W$ such that

$$g \cdot v = \chi^{k_{i-1}'}(g) \cdot v + v^* + w. \tag{4}$$

Since $v^* + w \in V_{i-1}$, we see G acts on V_i/V_{i-1} via $\chi^{k_{i-1}'}$. This completes the proof of the lemma (letting $k_i = k_{i-1}'$ for $i \ge 2$). □

3. Applying the Lemma

Proof of Theorem 2. We want to show that the set $\mathscr{A}(\mathbb{Q}, 1)$ is finite. First, recall that for any ℓ, $\mathscr{A}(\mathbb{Q}, 1, \ell)$ must be finite, since any element of the set is represented by an E with good reduction away from ℓ. Hence, it is enough to demonstrate a bound for all ℓ appearing in a pair $([E], \ell) \in \mathscr{A}(\mathbb{Q}, 1)$.

Let $([E], \ell) \in \mathscr{A}(\mathbb{Q}, 1)$. Since the ℓ-power torsion of E is rational over Λ_ℓ, the group $G = \mathrm{Gal}(\Lambda_\ell/\mathbb{Q})$ acts on the $\mathbb{F}_\ell$-vector space $E[\ell]$. By Lemma 3, the representation of this action

$$\rho_{E,\ell}\colon G \longrightarrow \mathrm{Aut}(E[\ell]) \cong GL_2(\mathbb{F}_\ell) \tag{5}$$

must have the form

$$\rho_{E,\ell} = \begin{pmatrix} \chi^i & * \\ 0 & \chi^{1-i} \end{pmatrix}, \tag{6}$$

where $\chi\colon G \to \mathbb{F}_\ell^\times$ is the ℓ-cyclotomic character mod ℓ (The powers of χ on the diagonal are determined by the condition $\det \rho_{E,\ell} = \chi$). Hence, $E[\ell]$ has a G-stable subspace C of dimension 1, corresponding to the space $\langle \binom{1}{0} \rangle \subset \mathbb{F}_\ell^2$. Of course, C is therefore a (cyclic) subgroup of order ℓ of E which is rational over $\mathbb{Q}$.

Recall that $Y_0(N)$ denotes the moduli space (over $\mathbb{Z}[1/N]$) for isomorphism classes of pairs (E', C'), where E' is an elliptic curve, and C' is a cyclic subgroup of E' of order N. A point of $Y_0(N)$ corresponding to a class $[(E', C')]$ is defined over a field k if and only if both E' and C' are defined over k.

So the pair (E, C) corresponds to a point in the set $Y_0(\ell)(\mathbb{Q})$. However, Mazur [7] has proven that for sufficiently large ℓ, $Y_0(\ell)(\mathbb{Q}) = \varnothing$. More precisely, $Y_0(\ell)(\mathbb{Q}) \neq \varnothing$ if and only if

$$\ell \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

(We call this the *exceptional set* of primes.) Thus, the set $\mathscr{A}(\mathbb{Q}, 1)$ is finite. □

In the proof, our restriction to the field $\mathbb{Q}$ is due to the fact that Mazur's result is not known for general number fields. However, let K be any quadratic number field other than one of the nine quadratic imaginary fields of class number one. Then Momose [8, Thm. B] has shown that there are only finitely many primes ℓ for which $Y_0(\ell)(K) \neq \varnothing$. Hence, we also have:

Theorem 4. *Let K be a quadratic number field other than the imaginary quadratic fields of class number one. Then the set $\mathscr{A}(K, 1)$ is finite.*

Proof. The argument is essentially the same as for Theorem 2, replacing the group $\mathrm{Gal}(\Lambda_\ell/\mathbb{Q})$ with $\mathrm{Gal}(\tilde{K}_\ell/K)$. The only concern is the application of Lemma 3. If $K \subseteq \mathbb{Q}(\boldsymbol{\mu}_\ell)$, then the group $\Delta = \mathrm{Gal}(K(\boldsymbol{\mu}_\ell)/K) \ncong \mathbb{F}_\ell^\times$, violating a hypothesis of Lemma 3. However, this concerns at most one prime ℓ_0. Because $\mathscr{A}(K, 1, \ell_0)$ is certainly finite, it follows that $\mathscr{A}(K, 1)$ is finite also. □

In the proof of Theorem 2, we have shown that $([E], \ell) \in \mathscr{A}(\mathbb{Q}, 1)$ implies E has good reduction away from ℓ and that E has a rational ℓ-isogeny (corresponding to the rational cyclic subgroup of order ℓ). The converse also holds, and we finish the section with a proof of this fact. We will need this in the next section to determine the set $\mathscr{A}(\mathbb{Q}, 1)$ precisely.

Proposition 5. *Let E be an elliptic curve defined over $\mathbb{Q}$, and let ℓ be a prime number. If E has good reduction away from ℓ and possesses a $\mathbb{Q}$-rational ℓ-isogeny, then $\mathbb{Q}(E[\ell^\infty]) \subseteq \Lambda_\ell$.*

Proof. From the assumption that E is good away from ℓ, we know that $\mathbb{Q}(E[\ell^\infty])$ is unramified away from ℓ, and is a pro-ℓ extension of $\mathbb{Q}(E[\ell])$. Hence, it suffices to show that the extension $\mathbb{Q}(E[\ell])/\mathbb{Q}(\boldsymbol{\mu}_\ell)$ has degree a power of ℓ. Denote by G° the group $\mathrm{Gal}\big(\mathbb{Q}(E[\ell])/\mathbb{Q}(\boldsymbol{\mu}_\ell)\big)$.

Choose $P \in E[\ell]$ so that $\langle P \rangle$ is the kernel of the rational ℓ-isogeny. As a set, $\langle P \rangle$ is defined over $\mathbb{Q}$. Choose $Q \in E[\ell]$ so that $\{P, Q\}$ is a basis for $E[\ell]$. Relative to this basis, the Galois representation on $E[\ell]$, $\rho_{E,\ell}$, is upper-triangular. Hence, there exists a multiplicative character $\psi\colon G_\mathbb{Q} \to \mathbb{F}_\ell^\times$ such that $\rho_{E,\ell}$ has the form

$$\begin{pmatrix} \psi & * \\ 0 & \chi \cdot \psi^{-1} \end{pmatrix}.$$

The form of the lower right entry is again forced by the determinant condition. Of course, ψ factors through $G_{\mathbb{Q}}^{\mathrm{ab}} \simeq \prod_p \mathbb{Z}_p^\times$ (viewed as a product of inertia groups). The assumptions on E guarantee that $\rho_{E,\ell}$ is unramified at all $p \neq \ell$, and so the same holds for ψ. For $p \neq \ell$ the image of inertia at p must be trivial, and so ψ must factor through $\mathbb{Z}_\ell^\times \simeq \mathbb{F}_\ell^\times \times (1 + \ell\mathbb{Z}_\ell)$. However, the second component is pro-ℓ, so ψ must further factor through $\mathbb{F}_\ell^\times$! Any such character is necessarily a power of χ. Consequently, the form of $\rho_{E,\ell}$ must be

$$\begin{pmatrix} \chi^i & * \\ 0 & \chi^{1-i} \end{pmatrix}.$$

Further, $\rho_{E,\ell}$ is injective on $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$, and so is still injective on the subgroup G°. But if $\sigma \in G^\circ$, then $\chi(\sigma) = 1$, because σ fixes $\mathbb{Q}(\boldsymbol{\mu}_\ell)$. So $\rho_{E,\ell}(G^\circ)$ must be contained in the ℓ-group

$$\left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in \mathbb{F}_\ell \right\}.$$

Thus, $\#G^\circ$ divides ℓ, and it follows that $\mathbb{Q}(E[\ell^\infty]) \subseteq \Lambda_\ell$. □

4. Analysis of $\mathscr{A}(\mathbb{Q}, 1)$

We now turn to the task of identifying precisely the set $\mathscr{A}(\mathbb{Q}, 1)$. Let $\mathscr{S}$ denote the finite set of $\mathbb{Q}$-isomorphism classes of elliptic curves over $\mathbb{Q}$ which have good reduction away from exactly one prime in the exceptional set of primes. Of course, the curves representing classes in $\mathscr{S}$ are already known – for example, they are given explicitly in Cremona's tables [3].

Note that for any element $([E], \ell) \in \mathscr{A}(\mathbb{Q}, 1)$, ℓ is determined by $[E]$, as ℓ must be the unique prime dividing the conductor of E. Hence, we will abuse the notation $\mathscr{A}(\mathbb{Q}, 1)$ and consider it as just a set of isomorphism classes of elliptic curves. In this sense, it follows that $\mathscr{A}(\mathbb{Q}, 1) \subseteq \mathscr{S}$ by the results of the previous section.

Let $\varphi\colon C_1 \to C_2$ be a non-constant morphism between projective smooth curves defined over $\mathbb{Q}$. Then there is a natural inclusion of the ℓ-adic Tate modules of the associated Jacobian varieties $T_\ell J_2 \hookrightarrow T_\ell J_1$ ($J_i := \mathrm{Jac}(C_i)$) as Galois modules, and so we have the containment $\mathbb{Q}(J_2[\ell^\infty]) \subseteq \mathbb{Q}(J_1[\ell^\infty])$. Consequently, if $[E]$ lies in the set $\mathscr{A}(\mathbb{Q}, 1)$, then so do all classes $[E']$ for curves E' which are $\mathbb{Q}$-isogenous to E. Hence, it is only necessary to decide membership in $\mathscr{A}(\mathbb{Q}, 1)$ for one curve in each $\mathbb{Q}$-isogeny class. Following Cremona's notation for such classes, we note that $\mathscr{S}$ is the union of the classes in Table 1. We will find $\mathscr{A}(\mathbb{Q}, 1)$ by computing its complement inside $\mathscr{S}$. Let E be an elliptic curve over $\mathbb{Q}$ with good reduction away from ℓ, and suppose E possesses an ℓ-isogeny. Let $p \neq \ell$ be another prime number, and let Fr_p denote the Frobenius element satisfying $\mathrm{Fr}_p(\zeta) = \zeta^p$ for any primitive $\zeta \in \boldsymbol{\mu}_\ell$. Then $\chi(\mathrm{Fr}_p) \equiv p \pmod{\ell}$. Hence, there exists an integer $0 \leq i \leq \ell - 2$, such that for all $p \neq \ell$

$$\rho_{E,\ell}(\mathrm{Fr}_p) = \begin{pmatrix} p^i & * \\ 0 & p^{1-i} \end{pmatrix}. \tag{7}$$

Recall that for each prime we define the integer a_p by

$$\#E(\mathbb{F}_p) = 1 + p - a_p, \tag{8}$$

ℓ	$\mathbb{Q}$-isogeny classes in $\mathscr{S}$
2	32a, 64a, 128a, 128b, 128c, 128d, 256a, 256b, 256c, 256d
3	27a, 243a, 243b
5	none
7	49a
11	11a, 121a, 121b, 121c, 121d
13	none
17	17a, 289a
19	19a, 361a, 361b
37	37a, 37b, 1369a, 1369b, 1369c, 1369d, 1369e, 1369f
43	43a, 1849a, 1849b, 1849c, 1849d
67	67a, 4489a, 4489b
163	163a, 26569a, 26569b

TABLE 1. Isogeny classes in $\mathscr{S}$.

which is known to give the trace of the image of $\rho_{E,\ell}$ on the Fr_p. Consequently, for all $p \neq \ell$:

$$p^i + p^{1-i} \equiv a_p \pmod{\ell}. \tag{9}$$

Now, let $[E] \in \mathscr{S}$. We have $[E] \in \mathscr{A}(\mathbb{Q}, 1)$ only if there exists a *fixed* number i, for which (9) holds for *all* $p \neq \ell$ (otherwise E cannot possess an ℓ-isogeny). For most of the isogeny classes in $\mathscr{S}$, a computer search easily finds a prime $p \neq \ell$ for which (9) fails for every i. Hence, these classes cannot belong to $\mathscr{A}(\mathbb{Q}, 1)$.

One expects that the remaining classes in $\mathscr{S}$ do possess an ℓ-isogeny, and this is indeed the case. Stein [13] has produced a probable list of all isogenies among elliptic curves over $\mathbb{Q}$ with small conductor $N < 40000$ – this extends the list for $N < 200$ provided in [2]. By 'probable,' it is meant that it is possible (though unlikely) that there exist $\mathbb{Q}$-isogenies not appearing on the list. It does not matter here; Stein's list verifies existence of an ℓ-isogeny for each remaining class in $\mathscr{S}$. This proves the following result.

Proposition 6. *The set $\mathscr{A}(\mathbb{Q}, 1)$ consists precisely of the 50 $\mathbb{Q}$-isomorphism classes spanned by the 21 $\mathbb{Q}$-isogeny classes listed in Table 2.*

Most of the classes in $\mathscr{A}(\mathbb{Q}, 1)$ have complex multiplication over a quadratic extension $F \subset \mathbb{Q}(\boldsymbol{\mu}_{\ell^\infty})$. If $\ell > 2$, $F = \mathbb{Q}(\sqrt{-\ell})$. The only classes without complex multiplication occur when $\ell = 2$ or $\ell = 11$. Those exceptions are set in boldface in Table 2.

5. Containment in Ω_ℓ.

We conclude with a brief argument showing that most of the classes in $\mathscr{A}(\mathbb{Q}, 1)$ have ℓ-power torsion rational over the possibly smaller field Ω_ℓ. This has already been proven for $\ell \leq 3$ in [10], [9]. For the remainder, suppose $\ell > 3$ is a prime in the exceptional set.

ℓ	$\mathbb{Q}$-isogeny classes in $\mathscr{A}(\mathbb{Q},1,\ell)$
2	32 a, 64 a, **128 a**, **128 b**, **128 c**, **128 d**, 256 a, 256 b, 256 c, 256 d
3	27 a, 243 a, 243 b
7	49 a
11	**121 a**, 121 b, **121 c**
19	361 a
43	1849 a
67	4489 a
163	26569 a

TABLE 2. Isogeny classes in $\mathscr{A}(\mathbb{Q},1)$.

As in [6], set $K := \mathbb{Q}(\boldsymbol{\mu}_{\ell^\infty})$, and let L be the maximal abelian pro-ℓ extension of K unramified away from ℓ. Set

$$S := \left\{(1-\zeta)^{1/\ell^n} : n \geq 1, \zeta \in \boldsymbol{\mu}_{\ell^\infty}, \zeta \neq 1\right\}, \tag{10}$$

and let $\tilde{L} = K(S)$. Then by definition $K \subset \tilde{L} \subseteq L \subset \Lambda_\ell$. By explicit construction (see [1]), one has $\tilde{L} \subset \Omega_\ell$.

Set $G := \mathrm{Gal}(L/K)$. As an abelian pro-ℓ group, G is naturally a $\mathbb{Z}_\ell$-module. Let c denote the automorphism of complex conjugation, or its restriction to any appropriate field. Then conjugation-by-c gives an automorphism of G, under which G decomposes into a direct sum $G_+ \oplus G_-$, where $G_\pm := \{\sigma \in G : c\sigma c = \sigma^{\pm 1}\}$. Let $L_\pm$ denote the subfields of L fixed by $G_\mp$, respectively. For all ℓ in the exceptional set, the Vandiver conjecture is known to hold, and as a consequence $L_- = \tilde{L}$. ([6, pg. 248]).

Let E be an elliptic curve representing a class in $\mathscr{A}(\mathbb{Q},1)$. With only two exceptions, E has complex multiplication over the field $F = \mathbb{Q}(\sqrt{-\ell})$. Therefore, the field $T := \mathbb{Q}(E[\ell^\infty])$ is an abelian pro-ℓ extension of F (hence of K), and we have $T \subset L$. Define $T_\pm := L_\pm \cap T$.

Proposition 7. *Assuming E has complex multiplication over F, $T_- = T$.*

Proof. It is enough to prove that $T_+ = K$, or equivalently, that $\mathrm{Gal}(T_+/\mathbb{Q})$ is abelian. We of course have an exact sequence

$$1 \longrightarrow A := \mathrm{Gal}(T_+/F) \longrightarrow H := \mathrm{Gal}(T_+/\mathbb{Q}) \longrightarrow B := \mathrm{Gal}(F/\mathbb{Q}) \longrightarrow 1\ ,$$

which is split by the homomorphism $c|_F \mapsto c|_{T_+}$. Because $T_+ \subset L_+$, we know c commutes with any $\sigma \in A$. We claim A is contained in the center of H. Fix $\alpha \in A$, and choose $\sigma \in H$. If $\sigma|_F = \mathrm{id}_F$, then $\sigma \in A$, which is abelian, and so σ commutes with α. Otherwise, $\sigma|_F = c|_F$, and so $(\sigma c)|_F = \mathrm{id}_F$. Therefore, $\sigma c \in A$ by definition. We have $\sigma\alpha = \sigma(c\alpha c) = \alpha(\sigma c)c = \alpha\sigma$, and so $A \subset Z(H)$. Thus, H is a split central extension by the abelian groups A and B, and hence H is also abelian. This means $T_+/\mathbb{Q}$ is an abelian extension, which implies $T_+ = K$ and $T = T_- \subset L_-$. □

Corollary 8. *With at most two exceptions (i.e., 121a and 121c in Table 2), an elliptic curve E representing a class in $\mathscr{A}(\mathbb{Q},1)$ satisfies $\mathbb{Q}(E[\ell^\infty]) \subset \Omega_\ell$.*

It is desirable to resolve the situation for the remaining two classes (E: 121a, 121c). In the (very unlikely) case that $\mathbb{Q}(E[11^\infty]) \not\subset \Omega_{11}$, this gives a counterexample to Deligne's conjecture at $\ell = 11$ ([12, Theorem 1.1]). More likely, the field gives an explicit example of an infinite non-abelian subextension of Ω_{11}/K.

Acknowledgments

The authors wish to thank Romyar Sharifi for a helpful communication regarding the field $\tilde{L}$ of §5, and Kesuke Arai for bringing the work of Fumiyuki Momose to our attention. We are also grateful to the referee for his or her many helpful comments during this article's review.

References

[1] G. Anderson and Y. Ihara, *Pro-ℓ branched coverings of $\mathbf{P}^1$ and higher circular ℓ-units*, Ann. of Math. (2) **128** (1988), no. 2, 271–293.

[2] B. J. Birch and W. Kuyk, editors, Modular functions of one variable. IV, Springer-Verlag, Berlin (1975). Lecture Notes in Mathematics, Vol. 476.

[3] J. E. Cremona, *Elliptic Curve Data* (2005). URL: `http://www.maths.nottingham.ac.uk/personal/jec/ftp/data/INDEX.html`.

[4] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

[5] Y. Ihara, *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. (2) **123** (1986), no. 1, 43–106.

[6] ———, *Some arithmetic aspects of Galois actions in the pro-p fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$*, in Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Vol. 70 of *Proc. Sympos. Pure Math.*, 247–273, Amer. Math. Soc., Providence, RI (2002).

[7] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[8] F. Momose, *Isogenies of prime degree over number fields*, Compositio Math. **97** (1995), no. 3, 329–348.

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

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

[11] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968) 492–517.

[12] R. T. Sharifi, *Relationships between conjectures on the structure of pro-p Galois groups unramified outside p*, in Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Vol. 70 of *Proc. Sympos. Pure Math.*, 275–284, Amer. Math. Soc., Providence, RI (2002).

[13] W. Stein, *Isogeny Matrix Table* (2005). URL: `http://modular.math.washington.edu/Tables/allisog/`.

Wesleyan University, Middletown, CT, 06459, USA
E-mail address: `crasmussen@wesleyan.edu`

Research Institute for Mathematical Sciences, Kyoto 606–8502, JAPAN
E-mail address: `tamagawa@kurims.kyoto-u.ac.jp`