Mathematical Research Letters **11**, 529–538 (2004)

ON THE FIELDS OF 2-POWER TORSION OF CERTAIN ELLIPTIC CURVES

C. Rasmussen

Abstract. Let μ_{2^∞} denote the group of 2-power roots of unity. The outer pro-2 Galois representation on the projective line minus three points has a kernel whose fixed field, Ω_2, is a pro-2 extension of $\mathbb{Q}(\mu_{2^\infty})$, unramified away from 2. The fields of 2-power torsion of elliptic curves defined over $\mathbb{Q}$ possessing good reduction away from 2 are also pro-2 extensions of $\mathbb{Q}(\mu_{2^\infty})$, unramified away from 2. In this paper, we show that these fields are contained in Ω_2. An analogous result is shown for a certain family of elliptic curves defined over $\mathbb{Q}(\mu_{2^\infty})$.

1. Introduction

For a geometrically connected $\mathbb{Q}$-scheme X, the algebraic fundamental group is given by $\pi_1(X) := \varprojlim \mathrm{Aut}_X(X_i)$, where the $\{X_i\}$ are a collection of finite étale Galois coverings of X (see [4] for details). Hence, each element of $\pi_1(X)$ is a consistent choice of X-automorphisms of the X_i, and such an element in fact determines an X-automorphism of *any* finite étale covering of X. Conversely, any deck transformation τ of a covering $Z \to X$ can be lifted to an element $\tilde{\tau} \in \pi_1(X)$. Let ℓ be a fixed prime number. We may define, similarly, the pro-ℓ fundamental group, $\pi_1^\ell(X)$, by restricting to only those Galois étale coverings of X which have degree a power of ℓ.

In the case X is a curve defined over $k \subseteq \bar{\mathbb{Q}}$, the natural correspondence between morphisms of curves and extensions of function fields provides an alternative description for the fundamental group; $\pi_1(X)$ is isomorphic to $\mathrm{Gal}\big(K(X)^{\mathrm{unr}}/K(X)\big)$, where $K(X)^{\mathrm{unr}}$ is the maximal unramified extension of $K(X)$. Similarly,

$$\pi_1^\ell(X) \cong \mathrm{Gal}\left(K(X)^{\mathrm{unr,\ pro}-\ell}/K(X)\right), \tag{1}$$

where $K(X)^{\mathrm{unr,\ pro}-\ell}$ denotes the maximal pro-ℓ unramified extension of $K(X)$.

Now consider the case where $X = \mathbb{P}^1_{\mathbb{Q}} \smallsetminus \{0, 1, \infty\}$, and let $\bar{X} = X \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}$. In this case, the pro-$\ell$ fundamental group of $\bar{X}$ is isomorphic to $\mathrm{Gal}\big(M/\bar{\mathbb{Q}}(t)\big)$, where M is the maximal pro-ℓ extension of $\mathbb{Q}(t)$ unramified away from $t = 0, 1, \infty$. There

Received April 19, 2003.

is an exact sequence of Galois groups

(2)

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{Gal}\big(M/\bar{\mathbb{Q}}(t)\big) \arrow[r] & \mathrm{Gal}\big(M/\mathbb{Q}(t)\big) \arrow[r] & \mathrm{Gal}\big(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t)\big) \arrow[r] & 1 \, , \\ & \pi_1^{\ell}\left(\bar{X}\right) \arrow[u, "\cong"'] & & \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \arrow[u, "\cong"'] & \end{tikzcd}$$

which determines an associated Galois representation

$$\rho_\ell \colon \mathrm{Gal}\left(\bar{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{Out}\left(\pi_1^{\ell}(\bar{X})\right). \tag{3}$$

The action of ρ_ℓ is given as follows. For any $\sigma \in \mathrm{Gal}\left(\bar{\mathbb{Q}}/\mathbb{Q}\right)$, we may choose a lift $\tilde{\sigma} \in \mathrm{Gal}\big(M/\mathbb{Q}(t)\big)$.Thenconjugation by $\tilde{\sigma}$ is an automorphism of $\mathrm{Gal}\big(M/\bar{\mathbb{Q}}(t)\big)$, which is well-defined up to the choice of $\tilde{\sigma}$. But $\tilde{\sigma}$ is defined up to elements of $\mathrm{Gal}\big(M/\bar{\mathbb{Q}}(t)\big)$, and so this action is defined up to inner automorphism. This is the action of ρ_ℓ.

The kernel of ρ_ℓ is a normal subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and we denote its fixed field by Ω_ℓ. Anderson and Ihara have demonstrated that Ω_ℓ is the field generated by the "higher circular ℓ-units" [1]. It is a pro-ℓ extension of $\mathbb{Q}\left(\mu_{\ell^\infty}\right)$, unramified outside of ℓ. Ihara has asked if Ω_ℓ is the maximal such extension [3].

In this article, we consider specifically the case $\ell = 2$. If Ihara's question has an affirmative answer, then any pro-2 extension of $\mathbb{Q}\left(\mu_{2^\infty}\right)$, unramified away from 2, will appear as a subfield of Ω_2. Such fields occur quite naturally. Let E be an elliptic curve defined over $\mathbb{Q}$, with good reduction away from 2, satisfying

$$\mathbb{Q}\left(E[2]\right) \subseteq \mathbb{Q}\left(\mu_{2^\infty}\right). \tag{4}$$

Then $\mathbb{Q}\left(E[2^\infty]\right)$ is a pro-2 extension of $\mathbb{Q}\left(\mu_{2^\infty}\right)$ unramified away from 2. In fact, equation (4) holds for all 24 elliptic curves over $\mathbb{Q}$ with good reduction away from 2. Our main result is the following.

Theorem 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve with good reduction away from* 2*. Then $\mathbb{Q}\left(E[2^\infty]\right) \subseteq \Omega_2$.*

The key to the proof is to demonstrate these elliptic curves provide 2-covers for $\bar{X}$. We say a morphism $f \colon Y \to Z$ is an **ℓ-cover** of Z if f is unramified and the Galois closure of f has degree a power of ℓ. In particular, an ℓ-cover is not assumed to be Galois itself. For convenience, we will also call a morphism $\varphi \colon C \to \mathbb{P}^1$ an ℓ-cover of $\bar{X}$ if φ can be restricted to an ℓ-cover of $\bar{X}$.

Once a 2-cover $g_0 \colon E \to \mathbb{P}^1$ of $\bar{X}$ has been constructed, one may demonstrate that a Galois element σ cannot act trivially through ρ_2 while acting non-trivially on $E[2^\infty]$. This implies the containment $\mathbb{Q}(E[2^\infty]) \subseteq \Omega_2$.

In §2, we will assume the existence of g_0 and give the proof of Theorem 1.1. In §3, we will demonstrate the construction of g_0 for each of the elliptic curves in question. In §4 we will extend the result, by demonstrating an infinite family of elliptic curves which provide 2-covers of $\bar{X}$, and which therefore satisfy $\mathbb{Q}(E[2^\infty]) \subseteq \ \Omega_2$.

2. Proof of Theorem 1.1

We begin the proof of Theorem 1.1 with the following lemma. Let ζ_8 be a primitive 8th root of unity.

Lemma 2.1. *Let $E/\mathbb{Q}$ be an elliptic curve with good reduction outside 2. Then*

1. *E has a minimal model of the form $y^2 = (x - e_1)(x - e_2)(x - e_3)$, with $e_1 \in \mathbb{Z}$, $e_2, e_3 \in \mathbb{Z}[\zeta_8]$,*
2. *$\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(\zeta_8)$,*
3. *E has a point R of exact order 4 which is Ω_2-rational.*

Proof. The work is entirely by computation. The only nontrivial calculation is in the construction of R. To demonstrate R is Ω_2-rational, we use the description of Ω_2 as the higher circular 2-units. Anderson and Ihara have shown ([1, §2]) that Ω_2 is generated by the sets $f^{-1}(\{0, 1, \infty\})$ of ramification of all *elementary* 2-covers $f\colon \mathbb{P}^1 \to \mathbb{P}^1$ of $\bar{X}$. For example, to demonstrate the membership

$$\theta = \sqrt{1 - i} \in \Omega_2, \tag{5}$$

we note $\theta \mapsto 1$ under the elementary 2-cover $\mathbb{P}^1 \to \mathbb{P}^1$ of $\bar{X}$ given by $x \mapsto (x^2-1)^4$.

Table 1 demonstrates the results for all 24 elliptic curves over $\mathbb{Q}$ with good reduction away from 2, as enumerated in Cremona's tables [2]. The first column gives the designation and equation for the elliptic curve, and the second column gives the field generated by the 2-torsion of E. The third column gives a rational point P of E of exact order 2 (hence, determining e_1), and the fourth column gives a point R, of exact order 4, rational over Ω_2. □

Before proceeding to the proof of Theorem 1.1, we prove the following lemma.

Lemma 2.2. *Suppose $g_0\colon E \to \mathbb{P}^1$ is a 2-cover of $\bar{X}$, defined over $\mathbb{Q}(\mu_{2^\infty})$. Then for any $n \geq 1$, the morphism $g_n := g_0 \circ [2^n]$ is also a 2-cover of $\bar{X}$, defined over $\mathbb{Q}(\mu_{2^\infty})$.*

Proof. Let $\bar{\mathbb{Q}}(t) \hookrightarrow K_1$ be the inclusion of function fields corresponding to g_0. Let $\tilde{K}_1/K_1$ be the extension corresponding to the morphism $[2^n]$. Let L be the Galois closure of $K_1/\bar{\mathbb{Q}}(t)$, and let $\tilde{L}$ be the Galois closure of $\tilde{K}_1/\bar{\mathbb{Q}}(t)$. We must show that $[\tilde{L} : \bar{\mathbb{Q}}(t)]$ is a power of 2.

Let $\tilde{K}_2, \ldots, \tilde{K}_s$ be the Galois conjugates of $\tilde{K}_1$ in $\tilde{L}$. Since $\tilde{K}_1/K_1$ is Galois, there are corresponding Galois extensions $\tilde{K}_i/K_i$, for each i, within $\tilde{L}$. Because $L/\bar{\mathbb{Q}}(t)$ is Galois of degree a power of 2, and each of the K_i appear within L, it follows that L/K_i is Galois with degree a power of 2 also. Hence for each i, the Galois extensions $\tilde{K}_i/K_i$ and L/K_i form a compositum $L\tilde{K}_i/K_i$ which is Galois and whose degree must also be a power of 2.

Further, each $L\tilde{K}_i$ contains $\tilde{K}_i$, and so the compositum of the $L\tilde{K}_i$ must contain $\tilde{L}$. But the compositum of the Galois extensions $L\tilde{K}_i/\bar{\mathbb{Q}}(t)$ must have a degree dividing the product of the degrees of the extensions. Hence this compositum, as well as the sub-extension $\tilde{L}$, has degree a power of 2 over $\bar{\mathbb{Q}}(t)$.

TABLE 1. Data for the Proof of Lemma 2.1

Let $u = -1 + \sqrt{2}$, $\beta = 1 + i$, and let ζ be a primitive 8th root of unity.

E	$\mathbb{Q}(E[2])$	$P \in E[2]$	$R \in E[4]$
32A1 : $y^2 = x^3 + 4x$	$\mathbb{Q}(\sqrt{-2})$	$(0,0)$	$(2,4)$
32A2 : $y^2 = x^3 - x$	$\mathbb{Q}$	$(0,0)$	$(i, 2\beta^{-1})$
32A3 : $y^2 = x^3 - 11x - 14$	$\mathbb{Q}(\sqrt{2})$	$(-2,0)$	$(-1, 2i)$
32A4 : $y^2 = x^3 - 11x + 14$	$\mathbb{Q}(\sqrt{2})$	$(2,0)$	$(1,2)$
64A1 : $y^2 = x^3 - 4x$	$\mathbb{Q}$	$(0,0)$	$(2i, 2^{5/2}\beta^{-1})$
64A2 : $y^2 = x^3 - 44x - 112$	$\mathbb{Q}(\sqrt{2})$	$(-4,0)$	$(-6, 8i)$
64A3 : $y^2 = x^3 - 44x + 112$	$\mathbb{Q}(\sqrt{2})$	$(4,0)$	$(6,8)$
64A4 : $y^2 = x^3 + x$	$\mathbb{Q}(i)$	$(0,0)$	$(1, 2^{1/2})$
128A1 : $y^2 = x^3 + x^2 + x + 1$	$\mathbb{Q}(i)$	$(-1,0)$	$(u, 2u^{1/2})$
128A2 : $y^2 = x^3 + x^2 - 9x + 7$	$\mathbb{Q}(\sqrt{2})$	$(1,0)$	$(1+2i, 4i\beta^{1/2})$
128B1 : $y^2 = x^3 + x^2 + 3x - 5$	$\mathbb{Q}(\sqrt{-2})$	$(1,0)$	$(1+2\sqrt{2}, 2^{5/2}u^{-1/2})$
128B2 : $y^2 = x^3 + x^2 - 2x - 2$	$\mathbb{Q}(\sqrt{2})$	$(-1,0)$	$(-2\beta^{-1}, 2\beta^{-1/2})$
128C1 : $y^2 = x^3 - x^2 + x - 1$	$\mathbb{Q}(i)$	$(1,0)$	$(u^{-1}, 2u^{-1/2})$
128C2 : $y^2 = x^3 - x^2 - 9x - 7$	$\mathbb{Q}(\sqrt{2})$	$(-1,0)$	$(-1+2i, 2^{5/2}\beta^{-1/2})$
128D1 : $y^2 = x^3 - x^2 + 3x + 5$	$\mathbb{Q}(\sqrt{-2})$	$(-1,0)$	$(-1+2\sqrt{2}, 2^{5/2}u^{1/2})$
128D2 : $y^2 = x^3 - x^2 - 2x + 2$	$\mathbb{Q}(\sqrt{2})$	$(1,0)$	$(\beta, i2^{1/2}\beta^{1/2})$
256A1 : $y^2 = x^3 + x^2 - 3x + 1$	$\mathbb{Q}(\sqrt{2})$	$(1,0)$	$(u^{-1}, 2^{5/4}u^{-1/2})$
256A2 : $y^2 = x^3 + x^2 - 13x - 21$	$\mathbb{Q}(\sqrt{2})$	$(-3,0)$	$(-u^2, i2^{11/4}u^{1/2})$
256B1 : $y^2 = x^3 - 2x$	$\mathbb{Q}(\sqrt{2})$	$(0,0)$	$(i2^{1/2}, \zeta^3 2^{5/4})$
256B2 : $y^2 = x^3 + 8x$	$\mathbb{Q}(\sqrt{-2})$	$(0,0)$	$(2^{3/2}, 2^{11/4})$
256C1 : $y^2 = x^3 + 2x$	$\mathbb{Q}(\sqrt{-2})$	$(0,0)$	$(2^{1/2}, 2^{5/4})$
256C2 : $y^2 = x^3 - 8x$	$\mathbb{Q}(\sqrt{2})$	$(0,0)$	$(i2^{3/2}, \zeta^3 2^{11/4})$
256D1 : $y^2 = x^3 - x^2 - 3x - 1$	$\mathbb{Q}(\sqrt{2})$	$(-1,0)$	$(u, i2^{5/4}u^{1/2})$
256D2 : $y^2 = x^3 - x^2 - 13x + 21$	$\mathbb{Q}(\sqrt{2})$	$(3,0)$	$(u^{-2}, 2^{11/4}u^{-1/2})$

Finally, we note that for an elliptic curve E defined over $\mathbb{Q}$, the morphism $[2]$ is also defined over $\mathbb{Q}$. Hence, the morphism g_n is defined over $\mathbb{Q}(\mu_{2^\infty})$ if g_0 is. $\square$

In the next section, we will construct a 2-cover $g_0 \colon E \to \mathbb{P}^1$ of $\bar{X}$, defined over $\mathbb{Q}(\mu_{2^\infty})$, for each of the 24 curves. The following proposition finishes the proof of Theorem 1.1. See also [1, Prop. 3.8.1] for a more general result regarding when the Jacobian of a curve appearing as an ℓ-cover of $\bar{X}$ has ℓ-power torsion rational over Ω_ℓ.

Proposition 2.3. *Let $E/\mathbb{Q}$ be an elliptic curve with good reduction away from 2. Suppose there exists $g_0 \colon E \to \mathbb{P}^1$, a 2-cover of $\bar{X}$, defined over $\mathbb{Q}(\mu_{2^\infty})$. Let $\sigma \in \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be such that σ acts non-trivially on $E[2^\infty]$. Then $\sigma \notin \ker \rho_2$.*

Proof. By assumption, there exists $n \geq 1$ and $P \in E[2^n]$ such that $P^\sigma \neq P$. We have demonstrated above that the morphism $g_n \colon E \to \mathbb{P}^1$ is a 2-cover of $\bar{X}$, defined over $\mathbb{Q}\big(\mu_{2^\infty}\big)$. Let C be the Galois closure of (E, g_n). Let t_P denote the deck transformation of g_n given by translation-by-P. It is an $\bar{X}$-automorphism of (E, g_n), and necessarily extends to some $\bar{X}$-automorphism $\tilde{t}_P$ of C.

If σ does not fix $\mathbb{Q}\big(\mu_{2^\infty}\big)$, then σ cannot fix Ω_2, and so $\sigma \notin \ker \rho_2$. Hence, we may assume σ fixes $\mathbb{Q}\big(\mu_{2^\infty}\big)$, and so $g_n^\sigma = g_n$. Let $\bar{\mathbb{Q}}(t, y)$ be the function field of (E, g_n). We choose a lift $\tilde{\sigma} \in \mathrm{Gal}\big(M/\mathbb{Q}(t)\big)$ such that under $\tilde{\sigma}$, $t \mapsto t$ and $y \mapsto y$. Suppose that $\sigma \in \ker \rho_2$. Then there exists $\varphi \in \pi_1^2(\bar{X})$ such that for every $\eta \in \pi_1^2(\bar{X})$,

$$\rho(\sigma)(\eta) = \eta^{\tilde{\sigma}} = \varphi\eta\varphi^{-1}. \tag{6}$$

That is to say, $\tilde{\sigma}$ must act as some inner automorphism of $\pi_1^2(\bar{X}) \cong \mathrm{Gal}\left(M/\bar{\mathbb{Q}}(t)\right)$. Further, this equality holds for deck transformations of C; in particular, it holds for $\tilde{t}_P$.

Lemma 2.4. *Under these assumptions, $\varphi(E) = E$.*

Proof. To see this, let $\tau \in \mathrm{Gal}(C/E)$. We also denote by τ its lift to an element of $\mathrm{Gal}\big(M/\bar{\mathbb{Q}}(t)\big)$. Our choice of $\tilde{\sigma}$ satisfies $\tilde{\sigma}^{-1}\left(\bar{\mathbb{Q}}(E)\right) \subseteq \bar{\mathbb{Q}}(E)$, as $\tilde{\sigma}$ fixes t and y. Hence, $\tilde{\sigma}^{-1}(s) \in \bar{\mathbb{Q}}(E)$ for any $s \in \bar{\mathbb{Q}}(E)$, and so $\tilde{\sigma}^{-1}(s)$ is necessarily fixed by τ. Then

$$\begin{aligned} \tau\left(\varphi^{-1}(s)\right) &= \varphi^{-1}\left(\varphi\left(\tau\left(\varphi^{-1}(s)\right)\right)\right) \\ &= \varphi^{-1}\left(\tilde{\sigma}\left(\tau\left(\tilde{\sigma}^{-1}(s)\right)\right)\right) \\ &= \varphi^{-1}\left(\tilde{\sigma}\left(\tilde{\sigma}^{-1}(s)\right)\right) = \varphi^{-1}(s). \end{aligned} \tag{7}$$

So $\varphi^{-1}(s)$ is fixed by all $\tau \in \mathrm{Gal}(C/E)$. Hence, $\varphi^{-1}(s) \in \bar{\mathbb{Q}}(E)$ for every $s \in \bar{\mathbb{Q}}(E)$, and so $\varphi(E) = E$. $\square$

In particular, for $\tilde{t}_P$ we have $\tilde{t}_P^{\tilde{\sigma}} = \varphi\tilde{t}_P\varphi^{-1}$. Since $\tilde{\sigma}(E) = E$,

$$\begin{aligned} \tilde{t}_P^{\tilde{\sigma}}\big|_E &= \tilde{\sigma} \circ \tilde{t}_P \circ \tilde{\sigma}^{-1}\big|_E \\ &= \tilde{\sigma} \circ \tilde{t}_P\big|_E \circ \tilde{\sigma}^{-1}\big|_E = \tilde{\sigma} t_P \tilde{\sigma}^{-1}\big|_E . \end{aligned} \tag{8}$$

Similarly, $\varphi\tilde{t}_P\varphi^{-1}\big|_E = \varphi t_P\varphi^{-1}\big|_E$. Hence, the action of $\tilde{\sigma}$ on $\tilde{t}_P$ descends, and we know that on E,

$$t_P^{\tilde{\sigma}} = \varphi t_P \varphi^{-1}. \tag{9}$$

Then φ cannot be the identity morphism on E, since for an arbitrary $T \in E$,

$$\begin{aligned} t_P^{\tilde{\sigma}}(T) &= \tilde{\sigma}\left(t_P\left(\tilde{\sigma}^{-1}(T)\right)\right) = t_P(T^{\sigma^{-1}})^{\sigma} \\ &= (P + T^{\sigma^{-1}})^{\sigma} = P^{\sigma} + T \neq P + T = t_P(T). \end{aligned} \tag{10}$$

So $\varphi|_E$ is a nontrivial $\bar{X}$-automorphism of E. But *any* curve automorphism of E must be a composition of a translation and a group isomorphism, so we may write $\varphi = t_Q \circ \varphi'$. One quickly sees that $\varphi t_P \varphi^{-1} = \varphi' t_P \varphi'^{-1}$, and so without loss of generality, we may assume that φ is a group isomorphism of E.

However, φ also represents an element of $\mathrm{Gal}(E/\bar{X})$, which by assumption has order a power of 2. So as an element of $\mathrm{Aut}(E)$, φ must have order a power of 2. Since we are in characteristic 0, the only possibilities are that φ or φ^2 is the automorphism $-1 \in \mathrm{Aut}(E)$ ([6, pg. 103]). We consider the two possible cases.

Case I: $\varphi = -1$. In this case, we note

$$P^\sigma = \sigma t_P \sigma^{-1}(O) = \varphi t_P \varphi^{-1}(O) = \varphi(P) = -P. \tag{11}$$

But this must hold for any $P \in E[2^\infty]$ not fixed by σ. Hence, $P^\sigma = \pm P$ for every $P \in E[2^\infty]$. However, this is only possible if $P^\sigma = -P$ for every P, or if σ acts trivially on $E[2^\infty]$. Indeed, if $P, Q \in E[2^\infty] \smallsetminus E[2]$ are such that $P^\sigma = P, Q^\sigma = -Q$, then $(P+Q)^\sigma \neq \pm(P+Q)$.

Since σ does not fix all of $E[2^\infty]$, we know $P^\sigma = -P$ for every $P \in E[2^\infty]$. But by Lemma 2.1, there is an $R \in E[4]$ rational over Ω_2, and so $R^\sigma = R$! This is a contradiction, and so $\sigma \notin \ker \rho_2$.

Case II: $\varphi^2 = -1$. In this case, φ is given by

$$(x, y) \mapsto (\zeta^2 x, \zeta^3 y), \qquad \zeta \in \mu_4. \tag{12}$$

Since σ fixes Ω_2, $\zeta^\sigma = \zeta$, and so φ and σ commute in their action on the points of E. As in Case I, we see that $P^\sigma = \varphi(P)$ for every $P \in E[2^\infty]$ not fixed by σ. Hence, $P^{\sigma^2} = \varphi^2(P) = -P$ or $P^{\sigma^2} = P$ for every $P \in E[2^\infty]$. It follows that σ^2 must act as -1 on all of $E[2^\infty]$. The existence of $R \in E[4]$ fixed by σ^2 again provides a contradiction, and so $\sigma \notin \ker \rho_2$. □

Corollary 2.5. *For every elliptic curve $E/\mathbb{Q}$ which has good reduction away from 2, $\mathbb{Q}(E[2^\infty]) \subseteq \Omega_2$.*

Proof. Proposition 2.3 shows that if σ does not fix $\mathbb{Q}(E[2^\infty])$, then σ does not fix Ω_2. This is equivalent to saying that every σ fixing Ω_2 also fixes $\mathbb{Q}(E[2^\infty])$, or equivalently, that $\mathbb{Q}(E[2^\infty]) \subseteq \Omega_2$. □

3. Construction of the 2-Cover g_0

We now demonstrate that for each of the 24 elliptic curves $E/\mathbb{Q}$ with good reduction away from 2, there exists a 2-cover $g_0 \colon E \to \mathbb{P}^1$ of $\bar{X}$, defined over $\mathbb{Q}(\mu_{2^\infty})$. That is, we will construct a morphism $g_0 \colon E \to \mathbb{P}^1$, unramified away from $\{0, 1, \infty\}$, whose Galois closure has degree a power of 2. In fact, the cover g_0 that we construct will be a composition of degree 2 morphisms. In this case, the degree of the Galois closure will automatically be a power of 2. We remind the reader of the proof.

Lemma 3.1. *Let $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$ be a tower of quadratic field extensions. Then the Galois closure of K/F has degree a power of 2.*

Proof. We proceed by induction. The base case $n = 1$ is trivial. Suppose that the Galois closure of K_{n-1}/F, K_{n-1}^g, has degree a power of 2 over F. We label by $K_n = K_n^1, \dots, K_n^k$ the Galois conjugates of K_n. Each K_n^i contains a Galois conjugate of K_{n-1}, denoted K_{n-1}^i.

Since K_{n-1}^g and K_n^1 are both Galois over K_{n-1}, the compositum $K_n^1 K_{n-1}^g$ is Galois over K_{n-1} also, and has degree a power of 2 over K_{n-1}. But this compositum contains the field K_{n-1}^2, and so must be Galois and degree a power of 2 over K_{n-1}^2. Hence, the compositum $K_n^2 K_n^1 K_{n-1}^g$ is likewise Galois and degree a power of 2 over K_{n-1}^g. Continuing in this fashion, we see that the compositum $K_n^k \cdots K_n^1 K_{n-1}^g$ is Galois and has degree a power of 2 over K_{n-1}^g. But this compositum clearly contains all the Galois conjugates of K_n, and so also contains K_n^g, the Galois closure of K_n. Thus, the Galois closure of K_n also has degree a power of 2 over F. $\square$

We now set out to construct the covers g_0. We begin by selecting a degree 2 morphism $f\colon E \to \mathbb{P}^1$, which necessarily branches over a 4-point set. We will then use the arithmetic properties of E to prove that f may be extended by degree 2 morphisms $\mathbb{P}^1 \to \mathbb{P}^1$ that collapses the branching to the set $\{0, 1, \infty\}$.

Let E be one of the 24 elliptic curves over $\mathbb{Q}$ with good reduction away from 2. We note that $\mathbb{Q}(\zeta_8)$ has class number 1, and in its ring of integers, there is a unique prime ideal over 2, generated by $\pi = 1 - \zeta_8$. We will use the minimal model of E, together with the properties noted in Lemma 2.1, to construct g_0. We note the discriminant of E,

$$\Delta = 2^4(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2, \tag{13}$$

must have the form $\Delta = u \cdot \pi^k$, for some unit $u \in \mathbb{Z}[\zeta_8]^\times$. For any $\wp \nmid 2$, $v_\wp(\Delta) = 0$. Since the $e_i - e_j$ are all algebraic integers, it follows that $v_\wp(e_i - e_j) = 0$ also.

Now of the quantities $e_i - e_j$, any one can be written as a difference of the other two. Hence, at least two of the valuations $v_\pi(e_i - e_j)$ must be equal. Let us relabel the e_i such that

$$v_\pi(e_1 - e_2) = v_\pi(e_1 - e_3). \tag{14}$$

Now the morphism $f\colon E \to \mathbb{P}^1$ given by

$$f(x, y) = \frac{x - e_1}{e_2 - e_1} \tag{15}$$

has degree 2 and branches over the set $\{0, 1, \infty, \alpha\}$, where

$$\alpha = \frac{e_3 - e_1}{e_2 - e_1}. \tag{16}$$

By (14) and the reduction type of E, α has valuation 0 with respect to every prime ideal in $\mathbb{Q}(\zeta_8)$. Hence, α is a unit in the ring of integers of $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(\zeta_8)$. For 10 of the curves in the table, the field generated by $E[2]$ has a unit group with rank 0, and so α must be a root of unity. Those curves are 32A1, 32A2, 64A1, 64A4, 128A1, 128B1, 128C1, 128D1, 256B2, and 256C1. For any of these curves, then, the composition

$$g_0 = (x \mapsto x^{2^k}) \circ f, \qquad k \leq 2, \tag{17}$$

gives a morphism $g_0\colon E \to \mathbb{P}^1$, ramified only over $\{0,1,\infty\}$, which is a composition of degree 2 morphisms. This is a 2-cover of $\bar{X}$, defined over $\mathbb{Q}$.

The remaining curves have 2-torsion which generates a field with a unit group of positive rank. However, for two of these curves, 256B1 and 256C2, computation shows $\alpha = -1$, and so the morphism $g_0 = (x \mapsto x^2) \circ f$ provides a 2-cover $E \to \mathbb{P}^1$ of $\bar{X}$, defined over $\mathbb{Q}$.

For the eight curves 128A2, 128B2, 128C2, 128D2, 256A1, 256A2, 256D1, and 256D2, computation reveals $\alpha = \pm u^2$, where u is a unit which generates the torsion-free part of the unit group of $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{2})$. Hence, the morphism $\frac{1}{u} \cdot f$ ramifies over the set $\{0, \infty, \frac{1}{u}, u\}$ or $\{0, \infty, \frac{1}{u}, -u\}$, where $u = 1 + \sqrt{2}$ or $u = -1 + \sqrt{2}$. We note the following degree 2 morphisms are unramified:

$$
\begin{aligned}
&A_1\colon \mathbb{P}^1 \smallsetminus \{0,\infty,\pm 1+\sqrt{2}\} \longrightarrow \mathbb{P}^1 \smallsetminus \{0,1,2,\infty\} && x \mapsto (x-\sqrt{2})^2\\
&A_2\colon \mathbb{P}^1 \smallsetminus \{0,\infty,\pm 1-\sqrt{2}\} \longrightarrow \mathbb{P}^1 \smallsetminus \{0,1,2,\infty\} && x \mapsto (x+\sqrt{2})^2\\
&A_3\colon \mathbb{P}^1 \smallsetminus \{0,\infty,-1\pm\sqrt{2}\} \longrightarrow \mathbb{P}^1 \smallsetminus \{0,1,2,\infty\} && x \mapsto (x+1)^2\\
&A_4\colon \mathbb{P}^1 \smallsetminus \{0,\infty,\ \ 1\pm\sqrt{2}\} \longrightarrow \mathbb{P}^1 \smallsetminus \{0,1,2,\infty\} && x \mapsto (x-1)^2\\
&B\colon \mathbb{P}^1 \smallsetminus \{0,1,2,\infty\} \longrightarrow \mathbb{P}^1 \smallsetminus \{0,1,\infty\} && x \mapsto 2x-x^2
\end{aligned}
\tag{18}
$$

Hence, for these eight curves, a composition of the form $B \circ A_i \circ \frac{1}{u} f$ gives a 2-cover $g_0\colon E \to \mathbb{P}^1$ of $\bar{X}$, defined over $\mathbb{Q}(\zeta_8)$.

Unfortunately, for the remaining four curves, the unit α is the fourth power of a fundamental unit in $\mathbb{Q}(\sqrt{2})$, and the author could not find a composition of degree 2 morphisms that could extend f to an appropriate 2-cover in these cases. However, the situation is quickly remedied by considering a different morphism $E \to \mathbb{P}^1$ to start. The morphism $h\colon E \to \mathbb{P}^1$ given by

$$h(x,y) = \frac{y}{x-e_1} \tag{19}$$

is of degree 2. One calculates its branch set to be $\{\delta_2 \pm \delta_3, -\delta_2 \pm \delta_3\}$, where

$$\delta_i = \sqrt{e_1 - e_i}. \tag{20}$$

For the four remaining curves, 32A3, 32A4, 64A2, 64A3, one sees that δ_2, δ_3 are algebraic integers in $\mathbb{Q}(\zeta_8)$, and for these curves, the set of branch points of h has the form $\{\pm\gamma, \pm\gamma\sqrt{2}\}$, for some $\gamma \in \mathbb{Q}(\zeta_8)$. Hence, the composition

$$g_0 = B \circ (x \mapsto x^2) \circ \frac{1}{\gamma} h \tag{21}$$

gives a 2-cover $g_0\colon E \to \mathbb{P}^1$ of $\bar{X}$, defined over $\mathbb{Q}(\zeta_8)$. This completes the construction of g_0 for each of the 24 elliptic curves, and we conclude the following.

Proposition 3.2. *For every elliptic curve $E/\mathbb{Q}$ with good reduction away from 2, there exists a 2-cover $g_0\colon E \to \mathbb{P}^1$ of $\bar{X}$, defined over $\mathbb{Q}(\mu_{2^\infty})$.*

4. Curves Over $\mathbb{Q}(\mu_{2^\infty})$

We finish this article with an extension of the main theorem, and an example of an infinite family of elliptic curves defined over $\mathbb{Q}(\mu_{2^\infty})$ whose 2-power torsion is Ω_2-rational.

Theorem 4.1. *Let ζ be a primitive 2^n-th root of unity, and suppose that E is an elliptic curve defined over $\mathbb{Q}(\zeta)$, with a minimal model of the form*

$$y^2 = (x - e_1)(x - e_2)(x - e_3), \qquad e_i \in \mathbb{Z}[\zeta]. \tag{22}$$

Further, suppose that E has good reduction away from $(\pi) = (1-\zeta)$, and that E possesses a point R of exact order 4 which is Ω_2-rational. If there exists a 2-cover $g_0 \colon E \to \mathbb{P}^1$ of $\bar{X}$, defined over $\mathbb{Q}\big(\mu_{2^\infty}\big)$, then $\mathbb{Q}\left(E[2^\infty]\right) \subseteq \Omega_2$.

Proof. Under these hypotheses, we may follow the proof of Theorem 1.1 directly, and so $\mathbb{Q}(E[2^\infty]) \subseteq \Omega_2$. □

Now, for any 2^n-th root of unity ζ, let E_ζ be the elliptic curve given by

$$y^2 = x(x+\zeta)(x-\pi), \qquad \pi = 1 - \zeta. \tag{23}$$

We check with Tate's algorithm (see [5] or [7]) that this equation gives a global minimal model for E_ζ over $\mathbb{Q}(\zeta)$. The discriminant is $\Delta = 16\zeta^2\pi^2$, and so E_ζ has good reduction away from (π). Let η be a root of unity satisfying $\zeta = \eta^2$. Then the point $R = \big(\eta - \eta^2, i(\eta - \eta^2)\big)$ has exact order 4, and clearly is rational over Ω_2. We note that $f \colon E \to \mathbb{P}^1$, given by $f(x,y) = x + \zeta$, branches over the set $\{0, 1, \infty, \zeta\}$, and so

$$g_0 = (x \mapsto x^{2^n}) \circ f \tag{24}$$

gives a 2-cover $E \to \mathbb{P}^1$ of $\bar{X}$, defined over $\mathbb{Q}\big(\mu_{2^\infty}\big)$. Applying Theorem 4.1, we have $\mathbb{Q}\left(E_\zeta[2^\infty]\right) \subseteq \Omega_2$.

Acknowledgments

I am very grateful to the referee for their close reading and valuable suggestions. I wish to thank my advisor, Minhyong Kim, for his supervision on this research, and Bill McCallum for many helpful conversations. This research was supported by the University of Arizona's NSF VIGRE Grant #9977116.

References

[1] G. Anderson and Y. Ihara, *Pro-ℓ branched coverings of $\mathbb{P}^1$ and higher circular ℓ-units*, Annals of Mathematics, **128** (1988), 271–293.

[2] J. Cremona, *Elliptic curve data*, Table 1. URL: `http://www.maths.nottingham.ac.uk/personal/jec/ftp/data/INDEX.html`

[3] Y. Ihara, *Braids, Galois groups, and some arithmetic functions*, Proceedings of the International Congress of Mathematicians, Kyoto, Japan, (1990), 99–120.

[4] J. Milne, *Étale cohomology*, Princeton University Press, Princeton, 1980.

[5] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, 1994.

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

[7] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in Modular functions of one variable, IV, Lecture Notes in Math., **476**, B. Birch and W. Kyuk eds., Springer, Berlin, (1875), 33–52.

University of Arizona, Department of Mathematics, 617 North Santa Rita, Tucson AZ, 85721, USA

E-mail address: chras@math.arizona.edu