Title

On elliptic curves with an isogeny of degree 7

Journal

American Journal of Mathematics, 136(1)

ISSN

0002-9327

Authors

Greenberg, R
Rubin, K
Silverberg, A
et al.

Publication Date

2014

DOI

10.1353/ajm.2014.0005

Peer reviewed

ON ELLIPTIC CURVES WITH AN ISOGENY OF DEGREE 7

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

ABSTRACT. We show that if E is an elliptic curve over $\mathbf{Q}$ with a $\mathbf{Q}$-rational isogeny of degree 7, then the image of the 7-adic Galois representation attached to E is as large as allowed by the isogeny, except for the curves with complex multiplication by $\mathbf{Q}(\sqrt{-7})$.

The analogous result with 7 replaced by a prime $p > 7$ was proved by the first author in [8]. The present case $p = 7$ has additional interesting complications. We show that any exceptions correspond to the rational points on a certain curve of genus 12. We then use the method of Chabauty to show that the exceptions are exactly the curves with complex multiplication.

As a by-product of one of the key steps in our proof, we determine exactly when there exist elliptic curves over an arbitrary field k of characteristic not 7 with a k-rational isogeny of degree 7 and a specified Galois action on the kernel of the isogeny, and we give a parametric description of such curves.

1. Introduction

Suppose that E is an elliptic curve defined over $\mathbf{Q}$, p is a rational prime, $T_p(E)$ is the p-adic Tate module of E, and $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Then there is 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 $\mathrm{GL}_2(\mathbf{Z}_p)$. Serre [20] showed that if E does not have complex multiplication (CM), then $\rho_{E,p}(G_{\mathbf{Q}})$ has finite index in $\mathrm{Aut}(T_p(E))$, and $\rho_{E,p}$ is surjective for all but finitely many primes p.

Suppose now that E has an isogeny of degree p that is defined over $\mathbf{Q}$ (in other words, E has a $\mathbf{Q}$-rational p-isogeny). Mazur [15] showed that p is then in the finite set $\{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$, and if further E is non-CM, then $p \in \{2, 3, 5, 7, 11, 13, 17, 37\}$. The kernel of the isogeny is a $\mathbf{Q}$-rational subgroup Ψ of $E(\bar{\mathbf{Q}})$ of order p. Since $\mathrm{Aut}(\Psi) \cong \mathbf{F}_p^\times$, the action of $G_{\mathbf{Q}}$ on Ψ is given by a homomorphism $\psi : G_{\mathbf{Q}} \to \mathbf{F}_p^\times$. We refer to ψ as the *character* of the isogeny.

The isogeny and the corresponding character ψ put an obvious constraint on the image of the map $\rho_{E,p}$. In particular, $\rho_{E,p}$ cannot be surjective. If E has complex multiplication, then the additional endomorphisms of E put another constraint on the image of $\rho_{E,p}$. In that case, $\rho_{E,p}(G_{\mathbf{Q}})$ is a p-adic Lie group of dimension 2. 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 $\rho_{E,p}(G_{\mathbf{Q}})$ does not contain

2000 *Mathematics Subject Classification.* 11G05 (primary), 11D45, 11F80, 11G18, 11G30, 14G05 (secondary).

Key words and phrases. elliptic curves, isogeny, explicit families, Galois representations, method of Chabauty.

This material is based upon work supported by the National Science Foundation under grants DMS-0200785, DMS-0757807, and CNS-0831004.

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 $\mathrm{Aut}_{\mathbf{Z}_p}(T_p(E))$.

In other words, a curve E with a $\mathbf{Q}$-rational p-isogeny is p-exceptional if the index of $\rho_{E,p}(G_{\mathbf{Q}})$ in $\mathrm{Aut}_{\mathbf{Z}_p}(T_p(E))$ is divisible by p. If E is not p-exceptional, then 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 curve $\mathbf{Q}$-isogenous to E, and if $p > 2$ then so is any quadratic twist of E (see [8]). If E has CM, then as remarked above, E is p-exceptional.

If $p < 7$, then non-CM p-exceptional curves exist in abundance. Concerning the case $p = 5$, Theorem 2 in [8] describes completely the possible images of $\rho_{E,5}$. Its index cannot be divisible by 5^2 and is divisible by 5 if and only if E has a cyclic $\mathbf{Q}$-isogeny of degree 5^2 or two independent $\mathbf{Q}$-isogenies of degree 5.

In this paper we prove that the only 7-exceptional elliptic curves are the elliptic curves with complex multiplication by $\mathbf{Q}(\sqrt{-7})$. The method of proof is as follows. We begin with two results from [8]. Let $\omega : G_{\mathbf{Q}} \to \mathbf{F}_p^\times$ denote the cyclotomic character giving the action of $G_{\mathbf{Q}}$ on $\boldsymbol{\mu}_p$.

Theorem 1.2 ([8], 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 E is not p-exceptional.*

Proposition 1.3 ([8], 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 $p > 7$. However, Proposition 1.3 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 1.2, 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 2. Thus, replacing E by a quadratic twist if necessary, we may assume that $\psi = \omega^5$. In §2 we show that if E is 7-exceptional, then the ratio of the minimal discriminants of E and its 7-isogenous curve is of the form $7^s w^7$ with $w \in \mathbf{Q}$ and $s \in \mathbf{Z}$.

An explicit description of the family $\{B_v\}$ of elliptic curves over $\mathbf{Q}$ with a $\mathbf{Q}$-rational 7-isogeny with character $\psi = \omega^5$ follows from the results in §3. The curve E is isomorphic over $\mathbf{Q}$ to B_v for some $v \in \mathbf{Q}$. In Corollary 4.6 we show that for $v \in \mathbf{Q}$, the ratio of the minimal discriminants of B_v and its 7-isogenous curve is $7^{\pm 6} g(v)^6$, where $g(v) := (v^3 - 2v^2 - v + 1)/(v^3 - v^2 - 2v + 1)$. Thus the exceptional E's correspond to $\mathbf{Q}$-rational points on the genus 12 curves $C_j : w^7 = 7^j g(v)$. If $7 \nmid j$, then it turns out that C_j has no rational points over $\mathbf{Q}_7$, and hence none over $\mathbf{Q}$. Thus, the question is reduced to finding the $\mathbf{Q}$-rational points on the curve

$$C_0 : w^7 = (v^3 - 2v^2 - v + 1)/(v^3 - v^2 - 2v + 1).$$

In §7 we use the method of Chabauty to show that

$$C_0(\mathbf{Q}) = \{(0,1), (1,1), (\infty,1), (2,-1), (1/2,-1), (-1,-1)\},$$

and it follows that the only 7-exceptional elliptic curves E are the curves with $j(E) = -15^3$ or 255^3, i.e., the curves with complex multiplication by $\mathbf{Q}(\sqrt{-7})$.

Now suppose that k is a field of characteristic different from 7, that E is an elliptic curve defined over k, and that E has a k-rational isogeny of degree 7. Then the kernel of the isogeny is a k-rational subgroup Ψ of $E(k^{\mathrm{s}})$ of order 7, where k^{s} denotes a fixed separable closure of k. Let $G_k = \mathrm{Gal}(k^{\mathrm{s}}/k)$. Since $\mathrm{Aut}(\Psi) \cong \mathbf{F}_7^\times$, the action of G_k on Ψ is given by a homomorphism $\psi : G_k \to \mathbf{F}_7^\times$. Again, we refer to ψ as the *character* of the isogeny. For example, the character ψ is trivial if and only if $\Psi \subset E(k)$.

Now let $\psi : G_k \to \mathbf{F}_7^\times$ be a fixed homomorphism. In §3 we describe all elliptic curves defined over k that have a k-rational 7-isogeny with 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 $\mathbb{P}^1$, such that

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

See Theorems 3.6 and 3.10 for more precise statements. 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-rational 7-isogeny with character ψ (see Corollary 3.12). Note that these explicit families are of a different nature and are constructed differently from the explicit families of elliptic curves with a given mod N representation that were constructed earlier by the second and third authors of this paper.

The route we took to exactly determine $C_0(\mathbf{Q})$ is interesting in itself. (See Remark 6.8 and the appendix for more information.) By Faltings' proof of the Mordell Conjecture, $|C_0(\mathbf{Q})|$ is finite. An action of the group S_3 on C_0 shows that $|C_0(\mathbf{Q})|$ is divisible by 6. A descent argument (see §6) shows that the rank of the Jacobian J of C_0 is at most 6. In fact, the 6 known points generate a subgroup of $J(\mathbf{Q})$ of rank 4 and J is $\mathbf{Q}$-isogenous to the square of the Jacobian of a genus 6 curve D defined over $\mathbf{Q}$. Thus the rank of $J(\mathbf{Q})$ must be either 4 or 6.

A Chabauty argument at the prime 2 then gives that $|C_0(\mathbf{Q})|$ is either 6 or 12. At our request, Kiran Kedlaya and Jennifer Balakrishnan, with help from Joseph Wetherell, computed 2-adic Coleman integrals that we hoped would directly rule out the case $|C_0(\mathbf{Q})| = 12$. However, the computed dimensions worked out in such a way that one would need to show that the rank of $J(\mathbf{Q})$ were 4 to use this method to show $|C_0(\mathbf{Q})| \neq 12$.

This gave motivation to determine the rank of $J(\mathbf{Q})$, i.e., to determine the parity of the rank of the Jacobian $\mathrm{Jac}(D)$ of the genus 6 curve D. Using data and information provided by Balakrishnan, Sutherland, Kedlaya and the fourth author of this paper, Michael Rubinstein performed computations that gave convincing evidence that the analytic rank of $\mathrm{Jac}(D)$ is 3, so one expects $\mathrm{rank}(J(\mathbf{Q})) = 6$.

This gave motivation to find additional generators of $J(\mathbf{Q})$, which is done at the end of §6 below. We used these additional points to finish the proof that $|C_0(\mathbf{Q})| = 6$, using a Chabauty argument at the prime 5 (see §7).

We thank Bjorn Poonen for helpful conversations. We thank Jennifer Balakrishnan, Kiran Kedlaya, Michael Rubinstein, Andrew Sutherland, and Joseph Wetherell for computations that pointed the way to the correct path to take to achieve Theorem 5.4. We made use of PARI/GP [16] and Magma [1]. The fourth author thanks Wojciech Gajda and the University of Poznań for an invitation to spend a week there, where some of the work on this paper was done.

2. 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 $\psi, \varphi : G_{\mathbf{Q}} \to \mathbf{F}_p^\times$, respectively. Let $\omega : G_{\mathbf{Q}} \to \mathbf{F}_p^\times$ denote the cyclotomic character giving the action of $G_{\mathbf{Q}}$ on $\boldsymbol{\mu}_p$. That is, if $\sigma \in G_{\mathbf{Q}}$ and ζ_p is a primitive p-th root of unity in $\bar{\mathbf{Q}}$, then $\zeta_p^\sigma = \zeta_p^{\omega(\sigma)}$. 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 $\rho_{E,p} : G_{\mathbf{Q}} \to \mathrm{Aut}_{\mathbf{Z}_p}\big(T_p(E)\big)$ 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 $G := \mathrm{Gal}(K_\infty/\mathbf{Q})$, and defines an injective homomorphism from G into $\mathrm{Aut}_{\mathbf{Z}_p}\big(T_p(E)\big)$. To simplify the discussion, we identify G with its image in $\mathrm{Aut}_{\mathbf{Z}_p}\big(T_p(E)\big)$.

Recall the definition of p-exceptional from §1. We would like to know whether $\rho_{E,p}(G_{\mathbf{Q}})$ contains a Sylow pro-p subgroup of $\mathrm{Aut}(T_p(E))$, or equivalently, whether the index $[\mathrm{Aut}_{\mathbf{Z}_p}(T_p(E)) : \rho_{E,p}(G_{\mathbf{Q}})]$ is prime to p.

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

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

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 2.1. 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 [15] for most primes, Ligozat [13] or Kenku [10] for $p = 7$, and Kenku [9] 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 2.2 ([8], 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 [8] is based on the Burnside Basis Theorem. The Frattini quotient of a Sylow pro-p subgroup S_p of $\mathrm{Aut}(T_p(E))$ 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 2.3. *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 [21]). 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 [20] 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. □

Remark 2.4. Lemma 2.3 can also be proved by studying how the Tate period for E over $\mathbf{Q}_\ell$ changes under the isogeny $E \to E'$. 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 2.5. *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. □

Proposition 2.6. *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 2.1, L and L' are cyclic extensions of K of degree p.

Suppose first that E is p-exceptional, and $\ell \neq p$. By Lemma 2.3, the ramification degree of ℓ in at least one of $L/\mathbf{Q}$ and $L'/\mathbf{Q}$ is prime to p. But by Proposition 2.2 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 $\mathrm{Gal}(K/\mathbf{Q})$ on both $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L'/K)$ 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 2.5. We can regard ξ as a character of $\mathrm{Gal}(F/\mathbf{Q})$. Since $\mathrm{Gal}(K/F)$ acts trivially on $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L'/K)$, 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 $\mathrm{Gal}(F/\mathbf{Q})$ acts on both $\mathrm{Gal}(J/F)$ and $\mathrm{Gal}(J'/F)$ 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 [7, 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 2.2. □

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

Theorem 2.7. *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 $\mathbf{Q}_\ell$. Let $q_{E,\ell}$ denote the corresponding Tate period for E. Then we have

$$\mathbf{Q}_\ell(E[p]) = \mathbf{Q}_\ell\big(\boldsymbol{\mu}_p, \sqrt[p]{q_{E,\ell}}\big)$$

and therefore the ramification degree for ℓ in $\mathbf{Q}(E[p])$ is divisible by p if and only if $\mathrm{ord}_\ell\big(q_{E,\ell}\big) \not\equiv 0 \pmod{p}$. Furthermore, we have (Proposition VII.5.1(b) of [22])

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

Thus, the ramification degree for ℓ in $\mathbf{Q}(E[p])/\mathbf{Q}$ is divisible by p if and only if $\mathrm{ord}_\ell\big(\Delta_{\min}(E)\big)$ 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 2.3, at least one of the integers $\mathrm{ord}_\ell\big(\Delta_{\min}(E)\big)$, $\mathrm{ord}_\ell\big(\Delta_{\min}(E')\big)$ is divisible by p. Therefore, both are divisible by p if and only if their difference is divisible by p. Now apply Proposition 2.6. □

3. Twisting $X_1(7)$ by characters

Fix a field k of characteristic different from 7. Suppose $\psi : G_k \to \mathbf{F}_7^\times$ 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. The method of our construction is as follows. When $\psi = 1$, we are parametrizing elliptic curves with a point of order 7, so the desired elliptic curves are the fibers of the universal elliptic curve $\mathcal{E}_1$ over the modular curve $X_1(7)$ of genus zero. For general ψ, we twist the elliptic surface $\mathcal{E}_1$ to obtain the appropriate elliptic surface $\mathcal{E}_\psi$, and then the A_v are the fibers of $\mathcal{E}_\psi$. Theorem 3.6 deals with 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, in Theorem 3.10.

Definition 3.1. If E, E' are elliptic curves over k, and $P \in E(k^{\mathrm{s}}), P' \in E'(k^{\mathrm{s}})$ 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 3.2. *Suppose E, E' are elliptic curves over k, $P \in E(k^{\mathrm{s}}), P' \in E'(k^{\mathrm{s}})$ 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*

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

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). □

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

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

The discriminant of E_u is

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

The next result is #15 in Table 3 on p. 217 of [11].

Theorem 3.3 ([11]). *Let E_u be as above.*

(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

$$\eta(v) = 1/(1-v). \tag{3}$$

The following lemma will be used in the proofs of Theorems 3.6 and 5.5 below.

Lemma 3.4. *Suppose $u \in k^{\mathrm{s}}$ 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

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

is such an isomorphism. Uniqueness follows from Lemma 3.2(i). □

The following lemma is taken from a paper of Washington [27, pp. 64–65].

Lemma 3.5 (Washington [27]). *Suppose that K/k is a cyclic cubic extension, and σ is a generator of $\mathrm{Gal}(K/k)$. 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 $\phi \in \mathrm{PGL}_2(k)$ such that $\alpha^\sigma = \phi(\alpha)$. Note that ϕ^3 fixes α, α^σ, and α^{σ^2}, so $\phi^3 = 1$ in $\mathrm{PGL}_2(k)$.

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

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

for some $a \in k$, so

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

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

$$\tilde\xi\tilde\phi\tilde\xi^{-1} = \tilde\eta. \tag{4}$$

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

$$\gamma^\sigma = \eta(\gamma). \tag{5}$$

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

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

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

Theorem 3.6. *Suppose that $\chi : G_k \to \mathbf{F}_7^\times$ 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 3.5 for K and σ, and let

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

Proof. If $\chi = 1$, then A_v is the curve E_v of (1), and the theorem follows from Theorem 3.3.

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

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

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 (3.5)(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 3.3(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

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

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

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

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 3.2(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 3.4. Thus by the uniqueness of u in Theorem 3.3(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 3.5(ii), it is easy to check that $\delta^\sigma = \eta\delta$. Hence we have

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

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 3.2(ii). □

Remark 3.7. Suppose $\chi \neq 1$ in Theorem 3.6. With notation as in Theorem 3.6, the discriminant of A_v is given by

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

Remark 3.8. With notation as in Theorem 3.6 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 3.5(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 six values of $v \in k^{\mathrm{s}}$.

Definition 3.9. If E is an elliptic curve over k and $\epsilon : G_k \to \{\pm 1\} \subseteq \mathrm{Aut}(E)$ 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 $\lambda : E^{(\epsilon)} \to E$ over k^{s} with $\lambda^\sigma \circ \lambda^{-1} = \epsilon(\sigma)$ for all $\sigma \in G_k$.

If $\mathrm{char}(k) \neq 2$, 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 3.10. *Suppose that $\psi : G_k \to \mathbf{F}_7^\times$ 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 3.6 for the character $\chi = \psi^4$.*

In particular, if $\operatorname{char}(k) \neq 2$ 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 3.6, and we can also twist by ψ^3 as in Definition 3.9. Let $\lambda : E^{(\psi^3)} \xrightarrow{\sim} E$ be as in Definition 3.9. For $P \in E(k^{\mathrm{s}})$ 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 3.6,

E has a k-rational subgroup of order 7 on which G_k acts via ψ

$\Leftrightarrow E^{(\psi^3)}$ has a k-rational subgroup of order 7 on which G_k acts via ψ^4

$\Leftrightarrow E^{(\psi^3)}$ is isomorphic over k to A_v for some $v \in k$

$\Leftrightarrow E$ is isomorphic over k to $A_v^{(\psi^3)}$ for some $v \in k$.

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

Lemma 3.11. *Let $A_v^{(d)}$ be as in Theorem 3.10, 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 3.4. We can easily reduce to the case $d = 1$.

Let δ be the linear fractional transformation defined by (6) in the proof of Theorem 3.6. The proof of Theorem 3.6 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 3.4. 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 3.2(ii). □

Corollary 3.12. *Suppose that $\psi : G_k \to \mathbf{F}_7^\times$ is a homomorphism. If $k \neq \mathbf{F}_2$, then there exists an elliptic curve E over k with a k-rational subgroup of order 7 on which G_k acts via ψ. If $k = \mathbf{F}_2$, 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 and ω is the cyclotomic character.*

Proof. Let A_v be as defined in Theorem 3.6, for the (at most cubic) character ψ^4. If $v \in k$ is not a zero of the discriminant $\Delta(A_v)$, then Theorem 3.10 shows that the twist of A_v by ψ^3 has the desired property. Suppose $k \neq \mathbf{F}_2$. 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 3.8, $c \neq 0$, 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 $\mathrm{char}(k) \neq 7$), so there are $v \in k$ with $\Delta(A_v) \neq 0$ if and only if $k \neq \mathbf{F}_2$.

When $k = \mathbf{F}_2$, the stated result 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, it 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.) Note that 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. □

Remark 3.13. Here is another interpretation of Theorem 3.10. 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 $\psi : G_k \to \mathrm{Aut}(\Psi) \cong \mathbf{F}_7^\times$ be the character giving the action of G_k on Ψ. Let A_v be as defined in Theorem 3.6 with $\chi = \psi^4$, and let $f_v : \Psi \to A_v[7]$ be the unique homomorphism with $f_v(P) = P_v$, where P_v is as in the proof of Theorem 3.6. Then Theorem 3.10 says that the elliptic surface A_v is the universal elliptic curve over $X(\Psi)$, in the following sense. For every $v \in k^{\mathrm{s}}$ 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 $v \in k^{\mathrm{s}}$ 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 3.11 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 $\psi = \omega^5$

As before, let $\omega : G_{\mathbf{Q}} \to \mathbf{F}_7^\times$ denote the cyclotomic character, and 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

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

where

$$\alpha(v) := -\tfrac{35}{16}v^8 + \tfrac{63}{4}v^7 - \tfrac{833}{24}v^6 + \tfrac{49}{2}v^5 + \tfrac{245}{48}v^4 - \tfrac{49}{2}v^3 + \tfrac{343}{24}v^2 + \tfrac{7}{4}v - 2,$$

$$\beta(v) := -\tfrac{49}{32}v^{12} + \tfrac{637}{48}v^{11} - \tfrac{1617}{32}v^{10} + \tfrac{44149}{432}v^9 - \tfrac{16555}{192}v^8 - \tfrac{1477}{36}v^7 + \tfrac{1911}{16}v^6 - \tfrac{8183}{144}v^5 - \tfrac{2009}{192}v^4 + \tfrac{7007}{432}v^3 - \tfrac{147}{16}v^2 + \tfrac{14}{3}v - 1.$$

The discriminant of B_v is

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

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*

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

Proof. We will deduce part (i) from Theorem 3.10. The cyclotomic character ω has order 6. Let $\psi = \omega^5$. The cubic character $\psi^4 = \omega^2$ cuts out the unique cubic subfield $K := \mathbf{Q}(\boldsymbol{\mu}_7)^+$ of $\mathbf{Q}(\boldsymbol{\mu}_7)$. The automorphism $\sigma \in \operatorname{Gal}(K/\mathbf{Q})$ 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 3.5, 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 $\mathbf{Q}(\boldsymbol{\mu}_7)$. The map $(x, y) \mapsto (x', y')$ where

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

is an isomorphism from the curve $A_v^{(d)}$ of Theorem 3.10 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 3.6, which is used to define $A_v^{(d)}$ in Theorem 3.10). Now (i) follows from Theorem 3.10.

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 [22, §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 [22, 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 $\operatorname{ord}_7(\Delta(B_v)) < 12$, 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

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

B_v has a model

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

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). □

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 $\left(\begin{smallmatrix}\omega^5 & * \\ 0 & \omega^2\end{smallmatrix}\right)$.

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

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

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

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:*

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

Proof. If v is not integral at 7, then $\mathrm{ord}_7(f_1(v)) = \mathrm{ord}_7(f_2(v)) = 3\mathrm{ord}_7(v)$. 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 $\Delta(B_v) = -7^3 f_1(v)f_2(v)^7$, so (c) follows from (a) and (b). Assertion (d) follows directly from (c) and Theorem 4.1(ii,iii).

We compute that

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

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). □

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 Vélu [26] (see [2, §4.1]) to exhibit the isogeny. (See especially Proposition 4.1 of [2] and the formulas for $\tilde{A}$ and $\tilde{B}$ in the paragraph after its proof.) □

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) $\dfrac{\Delta_{\min}(B'_v)}{\Delta_{\min}(B_v)} = 7^{s_v}\left(\dfrac{v^3-2v^2-v+1}{v^3-v^2-2v+1}\right)^6$ *for some $s_v \in \{\pm 6\}$, and*

(ii) $\operatorname{ord}_7\left(\dfrac{\Delta_{\min}(B'_v)}{\Delta_{\min}(B_v)}\right) = \begin{cases} 0 & \textit{if } v \textit{ is integral at } 7 \textit{ and } v \equiv 3 \textit{ or } 5 \pmod 7, \\ 6 & \textit{otherwise.}\end{cases}$

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 $B^{(-7)}_{1-v}$ denote the quadratic twist of B_{1-v} by -7, and let

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

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 $B'_v \cong B^{(-7)}_{1-v}$. Thus

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

proving (i).

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

$$\operatorname{ord}_7\big(j(B^{(-7)}_{1-v})\big) = \operatorname{ord}_7\big(j(B_{1-v})\big) \geq 0.$$

Hence, by Tate's algorithm (see for example [22, Table 15.1]), we have

$$0 \leq \operatorname{ord}_7\big(\Delta_{\min}(B^{(-7)}_{1-v})\big) \leq 10.$$

It follows that the integer s_v of (11) satisfies

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

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

Proposition 4.7. *Suppose that $v \in \mathbb{P}^1(\mathbf{Q})$. 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 $v \in \mathbb{P}^1(\mathbf{Q})$, 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 $v \in \mathbb{P}^1(\mathbf{Q})$. 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 [20, 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 [20, 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 [20, §5.6], especially Proposition 23(b).) This contradicts the facts that ℓ is unramified in $\mathbf{Q}(\boldsymbol{\mu}_7)/\mathbf{Q}$ and $[\mathbf{Q}(B_v[7]) : \mathbf{Q}(\boldsymbol{\mu}_7)]$ 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 $\mathbf{Q}_\ell$ to $\boldsymbol{\mu}_7$ 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). □

Remark 4.8. There is an S_3-action on $\mathbb{P}^1(\mathbf{Q})$ defined by the linear fractional transformations η of (3) and τ defined by $\tau(v) = 1 - v$. 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, $\{2, 1/2, -1\}$ 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 $v \in \mathbb{P}^1(\mathbf{Q})$. However, if $1 - v \in \{v, \eta(v), \eta^2(v)\}$, then Lemma 3.11 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 the conductor of B_v is 49. If $v \in \{0, 1, \infty\}$, then $j(B_v) = -15^3$ and $\mathrm{End}(B_v)$ is the maximal order in F. If $v \in \{2, 1/2, -1\}$, then $j(B_v) = 255^3$ and $\mathrm{End}(B_v)$ is the nonmaximal order of conductor 2 in F.

5. The image of $\rho_{E,7}$

Suppose E is an elliptic curve over $\mathbf{Q}$ with a $\mathbf{Q}$-isogeny of prime degree $p \geq 7$. We retain the notation of §2. 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 1.2 ([8, Theorem 1]), if E is p-exceptional then $\psi\varphi^{-1}$ has order 2. If $p > 7$ then Proposition 1.3 ([8, 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 image$(\rho_{E,p})$ is a p-adic Lie group of dimension 2, and so it cannot contain a Sylow pro-p subgroup of $\mathrm{Aut}(T_p(E))$. Thus for $p > 7$, an elliptic curve over $\mathbf{Q}$ is p-exceptional if and only if it 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 Theorem 2.7 to study 7-exceptional curves. We assume from now on that $p = 7$.

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

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

Lemma 5.1. *Let C_j be as above.*

(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 $\mathbb{P}^1(\mathbf{C})$ 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

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

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. □

Recall the elliptic curve B_v defined by (8), and the definition of p-exceptional in Definition 1.1.

Proposition 5.2. *Suppose $v \in \mathbf{Q}$. Then the following are equivalent:*

(i) *B_v is 7-exceptional;*
(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 Theorem 2.7 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 $0 \le j \le 6$. But by Lemma 5.1(ii), $C_j(\mathbf{Q})$ is empty if $1 \le j \le 6$. This proves the lemma. □

Theorem 5.3. *Suppose that E is an elliptic curve over $\mathbf{Q}$ with a $\mathbf{Q}$-isogeny of degree 7. Then the following are equivalent:*

(i) *E is 7-exceptional;*
(ii) *E is a quadratic twist of B_v for some $(v,w) \in C_0(\mathbf{Q})$.*

Proof. Suppose (i), i.e., the image of $\rho_{E,7}$ does not contain a Sylow pro-7 subgroup of $\mathrm{Aut}_{\mathbf{Z}_7}(T_7(E))$. By Theorem 1.2 ([8, Theorem 1]), $\psi\varphi^{-1}$ has order 2, so by Lemma 2.5 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 Proposition 5.2. □

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 $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ 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 5.3, we wish to determine $C(\mathbf{Q})$. One finds easily the following rational points on C. Let

$$P_0 = (0,1), \quad P_1 = (1,1), \quad P_\infty = (\infty,1),$$
$$P_2 = (2,-1), \quad P_3 = (\tfrac{1}{2},-1), \quad P_4 = (-1,-1)$$

and

$$Z = \{P_0, P_1, P_\infty, P_2, P_3, P_4\} \subseteq C(\mathbf{Q}).$$

Theorem 5.4. *$C(\mathbf{Q}) = Z$.*

We will prove Theorem 5.4 using the method of Chabauty, as made explicit in [24]. Before that we deduce the following consequence.

Theorem 5.5. *If E is an elliptic curve over $\mathbf{Q}$ with a $\mathbf{Q}$-rational subgroup of order 7, and E is exceptional for 7, then E has CM by $\mathbf{Q}(\sqrt{-7})$, i.e., $j(E) \in \{-15^3, 255^3\}$, i.e., E is a quadratic twist of an elliptic curve of conductor 49.*

Proof. By Theorem 5.3, E is a quadratic twist of B_v for some $(v,w) \in C(\mathbf{Q})$. By Theorem 5.4, $(v,w) \in Z$. If $v \in \{0,1,\infty\}$, then B_v is isomorphic to the curve 49A1 in Cremona's tables [6]. If $v \in \{2,1/2,-1\}$, then B_v is isomorphic to the curve 49A2. □

6. The rank of $J(\mathbf{Q})$

Let J be the Jacobian of C. The first step in bounding $C(\mathbf{Q})$ is to compute the rank of $J(\mathbf{Q})$. In this section we prove that the rank is 6. We first prove that 6 is an upper bound, following the method described by Poonen and Schaefer in [17]. To keep our notation as close as possible to theirs, we 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 $\mathrm{End}_k(J)$ by sending ζ to the automorphism of J induced by the automorphism $(x, y) \mapsto (x, \zeta y)$ of X. We will use [17] to compute an upper bound for the size of $J(k)/\pi J(k)$.

Define

$$f(x) = (x^3 - 2x^2 - x + 1)(x^3 - x^2 - 2x + 1)^6,$$
$$f_0(x) = (x^3 - 2x^2 - x + 1)(x^3 - x^2 - 2x + 1).$$

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

Suppose K is a field containing k. Let $\mathrm{Div}(X/K)$ 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 $\mathrm{Div}^0(X/K)$ denote the subgroup of divisors of degree zero, and let $\mathrm{Pic}^0(X/K) = \mathrm{Div}^0(X/K)/P(X/K)$ 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 $\mathrm{Pic}^0(X/K) \cong J(K)$, 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 [17, §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 $D = \sum_P n_P P \in \mathrm{Div}^0(X)$ is supported on points $P \in X(\bar{K})$ with x-coordinate $x(P) \notin \{\alpha_i : 1 \le i \le 6\} \cup \{\infty\}$, then

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

Lemma 6.1 (Poonen-Schaefer [17])**.** *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 $x(P) \notin \{\alpha_i : 1 \le i \le 6\} \cup \{\infty\}$ then*

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

Proof. This follows from [17, 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 [17]:

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

Theorem 6.2 (Poonen-Schaefer [17]). *In the commutative diagram*

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

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

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

Proof. That the maps are injective follows from [17, 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 [17, Proposition 12.4] since J has good reduction outside of 7, and $U \subseteq \ker(N)$ by [17, Proposition 12.1]. The commutativity of the diagram shows that $U \subseteq \mathrm{loc}_\pi^{-1}(\mathrm{image}((x-T)_{k_\pi}))$. □

Lemma 6.3 (Poonen-Schaefer [17]). *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 [17, Lemma 12.9], since $f(x)$ factors into linear factors in $k[x]$, of which 6 are distinct.

Similarly, [17, Lemma 12.9] shows that $\dim_{\mathbf{F}_7} J(k_\pi)[\pi] = 4$, and then [17, 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. □

Remark 6.4. We observe that C has an action of the group $\Sigma \cong S_3$ generated by the two involutions

$$(v, w) \longmapsto (v^{-1}, w^{-1}) \quad \text{and} \quad (v, w) \longmapsto (1 - v, w^{-1}).$$

The group Σ has the two orbits $\{P_0, P_1, P_\infty\}$ and $\{P_2, P_3, P_4\}$ on the set Z of known rational points.

Proposition 6.5. $\mathrm{rank}_{\mathcal{O}} J(k) \le 6$.

Proof. We will use Theorem 6.2 to bound the $\mathcal{O}$-rank of $J(k)$. All of the terms in Theorem 6.2 are $\mathbf{F}_7$-vector spaces, and we need to compute them explicitly.

It follows from Theorem 5.1 of Chapter 3 of [12], 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 6.2 and Lemma 6.3(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 $1 \le i \le 6$ with x-coordinates:

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

Using PARI/GP and Lemma 6.1, we compute $(x-T)_{k_\pi}(\sigma(Q_i) - \infty)$ for $1 \le i \le 6$ 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

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

Therefore by Theorem 6.2 we have $\dim_{\mathbf{F}_7} J(k)/\pi J(k) \le 10$. Since

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

and $\dim_{\mathbf{F}_7} J(k)[\pi] = 4$ by Lemma 6.3(i), we conclude that $\operatorname{rank}_{\mathcal{O}} J(k) \le 6$. □

Lemma 6.6. $\operatorname{rank}_{\mathbf{Z}} J(\mathbf{Q}) \le 6$.

Proof. This follows from Proposition 6.5 and [17, Lemma 13.4]. □

Remark 6.7. The involution $(v, w) \mapsto (v^{-1}, w^{-1})$ has exactly the two fixed points P_1 and P_4, therefore the quotient of C by this involution is a curve D of genus 6. The Jacobian J of C is isogenous to a product of two copies of the Jacobian of D. The genus 6 curve D is

$$Y^7 - 7Y^5 + 14Y^3 - 7Y = (2X^3 - 6X^2 - 7X + 24)/(X^3 - 3X^2 - 4X + 13)$$

which by a change of variables is

$$(-2+Y)(-1-2Y+Y^2+Y^3)^2 = X/(1-4X+3X^2+X^3).$$

Remark 6.8. We now elaborate on the path that led to the proof that $|C(\mathbf{Q})| = 6$ (although it isn't actually used in our proof). The subgroup of $J(\mathbf{Q})$ generated by differences of known rational points on C has rank 4. Since J is $\mathbf{Q}$-isogenous to $\operatorname{Jac}(D)^2$, the rank of $J(\mathbf{Q})$ is even, so it must be either 4 or 6. The S_3-action shows that $|C(\mathbf{Q})|$ is divisible by 6. A Chabauty argument at the prime 2, using [24], then gives that $|C(\mathbf{Q})|$ is 6 or 12. The argument is as follows. Consider the pairing $J(\mathbf{Q}_2) \times \Omega(C/\mathbf{Z}_2) \to \mathbf{Q}_2$ defined by $G, \omega \mapsto (G, \omega) := \int_G \omega$ where $\Omega(C/L)$ is the set of holomorphic differentials on C over L and G is a degree 0 divisor on C. View $Z \subset C(\mathbf{Q}) \subset J(\mathbf{Q})$ (fixing a basepoint in Z) and let

$$V := \{\omega \in \Omega(C/\mathbf{Z}_2) : (J(\mathbf{Q}), \omega) = 0\} \subseteq V_0 := \{\omega \in \Omega(C/\mathbf{Z}_2) : (Z, \omega) = 0\}.$$

Let $\widetilde{V}$ (resp., $\widetilde{V_0}$) be the image of V (resp., V_0) under the reduction map $\Omega(C/\mathbf{Z}_2) \to \Omega(C/\mathbf{F}_2)$. Then $\dim_{\mathbf{F}_2} \widetilde{V} = \operatorname{rank}_{\mathbf{Z}_2} V \geq 12 - \operatorname{rank} J(\mathbf{Q}) \geq 6$. Let

$$W := \{\omega \in \Omega(C/\mathbf{F}_2) : \operatorname{ord}_P(\omega) \geq 2 \text{ for all } P \in \{P_0, P_1, P_\infty\}\}.$$

If $|C(\mathbf{Q})| = 12$, each fiber of $C(\mathbf{Q}) \to C(\mathbf{F}_2)$ has size 4, and it follows (using [24]) that $\widetilde{V} \subseteq W \cap \widetilde{V_0}$. So if $\dim(W \cap \widetilde{V_0}) < 6$, then $|C(\mathbf{Q})| = 6$. Balakrishnan, using ideas of Kedlaya and Wetherell, computed $\int_P^Q \omega$ for $\omega \in \Omega(C/\mathbf{Z}_2)$ and $P, Q \in Z$. This gives V_0 and $\widetilde{V_0}$. Unfortunately, $\dim(W \cap \widetilde{V_0}) = 6$. However, if $\operatorname{rank} J(\mathbf{Q})$ were 4, then $\dim_{\mathbf{F}_2} \widetilde{V} = \operatorname{rank}_{\mathbf{Z}_2} V \geq 12 - \operatorname{rank} J(\mathbf{Q}) = 8$. This would imply that $|C(\mathbf{Q})| = 6$, since $\widetilde{V} \subseteq W \cap \widetilde{V_0}$ when $|C(\mathbf{Q})| = 12$. As explained in Appendix A, we had reason to believe that $\operatorname{rank}_{\mathbf{Z}} J(\mathbf{Q}) = 6$. This gave motivation to find additional generators of $J(\mathbf{Q})$, which we do in the proof of the following theorem.

Theorem 6.9. $\operatorname{rank}_{\mathbf{Z}} J(\mathbf{Q}) = 6$.

Proof. By Lemma 6.6, we have $\operatorname{rank}_{\mathbf{Z}} J(\mathbf{Q}) \leq 6$.

We look for closed points of higher degree on the genus 6 quotient D of C defined in Remark 6.7. For D, we use the model in $\mathbb{P}^3$ obtained as the image of the map sending a point (v, w) on C to $(v + \frac{1}{v} : w + \frac{1}{w} : \frac{v}{w} + \frac{w}{v} : 1)$. This model is a smooth curve of genus 6 (and degree 10) still having bad reduction only at 7. We intersect D with hyperplanes and quadrics of increasing height and split the resulting divisor as a sum of prime divisors. If it splits, we check if the new prime divisor leads to a larger subgroup in the Jacobian of D. For this check, we use the homomorphism

$$\operatorname{Pic}(D) \longrightarrow \prod_{p \in S} \operatorname{Pic}(D/\mathbf{F}_p)$$

where S is a suitable set of primes (we used $S = \{2, 3, 5, 11, 13, 17\}$); compare [25] for details.

In this way, we find a point of degree 4 that leads to a larger group that is still of rank 2, and a point of degree 8 that increases the rank to 3. Pulling back these points to C, we obtain a point of degree 8 of the form

$$(-\alpha^7 + 2\alpha^6 + \alpha^4 + \alpha^2 + 2, \alpha)$$

with α a root of

$$t^8 - 2t^7 - t^5 - t^3 - 2t + 1\,,$$

and a point of degree 16 of the form

$$\Big(\tfrac{1}{216}(187\beta^{15} + 894\beta^{14} + 98\beta^{13} + 408\beta^{12} + 1037\beta^{11} + 1245\beta^{10} + 1754\beta^9 + 1371\beta^8 + 783\beta^7 + 1702\beta^6 + 1497\beta^5 + 793\beta^4 + 708\beta^3 + 250\beta^2 + 450\beta + 575), \beta\Big)$$

with β a root of

$$t^{16} + 5t^{15} + 2t^{14} + 4t^{13} + 5t^{12} + 10t^{11} + 11t^{10} + 13t^9 + 6t^8 + 13t^7 + 11t^6 + 10t^5 + 5t^4 + 4t^3 + 2t^2 + 5t + 1\,.$$

Denote the corresponding prime divisors on C by Q_1 and Q_2, respectively. Let $Q_3 = \sigma(Q_1)$ and $Q_4 = \sigma(Q_2)$, where $\sigma \in \Sigma$ is the map $(v, w) \mapsto (\frac{1}{1-v}, w)$. Let $H \subset J(\mathbf{Q})$ be the subgroup generated by degree-zero linear combinations of the ten prime divisors:

$$\{P_0, P_1, P_\infty, P_2, P_3, P_4, Q_1, Q_2, Q_3, Q_4\}. \tag{14}$$

We compute that $|J(\mathbf{F}_{13})| = 3^6 \cdot 7^4 \cdot 13^2 \cdot 349^2$, and therefore $J(\mathbf{Q})$ has no 5-torsion. (By considering additional reductions one can show that $|J(\mathbf{Q})_{\mathrm{tors}}|$ divides 7^2.) In addition, we check that the image of

$$H \longrightarrow J(\mathbf{F}_2) \times J(\mathbf{F}_3) \times J(\mathbf{F}_{11})$$

has a quotient isomorphic to $(\mathbf{Z}/5\mathbf{Z})^6$. It follows that $\mathrm{rank}_{\mathbf{Z}} H \geq 6$, so $\mathrm{rank}_{\mathbf{Z}} J(\mathbf{Q}) = 6$ and H has finite index in $J(\mathbf{Q})$. □

Remark 6.10. In the course of the calculations in the proof of Theorem 6.9, we showed also that the subgroup $H \subset J(\mathbf{Q})$ is free of rank 6, and that the relations among the divisors (14) are generated by:

$$\begin{aligned} P_0 + P_1 + P_\infty &\sim P_2 + P_3 + P_4, \\ P_1 + P_4 + Q_1 &\sim P_2 + P_\infty + Q_3, \\ 5P_0 + 3P_1 + 4P_\infty + 4P_2 + 5P_3 + 3P_4 &\sim 2Q_1 + Q_3. \end{aligned}$$

7. Proof of Theorem 5.4

Since the Mordell-Weil rank of $J(\mathbf{Q})$ is smaller than the genus of C, we can apply Chabauty's method (see [4, 5, 24]) to calculate $C(\mathbf{Q})$.

Define divisors on C:

$$D_x = \sum_{\zeta \in \boldsymbol{\mu}_7} (x, \zeta) \text{ for } x \in \{0, 1, \infty\}, \quad G_1 = \sum_{i=1}^{3} (\alpha_i, 0), \quad G_2 = \sum_{i=4}^{6} (\alpha_i, \infty),$$

where (as before), $\alpha_1, \alpha_2, \alpha_3$ (resp., $\alpha_4, \alpha_5, \alpha_6$) are the roots of $v^3 - 2v^2 - v + 1$ (resp., $v^3 - v^2 - 2v + 1$). One checks easily that the divisors of the rational functions v, w, and $v^3 - v^2 - 2v + 1$ are given by

$$(v) = D_0 - D_\infty, \quad (w) = G_1 - G_2, \quad (v^3 - v^2 - 2v + 1) = 7G_2 - 3D_\infty. \tag{15}$$

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.

Lemma 7.1. *Suppose L is a field of characteristic different from 7.*

(i) *The divisor of the differential dv is $(dv) = 6G_1 + 6G_2 - 2D_\infty$.*

(ii) *A basis for the L-vector space $\Omega(C/L)$ is given by*

$$\omega_{i,j} := \frac{v^i w^j}{(v^3 - v^2 - 2v + 1)w^6} dv, \quad 0 \leq i \leq 1, \ 0 \leq j \leq 5.$$

Proof. The function v has (simple) poles at each of the 7 points $\{(\infty, \zeta) : \zeta \in \boldsymbol{\mu}_7\}$, and no other poles. Hence $\mathrm{ord}_{(\infty,\zeta)}(dv) = -2$, and $\mathrm{ord}_P(dv) \geq 0$ for all other points P. If α is a root of $v^3 - 2v^2 - v + 1$, then the equation for C shows that $\mathrm{ord}_{(\alpha,0)}(v - \alpha)$ is a (positive) multiple of 7. Since the polar divisor of v is D_∞, we conclude that $\mathrm{ord}_{(\alpha,0)}(v - \alpha) = 7$, and

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

Similarly, if α is a root of $v^3 - v^2 - 2v + 1$ then $\mathrm{ord}_{(\alpha,\infty)}(dv) = 6$. Since the divisor (dv) has degree $2g - 2 = 22$, we conclude that $(dv) = 6G_1 + 6G_2 - 2D_\infty$, giving (i).

It now follows from (15) that the differential $\omega_{i,j}$ has divisor

$$(\omega_{i,j}) = iD_0 + (1 - i)D_\infty + jG_1 + (5 - j)G_2.$$

In particular ω_{ij} is holomorphic if (and only if) $0 \le i \le 1$ and $0 \le j \le 5$.

Since v is transcendental over L and w has degree 7 over $L(v)$, the set $\{v^i w^j : 0 \le i \le 1, 0 \le j \le 5\}$ is linearly independent over L, so $\{\omega_{ij} : 0 \le i \le 1, 0 \le j \le 5\}$ is linearly independent over L. Since $\dim_L(\Omega(C/L)) = \text{genus}(C) = 12$, we have (ii). □

Let $\Omega(C/\mathbf{Z}_5)$ be the $\mathbf{Z}_5$-span of the differentials $\omega_{i,j}$ with $0 \le i \le 1$ and $0 \le j \le 5$. Consider the bilinear pairing

$$J(\mathbf{Q}_5)/J(\mathbf{Q}_5)_{\text{tors}} \times \Omega(C/\mathbf{Z}_5) \to \mathbf{Q}_5$$

of free $\mathbf{Z}_5$-modules of rank 12 with trivial left and right kernel that is used on p. 1210 of [24]. Let $V \subset \Omega(C/\mathbf{Z}_5)$ be the orthogonal complement under this pairing of (the closure of) $J(\mathbf{Q}) \subset J(\mathbf{Q}_5)$. By Theorem 6.9 we have $\text{rank}_{\mathbf{Z}} J(\mathbf{Q}) = 6$.

Let $\tilde{V} \subset \Omega(C/\mathbf{F}_5)$ be the image of V under the (surjective) reduction map $\text{red}_5 : \Omega(C/\mathbf{Z}_5) \to \Omega(C/\mathbf{F}_5)$. Since $\text{rank}_{\mathbf{Z}_5}(\Omega(C/\mathbf{Z}_5)) = 12 = \dim_{\mathbf{F}_5}(\Omega(C/\mathbf{F}_5))$, we have $\ker(\text{red}_5) = 5\Omega(C/\mathbf{Z}_5)$. Since $\Omega(C/\mathbf{Z}_5)/V$ is torsion-free, we have $5V = V \cap 5\Omega(C/\mathbf{Z}_5) = \ker(\text{red}_5|_V)$. Thus $\tilde{V} \cong V/5V$, so $\dim_{\mathbf{F}_5}(\tilde{V}) = \text{rank}_{\mathbf{Z}_5}(V) = 6$.

We will show that for each point $P \in C(\mathbf{F}_5)$, there exists a differential $\omega_P \in \tilde{V}$ that does not vanish at P. Proposition 6.3 of [24] then shows that there is at most one point in $C(\mathbf{Q})$ that reduces to P. Since the set $Z \subseteq C(\mathbf{Q})$ bijects onto $C(\mathbf{F}_5)$ via the reduction map, that will show $Z = C(\mathbf{Q})$, as desired.

Next we determine the space $\tilde{V}$ explicitly.

Using lattice basis reduction (with higher weights on the higher-degree points), we find the following generators of the intersection of the known finite-index subgroup of $J(\mathbf{Q})$ and the kernel of reduction mod 5:

$$\begin{aligned}
B_1 &= P_1 - P_\infty + P_2 - P_4 - 6Q_2 + 6Q_4,\\
B_2 &= -4P_0 + 9P_\infty + 5P_2 - 3P_3 + P_4 + 4Q_1 - 7Q_3 + Q_4,\\
B_3 &= -4P_0 + 9P_1 + P_2 - 3P_3 + 5P_4 - 7Q_1 + Q_2 + 4Q_3,\\
B_4 &= -2P_0 - 2P_1 + 4P_\infty - 11P_2 + 13P_3 - 2P_4 - 4Q_1 + Q_2 - 2Q_3 + 2Q_4,\\
B_5 &= -6P_1 + 6P_\infty - 9P_2 + 9P_4 - 2Q_1 - Q_2 + 2Q_3 + Q_4,\\
B_6 &= 10P_0 - 8P_1 - 14P_\infty + P_2 - 7P_3 - 6P_4 - 12Q_1 + 11Q_2 - 15Q_3 + 4Q_4.
\end{aligned}$$

For each of these divisors B_m, we compute the Riemann-Roch space of $\pm B_m + 12P_0$ (with sign chosen in an attempt to make the computation more efficient). We check that it is of dimension one and that the same is true for the corresponding Riemann-Roch space over $\mathbf{F}_5$. Let f_m be a function spanning the space; then it follows that the divisor of f_m must be $\mp B_m - 12P_0 + D_m$ with an effective divisor D_m of degree 12 supported on points having the same reduction mod 5 as P_0. (Note that the divisor of the reduction of f_m mod 5 must be the reduction of $\mp B_m$, since this reduction is a principal divisor and the Riemann-Roch space of the reduction of $\pm B_m + 12P_0$ has dimension one.)

We write each basis element $\omega_{ij} \in \Omega(C/\mathbf{Z}_5)$ as a power series in t times dt, where $t = v$ is a uniformizer at P_0 (and also a uniformizer at the reduction of P_0 mod 5). We then integrate formally to obtain the corresponding logarithms λ_{ij} as power series in t. These power series converge 5-adically on points in the same residue class as P_0. The expansion of f_m as a Laurent series in t is of the form $t^n F_m(t)$ where n is $-12 \mp$ the multiplicity of P_0 in B_m. After scaling by a power of 5 if necessary, the series $F_m(t)$ is in $\mathbf{Z}_5[\![t]\!]$, the coefficients of t^k with $k < 12$ have positive valuation, and the coefficient of t^{12} is a 5-adic unit. This reflects the facts that D_m has the same reduction mod 5 as $12P_0$, and P_0 is not in the support of the reductions mod 5 of any of the Q_i or P_j with $j \neq 0$ (as is easily checked). We multiply this series by an invertible series in $\mathbf{Z}_5[\![t]\!]$ such that we obtain a polynomial of degree 12 (to sufficient 5-adic precision). The roots of this polynomial are then the values $t_1, \dots, t_{12}$ of t at the points in the support of D_m. We can then easily compute the power sums of these values (by looking at the logarithmic derivative of the reverse of the polynomial, see again [25]) and therefore evaluate the integrals

$$\int_{[D_m - 12P_0]} \omega_{ij} = \sum_{k=1}^{12} \lambda_{ij}(t_k)\,.$$

The values are in $5\mathbf{Z}_5$. Dividing by 5 and reducing mod 5, we obtain a linear relation that every differential in $\tilde{V}$ has to satisfy.

We used Magma [1] for these computations. A recent version (2.17-1) spends less than 16 hours on current hardware to produce the relations we are looking for. We obtain a 6-dimensional space of relations generated by the following elements (in terms of the basis dual to $\omega_{00}, \dots, \omega_{05}, \omega_{10}, \dots, \omega_{15}$):

$$\begin{gathered}(1,0,0,0,0,0,4,1,1,3,3,4),\\(0,1,0,0,0,0,1,1,0,2,3,0),\\(0,0,1,0,0,0,3,4,0,0,4,2),\\(0,0,0,1,0,0,3,1,0,1,1,2),\\(0,0,0,0,1,0,0,2,3,0,0,4),\\(0,0,0,0,0,1,1,2,2,4,4,2).\end{gathered}$$

As stated above, Theorem 5.4 would follow if we can find, for $P \in C(\mathbf{F}_5)$, a differential $\omega_P \in \tilde{V}$ that does not vanish at P. Next we give an explicit differential ω that works for all $P \in C(\mathbf{F}_5)$. Let $h(v,w) = 3 + w + 3w^3 + 2w^4 + v(w^2 + 2w^3)$, $f_2(v) = v^3 - v^2 - 2v + 1$, and

$$\omega := 3\omega_{00} + \omega_{01} + 3\omega_{03} + 2\omega_{04} + \omega_{12} + 2\omega_{13} = \frac{h(v,w)}{w^6} \cdot \frac{dv}{f_2(v)} \in \Omega(C/\mathbf{F}_5).$$

The coefficients of the ω_{ij} that define ω satisfy the relations above, so $\omega \in \tilde{V}$.

If $0 \le i \le 4$ then (15) and Lemma 7.1(i) show that $dv/f_2(v)$ does not vanish at P_i. By inspection $h(v,w)/w^6$ does not vanish at P_i, so ω does not vanish at P_i.

Similarly, $dv/f_2(v)$ vanishes at P_∞ but $v\,dv/f_2(v)$ does not, by (15) and Lemma 7.1(i). Since $w^2 + 2w^3$ also does not vanish at P_∞, it follows that ω does not vanish at P_∞. This concludes the proof of Theorem 5.4.

As an independent check, we have performed a similar computation on the curve D. There are four points in $D(\mathbf{F}_5)$ that are images of points in $C(\mathbf{F}_5)$. For each of these points, we find a differential that kills the Mordell-Weil group of D and whose reduction mod 5 does not vanish at the given point. This shows that D can have at most four rational points that are in the image of $C(\mathbf{Q})$; this number is accounted for by the known points.

Appendix A. Conjectural determination of the rank

Recall that J is isogenous to the square of the Jacobian J_D of a curve D over $\mathbf{Q}$ of genus 6 defined in Remark 6.7. In this appendix, we explain the computations that led us to believe that the Mordell-Weil rank of J_D is 3 and hence that the rank of $J(\mathbf{Q})$ is 6, assuming standard conjectures on L-series and the conjecture of Birch and Swinnerton-Dyer for J_D.

Since we already knew that the rank of $J_D(\mathbf{Q})$ must be either 2 or 3, it would be sufficient to verify that a positive sign in the functional equation for the L-series of J_D is not consistent with standard conjectures. The result would be even more convincing if it could also be shown that a negative sign, and analytic rank 3 in particular, *is* consistent with the conjectures.

Two of the main ingredients for the computation are the conductor of J_D and the Fourier coefficients of its L-series. Since D (and therefore J_D) has bad reduction only at 7, the conductor is of the form 7^n for some n. Since the reduction of J_D at 7 is totally unipotent (this is shown by computing a proper regular model of D over $\mathbf{Z}_7$, whose special fiber turns out to be tree-like and without components of positive genus), it follows that $n \geq 2 \cdot \mathrm{genus}(D) = 12$. An upper bound $n \leq 26$ follows from [14] or [3].

The Fourier coefficients of the L-series can be obtained by counting points on D or C over all finite fields $\mathbf{F}_{p^e}$ for p^e below some bound N (and $e \leq \mathrm{genus}(D) = 6$, making use of the Weil conjectures). This provides the first N coefficients. In our case, Balakrishnan, Sutherland, and Kedlaya provided these coefficients for $N = 10^7$ and $p \neq 7$. The Euler factor at 7 is trivial, since the reduction is totally unipotent. This many coefficients turned out to be enough to produce satisfactory results ("a handful" of digits of accuracy, according to Rubinstein).

Rubinstein performed the L-series computations for us, using his `lcalc` package [19]. He first checked that the rank of $J_D(\mathbf{Q})$ being 2 is not consistent with the standard conjectures, by computing the central L-value assuming the root number to be $+1$ and the conductor to be $7^{12}, 7^{13}, \ldots, 7^{26}$. In each case the result is clearly non-zero. Since we know that the rank is 2 or 3, the Birch and Swinnerton-Dyer conjecture leads to the conclusion that the rank must be 3. This computation is based on the approximate functional equation; see [18, Thm. 1].

As a further check, Rubinstein used the approximate functional equation to compute the first 17 zeros on the critical line (normalized to be $s = 1/2$) with positive imaginary part, assuming the root number to be -1 and the conductor to be 7^{26}. He then compared the two sides of the "explicit formula", assuming a triple zero at the critical point and using the function $\phi(x) = \bigl(\frac{\sin 4x}{4x}\bigr)^4$ (whose Fourier transform has compact support of a size that allows essentially exact computation of the right hand side of the explicit formula with the known Fourier coefficients). The values obtained for $\sum_\gamma \phi(\gamma - t)$, where γ runs through the zeros and $0 \leq t \leq 3$, agree almost perfectly. See Figure 1 for the corresponding calculation using only 16 zeros away from the real axis, where the two graphs can be seen to begin to diverge for $t > 2.8$.

Heuristic considerations indicate that the discriminant of C should be 7^{52}. The given model of C is already regular at 7, so the exponent of the conductor should equal that of the discriminant. Since the conductor of C is the square of that of D, this provides further evidence that D has conductor 7^{26}.

Note that the global root number of the L-function of J_D should be the product of local root numbers, which in our case will all be $+1$ except at $p = 7$. So it would be sufficient to determine the local root number at 7 in order to get the parity

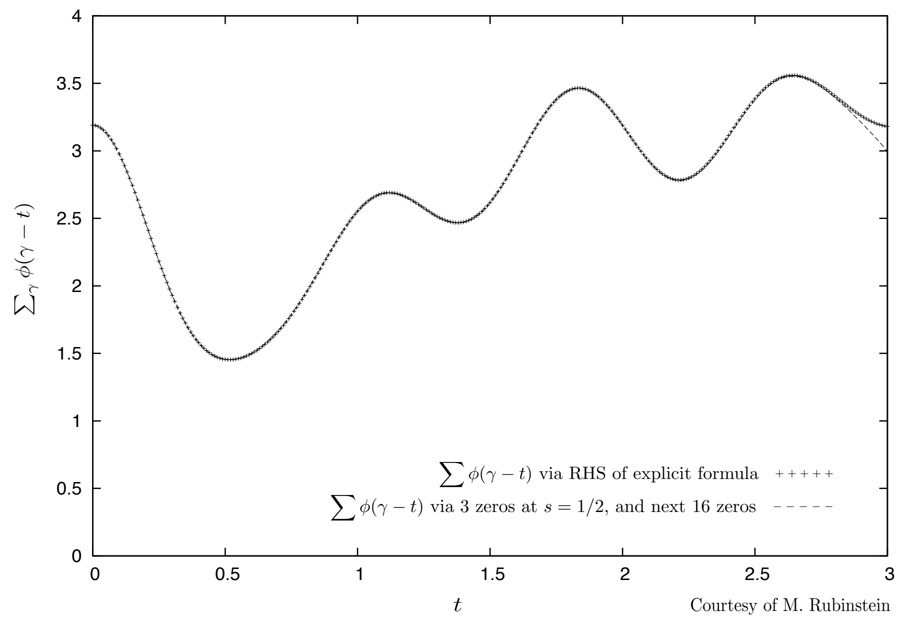

FIGURE 1. Comparison of left and right sides of the explicit formula.

of the rank. However, computing such a local root number when the reduction is unipotent seems to be rather hard.

REFERENCES

[1] W. BOSMA, J. CANNON, C. PLAYOUST, *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://www.maths.usyd.edu.au/`)

[2] A. BOSTAN, F. MORAIN, B. SALVY, É. SCHOST, Fast algorithms for computing isogenies between elliptic curves, *Math. Comp.* **77** (2008), 1755–1778.

[3] A. BRUMER, K. KRAMER, *The conductor of an abelian variety*, Compositio Math., **92**:2 (1994), 227–248.

[4] C. CHABAUTY, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité* (French), C. R. Acad. Sci. Paris **212** (1941), 882–885.

[5] R.F. COLEMAN, *Effective Chabauty*, Duke Math. J. **52** (1985), 765–770.

[6] J. CREMONA, Algorithms for modular elliptic curves, Cambridge University Press (1992).

[7] 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.

[8] R. GREENBERG, The image of Galois representations attached to elliptic curves with an isogeny, *Amer. J. Math.* **134** (2012), 1167–1196.

[9] M. A. KENKU, The modular curves $X_0(169)$ and rational isogeny, *J. London Math. Soc.* **22** (1981), 239–244.

[10] 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.

[11] D. KUBERT, Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc.* **33** (1976), 193–237.

[12] S. LANG, Cyclotomic fields, Graduate Texts in Mathematics, Vol. 59, Springer-Verlag, New York-Heidelberg, 1978.

[13] G. LIGOZAT, Courbes modulaires de genre 1, *Bull. Soc. Math. France, Mémoire* **43** (1975), 1–80.

[14] P. LOCKHART, M. ROSEN, J. H. SILVERMAN, An upper bound for the conductor of an abelian variety, *J. Algebraic Geom.* **2** (1993), 569–601.

[15] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–162.
[16] PARI/GP, `http://pari.math.u-bordeaux.fr`.
[17] B. Poonen, E. F. Schaefer, Explicit descent for Jacobians of cyclic covers of the projective line, *J. Reine Angew. Math.* **488** (1997), 141–188.
[18] M. Rubinstein, *Computational methods and experiments in analytic number theory.* Recent perspectives in random matrix theory and number theory, 425–506, London Math. Soc. Lecture Note Ser., 322, Cambridge Univ. Press, Cambridge, 2005.
[19] M. Rubinstein, *C++ L-function class library and command line interface*, http://oto.math.uwaterloo.ca/~mrubinst/L_function_public/L.html
[20] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.
[21] J-P. Serre, J. Tate, Good reduction of abelian varieties, *Ann. of Math.* (2) **88** (1968), 492–517.
[22] J. Silverman, The arithmetic of elliptic curves, *Grad. Texts in Math.* **106**, Springer, New York, 1986.
[23] J. Silverman, Advanced topics in the arithmetic of elliptic curves, *Grad. Texts in Math.* **151**, Springer, New York, 1994.
[24] M. Stoll, Independence of rational points on twists of a given curve, *Compos. Math.* **142** (2006), 1201–1214.
[25] M. Stoll, *Rational 6-cycles under iteration of quadratic polynomials*, London Math. Soc. J. Comput. Math. **11** (2008), 367–380.
[26] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris Sér. A-B* **273** (1971), A238–A241.
[27] 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`

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany
E-mail address: `Michael.Stoll@uni-bayreuth.de`