

ON ELLIPTIC CURVES WITH AN ISOGENY OF DEGREE 7

R. GREENBERG, K. RUBIN, AND A. SILVERBERG

ABSTRACT. We have two principal objectives in this paper. First of all, under mild assumptions on the field k , we prove the existence of elliptic curves E over k with a k -rational isogeny of degree 7 and any specified Galois action on the kernel of the isogeny. We give a parametric description of such curves. Secondly, we consider the specific case where $k = \mathbf{Q}$. If E is an elliptic curve over \mathbf{Q} with a \mathbf{Q} -rational isogeny of degree 7, we show that the image of $G_{\mathbf{Q}}$ in $\text{Aut}_{\mathbf{Z}_7}(T_7(E))$ is almost always as large as allowed by the isogeny. The exceptions correspond to the rational points on a certain curve of genus 12. By the method of Chabauty, we show that there are at most four possible j -invariants for the exceptional elliptic curves, two of which correspond to elliptic curves with complex multiplication by $\mathbf{Q}(\sqrt{-7})$.

1. INTRODUCTION

Fix a rational prime p , and a field k of characteristic different from p . Suppose that E is an elliptic curve defined over k , and that E has an isogeny of degree p that is also defined over k . Then the kernel of the isogeny is a k -rational subgroup Ψ of $E(k^s)$ of order p , where k^s denotes a fixed separable closure of k . Let $G_k = \text{Gal}(k^s/k)$. Since $\text{Aut}(\Psi) \cong \mathbf{F}_p^\times$, the action of G_k on Ψ is given by a homomorphism $\psi : G_k \rightarrow \mathbf{F}_p^\times$. We refer to ψ as the *character* of the isogeny. For example, the character ψ is trivial if and only if $\Psi \subset E(k)$.

Suppose now that $p = 7$, and let $\psi : G_k \rightarrow \mathbf{F}_7^\times$ be a fixed homomorphism. One of the objectives of this paper is to describe all elliptic curves defined over k that have a k -isogeny of degree 7 and character ψ . We will give explicit formulas for a family of elliptic curves $\{A_v\}$, where v varies over an explicit Zariski open subset of the projective line $\mathbf{P}^1(k)$, such that

- for every v , the elliptic curve A_v has a k -isogeny of degree 7 and character ψ ,
- if E is an elliptic curve over k with a k -isogeny of degree 7 and character ψ , then E is isomorphic over k to A_v for some v .

See Theorems 3.2 and 3.6 for a more precise statement. One consequence of this explicit description is that if $k \neq \mathbf{F}_2$, and if ψ is any character, then there is an elliptic curve over k that has a k -isogeny of degree 7 with character ψ (see Corollary 3.8).

The method of our construction is as follows. When $\psi = 1$, we are parametrizing elliptic curves with a point of order 7, so the A_v are the fibers of the universal elliptic curve \mathcal{E}_1 over the modular curve $X_1(7)$ of genus zero (see §2). For general ψ , in §3 we twist the elliptic surface \mathcal{E}_1 to obtain the appropriate elliptic surface \mathcal{E}_ψ , and then the A_v are the fibers of \mathcal{E}_ψ .

The authors thank the National Science Foundation for financial support.

The second objective of this paper concerns the special case where $k = \mathbf{Q}$. If E is an elliptic curve defined over \mathbf{Q} and p is any prime, let $T_p(E)$ denote the p -adic Tate module for E . There is then a natural homomorphism

$$\rho_{E,p} : G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}_{\mathbf{Z}_p}(T_p(E))$$

giving the action of $G_{\mathbf{Q}}$ on $T_p(E)$. Since $T_p(E)$ is a free \mathbf{Z}_p -module of rank 2, $\mathrm{Aut}_{\mathbf{Z}_p}(T_p(E))$ can be identified (non-canonically) with $GL_2(\mathbf{Z}_p)$. If E has a \mathbf{Q} -isogeny of degree p , then $\rho_{E,p}$ cannot be surjective. The isogeny and the corresponding character $\psi : G_{\mathbf{Q}} \rightarrow \mathbf{F}_p^\times$ put an obvious constraint on the image of $\rho_{E,p}$. If E has complex multiplication (CM), then that puts another constraint on the image of $\rho_{E,p}$. We wish to understand whether these are the only constraints, or equivalently, whether there are any non-CM elliptic curves over \mathbf{Q} for which the image of $\rho_{E,p}$ does not contain a Sylow pro- p subgroup of $\mathrm{Aut}_{\mathbf{Z}_p}(T_p(E))$. This is the motivation for the following definition.

Definition 1.1. We will say that a curve E over \mathbf{Q} is *p -exceptional* if E has an isogeny of degree p defined over \mathbf{Q} and the image of $\rho_{E,p}$ does *not* contain a Sylow pro- p subgroup of $\mathrm{Aut}_{\mathbf{Z}_p}(T_p(E))$.

When $p > 7$, the first author proved in [4] that the only p -exceptional curves are those with complex multiplication by $\mathbf{Q}(\sqrt{-p})$. In this paper we consider the case $p = 7$ and prove the following.

Theorem 1.2. *Let C_0 be the curve*

$$w^7 = (v^3 - 2v^2 - v + 1)/(v^3 - v^2 - 2v + 1)$$

and let $Z = \{(0, 1), (1, 1), (\infty, 1), (-1, -1), (2, -1), (1/2, -1)\} \subset C_0(\mathbf{Q})$. If $C_0(\mathbf{Q}) = Z$, then the only 7-exceptional curves are those with complex multiplication by $\mathbf{Q}(\sqrt{-7})$. If $C_0(\mathbf{Q}) \supsetneq Z$, then up to quadratic twist there are exactly 2 non-CM 7-exceptional curves.

See Theorem 6.10 for a more precise statement, including an explicit equation for the 7-exceptional curves E , given a point $(v, w) \in C_0(\mathbf{Q}) - Z$. Unfortunately we have not been able to rule out the existence of the pair of non-CM 7-exceptional curves in Theorem 1.2. However, by considering $C_0(\mathbf{Q}_7)$ we can show (Corollary 6.5) that if E is 7-exceptional, then $j(E) \equiv -15^3$ or $255^3 \pmod{49}$. The CM-elliptic curves of conductor 49 have j -invariants -15^3 and 255^3 .

The method of our proof of Theorem 1.2 is as follows. We begin with two results from [4]. Let $\omega : G_{\mathbf{Q}} \rightarrow \mathbf{F}_p^\times$ denote the character giving the action of $G_{\mathbf{Q}}$ on μ_p .

Theorem 1.3 ([4], Theorem 1). *Suppose $p \geq 7$ and E is an elliptic curve over \mathbf{Q} with a \mathbf{Q} -isogeny of degree p . Let ψ denote the character of the isogeny. If $\psi^4 \neq \omega^2$, then the image of $\rho_{E,p}$ contains a Sylow pro- p subgroup of $\mathrm{Aut}_{\mathbf{Z}_p}(T_p(E))$.*

Proposition 1.4 ([4], Remark 4.2.1). *Suppose $p > 7$ and E is an elliptic curve over \mathbf{Q} with a \mathbf{Q} -isogeny of degree p and character ψ . If $\psi^4 = \omega^2$, then E has CM.*

These two results combine to show that there are no non-CM p -exceptional curves when $p > 7$. Unfortunately, Proposition 1.4 fails when $p = 7$ (as can be seen by considering the family of elliptic curves with a \mathbf{Q} -isogeny of degree 7 and character $\psi = \omega^5$; see §4).

Suppose E is a 7-exceptional elliptic curve. By Theorem 1.3, if ψ is the character of the isogeny, then $\psi^4 = \omega^2$. It follows that the \mathbf{F}_7^\times -valued character $\psi\omega^{-5}$ has

order dividing 4, and hence dividing 2. Thus, replacing E by a quadratic twist if necessary, we may assume that $\psi = \omega^5$.

In §4 we describe in detail the family of elliptic curves over \mathbf{Q} with a \mathbf{Q} -isogeny of degree 7 and character $\psi = \omega^5$. In this special case we denote the family by $\{B_v\}$ instead of $\{A_v\}$. It follows that E is isomorphic over \mathbf{Q} to B_v for some $v \in \mathbf{Q}$. By studying the minimal discriminants of B_v and its 7-isogenous curve, we show in §5 and §6 that if E is 7-exceptional then $(v^3 - 2v^2 - v + 1)/(v^3 - v^2 - 2v + 1)$ must be a 7-th power, i.e., v corresponds to a rational point on the curve C_0 of Theorem 1.2. The points $Z \subset C_0(\mathbf{Q})$ correspond to the 2 curves of conductor 49 with CM by $\mathbf{Q}(\sqrt{-7})$, and any additional points in $C_0(\mathbf{Q})$ correspond to non-CM 7-exceptional curves.

To complete the proof, in §7 we use the method of Chabauty to show that $C_0(\mathbf{Q}) - Z$ has cardinality either 0 or 6, and in the latter case there are exactly 2 non-CM 7-exceptional curves, up to quadratic twist.

2. THE MODULAR CURVE $X_1(7)$

Fix a field k of characteristic different from 7.

Definition 2.1. If E, E' are elliptic curves over k , and $P \in E(k^s), P' \in E'(k^s)$ are points of order 7, we say that $\lambda : (E, P) \xrightarrow{\sim} (E', P')$ is an isomorphism if λ is an isomorphism from E to E' and $\lambda(P) = P'$. If such a λ exists, we say that (E, P) and (E', P') are isomorphic. If further $\lambda : E \xrightarrow{\sim} E'$ is defined over k , then we say that (E, P) and (E', P') are isomorphic over k .

Lemma 2.2. *Suppose E, E' are elliptic curves over k , $P \in E(k^s), P' \in E'(k^s)$ are points of order 7, and (E, P) is isomorphic to (E', P') .*

- (i) *The isomorphism $\lambda : (E, P) \xrightarrow{\sim} (E', P')$ is unique.*
- (ii) *Suppose that the groups Ψ and Ψ' generated by P and P' , respectively, are stable under G_k . Then (E, P) and (E', P') are isomorphic over k if and only if the two characters*

$$G_k \rightarrow \text{Aut}(\Psi) \xrightarrow{\sim} \mathbf{F}_7^\times, \quad G_k \rightarrow \text{Aut}(\Psi') \xrightarrow{\sim} \mathbf{F}_7^\times$$

are equal.

Proof. If $\lambda, \lambda' : (E, P) \xrightarrow{\sim} (E', P')$ are isomorphisms over k^s , then $\epsilon = \lambda^{-1} \circ \lambda'$ is an automorphism of E fixing P , i.e., $(\epsilon - 1)(P) = 0$. But then (viewing ϵ as a root of unity in an imaginary quadratic field) if $\epsilon \neq 1$ we have

$$7 \leq |\ker(\epsilon - 1)| = \deg(\epsilon - 1) = (\epsilon - 1)(\bar{\epsilon} - 1) = 2 - (\epsilon + \bar{\epsilon}) \leq 4$$

which is impossible. This proves (i).

For (ii), let ψ and ψ' be the characters giving the action of G_k on Ψ and Ψ' , respectively. If $\sigma \in G_k$, then $\lambda^\sigma : E \xrightarrow{\sim} E'$ is an isomorphism, and

$$\lambda^\sigma(P) = \lambda^\sigma(\psi^{-1}(\sigma)P^\sigma) = \psi^{-1}(\sigma)\lambda(P)^\sigma = \psi^{-1}(\sigma)(P')^\sigma = \psi^{-1}(\sigma)\psi'(\sigma)P'$$

If $\psi(\sigma) = \psi'(\sigma)$, then $\lambda^\sigma : (E, P) \xrightarrow{\sim} (E', P')$ is an isomorphism, so $\lambda^\sigma = \lambda$ by part (i). On the other hand, if $\psi(\sigma) \neq \psi'(\sigma)$, then $\lambda^\sigma(P) \neq \lambda(P)$, so $\lambda^\sigma \neq \lambda$. This proves (ii). \square

If $u \in k^s$, define a curve E_u over $k(u)$ by

$$(1) \quad E_u : y^2 - (u^2 - u - 1)xy - (u^3 - u^2)y = x^3 - (u^3 - u^2)x^2.$$

The discriminant of E_u is

$$(2) \quad \Delta(E_u) = u^7(u-1)^7(u^3 - 8u^2 + 5u + 1).$$

The next result is #15 in Table 3 on p. 217 of [7].

Theorem 2.3 ([7]). (i) *If $u \in k$ and $\Delta(E_u) \neq 0$, then E_u is an elliptic curve over k and $(0, 0)$ is a point of order 7 in $E(k)$.*
(ii) *If E is an elliptic curve over k and $P \in E(k)$ is a point of order 7 then there is a unique $u \in k$ such that (E, P) is isomorphic over k to $(E_u, (0, 0))$.*

Define a linear fractional transformation

$$(3) \quad \eta(v) = 1/(1-v).$$

The following lemma will be used in the proofs of Theorems 3.2 and 6.10 below.

Lemma 2.4. *Suppose $u \in k^s$ and $\Delta(E_u) \neq 0$. Then there is a unique isomorphism defined over $k(u)$:*

$$(E_{\eta(u)}, 2 \cdot (0, 0)) \xrightarrow{\sim} (E_u, (0, 0)).$$

Proof. A direct computation shows that the map

$$(x, y) \mapsto ((u-1)^4x + u^2 - u, (u-1)^6y + (u-1)^4(u^2 - 2u)x + u^4 - 2u^3 + u^2)$$

is such an isomorphism. Uniqueness follows from Lemma 2.2(i). \square

3. TWISTING $X_1(7)$ BY CHARACTERS

Suppose $\psi : G_k \rightarrow \mathbf{F}_7^\times$ is a homomorphism. In this section we will construct the family of all elliptic curves over k with a k -rational subgroup of order 7 on which G_k acts via the character ψ . We first consider the case where ψ has order dividing 3. Since any character ψ into \mathbf{F}_7^\times can be written uniquely as the product of a character of order dividing 3 and a character of order dividing 2 (namely, $\psi = \psi^4\psi^3$), we will obtain the family for a general ψ as a quadratic twist of a family with a cubic ψ .

The following lemma is taken from a paper of Washington [18, pp. 64–65].

Lemma 3.1 (Washington [18]). *Suppose that K/k is a cyclic cubic extension, and σ is a generator of $\text{Gal}(K/k)$. Then there is a $t \in k$ such that*

- (i) *K is the splitting field of the polynomial $f(x) := x^3 - (t+3)x^2 + tx + 1$,*
- (ii) *if γ is a root of f then $\gamma^\sigma = \eta(\gamma)$, where η is the linear fractional transformation defined by (3).*

Proof. Choose $\alpha \in K$ such that $K = k(\alpha)$. The set $\{1, \alpha, \alpha^\sigma, \alpha\alpha^\sigma\}$ is linearly dependent over k (but $\{1, \alpha\}$ is not), so we can find a linear fractional transformation $\phi \in \text{PGL}_2(k)$ such that $\alpha^\sigma = \phi(\alpha)$. Note that ϕ^3 fixes α, α^σ , and $\alpha\alpha^\sigma$, so $\phi^3 = 1$ in $\text{PGL}_2(k)$.

Let $\tilde{\phi}$ be an element in $\text{GL}_2(k)$ whose image under the map $\text{GL}_2(k) \rightarrow \text{PGL}_2(k)$ is ϕ . We must have $\text{trace}(\tilde{\phi}) \neq 0$. Otherwise, $\tilde{\phi}^2$ would be a scalar matrix and we would then have $\alpha\alpha^{\sigma^2} = \alpha$. Therefore we can choose the lift $\tilde{\phi}$ so that $\text{trace}(\tilde{\phi}) = -1$. Then, writing I for the identity in $\text{GL}_2(k)$,

$$\tilde{\phi}^2 + \tilde{\phi} = -\text{det}(\tilde{\phi})I, \quad \tilde{\phi}^3 = aI$$

for some $a \in k$, so

$$(1 - \text{det}(\tilde{\phi}))\tilde{\phi} = \tilde{\phi} + \tilde{\phi}^3 + \tilde{\phi}^2 = (a - \text{det}(\tilde{\phi}))I.$$

Since $\alpha^\sigma \neq \alpha$, $\tilde{\phi}$ cannot be a scalar matrix. It follows that $\det(\tilde{\phi}) = 1$ and the minimal polynomial of $\tilde{\phi}$ over k is $x^2 + x + 1$. Let $\tilde{\eta} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, which is a lift to $\mathrm{GL}_2(k)$ corresponding to η . Since $\tilde{\eta}$ has the same minimal polynomial as $\tilde{\phi}$, there is a $\tilde{\xi} \in \mathrm{GL}_2(k)$ such that

$$(4) \quad \tilde{\xi}\tilde{\phi}\tilde{\xi}^{-1} = \tilde{\eta}.$$

Set $\gamma = \xi(\alpha)$, where ξ is the linear fractional transformation corresponding to $\tilde{\xi}$. Then $k(\gamma) = k(\alpha) = K$, and by (4) we have

$$(5) \quad \gamma^\sigma = \eta(\gamma).$$

Applying σ and σ^2 to (5) shows that (5) holds with γ replaced by either of its conjugates, and that $\gamma^{\sigma^2} = (\gamma - 1)/\gamma$. We compute

$$(x - \gamma)(x - \gamma^\sigma)(x - \gamma^{\sigma^2}) = x^3 - \left(\frac{\gamma^3 - 3\gamma + 1}{\gamma^2 - \gamma}\right)x^2 + \left(\frac{\gamma^3 - 3\gamma^2 + 1}{\gamma^2 - \gamma}\right)x + 1$$

so the lemma holds with $t := \frac{\gamma^3 - 3\gamma^2 + 1}{\gamma^2 - \gamma} \in k$. \square

Theorem 3.2. *Suppose that $\chi : G_k \rightarrow \mathbf{F}_7^\times$ is a homomorphism, $\chi^3 = 1$, and E is an elliptic curve over k . Then E has a k -rational subgroup of order 7 on which G_k acts via χ if and only if there is a $v \in k$ such that E is isomorphic over k to the elliptic curve*

$$A_v : y^2 + a_1(v)xy + a_3(v)y = x^3 + a_2(v)x^2 + a_4(v)x + a_6(v)$$

over k defined as follows. If $\chi = 1$, let

$$a_1(v) = -v^2 + v + 1, \quad a_2(v) = a_3(v) = -v^3 + v^2, \quad a_4(v) = a_6(v) = 0.$$

If $\chi \neq 1$, then let K be the cubic extension of k cut out by χ , let $\sigma \in \mathrm{Gal}(K/k)$ be the element with $\chi(\sigma) = 4$, fix $t \in k$ satisfying Lemma 3.1 for K and σ , and let

$$\begin{aligned} c &= t^2 + 3t + 9, & f(v) &= v^3 - (t + 3)v^2 + tv + 1, \\ a_1(v) &= c(v^2 - v + 1), \\ a_2(v) &= cf(v)t(2v - 1), \\ a_3(v) &= cf(v)[(t^3 - 1)v^3 + (t^3 - 1)v + t^2 - t + 1], \\ a_4(v) &= c^2f(v)[(-3t^2 - 5t - 2)v^5 + (2t^3 + 8t^2 + 8t - 7)v^4 \\ &\quad - (3t^3 + 6t^2 + 5t - 20)v^3 + (2t^3 - t - 23)v^2 + 2(t^2 + 2t + 7)v - t - 1], \\ a_6(v) &= c^2f(v)^2[(2t^5 + 9t^4 + 23t^3 + 35t^2 + 24t + 11)v^6 \\ &\quad + (-t^6 - 6t^5 - 23t^4 - 38t^3 - 33t^2 + 36t)v^5 \\ &\quad + (t^6 + 6t^5 + 18t^4 - 6t^3 - 60t^2 - 180t + 13)v^4 \\ &\quad + (-t^6 - 2t^5 + 46t^3 + 84t^2 + 142t - 139)v^3 \\ &\quad + (-t^5 - 5t^4 - 27t^3 - 15t^2 + 9t + 182)v^2 \\ &\quad + (2t^4 + 3t^3 - 10t^2 - 32t - 67)v + 2t^3 + 5t^2 + 11t + 11]. \end{aligned}$$

Proof. If $\chi = 1$, then A_v is the curve E_v of (1), and the theorem follows from Theorem 2.3.

Suppose now that $\chi \neq 1$. Let $\gamma \in K$ be a root of $f(x)$. Define

$$\begin{aligned} U_v &:= ((\gamma - 1)v + 1)^2(2\gamma^2 - (2t + 5)\gamma + t - 1)^2, \\ R_v &:= cf(v)[(\gamma - t - 3)\gamma v - \gamma^2 + (t + 2)\gamma + 1], \\ S_v &:= ((t + 3)\gamma^2 - (t^2 + 5t + 9)\gamma - 3)v^2 \\ &\quad - (2t\gamma^2 - 2(t^2 + 3t + 3)\gamma + (t^2 + t + 3))v - 3\gamma^2 + (2t + 6)\gamma - t, \\ T_v &:= cf(v)[(2t^2 + 6t + 5)v^3 - (t^2 + 3t + 9)v^2 - 13v + 2t + 4]. \end{aligned}$$

If $v \in k$ and A_v is nonsingular, then we compute that $P_v := (R_v, T_v)$ is a point of order 7 in $A_v(K)$, and using Lemma (3.1)(ii) we compute that $P_v^\sigma = 4P_v = \chi(\sigma)P_v$. Thus P_v generates a k -rational subgroup of order 7 on A_v , on which G_k acts via χ . If E is isomorphic over k to A_v , then E also has such a subgroup.

Conversely, suppose E is an elliptic curve over k with a k -rational subgroup of order 7 on which G_k acts via χ . Let $P \in E(K)$ be a generator of that subgroup (so $P^\sigma = \chi(\sigma)P = 4P$). By Theorem 2.3(ii) applied with K in place of k , (E, P) corresponds to a K -rational point of $X_1(7)$, i.e., there are a $u \in K$ and an isomorphism $\varphi : E \xrightarrow{\sim} E_u$ defined over K such that $\varphi(P) = (0, 0) \in E_u[7]$.

Let δ be the linear fractional transformation

$$(6) \quad \delta(z) = \frac{-z + \gamma}{(\gamma - 1)z + 1}$$

and let $v = \delta^{-1}(u) \in K$. We compute that the map λ defined by

$$\lambda(x, y) := (U_v^2x + R_v, U_v^3y + U_v^2Sx + T_v)$$

is an isomorphism over K from $(E_u, (0, 0))$ to (A_v, P_v) . (Since $\delta(v) = u$, by (6) we have $(\gamma - 1)v + 1 \neq 0$; since also $[k(\gamma) : k] = 3$, we have $U_v \neq 0$.) Therefore $\lambda \circ \varphi$ is an isomorphism from (E, P) to (A_v, P_v) . If we show that $v \in k$, then Lemma 2.2(ii) will imply that (E, P) and (A_v, P_v) are isomorphic over k .

Suppose $\sigma \in G_k$. Then φ^σ is an isomorphism from E to E_{u^σ} , and

$$\varphi^\sigma(P) = \varphi^\sigma(2P^\sigma) = 2\varphi^\sigma(P^\sigma) = 2\varphi(P)^\sigma = 2(0, 0)^\sigma = 2(0, 0).$$

Thus we have isomorphisms

$$(E_u, (0, 0)) \xrightarrow{\varphi^{-1}} (E, P) \xrightarrow{\varphi^\sigma} (E_{u^\sigma}, 2(0, 0)) \xrightarrow{\sim} (E_{\eta^{-1}(u^\sigma)}, (0, 0))$$

where η is defined by (3) and the final isomorphism comes from Lemma 2.4. Thus by the uniqueness of u in Theorem 2.3(ii) (applied with K in place of k) we see that $u = \eta^{-1}(u^\sigma)$, so $u^\sigma = \eta(u)$.

Using the definition of δ and Lemma 3.1(ii), it is easy to check that $\delta^\sigma = \eta\delta$. Hence we have

$$v^\sigma = \delta^{-1}(u)^\sigma = (\delta^\sigma)^{-1}(u^\sigma) = \delta^{-1}\eta^{-1}(u^\sigma) = \delta^{-1}(u) = v.$$

Therefore $v \in k$, so A_v is defined over k , G_k acts on both P and P_v by multiplication by χ , and so the isomorphism $\lambda \circ \varphi : (E, P) \xrightarrow{\sim} (A_v, P_v)$ is defined over k by Lemma 2.2(ii). \square

Remark 3.3. Suppose $\chi \neq 1$ in Theorem 3.2. With notation as in Theorem 3.2, the discriminant of A_v is given by

$$(7) \quad \Delta(A_v) = c^8 f(v)^7 [(t - 5)v^3 + (5t + 24)v^2 - (8t + 9)v + t - 5].$$

Remark 3.4. With notation as in Theorem 3.2 with $\chi \neq 1$, the cubic Galois extension K of k is the splitting field over k of the polynomial $f(x) \in k[x]$, by Lemma 3.1(i). Thus, $f(x)$ is separable and irreducible over k . One can compute that c^2 is the discriminant of f , so $c \neq 0$. It then follows from (7) that $\Delta(A_v) = 0$ for at most three values of $v \in k^s$.

Definition 3.5. If E is an elliptic curve over k and $\epsilon : G_k \rightarrow \{\pm 1\} \subseteq \text{Aut}(E)$ is a homomorphism, then the (quadratic) *twist* of E by ϵ is an elliptic curve $E^{(\epsilon)}$ over k such that there is an isomorphism $\lambda : E^{(\epsilon)} \rightarrow E$ over k^s with $\lambda^\sigma \circ \lambda^{-1} = \epsilon(\sigma)$ for all $\sigma \in G_k$.

If $\text{char}(k) \neq 2$, E is an elliptic curve over k defined by an equation of the form $y^2 = F(x)$, and $k(\sqrt{d})$ is the field cut out by such a character ϵ , then $E^{(\epsilon)}$ is isomorphic over k to the curve defined by $dy^2 = F(x)$, i.e., the quadratic twist of E by d .

Theorem 3.6. *Suppose that $\psi : G_k \rightarrow \mathbf{F}_7^\times$ is a homomorphism. If E is an elliptic curve over k , then E has a k -rational subgroup of order 7 on which G_k acts via ψ if and only if there is a $v \in k$ such that E is isomorphic over k to the twist of A_v by ψ^3 , where A_v is as in Theorem 3.2 for the character $\chi = \psi^4$.*

In particular, if $\text{char}(k) \neq 2$ and $k(\sqrt{d})$ is the field cut out by ψ^3 , then the twist of A_v by ψ^3 is

$$A_v^{(d)} : y^2 = x^3 + db_2(v)x^2 + 8d^2b_4(v)x + 16d^3b_6(v),$$

where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$ are the usual invariants of the curve A_v .

Proof. Since $\psi^6 = 1$, we have $(\psi^4)^3 = 1$, so we can apply Theorem 3.2, and we can also twist by ψ^3 as in Definition 3.5. Let $\lambda : E^{(\psi^3)} \xrightarrow{\sim} E$ be as in Definition 3.5. For $P \in E(k^s)$ and $\sigma \in G_k$, $P^\sigma = \psi(\sigma)P$ if and only if $\lambda^{-1}(P)^\sigma = \psi^4(\sigma)\lambda^{-1}(P)$. Thus by Theorem 3.2,

$$\begin{aligned} E &\text{ has a } k\text{-rational subgroup of order 7 on which } G_k \text{ acts via } \psi \\ &\Leftrightarrow E^{(\psi^3)} \text{ has a } k\text{-rational subgroup of order 7 on which } G_k \text{ acts via } \psi^4 \\ &\Leftrightarrow E^{(\psi^3)} \text{ is isomorphic over } k \text{ to } A_v \text{ for some } v \in k \\ &\Leftrightarrow E \text{ is isomorphic over } k \text{ to } A_v^{(\psi^3)} \text{ for some } v \in k. \end{aligned}$$

If $\text{char}(k) \neq 2$, then $A_v^{(d)}$ is a Weierstrass model for $A_v^{(\psi^3)}$. \square

Let $\omega : G_k \rightarrow \mathbf{F}_7^\times$ denote the cyclotomic character giving the action of G_k on μ_7 . That is, $\zeta_7^{\omega(\sigma)} = \zeta_7^\sigma$, where ζ_7 is a primitive seventh root of unity in k^s .

Lemma 3.7. *Let $A_v^{(d)}$ be as in Theorem 3.6, and let η be as defined by (3). Then for every v , we have $A_{\eta(v)}^{(d)} \cong A_v^{(d)}$ over $k(v)$.*

Proof. This can be shown by exhibiting an explicit isomorphism. We will give a slightly less computational way to deduce the lemma from Lemma 2.4. We can easily reduce to the case $d = 1$.

Let δ be the linear fractional transformation defined by (6) in the proof of Theorem 3.2. The proof of Theorem 3.2 showed that $(A_v, P_v) \cong (E_{\delta(v)}, (0, 0))$ for every

v , so we have

$$(A_v, P_v) \cong (E_{\delta(v)}, (0, 0)) \cong (E_{\eta\delta(v)}, 2 \cdot (0, 0)) \cong (A_{\delta^{-1}\eta\delta(v)}, 2 \cdot P_{\delta^{-1}\eta\delta(v)})$$

where the middle isomorphism is from Lemma 2.4. A simple calculation shows that $\delta^{-1}\eta\delta(v) = \eta^2 = \eta^{-1}$, and so $A_v \cong A_{\eta^{-1}(v)}$ over $k(v)$ by Lemma 2.2(ii). \square

Corollary 3.8. *Suppose that $\psi : G_k \rightarrow \mathbf{F}_7^\times$ is a homomorphism and that $k \neq \mathbf{F}_2$. Then there exists an elliptic curve E over k with a k -rational subgroup of order 7 on which G_k acts via ψ .*

Proof. Let A_v be as defined in Theorem 3.2, for the (at most cubic) character ψ^4 . If $v \in k$ is not a zero of the discriminant $\Delta(A_v)$, then Theorem 3.6 shows that the twist of A_v by ψ^3 has the desired property. We need only show that there exists a $v \in k$ such that $\Delta(A_v) \neq 0$.

Suppose $\psi^4 = 1$. Then $A_v = E_v$, so $\Delta(A_v) = \Delta(E_v)$ is given by (2). That polynomial has at most 5 roots, and it is easy to check that it has only the roots 0 and 1 if $|k| \leq 5$. Hence, there are $v \in k$ with $\Delta(A_v) \neq 0$ if and only if $k \neq \mathbf{F}_2$.

Now suppose $\psi^4 \neq 1$. Then $\Delta(A_v)$ is the polynomial given in (7). By Remark 3.4, $c \neq 0$, and $f(v) \neq 0$ for every $v \in k$. Thus for $v \in k$, $\Delta(A_v) = 0$ if and only if $(t-5)v^3 + (5t+24)v^2 - (8t+9)v + t - 5 = 0$. If $t \neq 5$, then $\Delta(A_v) \neq 0$ when $v = 0$. If $t = 5$, then $\Delta(A_v) = 0$ only when $v = 0$ or 1 (since $\text{char}(k) \neq 7$), so there are $v \in k$ with $\Delta(A_v) \neq 0$ if and only if $k \neq \mathbf{F}_2$. \square

Remark 3.9. Suppose that $k = \mathbf{F}_2$ and $\psi : G_{\mathbf{F}_2} \rightarrow \mathbf{F}_7^\times$ is a homomorphism. Then there exists an elliptic curve E over \mathbf{F}_2 with an \mathbf{F}_2 -rational subgroup of order 7 on which $G_{\mathbf{F}_2}$ acts via ψ if and only if ψ is ω^{-1} or $\omega^{-1}\epsilon$, where ϵ is the unique character of $G_{\mathbf{F}_2}$ of order 2. The remaining characters are 1, ω , ϵ , and $\omega\epsilon$; for each of these characters there is no elliptic curve over \mathbf{F}_2 with an \mathbf{F}_2 -rational subgroup of order 7 on which $G_{\mathbf{F}_2}$ acts via that character. This follows from the above proof, the fact that ω has order 3, and the fact that $t = 1$ when $\psi^4 = \omega$ while $t = 0$ when $\psi^4 = \omega^{-1}$. (Alternatively, this can also be deduced from the fact that no elliptic curve defined over \mathbf{F}_2 has a rational point of order 7, which follows from the Weil bounds.)

Remark 3.10. Here is another interpretation of Theorem 3.6. Suppose Ψ is a cyclic group of order 7 with an action of G_k . Consider isomorphism classes (in the obvious sense) of pairs (E, f) where E is an elliptic curve and $f : \Psi \hookrightarrow E[7]$ is an injection. We say that (E, f) is k -rational if (E^σ, f^σ) is isomorphic to (E, f) for every $\sigma \in G_k$, and we let $X(\Psi)$ denote the moduli space of such isomorphism classes. If K is an extension of k such that G_K acts trivially on Ψ , and P is a generator of Ψ , then the map

$$(E, f) \mapsto (E, f(P))$$

induces an isomorphism from $X(\Psi)$ to $X_1(7)$ defined over K . Thus $X(\Psi)$ is a twist of $X_1(7)$.

Let $\psi : G_k \rightarrow \text{Aut}(\Psi) \cong \mathbf{F}_7^\times$ be the character giving the action of G_k on Ψ . Let A_v be as defined in Theorem 3.2 with $\chi = \psi^4$, and let $f_v : \Psi \rightarrow A_v[7]$ be the unique homomorphism with $f_v(P) = P_v$, where P_v is as in the proof of Theorem 3.2. Then Theorem 3.6 says that the elliptic surface A_v is the universal elliptic curve over $X(\Psi)$, in the following sense. For every $v \in k^s$ such that $\Delta(A_v) \neq 0$, the

pair (A_v, f_v) is $k(v)$ -rational, and conversely for every pair (E, f) with E defined over k^s , there is a unique $v \in k^s$ such that (E, f) is isomorphic to (A_v, f_v) .

If $a \in \mathbf{F}_7^\times / (\pm 1)$ there is a natural automorphism of $X(\Psi)$ induced by $(E, f) \mapsto (E, af)$. The proof of Lemma 3.7 shows that the automorphism corresponding to $a = 2$ is η , in the sense that $(A_{\eta(v)}, f_{\eta(v)}) \cong (A_v, 2f_v)$.

4. THE SPECIAL CASE WHERE $k = \mathbf{Q}$ AND $\psi = \omega^5$

Let $\omega : G_{\mathbf{Q}} \rightarrow \mathbf{F}_7^\times$ denote the cyclotomic character. If E is an elliptic curve defined over \mathbf{Q} , let $\Delta_{\min}(E)$ denote the discriminant of a minimal model of E .

Define an elliptic curve

$$(8) \quad B_v : y^2 + xy = x^3 - x^2 + \alpha(v)x + \beta(v),$$

where

$$\begin{aligned} \alpha(v) &:= -\frac{35}{16}v^8 + \frac{63}{4}v^7 - \frac{833}{24}v^6 + \frac{49}{2}v^5 + \frac{245}{48}v^4 - \frac{49}{2}v^3 + \frac{343}{24}v^2 + \frac{7}{4}v - 2, \\ \beta(v) &:= -\frac{49}{32}v^{12} + \frac{637}{48}v^{11} - \frac{1617}{32}v^{10} + \frac{44149}{432}v^9 - \frac{16555}{192}v^8 - \frac{1477}{36}v^7 + \frac{1911}{16}v^6 \\ &\quad - \frac{8183}{144}v^5 - \frac{2009}{192}v^4 + \frac{7007}{432}v^3 - \frac{147}{16}v^2 + \frac{14}{3}v - 1. \end{aligned}$$

The discriminant of B_v is

$$(9) \quad \Delta(B_v) = -7^3(v^3 - 2v^2 - v + 1)(v^3 - v^2 - 2v + 1)^7.$$

Theorem 4.1. *Let B_v be as above.*

- (i) *Suppose E is an elliptic curve over \mathbf{Q} . Then E has a rational subgroup of order 7 on which $G_{\mathbf{Q}}$ acts via ω^5 if and only if there is a $v \in \mathbf{Q}$ such that $E \cong B_v$ over \mathbf{Q} .*
- (ii) *If p is a prime and $v \in \mathbf{Q}$ is integral at p , then the above model for B_v is integral at p and minimal at p .*
- (iii) *If p is a prime and $v \in \mathbf{Q}$ is not integral at p , then*

$$\text{ord}_p(\Delta_{\min}(B_v)) = \text{ord}_p(\Delta(B_v)) - 24 \text{ord}_p(v).$$

Proof. We will deduce part (i) from Theorem 3.6. The cyclotomic character ω has order 6. Let $\psi = \omega^5$. The cubic character $\psi^4 = \omega^2$ cuts out the unique cubic subfield $K := \mathbf{Q}(\mu_7)^+$ of $\mathbf{Q}(\mu_7)$. The automorphism $\sigma \in \text{Gal}(K/\mathbf{Q})$ that sends $\zeta_7 + \zeta_7^{-1}$ to $\zeta_7^2 + \zeta_7^{-2}$ satisfies $\omega(\sigma) = 2$, so $\psi(\sigma) = 2^5 = 4$. Using the construction of γ and t in the proof of Lemma 3.1, we obtain $t = -2$ and $\gamma = -(\zeta_7 + \zeta_7^{-1})$.

Further, the quadratic character $\psi^3 = \omega^3$ cuts out the unique quadratic subfield $\mathbf{Q}(\sqrt{-7})$ of $\mathbf{Q}(\mu_7)$. The map $(x, y) \mapsto (x', y')$ where

$$x' = \frac{1}{4}x + \frac{3}{4}v^4 - \frac{5}{6}v^3 - \frac{15}{4}v^2 + \frac{23}{6}v - 1, \quad y' = \frac{1}{8}y - \frac{1}{2}x'$$

is an isomorphism from the curve $A_v^{(d)}$ of Theorem 3.6 with $t = -2$ and $d = -1/7$, to the curve B_v of (8) (recall that t is in the definition of A_v in Theorem 3.2, which is used to define $A_v^{(d)}$ in Theorem 3.6). Now (i) follows from Theorem 3.6.

The polynomials $\alpha(v)$ and $\beta(v)$ take \mathbf{Z} to \mathbf{Z} , as can be seen, for example, by expressing them as integral linear combinations of binomial coefficient polynomials $\binom{v}{n}$. It follows that if $v \in \mathbf{Q}$ is integral at p , then the model (8) is integral at p .

Suppose first that $p \neq 7$. With c_4 the usual invariant (see [14, §III.1]), we check that the polynomial $c_4(B_v)$ is in $\mathbf{Z}[v]$. The resultant of the polynomials $\Delta(B_v)$ and $c_4(B_v)$ is 7^{98} , which is a unit at p . Hence if v is integral at p , then $\Delta(B_v)$

and $c_4(B_v)$ cannot both vanish mod p , so by Tate's algorithm (or [14, Proposition III.1.4(ii)]), the equation defining B_v is minimal at p .

If $p = 7$ and $v \in \mathbf{Q}$ is integral at 7, then Lemma 4.4(c) below shows that $\text{ord}_7(\Delta(B_v)) < 12$, so the equation defining B_v is minimal at 7. This proves (ii).

Now suppose that v is not integral at p . Then $w := 1/v$ is integral at p , and via the change of variables

$$(x, y) \mapsto (w^4x - \frac{w^4-1}{4}, w^6y + \frac{w^4(w^2-1)}{2}x + \frac{w^4-1}{8}),$$

B_v has a model

$$\begin{aligned} \hat{B}_v : y^2 + xy = x^3 - x^2 + (\tilde{\alpha}(w) + \frac{3}{16}(1 - w^8))x \\ + \tilde{\beta}(w) + \frac{w^4-1}{4}\tilde{\alpha}(w) - \frac{2w^{12}-3w^8+1}{64} \end{aligned}$$

where $\tilde{\alpha}(z) := z^8\alpha(1/z)$, $\tilde{\beta}(z) := z^{12}\beta(1/z) \in \mathbf{Q}[z]$ with α and β as in (8). Again, one can check that the polynomials

$$\tilde{\alpha}(z) + 3(1 - z^8)/16 \quad \text{and} \quad \tilde{\beta}(z) + (z^4 - 1)\tilde{\alpha}(z)/4 + (-2z^{12} + 3z^8 - 1)/16$$

take \mathbf{Z} to \mathbf{Z} . Hence \hat{B}_v is integral at p . Exactly as for (ii) one can show that \hat{B}_v is minimal at p , and hence $\Delta_{\min}(B_v) = \Delta(\hat{B}_v) = v^{-24}\Delta(B_v)$. This proves (iii). \square

Remark 4.2. Theorem 4.1(i) shows that for $v \in \mathbf{Q}$, the representation of $G_{\mathbf{Q}}$ acting on $B_v[7]$ is of the form $\begin{pmatrix} \omega^5 & * \\ 0 & \omega^2 \end{pmatrix}$.

Corollary 4.3. *If $v \in \mathbf{Q}$ has denominator d , then*

$$\Delta_{\min}(B_v) = \Delta(B_v)d^{24} = -7^3d^{24}(v^3 - 2v^2 - v + 1)(v^3 - v^2 - 2v + 1)^7.$$

Proof. This follows directly from Theorem 4.1(ii,iii). \square

Lemma 4.4. *Let $f_1(v) = v^3 - 2v^2 - v + 1$ and $f_2(v) = v^3 - v^2 - 2v + 1$. For $v \in \mathbf{Q}$ and B_v as above, we have the following table:*

	<i>v</i> integral at 7			<i>v</i> not integral at 7
	<i>v</i> $\equiv 3 \pmod{7}$	<i>v</i> $\equiv 5 \pmod{7}$	otherwise	
(a) $\text{ord}_7(f_1(v))$	1	0	0	$3 \text{ord}_7(v)$
(b) $\text{ord}_7(f_2(v))$	0	1	0	$3 \text{ord}_7(v)$
(c) $\text{ord}_7(\Delta(B_v))$	4	10	3	$3 + 24 \text{ord}_7(v)$
(d) $\text{ord}_7(\Delta_{\min}(B_v))$	4	10	3	3
(e) $\text{ord}_7(j(B_v))$	≥ 2	≥ 5	0	0

Proof. If v is not integral at 7, then $\text{ord}_7(f_1(v)) = \text{ord}_7(f_2(v)) = 3\text{ord}_7(v)$. If v is integral at 7, then a direct computation shows that $f_1(v), f_2(v) \not\equiv 0 \pmod{7^2}$. Since $f_1(v) \equiv (v - 3)^3 \pmod{7}$ and $f_2(v) \equiv (v - 5)^3 \pmod{7}$, (a) and (b) follow.

By (9) we have $\Delta(B_v) = -7^3f_1(v)f_2(v)^7$, so (c) follows from (a) and (b). Assertion (d) follows directly from (c) and Theorem 4.1(ii,iii).

We compute that

$$(10) \quad j(B_v) = -\frac{[(v^2 - 3v - 3)(v^2 - v + 1)(3v^2 - 9v + 5)(5v^2 - v - 1)]^3}{f_1(v)f_2(v)^7}.$$

If $v \equiv 5 \pmod{7}$, then each quadratic factor in the numerator vanishes modulo 7. If $v \equiv 3 \pmod{7}$, then $v^2 - v + 1 \equiv 0 \pmod{7}$. If $v \not\equiv 3$ or $5 \pmod{7}$, then none

of the factors in the numerator vanish modulo 7. These remarks together with (a) and (b) imply the assertions in (e). \square

Proposition 4.5. *For $v \in \mathbf{Q}$ and B_v as above, let Ψ_v be the \mathbf{Q} -rational subgroup of B_v of order 7 on which $G_{\mathbf{Q}}$ acts via ω^5 . Let B'_v be the quotient of B_v by Ψ_v , so there is an isogeny from B_v to B'_v defined over \mathbf{Q} . Then the isogenous curve B'_v is isomorphic over \mathbf{Q} to the twist of B_{1-v} by ω^3 .*

Proof. One can verify this by a direct calculation, using the formulas of Vélú [17] (see [1, §4.1]) to exhibit the isogeny. (See especially Proposition 4.1 of [1] and the formulas for \tilde{A} and \tilde{B} in the paragraph after its proof.) \square

Note that B'_v has a subgroup of order 7 on which $G_{\mathbf{Q}}$ acts via ω^2 , namely, $B_v[7]/\Psi_v$. Also, the twist of B_{1-v} by ω^3 is the quadratic twist of B_{1-v} by -7 .

Corollary 4.6. *Suppose $v \in \mathbf{Q}$. Then:*

- (i) $\frac{\Delta_{\min}(B'_v)}{\Delta_{\min}(B_v)} = 7^{s_v} \left(\frac{v^3 - 2v^2 - v + 1}{v^3 - v^2 - 2v + 1} \right)^6$ for some $s_v \in \{\pm 6\}$, and
- (ii) $\text{ord}_7 \left(\frac{\Delta_{\min}(B'_v)}{\Delta_{\min}(B_v)} \right) = \begin{cases} 0 & \text{if } v \text{ is integral at 7 and } v \equiv 3 \text{ or } 5 \pmod{7}, \\ 6 & \text{otherwise.} \end{cases}$

Proof. Let $f_1(v) = v^3 - 2v^2 - v + 1$ and $f_2(v) = v^3 - v^2 - 2v + 1$ as in Lemma 4.4, let $B_{1-v}^{(-7)}$ denote the quadratic twist of B_{1-v} by -7 , and let

$$(11) \quad s_v := \text{ord}_7 \left(\frac{\Delta_{\min}(B_{1-v}^{(-7)})}{\Delta_{\min}(B_{1-v})} \right) \in \{\pm 6\}.$$

Note that $f_1(1-v) = -f_2(v)$ and $f_2(1-v) = -f_1(v)$. Since v and $1-v$ have the same denominator, by Corollary 4.3 we have

$$\Delta_{\min}(B_{1-v})/\Delta_{\min}(B_v) = f_1(v)^6/f_2(v)^6.$$

By Proposition 4.5 we have $B'_v \cong B_{1-v}^{(-7)}$. Thus

$$(12) \quad \frac{\Delta_{\min}(B'_v)}{\Delta_{\min}(B_v)} = \frac{\Delta_{\min}(B_{1-v}^{(-7)})}{\Delta_{\min}(B_v)} = \frac{7^{s_v} \Delta_{\min}(B_{1-v})}{\Delta_{\min}(B_v)} = 7^{s_v} \left(\frac{f_1(v)}{f_2(v)} \right)^6,$$

proving (i).

To prove (ii) we need to compute s_v . Using Lemma 4.4(e), it follows that

$$\text{ord}_7(j(B_{1-v}^{(-7)})) = \text{ord}_7(j(B_{1-v})) \geq 0.$$

Hence, by Tate's algorithm (see for example [14, Table 15.1]), we have

$$0 \leq \text{ord}_7(\Delta_{\min}(B_{1-v}^{(-7)})) \leq 10.$$

It follows that the integer s_v of (11) satisfies

$$s_v = \begin{cases} 6 & \text{if } \text{ord}_7(\Delta_{\min}(B_{1-v})) < 6 \\ -6 & \text{if } \text{ord}_7(\Delta_{\min}(B_{1-v})) \geq 6. \end{cases}$$

Now Lemma 4.4(d) shows that $s_v = -6$ if v is both integral at 7 and congruent to 3 (mod 7), and $s_v = 6$ otherwise. Assertion (ii) now follows from (12) and Lemma 4.4(a,b). \square

Proposition 4.7. *Suppose that $v \in \mathbf{P}^1(\mathbf{Q})$. Then:*

- (i) *The conductor of the elliptic curve B_v is of the form $49 \prod_{i=1}^m \ell_i$, where the ℓ_i 's are distinct primes such that $\ell_i \equiv \pm 1 \pmod{7}$.*
- (ii) *The curve B_v has potentially good reduction at 7. Further, if v is integral at 7 and $v \equiv 3$ or $5 \pmod{7}$, then B_v has potentially ordinary reduction at 7, and for all other $v \in \mathbf{P}^1(\mathbf{Q})$, B_v has potentially supersingular reduction at 7.*
- (iii) *The conductor of B_v is 49 if and only if $v \in \{0, 1, \infty, 2, 1/2, -1\}$.*

Proof. Lemma 4.4(e) shows that $j(B_v)$ is integral at 7 for all $v \in \mathbf{P}^1(\mathbf{Q})$. Hence B_v always has potentially good reduction at 7, giving (ii). However, B_v cannot have good reduction at 7. One sees this by considering the action of $G_{\mathbf{Q}_7}$ on $B_v[7]$. If B_v had good ordinary reduction at 7, then $B_v[7]$ would have a nontrivial unramified quotient over \mathbf{Q}_7 (by [12, Proposition 11]), which is not the case since ω^2 and ω^5 are ramified characters of $G_{\mathbf{Q}_7}$. If B_v had good supersingular reduction, then $B_v[7]$ would be irreducible over \mathbf{Q}_7 (by [12, Proposition 12(c)]), which is also not the case. It follows that the conductor of B_v is $49M$, where M is not divisible by 7.

By examining the elliptic curves over \mathbf{F}_7 , we see that an elliptic curve E over \mathbf{Q} has supersingular or potentially supersingular reduction at 7 if and only if $j(E) \equiv -1 \pmod{7}$. If v is integral at 7 and satisfies $v \equiv 3$ or $5 \pmod{7}$, then Lemma 4.4(e) shows that $j(B_v) \equiv 0 \pmod{7}$, and so B_v has potentially ordinary reduction at 7. For the other v 's, the formula for $j(B_v)$ in (10) shows that we indeed have $j(B_v) \equiv -1 \pmod{7}$. This proves (ii).

Suppose ℓ is a prime dividing M . If B_v has additive reduction at ℓ , then B_v becomes semistable over $\mathbf{Q}(B_v[7])$ and the ramification degree of ℓ in $[\mathbf{Q}(B_v[7]) : \mathbf{Q}]$ is divisible by 2 or 3. (A good summary of the ramification properties in the non-semistable case can be found in [12, §5.6], especially Proposition 23(b).) This contradicts the facts that ℓ is unramified in $\mathbf{Q}(\mu_7)/\mathbf{Q}$ and $[\mathbf{Q}(B_v[7]) : \mathbf{Q}(\mu_7)]$ is (by Remark 4.2) 1 or 7. Thus, B_v has multiplicative reduction at ℓ . It follows that M is not divisible by ℓ^2 .

The action of $G_{\mathbf{Q}_\ell}$ on $B_v[7^\infty]$ can be described by the Tate parametrization. One sees that $B_v[7]$, or an unramified quadratic twist of $B_v[7]$, has composition factors isomorphic over \mathbf{Q}_ℓ to μ_7 and $\mathbf{Z}/7\mathbf{Z}$. Let ω_ℓ denote the restriction of ω to $G_{\mathbf{Q}_\ell}$. Thus, $G_{\mathbf{Q}_\ell}$ acts on the composition factors by two \mathbf{F}_7^\times -valued characters whose ratio is ω_ℓ , or its inverse. On the other hand, $G_{\mathbf{Q}_\ell}$ acts on the composition factors via ω_ℓ^2 and ω_ℓ^5 , whose ratio is $\omega_\ell^{\pm 3}$, a character of order 1 or 2. Therefore ω_ℓ has order 1 or 2, so $\ell \equiv \pm 1 \pmod{7}$, giving (i).

There are exactly two j -invariants of curves of conductor 49. Using (10) we see that these correspond precisely to the six values of v listed in (iii). \square

Remark 4.8. There is an S_3 -action on $\mathbf{P}^1(\mathbf{Q})$ defined by the linear fractional transformations η of (3) and ι defined by $\iota(v) = 1 - v$. Since the fixed points of η (the primitive sixth roots of unity) are not in \mathbf{Q} , the orbits under the action of η always have length 3. There are just two orbits of length 3 under the action of S_3 . For v is in such an orbit if and only if $1 - v = \eta^i(v)$ for some $i \in \{0, 1, 2\}$. One easily determines the possible orbits of that type: $\{0, 1, \infty\}$ is one, $\{-1, 1/2, 2\}$ is the other. By Proposition 4.7(iii) the corresponding curves B_v have conductor 49, and hence have complex multiplication. One can also explain this as follows.

By Proposition 4.5, the elliptic curves $B_{1-v}^{(-7)}$ and B_v/Ψ_v are \mathbf{Q} -isomorphic for every $v \in P_1(\mathbf{Q})$. However, if $1 - v \in \{v, \eta(v), \eta^2(v)\}$, then Lemma 3.7 shows that

B_{1-v} is \mathbf{Q} -isomorphic to B_v , so there is an isomorphism $B_v/\Psi_v \cong B_v$ defined over $F = \mathbf{Q}(\sqrt{-7})$. Therefore, B_v has an endomorphism of degree 7 defined over F . This means that B_v has CM by F . Furthermore, since a CM curve has no primes of multiplicative reduction, Proposition 4.7 shows that the conductor of B_v is 49. If $v \in \{0, 1, \infty\}$, then $j(B_v) = -15^3$ and $\text{End}(B_v)$ is the maximal order in F . If $v \in \{-1, 1/2, 2\}$, then $j(B_v) = 255^3$ and $\text{End}(B_v)$ is the nonmaximal order of conductor 2 in F .

5. THE IMAGE OF $\rho_{E,p}$

We assume throughout this section that E is an elliptic curve defined over \mathbf{Q} that has a \mathbf{Q} -isogeny of prime degree $p \geq 7$. Let Ψ denote the kernel of the isogeny and let $\Phi = E[p]/\Psi$. The actions of $G_{\mathbf{Q}}$ on Ψ and Φ are given by characters $\psi, \varphi : G_{\mathbf{Q}} \rightarrow \mathbf{F}_p^\times$, respectively. Since $\psi\varphi = \omega$, which is an odd character, we have $\psi \neq \varphi$. Hence $\Psi \not\cong \Phi$ as $G_{\mathbf{Q}}$ -modules.

Let $K_\infty = \mathbf{Q}(E[p^\infty])$ and let $\rho_{E,p} : G_{\mathbf{Q}} \rightarrow \text{Aut}_{\mathbf{Z}_p}(T_p(E))$ be the homomorphism giving the action of $G_{\mathbf{Q}}$ on the Tate module $T_p(E)$. Then $\rho_{E,p}$ factors through the Galois group $G := \text{Gal}(K_\infty/\mathbf{Q})$, and defines an injective homomorphism from G into $\text{Aut}_{\mathbf{Z}_p}(T_p(E))$. To simplify the discussion, we identify G with its image in $\text{Aut}_{\mathbf{Z}_p}(T_p(E))$.

We would like to know whether $\text{image}(\rho_{E,p})$ contains a Sylow pro- p subgroup of $\text{Aut}(T_p(E))$, or equivalently, whether the index $[\text{Aut}_{\mathbf{Z}_p}(T_p(E)) : \text{image}(\rho_{E,p})]$ is prime to p .

Definition 5.1. An elliptic curve E over \mathbf{Q} with a \mathbf{Q} -isogeny of degree p is said to be *p -exceptional* if $\text{image}(\rho_{E,p})$ does *not* contain a Sylow pro- p subgroup of $\text{Aut}(T_p(E))$.

In other words, E is not p -exceptional if the image of $\rho_{E,p}$ is as large as it could be, given the existence of a \mathbf{Q} -isogeny for E of degree p with character ψ . Note that if E is p -exceptional, then so is any quadratic twist of E , and so is any curve \mathbf{Q} -isogenous to E (see [4]).

If we choose a basis for $T_p(E)$ to identify $\text{Aut}(T_p(E))$ with $\text{GL}_2(\mathbf{Z}_p)$, then the Sylow pro- p subgroups of $\text{Aut}(T_p(E))$ are identified with the conjugates of

$$\begin{pmatrix} 1 + p\mathbf{Z}_p & \mathbf{Z}_p \\ p\mathbf{Z}_p & 1 + p\mathbf{Z}_p \end{pmatrix}.$$

There are $p + 1$ such conjugates, all containing $I_2 + pM_2(\mathbf{Z}_p)$.

Let $K = \mathbf{Q}(\Psi, \Phi)$, the fixed field for the intersections of the kernels of ψ and φ . Then K is an abelian extension of \mathbf{Q} and $[\mathbf{Q}(E[p]) : K]$ is 1 or p . Since $[K : \mathbf{Q}]$ divides $(p - 1)^2$, it is not divisible by p . Let

$$S := \text{Gal}(K_\infty/K).$$

Then S is a normal subgroup of G and is the (unique) Sylow pro- p subgroup of G .

Let

$$E' := E/\Psi.$$

Thus E' has a \mathbf{Q} -isogeny of degree p with kernel Φ and character φ .

Remark 5.2. The assumption that $p \geq 7$ implies that an elliptic curve over \mathbf{Q} cannot have a $G_{\mathbf{Q}}$ -invariant cyclic subgroup of order p^2 . This is due to Mazur [10] for most primes, Ligozat [9] or Kenku [6] for $p = 7$, and Kenku [5] for $p = 13$.

It follows that an elliptic curve over \mathbf{Q} cannot have two independent \mathbf{Q} -isogenies of degree $p \geq 7$. To see this, suppose to the contrary that $E[p] \cong \Psi \times \Phi$. Let $C = \{P \in E : pP \in \Phi\} \subset E[p^2]$, which is obviously $G_{\mathbf{Q}}$ -invariant. Then C/Ψ is a $G_{\mathbf{Q}}$ -invariant cyclic subgroup of E' of order p^2 , which is not possible. It follows that both of the fields $\mathbf{Q}(E[p])$ and $\mathbf{Q}(E'[p])$ are cyclic extensions of K of degree p .

Proposition 5.3 ([4], Proposition 4.3.2). *The curve E is p -exceptional if and only if $\mathbf{Q}(E[p]) = \mathbf{Q}(E'[p])$.*

The proof of this proposition in [4] is based on the Burnside Basis Theorem. The Frattini quotient of a Sylow pro- p subgroup S_p of $\text{Aut}(T_p(E))$ containing S has \mathbf{F}_p -dimension 3. It turns out that the image of S in that Frattini quotient has \mathbf{F}_p -dimension 2 if $\mathbf{Q}(E[p]) = \mathbf{Q}(E'[p])$, and \mathbf{F}_p -dimension 3 if those two fields are distinct. In the latter case, one can find a set of topological generators for S_p in S , which then implies that $S = S_p$.

The following lemma will provide one way to verify that $\mathbf{Q}(E[p]) \neq \mathbf{Q}(E'[p])$. Note that if L is a Galois extension of \mathbf{Q} containing K and $[L : K] = p$, then the ramification degree for a prime ℓ in the extension L/\mathbf{Q} is divisible by p if and only if the primes of K lying over ℓ are ramified in L/K . We then simply say that ℓ is ramified in L/K . Interestingly, if $\ell \neq p$, then ℓ can be ramified in at most one of the extensions $\mathbf{Q}(E[p])/K$ or $\mathbf{Q}(E'[p])/K$.

Lemma 5.4. *Assume that ℓ is a prime and that $\ell \neq p$. Then the ramification degree of ℓ in at least one of the two extensions $\mathbf{Q}(E[p])/\mathbf{Q}$ and $\mathbf{Q}(E'[p])/\mathbf{Q}$ is prime to p .*

Proof. Assume that the ramification degree of ℓ in $\mathbf{Q}(E[p])/\mathbf{Q}$ is divisible by p . This implies that E has bad reduction at ℓ . If E had potentially good reduction at ℓ , then the only primes that could divide the ramification degree for ℓ in $\mathbf{Q}(E[p])/\mathbf{Q}$ are 2 and 3 (see for example the proof of Corollary 2(a) to Theorem 2 of [13]). This contradicts the assumption that $p \geq 7$. Hence, E must have multiplicative or potentially multiplicative reduction at ℓ . It follows from Proposition 23(b) of [12] that E has multiplicative reduction over K at all primes above ℓ .

Fix a prime λ of K_∞ lying above ℓ , and let I be the inertia group for λ in S . The Tate parametrization shows that for every n , the group $E[p^n]^I$ contains a cyclic subgroup of order p^n . Since I fixes $K = \mathbf{Q}(\Psi, \Phi)$, we have $\Psi \subseteq E[p]^I$. On the other hand, since the ramification degree of ℓ in $\mathbf{Q}(E[p])/\mathbf{Q}$ is divisible by p , I acts nontrivially on $E[p]$, and so we have $E[p]^I = \Psi$. Hence $E[p^n]^I$ is cyclic of order p^n for every n . In particular, multiplication by p gives an I -equivariant isomorphism $E[p^2]^I/\Psi \xrightarrow{\sim} \Psi$. Therefore, we have I -equivariant isomorphisms

$$E'[p] = (E/\Psi)[p] \cong E[p^2]^I/\Psi \times E[p]/\Psi \cong \Psi \times \Phi.$$

Since I acts trivially on both Φ and Ψ , it acts trivially on $E'[p]$, so $\mathbf{Q}(E'[p])/K$ is unramified above ℓ . Since $[K : \mathbf{Q}]$ is prime to p , it follows that the ramification degree of ℓ in $\mathbf{Q}(E'[p])/\mathbf{Q}$ is prime to p . \square

Remark 5.5. Lemma 5.4 can also be proved by studying how the Tate period for E over \mathbf{Q}_ℓ changes under the isogeny $E \rightarrow E'$. The advantage of the above proof is that it also could be applied to the p -adic representations attached to modular forms, under suitable assumptions.

Lemma 5.6. *If $\psi\varphi^{-1}$ has order 2, then $p \equiv 3 \pmod{4}$ and $\psi\varphi^{-1} = \omega^{(p-1)/2}$.*

Proof. Since $\psi\varphi = \omega$ and φ has order dividing $p-1$, we have

$$(\psi\varphi^{-1})^{\frac{p-1}{2}} = (\omega\varphi^{-2})^{\frac{p-1}{2}} = \omega^{\frac{p-1}{2}}$$

Since ω has order $p-1$, we see that $(\psi\varphi^{-1})^{(p-1)/2}$ is nontrivial. If $\psi\varphi^{-1}$ is quadratic, we conclude that $(p-1)/2$ is odd and hence that $(\psi\varphi^{-1})^{(p-1)/2} = \psi\varphi^{-1}$. The lemma follows. \square

Proposition 5.7. *Suppose that $\psi\varphi^{-1}$ has order 2. Then E is p -exceptional if and only if for every prime $\ell \neq p$, the ramification degrees of ℓ in $\mathbf{Q}(E[p])/\mathbf{Q}$ and $\mathbf{Q}(E'[p])/\mathbf{Q}$ are both prime to p .*

Proof. Let $L = \mathbf{Q}(E[p])$ and $L' = \mathbf{Q}(E'[p])$. By Remark 5.2, L and L' are cyclic extensions of K of degree p .

Suppose first that E is p -exceptional, and $\ell \neq p$. By Lemma 5.4, the ramification degree of ℓ in at least one of L/\mathbf{Q} and L'/\mathbf{Q} is prime to p . But by Proposition 5.3 we have $L = L'$, so the ramification degrees of ℓ in L/\mathbf{Q} and L'/\mathbf{Q} must both be prime to p .

Now suppose that for every prime $\ell \neq p$, the ramification degrees of ℓ in L/\mathbf{Q} and L'/\mathbf{Q} are both prime to p . Let $\xi = \psi\varphi^{-1}$. Since $\xi = \xi^{-1}$, the action of $\text{Gal}(K/\mathbf{Q})$ on both $\text{Gal}(L/K)$ and $\text{Gal}(L'/K)$ is given by ξ . Let F denote the quadratic extension of \mathbf{Q} corresponding to ξ . Then $F \subset K$, and $F = \mathbf{Q}(\sqrt{-p})$ by Lemma 5.6. We can regard ξ as a character of $\text{Gal}(F/\mathbf{Q})$. Since $\text{Gal}(K/F)$ acts trivially on $\text{Gal}(L/K)$ and $\text{Gal}(L'/K)$, it follows that L and L' are abelian extensions of F . Since $[K:F]$ is prime to p , there exist cyclic extensions J and J' of F of degree p such that $L = KJ$ and $L' = KJ'$. Now $\text{Gal}(F/\mathbf{Q})$ acts on both $\text{Gal}(J/F)$ and $\text{Gal}(J'/F)$ by the character ξ , so J and J' are dihedral extensions of \mathbf{Q} of degree $2p$.

By our assumption on the ramification of primes $\ell \neq p$, the extensions J/F and J'/F can ramify only at primes above p . The class number of $F = \mathbf{Q}(\sqrt{-p})$ is not divisible by p (because it is less than p ; see for example [3, page 365]). Hence, by class field theory, one sees that F has only one cyclic extension of degree p that is both unramified outside of p and dihedral over \mathbf{Q} . (This extension is the first layer of the so-called ‘‘anticyclotomic’’ \mathbf{Z}_p -extension of F .) Therefore, we must have $J = J'$, and hence $L = L'$. Now E is p -exceptional by Proposition 5.3. \square

Recall that $\Delta_{\min}(E)$ and $\Delta_{\min}(E')$ are the discriminants of minimal integral models for E and E' , respectively.

Proposition 5.8. *Assume that $\psi\varphi^{-1}$ has order 2 and that E has semistable reduction at all primes ℓ dividing the conductor of E , except possibly $\ell = p$. Then E is p -exceptional if and only if $\Delta_{\min}(E')/\Delta_{\min}(E) = p^a w^p$ for some $a \in \mathbf{Z}$ and $w \in \mathbf{Q}^\times$.*

Proof. Suppose first that $\ell \neq p$ is a prime where E has split multiplicative reduction. Then E is a Tate curve over \mathbf{Q}_ℓ . Let $q_{E,\ell}$ denote the corresponding Tate period for E . Then we have

$$\mathbf{Q}_\ell(E[p]) = \mathbf{Q}_\ell(\mu_p, \sqrt[p]{q_{E,\ell}})$$

and therefore the ramification degree for ℓ in $\mathbf{Q}(E[p])$ is divisible by p if and only if $\text{ord}_\ell(q_{E,\ell}) \not\equiv 0 \pmod{p}$. Furthermore, we have (Proposition VII.5.1(b) of [14])

$$\text{ord}_\ell(\Delta_{\min}(E)) = -\text{ord}_\ell(j(E)) = \text{ord}_\ell(q_{E,\ell}).$$

Thus, the ramification degree for ℓ in $\mathbf{Q}(E[p])/\mathbf{Q}$ is divisible by p if and only if $\text{ord}_\ell(\Delta_{\min}(E))$ is not divisible by p . This criterion is also valid if E has nonsplit multiplicative reduction at ℓ , since both the ramification degree for ℓ in $\mathbf{Q}(E[p])$ and the power of ℓ dividing $\Delta_{\min}(E)$ are unchanged by twisting E by a quadratic character that is unramified at ℓ .

By Lemma 5.4, at least one of the integers $\text{ord}_\ell(\Delta_{\min}(E))$, $\text{ord}_\ell(\Delta_{\min}(E'))$ is divisible by p . Therefore, both are divisible by p if and only if their difference is divisible by p . Now apply Proposition 5.7. \square

6. THE IMAGE OF $\rho_{E,7}$

We continue to assume that E is an elliptic curve over \mathbf{Q} with a \mathbf{Q} -isogeny of prime degree $p \geq 7$. We keep the rest of the notation of §5 as well. Note that since $\psi\varphi = \omega$, we have that $\psi\varphi^{-1}$ has order 2 if and only if $\psi^4 = \omega^2$.

By Theorem 1.3 ([4, Theorem 1]), if E is p -exceptional then $\psi\varphi^{-1}$ has order 2. If $p > 7$ then Proposition 1.4 ([4, Remark 4.2.1]) says that if $\psi\varphi^{-1}$ has order 2 then E has CM by $\mathbf{Q}(\sqrt{-p})$. If E has CM, then $\text{image}(\rho_{E,p})$ is a p -adic Lie group of dimension 2, and so it cannot contain a Sylow pro- p subgroup of $\text{Aut}(T_p(E))$. Thus for $p > 7$, an elliptic curve over \mathbf{Q} is p -exceptional if and only if E has CM by $\mathbf{Q}(\sqrt{-p})$.

However, for $p = 7$, it is possible for $\psi\varphi^{-1}$ to have order 2 even if E does not have complex multiplication. For example, for every $v \in \mathbf{Q}$, the curve B_v of §4 has a \mathbf{Q} -isogeny of degree 7 with $\psi = \omega^5$ and $\psi\varphi^{-1} = \omega^3$ of order 2. In this section we will use Proposition 5.8 to study 7-exceptional curves. We assume from now on that $p = 7$.

For $j \in \mathbf{Z}$, let C_j denote the curve

$$(13) \quad w^7 = 7^j \left(\frac{v^3 - 2v^2 - v + 1}{v^3 - v^2 - 2v + 1} \right).$$

Lemma 6.1. (i) For every $j \in \mathbf{Z}$, the curve C_j has genus 12.
(ii) If $7 \nmid j$, then $C_j(\mathbf{Q}) = \emptyset$.

Proof. The curves C_j are degree 7 covers of $\mathbf{P}^1(\mathbf{C})$ with six branch points, each with ramification degree 7, so by the Riemann-Hurwitz formula they have genus 12.

To prove (ii), we will show that $C_j(\mathbf{Q}_7) = \emptyset$ if $7 \nmid j$. The map $(v, w) \mapsto (1/v, 1/w)$ defines an isomorphism from C_j to C_{-j} . Since $C_j \cong C_{j'}$ if $j \equiv j' \pmod{7}$, it suffices to consider just $j = 1, 2$, and 3. Then if (v, w) is a point on C_j or C_{-j} defined over \mathbf{Q}_7 , and $v \in \mathbf{Z}_7$, then $w \in \mathbf{Z}_7^\times$; this follows immediately from Lemma 4.4(a,b), which is clearly valid even for $v \in \mathbf{Q}_7$. Thus, to show that $C_j(\mathbf{Q}_7)$ is empty, it suffices to show that neither of the equations

$$\begin{aligned} v^3 - 2v^2 - v + 1 &= 7^j w^7 (v^3 - v^2 - 2v + 1), \\ v^3 - v^2 - 2v + 1 &= 7^j w^7 (v^3 - 2v^2 - v + 1) \end{aligned}$$

has solutions $v, w \in \mathbf{Z}_7$. If $j = 2$ or 3, this follows from Lemma 4.4(a,b) since the powers of 7 on the two sides differ. If $j = 1$, then one finds easily that neither equation has a solution modulo 7^3 . \square

Recall the elliptic curve B_v defined by (8).

Lemma 6.2. *Suppose $v \in \mathbf{Q}$. Then the following are equivalent:*

- (i) $\rho_{B_v,7}(G_{\mathbf{Q}})$ does not contain a Sylow pro-7 subgroup of $\text{Aut}_{\mathbf{Z}_7}(T_7(B_v))$;
- (ii) there is a $w \in \mathbf{Q}$ such that $(v, w) \in C_0(\mathbf{Q})$.

Proof. By Proposition 4.7, B_v has multiplicative reduction at all primes of bad reduction different from 7. Thus we can apply Proposition 5.8 to B_v with $p = 7$ to conclude that

$$\begin{aligned} \text{Assertion (i)} &\iff \frac{\Delta_{\min}(B'_v)}{\Delta_{\min}(B_v)} \in 7^{\mathbf{Z}} \cdot (\mathbf{Q}^\times)^7 \\ &\iff \left(\frac{v^3 - 2v^2 - v + 1}{v^3 - v^2 - 2v + 1} \right)^6 \in 7^{\mathbf{Z}} \cdot (\mathbf{Q}^\times)^7 \\ &\iff \frac{v^3 - 2v^2 - v + 1}{v^3 - v^2 - 2v + 1} \in 7^{\mathbf{Z}} \cdot (\mathbf{Q}^\times)^7, \end{aligned}$$

the middle equivalence by Corollary 4.6(i). This in turn is equivalent to saying there is a point $(v, w) \in C_j(\mathbf{Q})$ for some j with $0 \leq j \leq 6$. But by Lemma 6.1(ii), $C_j(\mathbf{Q})$ is empty if $1 \leq j \leq 6$. This proves the lemma. \square

Theorem 6.3. *Suppose that E is an elliptic curve over \mathbf{Q} with a \mathbf{Q} -isogeny of degree 7. Then the following are equivalent:*

- (i) $\rho_{E,7}(G_{\mathbf{Q}})$ does not contain a Sylow pro-7 subgroup of $\text{Aut}_{\mathbf{Z}_7}(T_7(E))$;
- (ii) E is a quadratic twist of B_v for some $(v, w) \in C_0(\mathbf{Q})$.

Proof. Suppose that the image of $\rho_{E,7}$ does not contain a Sylow pro-7 subgroup of $\text{Aut}_{\mathbf{Z}_7}(T_7(E))$. By Theorem 1.3 ([4, Theorem 1]), $\psi\varphi^{-1}$ has order 2, so by Lemma 5.6 we have $\psi\varphi^{-1} = \omega^3$. Since $\psi\varphi = \omega$, we have $\psi^2 = \varphi^2 = \omega^4$. Let $\epsilon = \psi\omega$. Then ϵ is a quadratic character, $\psi = \omega^5\epsilon$, and $\varphi = \omega^2\epsilon$. Replacing E by its quadratic twist by ϵ , we may assume that $\psi = \omega^5$ and $\varphi = \omega^2$. By Theorem 4.1(i), we have that $E \cong B_v$ for some $v \in \mathbf{Q}$. Now the theorem follows from Lemma 6.2. \square

Remark 6.4. The curve C_0 has 6 rational points that we know, namely the ones with $v \in \{0, 1, \infty, -1, 2, 1/2\}$. The corresponding elliptic curves B_v are the two isogenous CM curves of conductor 49. We would like to know that these are *all* the rational points on C_0 , and then it would follow by Theorem 6.3 that $\rho_{E,7}(G_{\mathbf{Q}})$ contains a Sylow pro-7 subgroup of $\text{Aut}(T_7(E))$ for *every* non-CM elliptic curve over \mathbf{Q} with a cyclic subgroup of order 7. We have so far been unable to prove this. However, we will show in the next section (Theorem 6.10) that $|C_0(\mathbf{Q})| = 6$ or 12, and we will deduce that up to quadratic twist, there is at most one other pair of 7-isogenous elliptic curves E (in addition to the CM pair) such that $\rho_{E,7}(G_{\mathbf{Q}})$ does not contain a Sylow pro-7 subgroup of $\text{Aut}(T_7(E))$.

Corollary 6.5. *If $v \in \mathbf{Q}$ and $\rho_{B_v,7}(G_{\mathbf{Q}})$ does not contain a Sylow pro-7 subgroup of $\text{Aut}_{\mathbf{Z}_7}(T_7(B_v))$, then v satisfies one of the following congruences:*

$$v \equiv 0, 1, \infty, -1, 1/2, \text{ or } 2 \pmod{49}.$$

Furthermore, $j(B_v) \equiv -15^3$ or $255^3 \pmod{49}$.

Proof. If $v \in \mathbf{Q}$ and the image of $\rho_{B_v,7}$ does not contain a Sylow pro-7 subgroup of $\text{Aut}_{\mathbf{Z}_7}(T_7(B_v))$, then by Lemma 6.2 there is a $w \in \mathbf{Q}$ such that $(v, w) \in C_0(\mathbf{Q})$. Computing modulo 49, it is straightforward to check that all points $(v, w) \in C_0(\mathbf{Q}_7)$ satisfy $v \equiv 0, 1, \infty, -1, 1/2, \text{ or } 2 \pmod{49}$ and $w \equiv \pm 1 \pmod{49}$. The congruence for $j(B_v)$ now follows directly from (10). \square

The curve

$$C_0 \quad : \quad w^7 = \frac{v^3 - 2v^2 - v + 1}{v^3 - v^2 - 2v + 1}.$$

of (13) has a nonsingular model $C \subset \mathbf{P}^1 \times \mathbf{P}^1$ with coordinates $((v : u), (w : z))$ (that we will abbreviate as (v, w)) given by

$$w^7(v^3 - v^2u - 2vu^2 + u^3) = z^7(v^3 - 2v^2u - vu^2 + u^3),$$

which has good reduction outside of 7. By Theorem 6.3, we wish to determine $C(\mathbf{Q})$.

Definition 6.6. Let $\iota, \eta \in \text{Aut}(C)$ be the automorphisms defined by

$$\iota(v, w) = (1 - v, 1/w), \quad \eta(v, w) = (1/(1 - v), w)$$

and let Σ be the group they generate. Then ι has order 2, η has order 3, and $\Sigma \cong S_3$. Clearly Σ preserves $C(\mathbf{Q})$. Let

$$Z = \{(0, 1), (1, 1), (\infty, 1), (-1, -1), (2, -1), (1/2, -1)\} \subset C(\mathbf{Q}).$$

Note that Z is partitioned into two orbits of length 3 under the action of Σ , as pointed out in Remark 4.8.

Lemma 6.7. *The action of Σ partitions $C(\mathbf{Q}) - Z$ into disjoint orbits of length 6.*

Proof. Suppose $(v', w') \in C(\mathbf{Q}) - Z$, and let $H \subset \Sigma$ be the stabilizer of (v', w') . We will show that H is trivial.

If $|H|$ is divisible by 3, then $\eta \in H$, so $v' = 1/(1 - v')$. But then v' is a primitive sixth root of unity, which is impossible since $v' \in \mathbf{Q}$.

If $|H|$ is even, then (v', w') is fixed by an element of order 2 in Σ . The elements of order 2 in Σ are the maps

$$(v, w) \mapsto \begin{cases} (1/v, 1/w), \\ (1 - v, 1/w), \\ (v/(v - 1), 1/w). \end{cases}$$

Thus we must have either $v' = 1/v'$, or $v' = 1 - v'$, or $v' = v'/(v' - 1)$, i.e., either $v' \in \{1, -1\}$, or $v' \in \{1/2, \infty\}$, or $v' \in \{2, 0\}$, respectively. But then $(v', w') \in Z$.

Therefore H is trivial, and the lemma follows. \square

The next result will be used to prove Theorems 6.9 and 7.7 below.

Corollary 6.8. *There is a positive integer N such that:*

- (i) $|C(\mathbf{Q})| = 6N$, and
- (ii) every fiber of the reduction map $C(\mathbf{Q}) \rightarrow C(\mathbf{F}_2)$ has $2N$ points.

Proof. Let $N - 1$ be the number of orbits of Σ acting on $C(\mathbf{Q}) - Z$. By Lemma 6.7 we have $|C(\mathbf{Q})| = 6N$.

The Σ -action on C commutes with the reduction map $C(\mathbf{Q}) \rightarrow C(\mathbf{F}_2)$, and Σ acts transitively on the set $C(\mathbf{F}_2) = \{(0, 1), (1, 1), (\infty, 1)\}$. Hence all fibers of the reduction map have the same number of points, and (ii) follows. \square

We expect that $C(\mathbf{Q}) = Z$, but we will prove only the following.

Theorem 6.9. *Either $C(\mathbf{Q}) = Z$, or $C(\mathbf{Q})$ is the disjoint union of Z and the Σ -orbit of a single point. Moreover, $|C(\mathbf{Q})| = 6$ or 12 .*

We will prove Theorem 6.9 using the method of Chabauty, as made explicit by Stoll in [16]. Before that we will deduce the following consequence.

Theorem 6.10. *Suppose E is an elliptic curve over \mathbf{Q} with a \mathbf{Q} -rational subgroup of order 7, and $\rho_{E,7}(G_{\mathbf{Q}})$ does not contain a Sylow pro-7 subgroup of $\text{Aut}_{\mathbf{Z}_7}(T_7(E))$.*

- (i) *If $C(\mathbf{Q}) = Z$, then E has CM, i.e., E is a quadratic twist of one of the elliptic curves of conductor 49.*
- (ii) *If $(v, w) \in C(\mathbf{Q}) - Z$, then either E has CM or E is a quadratic twist of B_v or of B_{1-v} .*

Proof. By Theorem 6.3, E is a quadratic twist of B_v for some $(v, w) \in C(\mathbf{Q})$. If $v \in \{0, 1, \infty\}$, then B_v is isomorphic to the curve 49A1 in Cremona's tables [2]. If $v \in \{2, 1/2, -1\}$, then B_v is isomorphic to the curve 49A2.

Suppose $C(\mathbf{Q}) - Z$ is nonempty, and $(v, w) \in C(\mathbf{Q}) - Z$. Then $C(\mathbf{Q}) - Z = \Sigma \cdot (v, w)$ by Theorem 6.9. But for every $(v', w') \in C(\mathbf{Q}) - Z$ we have either $v' \in \{v, \eta(v), \eta^2(v)\}$ or $v' \in \{1-v, \eta(1-v), \eta^2(1-v)\}$, so $B_{v'}$ is isomorphic to B_v or B_{1-v} , respectively, by Lemma 3.7. \square

Corollary 6.11. *Suppose E is an elliptic curve over \mathbf{Q} with a \mathbf{Q} -rational subgroup of order 7, and $\rho_{E,7}(G_{\mathbf{Q}})$ does not contain a Sylow pro-7 subgroup of $\text{Aut}_{\mathbf{Z}_7}(T_7(E))$.*

- (i) *If $C(\mathbf{Q}) = Z$, then $j(E) \in \{-15^3, 255^3\}$.*
- (ii) *If $(v, w) \in C(\mathbf{Q}) - Z$, then $j(E) \in \{-15^3, 255^3, j(B_v), j(B_{1-v})\}$.*

Proof. This is a restatement of Theorem 6.10 since the curves of conductor 49 have j -invariants -15^3 and 255^3 . \square

7. PROOF OF THEOREM 6.9

Let J be the jacobian of C . The first step in bounding $C(\mathbf{Q})$ is to compute the rank of $J(\mathbf{Q})$. We will do this following the method described by Poonen and Schaefer in [11]. To keep our notation as close as possible to theirs, we will replace C by the (birationally) isomorphic curve

$$X : y^7 = (x^3 - 2x^2 - x + 1)(x^3 - x^2 - 2x + 1)^6.$$

Let ζ be a primitive 7-th root of unity, $k = \mathbf{Q}(\zeta)$, $\mathcal{O} = \mathbf{Z}[\zeta]$, and $\pi = \zeta - 1 \in \mathcal{O}$, a generator of the prime ideal of \mathcal{O} above 7. We identify \mathcal{O} with a subring of $\text{End}_k(J)$ by sending ζ to the automorphism of J induced by the automorphism $(x, y) \mapsto (x, \zeta y)$ of X . We will use [11] to compute an upper bound for the size of $J(k)/\pi J(k)$.

Define

$$\begin{aligned} f(x) &= (x^3 - 2x^2 - x + 1)(x^3 - x^2 - 2x + 1)^6, \\ f_0(x) &= (x^3 - 2x^2 - x + 1)(x^3 - x^2 - 2x + 1). \end{aligned}$$

A calculation in PARI/GP shows that the roots of $x^3 - 2x^2 - x + 1$ are $\alpha_i := 1 + \zeta^i + \zeta^{-i} \in k$ for $1 \leq i \leq 3$, and the roots of $x^3 - x^2 - 2x + 1$ are $\alpha_i := -\zeta^i - \zeta^{-i} \in k$ for $4 \leq i \leq 6$. In particular, f and f_0 factor into linear factors in $k[x]$.

Suppose K is a field containing k . Let $\text{Div}(X/K)$ denote the group of K -rational divisors on X , i.e., the group of \mathbf{Z} -linear combinations of points in $X(\bar{K})$ that are fixed by G_K , let $\text{Div}^0(X/K)$ denote the subgroup of divisors of degree zero, and let $\text{Pic}^0(X/K) = \text{Div}^0(X/K)/P(X/K)$ where $P(X/K)$ is the group of divisors of K -rational functions on X (i.e., the principal divisors). Since $X(k)$ is nonempty,

there is a natural isomorphism $\text{Pic}^0(X/K) \cong J(K)$, and we will identify these two groups.

If R is a (multiplicative) abelian group, let

$$V(R) := (R/R^7)^6/(R/R^7)$$

where R^7 denotes seventh powers in R , and R/R^7 is embedded diagonally in the direct product $(R/R^7)^6$.

In [11, §5], Poonen and Schaefer define what they call the “ $(x - T)$ map” for every field K containing k :

$$(x - T)_K : J(K)/\pi J(K) \longrightarrow V(K^\times).$$

This map is characterized as follows. If $D = \sum_P n_P P \in \text{Div}^0(X)$ is supported on points $P \in X(\bar{K})$ with x -coordinate $x(P) \notin \{\alpha_i : 1 \leq i \leq 6\} \cup \{\infty\}$, then

$$(x - T)_K(D) := \prod_P ((x(P) - \alpha_1)^{n_P}, \dots, (x(P) - \alpha_6)^{n_P}).$$

Lemma 7.1 (Poonen-Schaefer [11]). *Suppose K is a field containing k , and $P = (x(P), y(P)) \in X(K)$. Let ∞ denote the rational point with $x = \infty$, i.e., the point corresponding to $(\infty, 1)$ on the nonsingular model C of X . If $x(P) \notin \{\alpha_i : 1 \leq i \leq 6\} \cup \{\infty\}$ then*

$$(x - T)_K(P - \infty) = (x(P) - \alpha_1, \dots, x(P) - \alpha_6).$$

Proof. This follows from [11, Proposition 5.1]. □

There is a natural localization map from $V(k^\times)$ to $V(k_\pi^\times)$, where k_π is the completion of k at π . Let N be the “weighted norm” map from §6 of [11]:

$$N : V(k^\times) \rightarrow k^\times/(k^\times)^7, \quad (z_1, z_2, z_3, z_4, z_5, z_6) \mapsto z_1 z_2 z_3 (z_4 z_5 z_6)^6.$$

Theorem 7.2 (Poonen-Schaefer [11]). *In the commutative diagram*

$$\begin{array}{ccc} J(k)/\pi J(k) & \xrightarrow{(x-T)_k} & V(k^\times) \\ \downarrow & & \downarrow \text{loc}_\pi \\ J(k_\pi)/\pi J(k_\pi) & \xrightarrow{(x-T)_{k_\pi}} & V(k_\pi^\times) \end{array}$$

the maps $(x - T)_k$ and $(x - T)_{k_\pi}$ are injective, and the image of $(x - T)_k$ is contained in

$$V(\mathcal{O}[1/\pi]^\times) \cap \ker(N) \cap \text{loc}_\pi^{-1}(\text{image}((x - T)_{k_\pi})).$$

Proof. That the maps are injective follows from [11, Theorem 11.3], since X has k -rational points and $f(x)$ factors into linear factors in $k[x]$.

Let U denote the image of $(x - T)_k$. Then $U \subseteq V(\mathcal{O}[1/\pi]^\times)$ by [11, Proposition 12.4] since J has good reduction outside of 7, and $U \subseteq \ker(N)$ by [11, Proposition 12.1]. The commutativity of the diagram shows that $U \subseteq \text{loc}_\pi^{-1}(\text{image}((x - T)_{k_\pi}))$. □

Lemma 7.3 (Poonen-Schaefer [11]). *We have*

- (i) $\dim_{\mathbf{F}_7} J(k)[\pi] = 4$,
- (ii) $\dim_{\mathbf{F}_7} J(k_\pi)/\pi J(k_\pi) = 16$.

Proof. Assertion (i) is [11, Lemma 12.9], since $f(x)$ factors into linear factors in $k[x]$, of which 6 are distinct.

Similarly, [11, Lemma 12.9] shows that $\dim_{\mathbf{F}_7} J(k_\pi)[\pi] = 4$, and then [11, Lemma 12.10] shows that

$$\dim_{\mathbf{F}_7} J(k_\pi)/\pi J(k_\pi) = g + \dim_{\mathbf{F}_7} J(k_\pi)[\pi] = 12 + 4 = 16,$$

where $g = 12$ is the genus of X . \square

Theorem 7.4. $\text{rank}_{\mathcal{O}} J(k) \leq 6$.

Proof. We will use Theorem 7.2 to bound the \mathcal{O} -rank of $J(k)$. All of the terms in Theorem 7.2 are \mathbf{F}_7 -vector spaces, and we need to compute them explicitly.

It follows from Theorem 5.1 of Chapter 3 of [8], and the fact that $\mathbf{Q}(\zeta + \zeta^{-1})$ has class number one, that $\mathcal{O}[1/\pi]^\times$ is generated by the roots of unity, the cyclotomic units, and π . Thus an \mathbf{F}_7 -basis of $\mathcal{O}[1/\pi]^\times/(\mathcal{O}[1/\pi]^\times)^7$ is given by $\{\zeta, 1 + \zeta, 1 + \zeta + \zeta^2, \pi\}$.

We need to compute the image of $(x - T)_{k_\pi}$. By Theorem 7.2 and Lemma 7.3(ii), $\dim_{\mathbf{F}_7}(\text{image}((x - T)_{k_\pi})) = 16$. Using PARI/GP, we find points $Q_i = (x_i, y_i) \in X(k_\pi)$ for $1 \leq i \leq 6$ with x -coordinates:

$$\begin{aligned} x_1 &= 0, & x_2 &= -1, \\ x_3 &= 3 + 4\pi^2 + 5\pi^3 + \pi^4 + 4\pi^5 + 2\pi^6 + 6\pi^7 + 5\pi^8 + 5\pi^9 + 5\pi^{10}, \\ x_4 &= 3 + \pi^2 + 5\pi^3 + 5\pi^4 + 5\pi^5 + 5\pi^6 + 2\pi^8 + 5\pi^9 + \pi^{10}, \\ x_5 &= 3 + \pi^2 + 2\pi^4 + 4\pi^5 + 2\pi^6 + \pi^7 + 2\pi^8, \\ x_6 &= 3 + 2\pi^2 + 5\pi^3 + \pi^4 + 6\pi^7 + 2\pi^8 + 6\pi^9 + 2\pi^{10} \\ &\quad + 5\pi^{11} + 4\pi^{12} + 2\pi^{14} + 2\pi^{15} + 6\pi^{16} + \pi^{17}. \end{aligned}$$

Using PARI/GP and Lemma 7.1, we compute $(x - T)_{k_\pi}(\sigma(Q_i) - \infty)$ for $1 \leq i \leq 6$ and for all $\sigma \in \Sigma$, and we find that those values generate an \mathbf{F}_7 -subspace of $V(k_\pi^\times)$ of dimension 16. (We work inside the \mathbf{F}_7 -vector space $k_\pi^\times/(k_\pi^\times)^7$, using the basis

$$\{\pi, 1 + \pi, 1 + \pi^2, 1 + \pi^3, 1 + \pi^4, 1 + \pi^5, 1 + \pi^6, 1 + \pi^7\}.$$

It follows that we have found the full image of $(x - T)_{k_\pi}$.

Using the above information, a linear algebra computation in PARI/GP now shows that

$$\dim_{\mathbf{F}_7}(V(\mathcal{O}[1/\pi]^\times) \cap \ker(N) \cap \text{loc}_\pi^{-1}(\text{image}((x - T)_{k_\pi}))) = 10.$$

Therefore by Theorem 7.2 we have $\dim_{\mathbf{F}_7} J(k)/\pi J(k) \leq 10$. Since

$$\dim_{\mathbf{F}_7} J(k)/\pi J(k) = \text{rank}_{\mathcal{O}} J(k) + \dim_{\mathbf{F}_7} J(k)[\pi],$$

and $\dim_{\mathbf{F}_7} J(k)[\pi] = 4$ by Lemma 7.3(i), we conclude that $\text{rank}_{\mathcal{O}} J(k) \leq 6$. \square

Corollary 7.5. $\text{rank}_{\mathbf{Z}} J(\mathbf{Q}) \leq 6$.

Proof. This follows from Theorem 7.4 and [11, Lemma 13.4]. \square

Next we will use Corollary 7.5 and the method of Chabauty as described in [16] to bound the number of points in $C(\mathbf{Q})$.

If $x \in \{0, 1, \infty\}$, define $P_x := (x, 1) \in C(\mathbf{Q})$. Define divisors on C :

$$D_x = \sum_{\zeta \in \mu_7} (x, \zeta) \text{ for } x \in \{0, 1, \infty\}, \quad B_1 = \sum_{i=1}^3 (\alpha_i, 0), \quad B_2 = \sum_{i=4}^6 (\alpha_i, \infty).$$

We have the following table of functions on C and their divisors (where we abuse notation, writing v and w for the functions v/u and w/z on C , corresponding to the functions v and w on C_0):

g	principal divisor (g)
v	$D_0 - D_\infty$
$v - 1$	$D_1 - D_\infty$
w	$B_1 - B_2$
$w - 1$	$P_0 + P_1 + P_\infty - B_2$
$w^7 - 1$	$D_0 + D_1 + D_\infty - 7B_2$

If L is a field of characteristic different from 7, let $\Omega(C/L)$ denote the L -vector space of holomorphic differentials on C/L . If $\omega \in \Omega(C/L)$ let (ω) denote the divisor of ω , and if $D \in \text{Div}(C/L)$ let

$$\Omega(C/L, D) = \{\omega \in \Omega(C/L) : (\omega) \geq D\}.$$

Lemma 7.6. *Suppose L is a field of characteristic different from 7. A basis for $\Omega(C/L)$ is given by*

$$\omega_{1,j} := \frac{(w^7 - 1)(w - 1)^j}{vw^6} dv, \quad \omega_{2,j} := \frac{(w^7 - 1)(w - 1)^j}{(v - 1)w^6} dv, \quad 0 \leq j \leq 5.$$

If $0 \leq m \leq 5$, then a basis for $\Omega(C/L, m(P_0 + P_1 + P_\infty))$ is given by

$$\omega_{1,j}, \omega_{2,j}, \quad m \leq j \leq 5.$$

Proof. We first compute the divisor of the differential dv . The function v has (simple) poles at each of the 7 points $\{(\infty, \zeta) : \zeta \in \mu_7\}$, and no other poles. Hence $\text{ord}_{(\infty, \zeta)}(dv) = -2$, and $\text{ord}_P(dv) \geq 0$ for all other points P . If α is a root of $v^3 - 2v^2 - v + 1$, then the equation for C shows that $\text{ord}_{(\alpha, 0)}(v - \alpha)$ is a (positive) multiple of 7. Since the polar divisor of v is D_∞ , we conclude that $\text{ord}_{(\alpha, 0)}(v - \alpha) = 7$, and

$$\text{ord}_{(\alpha, 0)}(dv) = \text{ord}_{(\alpha, 0)}(d(v - \alpha)) = 6.$$

Similarly, if β is a root of $v^3 - v^2 - 2v + 1$ then $\text{ord}_{(\beta, \infty)}(dv) = 6$. Since the divisor (dv) has degree $2g - 2 = 22$, we conclude that

$$(dv) = 6B_1 + 6B_2 - 2D_\infty.$$

It now follows from the table (14) that the differentials $\omega_{i,j}$ with $1 \leq i \leq 2$ and $0 \leq j \leq 5$ are holomorphic. Explicitly, their divisors are given by

$$(15) \quad \begin{aligned} (\omega_{1,j}) &= D_1 + (5 - j)B_2 + j(P_0 + P_1 + P_\infty), \\ (\omega_{2,j}) &= D_0 + (5 - j)B_2 + j(P_0 + P_1 + P_\infty). \end{aligned}$$

Since C has genus 12, to show that these differentials form a basis of $\Omega(C/L)$ we only need to show that they are linearly independent over L . But a nontrivial linear relation among them would be equivalent to a nontrivial polynomial relation

$$(v - 1)g_1(w) = vg_2(w)$$

with polynomials $g_1, g_2 \in L[w]$ of degree at most 5, and this is impossible since the degree of $L(v, w)/L(v)$ is 7.

Suppose $\omega = \sum_{j=0}^5 a_j \omega_{1,j} + \sum_{j=0}^5 b_j \omega_{2,j}$, with $a_j, b_j \in L$. By (15) we have

$$\begin{aligned} \text{ord}_{P_0}(\omega_{1,j}) &= \text{ord}_{P_1}(\omega_{2,j}) = \text{ord}_{P_\infty}(\omega_{1,j}) = \text{ord}_{P_\infty}(\omega_{2,j}) = j, \\ \text{ord}_{P_1}(\omega_{1,j}) &= \text{ord}_{P_0}(\omega_{2,j}) = j + 1. \end{aligned}$$

Let n be minimal such that $(a_n, b_n) \neq (0, 0)$. If $a_n \neq 0$, it then follows that $\text{ord}_{P_0}(\omega) = n$; if $b_n \neq 0$, it then follows that $\text{ord}_{P_1}(\omega) = n$. In particular we have

$$(\omega) \geq m(P_0 + P_1 + P_\infty) \iff a_j = b_j = 0 \text{ for } 0 \leq j < m.$$

This proves the final assertion of the lemma. \square

Theorem 7.7. $|C(\mathbf{Q})| \leq 12$.

Proof. Suppose $|C(\mathbf{Q})| > 12$. Then by Corollary 6.8 we have $|C(\mathbf{Q})| \geq 18$ and there are at least six points of $C(\mathbf{Q})$ reducing to each of the three points of $C(\mathbf{F}_2)$. We will use Stoll's version [16] of the method of Chabauty to show this is impossible.

Let $\Omega(C/\mathbf{Z}_2)$ be the \mathbf{Z}_2 -span of the differentials $\omega_{i,j}$ with $1 \leq i \leq 2$ and $0 \leq j \leq 5$. With J denoting the jacobian of C , consider the bilinear pairing

$$J(\mathbf{Q}_2)/J(\mathbf{Q}_2)_{\text{tors}} \times \Omega(C/\mathbf{Z}_2) \rightarrow \mathbf{Q}_2$$

of free \mathbf{Z}_2 -modules of rank 12 with trivial left and right kernel that is used on p. 1210 of [16]. Let $V \subset \Omega(C/\mathbf{Z}_2)$ be the orthogonal complement under this pairing of (the closure of) $J(\mathbf{Q}) \subset J(\mathbf{Q}_2)$. By Corollary 7.5 we have $\text{rank}_{\mathbf{Z}} J(\mathbf{Q}) \leq 6$, so $\text{rank}_{\mathbf{Z}_2}(V) \geq 6$.

Let $\tilde{V} \subset \Omega(C/\mathbf{F}_2)$ be the image of V under the (surjective) reduction map $\text{red}_2 : \Omega(C/\mathbf{Z}_2) \rightarrow \Omega(C/\mathbf{F}_2)$. Since $\text{rank}_{\mathbf{Z}_2}(\Omega(C/\mathbf{Z}_2)) = 12 = \dim_{\mathbf{F}_2}(\Omega(C/\mathbf{F}_2))$, we have $\ker(\text{red}_2) = 2\Omega(C/\mathbf{Z}_2)$. Since $\Omega(C/\mathbf{Z}_2)/V$ is torsion-free, we have $2V = V \cap 2\Omega(C/\mathbf{Z}_2) = \ker(\text{red}_2|_V)$. Thus $\tilde{V} \cong V/2V$, so $\dim_{\mathbf{F}_2}(\tilde{V}) = \text{rank}_{\mathbf{Z}_2}(V) \geq 6$.

Suppose that $x \in \{0, 1, \infty\}$ and $\omega \in \tilde{V}$. Since (by our assumption that $|C(\mathbf{Q})| > 12$) there are at least six points of $C(\mathbf{Q})$ that reduce to $P_x \in C(\mathbf{F}_2)$, it follows from Proposition 6.3 of [16] that

$$6 \leq 1 + \text{ord}_{P_x}(\omega) + \delta(2, \text{ord}_{P_x}(\omega))$$

where $\delta(2, n)$ is defined explicitly on p. 1209 of [16]. One checks easily that $\delta(2, 0) = \delta(2, 2) = 1$ and $\delta(2, 1) = \delta(2, 3) = 0$. We conclude that

$$\text{ord}_{P_x}(\omega) \geq 4 \quad \text{for every } x \in \{0, 1, \infty\} \text{ and every } \omega \in \tilde{V}.$$

In other words, we have $\tilde{V} \subset \Omega(C/\mathbf{F}_2, 4(P_0 + P_1 + P_\infty))$, so in particular

$$\dim_{\mathbf{F}_2}(\Omega(C/\mathbf{F}_2, 4(P_0 + P_1 + P_\infty))) \geq \dim_{\mathbf{F}_2}(\tilde{V}) \geq 6.$$

But by Lemma 7.6, $\dim_{\mathbf{F}_2}(\Omega(C/\mathbf{F}_2, 4(P_0 + P_1 + P_\infty))) = 4$. This contradiction shows that $|C(\mathbf{Q})| \leq 12$. \square

Theorem 6.9 follows directly from Theorem 7.7 and Lemma 6.7.

REFERENCES

- [1] A. Bostan, F. Morain, B. Salvy, É. Schost, Fast algorithms for computing isogenies between elliptic curves, *Math. Comp.* **77** (2008), 1755–1778.
- [2] J. Cremona, Algorithms for modular elliptic curves, Cambridge University Press (1992).
- [3] G. L. Dirichlet, Sur l’usage des séries infinies dans la théorie des nombres, *J. Reine Angew. Math.* **18** (1938), 259–274; Werke I (1889), 357–370.
- [4] R. Greenberg, Galois properties of elliptic curves with an isogeny, preprint, <http://www.math.washington.edu/~greenber/GalProp.pdf>.
- [5] M. A. Kenku, The modular curves $X_0(169)$ and rational isogeny, *J. London Math. Soc.* **22** (1981), 239–244.
- [6] M. A. Kenku, On the modular curves $X_0(125)$, $X_1(25)$, and $X_1(49)$, *J. London Math. Soc.* **23** (1981), 415–427.
- [7] D. Kubert, Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc.* **33** (1976), 193–237.
- [8] S. Lang, Cyclotomic fields, Graduate Texts in Mathematics, Vol. 59, Springer-Verlag, New York-Heidelberg, 1978.
- [9] G. Ligozat, Courbes modulaires de genre 1, *Bull. Soc. Math. France, Mémoire* **43** (1975), 1–80.
- [10] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–162.
- [11] B. Poonen, E. F. Schaefer, Explicit descent for Jacobians of cyclic covers of the projective line, *J. Reine Angew. Math.* **488** (1997), 141–188.
- [12] J-P. Serre, Propriétés galoisiennes des points d’ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.
- [13] J-P. Serre, J. Tate, Good reduction of abelian varieties, *Ann. of Math. (2)* **88** (1968), 492–517.
- [14] J. Silverman, The arithmetic of elliptic curves, *Grad. Texts in Math.* **106**, Springer, New York, 1986.
- [15] J. Silverman, Advanced topics in the arithmetic of elliptic curves, *Grad. Texts in Math.* **151**, Springer, New York, 1994.
- [16] M. Stoll, Independence of rational points on twists of a given curve, *Compos. Math.* **142** (2006), 1201–1214.
- [17] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris Sér. A-B* **273** (1971), A238–A241.
- [18] L. Washington, Abelian number fields of small degree, in Algebra and Topology (Taejon, 1990), Korea Adv. Inst. Sci. Tech., Taejon (1990), 63–78.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WASHINGTON, SEATTLE, WA 98195, USA
E-mail address: greenber@math.washington.edu

DEPARTMENT OF MATHEMATICS, UC IRVINE, IRVINE, CA 92697, USA
E-mail address: krubin@math.uci.edu

DEPARTMENT OF MATHEMATICS, UC IRVINE, IRVINE, CA 92697, USA
E-mail address: asilverb@math.uci.edu