RIMS Kôkyûroku Bessatsu
Bx (200x), 000–000

On elliptic curves of conductor 11^2 and an open question of Ihara

By

Christopher Rasmussen*

Abstract

In previous work, joint with Tamagawa, the author investigated a certain class of elliptic curves with constrained prime power torsion. If an open question of Ihara has an affirmative answer, then the prime power torsion of such curves must be rational over the fixed field Ω_ℓ of the canonical outer pro-ℓ Galois representation attached to $\mathbb{P}^1_{01\infty}$. This is indeed the case for most examples. In the current work, we consider the remaining examples – elliptic curves $E/\mathbb{Q}$ with good reduction away from $\ell = 11$ which do not have complex multiplication. In these cases, we demonstrate an explicit computation of subfields of $\mathbb{Q}(E[\ell^2])$ contained in Ω_ℓ.

§ 1. Introduction

§ 1.1. Tamagawa's Conjecture

For any $n \geq 1$, let $\boldsymbol{\mu}_n$ denote the n-th roots of unity. Let ℓ be a prime number. For any number field k, let $\tilde{k}_\ell$ be the maximal pro-ℓ extension of $k(\boldsymbol{\mu}_\ell)$ unramified away from ℓ. Then Tamagawa has conjectured that the set

$$\mathscr{A}(k,g) := \left\{([A],\ell) : \dim A = g, \mathbb{Q}(A[\ell^\infty]) \subseteq \tilde{k}_\ell\right\}, \tag{1.1}$$

is finite for any fixed choice of k and g. Here, all abelian varieties are assumed to be defined over k, and $[A]$ denotes the k-isomorphism class of A. In [RT08], the author, jointly with Tamagawa, proved the conjecture in the case $g = 1$ for $k = \mathbb{Q}$ and for k almost any quadratic extension of $\mathbb{Q}$. The unsettled cases among quadratic extensions

Received April 20, 200x. Revised September 11, 200x.
2000 Mathematics Subject Classification(s): 2000 Mathematics Subject Classification(s): 14G32, 14H52, 14K02
Supported by JSPS KAKENHI 19·07028.
*Department of Mathematics & Computer Science, Wesleyan University, Middletown, Connecticut 06459, United States.
e-mail: crasmussen@wesleyan.edu

are exactly the quadratic imaginary extensions of class number one.[1] Further, the set $\mathscr{A}(\mathbb{Q},1)$ was determined explicitly.

Roughly speaking, the finiteness result follows from the following proposition, proved in [RT08]:

Proposition 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $([E],\ell) \in \mathscr{A}(\mathbb{Q},1)$ if and only if E has good reduction away from ℓ and E admits a $\mathbb{Q}$-rational ℓ-isogeny.*

Recall that $Y_0(N)$ is the open modular curve which parametrizes pairs (E,ψ), where E is an elliptic curve and ψ is an isogeny on E of degree N. The proposition implies the finiteness of $\mathscr{A}(\mathbb{Q},1)$ as follows. We have by the Shafarevich Conjecture that for a fixed ℓ, there exist only finitely many pairs $([E],\ell) \in \mathscr{A}(\mathbb{Q},1)$. In addition, the existence of a $\mathbb{Q}$-rational ℓ-isogeny ψ on E implies the existence of a corresponding point $[(E,\psi)] \in Y_0(\ell)(\mathbb{Q})$. However, by Mazur [Maz78], $Y_0(\ell)(\mathbb{Q})$ is non-empty for only finitely many ℓ. Hence, $\mathscr{A}(\mathbb{Q},1)$ must be finite.

The proof of Proposition 1.1 involves carefully considering the structure of the action of Galois on the ℓ-torsion of E for the group $\mathrm{Gal}\left(\mathbb{Q}(E[\ell^\infty])/\mathbb{Q}(\boldsymbol{\mu}_\ell)\right)$. Under the assumption that $([E],\ell) \in \mathscr{A}(\mathbb{Q},1)$, this is a pro-$\ell$ group and must in fact stabilize a nontrivial cyclic subgroup of $E[\ell]$, whence we conclude the existence of the isogeny. In fact, one can be more explicit; the Galois representation on ℓ-torsion has the form

$$\rho_{1,E} \sim \begin{pmatrix} \chi^i & * \\ 0 & \chi^{1-i} \end{pmatrix}, \tag{1.2}$$

where χ denotes the ℓ-cyclotomic character modulo ℓ. A more general result is available for the action on the ℓ-torsion of a higher dimensional abelian variety – for details, see [RT08].

§ 1.2. Relation to a Question of Ihara

In [AI88], Anderson and Ihara study the canonical outer pro-ℓ Galois representation attached to the fundamental group of $\mathbb{P}^1_{01\infty}$, the projective line with three points deleted. That representation,

$$\varphi\colon \mathrm{Gal}\left(\bar{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{Out}\left(\pi_1^\ell(\mathbb{P}^1_{01\infty}, x)\right), \tag{1.3}$$

has a kernel whose fixed field we denote Ω_ℓ. Let $\boldsymbol{\mu}_{\ell^\infty} = \cup_{n\geq 1}\boldsymbol{\mu}_{\ell^n}$. Then Ω_ℓ is an infinite pro-ℓ extension of $\mathbb{Q}\left(\boldsymbol{\mu}_{\ell^\infty}\right)$, known to lie inside Λ_ℓ, the maximal pro-ℓ extension of $\mathbb{Q}(\boldsymbol{\mu}_\ell)$ unramified away from ℓ. It is unknown whether the fields Ω_ℓ and Λ_ℓ coincide – Ihara first

[1] In a forthcoming paper, the author and Tamagawa prove the conjecture in many new cases, including for any quadratic field k when $g = 1$.

asked this question in the mid 1980's [Iha86]. In light of this open problem, it is natural to consider the following question: Given $([E], \ell) \in \mathscr{A}(\mathbb{Q}, 1)$, does the containment

$$\mathbb{Q}\big(E[\ell^\infty]\big) \subseteq \Omega_\ell \tag{1.4}$$

hold? As discussed in [RT08], the containment does hold for almost every curve in $\mathscr{A}(\mathbb{Q}, 1)$. Each pair $([E], \ell) \in \mathscr{A}(\mathbb{Q}, 1)$ falls into one of the following cases:

(i) $\ell \leq 3$.

(ii) E has complex multiplication by $\mathbb{Q}(\sqrt{-\ell})$, with $\ell \equiv 3 \pmod 4$.

(iii) E has conductor $N = 121$ and no complex multiplication.

In case (i), there are geometric arguments demonstrating the containment (1.4). The case $\ell = 2$ is treated completely in [Ras04b]. The case $\ell = 3$ is partially treated in the author's Ph. D. thesis [Ras04a], and was completely settled in [PR07].

In case (ii), as $\mathbb{Q}(\sqrt{-\ell}) \subseteq \mathbb{Q}(\boldsymbol{\mu}_\ell)$, we see $\mathbb{Q}\left(E[\ell^\infty]\right)/\mathbb{Q}\left(\boldsymbol{\mu}_{\ell^\infty}\right)$ is an abelian extension. Let Λ_ℓ^0 be the maximal abelian pro-ℓ extension of $\mathbb{Q}(\boldsymbol{\mu}_{\ell^\infty})$ unramified away from ℓ, and let c denote complex conjugation. Then the $\mathbb{Z}_\ell$-module $G = \mathrm{Gal}\left(\Lambda_\ell^0/\mathbb{Q}(\boldsymbol{\mu}_{\ell^\infty})\right)$ decomposes into two eigenspaces relative to the automorphism of G given by conjugation-by-c. In [RT08, §5], it is shown that $\mathbb{Q}(E[\ell^\infty])$ is contained in the fixed field corresponding to the space with eigenvalue $+1$, and this field is known to be contained in Ω_ℓ when the Vandiver Conjectures holds at ℓ [Iha02].

Remark. When $\ell = 3$, both cases (i) and (ii) apply. Further, it may be possible to extend the argument of case (ii) for $E/\mathbb{Q}$ with $\ell = 2$ when E has complex multiplication. However, case (i) includes eight isomorphism classes of conductor $N = 128$, none of which have complex multiplication [BK75, Table 1].

The purpose of the present article is to consider the four $\mathbb{Q}$-isomorphism classes in case (iii). We demonstrate that for these curves, the field $\mathbb{Q}(E[11^2])$ always contains a subfield K, of degree 11^3 over $\mathbb{Q}(\boldsymbol{\mu}_{11})$, which is contained inside Ω_{11}. We compute explicit field generators for the extension $K/\mathbb{Q}(\boldsymbol{\mu}_{11})$.

This containment is in fact already established, because the extension $K/\mathbb{Q}(\boldsymbol{\mu}_{11})$ is abelian and 11 is a regular prime (see [Iha02, pg. 248], for a detailed explanation). However, the explicit generators for the extension have not previously been computed. In principle, the arguments presented here can be used to compute larger abelian extensions of $\mathbb{Q}(\boldsymbol{\mu}_{11})$ inside $\mathbb{Q}(E[11^\infty])$. It is unknown, for example, how the degree of the maximal abelian extension of $\mathbb{Q}(\boldsymbol{\mu}_{11})$ inside $\mathbb{Q}(E[11^n])$ grows with n, and this could be investigated with the techniques of this article.

§ 1.3. Notation

For the remainder of the article, let $\ell = 11$. Over $\mathbb{Q}$, there are four elliptic curves E up to $\mathbb{Q}$-isomorphism which have the following properties:

(i) E has conductor $N = \ell^2 = 121$,

(ii) E has a $\mathbb{Q}$-rational ℓ-isogeny,

(iii) E does not have complex multiplication.

Of course, the first two conditions imply $([E], \ell) \in \mathscr{A}(\mathbb{Q}, 1)$. The curves reside in two isogeny classes, 121a and 121c of Cremona's tables [Cre08], and they have the following minimal Weierstrass equations:

Table 1. Non-CM curves with $N = 121$ admitting an 11-isogeny

121a1	$y^2 + xy + y$	$=$	$x^3 + x^2 -$	$30x -$	76
121a2	$y^2 + xy + y$	$=$	$x^3 + x^2 -$	$305x +$	7888
121c1	$y^2 + xy$	$=$	$x^3 + x^2 -$	$2x -$	7
121c2	$y^2 + xy$	$=$	$x^3 + x^2 - 3632x +$		82757

Between the two curves in each pair, there is an ℓ-isogeny defined over $\mathbb{Q}$, and the kernel of this isogeny is generated by a point of order ℓ which is rational over $\mathbb{Q}(\boldsymbol{\mu}_\ell)$. Further, over the field $\mathbb{Q}(\sqrt{-\ell})$, there are isomorphisms 121a1 $\cong$ 121c2, 121a2 $\cong$ 121c1 (quadratic twists by $\sqrt{-\ell}$). Hence, the fields generated by ℓ-power torsion are the same for 121a1, 121c2 or 121a2, 121c1.

In the following, we let E denote an elliptic curve, assumed to be one of the four curves above. We let E' denote the elliptic curve which is ℓ-isogenous to E over $\mathbb{Q}$, and let P_1 be a $\mathbb{Q}(\boldsymbol{\mu}_\ell)$-rational point generating the kernel of the ℓ-isogeny $E \to E'$. We further choose points $P_n, Q_n \in E[\ell^n]$ so that for every $n \geq 1$, $[\ell]P_{n+1} = P_n$, $[\ell]Q_{n+1} = Q_n$, and $\{P_n, Q_n\}$ is a basis for $E[\ell^n]$.

For any $n \geq 1$, define $G_n := \mathrm{Gal}\big(\mathbb{Q}(E[\ell^n])/\mathbb{Q}(\boldsymbol{\mu}_\ell)\big)$, and define

$$\tilde{G}_n := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}/\ell^n\mathbb{Z}) : a, d \equiv 1, c \equiv 0 \,(\mathrm{mod}\, \ell) \right\}. \tag{1.5}$$

We also define $G_\infty := \mathrm{Gal}\big(\mathbb{Q}(E[\ell^\infty])/\mathbb{Q}(\boldsymbol{\mu}_\ell)\big)$, and

$$\tilde{G}_\infty := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_\ell) : a, d \equiv 1, c \equiv 0 \,(\mathrm{mod}\, \ell) \right\}. \tag{1.6}$$

The natural Galois action on torsion points of E gives representations $\rho_{n,E} \colon G_\mathbb{Q} \to \tilde{G}_n$ and $\rho_E \colon G_\mathbb{Q} \to \tilde{G}_\infty$, which are inclusions when restricted to G_n and G_∞, respectively. We will always write these representations with respect to the bases $\{P_n, Q_n\}$.

For any integers $n > m \geq 1$, the following diagram commutes by definition:

$$\begin{array}{ccc} G_n & \xrightarrow{(\mathrm{mod}\,\ell^m)} & G_m \\ {\scriptstyle \rho_{n,E}}\downarrow & & \downarrow{\scriptstyle \rho_{m,E}} \\ \tilde{G}_n & \xrightarrow[(\mathrm{mod}\,\ell^m)]{} & \tilde{G}_m \end{array} \tag{1.7}$$

Of course, we also have $\rho_{n,E} \equiv \rho_E \,(\mathrm{mod}\,\ell^n)$.

§ 2. Kummer extensions

§ 2.1. Kummer extensions from torsion

We consider the ℓ torsion of E. As $G_1 \cong \mathbb{Z}/\ell\mathbb{Z}$, the field $\mathbb{Q}(E[\ell])$ is a Kummer extension of $\mathbb{Q}(\boldsymbol{\mu}_\ell)$. Of course, finding a primitive element for the extension $\mathbb{Q}(E[\ell])/\mathbb{Q}(\boldsymbol{\mu}_\ell)$ is quite simple. Let $\Phi(x)$ denote the ℓ-division polynomial for E. We need only choose a root β of $\Phi(x)$ such that $\Phi(x)$ splits completely over $\mathbb{Q}(\boldsymbol{\mu}_\ell, \beta)$. Unfortunately, β is not a Kummer element – that is, $\beta^\ell \notin \mathbb{Q}(\boldsymbol{\mu}_\ell)$. In this section, we construct a Kummer element for this extension.

For ease of exposition, we now let E be the curve 121c1 specifically, but we work with the Weierstrass model

$$y^2 = x^3 - 3267x - 280962. \tag{2.1}$$

The computations are no different in the other case. Let $\zeta := \exp(2\pi i/\ell) \in \boldsymbol{\mu}_\ell$. Over $\mathbb{Q}$, $\Phi(x) = I(x)J(x)$, where $I(x)$ is a degree 5 polynomial which splits completely over $\mathbb{Q}(\boldsymbol{\mu}_\ell)$. The roots of $I(x)$ correspond to the x-coordinates of points inside $\langle P_1 \rangle$. Explicitly, we have:

$$I(x) = x^5 + 429x^4 + 10890x^3 - 2829222x^2 - 56169531x + 1480352841,$$

Given $I(x)$ and the Weierstrass equation for E, we compute the coordinates for a generator of $\langle P_1 \rangle$:

$$\begin{aligned} x(P_1) &= -21 + 36(\zeta^2 + 2\zeta^3 + 2\zeta^4 + 4\zeta^5 + 4\zeta^6 + 2\zeta^7 + 2\zeta^8 + \zeta^9), \\ y(P_1) &= -108(5 + 10\zeta + 15\zeta^2 + 20\zeta^3 + 14\zeta^4 + 8\zeta^5 + 2\zeta^6 - 4\zeta^7 - 10\zeta^8 - 5\zeta^9). \end{aligned}$$

Of course, we can easily compute the coordinates of $[k]P_1$ for $0 \leq k < \ell$ by use of the formulas for the group law on E. Let $Q_1 \in E[\ell]$ be such that $x(Q_1) = \beta$. Over $\mathbb{Q}(\boldsymbol{\mu}_\ell)$, $J(x)$ splits into five factors of degree 11, $J_1(x), \ldots, J_5(x)$. Then β is a root of one of these polynomials, say $J_1(x)$.

We have already seen that with respect to the basis $\{P_1, Q_1\}$, G_1 is isomorphic to the group of unit upper triangular matrices. Hence, there exists a generator σ of G_1 such that

$$\rho_{1,E}(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{2.2}$$

So σ^k fixes P_1 and $Q_1^{\sigma^k} = [k]P_1 + Q_1$. The conjugates of β are

$$\beta^{\sigma^k} = (x(Q_1))^{\sigma^k} = x(Q_1^{\sigma^k}) = x\left([k]P_1 + Q_1\right), \qquad 0 \le k \le 10.$$

Knowing this, we construct a Kummer element for $\mathbb{Q}(E[\ell])/\mathbb{Q}(\boldsymbol{\mu}_\ell)$ in the classic way. Let

$$\kappa := \sum_{k=0}^{\ell-1} \zeta^{-(k+1)} \beta^{\sigma^k}. \tag{2.3}$$

Then

$$\kappa^\sigma = \sum_{k=0}^{\ell-1} \zeta^{-(k+1)} \beta^{\sigma^{k+1}} = \zeta\kappa, \tag{2.4}$$

and so either κ generates $\mathbb{Q}(E[\ell])$ and gives a Kummer element, or $\kappa = 0$. We can manage the computation (2.3) quite nicely in `Maple`, and determine κ in terms of β. More importantly, we can recover κ independent of β. We compute κ^ℓ and use the relation for β^ℓ coming from $J_1(x)$, the minimal polynomial of β, to eliminate large powers of β. Since $\kappa^\ell \in \mathbb{Q}(\boldsymbol{\mu}_\ell)$, this expresses κ^ℓ independent of β. Carrying out this computation, we find

$$\begin{aligned} \kappa^\ell = C_1^\ell\big(&-1022575 + 1877112(\zeta^2 + \zeta^9) + 2417629(\zeta^3 + \zeta^8) \\ &+\ \ 983639(\zeta^4 + \zeta^7) -\ \ 750141(\zeta^5 + \zeta^6)\big), \end{aligned} \tag{2.5}$$

where $C_1 \in \mathbb{Q}$. Repeating this computation when E is 121a1 or 121c2 gives a Kummer element

$$\begin{aligned} \kappa^\ell = C_2^\ell\big(&24904476854 + 7713235886(\zeta^2 + \zeta^9) + 22514944732(\zeta^3 + \zeta^8) \\ &- 4585163186(\zeta^4 + \zeta^7) + 16106026167(\zeta^5 + \zeta^6)\big), \end{aligned} \tag{2.6}$$

where again $C_2 \in \mathbb{Q}$.

§ 2.2. Some Kummer extensions inside Ω_ℓ

We would like to demonstrate that $\mathbb{Q}(\zeta, \kappa) \subseteq \Omega_\ell$. Given two Kummer elements κ, η over the same ground field, recall that they generate the same Kummer extension

if and only if the quotient $\kappa^{\ell s}/\eta^{\ell}$ gives an ℓ-th power inside the ground field for some s, $0 < s < \ell$. Unfortunately, there are a very large number of Kummer extensions of $\mathbb{Q}(\boldsymbol{\mu}_\ell)$ inside Ω_ℓ. As explained in [Iha02], Ω_ℓ contains all elements of the form

$$(1-\zeta^{1/\ell^m})^{1/\ell^n}, \qquad m,n \geq 1. \tag{2.7}$$

Hence, Ω_ℓ contains the following large class of elements

$$\eta = \big(\zeta^b \cdot \prod_{i=1}^{5}(1-\zeta^i)^{a_i}\big)^{1/\ell}, \qquad 0 \leq b \leq \ell-1, \quad 0 \leq a_i < \ell-1, \tag{2.8}$$

and each of these $\eta \in \Omega_\ell$ generates a Kummer extension of $\mathbb{Q}(\boldsymbol{\mu}_\ell)$. Clearly, an exhaustive search comparing κ to each of these η is rather impractical! Fortunately, we can reduce greatly the number of candidates with the following observation: $\mathbb{Q}(E[\ell])$ is Galois not just over $\mathbb{Q}(\boldsymbol{\mu}_\ell)$, but also over $\mathbb{Q}$. Very few of the above η have the property that the extension $\mathbb{Q}(\zeta,\eta)/\mathbb{Q}$ is Galois.

Indeed, set $L = \mathbb{Q}(\zeta,\eta)$. Let $\Delta = \mathrm{Gal}\,(\mathbb{Q}(\boldsymbol{\mu}_\ell)/\mathbb{Q})$, and let $\delta \in \Delta$ be the generator for which $\zeta^\delta = \zeta^2$. Choose $\gamma \in \mathrm{Gal}\,(L/\mathbb{Q})$ such that $\gamma|_{\mathbb{Q}(\boldsymbol{\mu}_\ell)} = \delta$. Since $L/\mathbb{Q}$ is Galois, we know $\eta^\gamma \in L$. By Kummer theory, there must exist some s, $0 < s < \ell$, such that

$$\frac{(\eta^\gamma)^\ell}{\eta^{\ell s}} \tag{2.9}$$

is an ℓ-th power in $\mathbb{Q}(\boldsymbol{\mu}_\ell)$. Of course,

$$\begin{aligned}(\eta^\gamma)^\ell &= \gamma(\eta^\ell) = \delta(\eta^\ell) = \zeta^{2b}\cdot\prod_{i=1}(1-\zeta^{2i})^{a_i}\\ &= \zeta^{2b}(1-\zeta^2)^{a_1}(1-\zeta^4)^{a_2}(-\zeta^6)^{a_3}(1-\zeta^5)^{a_3}\\ &\qquad\qquad \times(-\zeta^8)^{a_3}(1-\zeta^3)^{a_4}(-\zeta^{10})^{a_5}(1-\zeta)^{a_5}\\ &= \zeta^{2b+6a_3+8a_4+10a_5}(1-\zeta)^{a_5}(1-\zeta^2)^{a_1}(1-\zeta^3)^{a_4}(1-\zeta^4)^{a_2}(1-\zeta^5)^{a_3}.\end{aligned} \tag{2.10}$$

Hence, the quotient (2.9) is an ℓ-th power in $\mathbb{Q}(\boldsymbol{\mu}_\ell)$ if and only if all the following conditions hold modulo ℓ:

$$a_1 \equiv sa_2, \quad a_2 \equiv sa_4, \quad a_3 \equiv sa_5, \quad a_4 \equiv sa_3, \quad a_5 \equiv sa_1, \tag{2.11}$$

$$b \equiv \frac{(3s^2+5s+1)a_5}{2-s}. \tag{2.12}$$

By (2.11), if any a_i vanishes modulo ℓ, then every a_i does. But in this case, η is a primitive ℓ^2-th root of unity, which is a contradiction (we want η to generate $\mathbb{Q}(E[\ell])$, which does not contain $\boldsymbol{\mu}_{\ell^2}$). So no a_i vanishes, and from (2.11) we conclude

$$s^5 - 1 \equiv 0, \tag{2.13}$$

or $s \in \{1, 3, 4, 5, 9\}$. We see the values b, a_i are all determined by the choice of s and a_5, leaving only 50 possible values for η of the form (2.8). Using `Maple`, we can compute which of the expressions $(\eta^{\ell s}/\kappa^\ell)$ give an ℓ-th power inside $\mathbb{Q}(\boldsymbol{\mu}_\ell)$.

Proposition 2.1. *For each curve E in Table 1, $\mathbb{Q}(E[\ell]) \subseteq \Omega_\ell$, and is given explicitly as $\mathbb{Q}(\boldsymbol{\mu}_\ell)(\eta)$, where η^ℓ is given in Table 2.*

Remark. In fact, we could have restricted the possible η even further before starting a computational search, by determining the structure of the action of Δ on $\mathrm{Gal}\,(\mathbb{Q}(\zeta, \eta)/\mathbb{Q}(\boldsymbol{\mu}_\ell))$. This action is given by a certain power χ^j of the ℓ-cyclotomic character, and can be computed from the data of a_i, b. But this power j is also determined by the action of G_1 on the ℓ-torsion of E, and so even fewer η are viable candidates. This reduction is not really necessary at the level of ℓ-torsion, but could be crucial in a future attempt to analyze the Kummer extensions of $\mathbb{Q}(\boldsymbol{\mu}_{\ell^n})$ lying inside both Ω_ℓ and $\mathbb{Q}(E[\ell^{n+1}])$, for $n > 1$.

Table 2. Generator for $\mathbb{Q}(E[\ell])$ over $\mathbb{Q}(\boldsymbol{\mu}_\ell)$

E	η^ℓ
121a1 121c2	$\zeta^8(1-\zeta)^2(1-\zeta^2)^{-4}(1-\zeta^3)^6(1-\zeta^4)^{-3}(1-\zeta^5)^{-1}$
121a2 121c1	$\zeta^{10}(1-\zeta)^{-4}(1-\zeta^2)^6(1-\zeta)^{-3}(1-\zeta^4)^2(1-\zeta^5)^{-1}$

§ 3. Computation of G_2^{ab}

In light of Proposition 2.1, one might hope to find larger abelian extensions of $\mathbb{Q}(\boldsymbol{\mu}_\ell)$ inside $\Omega_\ell \cap \mathbb{Q}(E[\ell^2])$. In this section we prove $\mathbb{Q}(E[\ell^2]) \cap \Lambda_\ell^0$ is a degree ℓ^3 extension of $\mathbb{Q}(\boldsymbol{\mu}_\ell)$, but that it essentially contains "nothing new" – being generated by $\boldsymbol{\mu}_{\ell^2}$ and the ℓ-torsion of E and E'.

Proposition 3.1. *The group G_2 is isomorphic to $\tilde{G}_2$, and $G_2^{ab} \cong (\mathbb{Z}/\ell\mathbb{Z})^3$.*

The key step is to construct a morphism $G_2^{ab} \twoheadrightarrow \tilde{G}_2^{ab}$, whose surjectivity is proven by considering the images of Frobenius elements. One then lifts this surjection to an isomorphism $G_2 \xrightarrow{\sim} \tilde{G}_2$ to prove the proposition.

Define $\tilde{\pi}\colon \tilde{G}_2 \to (\mathbb{Z}/\ell\mathbb{Z})^3$ by

$$\tilde{\pi}\colon X \mapsto (b,\, c,\, a + d - bc), \qquad X = \begin{pmatrix} 1 + \ell a & b + \ell b' \\ \ell c & 1 + \ell d \end{pmatrix}, \tag{3.1}$$

for any $a, b, b', c, d \in \mathbb{Z}/\ell\mathbb{Z}$. We want to show that $\pi := \tilde{\pi} \circ \rho_{2,E}$ is a surjection. We proceed by considering each component of $\tilde{\pi} = \tilde{\pi}_1 \times \tilde{\pi}_2 \times \tilde{\pi}_3$ separately, and giving criteria for $\pi_i := \tilde{\pi}_i \circ \rho_{2,E}$ to vanish at a Frobenius element f_p, defined below.

§ 3.1. Frobenius elements

For $r \geq 1$, let ζ denote a primitive ℓ^r-th root of unity. Let $L/\mathbb{Q}$ be an extension, unramified away from ℓ, which contains $\mathbb{Q}(\boldsymbol{\mu}_\ell)$. Fix a prime $p \neq \ell$, and let $\mathfrak{P}$ be a prime in $\mathscr{O}_L$, the ring of integers of L, dividing p. We let Fr_p denote the automorphism $x \mapsto x^p$ inside the Galois group of the residue field extension. There is a natural isomorphism between this Galois group and the decomposition group of $\mathfrak{P}$ inside $\mathrm{Gal}\,(L/\mathbb{Q})$. We let f_p denote the image of Fr_p under this isomorphism.

Lemma 3.2. *Let p be a prime congruent to 1 modulo ℓ, and suppose $\mathbb{Q}(\boldsymbol{\mu}_{\ell^r}) \subseteq L$. Then f_p fixes $\mathbb{Q}(\boldsymbol{\mu}_{\ell^r})$ if and only if $p \equiv 1 \pmod{\ell^r}$.*

Proof. This is quickly deducible from standard facts about cyclotomic fields. See, for example, [Was97, Ch. 2]. However, we give a proof here for the convenience of the reader.

Suppose that $p \equiv 1 \pmod{\ell^r}$. We have $f_p(\zeta) = \zeta^j$ for some $0 \leq j < \ell^r$, and by the definition of Frobenius, we have $\zeta^j - \zeta^p = \zeta^j - \zeta \in \mathfrak{P}$. Hence, $(1 - \zeta^{j-1}) \in \mathfrak{P}$, which divides p. Of course, if $(1 - \zeta^{j-1}) \neq 0$, then there exists $\beta \in \mathscr{O}_L$ such that $\ell = \beta(1 - \zeta^{j-1})$, and so $\ell \in \mathfrak{P}$, which is nonsense. Hence, $(1 - \zeta^{j-1}) = 0$, or equivalently $\zeta^j = \zeta$. So f_p fixes $\mathbb{Q}(\boldsymbol{\mu}_{\ell^r})$.

Conversely, if f_p fixes $\mathbb{Q}(\boldsymbol{\mu}_{\ell^r})$, then $f_p(\zeta) = \zeta$, and so $1 - \zeta^{p-1} \in \mathfrak{P}$. As in the preceding paragraph, this element must therefore be zero. This is only possible if $p \equiv 1 \pmod{\ell^r}$. □

§ 3.2. The first component of $\tilde{\pi}$

Let $\tilde{\pi}_1 \colon \tilde{G}_2 \to \mathbb{Z}/\ell\mathbb{Z}$ be defined by sending the matrix X in (3.1) to b, and let $\pi_1 = \tilde{\pi}_1 \circ \rho_{2,E}$. Consider $\Phi(x)$, the ℓ-division polynomial for E. As $\Phi(x)$ does not split completely over $\mathbb{Q}(\boldsymbol{\mu}_\ell)$, G_1 is nontrivial and $\rho_{1,E}$ is surjective. It follows that the composition

$$G_2 \twoheadrightarrow G_1 \xrightarrow{\rho_{1,E}} \tilde{G}_1 \longrightarrow \mathbb{Z}/\ell\mathbb{Z}, \tag{3.2}$$

where the right-hand arrow sends a matrix to its upper right entry, must be surjective. Notice that the composition of the first two arrows is also given by $\rho_{2,E} \pmod{\ell}$, and so (3.2) is just a different expression for π_1.

Suppose that $p \equiv 1 \pmod{\ell}$ is a prime. Set $L = \mathbb{Q}(E[\ell^2])$, choose any prime $\mathfrak{P}$ dividing p in $\mathscr{O}_L$, and let $f_p \in \mathrm{Gal}(L/\mathbb{Q})$ be defined as before. By Lemma 3.2, f_p fixes

$\mathbb{Q}(\boldsymbol{\mu}_\ell)$, and so we may view $f_p \in G_2$. Let $\tilde{E}$ be the reduction of E at $\mathfrak{P}$, and let Fr_p denote the Frobenius automorphism $x \mapsto x^p$ of the residue field $\mathscr{O}_L/\mathfrak{P}$.

Lemma 3.3. *Suppose that $p \equiv 1 \pmod{\ell}$. Then $\pi_1(f_p) = 0$ if and only if Φ splits completely over $\mathbb{F}_p$.*

Proof. Recalling some standard facts about the reduction of elliptic curves [Sil86, VIII.7.1], we know that the coordinates of any point $T \in E[\ell]$ are $\mathfrak{P}$-integral. Further, the reduction map $E \to \tilde{E}$ is injective on $E[\ell]$ because p is a prime of good reduction and $p \neq \ell$ [Sil86, VII.3.1]. Finally, we recall that the reduction map (which we denote by an overline) and the action of Frobenius commute, so that for any point T, $\overline{f_p(T)} = \mathrm{Fr}_p(\bar{T})$. Because Fr_p generates the Galois group of the residue field extension, we have the following chain of equivalent statements::

$$\begin{aligned}
\pi_1(f_p) = 0 \quad &\Leftrightarrow \quad \rho_{2,E}(f_p) \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{\ell} \\
&\Leftrightarrow \quad f_p(T) = T \text{ for every } T \in E[\ell] \\
&\Leftrightarrow \quad \mathrm{Fr}_p(\bar{T}) = \bar{T} \text{ for every } \bar{T} \in \tilde{E}[\ell] \\
&\Leftrightarrow \quad \tilde{E}[\ell] \subseteq \tilde{E}(\mathbb{F}_p)
\end{aligned}$$

The last statement holds if and only if Φ splits completely over $\mathbb{F}_p$. □

§ 3.3. The second component of $\tilde{\pi}$

Let $\tilde{\pi}_2 \colon \tilde{G}_2 \to \mathbb{Z}/\ell\mathbb{Z}$ be defined by sending the matrix X in (3.1) to c, and let $\pi_2 = \tilde{\pi}_2 \circ \rho_{2,E}$. Then the isogenous curve $E' := E/\langle P_1 \rangle$ has its ℓ^n-torsion generated by the basis $\{P_{n+1} + \langle P_1 \rangle, Q_n + \langle P_1 \rangle\}$. We denote by G'_n the group $\mathrm{Gal}\,(\mathbb{Q}(E'[\ell^n])/\mathbb{Q}(\boldsymbol{\mu}_\ell))$, and denote by $\rho_{n,E'}$ the representations into $\tilde{G}_n$, with respect to these bases. We now consider the composition

$$G_2 \twoheadrightarrow G'_1 \xrightarrow{\rho_{1,E'}} \tilde{G}_1 \longrightarrow \mathbb{Z}/\ell\mathbb{Z}, \tag{3.3}$$

where this time the right-hand arrow sends a matrix to its lower left entry. Suppose $\sigma \in G_2$, and $\rho_{2,E}(\sigma)$ is given by the matrix X in (3.1). Since

$$\begin{aligned}
(P_2 + \langle P_1 \rangle)^\sigma &= (1 + a\ell)P_2 + c\ell Q_2 + \langle P_1 \rangle = P_2 + cQ_1 + \langle P_1 \rangle, \\
(Q_1 + \langle P_1 \rangle)^\sigma &= (\ell Q_2 + \langle P_1 \rangle)^\sigma \\
&= \ell((b + \ell b')P_2 + Q_2) + \langle P_1 \rangle = Q_1 + \langle P_1 \rangle,
\end{aligned} \tag{3.4}$$

we have

$$\rho_{1,E'}(\sigma) = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \tag{3.5}$$

and so 3.3 gives precisely π_2. As before, $\Phi'(x)$, the ℓ-division polynomial for E', does not split completely over $\mathbb{Q}(\boldsymbol{\mu}_\ell)$. Hence $\rho_{1,E'}$ and π_2 are surjective. We obtain the following result, whose proof is essentially identical to the proof of Lemma 3.3.

Lemma 3.4. *Suppose that $p \equiv 1 \pmod{\ell}$. Then $\pi_2(f_p) = 0$ if and only if Φ' splits completely over $\mathbb{F}_p$.*

§ 3.4. The third component of $\tilde{\pi}$

Define $\tilde{\pi}_3 \colon \tilde{G}_2 \to \mathbb{Z}/\ell\mathbb{Z}$ as the composition

$$\tilde{G}_2 \xrightarrow{\det} 1 + \ell(\mathbb{Z}/\ell^2\mathbb{Z}) \xrightarrow{(1+x\ell)\mapsto x} \mathbb{Z}/\ell\mathbb{Z} \quad . \tag{3.6}$$

Explicitly, it sends the matrix X in (3.1) to $(a + d - bc)$. Define $\pi_3 := \tilde{\pi}_3 \circ \rho_{2,E}$. Then $\det(\rho_{2,E}) \equiv \chi \pmod{\ell^2}$, where χ is the ℓ-cyclotomic character. Hence, by Lemma 3.2, $\pi_3(f_p) = 0$ if and only if $p \equiv 1 \pmod{\ell^2}$.

§ 3.5. Proof of Proposition 3.1

It is possible to prove $G_2 \cong \tilde{G}_2$ by establishing an isomorphism between G_∞ and $\tilde{G}_\infty$ using a Frattini-type argument. However, here we present a direct, if elementary, proof.

Proof of Proposition 3.1. In view of the preceding Lemmas, it is a simple matter to search over the primes $p \equiv 1 \pmod{\ell}$ to find primes p for which Φ or Φ' splits completely over $\mathbb{F}_p$. We catalog the behavior for three such primes, and the consequences for $\pi(f_p)$, in the following table. (Note, we assume $E =$ 121a2 or 121c1. For the other choices of E, simply interchange the columns for Φ and Φ'.)

Table 3. Behavior of $\pi(f_p)$ for $E \in \{121\text{a}2, 121\text{c}1\}$

p	Φ splits completely over $\mathbb{F}_p$	Φ' splits completely over $\mathbb{F}_p$	$p \equiv 1 \pmod{\ell^2}$	$\pi(f_p)$
3631	✓	—	✓	$(0, *, 0)$
10429	✓	✓	—	$(0, 0, *)$
13553	—	✓	✓	$(*, 0, 0)$

In particular, the entries marked $*$ must be non-zero. Hence, π is a surjection, and $\#G_2^{ab} \geq \ell^3$. It is easy to verify that $\#[\tilde{G}_2, \tilde{G}_2] = \ell^2$, so $\#\tilde{G}_2^{ab} = \ell^3$. Via the

inclusion $\rho_{2,E}$, we view G_2 as a matrix subgroup of $\tilde{G}_2$. Certainly $\#[G_2, G_2] \leq \ell^2$. Both claims of the proposition follow if $\#[G_2, G_2] = \ell^2$.

As π is a surjection, we know for any $(x, y, z) \in (\mathbb{Z}/\ell\mathbb{Z})^3$ there exists at least one element $\sigma_i \in G_2$ such that $\pi(\sigma_i) = (x, y, z)$. That element σ_i has the form

$$\sigma_i = \begin{pmatrix} 1 + a_i\ell & x + b_i'\ell \\ y\ell & 1 + (xy + z - a_i)\ell \end{pmatrix}, \qquad a_i, b_i' \in \mathbb{Z}/\ell\mathbb{Z}. \tag{3.7}$$

Select $\sigma_1, \sigma_2 \in G_2$ to be inverse images of $(1, 0, 0)$ and $(0, 1, 0)$, respectively. Then we have

$$\begin{aligned} [\sigma_1, \sigma_2]^2 &= \begin{pmatrix} 1 + 2\ell & -(2 + 4a_2)\ell \\ 0 & 1 - 2\ell \end{pmatrix}, \\ [\sigma_1^2, \sigma_2] &= \begin{pmatrix} 1 + 2\ell & -(4 + 4a_2)\ell \\ 0 & 1 - 2\ell \end{pmatrix}. \end{aligned} \tag{3.8}$$

These two elements of $[G_2, G_2]$ clearly generate distinct subgroups of order ℓ. Hence, $\#[G_2, G_2] > \ell$ and the proposition follows. □

Let $K = \mathbb{Q}(E[\ell^2]) \cap \Lambda_\ell^0$, so that $G_2^{ab} = \mathrm{Gal}\,(K/\mathbb{Q}(\boldsymbol{\mu}_\ell))$. We have

Corollary 3.5. *For any E in Table 1, the field K is contained in Ω_ℓ, and is the compositum of $\mathbb{Q}(E[\ell])$, $\mathbb{Q}(E'[\ell])$ and $\mathbb{Q}(\boldsymbol{\mu}_{\ell^2})$.*

It is still open even whether the ℓ^2 torsion of these elliptic curves is rational over Ω_ℓ. This illustrates our general understanding of Ω_ℓ – its structure is quite mysterious beyond the subextension which is abelian over $\mathbb{Q}(\boldsymbol{\mu}_{\ell^\infty})$.

Acknowledgments

I am very grateful to the referee, who made many helpful comments on this article, including a simplification for the proof of Proposition 3.1. In addition, I would like to thank Akio Tamagawa for our many detailed conversations on several aspects of this paper. This research was conducted while the author was a guest of the Research Institute for Mathematical Sciences, and the author recognizes their generous hospitality.

References

[AI88] 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.

[BK75] B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable. IV*, Springer-Verlag, Berlin, 1975, Lecture Notes in Mathematics, Vol. 476.

[Cre08] J. E. Cremona, *Elliptic curve data*, 2008, URL: `http://www.warwick.ac.uk/~masgaj/ftp/data/INDEX.html`.

[Iha86] Y. Ihara, *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. (2) **123** (1986), no. 1, 43–106.

[Iha02] ———, *Some arithmetic aspects of Galois actions in the pro-p fundamental group of* $\mathbb{P}^1 - \{0, 1, \infty\}$, Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, RI, 2002, pp. 247–273.

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[PR07] 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.

[Ras04a] C. Rasmussen, *Jacobians of étale covers of the projective line minus three points*, Ph.D. thesis, University of Arizona, 2004.

[Ras04b] ———, *On the fields of 2-power torsion of certain elliptic curves*, Math. Res. Lett. **11** (2004), no. 4, 529–538.

[RT08] C. Rasmussen and A. Tamagawa, *A finiteness conjecture on abelian varieties with constrained prime power torsion*, Math. Res. Lett. **15** (2008), no. 6, 1223–1231.

[Sil86] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.