

*Pacific
Journal of
Mathematics*

NEAR COINCIDENCES AND NILPOTENT DIVISION FIELDS

HARRIS B. DANIELS AND JEREMY ROUSE

NEAR COINCIDENCES AND NILPOTENT DIVISION FIELDS

HARRIS B. DANIELS AND JEREMY ROUSE

Let E/\mathbb{Q} be an elliptic curve. We say that E has a near coincidence of level (n, m) if $m \mid n$ and $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m], \zeta_n)$. We classify near coincidences of prime power level and use this result to give a classification of values of n for which $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is a nilpotent group. Along the way we prove a Gauss–Wantzel analog for the elliptic curve $E : y^2 = x^3 - x$, showing that $\mathbb{Q}(E[n])/\mathbb{Q}$ is constructible if and only if $\varphi(n)$ is a power of 2. Assuming that there are no non-CM rational points on the modular curves $X_{ns}^+(p)$ for primes $p > 11$, we show that $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ nilpotent implies that n is a power of 2 or $n \in \{3, 5, 6, 7, 15, 21\}$.

1. Introduction

For much of mathematical history, compass and straightedge constructions have served as exemplars of mathematical reasoning. Central to the study of such constructions is the question of which regular polygons are constructible. First considered by the Greeks, an answer to this question long eluded mathematicians, with no progress made for hundreds of years. This changed when Gauss proved the following theorem:

Theorem 1.1 [15]. *Suppose that n is of the form*

$$n = 2^k \cdot p_1 \cdots p_j,$$

where p_i is a Fermat prime. Then it is possible to construct a regular n -gon using only a straightedge and compass.

Here we remind the reader that a Fermat prime is a Fermat number (i.e., a number of the form $2^{2^m} + 1$ with $m \geq 0$) which is prime.

In fact, in [15] Gauss states that he has a proof of the converse, but he says, “the limits of the present work exclude this demonstration here.” The final part of the question was formally answered in 1837 when Pierre Wantzel proved the converse.

Theorem 1.2 [43]. *Suppose n is a positive integer such that a regular n -gon is constructible. Then n is of the form $n = 2^k \cdot p_1 \cdots p_j$, where each p_i is a Fermat prime.*

MSC2020: primary 11G05; secondary 11R32, 14H52.

Keywords: elliptic curve, division field, Galois group, modular curve.

Together, these two results together form the Gauss–Wantzel theorem. If we let φ be Euler’s totient function, then we can summarize the Gauss–Wantzel theorem as saying a regular n -gon is constructible if and only if there exists a k such that $\varphi(n) = 2^k$.

A modern reformulation of this is to take the standard plane and turn it into the complex plane. A point in the complex plane is said to be *constructible* if there is a way to define that point using just a straightedge and compass. Interpreting the Gauss–Wantzel theorem through this more modern lens gives us a new interpretation of what it means for a complex number to be constructible.

Theorem 1.3 [32, Theorem 4.53]. *Let $\alpha \in \mathbb{C}$. Then, α is constructible if and only if there exists an ascending chain of fields*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subset \cdots \subseteq K_j$$

such that $\alpha \in K_j$ and $[K_i : K_{i-1}] = 2$.

A subfield of \mathbb{C} is said to be *constructible* if all of the elements in the field are constructible. Using Galois theory from here we can update [Theorem 1.3](#) to say that α is constructible if and only if there is a Galois extension K/\mathbb{Q} that contains α such that $\text{Gal}(K/\mathbb{Q})$ is a 2-group. Given that the n th roots of unity are equally spaced around the unit circle, from this updated perspective, the question of about the constructibility of a regular n -gon is exactly the same as the question about the constructibility of $\mathbb{Q}(\zeta_n)$. Here ζ_n is a primitive n th root of unity. This modern perspective allows us to examine the constructibility of more complicated fields. The primary objects of study in this paper are the division fields of elliptic curves.

First we fix $\overline{\mathbb{Q}}$, an algebraic closure of \mathbb{Q} and let E/\mathbb{Q} be an elliptic curve. A classical result is that the points on E can be given the structure of an abelian group. We let $E[n]$ be the n -torsion on E defined over $\overline{\mathbb{Q}}$, that is, $E[n] = \{P \in E(\overline{\mathbb{Q}}) : n \cdot P = \mathcal{O}\}$. Then we can define $\mathbb{Q}(E[n])$ to be the field of definition of the n -torsion points. With this we present the following theorem.

Theorem 1.4 (a Gauss–Wantzel analog). *Let E be the elliptic curve given by $y^2 = x^3 - x$ and let $n \geq 2$. Then, $\mathbb{Q}(E[n])$ is a constructible field if and only if $\varphi(n) = 2^k$ for some integer k .*

Proof. Suppose $n \in \mathbb{Z}$ such that $\mathbb{Q}(E[n])/\mathbb{Q}$ is a constructible extension. By properties of the Weil pairing, $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$, and so by the Gauss–Wantzel theorem $\varphi(n)$ is a power of 2.

In the opposite direction, suppose that $n \in \mathbb{Z}$ such that $\varphi(n)$ is a power of 2. Given that constructibility is closed under compositum, it is enough to understand when $\mathbb{Q}(E[p^k])$ is constructible for some prime power p^k .

Suppose $p = 2$. In this case, $\mathbb{Q}(E[2]) = \mathbb{Q}$ and $[\mathbb{Q}(E[2^{k+1}]) : \mathbb{Q}(E[2^k])] = 2^m$ for some $m \in \mathbb{Z}$ depending on k . Thus, for any k , $\text{Gal}(\mathbb{Q}(E[2^k])/\mathbb{Q})$ is a 2-group and hence constructible.

Next suppose that $p = 2^{2^n} + 1$ is a Fermat prime and $E : y^2 = x^3 - x$. We start this case by showing that $[\mathbb{Q}(E[p], i) : \mathbb{Q}(i)]$ is a power of 2, which implies the desired result. The endomorphism ring of E over $\mathbb{Q}(i)$ is isomorphic to $\mathbb{Z}[i]$. Moreover, since $p \equiv 1 \pmod{4}$ splits we can factor $p = \pi \bar{\pi}$ for $\pi \in \mathbb{Z}[i]$. (Explicitly, we have $\pi = 2^{2^{n-1}} + i$ and $\bar{\pi} = 2^{2^{n-1}} - i$.) We therefore have two isogenies $\phi_1 : E \rightarrow E$ and $\phi_2 : E \rightarrow E$ given by $\phi_1(P) = [\pi]P$ and $\phi_2(P) = [\bar{\pi}]P$ which are defined over $\mathbb{Q}(i)$. Let $E[\pi]$ and $E[\bar{\pi}]$ be the kernels of these two isogenies. It is straightforward to see that $E[p]$ is the direct product of $E[\pi]$ and $E[\bar{\pi}]$, that each of $E[\pi]$ and $E[\bar{\pi}]$ has order p , and both $E[\pi]$ and $E[\bar{\pi}]$ are Galois stable over $\mathbb{Q}(i)$. This shows that the image of the mod p Galois representation $\rho_{E,p} : \text{Gal}(\mathbb{Q}(E[p], i)/\mathbb{Q}(i)) \rightarrow \text{GL}_2(\mathbb{F}_p)$ is conjugate to a subgroup of the diagonal matrices. The set of diagonal matrices has order $(p-1)^2 = 2^{2^{n+1}}$. Since ρ is injective, Lagrange's theorem implies that $[\mathbb{Q}(E[p], i) : \mathbb{Q}(i)]$ is a power of 2. \square

One might think that the more general question of when $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ can be a p -group would add some interest, but it turns out the only interesting case here is when $p = 2$. This is easy to see since $[\mathbb{Q}(E[n]) : \mathbb{Q}]$ is even for all $n \geq 3$. If we want to study a condition on $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ that is more general than being a p -group, but is restrictive enough to yield meaningful results, a naive thing to do would be to study when $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is the direct product of a finite number of p -groups. This allows some additional flexibility, but still imposes some structure on the situation.

While at first this seems arbitrary and naive, it is a very natural thing to do.

Proposition 1.5 [18, Proposition II.7.5]. *Let G be a finite group, then G is nilpotent if and only if it is the direct product of its p -Sylow subgroups.*

Thus, our naive consideration is actually logically equivalent to the condition that $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is nilpotent. Looking at the literature, we find the following result about when $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is abelian.

Theorem 1.6 [16, Theorem 1.1]. *Let E/\mathbb{Q} be an elliptic curve and $n \geq 2$. If $\mathbb{Q}(E[n])/\mathbb{Q}$ is an abelian extension, then $n = 2, 3, 4, 5, 6$, or 8 .*

With this added context, our new goal is to understand when $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is nilpotent for E/\mathbb{Q} . To that end, we give the following definition:

Definition 1.7. Let K/k be a Galois extension of fields. We say that K/k is a *nilpotent extension* if $\text{Gal}(K/k)$ is a nilpotent group. When the base field k is clear from context, we will just say that K is a *nilpotent field* for brevity.

We will be able to give a complete answer to the question of when $\mathbb{Q}(E[n])/\mathbb{Q}$ is nilpotent that is conditional on a positive answer to Serre's uniformity question.

Conjecture 1.8 [46, Conjecture 1.1; 34, Conjecture 1.1.5]. *If $p > 11$, then there is no non-CM elliptic curve E/\mathbb{Q} for which the image of the mod p Galois representation is contained in the normalizer of the nonsplit Cartan subgroup.*

Before stating our next theorem we remind the reader that a Mersenne prime is a prime which is one less than a power of 2. Such a prime always has the form $2^p - 1$ for p a prime.

Theorem 1.9. *Let E/\mathbb{Q} be an elliptic curve.*

(1) *If E does not have complex multiplication, Conjecture 1.8 holds, and $\mathbb{Q}(E[n])/\mathbb{Q}$ is nilpotent then $n \in \{3, 5, 6, 7, 15, 21\} \cup \{2^k : k \in \mathbb{Z}^+\}$. Each of these cases occurs for infinitely many different rational j -invariants.*

(2) *If E does not have complex multiplication, $n \notin \{3, 5, 6, 7, 15, 21\} \cup \{2^k : k \in \mathbb{Z}^+\}$, then $\mathbb{Q}(E[n])/\mathbb{Q}$ is nilpotent if and only if one of the following holds: (i) n is a product of distinct Mersenne primes with the property that the mod p image of Galois is contained in the normalizer of the nonsplit Cartan for all primes $p \mid n$, or (ii) n is twice a product of distinct Mersenne primes with the property that the mod p image of Galois is contained in the normalizer of the nonsplit Cartan, and the mod 2 image has RSZB label 2.2.0.1.*

(3) *If E has complex multiplication by the order of discriminant $D \in \{-4, -7, -8, -12, -16, -28\}$, then $\mathbb{Q}(E[n])/\mathbb{Q}$ is nilpotent if and only if n is a power of two times a product of distinct Mersenne and Fermat primes, where the Mersenne primes are inert in the CM field and the Fermat primes are split in the CM field.*

(4) *If E has complex multiplication by the order of discriminant $D \in \{-11, -19, -43, -67, -163\}$, then $\mathbb{Q}(E[n])/\mathbb{Q}$ is nilpotent if and only if n is a product of distinct Mersenne and Fermat primes, where the Mersenne primes are inert in the CM field and the Fermat primes are split in the CM field.*

(5) *If E has complex multiplication by the order of discriminant $D = -27$, then $\mathbb{Q}(E[n])/\mathbb{Q}$ is never nilpotent.*

(6) *If $j(E) = 0$, then E is isomorphic over \mathbb{Q} to an elliptic curve of the form $E_d : y^2 = x^3 + d$. Then, $\mathbb{Q}(E_d[n])/\mathbb{Q}$ is nilpotent if and only if $n = p$ is a prime and*

$$\begin{cases} d \equiv 1 \pmod{(\mathbb{Q}^\times)^3} & \text{if } p = 2, \\ d \equiv 2 \pmod{(\mathbb{Q}^\times)^3} & \text{if } p = 3, \\ d \equiv 2 \cdot p^{\frac{1}{3}(p-1)} \pmod{(\mathbb{Q}^\times)^3} & \text{if } p = 3 \cdot 2^k + 1 \text{ for some } k \geq 1, \\ d \equiv 2 \cdot p^{\frac{1}{3}(p+1)} \pmod{(\mathbb{Q}^\times)^3} & \text{if } p = 3 \cdot 2^k - 1 \text{ for some } k \geq 1. \end{cases}$$

Corollary 1.10. *There is no elliptic curve E/\mathbb{Q} for which $\mathbb{Q}(E[19])/\mathbb{Q}$ is a nilpotent extension. Further, 19 is the smallest prime with this property.*

Along the way to proving [Theorem 1.9](#), a phenomenon appears that we point out here. When studying the question of when $\mathbb{Q}(E[p^n])/\mathbb{Q}$ nilpotent given that $\mathbb{Q}(E[p^{n-1}])/\mathbb{Q}$ is, we realized that we would need to classify exactly when $\mathbb{Q}(E[p^n]) = \mathbb{Q}(E[p^{n-1}], \zeta_{p^n})$.

Definition 1.11. Let E/\mathbb{Q} be an elliptic curve and let $m, n \in \mathbb{Z}^+$ such that $m \mid n$. We say that there is a *near coincidence* between the m - and n -division fields of E if

$$\mathbb{Q}(E[n]) = \mathbb{Q}(E[m], \zeta_n).$$

The terminology here is motivated by the definition given in [\[7\]](#) where an elliptic curve E/\mathbb{Q} is said to have a *coincidence* between its division fields if $\mathbb{Q}(E[m]) = \mathbb{Q}(E[n])$ for distinct integers m and n . In that paper is the following theorem:

Theorem 1.12 [\[7, Theorem 1.4\]](#). *Let E/\mathbb{Q} be an elliptic curve, p be a prime, and let $n \in \mathbb{Z}^+$.*

- (1) *Suppose $\mathbb{Q}(E[p^{n+1}]) = \mathbb{Q}(E[p^n])$. Then $p = 2$ and $n = 1$.*
- (2) *If $\mathbb{Q}(E[p^n]) \cap \mathbb{Q}(\zeta_{p^{n+1}}) = \mathbb{Q}(\zeta_{p^{n+1}})$, then $p = 2$.*

The problem of classifying such coincidences for elliptic curves defined over number fields was also recently investigated by Yvon in [\[44\]](#).

In the end, we are able to give a complete classification of elliptic curves over \mathbb{Q} with a near coincidence of their p^{n+1} and p^n division fields; i.e., when $\mathbb{Q}(E[p^{n+1}]) = \mathbb{Q}(E[p^n], \zeta_{p^{n+1}})$.

Theorem 1.13. *Let E/\mathbb{Q} be an elliptic curve, $p \in \mathbb{Z}$ prime, and $n \in \mathbb{Z}^+$. Suppose that*

$$\mathbb{Q}(E[p^{n+1}]) = \mathbb{Q}(E[p^n], \zeta_{p^{n+1}}).$$

Then $p \in \{2, 3\}$ and $n = 1$. Further, if $p = 2$, then E must correspond to a rational point on the one of the modular curves with RSZB label 4.48.0.3 or 4.16.0.2, while if $p = 3$, then E must come from a rational point on 9.27.0.1.

Remark 1.14. Before moving on, we point out that elliptic curves corresponding to rational points on 4.16.0.2 have the property that $\mathbb{Q}(E[4]) = \mathbb{Q}(E[2]) = \mathbb{Q}(E[2], i)$. Thus, these curves actually have a coincidence of division fields. In contrast, the elliptic curves corresponding to rational points on 4.48.0.3 have the property that $\mathbb{Q}(E[2]) = \mathbb{Q}$ and $\mathbb{Q}(E[4]) = \mathbb{Q}(i)$. So these curves have a near coincidence without having a coincidence of division fields. It is interesting to note that in order to have a near coincidence between the 2- and 4-division fields, without having an

actual coincidence between the 2- and 4-division fields, the 2-division field has to be trivial.

Similarly, the rational points on 9.27.0.1 yield elliptic curves with a near coincidence between their 3- and 9-division fields. Unlike the case with $p = 2$, a rational point on 9.27.0.1 corresponds to an elliptic curve E with either $j(E) = 0$ or a surjective $\bar{\rho}_{E,3}$. In particular, if E is a non-CM elliptic curve with $\mathbb{Q}(E[9]) = \mathbb{Q}(E[3], \zeta_9)$, we must have $[\mathbb{Q}(E[3]) : \mathbb{Q}] = 48$.

Remark 1.15. We choose to begin this paper with the Gauss–Wantzel theorem not only because of its classical significance, but because it serves as a natural entry point for a broad audience into the kinds of questions that we hope to address in this paper. The main objective here is to classify when the division field $\mathbb{Q}(E[n])/\mathbb{Q}$ of an elliptic curve E over \mathbb{Q} is nilpotent. Along the way, we uncover a surprising analog of the Gauss–Wantzel theorem as well as a result about near coincidences of division fields. We hope that the Gauss–Wantzel analog, while not the main thrust of the paper, illustrates the value of considering questions like these.

Outline of the paper. In [Section 2](#) we recall basic facts related to elliptic and modular curves that will be necessary for the proof of the main results. The proof of [Theorem 1.13](#) will be handled in [Section 3](#) by finding the smallest power n such that $\mathbb{Q}(E[p^{n+1}])$ cannot be $\mathbb{Q}(E[p^n], \zeta_{p^{n+1}})$ and then we prove that if $\mathbb{Q}(E[p^{n+1}]) \neq \mathbb{Q}(E[p^n], \zeta_{p^{n+1}})$, then $\mathbb{Q}(E[p^{n+2}]) \neq \mathbb{Q}(E[p^{n+1}], \zeta_{p^{n+2}})$. The proof will have to be broken down into cases depending on if $p = 2, 3, 5$, or $p \geq 7$.

The proof of [Theorem 1.9](#) starts in [Section 4](#) by using group theory to classify the nilpotent subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ according to their image in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$. We then apply known results about the corresponding modular curves to determine when the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ can be nilpotent. This is where we will employ [Conjecture 1.8](#).

In [Section 5](#) we use the information from the previous section to prove that if p is odd, then the p^2 -division field is never nilpotent. Lastly, in [Section 6](#) we study which combinations of mod p images can occur simultaneously, and prove [Theorem 1.9](#). Throughout the paper we address the case of elliptic curves with complex multiplication separately from those without complex multiplication because of their unique properties (which are outlined in [Section 2.1.1](#)).

All of the computations in this paper were performed using Magma [\[4\]](#) and the code can be found at [\[8\]](#).

2. Background

The goal of this section is to review some of the background information necessary for the proofs of the main theorems. In each subsection readers should find some additional resources to supplement what is written here.

2.1. Elliptic curves. For background about elliptic curves, see [39]. Given an elliptic curve E/\mathbb{Q} and a natural number n , the points of order dividing n defined over $\overline{\mathbb{Q}}$ form a group. Considering $E(\mathbb{C})$ as the quotient of \mathbb{C} by a lattice shows that

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

This isomorphism is noncanonical, but it only requires a choice of basis for $E[n]$.

Because the group law on an elliptic curve is given by rational functions, $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$ component-wise. That is, if $P = (x, y) \in E[n]$ and $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then $P^\sigma = (\sigma(x), \sigma(y)) \in E[n]$. This component-wise action induces a representation

$$\bar{\rho}_{E,n} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

with the property that $\text{Im } \bar{\rho}_{E,n} \simeq \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. We remark here that because the isomorphism $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ is noncanonical, $\text{Im } \bar{\rho}_{E,n}$ is really only defined up to conjugation.

A guiding principle in this paper is that oftentimes things can be broken down into cases depending on the shape of $\text{Im } \bar{\rho}_{E,p}$. We are able to do this thanks to the following proposition.

Proposition 2.1 [42, Lemma 2]. *Let p be a prime and let G be a subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$. If p divides $|G|$ then, either $\text{SL}_2(\mathbb{Z}/p\mathbb{Z}) \subseteq G$, or G is contained inside a Borel subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$. If p does not divide $|G|$, let H be the image of G in $\text{PGL}_2(\mathbb{Z}/p\mathbb{Z})$; then*

- (1) H is cyclic and G is contained inside a Cartan subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$, or
- (2) H is dihedral and G is contained in the normalizer of a Cartan subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$, but not the Cartan itself, or
- (3) H is isomorphic to A_4 , S_4 and A_5 .

In case (2), p must be odd. In case (3), p must be relatively prime to 6, 6, and 30 respectively.

We will say more about the Cartan subgroups when we discuss elliptic curves with complex multiplication in [Section 2.1.1](#).

Before moving on from Galois representations attached to elliptic curves, we draw attention to the fact that we can combine mod p^k representations using inverse limits to define the p -adic Galois representations

$$\rho_{E,p^\infty} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z}_p).$$

An important point, for our purposes, is that if $p \geq 5$, then the group $\text{SL}_2(\mathbb{Z}_p)$ has no proper closed subgroups whose image is $\text{SL}_2(\mathbb{Z}/p\mathbb{Z})$ under the standard reduction map. As Serre explains, this leads to the following proposition.

Proposition 2.2 [35, Section IV]. *Let E/\mathbb{Q} be an elliptic curve and let $p \geq 5$ be a prime. If $\bar{\rho}_{E,p}$ is surjective, then ρ_{E,p^∞} is also surjective.*

To see how this breaks down when $p = 2$ or 3 , the reader is encouraged to consult [11] and [13].

Lastly, we note that given an elliptic curve over \mathbb{Q} , the group $\text{Im } \bar{\rho}_{E,n}$ must have a few special properties.

Definition 2.3. Let $n \geq 2$ be a positive integer and let G be a subgroup of $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$. We say that G is an *admissible* group if

- $\det(G) = (\mathbb{Z}/n\mathbb{Z})^\times$, and
- G contains an element of determinant -1 and trace 0 that fixes a point of order n inside of $(\mathbb{Z}/n\mathbb{Z})^2$.

Proposition 2.4 [45, Proposition 2.2]. *Let $n \geq 2$ be an integer and let E/\mathbb{Q} be an elliptic curve. Then, $\text{Im } \bar{\rho}_{E,n}$ is an admissible subgroup of $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$.*

2.1.1. Elliptic curves with complex multiplication. Elliptic curves come in two distinct types depending on their endomorphism rings. Given an elliptic curve E , defined over a field of characteristic 0 , the endomorphism ring of E over $\bar{\mathbb{Q}}$ is either isomorphic to \mathbb{Z} or an order of an imaginary quadratic field, usually denoted by \mathcal{O} . When the endomorphism ring is larger than \mathbb{Z} we say that E has *complex multiplication* by \mathcal{O} . Throughout this section we follow the work done in [34, Section 12]. Many of the results we use were first proven in [28]. A reader looking for an introduction to elliptic curves with complex multiplication should see [38, Chapter II].

One way to think about elliptic curves with complex multiplication is as elliptic curves with additional symmetries. These added symmetries manifest themselves in many ways. They endow elliptic curves with complex multiplication with many interesting properties that make them unique among elliptic curves in general. Of particular interest to us is that the Galois representations attached to elliptic curves with complex multiplication behave very differently than those without complex multiplication.

We introduce some notation to state results about the Galois representations attached to elliptic curves with complex multiplication.

Given \mathcal{O} , an order of a quadratic imaginary field K . We define the *adelic Cartan subgroup associated to \mathcal{O}* to be

$$\mathcal{C}_{\mathcal{O}} = \varprojlim (\mathcal{O}/N\mathcal{O})^\times$$

where N is a positive integer and the inverse limit is taken with respect to divisibility.

Next, we let \mathcal{O}_K be the maximal order inside of K and we let $f = [\mathcal{O}_K : \mathcal{O}]$ be the conductor of \mathcal{O} . Continuing, we let $D = \text{disc}(\mathcal{O}) = f^2 \text{disc}\mathcal{O}$, and

$$\phi = \begin{cases} f & D \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

Then, we let

$$\omega = \frac{\phi + \sqrt{D}}{2} \quad \text{and} \quad \delta = \frac{D - \phi^2}{4},$$

so that $\mathcal{O} = \text{Span}_{\mathbb{Z}}\{1, \omega\}$ with $\omega^2 - \phi\omega - \delta = 0$. We can now define the level N Cartan subgroup associated to \mathcal{O} as

$$\begin{aligned} \mathcal{C}_{\mathcal{O}}(N) &= \left\{ \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix} : a, b \in \mathbb{Z}/N\mathbb{Z} \quad \text{and} \quad a^2 + ab\phi - \delta b^2 \in (\mathbb{Z}/N\mathbb{Z})^\times \right\} \\ &\subseteq \text{GL}_2(\mathbb{Z}/N\mathbb{Z}). \end{aligned}$$

Taking inverse limits as N runs over the positive integers ordered by divisibility of the level N , we can define

$$\mathcal{C}_{\mathcal{O}}(\widehat{\mathbb{Z}}) = \varprojlim \mathcal{C}_{\mathcal{O}}(N) \subseteq \text{GL}_2(\widehat{\mathbb{Z}}).$$

The group $\mathcal{C}_{\mathcal{O}}(\widehat{\mathbb{Z}})$ is a closed subgroup of $\text{GL}_2(\widehat{\mathbb{Z}})$ that is isomorphic to $\mathcal{C}_{\mathcal{O}}$ under the isomorphism

$$a + b\omega \mapsto \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix}.$$

Next, we define

$$\mathcal{N}_{\mathcal{O}}(N) = \langle \mathcal{C}_{\mathcal{O}}(N), \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix} \rangle$$

and let $\mathcal{N}_{\mathcal{O}}(\widehat{\mathbb{Z}}) \subseteq \text{GL}_2(\widehat{\mathbb{Z}})$ and $\mathcal{N}_{\mathcal{O}}(\mathbb{Z}_p) \subseteq \text{GL}_2(\widehat{\mathbb{Z}}_p)$ be the usual inverse limits of the $\mathcal{N}_{\mathcal{O}}(N)$.

Remark 2.5. Frequently the group $\mathcal{N}_{\mathcal{O}}$ is called the normalizer of $\mathcal{C}_{\mathcal{O}}$. It turns out that the group $\mathcal{N}_{\mathcal{O}}(\mathbb{Z}_p)$ is the normalizer of $\mathcal{C}_{\mathcal{O}}(\mathbb{Z}_p)$ in $\text{GL}_2(\mathbb{Z}_p)$ (by [28, Proposition 5.6(2)]), but $\mathcal{N}_{\mathcal{O}}$ is not the normalizer of $\mathcal{C}_{\mathcal{O}}$ in $\text{GL}_2(\widehat{\mathbb{Z}})$. See [34, Remark 12.1.2].

Before moving on we make a few more observations about these groups that will be useful later on. First we note that by construction each of the groups $\mathcal{C}_{\mathcal{O}}(N)$ is an abelian group since $\mathcal{O}/N\mathcal{O}$ is abelian. In contrast, the groups $\mathcal{N}_{\mathcal{O}}$ are not abelian unless $p = 2$. In order to compute the center of $\mathcal{N}_{\mathcal{O}}(N)$, it would be a simple matter of determining which matrices in $\mathcal{C}_{\mathcal{O}}(N)$ commute with $M = \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix}$. Let

$$A = \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix} \in \mathcal{C}_{\mathcal{O}}(N).$$

Computing the entry in the first row, second column of MA and AM we see that A commutes with M if and only if $b = -b$. Thus, if $p \neq 2$, then $A \in Z(\mathcal{N}_{\mathcal{O}}(N))$ if and only if $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI \in Z(\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}))$. From this we get:

Lemma 2.6. *Let $N > 2$ be an integer. Let G be a subgroup of $\mathcal{N}_{\mathcal{O}}(N)$ such that*

$$\begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix} \in G.$$

Then the center of G , $Z(G)$, is exactly the set of scalar matrices in G . In other words,

$$Z(G) = Z(\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})) \cap G.$$

The last few theorems we need will help us pin down the exact image of the Galois representations attached to elliptic curves with complex multiplication. We will state the following theorems for elliptic curves with complex multiplication defined over \mathbb{Q} , but we note that both [34, Section 12] and [28] handle the case where E is defined over a number field.

Proposition 2.7 [34, Proposition 12.1.4]. *Let E/\mathbb{Q} be an elliptic curve with complex multiplication by \mathcal{O} , let p be a prime, and let*

$$e = \begin{cases} 4 & \text{if } p = 2, \\ 3 & \text{if } p = 3, \\ 1 & \text{otherwise.} \end{cases}$$

Then $\mathrm{Im} \rho_{E,p^\infty}$ is the inverse image of $\mathrm{Im} \bar{\rho}_{E,p^e}$ under the reduction map $\mathcal{N}_{\mathcal{O}}(\mathbb{Z}_p) \rightarrow \mathcal{N}_{\mathcal{O}}(\mathbb{Z}/p^e\mathbb{Z})$.

Proposition 2.7 will be exactly what we need in order to understand how the division fields change as we go up the p -adic tower. This will be useful in [Section 5](#).

Proposition 2.8 [28, Theorem 1.2(4)]. *Let E/\mathbb{Q} be an elliptic curve with complex multiplication by $\mathcal{O} \neq \mathbb{Z}[\zeta_3]$. If p does not divide $2 \mathrm{disc}(\mathcal{O})$, then there is a choice of basis such that $\mathrm{Im} \rho_{E,p^\infty} = \mathcal{N}_{\mathcal{O}}(\mathbb{Z}_p)$.*

2.2. Modular curves. Modular curves are the main objects that we will use to classify the elliptic curves over \mathbb{Q} with a given admissible group as the image of their mod n representation. Given a natural number $n \geq 2$ and an admissible subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ there is a smooth, projective, and geometrically irreducible curve defined over \mathbb{Q} denoted X_G whose \mathbb{Q} -rational points classify elliptic curves with the property that $\mathrm{Im} \bar{\rho}_{E,n}$ is conjugate to a *subgroup* of G . Here we emphasize that the image of $\mathrm{Im} \bar{\rho}_{E,n}$ need not be all of G in order to have a corresponding point on X_G . Indeed, since subgroups of nilpotent groups are nilpotent, this will allow us to focus on finding the maximal admissible nilpotent groups of a given level.

The nature of this correspondence depends on whether $-I \in G$ or not, but if G were a nilpotent group that did not contain $-I$, then adding $-I$ would preserve

nilpotency. For this reason, we can assume that $-I \in G$. Then the curve X_G always comes with a natural morphism

$$\pi_G : X_G \rightarrow \mathbb{P}_{\mathbb{Q}}^1$$

such that an elliptic curve E/\mathbb{Q} with j -invariant $j_E \notin \{0, 1728\}$, has $\text{Im } \bar{\rho}_{E,n}$ conjugate to a subgroup of G if and only if $j_E = \pi_G(P)$ for some $P \in X_G(\mathbb{Q})$. The interested reader should see [34, Subsection 2.3] to see more details when $-I \notin G$.

We end this section by emphasizing that a complete classification of the points on these curves would give a corresponding classification of $\text{im } \bar{\rho}_{E,n}$ for every elliptic curve E/\mathbb{Q} . That is, if we can determine all of the maximal nilpotent subgroups H of $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and classify all the rational points on the corresponding X_H 's, then we would have classified all the elliptic curves with nilpotent n -division fields.

3. Near coincidences

In order to classify near coincidences, it will be useful to be able to detect them using the image of the corresponding Galois representation. With this in mind, we give the following definition.

Definition 3.1. Let $G \subseteq \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$ with surjective determinant and suppose that $m \mid n$. We say that G represents a near coincidence of level (n, m) if

$$(G \cap \text{SL}_2(\mathbb{Z}/n\mathbb{Z})) \cap \text{Ker}(\pi) = \{I\},$$

where $\pi : \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \rightarrow \text{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is the standard componentwise reduction map.

Remark 3.2. The idea behind this definition is that classically we know that $(G \cap \text{SL}_2(\mathbb{Z}/n\mathbb{Z}))$ fixes $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$ and $\text{Ker}(\pi)$ fixes $\mathbb{Q}(E[m]) \subseteq \mathbb{Q}(E[n])$. Therefore, $(G \cap \text{SL}_2(\mathbb{Z}/n\mathbb{Z})) \cap \text{Ker}(\pi)$ should fix $\mathbb{Q}(E[m], \zeta_n)$. Thus, the only way that $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m], \zeta_n)$ is if $(G \cap \text{SL}_2(\mathbb{Z}/n\mathbb{Z})) \cap \text{Ker}(\pi) = \{I\}$.

Of course this definition requires that $m \mid n$, but that lines up with the original definition of near coincidence.

The proof of [Theorem 1.13](#) will be done by first considering the case of prime level and then moving on to the case of prime power level. We will have to break the prime level case down into 3 smaller cases. These cases consist of when $p = 2$, $p = 3$, or $p \geq 5$.

3.1. Proof of [Theorem 1.13](#) for prime levels. We will start the case when $n = 1$ of the theorem by dealing with primes $p \geq 5$ and break the argument into cases depending on $\text{Im } \bar{\rho}_{E,p}$ based on [Proposition 2.1](#). First we handle the case that $\bar{\rho}_{E,p}$ is surjective.

Proposition 3.3. *Assume that E/\mathbb{Q} is an elliptic curve, $p \geq 5$ is prime, and $\text{Im } \bar{\rho}_{E,p} = \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Then $\mathbb{Q}(E[p^2]) \neq \mathbb{Q}(E[p], \zeta_{p^2})$.*

Proof. By [Proposition 2.2](#), we have $\text{Im } \rho_{E,p^\infty} = \text{GL}_2(\mathbb{Z}_p)$ and hence $\text{Im } \bar{\rho}_{E,p^2} = \text{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. Hence

$$[\mathbb{Q}(E[p^2]) : \mathbb{Q}] = |\text{GL}_2(\mathbb{Z}/p^2\mathbb{Z})| = p^5(p-1)^2(p+1),$$

while

$$\begin{aligned} [\mathbb{Q}(E[p], \zeta_{p^2})] &\leq [\mathbb{Q}(E[p], \zeta_{p^2}) : \mathbb{Q}(E[p])][\mathbb{Q}(E[p]) : \mathbb{Q}] \\ &\leq p(p-1) \cdot |\text{GL}_2(\mathbb{Z}/p\mathbb{Z})| \\ &= p^2(p-1)^3(p+1) < p^5(p-1)^2(p+1). \end{aligned}$$

This proves the claim. \square

Next we handle the case that $\text{Im } \bar{\rho}_{E,p}$ is a proper subgroup whose order is a multiple of p .

Proposition 3.4. *Assume that E/\mathbb{Q} is an elliptic curve, $p \geq 5$ is prime, and $\text{Im } \bar{\rho}_{E,p}$ is a proper subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ whose order is a multiple of p . Then $\mathbb{Q}(E[p^2]) \neq \mathbb{Q}(E[p], \zeta_{p^2})$.*

Proof. In this case, the image of $\text{Im } \bar{\rho}_{E,p}$ is contained in a Borel subgroup by [Proposition 2.1](#) and hence E has a cyclic p -isogeny defined over \mathbb{Q} . By the classification of Mazur, we have $p \in \{5, 7, 11, 17, 19, 43, 67, 163\}$. Let $H = \text{im } \rho_{E,p^\infty}$.

If E has complex multiplication, choose a basis so that $H \subseteq \mathcal{N}_{\mathcal{O}}(\mathbb{Z}_p)$. By [Proposition 2.7](#), H is the full preimage in $\mathcal{N}_{\mathcal{O}}(\mathbb{Z}_p)$ of $\text{Im } \bar{\rho}_{E,p}$. Since $\mathcal{N}_{\mathcal{O}}(\mathbb{Z}_p)$ contains all matrices of the form $\begin{pmatrix} 1+kp & 0 \\ 0 & 1-kp \end{pmatrix}$ with $k \in \mathbb{Z}/p\mathbb{Z}$ and this implies that $\mathbb{Q}(E[p^2])/\mathbb{Q}(E[p], \zeta_{p^2})$ is a nontrivial extension.

If E does not have complex multiplication, then Theorem 1.1.6 of [\[34\]](#) implies that X_H is isomorphic to \mathbb{P}^1 or a positive rank elliptic curve, or that X_H is listed in Table 1 of [\[34\]](#) as the other cases are ruled out by the assumption that $p \mid |\text{Im } \bar{\rho}_{E,p}|$. If we assume that $\mathbb{Q}(E[p^2]) = \mathbb{Q}(E[p], \zeta_{p^2})$, then $p^2 \nmid |\text{Im } \bar{\rho}_{E,p^2}|$ and this implies that the index of H in $\text{GL}_2(\mathbb{Z}_p)$ is a multiple of p^3 . Since $p \geq 5$, this implies that the index is ≥ 125 and this implies that X_H has genus ≥ 2 . There are groups H contained in a Borel subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ listed in Table 1 of [\[34\]](#) for $p = 11, 17$ and 37 , but in no case is the index of H a multiple of p^3 . This concludes the proof. \square

Next we handle the case that $\text{Im } \bar{\rho}_{E,p}$ is contained in the normalizer of a split Cartan subgroup. We divide the argument into the CM case and the non-CM case.

Proposition 3.5. *Let E/\mathbb{Q} be an elliptic curve and $p \geq 5$ a prime such that $\text{Im } \bar{\rho}_{E,p}$ is contained in the normalizer of a split Cartan subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Then $\mathbb{Q}(E[p^2]) \neq \mathbb{Q}(E[p], \zeta_{p^2})$.*

Proof. We first will show that E has complex multiplication. If E does not have complex multiplication, then the results of [3] rule out $p = 11$ and $p \geq 17$, and the results of [1] rule out $p = 13$. Hence $p \in \{5, 7\}$. If $H = \text{Im } \bar{\rho}_{E,p^2}$ and $\mathbb{Q}(E[p^2]) = \mathbb{Q}(E[p], \zeta_{p^2})$, then H is an index p^3 subgroup of the full preimage in $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ of $\text{Im } \bar{\rho}_{E,p}$ and hence

$$(*) \quad |H| \text{ divides } \frac{|\text{GL}_2(\mathbb{Z}/p^2\mathbb{Z})|}{p^4(p+1)/2},$$

since $\frac{p(p+1)}{2}$ is the index of the normalizer of the split Cartan in $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$. In addition, by Proposition 2.4, H must also be an admissible group. Finally, H must be nonabelian, since by [16] $\mathbb{Q}(E[n])/\mathbb{Q}$ is nonabelian if $n > 8$.

For these two primes p , we use Magma to search for admissible subgroups H of $\text{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ such that $(*)$ is satisfied and H is nonabelian. For $p = 5$ there are two conjugacy classes of such subgroups and for $p = 7$ there are four. In both cases, all such subgroups are contained in the normalizer of a split Cartan subgroup of $\text{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. (The code for these calculations can be found in the file prop35.m at [8].) The rational points on the modular curve corresponding to the normalizer of the split Cartan subgroup mod 25 are determined by Momose and Shimura in [30], and the mod 49 case is handled by Momose in [29]. In both cases, all such elliptic curves have CM. It follows that E has complex multiplication.

Now we show that if E has complex multiplication, then $\mathbb{Q}(E[p^2]) \neq \mathbb{Q}(E[p], \zeta_{p^2})$. The argument here is identical to that in the proof of Proposition 3.4. Choose a basis so that $\text{Im } \bar{\rho}_{E,p^2} \subseteq \mathcal{N}_{\mathcal{O}}(\mathbb{Z}_p)$. By Proposition 2.7, $\text{Im } \bar{\rho}_{E,p^2}$ is the full preimage in $\mathcal{N}_{\mathcal{O}}(\mathbb{Z}_p)$ of $\text{Im } \bar{\rho}_{E,p}$. Therefore, $\text{Im } \bar{\rho}_{E,p^2}$ contains all matrices of the form $\begin{pmatrix} 1+kp & 0 \\ 0 & 1-kp \end{pmatrix}$ with $k \in \mathbb{Z}/p\mathbb{Z}$ and this implies that $\mathbb{Q}(E[p^2])/\mathbb{Q}(E[p], \zeta_{p^2})$ is a nontrivial extension. \square

The last case to be dealt with is when $\text{Im } \bar{\rho}_{E,p}$ is contained in the normalizer of a nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for $p \geq 5$. Importantly, we know from [23, Appendix B] or [45, Proposition 1.13] that in this case any such elliptic curve has to have potentially supersingular reduction at p .

Proposition 3.6 [36, p. 312]. *Let E/\mathbb{Q} be an elliptic curve with potential good reduction at $p \geq 5$ and discriminant Δ . Then, E acquires good reduction over $\mathbb{Q}(\sqrt[12]{\Delta})$ at all primes over p .*

In [loc. cit.], Serre explains that not only does E gain good reduction over $\mathbb{Q}(\sqrt[12]{\Delta})$, but also that $\text{ord}_p(\Delta) \in \{0, 2, 3, 4, 6, 8, 9, 10\}$. Thus, if \mathfrak{p} is a prime above p in $\mathbb{Q}(\sqrt[12]{\Delta})$, then $e(\mathfrak{p}/p) \in \{1, 2, 3, 4, 6\}$.

Even with this in hand, for $p = 5$ we will have to rely on the classification of rational points provided in [34].

Proposition 3.7. *Let E/\mathbb{Q} be such that $\text{im } \bar{\rho}_{E,5}$ is contained in the normalizer of the nonsplit Cartan subgroup mod 5. Then $\mathbb{Q}(E[25]) \neq \mathbb{Q}(E[5], \zeta_{25})$.*

Proof. We search $\text{GL}_2(\mathbb{Z}/25\mathbb{Z})$ for groups that represent (25, 5) near coincidences. We then take the ones that are maximal with respect to containment (up to conjugation) and check if they have points. These groups are exactly the groups with RSZB labels

$$25.625.36.1, \quad 25.1250.76.1, \quad 25.2500.156.\{2,3\}, \quad 25.3750.236.\{1,2\}$$

(where we have used braces to combine almost identical labels). Using the data in [34], we see that there are no noncuspidal \mathbb{Q} -rational points on any of these curves and so there are no elliptic curves over \mathbb{Q} with a (25, 5) near coincidence. \square

We now turn to the case that $p \geq 7$.

Proposition 3.8. *Let E/\mathbb{Q} be an elliptic curve and let $p \geq 7$ be a prime such that $\text{Im } \bar{\rho}_{E,p}$ is a subgroup of the normalizer of a nonsplit Cartan subgroup $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Let Δ be the discriminant of E and suppose that $\mathbb{Q}(E[p^2]) = \mathbb{Q}(E[p], \zeta_{p^2})$. Let \mathfrak{p} be a prime over p in $\mathbb{Q}(\sqrt[p^2]{\Delta})$. The extension $\mathbb{Q}(\sqrt[p^2]{\Delta}, E[p^2])/\mathbb{Q}(\sqrt[p^2]{\Delta})$ is a degree $2p(p^2 - 1)$ extension that is totally ramified at \mathfrak{p} .*

Proof. Suppose towards a contradiction that there is a prime \mathfrak{P} above \mathfrak{p} such that $e(\mathfrak{P}/\mathfrak{p})$ is a proper divisor of $2p(p^2 - 1)$. Since $\text{Im } \bar{\rho}_{E,p}$ is a subgroup of the normalizer of a nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$, we know that $[\mathbb{Q}(E[p]) : \mathbb{Q}]$ is a divisor of $2(p^2 - 1)$. Further, because we assumed that $\mathbb{Q}(E[p^2]) = \mathbb{Q}(E[p], \zeta_{p^2})$, we know that $[\mathbb{Q}(E[p^2]) : \mathbb{Q}]$ is a divisor of $2p(p^2 - 1)$. Thus $\mathbb{Q}(\sqrt[p^2]{\Delta}, E[p^2])/\mathbb{Q}(\sqrt[p^2]{\Delta})$ has degree dividing $2p(p^2 - 1)$. Now, $e(\mathfrak{P}/\mathfrak{p})$ is a proper divisor of $|\bar{\rho}_{E,p^2}(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt[p^2]{\Delta})))|$, which itself divides $2p(p^2 - 1)$. Thus

$$e(\mathfrak{P}/\mathfrak{p}) \leq p(p^2 - 1) \quad \text{and} \quad e(\mathfrak{P}/p) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/p) \leq p(p^2 - 1) \cdot 6 < p^2(p^2 - 1).$$

But a result of Hanson Smith [40, Theorem 1.1] says that $e(\mathfrak{P}/p) \geq p^4 - p^2 = p^2(p^2 - 1)$, giving us our contradiction. \square

We now explain how the previous proposition rules out the possibility of a (p^2, p) near coincidence.

Proposition 3.9. *Let E/\mathbb{Q} be an elliptic curve and let $p \geq 7$ be a prime such that $\text{Im } \bar{\rho}_{E,p}$ is a subgroup of the normalizer of a nonsplit Cartan subgroup $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Then $\mathbb{Q}(E[p^2]) \neq \mathbb{Q}(E[p], \zeta_{p^2})$.*

Proof. Suppose towards a contradiction that $\mathbb{Q}(E[p^2]) = \mathbb{Q}(E[p], \zeta_{p^2})$. By the previous proposition, we know that $\mathbb{Q}(\sqrt[p^2]{\Delta}, E[p^2])/\mathbb{Q}(\sqrt[p^2]{\Delta})$ is totally ramified at \mathfrak{p} .

The assumption that $\mathbb{Q}(E[p^2]) = \mathbb{Q}(E[p], \zeta_{p^2})$ implies that $\text{Im } \bar{\rho}_{E,p^2}$ has order dividing $2p(p^2 - 1)$. On the other hand, [Proposition 3.8](#) implies that

$$|\bar{\rho}_{E,p^2}(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt[12]{\Delta})))| = 2p(p^2 - 1).$$

It follows from this that

$$\text{Im } \bar{\rho}_{E,p^2} = \bar{\rho}_{E,p^2}(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt[12]{\Delta})))$$

and hence

$$\text{Gal}(\mathbb{Q}(\sqrt[12]{\Delta}, E[p^2])/\mathbb{Q}(\sqrt[12]{\Delta})) \simeq \text{Im } \bar{\rho}_{E,p^2}.$$

However, a Galois extension that is totally ramified at a prime over p must have a Galois group which is an extension of a finite p -group (the wild inertia group) by a finite cyclic group of order coprime to p (the tame inertia group). This means that for any prime $q \neq p$, the q -Sylow subgroup of $\text{Im } \bar{\rho}_{E,p^2}$ must be cyclic. In particular, the Sylow 2-subgroup of $\text{Im } \bar{\rho}_{E,p^2}$ must be cyclic. However, by [\[16\]](#), $\mathbb{Q}(E[p])/\mathbb{Q}$ must be nonabelian, and so the projectivization of $\text{Im } \bar{\rho}_{E,p}$ must have a dihedral Sylow 2-subgroup. This is a contradiction. \square

The last remaining case is that $\text{Im } \bar{\rho}_{E,p}$ is contained in an exceptional group — that is, the image in $\text{PGL}_2(\mathbb{F}_p)$ falls into case 3 of [Proposition 2.1](#).

Proposition 3.10. *Let E/\mathbb{Q} be an elliptic curve and let $p \geq 5$ be a prime such that $\text{Im } \bar{\rho}_{E,p}$ is contained in an exceptional subgroup. Then $\mathbb{Q}(E[p^2]) \neq \mathbb{Q}(E[p], \zeta_{p^2})$.*

Proof. Serre showed [\[37, §8.4, lemme 18\]](#) that $\text{Im } \bar{\rho}_{E,p}$ can only be an exceptional subgroup if image in $\text{PGL}_2(\mathbb{F}_p)$ is isomorphic to S_4 , $p \leq 13$ and $p \equiv 3$ or $5 \pmod{8}$.

The elliptic curves with $\text{Im } \bar{\rho}_{E,13}$ contained in an exceptional subgroup were determined in [\[2\]](#) and in [\[34\]](#) it was shown that for each such elliptic curve, $\text{Im } \bar{\rho}_{E,13^2}$ contains all matrices $\equiv I \pmod{13}$, which implies that $\mathbb{Q}(E[p^2]) \neq \mathbb{Q}(E[p], \zeta_{p^2})$.

For $p = 11$, the elliptic curves with $\text{Im } \bar{\rho}_{E,11}$ contained an exceptional subgroup were determined by Ligozat [\[26, Proposition II.4.4.8.1\]](#) and the only possibility is $j(E) = 0$. For such an elliptic curve, we cannot have $\mathbb{Q}(E[11^2]) = \mathbb{Q}(E[11], \zeta_{11^2})$ by [Proposition 2.7](#).

For $p = 5$, if $\text{Im } \bar{\rho}_{E,5}$ is contained in an exceptional subgroup, then it either equals an exceptional subgroup, or is contained in a Borel or the normalizer of a split Cartan. The latter two cases are impossible by [Proposition 3.4](#) and [Proposition 3.5](#). If the image is the exceptional subgroup mod 5, then a group theory computation with Magma shows that the mod 25 image of Galois has RSZB label 25.625.36.1, which is shown to be impossible in [\[34, Subsection 8.6\]](#). \square

In the case when $p = 2$ and 3, we search $\text{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ for subgroups that represent a near coincidence of level (p^2, p) and then compute the maximal groups ordered by containment up to conjugation. Doing this yields curves with labels

4.16.0.1, 4.16.0.2 and 4.48.0.3 when $p = 2$, and 9.27.0.1, 9.162.4.1 and 9.324.10.1 when $p = 3$. Thanks to [27; 34; 33] we know that 4.16.0.2, 9.162.4.1, and 9.324.10.1 do not have any rational points and so can be omitted. To summarize:

Proposition 3.11. *Let E/\mathbb{Q} be an elliptic curve and let $p \in \mathbb{Z}$ be a prime such that $\mathbb{Q}(E[p^2]) = \mathbb{Q}(E[p], \zeta_{p^2})$. Then, $p = 2$ or $p = 3$ and E corresponds to a rational point on one of the modular curves with RSZB labels 4.48.0.3, 4.16.0.2, or 9.27.0.1.*

3.2. Proof of Theorem 1.13 for prime power levels. To start this section, we push a little further in the cases where $p = 2$ and 3. These searches were carried out using a Magma script, NearCoin.m, which can be found in [8]. In both of these cases, we can have near coincidence between the p^2 - and p -division fields, but what about the p^3 - and p^2 -division fields?

So we search for groups that represent (8, 4) and (27, 9) coincidences. In the first case, we find that the maximal groups that represent an (8, 4) coincidence all have genus 1 or higher. Using the data in [33], we know that this means that there is no elliptic curve without complex multiplication that has these images, and we have already completely dealt with the CM case.

When considering (27, 9) coincidences, the maximal groups are the ones with RSZB labels

$$27.729.43.1, \quad 27.4374.280.\{1,2,3,4\}, \quad 27.8748.568.\{1,2,3,5\}.$$

Again, [34] says that the corresponding modular curves have no noncuspidal \mathbb{Q} -rational points and so there are no elliptic curves over \mathbb{Q} with a (27, 9) near coincidence.

Remark 3.12. In [34], it was shown that 27.729.43.1 cannot occur as the image of $\rho_{E,27}$ for any elliptic curve over \mathbb{Q} by writing down the canonical model of this modular curve in \mathbb{P}^{42} and showing it has no mod 9 points. The argument given above in Proposition 3.8 and Proposition 3.9 can be modified to give a simpler proof that this modular curve has no rational points. In particular, one can show that if E/\mathbb{Q} has mod 9 image contained in 9.27.0.1 (a supergroup of 27.729.43.1), then $\text{ord}_3(j(E)) \geq 7$. Since any elliptic curve with $j(E) \equiv 0 \pmod{3}$ has potentially supersingular reduction at 3, the argument (using Theorem 1.1 of [40]) can proceed along similar lines.

Next we prove by induction the case of Theorem 1.13 when $n \geq 2$.

Proposition 3.13. *Suppose that E/\mathbb{Q} is an elliptic curve and $p > 2$ is a prime such that p^k divides $[\mathbb{Q}(E[p^{n+1}]) : \mathbb{Q}(E[p^n])]$ for some $k \in \{1, 2, 3, 4\}$ and $n \geq 1$. Then, p^k divides $[\mathbb{Q}(E[p^{n+2}]) : \mathbb{Q}(E[p^{n+1}])]$.*

Proof. Assume that $n \geq 1$ and p^k divides $[\mathbb{Q}(E[p^{n+1}]) : \mathbb{Q}(E[p^n])]$ for some $k \in \{1, 2, 3, 4\}$. This means that the set

$$S = \{A \in \text{Im } \bar{\rho}_{E, p^{n+1}} : A \equiv I \pmod{p^n}\}$$

must have size at least p^k . Next, we let

$$\tilde{S} = \{A \in \text{Im } \bar{\rho}_{E, p^{n+2}} : A \equiv I \pmod{p^{n+1}}\}.$$

Our goal now is to show that there is an injective homomorphism from S to \tilde{S} . Doing this would allow us to conclude that $|S|$ divides $|\tilde{S}|$.

We can represent an element of S in the form $I + p^n X$ with X in the additive group $M_2(\mathbb{Z}/p\mathbb{Z})$ of 2×2 matrices. Define $\phi : S \rightarrow \tilde{S}$ by $\phi(I + p^n X) = I + p^{n+1} X$. It is straightforward to see that this formula defines an injective homomorphism, but it is not immediately clear that if $I + p^n X \in S$, then $I + p^{n+1} X \in \tilde{S}$. We now justify this.

If $I + p^n X \in S$ for some $X \in M_2(\mathbb{Z}/p\mathbb{Z})$, then there is a $\sigma_0 \in \text{Gal}(\mathbb{Q}(E[p^{n+1}])/\mathbb{Q})$ such that $\bar{\rho}_{E, p^{n+1}}(\sigma_0) = I + p^n X$. Further, there must be a $\sigma \in \text{Gal}(\mathbb{Q}(E[p^{n+2}])/\mathbb{Q})$ such that $\sigma|_{\mathbb{Q}(E[p^{n+1}])} = \sigma_0$. In this case, since $\bar{\rho}_{E, p^{n+1}}(\sigma_0) \equiv I + p^n X$ we have

$$\bar{\rho}_{E, p^{n+2}}(\sigma) = I + p^n \tilde{X}$$

for some $\tilde{X} \in M_2(\mathbb{Z}/p^2\mathbb{Z})$ such that $\tilde{X} \equiv X \pmod{p}$. Then

$$\begin{aligned} \bar{\rho}_{E, p^{n+2}}(\sigma^p) &\equiv (I + p^n \tilde{X})^p \pmod{p^{n+2}} \\ &\equiv I + p \cdot p^n \tilde{X} + \frac{1}{2} p(p-1) p^{2n} \tilde{X}^2 + \dots \pmod{p^{n+2}} \\ &\equiv I + p^{n+1} \tilde{X} \pmod{p^{n+2}} \equiv I + p^{n+1} X \pmod{p^{n+2}}. \end{aligned}$$

Thus $I + p^{n+1} X \in \tilde{S}$.

Since $|S|$ divides $|\tilde{S}|$, this forces $\mathbb{Q}(E[p^{n+2}])/\mathbb{Q}(E[p^{n+1}])$ to have degree at least $|S|$ and so

$$p^k \mid [\mathbb{Q}(E[p^{n+2}]) : \mathbb{Q}(E[p^{n+1}])]. \quad \square$$

Remark 3.14. If $p \geq 3$, then the statement $p^2 \mid [\mathbb{Q}(E[p^{n+1}]) : \mathbb{Q}(E[p^n])]$ is equivalent to $\mathbb{Q}(E[p^{n+1}]) \neq \mathbb{Q}(E[p^n], \zeta_{p^{n+1}})$. This is because the field extension $\mathbb{Q}(E[p^{n+1}])/\mathbb{Q}(E[p^n])$ is a Galois extension whose Galois group is isomorphic to a subgroup of the additive group $M_2(\mathbb{Z}/p\mathbb{Z})$ of 2×2 matrices with entries in $\mathbb{Z}/p\mathbb{Z}$. The group $M_2(\mathbb{Z}/p\mathbb{Z})$ has order p^4 and so a priori $[\mathbb{Q}(E[p^{n+1}]) : \mathbb{Q}(E[p^n])] = p^k$ for some $k \in \{0, 1, 2, 3, 4\}$. We omit the case when $k = 0$ in [Proposition 3.13](#) since it is uninteresting.

Next, we notice that

$$\begin{aligned} [\mathbb{Q}(E[p^{n+1}]) : \mathbb{Q}(E[p^n])] \\ = [\mathbb{Q}(E[p^{n+1}]) : \mathbb{Q}(E[p^n], \zeta_{p^{n+1}})] [\mathbb{Q}(E[p^n], \zeta_{p^{n+1}}) : \mathbb{Q}(E[p^n])]. \end{aligned}$$

But, by [Theorem 1.12](#), in this case $\zeta_{p^{n+1}} \notin \mathbb{Q}(E[p^n])$ and so

$$[\mathbb{Q}(E[p^n], \zeta_{p^{n+1}}) : \mathbb{Q}(E[p^n])] = p.$$

Bringing it all together we see that

$$\begin{aligned} p^2 \mid [\mathbb{Q}(E[p^n]) : \mathbb{Q}(E[p^{n-1}])] &\iff p \mid [\mathbb{Q}(E[p^n]) : \mathbb{Q}(E[p^{n-1}], \zeta_{p^n})] \\ &\iff [\mathbb{Q}(E[p^n]) : \mathbb{Q}(E[p^{n-1}], \zeta_{p^n})] \neq 1. \end{aligned}$$

Examining the proof of [Proposition 3.13](#), the term $\frac{1}{2}p(p-1)p^{2n}\tilde{X}^2$ is $\equiv 0 \pmod{p^{n+2}}$ if $(p, n) \neq (2, 1)$ but could fail if $p = 2$ and $n = 1$. With this in mind, we immediately get the following corollary.

Corollary 3.15. *Suppose that $p = 2$ and E/\mathbb{Q} is an elliptic curve such that p^k divides $[\mathbb{Q}(E[p^{n+1}]) : \mathbb{Q}(E[p^n])]$ for some $k \in \{1, 2, 3, 4\}$ and $n \geq 2$. Then, p^k divides $[\mathbb{Q}(E[p^{n+2}]) : \mathbb{Q}(E[p^{n+1}])]$*

Thus, we find ourselves at the end. The work of [3.1](#) together with [Proposition 3.13](#) and [Corollary 3.15](#) completes the proof of [Theorem 1.13](#).

4. Nilpotent division fields of prime level

We are now ready to start classifying when the division fields of elliptic curves can give us nilpotent extensions of \mathbb{Q} . Before starting the classification in earnest, we will quickly remind the reader of some basic facts about nilpotent groups.

4.1. Nilpotent groups. This subsection will only cover the very basics of subgroups series and nilpotent groups. For more context the reader can consult [\[5; 6; 12; 19\]](#).

Definition 4.1. Let G be a group. An ascending series

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G$$

is called a *central series* if for all i , $G_i \triangleleft G$ and $G_{i+1}/G_i \subseteq Z(G/G_i)$. Here $Z(G)$ is the center of G . A descending series

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq \{e\}$$

is called a *central series* if $G_i \triangleleft G$ and $G_i/G_{i+1} \subseteq Z(G/G_{i+1})$.

Definition 4.2. A group G is called *nilpotent* if it has a central series.

Theorem 4.3 [\[19, Theorem 1.26\]](#). *Let G be a finite nontrivial group. The following are equivalent:*

- (1) G is a nilpotent group.
- (2) Every Sylow subgroup of G is normal.
- (3) G is the direct product of its Sylow subgroups.
- (4) If d divides $|G|$, then G has a normal subgroup of order d .

An immediate consequence of this result is that every abelian group and every finite p -group is nilpotent.

Proposition 4.4 [5, Theorem 5.7]. *Nilpotency is closed under subgroups, quotients, and direct products.*

In general, given a group G and a nilpotent normal subgroup N , it is not true that G/N nilpotent implies that G is nilpotent. However if $N \leq Z(G)$, this follows from Theorem 5.13 of [5].

Proposition 4.5. *If G is a finite nontrivial group such that $Z(G) = \{e\}$, then G is not nilpotent.*

Proof. Suppose G is a finite nontrivial group that is nilpotent. Then, by Theorem 4.3, part (3), G is the direct products of its p -Sylow subgroups. A classical result in group theory is that p -group have nontrivial centers and so G must have a nontrivial center. □

Example 4.6. Let D_n be the dihedral group of order $2n$. More specifically, let

$$D_n = \langle r, s \mid r^n = s^2 = e, srs^{-1} = r^{-1} \rangle.$$

A classical result is that D_n is nilpotent exactly when $n = 2^k$ for some $k \geq 2$. In order to keep the statement of Proposition 2.1 as clean as possible, we will need to adopt the convention that $(\mathbb{Z}/2\mathbb{Z})^2$ is a dihedral group.

Example 4.7. Let p be a prime. The goal of this example is to show that $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is not nilpotent. A simple computation shows that $Z(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})) = \langle -I \rangle$ and by definition $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/Z(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}))$ is $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$. A classical result [20] is that $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ is simple for all $p \geq 5$. Since the center of a group is always normal and $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ is clearly nonabelian, $Z(\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z}))$ is trivial. Thus, $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ is not nilpotent. This together with Proposition 4.4 shows that $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is not nilpotent when $p \geq 5$. The cases when $p = 2$ and $p = 3$ can be easily checked by hand.

4.2. Classification of nilpotent division fields of prime level. Step 1 in the process of determining when an elliptic curve E/\mathbb{Q} can have a nilpotent n -division field, is determining when the p -division fields can be nilpotent extensions of \mathbb{Q} . Proposition 4.4 tells us that if $\mathbb{Q}(E[n])/\mathbb{Q}$ is nilpotent, then $\mathbb{Q}(E[d])/\mathbb{Q}$ is nilpotent for all $d \mid n$. Moreover, if $n = p_1^{a_1} \cdots p_k^{a_k}$ is the prime factorization of n , then

$\mathbb{Q}(E[n])/\mathbb{Q}$ is nilpotent if and only if $\mathbb{Q}(E[p_i^{a_i}])/\mathbb{Q}$ is nilpotent for all i . To see why this is true, one only needs to recall the Galois correspondence as well as the fact that nilpotency is preserved under subgroups, quotients, and direct products.

For this reason, we start by studying $\mathbb{Q}(E[p])/\mathbb{Q}$ and use that information to understand what happens at level p^2 and further up the p -adic tower.

To that end, we need a way to divide up the subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ so that we can study them. Fortunately, [Proposition 2.1](#) gives us exactly what we need.

Remark 4.8. If G is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, then G is nilpotent if and only if its image in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is nilpotent. The reason is as follows. If G is nilpotent, then its image in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is a quotient of G and is hence nilpotent. Conversely, if $G \leq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and the image of G in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is nilpotent, then the image of G in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is the quotient G/N , where N is the set of scalar multiples of the identity in G . This subgroup $N \leq Z(G)$ and by Theorem 5.13 of [5], it follows that G is nilpotent, since N can be extended into a central series.

The following result gives a classification of when an admissible subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is nilpotent.

Proposition 4.9. *Let p be a prime and G an admissible subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Then G is nilpotent if and only if G is abelian, or the image of G in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is isomorphic to D_{2^k} for some $k \geq 2$. Further, if p is odd, then G is either contained in the normalizer of a split or nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.*

Proof. If G is abelian, then it must be nilpotent. [Remark 4.8](#) shows that if the image of G in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is isomorphic to D_{2^k} (a 2-group) then G is nilpotent.

Now we assume that G is nilpotent and consider the cases based on [Proposition 2.1](#). First, if G contains $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, then G cannot be nilpotent since $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is not nilpotent.

Next, suppose that G is an admissible nilpotent group such that $p \mid |G|$, and G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Conjugating G if necessary, we may assume G is contained in the set of upper triangular matrices. The set of upper triangular matrices contains a unique subgroup of order p , namely the cyclic group generated by

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Since we assumed that G was nilpotent, we have from part (3) of [Theorem 4.3](#) every element in G must commute with A . Let

$$B = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

be an arbitrary element of G . Next we compute

$$AB = \begin{pmatrix} a & b+d \\ 0 & d \end{pmatrix} \quad \text{and} \quad BA = \begin{pmatrix} a & a+b \\ 0 & d \end{pmatrix}.$$

From this we get that the only way that $AB = BA$ is if $a = d$. This implies that every element of G must have square determinant, and $\det(G) = (\mathbb{Z}/p\mathbb{Z})^\times$ now forces $p = 2$ and

$$G = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}),$$

which is abelian.

We now consider case (1) of [Proposition 2.1](#). In this case, G is contained in a Cartan subgroup and is hence abelian.

In case (2) of [Proposition 2.1](#), the projective image is dihedral and by [Example 4.6](#), a dihedral group is nilpotent if and only if its order is a power of 2.

In case (3) of [Proposition 2.1](#) the projective image is isomorphic to A_4 , S_4 or A_5 . If G were nilpotent this would imply that one of A_4 , S_4 or A_5 is nilpotent. [Proposition 4.5](#) shows this cannot happen, since all three have trivial center. \square

4.3. Modular curves associated to split Cartan subgroups. We now survey, and will soon apply, what is known about the modular curves associated to split Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. We let $C_s^+(p)$ be the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and $X_s^+(p)$ the corresponding modular curve.

The work of Bilu, Parent, and Rebolledo in [\[3\]](#) gives an almost complete picture of rational points on $X_s^+(p)$. This work together with the work of Balakrishnan, Dogra, Müller, Tuitman and Vonk in [\[1\]](#) gives, among other things, the following theorem.

Theorem 4.10 [\[1; 3\]](#). *If $p \geq 11$ is a prime, then the \mathbb{Q} -rational points on $X_s^+(p)$ are cusps or correspond to elliptic curves with complex multiplication.*

Using this result we prove the following.

Proposition 4.11. *Let E/\mathbb{Q} be an elliptic curve without complex multiplication and let p be a prime such that $\mathrm{Im} \bar{\rho}_{E,p}$ is contained in $C_s^+(p)$. If $\mathbb{Q}(E[p])/\mathbb{Q}$ is a nilpotent extension, then $p \in \{2, 3, 5\}$.*

Proof. By [Theorem 4.10](#), it suffices to rule out the case that $p = 7$. When $p = 7$, the projective image of $C_s^+(p)$ has size $2(7 - 1) = 12$ and so is not nilpotent. As shown in [\[34\]](#), there are three maximal admissible subgroups of $C_s^+(7)$, and for each of these, the corresponding modular curve has genus 1. For two of these, there are no non-CM points, while for the third of these, there is a non-CM point with $j = 3^3 \cdot 5 \cdot 7^5 / 2^7$. An elliptic curve with this j -invariant has mod 7 image isomorphic to either $\mathbb{Z}/6\mathbb{Z} \times S_3$ or $\mathbb{Z}/3\mathbb{Z} \times S_3$ and neither of these groups is nilpotent. \square

4.4. Modular curves associated to nonsplit Cartan subgroups. In this section, we survey what is known about the modular curves associated to nonsplit Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. To start, we will let p be an odd prime and we define

the nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ to be

$$C_{ns}(p) := \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z}/p\mathbb{Z} \text{ and } (a, b) \neq (0, 0) \right\},$$

where ϵ is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. The normalizer of this group in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is

$$C_{ns}^+(p) := \langle C_{ns}(p), \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rangle.$$

We will denote the modular curves corresponding to these groups by $X_{ns}(p)$ and $X_{ns}^+(p)$ respectively.

Much less is known about the rational points on the modular curves associated with the normalizers of the nonsplit Cartan subgroups compared to what is known about the split Cartan cases. These modular curves have some arithmetic properties that make analysis of their rational points particularly challenging. In particular, the Jacobians of these modular curves always have analytic rank at least as big as the genus of the curve. This rules out the traditional method of Chabauty and Coleman and requires more advanced techniques (which have been successful in two cases: see [1] and [2]). Fortunately for us, enough is known that we will be able to say quite a bit about the situation unconditionally, and the remainder of what we need is covered by [Conjecture 1.8](#).

We state some of the relevant theorems for these modular curves.

Proposition 4.12. *Let E/\mathbb{Q} be an elliptic curve that does not have complex multiplication and let $p \geq 7$ be a prime such that $\mathrm{Im} \bar{\rho}_{E,p}$ is contained in $C_{ns}^+(p)$. Then $\mathrm{Im} \bar{\rho}_{E,p} = C_{ns}^+(p)$.*

Proof. In [45] the stated result is proven for $p = 7$ (Theorem 1.5) and $p = 11$ (Theorem 1.6). For $p = 13$, [1] shows that there are no non-CM elliptic curves for which $\mathrm{Im} \bar{\rho}_{E,p}$ is contained in $C_{ns}^+(p)$. The cases that $p \geq 17$ are handled by combining Proposition 1.13 of [45] with Theorem 1.6 of [14]. \square

From this we can see that if E/\mathbb{Q} is an elliptic curve and $p \geq 7$ is a prime such that $\mathrm{Im} \bar{\rho}_{E,p}$ is conjugate to a subgroup of $C_{ns}^+(p)$, then $\mathrm{Im} \bar{\rho}_{E,p} = C_{ns}^+(p)$ and the image of $\bar{\rho}_{E,p}$ in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is a dihedral group with order

$$\frac{|C_{ns}^+(p)|}{p-1} = \frac{2(p^2-1)}{p-1} = 2(p+1).$$

Combining this with [Example 4.6](#) and [Remark 4.8](#), we get that in this case $\mathrm{Im} \bar{\rho}_{E,p}$ is nilpotent exactly when $2(p+1)$ is a power of 2 which can happen only when $p+1$ is a power of 2 or p is a Mersenne prime.

We summarize the discussion up to this point in the following proposition.

Proposition 4.13. *Let E/\mathbb{Q} be an elliptic curve without complex multiplication and let p be a prime such that $\mathrm{Im} \bar{\rho}_{E,p}$ is conjugate to a subgroup of $C_{ns}^+(p)$ and $\mathbb{Q}(E[p])/\mathbb{Q}$ is a nilpotent extension. Then p is a Mersenne prime.*

This will be as much as we can say unconditionally. What we really need here is something like [Theorem 4.10](#), but for $X_{ns}^+(p)$. This is exactly why we need [Conjecture 1.8](#).

Proposition 4.14. *Let E/\mathbb{Q} be an elliptic curve without complex multiplication and let p be a Mersenne prime. Assuming [Conjecture 1.8](#), if $\text{Im } \bar{\rho}_{E,p}$ is conjugate to a subgroup of $C_{ns}^+(p)$, then $p = 3$ or $p = 7$.*

Before moving on to the case where E/\mathbb{Q} has complex multiplication, we state a proposition summarizing this section.

Proposition 4.15. *Let E/\mathbb{Q} be an elliptic curve without complex multiplication and let p be a prime such that $\mathbb{Q}(E[p])/\mathbb{Q}$ is a nilpotent extension. Then [Conjecture 1.8](#) implies that $p \in \{2, 3, 5, 7\}$.*

In [Table 2](#) we give models for all modular curves of prime level $p \in \{2, 3, 5, 7\}$ for which $\mathbb{Q}(E[p])/\mathbb{Q}$ is nilpotent. These modular curves are isomorphic to \mathbb{P}^1 and hence there are infinitely many rational j -invariants of elliptic curves E/\mathbb{Q} for which $\mathbb{Q}(E[p])/\mathbb{Q}$ is nilpotent.

4.5. The case of complex multiplication. One of the interesting properties of elliptic curves with complex multiplication is that their mod p representations almost always have their images in the normalizer of a Cartan subgroup. [Proposition 1.14\(i\)](#) and [\(ii\)](#) of [\[45\]](#) state the following.

Proposition 4.16. *Let E/\mathbb{Q} be an elliptic curve with complex multiplication by an order $\mathcal{O} \neq \mathbb{Z}[\zeta_3]$ of a quadratic imaginary field K . Next, let $p \geq 3$ be a prime such that $p \nmid \text{disc}(\mathcal{O})$. Then, $\text{Im } \bar{\rho}_{E,p}$ is conjugate to*

$$\begin{cases} C_s^+(p) & \text{if } p\mathcal{O}_K \text{ splits in } \mathcal{O}_K, \\ C_{ns}^+(p) & \text{if } p\mathcal{O}_K \text{ is inert in } \mathcal{O}_K. \end{cases}$$

The point of this proposition is that in these cases the mod p images is as large as possible. This is useful because we know that in these cases the image of $\text{Im } \bar{\rho}_{E,p}$ of in $\text{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is dihedral by [Proposition 2.1](#) and has easily computable size. [Remark 4.8](#) and [Example 4.6](#) now imply that $\text{Im } \bar{\rho}_{E,p}$ is nilpotent exactly when its image in $\text{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is a 2-group.

Since $|C_s^+(p)| = 2(p-1)^2$ while $|C_{ns}^+(p)| = 2(p^2-1)$, we have that $\text{Im } \bar{\rho}_{E,p}$ is nilpotent if it equals $C_s^+(p)$ and p is a Fermat prime, or if it equals $C_{ns}^+(p)$ and p is a Mersenne prime.

The next result summarizes the situation and handles the cases that $p \mid \text{disc}(\mathcal{O})$.

Proposition 4.17. *Let E/\mathbb{Q} be an elliptic curve with complex multiplication by $\mathcal{O} \neq \mathbb{Z}[\zeta_3]$ and p an odd prime. Then, $\mathbb{Q}(E[p])/\mathbb{Q}$ is nilpotent if and only if either p splits in \mathcal{O} and p is a Fermat prime or p is inert in \mathcal{O} and p is a Mersenne prime.*

Proof. The discussion preceding this theorem covers the case where $p \nmid \text{disc}(\mathcal{O})$. To handle the case where $p \mid \text{disc}(\mathcal{O})$, we refer to [45, Theorem 1.14] which shows that in this case $\text{Im } \bar{\rho}_{E,p}$ is isomorphic to one of the following groups:

$$\begin{aligned} G &:= \left\{ \begin{pmatrix} a & b \\ 0 & \pm a \end{pmatrix} : a \in (\mathbb{Z}/p\mathbb{Z})^\times, b \in \mathbb{Z}/p\mathbb{Z} \right\}, \\ H_1 &:= \left\{ \begin{pmatrix} a & b \\ 0 & \pm a \end{pmatrix} : a \in ((\mathbb{Z}/p\mathbb{Z})^\times)^2, b \in \mathbb{Z}/p\mathbb{Z} \right\}, \text{ or} \\ H_2 &:= \left\{ \begin{pmatrix} \pm a & b \\ 0 & a \end{pmatrix} : a \in ((\mathbb{Z}/p\mathbb{Z})^\times)^2, b \in \mathbb{Z}/p\mathbb{Z} \right\}. \end{aligned}$$

In all three cases, the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is in $\text{Im } \bar{\rho}_{E,p}$ and so $\text{Im } \bar{\rho}_{E,p}$ is not nilpotent by Proposition 4.9. \square

4.5.1. *The case when E has complex multiplication by $\mathbb{Z}[\zeta_3]$.* If E/\mathbb{Q} has complex multiplication by $\mathcal{O} = \mathbb{Z}[\zeta_3]$ we know that $j(E) = 0$. Given such an elliptic curve, we know that there is always a $d \in \mathbb{Q}^\times$ such that E is isomorphic to the curve

$$E_d : y^2 = x^3 + d.$$

The images of the mod p representations of E depend on the value of d modulo 6th powers. This relationship is explicitly classified in [45, Propositions 1.15 and 1.16]. We summarize the relevant parts of those propositions here for the convenience of the reader.

Theorem 4.18 [45, Propositions 1.15 and 1.16]. *Let E/\mathbb{Q} be an elliptic curve with complex multiplication by $\mathbb{Z}[\zeta_3]$. Then the curve E can be given by a Weierstrass equation of the form*

$$y^2 = x^3 + d$$

for some $d \in \mathbb{Q}^\times$.

- (1) *If d is a cube, then $\text{Im } \bar{\rho}_{E,2} = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$. Otherwise, $\text{Im } \bar{\rho}_{E,2} = \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$.*
- (2) *If $4d$ is not a cube, then $\text{Im } \bar{\rho}_{E,3}$ is conjugate to*

$$\begin{aligned} &\left\{ \begin{pmatrix} \pm 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{Z}/3\mathbb{Z} \text{ and } b \in (\mathbb{Z}/3\mathbb{Z})^\times \right\} \text{ if neither } d \text{ nor } -3d \text{ is a square,} \\ &\left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in (\mathbb{Z}/3\mathbb{Z})^\times \text{ and } b \in \mathbb{Z}/3\mathbb{Z} \right\} \text{ if } d \text{ is a square,} \\ &\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbb{Z}/3\mathbb{Z})^\times \text{ and } b \in \mathbb{Z}/3\mathbb{Z} \right\} \text{ if } 3d \text{ is a square.} \end{aligned}$$

On the other hand, if $4d$ is a cube, then $\text{Im } \bar{\rho}_{E,3}$ is conjugate to

$$\begin{aligned} &\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in (\mathbb{Z}/3\mathbb{Z})^\times \right\} \text{ if neither } d \text{ nor } -3d \text{ is a square,} \\ &\left\{ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} : b \in (\mathbb{Z}/3\mathbb{Z})^\times \right\} \text{ if either } d \text{ or } -3d \text{ is a square.} \end{aligned}$$

- (3) *If $p \equiv 1 \pmod{9}$, then $\text{Im } \bar{\rho}_{E,p}$ is conjugate to $C_s^+(p)$.*
- (4) *If $p \equiv 8 \pmod{9}$, then $\text{Im } \bar{\rho}_{E,p}$ is conjugate to $C_{ns}^+(p)$.*

- (5) Suppose that $p \equiv 4$ or $7 \pmod{9}$ and $e \in \{1, 2\}$ such that $e \equiv \frac{1}{3}(p-1) \pmod{3}$. If $d \not\equiv 16p^e \pmod{(\mathbb{Q}^\times)^3}$, then $\text{Im } \bar{\rho}_{E,p}$ is conjugate to $C_s^+(p)$. If $d \equiv 16p^e \pmod{(\mathbb{Q}^\times)^3}$, then $\text{Im } \bar{\rho}_{E,p}$ is conjugate in $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ to the subgroup of $C_s^+(p)$ consisting of matrices of the form $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ and $\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$, with $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that a/b is a cube.
- (6) Suppose that $p \equiv 2$ or $5 \pmod{9}$ and let $e \in \{1, 2\}$ such that $-e \equiv \frac{1}{3}(p+1) \pmod{3}$. If $d \not\equiv 16p^e \pmod{(\mathbb{Q}^\times)^3}$, then $\text{Im } \bar{\rho}_{E,p}$ is conjugate to $C_{ns}^+(p)$. If $d \equiv 16p^e \pmod{(\mathbb{Q}^\times)^3}$, then $\text{Im } \bar{\rho}_{E,p}$ is conjugate in $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ to the subgroup generated by the unique index 3 subgroup of $C_{ns}(p)$ and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

The take-away from this theorem is that for $E_d : y^2 = x^3 + d$, whether or not $\text{Im } \bar{\rho}_{E,p}$ is nilpotent is completely controlled by $d \pmod{(\mathbb{Q}^\times)^3}$.

For example, condition (1) tells us that $\mathbb{Q}(E_d[2])/\mathbb{Q}$ is a nilpotent extension exactly when d is a cube. Similarly, condition (2) says that $\mathbb{Q}(E_d[3])/\mathbb{Q}$ is nilpotent when $4d$ is a cube.

We note that there are no Fermat primes $\equiv 1 \pmod{9}$. By [Remark 4.8](#), $\text{Im } \bar{\rho}_{E,p}$ is nilpotent if and only if its image in $\text{PGL}_2(\mathbb{F}_p)$, namely a dihedral group of order $2(p-1)$, is nilpotent. By [Example 4.6](#) this cannot occur since $2(p-1)$ is not a power of 2.

Thus if $p \equiv 1 \pmod{9}$ the image of $\bar{\rho}_{E,p}$ in $\text{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is nilpotent if and only if $2(p-1)$ is a power of two and so condition (3) never yields a nilpotent $\mathbb{Q}(E[p])/\mathbb{Q}$. Likewise, there are no Mersenne primes $p \equiv 8 \pmod{9}$.

The last cases that we have to deal with are the special cases that arise in cases (5) and (6) of [Theorem 4.18](#). In cases (5) and (6) respectively, the image of $\bar{\rho}_{E,p}$ is contained in an index 3 subgroup of $C_s^+(p)$ and $C_{ns}^+(p)$ respectively. If we are in condition (5), then image of $\text{Im } \bar{\rho}_{E,p}$ inside of $\text{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is a dihedral group of size $\frac{2}{3}(p-1)$, while in condition (6) the image of $\text{Im } \bar{\rho}_{E,p}$ inside of $\text{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is a dihedral group of size $\frac{2}{3}(p+1)$. This along with our previous analysis gives the following proposition.

Proposition 4.19. *Let $E_d : y^2 = x^3 + d$ and let p be a prime. Then $\mathbb{Q}(E_d[p])/\mathbb{Q}$ is nilpotent if and only if*

$$\begin{aligned} d &\equiv 1 \pmod{(\mathbb{Q}^\times)^3} && \text{if } p = 2, \\ d &\equiv 2 \pmod{(\mathbb{Q}^\times)^3} && \text{if } p = 3, \\ d &\equiv 2 \cdot p^{\frac{1}{3}(p-1)} \pmod{(\mathbb{Q}^\times)^3} && \text{if } p = 3 \cdot 2^k + 1 \text{ for some } k \geq 1, \\ d &\equiv 2 \cdot p^{\frac{1}{3}(p+1)} \pmod{(\mathbb{Q}^\times)^3} && \text{if } p = 3 \cdot 2^k - 1 \text{ for some } k \geq 1. \end{aligned}$$

Example 4.20. Let E be the elliptic curve given by

$$y^2 = x^3 + 16 \cdot 97^2.$$

We check in the LMFDB that the image of $\bar{\rho}_{E,97}$ is conjugate to the group with RSZB label 97.14259.1103.1. One can check directly that this group is nilpotent and so $\mathbb{Q}(E[97])/\mathbb{Q}$ is nilpotent.

Remark 4.21. If E is an elliptic curve with complex multiplication by $\mathcal{O} = \mathbb{Z}[\zeta_3]$, then Proposition 4.19 shows that $\mathbb{Q}(E[p])/\mathbb{Q}$ is nilpotent for at most one prime p .

Proof of Corollary 1.10. If E/\mathbb{Q} is an elliptic curve for which $\mathbb{Q}(E[19])/\mathbb{Q}$ is nilpotent then by Proposition 4.9, $\text{Im } \bar{\rho}_{E,p}$ is contained in the normalizer of a split or nonsplit Cartan subgroup. If E is non-CM, the split Cartan case cannot occur by Proposition 4.11 and the nonsplit Cartan case cannot occur by Proposition 4.13. If E has CM by an order \mathcal{O} , then Proposition 4.17 forces $\mathcal{O} = \mathbb{Z}[\zeta_3]$. However, by Proposition 4.19 only cases where $p = 3 \cdot 2^k \pm 1$ can occur and 19 does not have this form.

Proposition 4.19 allows us to construct elliptic curves $E_d : y^2 = x^3 + d$ for which $\mathbb{Q}(E_d[p])/\mathbb{Q}$ is nilpotent for $p = 2$, $p = 3$, $p = 5 = 3 \cdot 2 - 1$, $p = 7 = 3 \cdot 2 + 1$, $p = 11 = 3 \cdot 2^2 - 1$ and $p = 13 = 3 \cdot 2^2 + 1$. The prime $p = 17$ is a Fermat prime which splits in $\mathbb{Z}[i]$ and so if $E : y^2 = x^3 - x$, then $\mathbb{Q}(E[17])/\mathbb{Q}$ is nilpotent by Proposition 4.17. \square

5. Nilpotent groups of prime-power level

Suppose that p is a prime and that E/\mathbb{Q} is an elliptic curve such that $\mathbb{Q}(E[p^k])/\mathbb{Q}$ is a nilpotent extension for some $k \geq 2$. The first observation we make is that since nilpotency is closed under quotients, Proposition 4.4, we know that $\mathbb{Q}(E[p^i])/\mathbb{Q}$ is a nilpotent extension for all $1 \leq i \leq k$, in particular, and this would mean $\mathbb{Q}(E[p])/\mathbb{Q}$ is a nilpotent extension. As usual, we will have to handle the case when $p = 2$ separately, but thanks to Proposition 4.9, when p is odd, we only have to deal with the case that $\text{Im } \bar{\rho}_{E,p}$ is contained in either the normalizer of a split or nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

5.1. The case when $p = 2$. In this case there are exactly two ways that $\mathbb{Q}(E[2])/\mathbb{Q}$ can be nilpotent. In order for $\mathbb{Q}(E[2])/\mathbb{Q}$ to be nilpotent, either E can have a square discriminant or E can have a point of order 2 defined over \mathbb{Q} .

We start this case by considering what the image of $\bar{\rho}_{E,4}$ could be if we know that E has square discriminant and

$$\text{Im } \bar{\rho}_{E,2} \subseteq \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

Let $\pi_2 : \text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \rightarrow \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$ be the standard component-wise reduction map and let

$$G_2 = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \quad \text{and} \quad G_4 := \pi_2^{-1}(G_2).$$

The next step is to search for admissible nilpotent subgroups of G_4 up to conjugation with the additional property that their image mod 2 is exactly equal to G_2 . Such a subgroup must have order which is a multiple of 6 (a factor of 3 coming from the image in G_2 and a factor of 2 coming from the determinant being surjective). There are two such groups up to conjugacy: one with order 6 and one with order 12, with the former contained in the latter. Neither of these groups are admissible. Computing conjugacy classes of the order 12 subgroup shows that there are three conjugacy classes of elements of order 2 and none of these elements fix an element of $(\mathbb{Z}/4\mathbb{Z})^2$ of order 4, which the image of complex conjugation under $\bar{\rho}_{E,4}$ must. (Code for this calculation can be found in the file subsec51.m at [8].) Thus in the case when $\text{Im } \bar{\rho}_{E,2}$ is conjugate to G_2 , there is no way that $\mathbb{Q}(E[4])/\mathbb{Q}$ can be a nilpotent extension.

The next case is when E/\mathbb{Q} has a point of order 2 defined over \mathbb{Q} . In this case, $\mathbb{Q}(E[2])/\mathbb{Q}$ is either a quadratic extension or trivial. Letting $\pi_2 : \text{GL}_2(\mathbb{Z}/2^k\mathbb{Z}) \rightarrow \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$, we have $|\text{Ker}(\pi_2)| = 2^{4(k-1)}$. From this we have

$$|\pi_2^{-1}(G_2)| = 2^{4(k-1)}|G_2|$$

and in particular $\pi_2^{-1}(G_2)$ is a 2-group. From [Theorem 4.3](#), we know that $\pi_2^{-1}(G_2)$ is *always* nilpotent. The upshot of this is that if E/\mathbb{Q} is an elliptic curve with a point of order two defined over \mathbb{Q} , then for every $k \geq 1$, $\mathbb{Q}(E[2^k])/\mathbb{Q}$ is a nilpotent extension.

Proposition 5.1. *Let E/\mathbb{Q} be an elliptic curve such that $\mathbb{Q}(E[2])/\mathbb{Q}$ is a nilpotent extension. Then, either the discriminant of E is a square, in which case $\mathbb{Q}(E[2^k])/\mathbb{Q}$ is not nilpotent for any $k \geq 2$, or E has a rational point of order 2, in which case $\mathbb{Q}(E[2^k])/\mathbb{Q}$ is nilpotent for all $k \geq 1$.*

5.2. The case when p is odd.

Proposition 5.2. *Suppose that G is a nilpotent subgroup of $\text{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ and let $\pi : G \rightarrow \text{GL}_2(\mathbb{F}_p)$ be the reduction mod p map. Assume that $p \nmid |\pi(G)|$. Then at least one of the following is true:*

- (1) G is abelian.
- (2) $\text{Ker}(\pi) \subseteq \{\alpha I : \alpha \in (\mathbb{Z}/p^2\mathbb{Z})^\times \text{ with } \alpha \equiv 1 \pmod{p}\}$.

Proof. Let P be a Sylow p -subgroup of G . Since $|\pi(G)|$ has order coprime to p , we have $\pi(P) = \{1\}$. In particular, P is contained in the set of matrices $\equiv I \pmod{p}$. The set of matrices $\equiv I \pmod{p}$ is an abelian subgroup of $\text{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ order p^4 . In particular P is abelian and $\text{Ker } \pi = P$. Let

$$H = \prod_{\substack{Q \in \text{Syl}_q(G) \\ q \neq p}} Q$$

be a complement of P in G . Note that $\pi(G) = \pi(PH) = \pi(P)\pi(H) = \{1\} \cdot \pi(H) = \pi(H)$ and also $H \cap \text{Ker } \pi \subseteq H \cap P = \{1\}$. Thus $\pi : H \rightarrow \pi(G)$ is an isomorphism.

Case I: There exists an element of P that is not a scalar multiple of the identity.

This implies that there is some $X \in M_2(\mathbb{F}_p)$ so that $I + pX \in P$ and X is not a scalar multiple of the identity. If $Y \in \pi(G)$, there is some $\tilde{Y} \in H$ so that $\pi(\tilde{Y}) = Y$. The assumption that G is nilpotent implies that $(I + pX)$ must commute with \tilde{Y} , and this implies that $XY = YX$ in $M_2(\mathbb{F}_p)$. The assumption on X implies that X is a *cyclic matrix*. This is a matrix X whose minimal polynomial and characteristic polynomial are the same.

Corollary 4.4.18 of [17] implies that for every cyclic matrix X , its centralizer in $M_2(\mathbb{F}_p)$ is equal to $\mathbb{F}_p[X]$, the set of all polynomials in X with coefficients in \mathbb{F}_p . This is a commutative subring of $M_2(\mathbb{F}_p)$, and this implies that $\pi(G) \subseteq \mathbb{F}_p[X]^\times$ is abelian. Since $H \simeq \pi(G)$, it follows that H is abelian. Since $G \simeq P \times H$, it follows that G is abelian.

Case II: Every element of P is a scalar multiple of the identity.

Since $P = \text{Ker } \pi$, in this case, condition (2) is clearly true. □

As a consequence of this result, we can establish the following result.

Proposition 5.3. *Let E/\mathbb{Q} be an elliptic curve and let p be an odd prime. Then $\mathbb{Q}(E[p^2])/\mathbb{Q}$ is not a nilpotent extension.*

Proof. Assume that E/\mathbb{Q} is an elliptic curve, p is an odd prime, and $\mathbb{Q}(E[p^2])/\mathbb{Q}$ is nilpotent. Let $G = \text{Im } \bar{\rho}_{E,p^2}$. If we are in case (1) of Proposition 5.2, then $\mathbb{Q}(E[p^2])/\mathbb{Q}$ is abelian, which contradicts the main result of [16]. If we are in case (2) of Proposition 5.2 and $\pi : G \rightarrow \text{GL}_2(\mathbb{F}_p)$ is the reduction mod p map, then $\text{Ker}(\pi) \cap (G \cap \text{SL}_2(\mathbb{Z}/p^2\mathbb{Z})) = 1$ and this implies that we have a near coincidence of level (p^2, p) . By Proposition 3.11, we must have that $p = 3$ and E corresponds to a rational point on the curve with RSZB label 9.27.0.1. However, the main result of [34] implies that for such an elliptic curve, the mod 9 image of Galois must equal 9.27.0.1, which is not nilpotent. □

As a consequence, if E/\mathbb{Q} is an elliptic curve, p is an odd prime, and $n \geq 2$, $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is not a nilpotent extension.

6. Nilpotent groups of composite level

In this section, we will complete the proof of Theorem 1.9. Since $\mathbb{Q}(E[n])$ is the composite of $\mathbb{Q}(E[p^k])$ for every prime power factor p^k of n , the extension $\mathbb{Q}(E[n])/\mathbb{Q}$ is nilpotent if and only if every $\mathbb{Q}(E[p^k])/\mathbb{Q}$ is nilpotent. From Section 5, this only occurs if $k = 1$, or $p = 2$ and E has a rational point of order 2.

First, we consider the case that E/\mathbb{Q} is an elliptic curve with complex multiplication. From Section 4, we have a classification of when $\mathbb{Q}(E[p])/\mathbb{Q}$ is nilpotent based on the mod p image of Galois for E , which is determined by whether p splits, is inert, or ramifies in the CM field. From Section 5, $\mathbb{Q}(E[p^k])/\mathbb{Q}$ is nilpotent for $k \geq 2$ if and only if $p = 2$ and E has a rational point of order 2. From these results, the complex multiplication cases of Theorem 1.9 follow.

Next we consider the case that E/\mathbb{Q} is an elliptic curve without complex multiplication under the assumption of Conjecture 1.8. In this case, Section 4 implies that if $\mathbb{Q}(E[p])/\mathbb{Q}$ is nilpotent then either $p \in \{2, 5\}$ or p is a Mersenne prime and $\text{Im } \bar{\rho}_{E,p}$ is contained in the normalizer of the nonsplit Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$, which entails that $p \in \{2, 3, 5, 7\}$. All that remains is for us to determine which combinations of the possible nilpotent mod p images can occur simultaneously. Given possible mod p and mod q images of Galois G and H , we construct the fiber product $X_G \times_{X_0(1)} X_H$. This is the curve given by $\pi_G(x) = \pi_H(y)$. The results of this computation are listed in Table 1.

The curves of genus 1 or 2 with rank zero can be handled using standard techniques. The rank-0 genus-3 curve was shown in [31] to have no noncuspidal rational points corresponding to elliptic curves without complex multiplication. This leaves us with one remaining curve, with label 35.315.19.1. Theorem A.7 of [34] shows that if X_H is a modular curve of level N , every simple factor of the Jacobian of X_H is isogenous to a simple factor of $J_1(N^2)$, and Section 6 of [34] explains how this information can be used to determine the decomposition of the Jacobian of X_H . This decomposition is recorded in the beta version of the LMFDB at <http://beta.lmfdb.org/ModularCurve/Q/35.315.19.a.1>. In particular, X_H factors up to isogeny as the product of nine \mathbb{Q} -simple abelian varieties (of dimensions 2, 3 and 4).

(p, q)	$\text{Im } \bar{\rho}_{E,p}$	$\text{Im } \bar{\rho}_{E,q}$	$\text{Im } \bar{\rho}_{E,pq}$	has noncuspidal rational points?
(2,3)	2.2.0.1	3.3.0.1	6.6.1.1	no – genus 1, rank 0
	2.3.0.1	3.3.0.1	6.9.0.1	yes
(2,5)	2.2.0.1	5.15.0.1	10.30.2.2	no – genus 2, rank 0
	2.3.0.1	5.15.0.1	10.45.1.1	no – genus 1, rank 0
(2,7)	2.2.0.1	7.21.0.1	14.42.3.1	no – genus 3, rank 0
	2.3.0.1	7.21.0.1	14.63.2.1	no – genus 2, rank 0
(3,5)	3.3.0.1	5.15.0.1	15.45.1.1	yes
(3,7)	3.3.0.1	7.21.0.1	21.63.1.1	yes
(5,7)	5.15.0.1	7.21.0.1	35.315.19.1	no – genus 19, analytic rank 15

Table 1. Potential composite level nilpotent images.

Work of Kolyvagin and Logachev [21] shows that if a simple abelian variety A of GL_2 -type has analytic rank 0 it must have rank 0, while if it has analytic rank r equal to its dimension, then it must also have algebraic rank r . (This latter result is not stated by Kolyvagin and Logachev, but their ideas suffice to prove it. For more detail about how this follows, see [10, Section 7].) This hypothesis is easy to verify since $L(A, s)$ factors as a product of $\dim A$ modular L -functions. From this, it follows that the analytic and algebraic rank of the Jacobian of 35.315.19.1 are both 15. In theory, this curve could be attacked using the method of Chabauty and Coleman since the genus higher than the rank, but computing on a curve of genus 19 is rather unwieldy. However, the techniques of Lemos [25] apply to this situation:

Theorem 6.1 (Lemos [25, Theorem 1.4]). *Let E/\mathbb{Q} be an elliptic curve without complex multiplication. Suppose that there exists a prime q for which $\mathrm{Im} \bar{\rho}_{E,q}$ is contained in a subgroup of $C_s^+(q)$. Then $\bar{\rho}_{E,p}$ is surjective for all $p > 37$.*

The work in [25] does not, however, require full strength of the assumption that $p > 37$. We wish to explain why that work implies the following result.

Theorem 6.2. *Let E/\mathbb{Q} be an elliptic curve without complex multiplication. Suppose that there exist a prime q for which $\mathrm{Im} \bar{\rho}_{E,q}$ is contained in a subgroup of $C_s^+(q)$. Then $\bar{\rho}_{E,p}$ is not contained in $C_{ns}^+(p)$ for any $p > 3$ with $p \neq q$.*

Setting $p = 7$ and $q = 5$ above implies that the only rational points on the modular curve 35.315.19.1 are cusps or CM points.

Proof of Theorem 6.2. As this result is really contained in [25] we will give an overview of the steps in Lemos's argument highlighting the necessary hypotheses on p and q . First, Theorem 4.10 implies that $q \in \{2, 3, 5, 7\}$. As a consequence, $X_0(q)$ has genus zero.

The modular curve $X_s(q)$ parametrizes elliptic curves with two independent cyclic q -isogenies. In Lemma 3.4 of [25], Lemos shows that there is an isomorphism

$$\theta : X_s(q) \times_{X_0(1)} X_{ns}^+(p) \rightarrow X_0(q^2) \times_{X_0(1)} X_{ns}^+(p)$$

and that θ commutes with natural involutions on the source and the target. (The involution on the source interchanges the kernels of the two isogenies, and the involution on the target is the Atkin–Lehner involution w_{q^2} .) Lemos then defines a map $g : X_0(q^2) \times_{X_0(1)} X_{ns}^+(p) \rightarrow J(X_0(q) \times_{X_0(1)} X_{ns}^+(p))$ by taking a point P and mapping it to the difference of its images under the two different degeneracy maps (coming from the two covers $X_0(q^2) \rightarrow X_0(q)$).

Work of Darmon and Merel [9, Proposition 7.1] shows that there is a projection $\pi : J(X_0(q) \times_{X_0(1)} X_{ns}^+(p)) \rightarrow A$ to a positive-dimensional abelian variety with rank 0 for which the kernel of π is connected and is stable under the action of

Hecke operators. (For their application, Darmon and Merel only need this for $q = 2$ or $q = 3$, but as they indicate, this part of the argument applies to any q with $p \nmid q$.)

Define $h = \pi \circ g$ and let \mathcal{O} be the ring of integers in $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $R = \mathcal{O}[1/(2qp)]$. Roughly speaking, Proposition 3.6 of [25] shows that h is a formal immersion at ∞ for every prime ideal \mathfrak{p} of R . The proof of this proposition is standard and the key assumption is that $X_0(q)$ has genus 0. It follows from this that $\theta \circ h : X_s(q) \times_{X_0(1)} X_{ns}^+(p) \rightarrow A$ is a formal immersion at ∞ for every prime ideal \mathfrak{p} of R .

Now, if P is a rational point on $X_s(q) \times_{X_0(1)} X_{ns}^+(p)$ corresponding to an elliptic curve E which has potential multiplicative reduction at some prime $\ell \notin \{2, p, q\}$, then it meets one of the cusps at the fiber at ℓ . Without loss of generality this cusp can be chosen to be infinity and this implies that $\theta \circ h(P) = Q \in A(\mathbb{Q})$ reduces to zero in $\tilde{A}(\mathbb{F}_\ell)$. (Here \tilde{A} is the special fiber of the Néron model of A over \mathbb{Z}_ℓ .) This implies that $Q = 0$ and the fact that $\theta \circ h$ is a formal immersion and $\ell > 2$ implies that $P = \infty$. (One way to make this conclusion is using Proposition 2.4 of [22].)

It follows from this that if E/\mathbb{Q} is an elliptic curve with mod p image contained in $C_{ns}^+(p)$ and mod q image contained in $C_s^+(q)$, then E cannot have potentially multiplicative reduction at any prime $\ell \notin \{2, p, q\}$. The primes of potentially multiplicative reduction are precisely those that divide the denominator of $j(E)$. As a consequence $j(E) \in \mathbb{Z}[1/(2pq)]$. More is true however. Lemos notes in [25, Proposition 3.3] that the assumption that the mod p image of Galois is contained in $C_{ns}^+(p)$ implies that E has potentially supersingular reduction at p , and that if E has potentially multiplicative reduction at $\ell \neq p$, then $\ell \equiv \pm 1 \pmod{p}$. (These same observations were made earlier by Zywna.) It follows that the only primes that can divide the denominator of $j(E)$ are those that are $\equiv \pm 1 \pmod{p}$. Since $p > 3$, none of 2, 3, 5 or 7 (the only options for q) can be $\equiv \pm 1 \pmod{p}$. It follows that $j(E) \in \mathbb{Z}$.

Lemos proceeds to show using an explicit isomorphism $X_s^+(q) \simeq \mathbb{P}^1$ that there are only finite integral j -invariants of elliptic curves E/\mathbb{Q} with mod q image of Galois contained in $C_s^+(q)$. For $q \in \{3, 5, 7\}$ these are explicitly listed on [25, p. 749]. They all have CM except for $j = -5000$ ($q = 5$) and $j = -1728$ ($q = 3$). For elliptic curves with these j -invariants, the image of $\rho_{E,p}$ is not contained in the normalizer of a nonsplit Cartan subgroup for any $p > 3$. The case of $q = 2$ was previously handled in [24, p. 142]. Here there are 25 integral j -invariants of elliptic curves E with image in $C_s^+(2)$ (which is a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$). Of these 25, there are 18 non-CM j -invariants. For elliptic curves with these j -invariants, the LMFDB indicates that the image of $\rho_{E,p}$ is contained in $C_{ns}^+(p)$ for some p only for $p = 3$ and $j \in \{-64, 4913, 238328, 16974593\}$. \square

In Table 2, we give models for the modular curves from Table 1 that have noncuspidal rational points.

Working without the assumption of Conjecture 1.8, we must consider the

G	X_G	$\pi_G : X_G \rightarrow \mathbb{P}_{\mathbb{Q}}^1$
2.2.0.1	\mathbb{P}^1	$f_2(t) = t^2 + 1728$
2.3.0.1	\mathbb{P}^1	$h_2(t) = \frac{(256-t)^3}{(256-t)^3}$
3.3.0.1	\mathbb{P}^1	$f_3(t) = t^3$
5.15.0.1	\mathbb{P}^1	$f_5(t) = \frac{(t+5)^3(t^2-5)^3(t^2+5t+10)^3}{(t+5)^3(t^2-5)^3(t^2+5t+10)^3}$
6.9.0.1	\mathbb{P}^1	$f_6(t) = \frac{(t^3+3t^2+3t-15)^3}{(t^3+3t^2+3t-15)^3}$
7.21.0.1	\mathbb{P}^1	$f_7(t) = \frac{(2t-1)^3(t^2-t+2)^3(2t^2+5t+4)^3(5t^2+2t-4)^3}{(2t-1)^3(t^2-t+2)^3(2t^2+5t+4)^3(5t^2+2t-4)^3}$
15.45.1.1	$y^2+y=x^3+1$	$f_{15}(x, y) = \frac{(y+3)^3(y^2-4y-1)^3(y^2+y+4)^3}{(y+3)^3(y^2-4y-1)^3(y^2+y+4)^3}$
21.63.1.1	$y^2+y=x^3+12$	$f_{21}(x, y) = f_7\left(\frac{x^2+5x-14}{x^2+5x-14}\right)$

Table 2. Models of the modular curves relevant for [Theorem 1.9](#). The models for curves of prime level come from [\[41\]](#). The remaining genus 0 curves can be computed as fiber products of curves of prime level. The models for the genus 1 modular curves of composite level are computed as fiber products of the prime level modular curves also computed in [\[41\]](#).

possibility that there is an elliptic curve E/\mathbb{Q} for which $\text{Im } \bar{\rho}_{E,5}$ is contained in the normalizer of the split Cartan mod 5 and for which $\text{Im } \bar{\rho}_{E,p}$ is contained in the normalizer of a nonsplit Cartan modulo p for some Mersenne prime p . [Theorem 6.2](#) above shows this is only possible for $p = 3$, and the elliptic curves for which this occurs are parametrized by the modular curve with label 15.45.1.1.

In addition, we must consider the possibility that there is an elliptic curve E/\mathbb{Q} for which $\text{im } \bar{\rho}_{E,p}$ is contained in the normalizer of a nonsplit Cartan modulo p for some Mersenne prime p , and which also has a rational point of order 2. This implies the mod 2 image of Galois is contained in a Borel subgroup, which for $p = 2$ is equal to $C_s^+(2)$. The desired result again follows from [Theorem 6.2](#). This concludes the proof of [Theorem 1.9](#).

Acknowledgements

We thank David Zureick-Brown and Álvaro Lozano-Robledo for insightful conversations during the writing of this paper, and we thank Pedro Lemos for helpful

communications about the results in [25]. We also thank the referees whose careful reading has helped improve the clarity and accuracy of the paper.

References

- [1] J. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, “Explicit Chabauty–Kim for the split Cartan modular curve of level 13”, *Ann. of Math.* (2) **189**:3 (2019), 885–944. [MR](#)
- [2] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, “Quadratic Chabauty for modular curves: algorithms and examples”, *Compos. Math.* **159**:6 (2023), 1111–1152. [MR](#)
- [3] Y. Bilu, P. Parent, and M. Rebolledo, “Rational points on $X_0^+(p^r)$ ”, *Ann. Inst. Fourier (Grenoble)* **63**:3 (2013), 957–984. [MR](#)
- [4] W. Bosma, J. Cannon, and C. Playoust, “The Magma algebra system, I: the user language”, *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. [MR](#)
- [5] K. Conrad, “Subgroup series, I”, preprint, <https://kconrad.math.uconn.edu/blurbs/grouptheory/subgpseries1.pdf>.
- [6] K. Conrad, “Subgroup series, II”, preprint, <https://kconrad.math.uconn.edu/blurbs/grouptheory/subgpseries2.pdf>.
- [7] H. B. Daniels and Á. Lozano-Robledo, “Coincidences of division fields”, *Ann. Inst. Fourier (Grenoble)* **73**:1 (2023), 163–202. [MR](#)
- [8] H. Daniels and J. Rouse, “NearCoincidences”, code associated with arXiv:2409.00881 and the present paper, 2024, <https://github.com/HDaniels432/NearCoincidences>.
- [9] H. Darmon and L. Merel, “Winding quotients and some variants of Fermat’s last theorem”, *J. Reine Angew. Math.* **490** (1997), 81–100. [MR](#)
- [10] N. Dogra and S. Le Fourn, “Quadratic Chabauty for modular curves and modular forms of rank one”, *Math. Ann.* **380**:1-2 (2021), 393–448. [MR](#)
- [11] T. Dokchitser and V. Dokchitser, “Surjectivity of mod 2^n representations of elliptic curves”, *Math. Z.* **272**:3-4 (2012), 961–964. [MR](#)
- [12] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed., Wiley, Hoboken, NJ, 2004. [MR](#)
- [13] N. D. Elkies, “Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9”, preprint, 2006. [arXiv 0612734](https://arxiv.org/abs/0612734)
- [14] L. Furio and D. Lombardo, “Serre’s uniformity question and proper subgroups of $C_{n_s}^+(p)$ ”, preprint, 2023. [arXiv 2305.17780](https://arxiv.org/abs/2305.17780)
- [15] C. F. Gauss, *Disquisitiones arithmeticae*, Gerh. Fleischer, Leipzig, 1801.
- [16] E. González-Jiménez and Á. Lozano-Robledo, “Elliptic curves with abelian division fields”, *Math. Z.* **283**:3-4 (2016), 835–859. [MR](#)
- [17] R. A. Horn and C. R. Johnson, *Topics in matrix analysis*, Cambridge University Press, 1991. Corrected reprint, 1994. [MR](#)
- [18] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics **73**, Springer, 1974. [MR](#)
- [19] I. M. Isaacs, *Finite group theory*, Graduate Studies in Mathematics **92**, Amer. Math. Soc., 2008. [MR](#)
- [20] C. Jordan, *Traité des substitutions et des équations algébriques*, 1870. Reprinted Jacques Gabay, Sceaux (France), 1989.
- [21] V. A. Kolyvagin and D. Y. Logachëv, “Finiteness of the Shafarevich–Tate group and the group of rational points for some modular abelian varieties”, *Algebra i Analiz* **1**:5 (1989), 171–196. [MR](#)

- [22] S. Le Fourn, “Surjectivity of Galois representations associated with quadratic \mathbb{Q} -curves”, *Math. Ann.* **365**:1-2 (2016), 173–214. [MR](#)
- [23] S. Le Fourn and P. Lemos, “Residual Galois representations of elliptic curves with image contained in the normaliser of a nonsplit Cartan”, *Algebra Number Theory* **15**:3 (2021), 747–771. [MR](#)
- [24] P. Lemos, “Serre’s uniformity conjecture for elliptic curves with rational cyclic isogenies”, *Trans. Amer. Math. Soc.* **371**:1 (2019), 137–146. [MR](#)
- [25] P. Lemos, “Some cases of Serre’s uniformity problem”, *Math. Z.* **292**:1-2 (2019), 739–762. [MR](#)
- [26] G. Ligozat, “Courbes modulaires de niveau 11”, pp. 149–237 in *Modular functions of one variable* (Bonn, 1976), vol. 5, Lecture Notes in Math. **601**, Springer, 1977. [MR](#)
- [27] “The L-functions and modular forms database”, online resource, 2023, <https://www.lmfdb.org>.
- [28] Á. Lozano-Robledo, “Galois representations attached to elliptic curves with complex multiplication”, *Algebra Number Theory* **16**:4 (2022), 777–837. [MR](#)
- [29] F. Momose, “Rational points on the modular curves $X_0^+(p^r)$ ”, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **33**:3 (1986), 441–466. [MR](#)
- [30] F. Momose and M. Shimura, “Lifting of supersingular points on $X_0(p^r)$ and lower bound of ramification index”, *Nagoya Math. J.* **165** (2002), 159–178. [MR](#)
- [31] J. S. Morrow, “Composite images of Galois for elliptic curves over \mathbb{Q} and entanglement fields”, *Math. Comp.* **88**:319 (2019), 2389–2421. [MR](#)
- [32] J. J. Rotman, *A first course in abstract algebra*, 3rd ed., Prentice Hall, Upper Saddle River, NJ, 2006. [MR](#)
- [33] J. Rouse and D. Zureick-Brown, “Elliptic curves over \mathbb{Q} and 2-adic images of Galois”, *Res. Number Theory* **1** (2015), art. id. 12, 34 pp. [MR](#)
- [34] J. Rouse, A. V. Sutherland, and D. Zureick-Brown, “ ℓ -adic images of Galois for elliptic curves over \mathbb{Q} (and an appendix with John Voight)”, *Forum Math. Sigma* **10** (2022), art. id. e62, 63 pp. [MR](#)
- [35] J.-P. Serre, *Abelian l -adic representations and elliptic curves*, W. A. Benjamin, 1968. [MR](#)
- [36] J.-P. Serre, “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques”, *Invent. Math.* **15**:4 (1972), 259–331. [MR](#)
- [37] J.-P. Serre, “Quelques applications du théorème de densité de Chebotarev”, *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 123–201. [MR](#)
- [38] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994. [MR](#)
- [39] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, 2009. [MR](#)
- [40] H. Smith, “Ramification in division fields and sporadic points on modular curves”, *Res. Number Theory* **9**:1 (2023), art. id. 17, 19 pp. [MR](#)
- [41] A. V. Sutherland and D. Zywina, “Modular curves of prime-power level with infinitely many rational points”, *Algebra Number Theory* **11**:5 (2017), 1199–1229. [MR](#)
- [42] H. P. F. Swinnerton-Dyer, “On l -adic representations and congruences for coefficients of modular forms, II”, pp. 63–90 in *Modular functions of one variable* (Bonn, 1976), vol. 5, Lecture Notes in Math. **601**, Springer, 1977. [MR](#)
- [43] P. L. Wantzel, “Recherches sur les moyens de reconnaître si un problème de géométrie peut se résoudre avec la règle et le compas”, *J. Math. Pure Appl.* (1) **2** (1837).

- [44] Z. Yvon, “Coincidences of division fields of an elliptic curve defined over a number field”, preprint, 2024. [arXiv 2407.14370](#)
- [45] D. Zywina, “On the possible images of the mod ℓ representations associated to elliptic curves over \mathbb{Q} ”, preprint, 2015. [arXiv 1508.07660](#)
- [46] D. Zywina, “On the surjectivity of mod ℓ representations associated to elliptic curves”, *Bull. Lond. Math. Soc.* **54**:6 (2022), 2404–2417. [MR](#)

Received December 22, 2024. Revised December 9, 2025.

HARRIS B. DANIELS
DEPARTMENT OF MATHEMATICS AND STATISTICS
AMHERST COLLEGE
AMHERST, MA
UNITED STATES
hdaniels@amherst.edu

JEREMY ROUSE
DEPARTMENT OF MATHEMATICS
WAKE FOREST UNIVERSITY
WINSTON-SALEM, NC
UNITED STATES
rouseja@wfu.edu

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

EDITORS

Don Blasius (Managing Editor)
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
blasius@math.ucla.edu

Matthias Aschenbrenner
Fakultät für Mathematik
Universität Wien
Vienna, Austria
matthias.aschenbrenner@univie.ac.at

Vyjayanthi Chari
Department of Mathematics
University of California
Riverside, CA 92521-0135
chari@math.ucr.edu

Atsushi Ichino
Department of Mathematics
Kyoto University
Kyoto 606-8502, Japan
atsushi.ichino@gmail.com

Robert Lipshitz
Department of Mathematics
University of Oregon
Eugene, OR 97403
lipshitz@uoregon.edu

Kefeng Liu
School of Sciences
Chongqing University of Technology
Chongqing 400054, China
liu@math.ucla.edu

Sucharit Sarkar
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
sucharit@math.ucla.edu

Dimitri Shlyakhtenko
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
shlyakht@ipam.ucla.edu

Ruixiang Zhang
Department of Mathematics
University of California
Berkeley, CA 94720-3840
ruixiang@berkeley.edu

PRODUCTION

Silvio Levy, Scientific Editor, production@msp.org


See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2026 is US \$710/year for the electronic version, and \$965/year for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to Mathematical Sciences Publishers, 2000 Allston Way # 59, Berkeley, CA 94701-4004, U.S.A. The Pacific Journal of Mathematics is indexed by [Mathematical Reviews](#), [Zentralblatt MATH](#), [PASCAL CNRS Index](#), [Referativnyi Zhurnal](#), [Current Mathematical Publications](#) and [Web of Knowledge \(Science Citation Index\)](#).

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at Mathematical Sciences Publishers, 2000 Allston Way # 59, Berkeley, CA 94701-4004, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Mathematical Sciences Publishers, 2000 Allston Way # 59, Berkeley, CA 94701-4004.

PJM peer review and production are managed by EditFLOW[®] from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2026 Mathematical Sciences Publishers

PACIFIC JOURNAL OF MATHEMATICS

Volume 342 No. 1 May 2026

The $\bar{\partial}$ -problem on $Z(q)$ -domains	1
DEBRAJ CHAKRABARTI, PHILLIP S. HARRINGTON and ANDREW RAICH	
Polynomial identities and Azumaya loci for rational quantum spheres	37
ALEXANDRU CHIRVASITU	
From i -boxes to signed words	63
ALESSANDRO CONTU, FAN QIN and QIAOLING WEI	
Near coincidences and nilpotent division fields	79
HARRIS B. DANIELS and JEREMY ROUSE	
The Cauchy problem for 1D nonlinear Schrödinger equations with repulsive delta potential for data in L^p -based spaces	115
QINGQUAN DENG, PING LI and XIUHONG LONG	
Finite basis problem for involution semigroups of order four	163
MENG GAO, EDMOND W. H. LEE, YAN FENG LUO and WEN TING ZHANG	