AN INFINITE FAMILY OF SERRE CURVES

HARRIS B. DANIELS

Abstract. Given an elliptic curve $E/\mathbb{Q}$, the torsion points of E give rise to a natural Galois representation $\rho_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ associated to E. In 1972, Serre showed that $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] \geq 2$ for all non-CM elliptic curves. The main goal of this paper is to exhibit an elliptic surface such that the Galois representations associated to almost all of the rational specializations have maximal image. Further, we find an explicit set $S \subset \mathbb{Q}$, such that if $t \notin S$, then the Galois representation associated to the specialization at t has maximal image, with a bounded number of exceptions.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$, let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$, and let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group. We also let $E[n]$ be the subgroup of $E(\overline{\mathbb{Q}})$ of n-torsion points, that is

$$E[n] = \{P \in E(\overline{\mathbb{Q}}) : [n]P = \mathcal{O}\}.$$

It is a classical result that $E[n]$ is non-canonically isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and since the multiplication-by-n map is a rational map with coefficients in $\mathbb{Q}$, there is a natural (component-wise) $G_{\mathbb{Q}}$-action on $E[n]$. Fixing a $\mathbb{Z}/n\mathbb{Z}$-basis for $E[n]$, the $G_{\mathbb{Q}}$-action gives a natural Galois representation $\bar{\rho}_{E,n} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The map $\bar{\rho}_{E,n}$ is called the mod n Galois representation associated to E. Taking the inverse limit over all $n \geq 1$ with compatibly chosen bases, we get the full torsion representation associated to E

$$\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}}) = \lim_{\leftarrow} \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \prod_{\text{primes } p} \mathrm{GL}_2(\mathbb{Z}_p).$$

Question 1.1. Is it possible for $\mathrm{Im}\,\rho_E = \mathrm{GL}_2(\widehat{\mathbb{Z}})$?

With this question in mind, we give the following definition:

Definition 1.2. An integer $n \geq 2$ is said to be *exceptional* for E if $\bar{\rho}_{E,n}$ is not surjective.

Asking about the size of $\mathrm{Im}\,\rho_E$ is the same as asking about what numbers are exceptional for E and "how" exceptional they are. It turns out that when E is an elliptic curve with complex multiplication (CM), *every* integer except for possibly 2 is exceptional for E. See [Sil94, Theorem 2.3]. On the other hand if E does not have CM, Serre showed in [Ser72] that the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E]$ is finite. This implies that there are only finitely many exceptional primes for E. In fact, in the same paper, Serre answered Question 1.1.

Proposition 1.3. [Ser72, Proposition 22] *For any elliptic curve E defined over $\mathbb{Q}$, the image of $\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is contained in a group of index 2 inside $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.*

Remark 1.4. Let $E/\mathbb{Q}$ be an elliptic curve with discriminant Δ. The basic idea of the proof of Proposition 1.3 is that the field of definition of the two torsion, $\mathbb{Q}(E[2])$, contains the field $\mathbb{Q}(\sqrt{\Delta})$ and by the Kronecker-Weber theorem, we know that there is some positive integer m such that $\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(\zeta_m)$, where ζ_m is a primitive m^{th} root of unity. Next, it is a classical consequence of the Weil pairing that $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(E[m])$. Thus, for any elliptic curve $E/\mathbb{Q}$, there exists a positive integer m such that $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[m]) \neq \mathbb{Q}$. This forced "entanglement" of torsion fields is what limits the size of the image of ρ_E in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Key words and phrases. Elliptic Curves, Galois Representations.

In fact, also in [Ser72], Serre provided two examples of elliptic curves whose image has index exactly 2 inside $\mathrm{GL}_2(\widehat{\mathbb{Z}})$; namely,

$$E_1 : y^2 + y = x^3 - x$$

and

$$E_2 : y^2 + y = x^3 + x^2.$$

For more details see [Ser72, Examples 5.5.6 and 5.5.7]

Motivated by Proposition 1.3 we give the following definition:

Definition 1.5. An elliptic curve $E/\mathbb{Q}$ is called a *Serre curve* if $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im}\rho_E] = 2$.

The main goal of this paper is to prove the following theorem:

Theorem 1.6. *Let $\mathbb{E}/\mathbb{Q}(t)$ be the elliptic curve given by the Weierstrass equation*

$$\mathbb{E} : y^2 + xy = x^3 + t,$$

and for every $t \in \mathbb{Q}$ let $\mathbb{E}_t/\mathbb{Q}$ be the specialization of $\mathbb{E}$ at t. Then, we can completely determine a set S such that if $t \notin S$, then $\mathbb{E}_t$ is a Serre curve with at most 12 possible exceptions.

While there are a few individual examples of Serre curves in the literature, see [Ser72] and [LT76], there are no explicit elliptic surfaces in the literature where it has been determined which specialization are Serre Curves. Not only can we determine when the specializations are Serre curves, be we can also show that the specializations are almost always Serre curves. Here, when we say almost always, we mean that the set S is thin in the sense of [Ser07, Section 3.2].

The main theorem of this article should not be totally unexpected. In their paper [CGJ11], Cojocaru, Grant and Jones show that if $\mathbb{E}/\mathbb{Q}(t)$ is an elliptic curve such that $j(\mathbb{E}) \notin \mathbb{Q}$ and $\mathrm{Gal}(\mathbb{Q}(t)(E[n])/\mathbb{Q}(t)) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ for all n, then there is a thin set $S \subset \mathbb{Q}$ such that the specialization $\mathbb{E}_t/\mathbb{Q}$ is a Serre curve if and only if $t \notin S$. What makes this particular surface nice, is that the set S can actually be completely determined up to a bounded number of exceptions.

1.1. **Overview of the Proof of the Main Theorem.** Before we start to outline the proof of the main theorem, we need to address some potential complications that arise from the possible entanglement between the fields of definition of the 2 and 3 torsion points of an elliptic curve. In their paper [BJ14], Brau and Jones describe a genus 0 modular curve $X'(6)$ whose points correspond to $\bar{\mathbb{Q}}$-isomorphism classes of elliptic curves, whose 2 and 3-torsion fields are more entangled than predicted making them *not* Serre curves. The corresponding curves have the property that the field of definition of the 3-torsion points *completely* contained the field of definition of the 2-torsion points. Thus, the image of associated Galois representation must have index greater than two in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ since the image of the mod 6 representation has index greater than 2 in $\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$.

Theorem 1.7. [BJ14, Theorem 1.4] *There exists a uniformizer $h : X'(6) \to \mathbb{P}^1$ with the property that*

$$j_6 = 2^{10}3^3h^3(1 - 4h^3),$$

where $j_6 : X'(6) \to X(1)$ is the map that gives the j-invariant of the $\bar{\mathbb{Q}}$-equivalence class corresponding to points on $X'(6)$.

With this theorem we are now ready to start discussing the proof of Theorem 1.4. The main tool that we will use to prove Theorem 1.6 will be the following theorem:

Theorem 1.8. [BJ14, Theorem 1.6] *Suppose that $E/\mathbb{Q}$ is an elliptic curve. Then E is a Serre curve if and only if*

1. *E has no exceptional primes,*
2. *4 and 9 are not exceptional for E, and*
3. *$j(E) \notin j_6(X'(6)(\mathbb{Q}))$.*

Condition (1) is enough to assure that the p-adic Galois representation associated to E is surjective for all $p \geq 5$. While conditions (2) and (3) ensure that not only are the 2-adic and 3-adic Galois representations surjective, but also that if the entanglement predicted by Serre happens between the 2 and 3 torsion fields, then the 2-torsion field is not completely contained inside of the 3-torsion fields.

On its surface, condition (1) seems like it would be difficult to check since it requires showing the surjectivity of an infinite family of mod p representations. Fortunately, if E is semi-stable, all but a finite number of primes are covered by a result due to Mazur.

Theorem 1.9. [Maz78, Theorem 4] *Let E be a semi-stable elliptic curve defined over $\mathbb{Q}$, and p a prime number. Then the image of $\rho_{E,p}$ is $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ if $p \geq 11$.*

Therefore, if we can establish that $\mathbb{E}_t$ is semi-stable for all $t \in \mathbb{Q}$ such that $\mathbb{E}_t$ is nonsingular, then we will have reduced checking condition (1) of Theorem 1.8 to checking if 2, 3, 5, and 7 are exceptional for $\mathbb{E}_t$. In order to do this, we will need the following proposition about Galois representations associated to semi-stable elliptic curves.

Proposition 1.10. [Ser96, §3.1, Proposition 1] *and* [CR01, Proposition 1.1, page 156] *Let E be a semi-stable elliptic curve and p a prime. Then $\bar{\rho}_{E,p}$ is surjective if and only if it is irreducible.*

Thus, the first step to determine which specializations of $\mathbb{E}$ are Serre curves is to find when the corresponding mod p Galois representations are irreducible. To check which specializations of the elliptic surface $\mathbb{E}$ satisfy condition (2) of Theorem 1.8 we simply need to establish for which values of $t \in \mathbb{Q}$ are $\bar{\rho}_{\mathbb{E}_t,4}$ and $\bar{\rho}_{\mathbb{E}_t,9}$ both surjective. Lastly, for condition (3), we need to check which specializations of $\mathbb{E}$ correspond to points on the modular curve $X'(6)$. To do this we will find all of the rational solutions to the equation $j(\mathbb{E}_t) = j_6(h)$.

2. Semi-stability of the $\mathbb{E}_t$'s

Definition 2.1. Let $E/\mathbb{Q}$ be an elliptic curve, and let $\widetilde{E}$ be the reduction modulo some prime p of a minimal Weirestrass equation for E.

(1) We say that E has *good* (or *stable*) *reduction* if $\widetilde{E}$ is nonsingular.
(2) We say that E has *multiplicative* (or *semi-stable*) *reduction* if $\widetilde{E}$ has a node.
(3) We say that E has *additive* (or *unstable*) *reduction* if $\widetilde{E}$ has a cusp.

In both cases (2) and (3) we say that E has *bad reduction*.

Proposition 2.2. [Sil09, Proposition 5.1] *Let $E/\mathbb{Q}$ be an elliptic curve given by a minimal Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2a^2 + a_4x + a_6.$$

Let Δ be the discriminant of E and let $c_4 = (a_1^2 + 4a_4)^2 + 24(2a_4 + a_1a_3)$.

(1) *E has good reduction at p if and only if $p \nmid \Delta$.*
(2) *E has multiplicative reduction at p if and only if $p \mid \Delta$ and $p \nmid c_4$.*
(3) *E has additive reduction at p if and only if $p \mid \Delta$ and $p \mid c_4$.*

Definition 2.3. A *semi-stable* elliptic curve is an elliptic curve that has bad reduction only of multiplicative type.

Proposition 2.4. *Let $t \in \mathbb{Q}$ with $t \neq 0$, or $\frac{-1}{432}$, then the specialization $\mathbb{E}_t$ is a semi-stable elliptic curve.*

Proof: In this case, the discriminant of $\mathbb{E}_t$ is $\Delta_t = -t(432t+1) \neq 0$ and $c_{4,t} = 1$. Clearly, $\gcd(\Delta_t, c_{4,t}) = 1$ for all $t \in \mathbb{Q}$ and so the only possible type of bad reduction for the specialization $\mathbb{E}_t$ is multiplicative. ∎

3. Irreducible Representations and Division Polynomials

The next step in our proof is to determine for what values of t are 2, 3, 5 or 7 exceptional for $\mathbb{E}_t$. Before we start it will be worthwhile to develop a better understanding of what it means for the mod p Galois representation of an elliptic curve to be irreducible.

Suppose that E is an elliptic curve and p is a prime such that $\bar{\rho}_{E,p}$ is reducible, i.e. not irreducible. This means there must be a nontrivial proper subspace of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ that is fixed by $\operatorname{Im} \bar{\rho}_{E,p}$. Suppose that V is the proper subspace of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ that is fixed by $\operatorname{Im} \bar{\rho}_{E,p}$. Since V is a nontrivial proper subspace, it must be of the form $V = \langle \mathbf{v} \rangle$ for some $\mathbf{v} \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. In fact, $\{\mathbf{v}\}$ can be expanded to be a basis for all of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Fixing that basis $\mathcal{B} = \{\mathbf{v}, \mathbf{w}\}$ for $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and noting that V is stable under the action of $\operatorname{Im} \bar{\rho}_{E,p}$, we get that under this basis, the group $\operatorname{Im} \bar{\rho}_{E,p}$ must be contained in a subgroup of the form

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b \in (\mathbb{Z}/p\mathbb{Z})^\times, c \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

Using the algebraic interpretation of $\bar{\rho}_{E,p}$ as a representation of the action of $G_\mathbb{Q}$ on $E[p]$, we see that that there must be a point $P \in E[p]$, such that for each $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, there is an $a_\sigma \in \mathbb{Z}/p\mathbb{Z}$ such that $\sigma(P) = a_\sigma \cdot P$. That is, the subgroup $H = \langle P \rangle \subset E[p]$ is stable under the action of the Galois group. In particular, since the action of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is component-wise, the x-coordinates of the points in H are stable under the action $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The x-coordinates of the points if $E[p]$ are roots of the p-division polynomial f_p. The fact that there is a Galois stable subgroup means that the p-division polynomial must be reducible. This discussion gives the following proposition.

Proposition 3.1. *Let E be an elliptic curve and let p be a prime. Then $\bar{\rho}_{E,p}$, is irreducible if and only if the p-division polynomial of E is irreducible.*

Corollary 3.2. *If E is a semi-stable elliptic curve and p is a prime, then $\bar{\rho}_{E,p}$ is surjective if and only if the p-division polynomial of E irreducible.*

Proof: This follows immediately from Propositions 1.10 and 3.1. ∎

4. Condition (1)

4.1. **Determining when 2 is Exceptional for $\mathbb{E}_t$.** From the fact that the $\mathbb{E}_t$'s are semi-stable and Corollary 3.2, we know that 2 is exceptional for $\mathbb{E}_t$ if and only if the 2-division polynomial for $\mathbb{E}_t$ is irreducible over $\mathbb{Q}$.

Proposition 4.1. *Let $t \in \mathbb{Q}$ with $t \neq 0$ or $\frac{-1}{432}$. The 2-division polynomial of $\mathbb{E}_t$ is reducible if and only if there exists $c \in \mathbb{Q}$ such that $t = -\frac{1}{4}(c^2 + 4c^3)$.*

Proof: Let $t \in \mathbb{Q}$ with $t \neq 0$ or $\frac{-1}{432}$. The 2-division polynomial of $\mathbb{E}_t$ is given by $f_t(x) = 4x^3 + x^2 + 4t$. Since $\deg(f_t) = 3$, we know that $f_t(x)$ is reducible over $\mathbb{Q}$ if and only if it has a root. That is to say that $f_t(x)$ is reducible over $\mathbb{Q}$ if and only if there exists $a, b, c \in \mathbb{Q}$ such that $f_t(x) = (x - c)(4x^2 + ax + b)$. Inserting $f_t(x)$ into the equality and expanding the right side gives that $f_t(x)$ factors if and only there are $a, b, c \in \mathbb{Q}$ such that

$$4x^3 + x^2 + 4t = 4x^3 + (a - 4c)x^2 + (b - ac)x + -bc.$$

From here we get the following system of equations:

$$\begin{aligned} a - 4c &= 1 \\ b - ac &= 0 \\ -bc &= 4t. \end{aligned}$$

Solving the first two equation for a and b in terms of c and plugging into the third gives $f_t(x)$ is reducible if and only if $t = -\frac{1}{4}(c^2 + 4c^3)$. ∎

Corollary 4.2. *Let $S_2 = \left\{ -\frac{1}{4}(c^2 + 4c^3) : c \in \mathbb{Q} \right\}$, then $\overline{\rho}_{\mathbb{E}_t,2}$ is surjective if and only if $t \notin S_2$.*

4.2. **Determining when 3 is Exceptional for $\mathbb{E}_t$.** Determining when $\bar{\rho}_{\mathbb{E}_t,3}$ is not surjective is slightly more complicated since the degree of the 3-division polynomial is larger. Fortunately the degree is only 4, so in this case we can simply break this question up into two different cases. The first case is when the three division polynomial has a linear factor, while the second case is when the 3-division polynomial factors into two irreducible quadratics.

Proposition 4.3. *Let $t \in \mathbb{Q}$ with $t \neq 0$, or $\frac{-1}{432}$. The 3-division polynomial of the elliptic curve $\mathbb{E}_t$ has a linear factor if and only if there exists $d \in \mathbb{Q}$ such that $t = -\frac{(3d+1)d^3}{(1+12d)}$.*

Proof: The 3-division polynomial of $\mathbb{E}_t$ is given by $g_t(x) = 3x^4 + x^3 + 12tx + t$. Clearly, $g_t(x)$ has a linear factor in $\mathbb{Q}[x]$ if and only if there exists $a, b, c, d \in \mathbb{Q}$ such that $g_t(x) = (x-d)(3x^3 + ax^2 + bx + c)$. Again, expanding the right hand side we get that

$$3x^4 + x^3 + 12tx + t = 3x^4 + (a-3d)x^3 + (b-ad)x^2 + (c-bd)x - cd.$$

Setting the coefficients equal to each other we get, the following system of equations:

$$\begin{aligned} a - 3d &= 1, \\ b - ad &= 0, \\ c - bd &= 12t, \\ -cd &= t. \end{aligned}$$

Solving the first three equations for a, b, and c respectively, plugging into the fourth, and then solving for t gives that $t = -\frac{(3d+1)d^3}{(1+12d)}$. ∎

Proposition 4.4. *Let $t \in \mathbb{Q}$ with $t \neq 0$, or $\frac{-1}{432}$. The 3-division polynomial of the elliptic curve $\mathbb{E}_t$ never factors into the product of 2 irreducible rational quadratics.*

Proof: The 3-division polynomial of $\mathbb{E}_t$ factors into the product of 2 irreducible quadratics in $\mathbb{Q}[x]$ if and only if there exists $a, b, c, d \in \mathbb{Q}$ such that $g_t(x) = (3x^2 + ax + b)(x^2 + bx + c)$. Expanding this we get

$$3x^4 + x^3 + 12tx + t = 3x^4 + (3c + a)x^3 + (3d + ac + b)x^2 + (ad + bc)x = bd,$$

and the following system of equations:

$$\begin{aligned} 3c + a &= 1, \\ 3d + ac + b &= 0, \\ ad + bc &= 12t, \\ bd &= t. \end{aligned}$$

Solving the first two equations for a and b respectively and plugging into the last two equation gives

$$12t = d - 6cd - c^2 + 3c^3, \tag{4.1}$$

$$t = -3d^2 + 3c^2d - cd. \tag{4.2}$$

Plugging the equation (4.2) into equation (4.1) we get that (c, d) must be a rational point on the affine curve with defining equation

$$12(-3d^2 + 3c^2d - cd) = d - 6cd - c^2 + 3c^3.$$

Changing to projective coordinates, we can see that we are looking for points on the affine patch $F \neq 0$ of the curve

$$C_3 : 12(-3D^2F + 3C^2D - CDF) = DF^2 - 6CDF - C^2F + 3C^3.$$

Preforming a change of variables given by $X = \frac{1}{324}C$, $Y = \frac{1}{2916}D$ and $X = 6C + 36D + E$ we see that this is in fact an elliptic curve given by the

$$E_3 : Y^2Z + \frac{1}{54}XYZ - \frac{1}{104976}YZ^2 = X^3 - \frac{1}{2916}X^2Z.$$

Thus, the rational points on C_3 are in bijection with the rational points on E_3 which form a group isomorphic to $\mathbb{Z}/6\mathbb{Z}$ and so we know that $\#C(\mathbb{Q}) = 6$. A quick search shows that

$$C(\mathbb{Q}) = \{[0:1:0], [0:-1/36:1], [0:0:1], [12:1:0], [1/3:0;1], [1/3:1/36:1]\}.$$

Plugging the points in the affine patch $F \neq 0$ back into equation (4.2) we get that these correspond to the values $t = 0$ or $t = -\frac{1}{432}$.

■

Corollary 4.5. *Let $t \in \mathbb{Q}$ with $t \neq 0$, or $\frac{-1}{432}$ and let $S_3 = \left\{ -\frac{(3d+1)d^3}{(1+12d)} \;\middle|\; d \in \mathbb{Q} \right\}$. Then $\bar{\rho}_{\mathbb{E}_t,3}$ is surjective if and only if $t \notin S_3$.*

4.3. **Determining when 5 is Exceptional for $\mathbb{E}_t$.** As the primes that we need to consider grow, so does the degree of the division polynomials in question and it quickly becomes obvious that our approach needs to change. The degree of the 5-division polynomial for $\mathbb{E}_t$ is 12, so checking all the possible ways that it can factor is no longer feasible. Fortunately, there is a well developed theory of coarse moduli spaces of elliptic curves with proper $G_{\mathbb{Q}}$-stable subgroups of their n-torsion (or rational isogenies). As discussed in Section 3, since $\mathbb{E}_t$ is semi-stable for $t \neq 0$, or $\frac{-1}{432}$, for a fixed n, $\bar{\rho}_{\mathbb{E}_t,n}$ is either surjective, or the n-torsion points have a proper $G_{\mathbb{Q}}$-stable subgroup. Elliptic curves with a $G_{\mathbb{Q}}$-stable subgroup of their n-torsion points correspond to points on the modular curve $X_0(n)$. So our technique now is to determine which values of $t \in \mathbb{Q}$ give an elliptic curves $\mathbb{E}_t$ that corresponds to a point on the modular curve $X_0(5)$.

From [LR13, Table 3], we know that the curve $X_0(5)$ is a genus zero curve isomorphic to $\mathbb{P}^1$ and there is a map $j_5 : X_0(5) \to X(1)$ that takes a point on $X_0(5)$ and returns the j-invariant of corresponding elliptic curve with a proper $G_{\mathbb{Q}}$-stable subgroup of its 5-torsion points given by $h \mapsto \frac{(h^2+10h+5)^3}{h}$. So we need to determine for what values of $t \in \mathbb{Q}$ is there an $h \in \mathbb{Q}$ such that $j_5(h) = j(\mathbb{E}_t)$. In other words, we need to find all of the rational solutions to $\frac{(h^2+10h+5)^3}{h} = \frac{-1}{432t^2+t}$. Clearing denominators, we see that this is the same as finding the rationals points on the affine curve given by

$$(h^2 + 10h + 5)^3(432t^2 + t) + h = 0$$

with $h \neq 0$ and $t \neq 0$, or $\frac{-1}{432}$. Rather than working with this affine equation, we will look for rational points on the projective curve

$$C_5 : (H^2 + 10HW + 5W^2)^3(432T^2 + TW) + HW^7 = 0,$$

with $T \neq 0$, or $\frac{-1}{432}$, $H \neq 0$, and $W = 1$.

Proposition 4.6. *Let C_5 be the projective curve defined by*

$$C_5 : (H^2 + 10HW + 5W^2)^3(432T^2 + TW) + HW^7 = 0.$$

There exists a birational map from C_5 the elliptic curve E_5 given by the projective Weierstrass equation

$$E_5 : Y^2Z + 16XYZ + 716YZ^2 = X^3 + 94X^2Z + 2605XZ^2 + 18612Z^3,$$

that is well-defined on $C_5(\mathbb{Q})$ when $W \neq 0$.

Proof: Let $\varphi : C_5 \to E_5$ with $\varphi = [\varphi_1 : \varphi_2 : \varphi_3]$ given by

$$\begin{aligned}
\varphi_1([T:H:W]) &= 432TH^4W + 8640TH^3W^2 + H^4W^2 + 47520TH^2W^3 + 20H^3W^3 \\
&\quad + 43200THW^4 + 63H^2W^4 + 10800TW^5 - 52HW^5 + 36W^6, \\
\varphi_2([T:H:W]) &= 432TH^5 + 8640TH^4W + H^5W + 47520TH^3W^2 + 20H^4W^2 + 43200TH^2W^3, \\
&\quad + 110H^3W^3 + 10800THW^4 + 136H^2W^4 - 11HW^5 \\
\varphi_3([T:H:W]) &= H^2W^4 + 4HW^5 - W^6.
\end{aligned}$$

Notice that $\varphi_3 \neq 0$ if $W \neq 0$ and $H \neq W(2 \pm \sqrt{5})$ and so φ is well-defined on $C_5(\mathbb{Q})$ when $W \neq 0$. To show that φ is a degree 1 map, we simply demonstrate its birational inverse $\psi : E_5 \to C_5$. Let $\psi = [\psi_1 : \psi_2 : \psi_3]$ be given by

$$\begin{aligned}
\psi_1([X:Y:Z]) =& 4680XZ^3 + 1950YZ^3 + 56160Z^4,\\
\psi_2([X:Y:Z]) =& -6630X^2Y^2 - 1950XY^3 - 39390X^2YZ - 211770XY^2Z - 39780Y^3Z + 56160X^2Z^2\\
&- 866580XYZ^2 - 1379820Y^2Z^2 + 954720XZ^3 - 4976790YZ^3 + 3369600Z^4,\\
\psi_3([X:Y:Z]) =& -1950X^2Y^2 - 99060X^2YZ - 132600XY^2Z - 6630Y^3Z - 196950X^2Z^2\\
&- 3020550XYZ^2 - 1650480Y^2Z^2 - 5456100XZ^3 - 22192170YZ^3 - 36509070Z^4.
\end{aligned}$$

Using Magma, we check that $\varphi \circ \psi$ is the identity map on the domain of ψ and $\psi \circ \varphi$ is the identity on the domain of φ. ∎

From Proposition 4.6, we can find all of the points in $C_5(\mathbb{Q})$ with $W \neq 0$ by computing the image of the rational points on E_5 under ψ. The rational points on E_5 form a group isomorphic to $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and in fact $E_5(\mathbb{Q}) = \langle [-51:40:1], [-56:90:1] \rangle$ where $[-51:40:1]$ has infinite order and $[-56:90:1]$ has order 2. Letting $P_1 = [-51:40:1]$, $P_2 = [-56:90:1]$, and $P = mP_1 + nP_2$, we compute the image of some of the points on E_5 normalized to have $W = 1$ or 0.

(m,n)	$(-1,0)$	$(-1,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$\psi(P)$	$\left[\frac{-3}{1280} : -15 : 1\right]$	$\left[\frac{11}{6912} : -11 : 1\right]$	undefined	$\left[\frac{-2}{135} : -10 : 1\right]$	$\left[\frac{1}{80} : -10 : 1\right]$	$[0:1:0]$

Since we are only interested in the points on $C_5(\mathbb{Q})$ in the affine patch $W \neq 0$, we let U be the subset of $E_5(\mathbb{Q})$ such that ψ_3 is nonzero. Define $\xi_5 : U \to \mathbb{Q}$ by $\xi_5 = \frac{\psi_1}{\psi_3}$ and $S_5 = \{\xi_5(P) | P \in U\}$.

Corollary 4.7. *Let S_5 be defined as above and let $t \in \mathbb{Q}$ such that $t \neq 0$ or $\frac{-1}{432}$. Then $\bar{\rho}_{\mathbb{E}_t,5}$ is surjective if and only if $t \notin S_5$.*

4.4. **Determining when 7 is Exceptional for $\mathbb{E}_t$.** Again, from [LR13, Table 3] we know that when $n = 7$, the curve $X_0(7)$ is genus zero and the map $j_7 : X_0(7) \to X(1)$ is given by $h \mapsto \frac{(h^2+13h+49)(h^2+5h+1)^3}{h}$. So to determine which rational specializations of $\mathbb{E}$ have nonsurjective mod 7 Galois representation, it is enough to find all the rational solutions to $j_7(h) = j(\mathbb{E}_t)$. This is the same as finding all the rational points on the affine curve

$$(h^2 + 13h + 49)(h^2 + 5h + 1)^3(432t^2 + t) + h = 0$$

with $h \neq 0$ and $t \neq 0$, or $\frac{-1}{432}$. Instead of working with this affine equation, we will look for rational points on the projective curve

$$C_7 : (H^2 + 13HW + 49W^2)(H^2 + 5HW + W^2)^3(432T^2 + TW) + HW^9 = 0,$$

with $T \neq 0$, or $\frac{-1}{432}$, $H \neq 0$, and $W = 1$.

Proposition 4.8. *Let C_7 be the projective curve given by the equation*

$$C_7 : (H^2 + 13HW + 49W^2)(H^2 + 5HW + W^2)^3(432T^2 + TW) + HW^9 = 0.$$

There exists a birational map from C_7 the elliptic curve E_7 given by the projective Weierstrass equation

$$E_7 : Y^2Z + 9XYZ + 141YZ^2 = X^3 + 34X^2Z + 349XZ^2 + 1020Z^3,$$

that is well-defined on $C_7(\mathbb{Q})$ when $W \neq 0$.

PROOF: Let $\varphi : C_7 \to E_7$ with $\varphi = [\varphi_1 : \varphi_2 : \varphi_3]$ given by

$$\begin{aligned}
\varphi_1([T:H:W]) =& 432TH^6W + 9936TH^5W^2 + H^6W^2 + 88992TH^4W^3 + 23H^5W^3 + 367632TH^3W^4 \\
&+ 189H^4W^4 + 628128TH^2W^5 + 625H^3W^5 + 217296THW^6 + 503H^2W^6 \\
&+ 21168TW^7 - 375HW^7 + 84W^8, \\
\varphi_2([T:H:W]) =& 432TH^7 + 9936TH^6W + H^7W + 88992TH^5W^2 + 23H^6W^2 + 367632TH^4W^3 \\
&+ 206H^5W^3 + 628128TH^3W^4 + 863H^4W^4 + 217296TH^2W^5 \\
&+ 1574H^3W^5 + 21168THW^6 + 815H^2W^6 - 35HW^7, \\
\varphi_3([T:H:W]) =& H^4W^4 + 14H^3W^5 + 63H^2W^6 + 70HW^7 - 7W^8.
\end{aligned}$$

Notice that if $W \neq 0$, then φ_3 is zero if and only if $H = \frac{-7+\sqrt{-7}\pm\sqrt{2\sqrt{7}-7}}{2}W$ or $\frac{-7-2\sqrt{7}\pm i\sqrt{4\sqrt{7}+7}}{2}W$. Therefore, φ is well-defined on $C_7(\mathbb{Q})$ when $W \neq 0$. To show that φ is degree 1, we write down its birational inverse. Let $\psi : E_7 \to C_7$ be $\psi = [\psi_1 : \psi_2 : \psi_3]$ given by

$$\begin{aligned}
\psi_1([X:Y:Z]) =& 4680XZ^3 + 1950YZ^3 + 56160Z^4, \\
\psi_2([X:Y:Z]) =& -6630X^2Y^2 - 1950XY^3 - 39390X^2YZ - 211770XY^2Z - 39780Y^3Z \\
&+ 56160X^2Z^2 - 866580XYZ^2 - 1379820Y^2Z^2 + 954720XZ^3 - 4976790YZ^3 \\
&+ 3369600Z^4, \\
\psi_3([X:Y:Z]) =& -1950X^2Y^2 - 99060X^2YZ - 132600XY^2Z - 6630Y^3Z - 196950X^2Z^2 \\
&- 3020550XYZ^2 - 1650480Y^2Z^2 - 5456100XZ^3 - 22192170YZ^3 - 36509070Z^4.
\end{aligned}$$

Using Magma, we check that $\varphi \circ \psi$ is the identity map on the domain of ψ and that $\psi \circ \varphi$ is the identity on the domain of φ. ∎

From Proposition 4.8, we can find all of the points in $C_7(\mathbb{Q})$ with $W \neq 0$ by computing the image of the rational points on E_5 under ψ. The group $E_7(\mathbb{Q}) = \langle [-17:0:1], [-21:24:1] \rangle$ where $[-17:0:1]$ has infinite order and $[-21:24:1]$ has order 2. Letting $P_1 = [-17:0:1]$, $P_2 = [-21:24:1]$, and $P = mP_1 + nP_2$, we compute the image of some of the points on E_5 normalized to have $W = 1$ or 0.

(m,n)	$(-1,0)$	$(-1,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$\psi(P)$	$[0:1:0]$	$\left[\frac{2}{1323} : -6 : 1\right]$	Undefined	$\left[-\frac{3}{784} : -6 : 1\right]$	$\left[\frac{5}{144} : -5 : 1\right]$	$\left[-\frac{1}{441} : 1 : 1\right]$

Since we are only interested in the T-coordinates of the points on $C_7(\mathbb{Q})$ with $W = 1$, we let U be the subset of $E_7(\mathbb{Q})$ such that ψ_3 is nonzero. Define $\xi_7 : U \to \mathbb{Q}$ by $\xi_7 = \frac{\psi_1}{\psi_3}$ and $S_7 = \{\xi_7(P) | P \in U\}$.

Corollary 4.9. *Let S_7 be defined as above and let $t \in \mathbb{Q}$ such that $t \neq 0$ or $\frac{-1}{432}$. Then $\bar{\rho}_{\mathbb{E}_t,7}$ is surjective if and only if $t \notin S_7$.*

Example 4.10. Given an integer, it is isn't difficult to check if that integer is in S_2, S_3, S_5 or S_7. All one has to do is look at the corresponding elliptic curves division polynomials and see if it factors. Using this method, one can easily show that if ℓ is an odd prime that is not 7, then $\ell \notin S_2 \cup S_3 \cup S_5 \cup S_7$ since the 2, 3, 5, and 7 division polynomials of $\mathbb{E}_\ell$ are irreducible. Therefore, the infinite family of curves $\mathbb{E}_\ell$ for ℓ an odd prime note equal to 7 all satisfy condition 1. The reason we have to avoid 7 is because the curve $\mathbb{E}_7$ has a 2 torsion point; that is, $7 \in S_2$ since $7 = -\frac{1}{4}((-2)^2 + (-2)^3)$.

5. CONDITION (2)

We are now ready to start determining which specializations of $\mathbb{E}$ satisfy condition (2) of Theorem 1.8.

5.1. **Determining when 4 is Exceptional for $\mathbb{E}_t$.**

Theorem 5.1. [DD12] *Let E be an elliptic curve over $\mathbb{Q}$ with discriminant Δ and j-invariant $j(E)$. Then, $\bar{\rho}_{E,4}$ is surjective if and only if $\bar{\rho}_{E,2}$ is surjective and $-\Delta$ is not a non-zero square in $\mathbb{Q}$ and $j(E) \neq -4h^3(h+8)$ for any $h \in \mathbb{Q}$.*

So we start by determining for which values of $t \in \mathbb{Q}$ is $-\Delta_t$ a nonzero square. Note, $-\Delta_t = 432t^2 + t$ and so we simply need to determine for what values of t is $432t^2 + t$ a square.

Proposition 5.2. *Let $t \in \mathbb{Q}$ with $t \neq 0$ or $\frac{-1}{432}$ then $-\Delta_t$ is a square if and only if $t \in \left\{ \frac{1}{m^2-432} \mid m \in \mathbb{Q} \right\}$*

Proof: To prove the lemma we simply need to find all the rational solutions to the equation $y^2 = 432t^2 + t$. To find all of the rational points on this conic, we simply start with with a given solution, namely (0,0), and draw a line of rational slope and look for the second point of intersection. It is a classical argument that a point on the curve is rational if and only if it is on a line of rational slope through a the initial fixed rational point.

We start with the point $P = (0, 0)$ on the conic $y^2 = 432t^2 + t$ and write down the equation of the line through P of slope m. The line is given by $y = mt$, plugging into the equation in question we get $(mt)^2 = 432t^2 + t$. Moving everything over to one side, we get that $[(m^2 - 432)t - 1]t = 0$, which is possible if and only if $t = 0$ or $t = \frac{1}{m^2-432}$. Thus, $-\Delta_t$ is a nonzero rational square if and only if $t \in \left\{ \frac{1}{m^2-432} \mid m \in \mathbb{Q} \right\}$. ■

Next, we need to determine when the j-invariant of $\mathbb{E}_t$ is of the form $-4h^3(h + 8)$ for some $h \in \mathbb{Q}$. This is the same as finding all the rational points on

$$C_4 : -4H^3(H + 8W)(432T^2 + TW) + W^6 = 0,$$

with $T \neq 0$ or $\frac{-1}{432}$, $H \neq 0$, and $W = 1$.

Proposition 5.3. *Let C_4 be the projective curve given by the equation*

$$C_4 : -4H^3(H + 8W)(432T^2 + TW) + W^6 = 0.$$

There exists a birational map from C_4 the elliptic curve E_4 given by the projective Weierstrass equation

$$E_4 : Y^2Z + 2XYZ + 12YZ^2 = X^3 - 24X^2Z + 180XZ^2 - 432Z^3,$$

that is well-defined on $C_4(\mathbb{Q})$ when $W \neq 0$ except at the point $\left[\frac{-1}{864} : -6 : 1\right]$.

Proof: Let $\varphi : C_4 \to E_4$ with $\varphi = [\varphi_1 : \varphi_2 : \varphi_3]$ given by

$$\begin{aligned}
\varphi_1([T : H : W]) =& 432TH^3W + 3456TH^2W^2 + H^3W^2 + 8H^2W^3 + 12HW^4 + 36W^5, \\
\varphi_2([T : H : W]) =& 432TH^4 + 3456TH^3W + H^4W + 8H^3W^2 - 36HW^4, \\
\varphi_3([T : H : W]) =& HW^4 + 6W^5.
\end{aligned}$$

Notice that if $W \neq 0$ and $H \neq -6W$, then φ_3 is not zero and so φ is well-defined. So we look to see what points have $W \neq 0$ and $H = -6W$. Plugging $-6W$ in for H we get

$$746496T^2W^4 + 1728TW^5 + W^6 = 0.$$

Next, since $W \neq 0$ we know that we can normalize so that $W = 1$ and get $746496T^2 + 1728T + 1 = 0$, which factors as $(864T + 1)^2 = 0$. Therefore, there is only one point that with $W \neq 0$ such that φ possibly isn't well-defined, namely $Q = \left[\frac{-1}{864} : -6 : 1\right]$. One easily checks that in fact φ is not well-defined at Q, but this is the only point, so we simply keep it in mind when we define the set S_4.

We show that φ is a degree 1 map by demonstrating down its birational inverse, ψ. Let $\psi : E_4 \to C_4$ be $\psi = [\psi_1 : \psi_2 : \psi_3]$ given by

$$\begin{aligned}\psi_1([X:Y:Z]) &= -XZ^2 + 12Z^3,\\ \psi_2([X:Y:Z]) &= -4X^2Y + 48XYZ - 16Y^2Z - 144YZ^2,\\ \psi_3([X:Y:Z]) &= -24XYZ - 4Y^2Z + 144YZ^2.\end{aligned}$$

Using Magma we check that ψ is the birational inverse of φ defined on the image of φ. ∎

From Proposition 5.3, we can find all of the rational points on C_4 by finding the image of all of the rational points on E_4 under ψ, together with the point $\left[\frac{-1}{864} : -6 : 1\right]$. Fortunately, the curve E_4 has rank 0 over $\mathbb{Q}$ and $E_4(\mathbb{Q}) = \langle [6:0:1] \rangle \cong \mathbb{Z}/8\mathbb{Z}$. Thus, we can compute the complete image of $E_4(\mathbb{Q})$ under ψ and find all the points on $C_4(\mathbb{Q})$ with $W \neq 0$. Let $P = [6:0:1] \in E_4(\mathbb{Q})$.

n	0	1	2	3	4	5	6	7
$\psi(nP)$	Undef.	$[1:0:0]$	$[0:1:0]$	$\left[\frac{1}{3456} : 4 : 1\right]$	$\left[\frac{1}{108} : 1 : 1\right]$	$[1:0:0]$	Undef.	$\left[\frac{-1}{384} : 4 : 1\right]$

Here we notice that one of T values in the table and the T-value of the point where φ is not well-defined are both already in S_2. That is, $\frac{-1}{864}$ and $\frac{1}{108}$ are in S_2 since $\frac{-1}{864} = -\frac{1}{4}\left(\left(\frac{-1}{12}\right)^2 + 4\left(\frac{-1}{12}\right)^3\right)$ and $\frac{1}{108} = -\frac{1}{4}\left(\left(\frac{-1}{3}\right)^2 + 4\left(\frac{-1}{3}\right)^3\right)$.

Corollary 5.4. *Let* $S_4 = \left\{\frac{1}{m^2-432} \mid m \in \mathbb{Q}\right\} \cup \left\{\frac{-1}{384}, \frac{1}{3456}\right\}$. *Let* $t \in \mathbb{Q}$ *such that* $t \neq 0$ *or* $\frac{-1}{432}$. *Then* $\bar{\rho}_{\mathbb{E}_t,4}$ *is surjective if and only if* $t \notin S_2 \cup S_4$.

Example 5.5. Let ℓ be an odd prime with $\ell \neq 7$, then $\ell \notin S_2$ and is in S_4 if and only if there exists $m \in \mathbb{Q}$ such that $\frac{1}{m^2-432} = \ell$. Solving for m^2, we get that ℓ is in S_4 if and only if there is an $m \in \mathbb{Q}$ such that $m^2 = \frac{1+432\ell}{\ell}$, but this is not possible since $\frac{1+432\ell}{\ell}$ cannot be a rational square when ℓ is prime. Thus, when ℓ is an odd prime and $\ell \neq 7$, $\bar{\rho}_{\mathbb{E}_\ell,4}$ is surjective.

5.2. **Determining when 9 is Exceptional for $\mathbb{E}_t$.** In [Elk06], the Elkies shows that there is a subgroup, G, of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$, unique up to conjugation, such that the natural reduction map $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ restricted to G is actually an isomorphism. Therefore, the preimage of G in $\mathrm{SL}_2(\mathbb{Z}_3)$ is a proper closed subgroup that surjects onto $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. Therefore, it is possible that there exists an elliptic curve E such that the image of $\bar{\rho}_{E,9}$ is contained in G. In this case, we would have an elliptic curve with the property that $\bar{\rho}_{E,3}$ is surjective and $\bar{\rho}_{E,9}$ is not. Therefore, it is not sufficient to check that $\bar{\rho}_{E,3}$ to conclude that ρ_{E_3} is surjective. Fortunately, it is true that if $\bar{\rho}_{E,9}$ is surjective, then so is $\rho_{E,3}$. Further, in the same paper, Elkies completely classifies all of the elliptic curves with surjective mod 3 representation and non-surjective mod 9 representation.

Theorem 5.6. [Elk06] *Elliptic curves with surjective mod* 3 *representation whose mod* 9 *representation fails to be surjective have* j*-invariant of the form*

$$j = j_9(h) = -\frac{3^7(h^2-1)^3(h^6+3h^5+6h^4+h^3-3h^2+12h+16)^3(2h^3+3h^2-3h-5)}{(h^3-3h-1)^9},$$

for $h \in \mathbb{Q}$.

As before, we look for rational points on the appropriate curve that correspond to solutions to the equation $j_9(h) = j(\mathbb{E}_t)$.

Proposition 5.7. *Let C_9 be the projective curve given by*

$$\begin{aligned} C_9 : 0 = &(H^3 - 3HW^2 - W^3)^9 \\ &+ 3^7(H^2 - W^2)^3(H^6 + 3H^5W + 6H^4W^2 + H^3W^3 \\ &- 3H^2W^4 + 12HW^5 + 16W^6)^3(2H^3 + 3H^2W - 3HW^2 - 5W^3)(432T^2 + TW). \end{aligned}$$

There exists a birational map from C_9 to the genus 6 hyperelliptic curve given by the equation

$$\begin{aligned} H_9 : Y^2 + (X^6Z + X^5Z^2 + X^3Z^4 + X^2Z^5)Y = &X^{14} - 11X^{13}Z + 53X^{12} - 157X^{11}Z^3 + 336X^{10}Z^4 \\ &- 563X^9Z^5 + 617X^8Z^6 - 242X^7Z^7 - 151X^6Z^8 - 19X^5Z^9 + 138X^4Z^{10} \\ &+ 60X^3Z^{11} + 16X^2Z^{12} - 2XZ^{13} \end{aligned}$$

in $(1:7:1)$ weighted projective space that is well-defined on $C_9(\mathbb{Q})$ when $W \neq 0$.

Proof: Like the proofs before, we let $\varphi : C_9 \to H_9$ with $\varphi = [\varphi_1 : \varphi_2 : \varphi_3]$, but this time we abstain from giving all three equations explicitly because of their size. In this case, φ_1 and φ_3 are homogeneous of degree 14, while φ_2 has degree $7 \cdot 14 = 98$.

Unfortunately, in order to show that φ is well-defined on the points of $C_9(\mathbb{Q})$ with $W \neq 0$, we need to examine atleast one of the equations, and so we look at

$$\begin{aligned} \varphi_1([T:H:W]) = &H^{13}W + \frac{73}{7}H^{12}W^2 + \frac{228}{7}H^{11}W^3 + \frac{272}{7}H^{10}W^4 + \frac{101}{7}H^9W^5 \\ &+ \frac{45}{7}H^8W^6 - \frac{291}{7}H^7W^7 - \frac{1497}{7}H^6W^8 - \frac{1422}{7}H^5W^9 + \frac{1250}{7}H^4W^{10} \\ &+ \frac{2291}{7}H^3W^{11} - 21H^2W^{12} - \frac{1562}{7}HW^{13} - 92W^{14}. \end{aligned}$$

If $W \neq 0$, then we can normalize W to be 1 and get;

$$\begin{aligned} \varphi_1([T:H:1]) &= H^{13} + \frac{73}{7}H^{12} + \frac{228}{7}H^{11} + \frac{272}{7}H^{10} + \frac{101}{7}H^9 + \frac{45}{7}H^8 - \frac{291}{7}H^7 \\ &\quad - \frac{1497}{7}H^6 - \frac{1422}{7}H^5 + \frac{1250}{7}H^4 + \frac{2291}{7}H^3 - 21H^2 - \frac{1562}{7}H - 92 \\ &= (H+1)(H^6 + \frac{24}{7}H^5 + \frac{18}{7}H^4 - \frac{26}{7}H^3 - \frac{33}{7}H^2 + \frac{18}{7}H + 4) \\ &\quad \cdot (H^6 + 6H^5 + 4H^3 + 12H^2 - 18H - 23). \end{aligned}$$

From the equation, it is clear that φ_1 is only zero at a rational point when $H = -1$, but by inspection we see that there is no rational point with $H = -1$ and $W \neq 0$. Thus, φ_1 is nonzero on the rational points of C_9 when $W \neq 0$. ∎

All we need to do now is find all the rational points on H_9. From Falting's theorem we know a priori that the set $H_9(\mathbb{Q})$ is finite, but finding a provably complete list of the points is a difficult task. We start by examining the Jacobian of H_9 which is a 6-dimensional abelian variety into which H_9 embeds. According to Magma, the rank of the Jacobian over $\mathbb{Q}$ is 1, so $J_9(\mathbb{Q})$ has infinitely many points, only finitely many of which are coming from the points on H_9. Determining an exactly which of these infinitely many points are coming from rational points on H_9 is where the difficulty lies. The good news is that the rank is still less than the genus of the H_9 and so we can use the following theorem.

Theorem 5.8. [Sto06] *Let C be a curve of genus $g \geq 2$ over $\mathbb{Q}$. Let J be the Jacobian C and let p be a prime of good reduction. Then, if $\operatorname{rank}_{\mathbb{Q}}(J) < g$ and $p \geq 2g$, then*

$$C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2r.$$

The curve H_9 has genus 6 and according to Magma the rank of its Jacobian over $\mathbb{Q}$ is 1, so we search through some small primes of good reduction greater than $2g = 12$ to see which gives the best upper bound.

Unsurprisingly, the lowest upper bound we can find is when $p = 13$. In this case,

$$\widetilde{H_9}(\mathbb{F}_{13}) = \big\{[1:1:0],[1:12:0],[0:0:1],[2:11:1],[3:2:1],[3:4:1],[4:6:1],$$
$$[4:7:1],[5:5:1],[5:10:1],[6:9:1],[6:11:1],[9:7:1],[9:11:1]\big\}$$

Thus, from Theorem 5.8 we know that

$$\#H_9(\mathbb{Q}) \leq \#H_9(\mathbb{F}_{13}) + 2r = 14 + 2 = 16. \tag{5.1}$$

Unfortunately, this bound does not appear to be sharp. Searching for rational points on H_9 only yields 4 points,

$$H_9(\mathbb{Q}) \supseteq \big\{[1:-1:0],[1:1:0],[0:0:1],[2:-54:1]\big\}.$$

Checking the equations for φ, we see that there are no rational points on C_9 that map to any of the points that we have found. That is to say that the birational inverse of φ is not defined on points that we have found. The problem now is that are potentially 12 other points on $H_9(\mathbb{Q})$ that we cannot find or prove do not exist.

Using Magma, we search for rational points on C_9 with height bounded by 10^6, but the search only returns the two obvious points at infinity, $[1:0:0]$ and $[0:1:0]$. Thus, it is possible that there are 12 rational points of large height that we simply cannot find. Notice that there can't be anymore than 12 points unfound points as they would correspond to unique unfound points on H_9 and there are at most 12 of those from Equation (5.1). While we do not expect there to be any points other than the two that we already found, this would be rather difficult to prove and so we will settle for the following proposition:

Corollary 5.9. *Let $t \in \mathbb{Q}$ with $t \neq 0$, or $\frac{-1}{432}$. The there exists a set S_9, which is a subset of $\mathbb{Q}$, such that $\#S_9 \leq 12$ and $\bar{\rho}_{\mathbb{E}_t,9}$ is surjective if and only if $t \notin S_3 \cup S_9$.*

Example 5.10. It isn't hard to rule out a large class of possibilities for what can be in S_9. For example, it is easy to show that if $\mathbb{E}_t$ has good reduction at 2 and $t \notin S_3$, then $t \notin S_9$ using the signature of the group, G, discussed at the beginning of Section 5.2. That is, if $\mathbb{E}_t$ has good reduction at 2, then its mod 2 reduction must be $y^2 + xy = x^3 + 1$.

One quickly checks that there are 4 points on this curve. From this we know that if σ_2 is the 2-Frobenious element, and $A_2 = \bar{\rho}_{\mathbb{E}_2,9}(\sigma_2)$, then $\mathrm{Tr}(A_2) \equiv -1 \bmod 9$ and $\det(A_2) \equiv 2 \bmod 9$. So we search the proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ that surjects onto $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ worked out in [Elk06] for elements with trace -1 mod 9 and determinant 2 mod 9. It turns out that there are matrices in the group (or any of its conjugates) with this determinant and trance pair and so the image of $\bar{\rho}_{\mathbb{E}_t,9}$ cannot be contained in this proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$.

We note that if ℓ is any odd prime, then $\ell \notin S_3$ and $\mathbb{E}_\ell$ has good reduction at 2 since $\Delta_\ell = -\ell(432\ell + 1)$ is odd. Thus, by the argument above, $\bar{\rho}_{\mathbb{E}_\ell,9}$ must be surjective.

6. Condition (3)

To find which specializations satisfy condition (3), we proceed as we did in the previous sections, by looking for rational points on the appropriate curve. Recall that the map j_6 described in Theorem 1.7 is given by $h \mapsto 2^{10}3^3h^3(1 - 4h^3)$. So we are looking for rational points on

$$C_6 : 2^{10}3^3H^3(W^3 - 4H^3)(432T^2 + TW) + W^8 = 0,$$

with $T \neq 0$ or $\frac{-1}{432}$ and $W = 1$.

Proposition 6.1. *Let C_6 be the projective curve given by*

$$C_6 : 2^{10}3^3H^3(W^3 - 4H^3)(432T^2 + TW) + W^8 = 0.$$

There exists a birational map from C_4 to the elliptic curve given by the equation

$$E_6 : Y^2Z + 16384YZ^2 = X^3$$

that is well-defined on $C_5(\mathbb{Q})$ when $W \neq 0$.

PROOF: Let $\varphi : C_6 \to H_6$ with $\varphi = [\varphi_1 : \varphi_2 : \varphi_3]$ given by

$$\begin{aligned}\varphi_1([T:H:W]) &= 1769472TH^5W + 4096H^5W^2 - 442368TH^2W^4 - 768H^2W^5,\\ \varphi_2([T:H:W]) &= -113246208TH^6 - 262144H^6W + 28311552TH^3W^3 + 49152H^3W^4,\\ \varphi_3([T:H:W]) &= H^3W^4 - \frac{1}{8}W^7.\end{aligned}$$

Notice that $\varphi_3 = 0$ on $C_6(\mathbb{Q})$ when $W = 0$ or $H = \frac{1}{2}W$. A quick check show that there is no point in $C_6(\mathbb{Q})$ with $W \neq 0$ and $H = \frac{1}{2}W$. Thus, φ is well-defined when on $C_6(\mathbb{Q})$ when $W \neq 0$.

Again, we show that φ is a degree 1 map by writing down its birational inverse, ψ, which is defined of the image φ. Let $\psi : E_6 \to C_4 = 6$ be $\psi = [\psi_1 : \psi_2 : \psi_3]$ given by

$$\begin{aligned}\psi_1([X:Y:Z]) &= -1073741824XZ^2,\\ \psi_2([X:Y:Z]) &= 27Y^3 + 884736Y^2Z,\\ \psi_3([X:Y:Z]) &= -1728XY^2 - 56623104XYZ.\end{aligned}$$

One easily checks that ψ is the birational inverse of φ defined on the image of φ. ∎

We can use Proposition 6.1 to find all of the points on $C_6(\mathbb{Q})$ with $W \neq 0$. A quick analysis shows that $E_6(\mathbb{Q}) = \langle [0:0:1] \rangle = \{[0:-16384:1], [0:0:1], [0:1:0]\} \cong \mathbb{Z}/3\mathbb{Z}$. Plugging these points into ψ and looking for points with $W = 0$ we get that $C_6(\mathbb{Q}) = \{[0:1:0], [1:0:0], [-1/864:1/2:1]\}$. Recall that $\frac{-1}{864}$ is already in S_2. From this we get the following proposition:

Corollary 6.2. *Let $t \in \mathbb{Q}$ such that that $t \neq 0$ or $\frac{-1}{432}$. Then $\bar{\rho}_{\mathbb{E}_t,6}$ is not surjective if and only if $t \in S_2 \cup S_3$ or $\mathbb{E}_t$ is a Serre curve and the entanglement desctribed in Remark 1.4 occurs between the 2 and 3 torsion fields.*

Example 6.3. From Proposition 6.2 and Example 4.10 we know that if ℓ is an odd prime not equal to 7, then $\ell \notin S_2 \cup S_3$ and so $\bar{\rho}_{\mathbb{E}_\ell,6}$ is surjective.

7. Thin Sets

Before we prove the main theorem, we introduce a definition of what it means for a set to be thin and introduce a few results regarding properties of thin sets. Here we will use the definitions given in [BL05] as they are more convenient for the the context we are working in and logically equivalent to the traditional ones.

Definition 7.1. Let K be a field and let n be a positive integer. Let T be a subset of K^n. The set T is said to be a ***basic thin set of the first type*** if there exists a nonzero polynomial $f(t_1, \ldots, t_n) \in K(t_1, \ldots, t_n)$ such that a point $P = (P_1, \ldots, P_n)$ is in T if and only if $f(P_1, \ldots, P_n) = 0$. The set T is called a ***basic thin set of the second type*** if there exists an irreducible polynomial $f(t_1, \ldots, t_n, x)$ in $K(t_1, \ldots, t_n, x)$ with x-degree greater than 1 such that a point $P = (P_1, \ldots, P_n)$ is in T if and only if $f(P_1, \ldots, P_n, x)$ has a root in K. Lastly, T is called ***thin*** if it is contained in a finite union of basic thin sets.

From the definition, we get the following lemma immediately:

Lemma 7.2. *Any finite union of thin sets is a thin set.*

Proposition 7.3. [Ser07, Proposition 3.3.5] *Let K be a field, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and irreducible polynomial in $K(t_1, \ldots, t_n)[x]$, and let G_f be the Galois group of f. Then there exists a thin set $A \in K^n$ such that, if $P \notin A$, then:*

1. *P is not a pole of any of the a_i,*
2. *the specialization $f_P(x) = x^n + a_{n-1}(P)x^{n-1} + \cdots + a_1(P)x + a_0(P)$ is irreducible in $K[x]$,*
3. *the Galois group of f_P is G.*

Remark 7.4. If we can show that the p-th division polynomials of $\mathbb{E}$ are irreducible, then the sets S_p for $p = 2, 3, 5$, and 7, that we found in the previous sections are exactly the thin sets assured to exist in Proposition 7.3 for their respective polynomials in $\mathbb{Q}(t)[x]$. Also, the sets S_k for $k = 4, 6$, and 9 are clearly thin sets of the second type, since they can be viewed as the set of rational specializations of the irreducible polynomials that define the curve C_k that have a root in $\mathbb{Q}$. Therefore, by Lemma 7.2 we know that there union must also be a thin set.

For more information about thin sets and Hilbert irreducibility, the reader is encouraged to see chapter 3 of [Ser07].

8. Main Theorem

With all this work done, we are now ready to prove the main theorem.

Theorem 8.1. *Let $\mathbb{E}/\mathbb{Q}(t)$ be the elliptic curve given by the Weierstrass equation*

$$\mathbb{E} : y^2 + xy = x^3 + t,$$

and for every $t \in \mathbb{Q}$ let $\mathbb{E}_t/\mathbb{Q}$ be the specialization of $\mathbb{E}$ at t. Then, we can completely determine a set S such that if $t \notin S$, then $\mathbb{E}_t$ is a Serre curve with at most 12 possible exceptions.

Proof: Let $S = S_2 \cup S_3 \cup S_5 \cup S_7 \cup S_4 \cup S_9$. Then we know that $\mathbb{E}_t$ is a Serre curve if and only if $t \notin S$ from Theorems 1.8, 1.9, and Corollaries 4.2, 4.5, 4.7, 4.9, 5.4, 6.2, and 5.9. In fact, we completely determined S up to at most 12 exceptions, although we expect that there are no exceptions. ∎

Example 8.2. Let ℓ be an odd prime with $\ell \neq 7$. Then, as noted above, the elliptic curve,

$$\mathbb{E}_\ell : y^2 + xy = x^3 + \ell$$

is a Serre curve.

Remark 8.3. To see that S is thin, first notice that for $p = 2, 3, 5$, and 7, the p-division polynomial of $\mathbb{E}$ must be irreducible. This is because Galois groups do not increase under specialization and there are infinitely many examples of specialization for which p is not exceptional. Thus, by Proposition 7.3, we know that the sets S_p are thin. Next, for $k = 4$, and 9 we use Magma to check that the polynomials defining the affine patch curve of C_k with $W \neq 0$ are irreducible. Therefore, the set S_k is exactly the set of specializations such that this polynomials has a root. That is, S_k is a basic thin set of the first type, and by Lemma 7.2 we know that the set S is thin.

9. Acknowledgments

The author would like to thank Álvaro Lozano-Robledo, Nathan Jones, and Keith Conrad for their useful comments on various stages of this paper.

10. Magma Code and Outputs

10.1. Code for p=3.

Define C_3 and E_3 and determining the rational points on both.

```
> A<C,D,F> := ProjectiveSpace(Rationals(),2);
> C := Curve(A, 12*(-3*D^2*F+3*C^2*D-C*D*F) - (D*F^2-6*C*D*F-C^2*F+3*C^3));
> Genus(C);
1
> E, phi := EllipticCurve(C);
> E;
Elliptic Curve defined by y^2 + 1/54*x*y - 1/104976*y = x^3 - 1/2916*x^2 over
Rational Field
> phi;
Mapping from: CrvPln: C to CrvEll: E
```

```
with equations :
1/324*C
1/2916*D
6*C + 36*D + F
> Rank(E);
0
> TorsionSubgroup(E);
Abelian Group isomorphic to Z/6
Defined on 1 generator
Relations:
    6*$.1 = 0
> PtsC:=Points(C: Bound:= 10000);
> PtsE:=Points(E: Bound:= 10000);
> PtsE;
{@ (0 : 1 : 0), (0 : 1/104976 : 1), (0 : 0 : 1), (1/2916 : 1/314928 : 1),
(1/2916 : 0 : 1), (1/3888 : 1/419904 : 1) @}
> PtsC;
{@ (0 : 1 : 0), (0 : 0 : 1), (0 : -1/36 : 1), (12 : 1 : 0), (1/3 : 1/36 : 1),
(1/3 : 0 : 1) @}
```

10.2. **Code for p=5.**

Define C_5, E_5, and φ.

```
> A<T,H,W> := ProjectiveSpace(Rationals(),2);
> C := Curve(A, (H^2+10*H*W+5*W^2)^3*(432*T^2+T*W)+H*W^7);
> E, phi := EllipticCurve(C, C![0,1,0]);
> E;
Elliptic Curve defined by y^2 + 16*x*y + 716*y = x^3 + 94*x^2 + 2605*x + 18612
over Rational Field
> phi;
Mapping from: CrvPln: C to CrvEll: E
with equations :
432*T*H^4*W + 8640*T*H^3*W^2 + H^4*W^2 + 47520*T*H^2*W^3 + 20*H^3*W^3 +
    43200*T*H*W^4 + 63*H^2*W^4 + 10800*T*W^5 - 52*H*W^5 + 36*W^6
432*T*H^5 + 8640*T*H^4*W + H^5*W + 47520*T*H^3*W^2 + 20*H^4*W^2 +
    43200*T*H^2*W^3 + 110*H^3*W^3 + 10800*T*H*W^4 + 136*H^2*W^4 - 11*H*W^5
H^2*W^4 + 4*H*W^5 - W^6
```

Checking that φ and ψ are well-defined.

```
> EFF<x,y>:=FunctionField(E);
> psi1:=-36*x*1^2-11*y*1^2-1296*1^3;
> psi2:=247*x^2*y+14*x*y^2+11*y^3-6912*x^2*1+12706*x*y*1-2654*y^2*1-324864*x*1\
^2+224359*y*1^2-2737152*1^3;
> psi3:=14*x^2*y+11*x*y^2+1097*x^2*1+1956*x*y*1+764*y^2*1+67514*x*1^2+45202*y*\
1^2+998717*1^3;
> (psi2^2+10*psi2*psi3+5*psi3^2)^3*(432*psi1^2+psi1*psi3)+psi2*psi3^7;
0
> CFF<t,h>:=FunctionField(C);
> phi1 := 432*t*h^4*1 + 8640*t*h^3*1^2 + h^4*1^2 + 47520*t*h^2*1^3 + 20*h^3*1^\
3 + 43200*t*h*1^4 + 63*h^2*1^4 + 10800*t*1^5 - 52*h*1^5 + 36*1^6;
> phi2 := 432*t*h^5 + 8640*t*h^4*1 + h^5*1 + 47520*t*h^3*1^2 + 20*h^4*1^2 + 43\
200*t*h^2*1^3 + 110*h^3*1^3 + 10800*t*h*1^4 + 136*h^2*1^4 - 11*h*1^5;
> phi3 := h^2*1^4 + 4*h*1^5 - 1^6;
```

```
> phi2^2*phi3 + 16*phi1*phi2*phi3 + 716*phi2*phi3^2 - (phi1^3 + 94*phi1^2*phi3\
 + 2605*phi1*phi3^2 + 18612*phi3^3);
0
```

Checking φ and ψ are inverses.

```
> a1:=432*psi1*psi2^4*psi3 + 8640*psi1*psi2^3*psi3^2 + psi2^4*psi3^2 + 47520*ps\
 i1*psi2^2*psi3^3 + 20*psi2^3*psi3^3 + 43200*psi1*psi2*psi3^4 + 63*psi2^2*psi3^4\
 + 10800*psi1*psi3^5 - 52*psi2*psi3^5 + 36*psi3^6;
> a2:=432*psi1*psi2^5 + 8640*psi1*psi2^4*psi3 + psi2^5*psi3 + 47520*psi1*psi2^3\
*psi3^2 + 20*psi2^4*psi3^2 + 43200*psi1*psi2^2*psi3^3 + 110*psi2^3*psi3^3 + 108\
00*psi1*psi2*psi3^4 + 136*psi2^2*psi3^4 - 11*psi2*psi3^5;
> a3:=psi2^2*psi3^4 + 4*psi2*psi3^5 - psi3^6;
> a1/a3;
x
> a2/a3;
y
> b1:=-36*phi1*phi3^2-11*phi2*phi3^2-1296*phi3^3;
> b2:=247*phi1^2*phi2+14*phi1*phi2^2+11*phi2^3-6912*phi1^2*phi3+12706*phi1*phi2\
*phi3-2654*phi2^2*phi3-324864*phi1*phi3^2+224359*phi2*phi3^2-2737152*phi3^3;
> b3:=14*phi1^2*phi2+11*phi1*phi2^2+1097*phi1^2*phi3+1956*phi1*phi2*phi3+764*ph\
i2^2*phi3+67514*phi1*phi3^2+45202*phi2*phi3^2+998717*phi3^3;
> b1/b3;
t
> b2/b3;
h
```

Finding points on C_5 via E_5

```
> P1 := E![-51,40,1]; // infinite order
> for i in [-3..3] do
for>     for j in [0,1] do
for|for>         P:=i*P1+j*P2;
for|for>         x:=P[1];
for|for>         y:=P[2];
for|for>         T:=-36*x-11*y-1296;
for|for>         H:=247*x^2*y+14*x*y^2+11*y^3-6912*x^2+12706*x*y-2654*y^2-324864*x\
for|for>         +224359*y-2737152;
for|for>         W:=14*x^2*y+11*x*y^2+1097*x^2+1956*x*y+764*y^2+67514*x+45202*y\
for|for>         +998717;
for|for>         if W ne 0 then
for|for|if>             [[i,j],[T/W,H/W,1]];
for|for|if>         end if;
for|for>     end for;
for> end for;
[
    [ -3, 0 ],
    [ 28/148955, -140/11, 1 ]
]
[
    [ -3, 1 ],
    [ -2272/804357, -71/6, 1 ]
]
[
```

```
    [ -2, 0 ],
    [ -19/16, -19/2, 1 ]
]
[
    [ -2, 1 ],
    [ -1/432, 0, 1 ]
]
[
    [ -1, 0 ],
    [ -3/1280, -15, 1 ]
]
[
    [ -1, 1 ],
    [ 11/6912, -11, 1 ]
]
[
    [ 0, 0 ],
    [ -1307/1044683, -2515436/1044683, 1 ]
]
[
    [ 0, 1 ],
    [ -2/135, -10, 1 ]
]
[
    [ 1, 0 ],
    [ 1/80, -10, 1 ]
]
[
    [ 2, 0 ],
    [ -1/256, -11, 1 ]
]
[
    [ 2, 1 ],
    [ 1/34560, -15, 1 ]
]
[
    [ 3, 0 ],
    [ 0, 0, 1 ]
]
[
    [ 3, 1 ],
    [ 32/27, -19/2, 1 ]
]
```

10.3. **Code for p=7.**

Define C_7, E_7, and φ.

```
> A<T,H,W> := ProjectiveSpace(Rationals(),2);
> C := Curve(A, (H^2+13*H*W+49*W^2)*(H^2+5*H*W+W^2)^3*(432*T^2+T*W)+H*W^9);
> E, phi := EllipticCurve(C, C![0,1,0]);
> E;
Elliptic Curve defined by y^2 + 9*x*y + 141*y = x^3 + 34*x^2 + 349*x + 1020 over
```

```
Rational Field
> phi;
Mapping from: CrvPln: C to CrvEll: E
with equations :
432*T*H^6*W + 9936*T*H^5*W^2 + H^6*W^2 + 88992*T*H^4*W^3 + 23*H^5*W^3 +
    367632*T*H^3*W^4 + 189*H^4*W^4 + 628128*T*H^2*W^5 + 625*H^3*W^5 +
    217296*T*H*W^6 + 503*H^2*W^6 + 21168*T*W^7 - 375*H*W^7 + 84*W^8
432*T*H^7 + 9936*T*H^6*W + H^7*W + 88992*T*H^5*W^2 + 23*H^6*W^2 +
    367632*T*H^4*W^3 + 206*H^5*W^3 + 628128*T*H^3*W^4 + 863*H^4*W^4 +
    217296*T*H^2*W^5 + 1574*H^3*W^5 + 21168*T*H*W^6 + 815*H^2*W^6 - 35*H*W^7
H^4*W^4 + 14*H^3*W^5 + 63*H^2*W^6 + 70*H*W^7 - 7*W^8
```

Checking φ and ψ are well defined.

```
> EFF<x,y>:=FunctionField(E);
> psi1 := 4680*x*1^3+1950*y*1^3+56160*1^4;
> psi2 := -6630*x^2*y^2-1950*x*y^3-39390*x^2*y*1-211770*x*y^2*1-39780*y^3*1+56\
160*x^2*1^2-866580*x*y*1^2-1379820*y^2*1^2+954720*x*1^3-4976790*y*1^3+3369600*\
1^4;
> psi3 :=-1950*x^2*y^2-99060*x^2*y*1-132600*x*y^2*1-6630*y^3*1-196950*x^2*1^2-\
3020550*x*y*1^2-1650480*y^2*1^2-5456100*x*1^3-22192170*y*1^3-36509070*1^4;
> (psi2^2+13*psi2*psi3+49*psi3^2)*(psi2^2+5*psi2*psi3+psi3^2)^3*(432*psi1^2+ps\
i1*psi3)+psi2*psi3^9;
0
> CFF<t,h>:=FunctionField(C);
> phi1 := 432*t*h^6*1 + 9936*t*h^5*1^2 + h^6*1^2 + 88992*t*h^4*1^3 + 23*h^5*1^\
3 + 367632*t*h^3*1^4 + 189*h^4*1^4 + 628128*t*h^2*1^5 + 625*h^3*1^5 + 217296*t\
*h*1^6 + 503*h^2*1^6 + 21168*t*1^7 - 375*h*1^7 + 84*1^8;
> phi2 := 432*t*h^7 + 9936*t*h^6*1 + h^7*1 + 88992*t*h^5*1^2 + 23*h^6*1^2 + 36\
7632*t*h^4*1^3 + 206*h^5*1^3 + 628128*t*h^3*1^4 + 863*h^4*1^4 + 217296*t*h^2*1\
^5 + 1574*h^3*1^5 + 21168*t*h*1^6 + 815*h^2*1^6 - 35*h*1^7;
> phi3 := h^4*1^4 + 14*h^3*1^5 + 63*h^2*1^6 + 70*h*1^7 - 7*1^8;
> phi2^2*phi3 + 9*phi1*phi2*phi3 + 141*phi2*phi3^2 - (phi1^3 + 34*phi1^2*phi3 \
+ 349*phi1*phi3^2 + 1020*phi3^3);
0
```

Checking φ and ψ are inverses.

```
> a1 := 4680*phi1*phi3^3+1950*phi2*phi3^3+56160*phi3^4;
> a2 := -6630*phi1^2*phi2^2-1950*phi1*phi2^3-39390*phi1^2*phi2*phi3-211770*phi\
1*phi2^2*phi3-39780*phi2^3*phi3+56160*phi1^2*phi3^2-866580*phi1*phi2*phi3^2-13\
79820*phi2^2*phi3^2+954720*phi1*phi3^3-4976790*phi2*phi3^3+3369600*phi3^4;
> a3 :=-1950*phi1^2*phi2^2-99060*phi1^2*phi2*phi3-132600*phi1*phi2^2*phi3-6630\
*phi2^3*phi3-196950*phi1^2*phi3^2-3020550*phi1*phi2*phi3^2-1650480*phi2^2*phi3\
^2-5456100*phi1*phi3^3-22192170*phi2*phi3^3-36509070*phi3^4;
> a1/a3;
t
> a2/a3;
h
> b1 := 432*psi1*psi2^6*psi3 + 9936*psi1*psi2^5*psi3^2 + psi2^6*psi3^2 + 88992\
*psi1*psi2^4*psi3^3 + 23*psi2^5*psi3^3 + 367632*psi1*psi2^3*psi3^4 + 189*psi2^\
4*psi3^4 + 628128*psi1*psi2^2*psi3^5 + 625*psi2^3*psi3^5 + 217296*psi1*psi2*ps\
i3^6 + 503*psi2^2*psi3^6 + 21168*psi1*psi3^7 - 375*psi2*psi3^7 + 84*psi3^8;
> b2 := 432*psi1*psi2^7 + 9936*psi1*psi2^6*psi3 + psi2^7*psi3 + 88992*psi1*psi\
```

```
2^5*psi3^2 + 23*psi2^6*psi3^2 + 367632*psi1*psi2^4*psi3^3 + 206*psi2^5*psi3^3 \
+ 628128*psi1*psi2^3*psi3^4 + 863*psi2^4*psi3^4 + 217296*psi1*psi2^2*psi3^5 + \
1574*psi2^3*psi3^5 + 21168*psi1*psi2*psi3^6 + 815*psi2^2*psi3^6 - 35*psi2*psi3\
^7;
> b3 := psi2^4*psi3^4 + 14*psi2^3*psi3^5 + 63*psi2^2*psi3^6 + 70*psi2*psi3^7 -\
 7*psi3^8;
> b1/b3;
x
> b2/b3;
y
```

Finding points on C_7 using E_7

```
> P1 := E![-17 , 0 , 1]; // infinite order
> P2 := E![-21 , 24 , 1]; // order 2
> for i in [-3..3] do
for>     for j in [0,1] do
for|for>         P := i*P1+j*P2;
for|for>         x := P[1];
for|for>         y := P[2];
for|for>         z := P[2];
for|for>         t:=4680*x*1^3+1950*y*1^3+56160*1^4;
for|for>         h:=-6630*x^2*y^2-1950*x*y^3-39390*x^2*y*1-211770*x*y^2*1-3978\
0*y^3*1+56160*x^2*1^2-866580*x*y*1^2-1379820*y^2*1^2+954720*x*1^3-4976790*y*1^\
3+3369600*1^4;
for|for>         w:=-1950*x^2*y^2-99060*x^2*y*1-132600*x*y^2*1-6630*y^3*1-1969\
50*x^2*1^2-3020550*x*y*1^2-1650480*y^2*1^2-5456100*x*1^3-22192170*y*1^3-365090\
70*1^4;
for|for>         if w ne 0 then
for|for|if>             [[i,j],[t/w,h/w,w/w]];
for|for|if>         end if;
for|for>     end for;
for> end for;
[
    [ -3, 0 ],
    [ 1/18000, -8, 1 ]
]
[
    [ -3, 1 ],
    [ -128/55125, -19/2, 1 ]
]
[
    [ -2, 0 ],
    [ -1/27, -5, 1 ]
]
[
    [ -2, 1 ],
    [ -1/21168, 1, 1 ]
]
[
    [ -1, 1 ],
    [ 2/1323, -6, 1 ]
]
```

```
[
    [ 0, 0 ],
    [ -149/154765, 597/11905, 1 ]
]
[
    [ 0, 1 ],
    [ -3/784, -6, 1 ]
]
[
    [ 1, 0 ],
    [ 5/144, -5, 1 ]
]
[
    [ 1, 1 ],
    [ -1/441, 1, 1 ]
]
[
    [ 2, 0 ],
    [ -8/3375, -8, 1 ]
]
[
    [ 2, 1 ],
    [ 19/2646000, -19/2, 1 ]
]
[
    [ 3, 0 ],
    [ -1/432, 0, 1 ]
]
[
    [ 3, 1 ],
    [ -3712/9261, -29/6, 1 ]
]
```

10.4. **Code for $n = 4$.**

Define C_4, E_4, and φ.

```
> A<T,H,W> := ProjectiveSpace(Rationals(),2);
> C := Curve(A, -4*H^3*(H+8*W)*(432*T^2+T*W)+1*W^6);
> E, phi := EllipticCurve(C, C![0,1,0]);
> E;
Elliptic Curve defined by y^2 + 2*x*y + 12*y = x^3 - 24*x^2 + 180*x - 432 over
Rational Field
> phi;
Mapping from: CrvPln: C to CrvEll: E
with equations :
432*T*H^3*W + 3456*T*H^2*W^2 + H^3*W^2 + 8*H^2*W^3 + 12*H*W^4 + 36*W^5
432*T*H^4 + 3456*T*H^3*W + H^4*W + 8*H^3*W^2 - 36*H*W^4
H*W^4 + 6*W^5
```

Checking φ and ψ are well defined.

```
> EFF<x,y>:=FunctionField(E);
> psi1:=-x*1^2+12*1^3;
> psi2:=-4*x^2*y+48*x*y*1-16*y^2*1-144*y*1^2;
```

```
> psi3:=-24*x*y*1-4*y^2*1+144*y*1^2;
> -4*psi2^3*(psi2+8*psi3)*(432*psi1^2+psi1*psi3)+1*psi3^6;
0
> CFF<t,h>:=FunctionField(C);
> phi1 := 432*t*h^3*1 + 3456*t*h^2*1^2 + h^3*1^2 + 8*h^2*1^3 + 12*h*1^4 + 36*1\
^5;
> phi2 := 432*t*h^4 + 3456*t*h^3*1 + h^4*1 + 8*h^3*1^2 - 36*h*1^4;
> phi3 := h*1^4 + 6*1^5;
> phi2^2*phi3 + 2*phi1*phi2*phi3 + 12*phi2*phi3^2 - (phi1^3 - 24*phi1^2*phi3 +\
 180*phi1*phi3^2 - 432*phi3^3);
0
```

Checking φ and ψ are inverses.

```
> a1:=-phi1*phi3^2+12*phi3^3;
> a2:=-4*phi1^2*phi2+48*phi1*phi2*phi3-16*phi2^2*phi3-144*phi2*phi3^2;
> a3:=-24*phi1*phi2*phi3-4*phi2^2*phi3+144*phi2*phi3^2;
> a1/a3;
t
> a2/a3;
h
> b1 := 432*psi1*psi2^3*psi3 + 3456*psi1*psi2^2*psi3^2 + psi2^3*psi3^2 + 8*psi\
2^2*psi3^3 + 12*psi2*psi3^4 + 36*psi3^5;
> b2 := 432*psi1*psi2^4 + 3456*psi1*psi2^3*psi3 + psi2^4*psi3 + 8*psi2^3*psi3^\
2 - 36*psi2*psi3^4;
> b3 := psi2*psi3^4 + 6*psi3^5;
> b1/b3;
x
> b2/b3;
y
```

Finding points on C_4 via E_4

```
> Rank(E);
0
> TorsionSubgroup(E);
Abelian Group isomorphic to Z/8
Defined on 1 generator
Relations:
    8*$.1 = 0
> P1 := E![6, 0 , 1];
> for i in [0..7] do
for>     P := i*P1;
for>     x := P[1];
for>     y := P[2];
for>     z := P[3];
for>     t:=-x*z^2+12*z^3;
for>     h:=-4*x^2*y+48*x*y*z-16*y^2*z-144*y*z^2;
for>     w:=-24*x*y*z-4*y^2*z+144*y*z^2;
for>     if w ne 0 then
for|if>         [[i],[t/w,h/w,w/w]];
for|if>     end if;
for> end for;
[
```

```
    [ 3 ],
    [ 1/3456, 4, 1 ]
]
[
    [ 4 ],
    [ -1/108, 1, 1 ]
]
[
    [ 7 ],
    [ -1/384, 4, 1 ]
]
```

10.5. **Code for $n = 6$.**

Define C_6, E_6, and φ.

```
A<T,H,W> := ProjectiveSpace(Rationals(),2);
C := Curve(A, 2^(10)*3^3*H^3*(W^3-4*H^3)*(432*T^2+T*W)+W^8);
E, phi := EllipticCurve(C, C![0,1,0]);
E;
phi;
Rank(E);
TorsionSubgroup(E);>
> A<T,H,W> := ProjectiveSpace(Rationals(),2);
> C := Curve(A, 2^(10)*3^3*H^3*(W^3-4*H^3)*(432*T^2+T*W)+W^8);
> E, phi := EllipticCurve(C, C![0,1,0]);
> E;
Elliptic Curve defined by y^2 + 16384*y = x^3 over Rational Field
> phi;
Mapping from: CrvPln: C to CrvEll: E
with equations :
1769472*T*H^5*W + 4096*H^5*W^2 - 442368*T*H^2*W^4 - 768*H^2*W^5
-113246208*T*H^6 - 262144*H^6*W + 28311552*T*H^3*W^3 + 49152*H^3*W^4
H^3*W^4 - 1/8*W^7
> Rank(E);
0
> TorsionSubgroup(E);
Abelian Group isomorphic to Z/3
Defined on 1 generator
Relations:
    3*$.1 = 0
```

Checking φ and ψ are well defined.

```
> EFF<x,y>:=FunctionField(E);
> psi1:= -1073741824*x*1^2;
> psi2:= 27*y^3+884736*y^2*1;
> psi3:= -1728*x*y^2-56623104*x*y*1;
> 2^(10)*3^3*psi2^3*(psi3^3-4*psi2^3)*(432*psi1^2+psi1*psi3)+psi3^8;
0
> CFF<t,h>:=FunctionField(C);
> phi1 := 1769472*t*h^5*1 + 4096*h^5*1^2 - 442368*t*h^2*1^4 - 768*h^2*1^5;
> phi2 := -113246208*t*h^6 - 262144*h^6*1 + 28311552*t*h^3*1^3 + 49152*h^3*1^4\
;
> phi3 := h^3*1^4 - 1/8*1^7;
```

```
> phi2^2*phi3 + 16384*phi2*phi3^2 - phi1^3;
0
```

Checking φ and ψ are inverses.

```
> a1:= -1073741824*phi1*phi3^2;
> a2:= 27*phi2^3+884736*phi2^2*phi3;
> a3:= -1728*phi1*phi2^2-56623104*phi1*phi2*phi3;
> a1/a3;
t
> a2/a3;
h
> b1 := 1769472*psi1*psi2^5*psi3 + 4096*psi2^5*psi3^2 - 442368*psi1*psi2^2*psi\
3^4 - 768*psi2^2*psi3^5;
> b2 := -113246208*psi1*psi2^6 - 262144*psi2^6*psi3 + 28311552*psi1*psi2^3*psi\
3^3 + 49152*psi2^3*psi3^4;
> b3 := psi2^3*psi3^4 - 1/8*psi3^7;
> b1/b3;
x
> b2/b3;
y
```

Finding points on C_6 via E_6

```
> P1 := E![0, 0 , 1]; // order 3
> for i in [0..2] do
for>     P := i*P1;
for>     x := P[1];
for>     y := P[2];
for>     z := P[3];
for>     t:=-1073741824*x*1^2;
for>     h:= 27*y^3+884736*y^2*1;
for>     w:= -1728*x*y^2-56623104*x*y*1;
for>     if w ne 0 then
for|if>         [[i],[t/w,h/w,w/w]];
for|if>     end if;
for> end for;
> PtsC:= Points(C: Bound:=100);
> PtsC;
{@ (0 : 1 : 0), (1 : 0 : 0), (-1/864 : 1/2 : 1) @}
```

10.6. **Code for $n = 9$.**

Define C_9, H_9, J_9 and Computing the rank of J_9.

```
> A<t,h,w> := ProjectiveSpace(Rationals(),2);
> C := Curve(A, 3^7*(h^2-w^2)^3*(h^6+3*h^5*w+6*h^4*w^2+h^3*w^3-3*h^2*w^4+12*h*\
w^5+16*w^6)^3*(2*h^3+3*h^2*w-3*h*w^2-5*w^3)*(432*t^2+t*w)+(h^3-3*h*w^2-w^3)^9*\
w^2);
> Genus(C);
6
> time P:=Points(C: Bound:=100);
Time: 0.430
> _,H,phi := IsHyperelliptic(C);
> Degree(phi);
1
```

```
> _,H1,phi1 := HasOddDegreeModel(H);
> RankBounds(Jacobian(H1));
1 1
```

Computing the number of points on H_9 mod p for various primes.

```
> for p in [5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47] do
for>    _<x> := PolynomialRing(GF(p));
for>     H1 := HyperellipticCurve([x^14 - 11*x^13 + 53*x^12 - 157*x^11 + 336*x\
^10 - 563*x^9 + 617*x^8 - 242*x^7 - 151*x^6 - 19*x^5 + 138*x^4 + 60*x^3 + 16*x\
^2 - 2*x, x^6 + x^5 + x^3 + x^2]);
for>    P:=Points(H1);
for>    #P;
for> end for;
9
5
12
14
21
29
24
39
29
44
54
41
42
```

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[BJ14] Julio Brau and Nathan Jones. Elliptic curves with 2-torsion contained in the 3-torsion field. 06 2014.

[BL05] Yuri F. Bilu and Florian Luca. Divisibility of class numbers: enumerative approach. *J. Reine Angew. Math.*, 578:79–91, 2005.

[CGJ11] Alina-Carmen Cojocaru, David Grant, and Nathan Jones. One-parameter families of elliptic curves over $\mathbb{Q}$ with maximal Galois representations. *Proc. Lond. Math. Soc. (3)*, 103(4):654–675, 2011.

[CR01] Brian Conrad and Karl Rubin, editors. *Arithmetic algebraic geometry*. American Mathematical Society, Providence, RI; Institute for Advanced Study (IAS), Princeton, NJ, 2001.

[DD12] Tim Dokchitser and Vladimir Dokchitser. Surjectivity of mod 2^n representations of elliptic curves. *Math. Z.*, 272(3-4):961–964, 2012.

[Elk06] Noam Elkies. Elliptic curves with 3-adic galois representation surjective mod 3 but not mod 9. Available at http://arxiv.org/abs/math/0612734, 2006.

[GS] Daniel R. Grayson and Michael E. Stillman. Macaulay2, a software system for research in algebraic geometry. Available at `http://www.math.uiuc.edu/Macaulay2/`.

[LR13] Álvaro Lozano-Robledo. On the field of definition of p-torsion points on elliptic curves over the rationals. *Mathematische Annalen*, 357(1):279–305, 2013.

[LT76] Serge Lang and Hale Trotter. *Frobenius distributions in* GL_2*-extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers.

[Maz78] B. Mazur. Rational isogenies of prime degree. *Invent. Math.*, 44(2):129–162, 1978.

[S+14] W. A. Stein et al. *Sage Mathematics Software (Version 6.1.1)*. The Sage Development Team, `http://www.sagemath.org`, 2014.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser96] Jean-Pierre Serre. Travaux de Wiles (et Taylor, ...). I. *Astérisque*, (237):Exp. No. 803, 5, 319–332, 1996. Séminaire Bourbaki, Vol. 1994/95.

[Ser07] Jean-Pierre Serre. *Topics in Galois Theory*. Research Notes in Mathematics. A K Peters, second edition, 2007.
[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.
[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
[Sto06] Michael Stoll. Independence of rational points on twists of a given curve. *Compos. Math.*, 142(5):1201–1214, 2006.

(Harris B. Daniels) Department of Mathematics Amherst College Box 2239 P.O. 5000 Amherst, MA 01002-5000