Math. Proc. Camb. Phil. Soc. (2026), **181**, 1049–1078
doi:10.1017/S030500412610200X
First published online 16 April 2026

Minimal torsion curves in geometric isogeny classes

BY ABBEY BOURDON, NINA RYALLS
Wake Forest University, Winston-Salem, NC 27109*, U.S.A.*
e-mail: bourdoam@wfu.edu
e-mail: ninaryalls0@gmail.com

AND LORI D. WATSON
Trinity College, Hartford, CT 06106 *U.S.A.*
e-mail: lori.watson@trincoll.edu

(*Received* 28 *August* 2024*; revised* 11 *September* 2025*; accepted* 23 *November* 2025)

Abstract

In this paper, we introduce the study of minimal torsion curves within a fixed geometric isogeny class. For a $\overline{\mathbb{Q}}$-isogeny class $\mathcal{E}$ of elliptic curves and $N \in \mathbb{Z}^+$, we wish to determine the least degree of a point on the modular curve $X_1(N)$ associated to any $E \in \mathcal{E}$. We consider the cases where $\mathcal{E}$ is *rational*, i.e., contains an elliptic curve with rational j-invariant, or where $\mathcal{E}$ consists of elliptic curves with complex multiplication (CM). If $N = \ell^k$ is a power of a single prime, we give a complete characterisation upon restricting to points of odd degree, and also in the case where $\mathcal{E}$ is CM. We include various partial results in the more general setting.

2020 Mathematics Subject Classification: 11G05, 14G35 (Primary)

1. *Introduction*

The modular curve $X_1(N)$ is an algebraic curve over $\mathbb{Q}$ whose non-cuspidal points parameterise elliptic curves with a distinguished point of order N. Understanding degree d points[1] on $X_1(N)$ is an essential step in classifying torsion subgroups of elliptic curves defined over number fields of degree d—a problem which is solved only for $d \leq 4$ [**20**, **21**, **34–36**, **39**]. By the Riemann–Roch Theorem, the curve $X_1(N)$ has infinitely many points in any degree greater than its genus, so it suffices to characterise points of low degree. One important class of low degree points are *sporadic points*, which are $x \in X_1(N)$ for which there are only finitely many points of degree at most deg (x). Ruling out unexpected sporadic points on $X_1(N)$ would have implications for major open questions in the field, including Serre's Uniformity problem (as in [**11**, theorem 1·3]) and uniformity conjectures for the modular curve $X_0(N)$; see [**3**, conjecture 18] and [**1**, conjecture 1·1]. Such applications further motivate the need for an improved understanding of low degree points

[1] Recall that the degree of a closed point x on a curve C over a number field k is the degree of its residue field: $[k(x) : k]$. This is equivalent to the size of the Galois orbit of points in $C(\bar{k})$ associated to x.

© The Author(s), 2026. Published by Cambridge University Press on behalf of The Cambridge Philosophical Society. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

While studying low degree points on $X_1(N)$ is quite difficult in general, the problem can be made more tractable by restricting the class of points under consideration. One line of investigation considers only points associated to elliptic curves with complex multiplication (CM); see, for example, [7, 14, 15]. The least degree of a point on $X_1(N)$ associated to an elliptic curve with CM by an order $\mathcal{O}$ in an imaginary quadratic field K is given in [7, theorem 1·2]. One could more generally hope to characterise the least degree of a point on $X_1(N)$ as we range over elliptic curves with CM by *any* order in K. Since an elliptic curve with CM by $\mathcal{O} \subseteq K$ is isogenous over $\overline{\mathbb{Q}}$ to one with CM by the full ring of integers, this is in essence a special case of the following question: for a given geometric isogeny class $\mathcal{E}$ of elliptic curves and fixed $N \in \mathbb{Z}^+$, what is the least degree of a point on $X_1(N)$ associated to an elliptic curve in $\mathcal{E}$? And what elliptic curve(s) in $\mathcal{E}$ attain a point on $X_1(N)$ of least possible degree? We investigate these questions in this paper.

Let $\mathcal{E}$ be a geometric isogeny class of elliptic curves. That is, for any $E_1, E_2 \in \mathcal{E}$, there exists an isogeny $\varphi : E_1 \to E_2$ defined over $\overline{\mathbb{Q}}$. We want to find the minimum d such that there exists F of degree d and $E/F \in \mathcal{E}$ such that $E(F)$ contains a point P of order N. We call *E a minimal torsion curve for $\mathcal{E}$ of level N*. Because F is of minimal degree, the residue field of the closed point associated to $(E, P) \in X_1(N)(\overline{\mathbb{Q}})$ is also of degree d, and so we may alternatively view E as a curve over $\overline{\mathbb{Q}}$ identified by its j-invariant, j_{min}. In this paper, we study minimal torsion curves of prime-power level. For CM isogeny classes, we obtain a near complete characterisation.

THEOREM 1·1. *Let $\mathcal{E}$ be a $\overline{\mathbb{Q}}$-isogeny class of elliptic curves with CM by an order in the imaginary quadratic field K. For a prime number ℓ, the the least degree of a point on $X_1(\ell^k)$ associated to any $E \in \mathcal{E}$ is given in Propositions 9·1, 9·2, and 9·3. If ℓ is split in K, then an elliptic curve with CM by the full ring of integers in K is a minimal torsion curve for $\mathcal{E}$ of level ℓ^k and $[\mathbb{Q}(j_{min}) : \mathbb{Q}] = h_K$, the class number of K. Otherwise $[\mathbb{Q}(j_{min}) : \mathbb{Q}] \to \infty$ as $k \to \infty$.*

If $\mathcal{E}$ is a $\overline{\mathbb{Q}}$-isogeny class of elliptic curves with CM by an order in K, then $[\mathbb{Q}(j(E)) : \mathbb{Q}] \geq h_K$ for any $E \in \mathcal{E}$. Thus when ℓ is split in K, a minimal torsion curve has $[\mathbb{Q}(j_{min}) : \mathbb{Q}]$ minimal for $\mathcal{E}$. However, if ℓ is inert or ramified in K, the extension $[\mathbb{Q}(j_{min}) : \mathbb{Q}]$ will generally not be minimal for $\mathcal{E}$, and indeed must grow with k. These minimal torsion curves have exceptional arithmetic, such as the existence of a high-power ℓ^k-isogeny defined over $\mathbb{Q}(j_{min})$, which more than compensates for the degree of $\mathbb{Q}(j_{min})$. This phenomenon was previously observed for CM points of odd degree in [13, remark 2·7]. We illustrate with the following example.

Example 1·2. Let $\mathcal{E}$ be the $\overline{\mathbb{Q}}$-isogeny class of $E/\mathbb{Q}$ with LMFDB[2] label 27.a1. Here $K = \mathbb{Q}(\sqrt{-3})$, and we take $\ell = 3$ which is ramified in K. There are two rational j-invariants associated to elliptic curves in $\mathcal{E}$, namely -12288000 and 0. Thus 1 is the minimal degree of an extension generated by the j-invariant of $E \in \mathcal{E}$. However, by Proposition 9·3, the j-invariant of a minimal torsion curve of level 3^k generates an extension of degree at least $3^{(k-5)/2}$. Thus there is no minimal torsion curve with rational j-invariant for $k \geq 6$, and the degree of $\mathbb{Q}(j_{min})$ must grow with k.

[2] Here, the LMFDB label refers to that which is used by the L-functions and modular forms database [16].

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

Even in non-CM isogeny classes, minimal torsion curves may have j-invariant generating a field of unexpectedly large degree. In some cases, these minimal torsion curves improve degree bounds arising from elliptic curves having rational j-invariant.

Example 1·3. Let $\mathcal{E}$ be the $\overline{\mathbb{Q}}$-isogeny class containing $E/\mathbb{Q}$ with LMFDB label 9225.l1. Here $j(E) \in \mathbb{Q}$, but in Section 8 we see any minimal torsion curve for $\mathcal{E}$ of level 49 has $[\mathbb{Q}(j_{min}) : \mathbb{Q}] \geq 2$. This class is notable since $\mathcal{E}$ contains an elliptic curve giving a point on $X_1(49)$ of degree 42, which is lower than the degree of any $x \in X_1(49)$ with $j(x) \in \mathbb{Q}$. See Corollary 8·3.

Our next results concern the case where $\mathcal{E}$ is *rational*, i.e., contains an elliptic curve with j-invariant in $\mathbb{Q}$. For non-CM classes, we obtain a characterisation of minimal torsion curves upon restriction to points of odd degree, strengthening [**11**, proposition 4·1].

THEOREM 1·4. *Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of elliptic curves which is non-CM. If $E \in \mathcal{E}$ and $x = [E, P] \in X_1(\ell^k)$ is a point of odd degree, then $\ell \in \{2, 3, 5, 7, 11, 13\}$. The least odd degree point on $X_1(\ell^k)$ associated to $E' \in \mathcal{E}$ is given in Propositions 5·1, 6·1 and 7·1, while the following divisibility conditions hold and are best-possible across all such $\mathcal{E}$:*

(i) *if $\ell = 13$, then $3 \cdot 13^{2k-2} \mid \deg(x)$;*
(ii) *if $\ell = 11$, then $5 \cdot 11^{2k-2} \mid \deg(x)$;*
(iii) *if $\ell = 7$ and $\mathcal{E}$ does not contain E' with $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$, then $7^{2k-2} \mid \deg(x)$;*
(iv) *if $\ell = 7$ and $\mathcal{E}$ contains E' with $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$, then $9 \cdot 7^{\max(0,2k-3)} \mid \deg(x)$;*
(v) *if $\ell = 5$, then $5^{\max(0,2k-3)} \mid \deg(x)$;*
(vi) *if $\ell = 3$, then $3^{\max(0,2k-4)} \mid \deg(x)$;*
(vii) *if $\ell = 2$, then $k \leq 3$ and $1 \mid \deg(x)$.*

Moreover, among odd degree points on $X_1(\ell^k)$ coming from $E' \in \mathcal{E}$, a point of least odd degree can always be associated to $E_{min} \in \mathcal{E}$ with $j(E_{min}) \in \mathbb{Q}$ or which is ℓ-isogenous to an elliptic curve having rational j-invariant.

Remark 1·5. The exceptional class for $\ell = 7$ has also been identified in another context. By Sutherland [**47**], elliptic curves $E/\mathbb{Q}$ with $j(E) = 3^3 \cdot 5 \cdot 7^5/2^7$ provide the only counterexamples over $\mathbb{Q}$ to a local-global principle for rational isogenies of prime degree.

In particular, Theorem 1·4 states that under the given assumptions, there exists a minimal torsion curve for $\mathcal{E}$ of level ℓ^k which is at most ℓ-isogenous to an elliptic curve having rational j-invariant. Away from points of odd degree, Proposition 8·1 shows the same condition holds for $\mathcal{E}$ containing a rational elliptic curve with ℓ-adic Galois representation of level ℓ. These are special cases of the following result, which is a consequence of Serre's Open Image Theorem [**43**].

THEOREM 1·6. *Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves, and let ℓ be prime. There exists a constant $C = C(\mathcal{E}, \ell)$ such that for any $k \in \mathbb{Z}^+$ a point of least degree on $X_1(\ell^k)$ coming from $E' \in \mathcal{E}$ can be associated to $j_{min} \in \mathcal{E}$ which is d-isogenous to a rational j-invariant for some $d \leq C$.*

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

Thus unlike the CM case addressed in Theorem 1·1, there always exists a minimal torsion curve of level ℓ^k with j-invariant in an extension of bounded degree. Unfortunately, our proof does not make the constant C explicit; see Theorem 4·3. If $\mathcal{E}$ contains a non-CM elliptic curve $E/\mathbb{Q}$ with ℓ-adic Galois representation of level ℓ, then $C = \ell$ by Proposition 8·1 However, we fail to identify a more general connection between C and the level of $E/\mathbb{Q} \in \mathcal{E}$, though it is natural to ask whether one exists (Remark 4·4).

1·1. *General approach.*

If $\mathcal{E}$ is a rational geometric isogeny class of non-CM elliptic curves, then for any $E \in \mathcal{E}$ there exists an isogeny $\varphi : E \to E_0$ defined over $\overline{\mathbb{Q}}$, where E_0 is the base extension of an elliptic curve defined over $\mathbb{Q}$. Up to replacing E by a quadratic twist if necessary, we may assume E, E_0, and the isogeny φ are defined over a number field F. A key observation is that over F, the image of both ℓ-adic Galois representations have the same index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$:

$$[\mathrm{GL}_2(\mathbb{Z}_\ell) : \mathrm{im}\rho_{E/F,\ell^\infty}] = [\mathrm{GL}_2(\mathbb{Z}_\ell) : \mathrm{im}\rho_{E_0/F,\ell^\infty}].$$

See, for example, [**32**, proposition 2·1·1]. This can be leveraged to give lower bounds on the degree of a point on $X_1(\ell^k)$ associated to $\mathcal{E}$ in terms of $[\mathrm{GL}_2(\mathbb{Z}_\ell) : \mathrm{im}\rho_{E_0/\mathbb{Q},\ell^\infty}]$. We obtain the following proposition, which strengthens [**11**, lemma 4·6].

PROPOSITION 1·7. *Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves. Suppose ℓ is a prime number and $k \in \mathbb{Z}^+$. There exists $E_0/\mathbb{Q} \in \mathcal{E}$ and $x \in X_1(\ell)$ with $j(x) = j(E_0)$ such that the degree of any point on $X_1(\ell^k)$ associated to $\mathcal{E}$ is divisible by*

$$\delta := \begin{cases} \deg(x) \cdot \ell^{\max(0,2k-2-d)} & \text{if } \ell \text{ is odd,} \\ \deg(x) \cdot \ell^{\max(0,2k-3-d)} & \text{if } \ell = 2, \end{cases}$$

where $d := \mathrm{ord}_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell) : \mathrm{im}\rho_{E_0/\mathbb{Q},\ell^\infty}])$.

In some cases, we show these lower bounds are best-possible by explicitly constructing $E' \in \mathcal{E}$ giving a degree δ point on $X_1(\ell^k)$. A natural example is when $d = 0$ and ℓ is odd, in which case a twist of E_0 is a minimal torsion curve for $X_1(\ell^k)$; if $d > 0$, it may be that $j(E') \notin \mathbb{Q}$. In other instances, the lower bounds of Proposition 1·7 can be strengthened by showing that a point on $X_1(\ell^k)$ in degree δ would produce a subgroup of $\mathrm{im}\rho_{E_0/\mathbb{Q},\ell^\infty}$ which does not occur; see Proposition 6·6. Throughout we make use of the partial classification of images of ℓ-adic Galois representations of elliptic curves over $\mathbb{Q}$ due to Rouse and Zureick-Brown [**42**] and Rouse, Sutherland and Zureick-Brown [**41**].

Remark 1·8. Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves. By Theorem 1·6, any minimal torsion curve for $X_1(\ell^k)$ is at most C-isogenous to an elliptic curve with rational j-invariant for some C which does not depend on k. Thus there exists a finite set of j-invariants $\mathcal{J} = \{j_1, j_2, \ldots, j_r\}$ such that for any $k \in \mathbb{Z}^+$, there exists a minimal torsion curve for $\mathcal{E}$ of level ℓ^k with j-invariant in $\mathcal{J}$. However, our proof does not make $\mathcal{J}$ explicit, so our results may not be obtained by checking a finite number of j-invariants. On the other hand, for a fixed $k \in \mathbb{Z}^+$, a finite check is possible since the j-invariant of any minimal torsion curve must generate an extension degree at most $\deg(X_1(\ell^k) \to X_1(1))$.

Results concerning CM isogeny classes rely heavily on prior work of the first author in collaboration with Clark [**6**, **7**].

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

1·2. *Other related work*

Cremona and Najman [18] prove numerous results concerning torsion points of $\mathbb{Q}$-curves defined over number fields of odd degree. Any such elliptic curve is necessarily isogenous to one having rational j-invariant, providing immediate ties to our study of minimal torsion curves in rational geometric isogeny classes. This class of $\mathbb{Q}$-curves is again studied in [11], where the first author and Najman show the $\overline{\mathbb{Q}}$-isogeny class containing the elliptic curve with j-invariant $-140625/8$ is the unique rational non-CM class giving rise to a sporadic point of odd degree on any modular curve $X_1(N)$. More recent work of Genao [27] provides "typical" bounds on the size of the torsion subgroup of an elliptic curve over a number field which belongs to a rational $\overline{\mathbb{Q}}$-isogeny class, and his subsequent work [28] pursues polynomial bounds on such torsion subgroups.

Prior work of the first author and Clark [7] gives the least degree of a point on $X_1(N)$ associated to an elliptic curve with CM by a fixed order in an imaginary quadratic field, while work of Clark, Genao, Pollack, and Saia [15] investigates the least degree of any CM point on $X_1(N)$. Our results fall somewhat in the middle of these two directions of study – we investigate the least degree of a CM point across all orders within a fixed imaginary quadratic field.

1·3. *Code*

We make frequent use of the computer algebra system Magma [5]. All code is available at https://github.com/abbey-bourdon/minimal_torsion_curves.

2. *Background and notation*

2·1. *Conventions*

Throughout, F denotes a number field and $\overline{F}$ denotes a fixed algebraic closure of F. We write Gal_F for the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$.

For an elliptic curve E defined over F and $N \in \mathbb{Z}^+$, the collection of all points in $E(\overline{F})$ of order dividing N is denoted $E[N]$. This is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2. Any elliptic curve E/F corresponds to an equation of the form $y^2 = x^3 + Ax + B$, and we can define its j-invariant to be $j(E) := 1728(4A^3/4A^3 + 27B^2)$. This element of F characterises E up to $\overline{F}$-isomorphism, and we call any E' with $j(E') = j(E)$ a twist of E.

For a prime number ℓ, our notation for subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}_\ell)$ follows [41, 48], respectively. For ℓ-adic images, this is known as the "RSZB label, following the author names of [48], and has the form `N.i.g.n`, where `N` is the level, `i` is the index, `g` is the genus and `n` is a positive integer used to distinguish nonconjugate subgroups. We also refer to specific elliptic curves over $\mathbb{Q}$ by their L-functions and Modular forms database [16] (LMFDB) label.

We always view the modular curve $X_1(N)$ as an algebraic curve over $\mathbb{Q}$; see Section 2.4 for details. By closed point, we mean a $\mathrm{Gal}_{\mathbb{Q}}$-orbit of points in $X_1(N)(\overline{\mathbb{Q}})$. If $x \in X_1(N)$ is closed, we define the degree of x to be the degree of its residue field $\mathbb{Q}(x)$. By taking the sum of Galois conjugates, such a closed point of degree d can be viewed as an irreducible $\mathbb{Q}$-rational effective divisor of degree d.

2·2. *Galois representations*

Let E be an elliptic curve defined over a number field F, and let ℓ be a prime number. For any $k \in \mathbb{Z}^+$, the elements of Gal_F induce natural automorphisms of the points in

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

$E(\overline{F})$ of order dividing ℓ^k, denoted $E[\ell^k]$. This action is recorded in the **mod ℓ^k Galois representation** associated to E,

$$\rho_{E,\ell^k} : \mathrm{Gal}_F \to \mathrm{Aut}(E[\ell^k]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z}).$$

By choosing compatible bases as k ranges over all positive integers, the mod ℓ^k Galois representations fit together to give the **ℓ-adic Galois representation** associated to E,

$$\rho_{E,\ell^\infty} : \mathrm{Gal}_F \to \mathrm{GL}_2(\mathbb{Z}_\ell),$$

which encodes the Galois action on all points in $E(\overline{F})$ of order a power of ℓ. If E is non-CM, then $\mathrm{im}\rho_{E,\ell^\infty}$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ by Serre's open image theorem [43]. Thus there exists a nonnegative integer d such that $\mathrm{im}\rho_{E,\ell^\infty} = \pi^{-1}(\mathrm{im}\rho_{E,\ell^d})$, where $\pi : \mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^d\mathbb{Z})$ is the natural reduction map. The smallest such ℓ^d for which this holds is called the **level** of the ℓ-adic Galois representation.

Aside from $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, all groups which are known to occur as the image of the mod ℓ Galois representation associated to a non-CM elliptic curve over $\mathbb{Q}$ appear (up to conjugacy) in Tables 3 and 4 of [48]. This list is complete for $\ell \leq 13$ by work of Zywina [50] and Balakrishnan, Dogra, Müller, Tuitman, and Vonk [2], and it has been conjectured to be complete for all ℓ by both Sutherland [48, conjecture 1·1] and Zywina [50, conjecture 1·12]. Unconditionally, we have the following result for $\ell \geq 17$.

THEOREM 2·1 (Mazur [40], Serre [44], Bilu, Parent and Rebolledo [4]). *Suppose $E/\mathbb{Q}$ is a non-CM elliptic curve and $\ell \geq 17$ is prime. If $\mathrm{im}\rho_{E,\ell}$ is not equal to $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and not conjugate to a group in Table 3 or 4 of [48], then $\mathrm{im}\rho_{E,\ell}$ is contained in $C_{ns}^+(\ell)$, the normaliser of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*

Refinements of Theorem 2·1 appear in [50, proposition 1·13], which is also proven in [37, appendix B]. Recently, Furio and Lombardo [26] have shown that proper subgroups of the normaliser of a non-split Cartan subgroup do not occur for primes larger than 37. Taken together with prior work, [26, theorem 1·6] implies the following result.

THEOREM 2·2 (Furio, Lombardo [26]). *Suppose $E/\mathbb{Q}$ is a non-CM elliptic curve and $\ell \geq 17$ is prime. If $\mathrm{im}\rho_{E,\ell}$ is not equal to $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and not conjugate to a group in Table 4 of [48], then $\mathrm{im}\rho_{E,\ell}$ is conjugate to $C_{ns}^+(\ell)$.*

Many partial classification results exist for the image of the ℓ-adic Galois representation of an elliptic curve $E/\mathbb{Q}$. First suppose E is non-CM. The groups which occur as $\mathrm{im}\rho_{E,2^\infty}$ are known due to work of Rouse and Zureick-Brown [42]. For odd primes ℓ, Sutherland and Zywina [49] have identified the images that occur infinitely often, and work of Rouse, Sutherland and Zureick-Brown [41] provides additional classification results for $3 \leq \ell \leq 11$ which are complete up to computing rational points on 6 remaining modular curves. If E has complex multiplication, see work of Lozano-Robledo [38].

2·3. *Elliptic curves with an isogeny*

Suppose E/F is an elliptic curve with an F-rational cyclic N-isogeny for $N \in \mathbb{Z}^+$, which means there is a cyclic subgroup of order N fixed (as a group) by Gal_F. Thus there exists $P \in E(\overline{F})$ of order N such that for any $\sigma \in \mathrm{Gal}_F$, there is some $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$ for which

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

$\sigma(P) = \alpha P$. This defines a homomorphism called the *isogeny character*:

$$\chi : \mathrm{Gal}_F \to (\mathbb{Z}/N\mathbb{Z})^\times$$
$$\sigma \mapsto \alpha.$$

If the image of χ lands in $\{\pm 1\}$, then there is a twist of E for which the point corresponding to P becomes F-rational. In general, we have the following proposition.

PROPOSITION 2·3. *Let $N \geq 3$ be an integer, and let E/F be an elliptic curve with an F-rational cyclic isogeny of degree N. There is an abelian extension L/F with $[L : F] \mid (\varphi(N)/2)$ and a quadratic twist E' of E/L such that $E'(L)$ has a point of order N.*

Proof. This is a consequence of [8, theorem 5·5].

2·4. *Modular curves*

In this paper, we are interested in characterising degrees of points on the modular curve $X_1(N)$, where N is a positive integer. Recall $X_1(N)$ is an algebraic curve over $\mathbb{Q}$ whose non-cuspidal points correspond to isomorphism classes of elliptic curves with a distinguished point of order N. If E is an elliptic curve defined over a number field F with $P \in E(F)$ of order N, then (E, P) gives an F-valued point on $X_1(N)$ via this moduli interpretation. By definition, this is a morphism of $\mathbb{Q}$-schemes $f : \mathrm{Spec}\, F \to X_1(N)$, and the image of f is the associated closed point, denoted $[E, P]$. See [23, section 7·7], [22], [45, section 6·7], [46, appendix C, section 13], or [19] or [19] for more details. If $x \in X_1(N)$ is closed point, we define the **degree** of x to be the degree of the residue field $\mathbb{Q}(x)$. For a non-cuspidal point x, we can construct $\mathbb{Q}(x)$ explicitly via the following result.

LEMMA 2·4 *Let $E/\overline{\mathbb{Q}}$ be an elliptic curve and let $P \in E(\overline{\mathbb{Q}})$ be a point of order N. Then the residue field of the closed point $x = [E, P] \in X_1(N)$ is given by*

$$\mathbb{Q}(x) = \mathbb{Q}(j(E), \mathfrak{h}(P)),$$

where $\mathfrak{h} : E \to E/\mathrm{Aut}(E) \cong \mathbb{P}^1$ is a Weber function for E. There is Weierstrass equation for E defined over $\mathbb{Q}(x)$ for which $P \in E(\mathbb{Q}(x))$, and $\mathbb{Q}(x)$ is contained in any number field over which both E and P are defined.

Proof. See, for example, [11, lemma 2·5] and [19, p. 274, proposition VI·3·2].

Remark 2·5. If $E/\mathbb{Q}(j(E))$ corresponds to an equation of the form $y^2 = x^3 + Ax + B$ and $P = (x, y) \in E$, then we may take

$$\mathfrak{h}(P) = \begin{cases} x & AB \neq 0 \\ x^2 & B = 0 \\ x^3 & A = 0 \end{cases}.$$

Note $AB \neq 0$ if E is non-CM. Thus by Lemma 2·4 we can compute the degree of a closed point on $X_1(N)$ associated to a non-CM elliptic curve by factoring division polynomials. See [45, p. 107] for details, including a formulation of the Weber function which is more clearly model-independent.

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

Many of our results rely on first constructing an explicit point $x \in X_1(\ell^k)$ for some small integer k, and then obtaining information on the degree of lifts of x using formulas for the degree of maps between modular curves.

PROPOSITION 2·6. *For positive integers a and b, there is a $\mathbb{Q}$-rational map $f : X_1(ab) \to X_1(a)$ which sends $[E, P]$ to $[E, bP]$. Moreover*

$$\deg(f) = c_f \cdot b^2 \prod_{p \mid b,\, p \nmid a} \left(1 - \frac{1}{p^2}\right),$$

where $c_f = 1/2$ if $a \leq 2$ and $ab > 2$, and $c_f = 1$ otherwise.

Proof. The moduli interpretation ensures the map is defined over $\mathbb{Q}$, and the degree calculation follows from [23, p·66].

2·5. *Complex multiplication*

An elliptic curve E defined over a number field F has *complex multiplication (CM)* if the ring of endomorphisms of E defined over $\overline{F}$ is strictly larger than $\mathbb{Z}$. In this case, $\mathrm{End}_{\overline{F}}(E) \cong \mathcal{O}$, an order in an imaginary quadratic field K. We have $\mathcal{O} = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K$ where $\mathcal{O}_K$ is the ring of integers in K and $\mathfrak{f}$ is a positive integer called the *conductor* of $\mathcal{O}$. If $\mathfrak{f} = 1$, then $\mathcal{O} = \mathcal{O}_K$, the *maximal order* in K. Each imaginary quadratic order is uniquely identified by its *discriminant*,

$$\Delta = \Delta(\mathcal{O}) = \mathfrak{f}^2 \Delta_K,$$

where Δ_K is the discriminant of K. We have $\#\mathcal{O}^\times = 2$ unless $\Delta = -3$ or -4 in which case $\#\mathcal{O} = 6$ or 4, respectively. If E has CM by the order $\mathcal{O}$ in K, then $[\mathbb{Q}(j(E)) : \mathbb{Q}] = h(\mathcal{O})$ by [17, theorem 11·1], the class number of $\mathcal{O}$. If $\mathfrak{f} = 1$ then $h(\mathcal{O}) = h_K$, the class number of K. If $\mathfrak{f} > 1$, then by [17, corollary 7·24]

$$h(\mathcal{O}) = [\mathbb{Q}(j(E)) : \mathbb{Q}] = h_K \frac{\mathfrak{f}}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \prod_{p \mid \mathfrak{f}} \left(1 - \left(\frac{\Delta_K}{p}\right) \frac{1}{p}\right). \tag{2·1}$$

Any two j-invariants of $\mathcal{O}$-CM elliptic curves are Galois conjugate algebraic integers.

3. *Preliminary results*

In this section, we begin by establishing a brief technical result concerning the field of definition of an isogeny (section 3·1), which essential follows from prior work of Cremona and Najman [18, corollary A·5] or Clark [14, proposition 3·2]. This is used in Section 3·2 to prove a general divisibility condition for points on modular curves corresponding to a fixed rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves, strengthening [11, lemma 4·6]. In Section 3·3, we conclude with a lemma concerning the image of Galois representations attached to elliptic curves connected by a rational cyclic isogeny.

3·1. *Fields of definition for isogenies*

Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves. By definition, there exists $E_0 \in \mathcal{E}$ with $j(E_0) \in \mathbb{Q}$, and for any $E \in \mathcal{E}$ there is a $\overline{\mathbb{Q}}$-isogeny $\varphi : E \to E_0$. Since the degree of closed points on $X_1(N)$ can be computed using any Weierstrass model of E by Lemma 2·4,

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

we are free to replace E and E_0 by quadratic twists in order to achieve a more convenient representation of φ. The lemma given below essentially follows from the fact that $\mathbb{Q}(j(E), j(E_0)) = \mathbb{Q}(j(E))$ is contained in the residue field of any closed point on $X_1(N)$ associated to E, and this is the field of moduli of the isogeny φ; see [**14**, section 3.3] or [**18**, corollary A·5].

LEMMA 3·1 *Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves and let $E \in \mathcal{E}$. Suppose $x = [E, P] \in X_1(\ell^k)$ for some prime number ℓ and positive integer k, and let $F := \mathbb{Q}(x)$. There is a Weierstrass equation of E/F for which $P \in E(F)$ and such that there exists an F-rational cyclic isogeny $\varphi : E \to E_0$ with $j(E_0) \in \mathbb{Q}$.*

Proof. Since $\mathcal{E}$ is rational, there exists $E_0 \in \mathcal{E}$ with $j(E_0) \in \mathbb{Q}$. By definition there exists an isogeny $\varphi : E \to E_0$ defined over $\overline{\mathbb{Q}}$ which we may assume is cyclic of degree N; see Lemma A·1 in [**18**]. Let C denote its kernel. Note that $F = \mathbb{Q}(j(E), \mathfrak{h}(P))$ by Lemma 2·4 and there exists a Weierstrass equation of E/F with $P \in E(F)$. The proof strategy of [**14**, proposition 3·2] shows C is F-rational, as we will now explain. Suppose $\sigma(C) \neq C$ for some $\sigma \in \mathrm{Gal}_F$, and consider the induced isogeny $E^\sigma \to (E/C)^\sigma$. Since $j(E/C) = j(E_0) \in \mathbb{Q}$, we see that $j((E/C)^\sigma) = j(E_0)$. Thus composition with an isomorphism to E_0 yields a cyclic N-isogeny $\psi : E \to E_0$ with kernel $\sigma(C)$. But having two cyclic N-isogenies from E to E_0 with distinct kernels can happen only if E has complex multiplication (see the last paragraph of the proof of [**14**, proposition 3·2] for details). We have reached a contradiction.

3·2. *General divisibility conditions*

Let $\mathcal{E}$ be rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves. Fix a prime number ℓ and positive integer k. If $E \in \mathcal{E}$, then we can relate the degree of $[E, P] \in X_1(\ell^k)$ to the degree of $[E_0, P_0] \in X_1(\ell)$ for some $E_0 \in \mathcal{E}$ having $j(E_0) \in \mathbb{Q}$. This is formalised in the following proposition, which strengthens [**11**, lemma 4·6] and proves Proposition 1·7.

PROPOSITION 3·2. *Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves. Suppose ℓ is a prime number and $k \in \mathbb{Z}^+$. There exists $E_0/\mathbb{Q} \in \mathcal{E}$ and $x \in X_1(\ell)$ with $j(x) = j(E_0)$ such that the degree of any point on $X_1(\ell^k)$ associated to $\mathcal{E}$ is divisible by*

$$\begin{cases} \deg(x) \cdot \ell^{\max(0, 2k-2-d)} & \text{if } \ell \text{ is odd,} \\ \deg(x) \cdot \ell^{\max(0, 2k-3-d)} & \text{if } \ell = 2, \end{cases}$$

where $d := \mathrm{ord}_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell) : \mathrm{im}\rho_{E_0, \ell^\infty}])$.

Remark 3·3. Let $k \in \mathbb{Z}^{\geq 2}$. Since $\deg(X_1(\ell^k) \to X_1(\ell)) = \ell^{2k-2}$ for ℓ odd and $\deg(X_1(2^k) \to X_1(2)) = 2^{2k-3}$, these lower bounds are best-possible whenever $d = 0$. In this case E_0 itself is a minimal torsion curve for $X_1(\ell^k)$. This holds in certain cases; see, for example, Lemma 5·3. However, there are other $\overline{\mathbb{Q}}$-isogeny classes for which these bounds can be further refined. See Proposition 6·1.

Proof. Let $E \in \mathcal{E}$, and fix $P \in E$ of order ℓ^k. Define $F := \mathbb{Q}(j(E), \mathfrak{h}(P))$. By Lemma 3·1, there is a Weierstrass model of E/F where $P \in E(F)$ and such that there exists an F-rational cyclic isogeny $\varphi : E \to E'$ with $j(E') \in \mathbb{Q}$. By [**11**, lemma 4·6], we have $[F : \mathbb{Q}]$ is divisible by

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

$$\begin{cases} \ell^{\max(0,2k-2-d)} \text{ if } \ell \text{ is odd,} \\ \ell^{\max(0,2k-3-d)} \text{ if } \ell = 2, \end{cases}$$

where $d = \mathrm{ord}_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell) : \mathrm{im}\rho_{E_0,\ell^\infty}])$ for any elliptic curve $E_0/\mathbb{Q}$ with $j(E_0) = j(E')$.

By [11, corollary 4·3 (2)], the curve E' has a point of order ℓ over an extension F'/F of degree dividing ℓ. In particular, there exists a closed point $x = [E', P'] \in X_1(\ell)$ such that $\mathbb{Q}(x) \subseteq F'$. Hence

$$\deg(x) \mid \ell \cdot [F : \mathbb{Q}].$$

Since $j(E') = j(E_0)$, there exists a point $P_0 \in E_0$ such that the closed point $x = [E_0, P_0]$. If $\deg(x)$ is prime to ℓ, then $\deg(x) \mid [F : \mathbb{Q}]$, and the conclusion follows since F is the residue field of the closed point associated to $[E, P]$ by Lemma 2·4. So suppose $\deg(x) = \ell \cdot n_0$. Note that $\ell \nmid n_0$, since $\deg(X_1(\ell) \to X_1(1)) < \ell^2$, so $n_0 \mid [F : \mathbb{Q}]$. If there exists $x_1 \in X_1(\ell)$ associated to E_0 with $\deg(x_1) \mid n_0$, then the conclusion follows with x_1 in place of x. So suppose not. By checking the possible images of the mod ℓ Galois representation associated to E_0 as in [30, theorem 5·6, Tables 1 and 2], we see that we must be in one of the following cases (see Section 2·1 for an explanation of subgroup labels used):

(i) $\ell = 5$, $\mathrm{im}\rho_{E_0,5} = 5B.1.2$, $5B.1.3$, or $5B.4.2$;
(ii) $\ell = 7$, $\mathrm{im}\rho_{E_0,7} = 7B.1.3$, $7B.1.4$, or $7B.6.3$;
(iii) $\ell = 13$, $\mathrm{im}\rho_{E_0,13} = 13B.3.2$, $13B.3.7$, $13B.5.2$ or $13B.4.2$;
(iv) $\ell = 17$, $\mathrm{im}\rho_{E_0,17} = 17B.4.6$;
(v) $\ell = 37$, $\mathrm{im}\rho_{E_0,37} = 37B.8.2$.

In each case, there exists a $\mathbb{Q}$-rational cyclic subgroup C of E_0 such that E_0/C has mod ℓ image outside this list; see [48, theorem 3·32, Tables 3 and 4]. That is, in each case there exists a point on $X_1(\ell)$ associated to E_0/C of degree dividing n_0, and the result holds with E_0/C in place of E_0.

Remark 3·4. From the proof, we see that the statement of Proposition 3·2 holds for any $E_0/\mathbb{Q} \in \mathcal{E}$ which satisfies the following constraints:

(i) $\ell = 5$, $\mathrm{im}\rho_{E_0,5} \neq 5B.1.2$, $5B.1.3$ or $5B.4.2$;
(ii) $\ell = 7$, $\mathrm{im}\rho_{E_0,7} \neq 7B.1.3$, $7B.1.4$ or $7B.6.3$;
(iii) $\ell = 13$, $\mathrm{im}\rho_{E_0,13} \neq 13B.3.2$, $13B.3.7$, $13B.5.2$ or $13B.4.2$;
(iv) $\ell = 17$, $\mathrm{im}\rho_{E_0,17} \neq 17B.4.6$;
(v) $\ell = 37$, $\mathrm{im}\rho_{E_0,37} \neq 37B.8.2$;

3·3. *Image of galois representations under isogeny*

PROPOSITION 3·5. *Let E_1/F be a non-CM elliptic curve, and fix a prime number ℓ. Suppose $\varphi: E_1 \to E_2$ is an F-rational cyclic ℓ^r-isogeny of elliptic curves over F for $r \in \mathbb{Z}^+$. Then*:

(i) $\mathrm{im}\rho_{E_2,\ell^k}$ *is completely determined by* $\mathrm{im}\rho_{E_1,\ell^{r+k}}$;
(ii) *If* $\mathrm{im}\rho_{E_1,\ell^\infty} = \pi^{-1}(\mathrm{im}\rho_{E_1,\ell^{k_1}})$ *for some* $k_1 \in \mathbb{Z}^+$, *then* $\mathrm{im}\rho_{E_2,\ell^\infty} = \pi^{-1}(\mathrm{im}\rho_{E_2,\ell^{k_1+r}})$. *Here,* π *denotes the reduction map from* $\mathrm{GL}_2(\mathbb{Z}_\ell)$ *to* $\mathrm{GL}_2(\mathbb{Z}/\ell^{k_1}\mathbb{Z})$ *or* $\mathrm{GL}_2(\mathbb{Z}/\ell^{k_1+r\mathbb{Z}})$, *respectively.*

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

Proof. Let $\{P, Q\}$ be a basis for $E_1[\ell^{r+k}]$, where $\ker(\varphi) = \langle \ell^k P \rangle$. Then with respect to this basis, for any $\sigma \in \mathrm{Gal}_F$, there exist $a, b, c, d \in \mathbb{Z}$ such that

$$\rho_{E_1,\ell^{r+k}}(\sigma) = \begin{pmatrix} a & b \\ \ell^r c & d \end{pmatrix}.$$

One can check that $\{\varphi(P), \ell^r \varphi(Q)\}$ gives a basis for $E_2[\ell^k]$. Moreover, for $\sigma \in \mathrm{Gal}_F$, we have

$$\sigma(\varphi(P)) = \varphi(\sigma(P)) = \varphi(aP + \ell^r cQ) = a\varphi(P) + c\ell^r \varphi(Q),$$
$$\sigma(\ell^r \varphi(Q)) = \ell^r \varphi(\sigma(Q)) = \ell^r \varphi(bP + dQ) = \ell^r b\varphi(P) + d\ell^r \varphi(Q).$$

Thus

$$\rho_{E_2,\ell^k}(\sigma) = \begin{pmatrix} a & \ell^r b \\ c & d \end{pmatrix},$$

and $\mathrm{im}\rho_{E_2,\ell^k}$ can be deduced from $\mathrm{im}\rho_{E_1,\ell^{r+k}}$.

Finally, suppose $\mathrm{im}\rho_{E_1,\ell^\infty} = \pi^{-1}(\mathrm{im}\rho_{E_1,\ell^{k_1}})$, and let $M \in \mathrm{GL}_2(\mathbb{Z}/\ell^{k_1+r+1}\mathbb{Z})$ where

$$M \pmod{\ell^{k_1+r}} \in \mathrm{im}\rho_{E_2,\ell^{k_1+r}}.$$

If we can show that $M \in \mathrm{im}\rho_{E_2,\ell^{k_1+r+1}}$, then $\mathrm{im}\rho_{E_2,\ell^\infty} = \pi^{-1}(\mathrm{im}\rho_{E_2,\ell^{k_1+r}})$ by, e.g., [**9**, proposition 3·5]. By the first paragraph, we may assume

$$M = \begin{pmatrix} a + \ell^{k_1+r}\alpha & \ell^r b + \ell^{k_1+r}\beta \\ c + \ell^{k_1+r}\gamma & d + \ell^{k_1+r}\delta \end{pmatrix} = \begin{pmatrix} a + \ell^{k_1+r}\alpha & \ell^r(b + \ell^{k_1}\beta) \\ c + \ell^{k_1+r}\gamma & d + \ell^{k_1+r}\delta \end{pmatrix}$$

for some

$$\begin{pmatrix} a & b \\ \ell^r c & d \end{pmatrix} \in \mathrm{im}\rho_{E_1,\ell^{k_1+2r}}.$$

Since $\mathrm{im}\rho_{E_1,\ell^\infty} = \pi^{-1}(\mathrm{im}\rho_{E_1,\ell^{k_1}})$, there exists $\sigma \in \mathrm{Gal}_F$ such that

$$\rho_{E_1,\ell^{r+k_1+r+1}}(\sigma) = \begin{pmatrix} a + \ell^{k_1+r}\alpha & b + \ell^{k_1}\beta \\ \ell^r(c + \ell^{k_1+r}\gamma) & d + \ell^{k_1+r}\delta \end{pmatrix},$$

as its reduction mod ℓ^{k_1} is in $\mathrm{im}\rho_{E_1,\ell^{k_1}}$. By the first paragraph,

$$\rho_{E_2,\ell^{k_1+r+1}}(\sigma) = \begin{pmatrix} a + \ell^{k_1+r}\alpha & \ell^r(b + \ell^{k_1}\beta) \\ c + \ell^{k_1+r}\gamma & d + \ell^{k_1+r}\delta \end{pmatrix} = M.$$

COROLLARY 3·6. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. For any prime number ℓ and $k \in \mathbb{Z}^+$, the degrees of closed points on $X_1(\ell^k)$ associated to elliptic curves ℓ^r-isogenous to E over $\overline{\mathbb{Q}}$ are entirely determined by* $\mathrm{im}\rho_{E/\mathbb{Q},\ell^\infty}$.

Proof. Suppose there exists an isogeny $\varphi : E \to E'$ defined over $\overline{\mathbb{Q}}$ which is cyclic of order ℓ^r. Thus there exists a point $P \in E$ of order ℓ^r such that $E' \cong E/\langle P \rangle$. Let $F := \mathbb{Q}(\langle P \rangle)$, and

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

let $\psi : E \to E/\langle P \rangle$ be the induced F-rational isogeny. By Proposition 3·5 the ℓ-adic Galois representation of $E/\langle P \rangle$, and thus the degrees of all closed points on $X_1(\ell^k)$ associated to $E/\langle P \rangle$, is determined by $\mathrm{im}\rho_{E/F,\ell^\infty}$. Since $\mathrm{im}\rho_{E/F,\ell^\infty}$ can be obtained from $\mathrm{im}\rho_{E/\mathbb{Q},\ell^\infty}$ and the definition of F, the result follows.

4. *Properties of minimal torsion curves*

Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of elliptic curves. In this section, we show that for a fixed positive integer N, there are finitely many minimal torsion curves in $\mathcal{E}$ for $X_1(N)$. In some cases, there is a unique minimal torsion curve, but this should not be expected in general (see Remark 4·2). Next, we suppose $\mathcal{E}$ is non-CM,[3] and let $E_0 \in \mathcal{E}$ be an elliptic curve with rational j-invariant. Fix a prime ℓ. In Theorem 4·3 we show that for any $k \in \mathbb{Z}^+$, there exists a minimal torsion curve $E \in \mathcal{E}$ for $X_1(\ell^k)$ such that the degree of the isogeny from E to E_0 is at most C, where C is a constant that does not depend on k. This implies Theorem 1·6, as stated in the introduction.

4·1. *Minimal torsion curves for fixed modular curve*

PROPOSITION 4·1. *Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of elliptic curves. For a fixed positive integer N, there exist finitely many minimal torsion curves for $X_1(N)$ up to isomorphism over $\overline{\mathbb{Q}}$.*

Proof. Let d be the minimal degree of a point on $X_1(N)$ associated to $\mathcal{E}$, and let j_{min} be the j-invariant of a minimal torsion curve for $\mathcal{E}$. Then $[\mathbb{Q}(j_{min}) : \mathbb{Q}] \leq d$. If $\mathcal{E}$ is CM, then the conclusion follows as there are only finitely many CM j-invariants in an extension of bounded degree (since there are only finitely many imaginary quadratic fields—and hence imaginary quadratic orders—of a given class number [**33**], this is a consequence of [**17**, theorem 11·1 proposition 13·2]). So suppose $\mathcal{E}$ is non-CM.

Let $E_{min} \in \mathcal{E}$ be an elliptic curve with $j(E_{min}) = j_{min}$. Since $\mathcal{E}$ is rational, there exists an elliptic curve $E_0/\mathbb{Q} \in \mathcal{E}$ with an isogeny $\varphi : E_0 \to E_{min}$ defined over $\overline{\mathbb{Q}}$. We may assume φ is cyclic of degree n by [**18**, lemma A·1]. By [**14**, proposition 3·2] or [**18**, corollary A·5], the field of moduli of this isogeny is

$$\mathbb{Q}(j_{min}, j(E_0)) = \mathbb{Q}(j_{min}).$$

Thus φ can be defined over $\mathbb{Q}(j_{min})$ by replacing E_0 and E_{min} with appropriate twists, and in particular a twist of E_0 defined over this field has a rational cyclic n-isogeny. Since isogenies are twist invariant (i.e., if E_1, E_2 are two elliptic curves over F with the same j-invariant, then E_1 has an F-rational cyclic n-isogeny if and only if E_2 does), it follows that E_0 attains a rational cyclic n-isogeny over $\mathbb{Q}(j_{min})$, a number field of degree at most d.

By Serre's open image theorem [**43**], the image of the adelic Galois representation associated to $E_0/\mathbb{Q}$ has finite index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. For d fixed, it follows that there is a bound on the order of a cyclic subgroup of E_0 which can become F-rational over *any* number field F of degree at most d. Thus there are only finitely many choices for C such that $E_{min} \cong E_0/C$ over $\overline{\mathbb{Q}}$.

[3] Recall $\mathrm{End}(E) \otimes \mathbb{Q}$ is an isogeny invariant, so the entire class $\mathcal{E}$ either is CM or non-CM.

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

Remark 4·2. The minimal torsion curve within a fixed geometric isogeny class may or may not be unique (up to isomorphism over $\overline{\mathbb{Q}}$). For example, let $E_0/\mathbb{Q}$ be the elliptic curve with LMFDB label 38.b2 and let $\mathcal{E}$ denote its geometric isogeny class. Since there exists $P_0 \in E_0(\mathbb{Q})$ of order 5, the least degree of a point on $X_1(5)$ associated to $\mathcal{E}$ is 1, and so any minimal torsion curve for $X_1(5)$ must have j-invariant in $\mathbb{Q}$. By Lemma 3·1, the only other elliptic curve $E' \in \mathcal{E}$ with j-invariant in $\mathbb{Q}$ has $j(E') = -37966934881/4952198$. However, this curve does not give points on $X_1(5)$ of minimal degree. Thus E_0 is a unique minimal torsion curve for $X_1(5)$, up to $\overline{\mathbb{Q}}$-isomorphism.

On the other hand, let $E_0/\mathbb{Q}$ be the elliptic curve with LMFDB label 50.b1 and let $\mathcal{E}$ denote its geometric isogeny class. Then a similar argument shows that *any* elliptic curve $\mathbb{Q}$-isogenous to E_0 is a minimal torsion curve for $X_1(3)$, giving 4 distinct minimal torsion curves for this class up to $\overline{\mathbb{Q}}$-isomorphism. Representatives for these curves can be found in the LMFDB isogeny class 50.b.

4·2. *Minimal torsion curves of varying level*

If we allow N to vary, there may be infinitely many elliptic curves (up to isomorphism over $\overline{\mathbb{Q}}$) within a fixed geometric isogeny class which are minimal for $X_1(N)$. For example, suppose the ℓ-adic Galois representation of a non-CM elliptic curve $E/\mathbb{Q}$ is surjective, and let C be a cyclic subgroup of E of order ℓ^k for $k \in \mathbb{Z}^+$. The elliptic curve E/C can be defined over the extension $\mathbb{Q}(C)$ of degree $\ell^{k-1}(\ell+1)$ and possesses a $\mathbb{Q}(C)$-rational cyclic ℓ^k-isogeny. By Proposition 2·3, the curve E/C gives a closed point on $X_1(\ell^k)$ of degree $\ell^{2k-2}(\ell^2-1)/2$. This is minimal for the geometric isogeny class of E by Proposition 3·2. However, if $\mathcal{E}$ is a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves, there always exists a minimal torsion curve for $X_1(\ell^k)$ whose isogeny degree to a rational elliptic curve is bounded.

THEOREM 4·3. *Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves, and let ℓ be prime. There exists a constant $C = C(\mathcal{E}, \ell)$ such for any $k \in \mathbb{Z}^+$ a point of least degree on $X_1(\ell^k)$ coming from $\mathcal{E}$ can be associated to $j_{min} \in \mathcal{E}$ which is d-isogenous to a rational j-invariant for some $d \leq C$.*

Proof. By Proposition 3·2, there exists $E_0/\mathbb{Q} \in \mathcal{E}$ and $x = [E_0, P_0] \in X_1(\ell)$ such that the degree of any point on $X_1(\ell^n)$ associated to $\mathcal{E}$ is divisible by

$$d_{\min}(\ell^n) := \begin{cases} \deg(x) \cdot \ell^{\max(0,2n-2-d)} & \text{if } \ell \text{ is odd,} \\ \deg(x) \cdot \ell^{\max(0,2n-3-d)} & \text{if } \ell = 2, \end{cases}$$

where $d := \operatorname{ord}_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell) : \mathrm{im}\rho_{E_0,\ell^\infty}])$.

We note $\mathrm{im}\rho_{E_0,\ell^\infty}$ has level ℓ^{k_0} for some $k_0 \in \mathbb{Z}^{\geq 0}$ by Serre's open image theorem [**43**]. Replacing k_0 with a larger integer if necessary, we may assume $2k_0 - 2 - d \geq 0$ if ℓ is odd and $2k_0 - 3 - d \geq 0$ if $\ell = 2$. Now, let k be an integer with $k \geq k_0$. Then by Proposition 3·2, there exists $\alpha_0 \in \mathbb{Z}^+$ such that the least degree of a closed point on $X_1(\ell^k)$ associated to $E_0 \in \mathcal{E}$ is

$$\begin{aligned} d_{\min,E_0}(\ell^k) &= d_{\min}(\ell^k) \cdot \alpha_0 \\ &= d_{\min}(\ell^{k_0}) \cdot \ell^{2(k-k_0)} \cdot \alpha_0. \end{aligned}$$

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

Since $\deg(X_1(\ell^k) \to X_1(\ell^{k_0})) = \ell^{2(k-k_0)}$, the assumptions concerning the level of $\mathrm{im}\rho_{E_0,\ell^\infty}$ imply

$$d_{\min,E_0}(\ell^{k_0}) = d_{\min}(\ell^{k_0}) \cdot \alpha_0.$$

In particular, α_0 does not depend on k.

Suppose first that E_0 is a minimal torsion curve for $X_1(\ell^k)$ for sufficiently large k. Then by Proposition 4·1 there exists a finite collection of elliptic curves $E_0, E_1, \ldots, E_s$ such that for any positive integer n a point of least degree on $X_1(\ell^n)$ coming from $\mathcal{E}$ can be associated to E_i for some $0 \le i \le s$. We may assume the isogeny $\varphi : E_i \to E_0$ is cyclic of degree d_i by [**18**, lemma A·1]. The result follows in this case with $C = \max\{d_0, d_1, \ldots, d_s\}$.

On the other hand, suppose E_0 is not a minimal torsion curve for $X_1(\ell^k)$ for all $k \ge k_0$. Then there exists $E_1 \in \mathcal{E}$ which is a minimal torsion curve for some $X_1(\ell^{k_1})$ where $k_1 \ge k_0$. Choose a Weierstrass equation for E_1 defined over $F := \mathbb{Q}(j(E_1))$. Replacing k_1 with a larger integer if necessary, we may assume that $\mathrm{im}\rho_{E_1,\ell^\infty} = \pi^{-1}(\mathrm{im}\rho_{E_1,\ell^{k_1}})$. By assumption, there exists a positive integer α_1 with $\alpha_1 < \alpha_0$ such that

$$d_{\min,E_1}(\ell^k) = d_{\min}(\ell^k) \cdot \alpha_1$$

for all $k \ge k_1$. If E_1 is a minimal torsion curve for $X_1(\ell^k)$ for sufficiently large k, then we are done as before. Continuing in this way produces a decreasing sequence of positive integers $\alpha_0 > \alpha_1 > \alpha_2 \ldots$, so the process must stop after a finite number of steps.

Remark 4·4. It would be interesting to make the constant $C = C(\mathcal{E}, \ell)$ explicit, perhaps in terms of invariants one could compute from the elliptic curve $E_0/\mathbb{Q}$.

From Theorem 4·3 we can immediately deduce the following corollary.

COROLLARY 4·5. *Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves. There exists a finite collection of j-invariants $j_1, \ldots, j_s \in \mathcal{E}$ such that for any $n \in \mathbb{Z}^+$, a point of least degree on $X_1(\ell^n)$ coming from $\mathcal{E}$ can be associated to an elliptic curve with j-invariant j_i for some $1 \le i \le s$.*

5. *Results for non-CM classes and primes $\ell \ge 5$*

The main result of this section is the following, which proves Theorem 1·4 for $\ell \ge 5$. It refines [**11**, proposition 4·1], which gives divisibility conditions which hold across all rational non-CM classes $\mathcal{E}$ and does not address whether they are best-possible.

PROPOSITION 5·1. *Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves. Suppose $\ell \ge 5$ is prime. If $E \in \mathcal{E}$ and $x = [E, P] \in X_1(\ell^k)$ is a point of odd degree for $k \in \mathbb{Z}^+$, then $\ell \in \{5, 7, 11, 13\}$ and $\delta \mid \deg(x)$ for δ defined as follows*:

(i) *if $\ell = 5$ and $\mathcal{E}$ does not contain $E'/\mathbb{Q}$ with a rational cyclic 25-isogeny, then $\delta = 5^{2k-2}$;*

(ii) *if $\ell = 5$ and $\mathcal{E}$ contains $E'/\mathbb{Q}$ with a rational cyclic 25-isogeny, then $\delta = 5^{\max(0,2k-3)}$;*

(iii) *if $\ell = 7$ and $\mathcal{E}$ contains $E'/\mathbb{Q}$ with $\mathrm{im}\rho_{E',7} \in \{7B.1.1, 7B.1.6, 7B.6.1\}$, then $\delta = 7^{2k-2}$;*

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

(iv) *if* $\ell = 7$ *and* $\mathcal{E}$ *contains* $E'/\mathbb{Q}$ *with* $\mathrm{im}\rho_{E',7} \in \{7B.1.2, 7B.6.2, 7B.2.1, 7B\}$, *then* $\delta = 3 \cdot 7^{2k-2}$;

(v) *if* $\ell = 7$ *and* $\mathcal{E}$ *contains E' with* $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$, *then* $\delta = 9 \cdot 7^{\max(0,2k-3)}$;

(vi) *if* $\ell = 11$, *then* $\delta = 5 \cdot 11^{2k-2}$;

(vii) *if* $\ell = 13$, *then* $\delta = 3 \cdot 13^{2k-2}$.

Moreover, there exists a point of degree δ *on* $X_1(\ell^k)$ *associated to* $j_{min} \in \mathcal{E}$ *which is at most* ℓ*-isogenous to a rational j-invariant. One can take* $j_{min} \in \mathbb{Q}$ *unless* $\ell = 7$ *and* $\mathcal{E}$ *contains the elliptic curve with j-invariant* $3^3 \cdot 5 \cdot 7^5/2^7$.

5·1. *A preliminary result*

We begin with a preliminary result concerning geometric isogeny classes $\mathcal{E}$ containing an elliptic curve over $\mathbb{Q}$ with a rational cyclic isogeny. When this occurs, we will say $\mathcal{E}$ *gives a point* in $X_0(\ell)(\mathbb{Q})$. In this case, the result is largely a consequence of the following theorem and Proposition 3·2.

THEOREM 5·2 (Greenberg [32], Greenberg, Rubin, Silverberg and Stoll [31]) *Let* $E/\mathbb{Q}$ *be a non-CM elliptic curve with a* $\mathbb{Q}$*-rational cyclic isogeny of prime degree* ℓ. *By choice of basis, we may assume* $\mathrm{im}\rho_{E,\ell^\infty}$ *is a subgroup of* $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

(i) *if* $\ell \geq 7$, *then* $\mathrm{im}\rho_{E,\ell^\infty}$ *contains a Sylow pro-*ℓ *subgroup of* $\mathrm{GL}_2(\mathbb{Z}_\ell)$;

(ii) *let* $\ell = 5$. *If none of the elliptic curves in the* $\mathbb{Q}$*-isogeny class of E has two independent isogenies of degree* 5, *then* $\mathrm{im}\rho_{E,5^\infty}$ *contains a Sylow pro-5 subgroup of* $\mathrm{GL}_2(\mathbb{Z}_5)$. *Otherwise the index of* $\mathrm{im}\rho_{E,5^\infty}$ *in* $\mathrm{GL}_2(\mathbb{Z}_5)$ *is divisible by* 5, *but not by* 25.

Proof. If $\ell \geq 11$ or $\ell = 5$, this follows from [32, theorems 1&2]. Note if $\ell \geq 11$ or if $\ell = 5$, the assumption in [32, theorems 1] holds, as explained in [32, remark 4·2·1, p. 1186-1187]. For $\ell = 7$, this follows from [31, theorem 5·5].

LEMMA 5·3 *Suppose* $\ell \geq 5$ *is prime and* $k \in \mathbb{Z}^+$. *Let* $\mathcal{E}$ *be a rational* $\overline{\mathbb{Q}}$*-isogeny class of non-CM elliptic curves which gives a point in* $X_0(\ell)(\mathbb{Q})$. *Then there exists* $E_0/\mathbb{Q} \in \mathcal{E}$ *and* $x \in X_1(\ell)$ *with* $j(x) = j(E_0)$ *such that the degree of any point on* $X_1(\ell^k)$ *arising from* $\mathcal{E}$ *is divisible by*

$$\delta := \begin{cases} \deg(x) \cdot \ell^{2k-2} \text{ if } \ell \neq 5 \text{ or } \mathcal{E} \text{ does not contain } E'/\mathbb{Q} \text{ with a rational cyclic 25-isogeny}, \\ \deg(x) \cdot 5^{\max(0,2k-3)} \text{ if } \ell = 5 \text{ and } \mathcal{E} \text{ contains } E'/\mathbb{Q} \text{ with a rational cyclic 25-isogeny}. \end{cases}$$

Moreover, there exists a point of degree δ *on* $X_1(\ell^k)$ *associated to* $j_{min} \in \mathcal{E}$ *with* $j_{min} \in \mathbb{Q}$.

Proof. Suppose first that $\ell > 5$ or that $\ell = 5$ and $\mathcal{E}$ does not contain $E'/\mathbb{Q}$ with a rational cyclic 25-isogeny. By Proposition 3·2, there exists $E_0/\mathbb{Q} \in \mathcal{E}$ and $x = [E_0, P_0] \in X_1(\ell)$ such that

$$\deg(x) \cdot \ell^{\max(0,2k-2-d)}$$

divides the degree of any point on $X_1(\ell^k)$ associated to $\mathcal{E}$, where $d = \mathrm{ord}_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell) : \mathrm{im}\rho_{E_0,\ell^\infty}])$. By Theorem 5·2, we have $d = 0$. Since $\deg(X_1(\ell^k) \to X_1(\ell)) = \ell^{2k-2}$, lifts of x on $X_1(\ell^k)$ show this divisibility condition is best-possible with $j_{min} = j(E_0)$.

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

Now, suppose $\ell = 5$ and $\mathcal{E}$ contains $E'/\mathbb{Q}$ with a rational cyclic 25-isogeny. Then by Theorem 5·2, we have $\mathrm{ord}_5([\mathrm{GL}_2(\mathbb{Z}_5) : \mathrm{im}\rho_{E',5^\infty}]) = 1$. By replacing E' with a curve $\mathbb{Q}$-isogenous, we may assume E' has two independent 5-isogenies. The index of the image of the 5-adic Galois representation is unchanged by [**32**, proposition 2·1·1]. Then $\mathrm{im}\rho_{E',5}$ is one of the following, and we consider each case separately:

(1) 5Cs.1.1, 5Cs.1.3, or 5Cs.4.1: replacing E' with a quadratic twist if necessary, we may assume $\mathrm{im}\rho_{E',5} = 5Cs.1.1$. By Proposition 3·2 and Remark 3·4, we see $5^{\max(0,2k-3)}$ divides the degree of any point on $X_1(5^k)$ associated to $\mathcal{E}$. The curve E' has a subgroup C_1 generated by a rational point P of order 5 and an independent rational cyclic subgroup C_2 of order 5. Then $E_2 := E'/C_2$ has a rational cyclic 25-isogeny, and the image of P is a point of order 5 in $E_2(\mathbb{Q})$ lying in its kernel. Thus the image of the isogeny character $\chi : \mathrm{Gal}_\mathbb{Q} \to (\mathbb{Z}/25\mathbb{Z})^\times$ lands in the subgroup $\{a : a \equiv 1 \pmod 5\}$ and so has order dividing 5. It follows that E_2 attains a rational point of order 25 in an extension of degree dividing 5. By Proposition 2·6, there are lifts of this point on $X_1(5^k)$ of degree at most 5^{2k-3} for all $k \geq 2$. Thus the condition is best-possible for all k with $j_{min} = j(E_2)$.

(2) 5Cs: by Proposition 3·2 and Remark 3·4, we see $2 \cdot 5^{2k-3}$ divides the degree of any point on $X_1(5^k)$ associated to $\mathcal{E}$. Note E' has two independent 5-isogenies with kernels C_1 and C_2. Then $E_2 := E'/C_2$ has a rational cyclic 25-isogeny. By Proposition 2·3, the curve E_2 gives a closed point on $X_1(5)$ in degree dividing 2 and a closed point on $X_1(25)$ in degree dividing 10. Again by considering lifts of this point with degree bounds given by Proposition 2·6, we see the divisibility condition is best-possible for all k with $j_{min} = j(E_2)$.

5·2. *Proof of Proposition* 5·1.

Let $F = \mathbb{Q}(x)$. By Lemma 3·1, there is a model of E/F where $P \in E(F)$ and such that there exists an F-rational cyclic isogeny $\varphi : E \to E'$ with $j(E') \in \mathbb{Q}$. Since E has an ℓ-isogeny over F, so does E' by [**18**, proposition 3·2]. It follows from [**18**, proposition 3·3] that any $E_0/\mathbb{Q} \in \mathcal{E}$ with $j(E_0) = j(E')$ has a $\mathbb{Q}$-rational cyclic ℓ-isogeny, unless $\ell = 7$ and $j(E_0) = 3^3 \cdot 5 \cdot 7^5/2^7$. Work of Mazur [?] implies $\ell \leq 37$. By applying Lemma 5·3 and checking the possible $x \in X_1(\ell)$ of odd degree associated to elliptic curves over $\mathbb{Q}$ in $\mathcal{E}$, where we may omit images as appearing in Remark 3·4, we see that we are done unless $\ell = 7$ and $\mathcal{E}$ contains an elliptic curve with j-invariant $3^3 \cdot 5 \cdot 7^5/2^7$.

Let us discuss the case $\ell = 7$ and $j(E_0) = 3^3 \cdot 5 \cdot 7^5/2^7$. Recall $P \in E(F)$ is a point of order 7^k. Notice that $7^{k-1}P$ is a point of order 7 on E and is also defined over F on E. By [**11**, corollary 4·3], the curve E' has a rational point of order 7 over an extension F'/F of degree 1 or 7. As $j(E') = 3^3 \cdot 5 \cdot 7^5/2^7$, a computation with division polynomials shows the residue field of a closed point on $X_1(7)$ associated to E' has degree 6 or 9, so $[F' : \mathbb{Q}]$ is divisible by 6 or 9. Since $[F' : F]$ divides 7, it follows that 6 or 9 must divide $[F : \mathbb{Q}]$. Since F is an extension of odd degree, we must have $9 \mid [F : \mathbb{Q}]$. Moreover, in [**11**, proposition 4·1], it is proven that $3 \cdot 7^{\max(0,2k-3)}$ divides $[F : \mathbb{Q}]$. Therefore, $9 \cdot 7^{\max(0,2k-3)}$ divides $[F : \mathbb{Q}]$.

Conversely, we will now show there is a point on $X_1(7^k)$ of degree $9 \cdot 7^{\max(0,2k-3)}$ which is associated to $\mathcal{E}$. By replacing E_0 with a quadratic twist if necessary, we may assume E_0 has LMFDB label 2450.y1. A computation with division polynomials confirms that E_0 gives a closed point on $X_1(7)$ of degree 9, which fulfills the $k = 0$ case. In addition, the mod 7 image

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

of E_0 is 7Ns.2.1, which is of order 18 and generated by the following matrices:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

A Magma computation shows that 7Ns.2.1 contains an index 3 subgroup conjugate to the group generated by

$$\begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Thus over a cubic extension F, the curve E_0 attains two independent 7 isogenies, and is F-isogenous to an elliptic curve E_1/F with a rational cyclic 49-isogeny. By Proposition 2·3, the curve E_1 gives a closed point on $X_1(49)$ of degree dividing $9 \cdot 7$. The previous paragraph shows it must have degree exactly $9 \cdot 7$, and since $\deg(X_1(7^k) \to X_1(7^2))$ has degree 7^{2k-4}, the divisibility conditions of Proposition 3·2 are the best-possible.

6. *Results for non-CM classes and $\ell = 3$*

In this section, we will prove the following result, which includes instances where the divisibility conditions of Proposition 3·2 can be improved. It proves Theorem 1·4 if $\ell = 3$. See Section 2.1 for a discussion of the notation used for subgroups of $\mathrm{GL}_2(\mathbb{Z}_3)$.

PROPOSITION 6·1. *Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves. If $E \in \mathcal{E}$ and $x = [E, P] \in X_1(3^k)$ is a point of odd degree for $k \in \mathbb{Z}^+$, then $\delta \mid \deg(x)$ for δ defined as follows*:

$$\delta := \begin{cases} 3^{\max(0,2k-3)} & \text{if there is } E'/\mathbb{Q} \in \mathcal{E} \text{ with } \mathrm{im}\rho_{E',3^\infty} \in \{9.36.0.6, 9.36.0.8\}, \\ 3^{\max(0,2k-2-d)} & \text{otherwise,} \end{cases}$$

where $d = \mathrm{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \mathrm{im}\rho_{E_0,3^\infty}])$ for any $E_0/\mathbb{Q} \in \mathcal{E}$. These are generally best-possible:

(i) *suppose there is no $E'/\mathbb{Q} \in \mathcal{E}$ with $\mathrm{im}\rho_{E',3^\infty} \in \{9.12.0.2, 9.36.0.2, 9.36.0.7, 9.36.0.8\}$. For any $k \in \mathbb{Z}^+$, there exists a point of degree δ on $X_1(3^k)$ associated to $j_{min} \in \mathcal{E}$;*

(ii) *suppose there is an $E'/\mathbb{Q} \in \mathcal{E}$ with $\mathrm{im}\rho_{E',3^\infty} \in \{9.12.0.2, 9.36.0.7, 9.36.0.8\}$. For $k = 1$ or $k \geq 3$, there exists a point of degree δ on $X_1(3^k)$ associated to $j_{\min} \in \mathcal{E}$. If $k = 2$, then $3\delta \mid \deg(x)$ and there exists a point of degree 3δ on $X_1(3^k)$ associated to $j_{min} \in \mathcal{E}$;*

(iii) *suppose there is an $E'/\mathbb{Q} \in \mathcal{E}$ with $\mathrm{im}\rho_{E',3^\infty} = 9.36.0.2$. For $k = 1$ or $k \geq 4$, there exists a point of degree δ on $X_1(3^k)$ associated to $j_{min} \in \mathcal{E}$. Otherwise $3\delta \mid \deg(x)$ and there exists a point of degree 3δ on $X_1(3^k)$ associated to $j_{min} \in \mathcal{E}$.*

One can take $j_{min} \in \mathbb{Q}$, unless we are in case (ii) *with $k > 2$ or case* (iii) *with $k > 3$; in these latter cases one can take j_{min} to be 3-isogenous to a rational j-invariant.*

The proof shows that $d \leq 2$ for the classes which produce points of odd degree. Thus we immediately deduce the following corollary.

COROLLARY 6·2. *Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves. If $E \in \mathcal{E}$ and $x = [E, P] \in X_1(3^k)$ is a point of odd degree, then $3^{\max(0,2k-4)} \mid \deg(x)$, and this is the best possible across all such $\mathcal{E}$.*

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

Remark 6·3. Suppose there exists $E' \in \mathcal{E}$ with $\mathrm{im}\rho_{E',3^\infty} = 9.36.0.6$. By Proposition 6·1, any odd degree point on $X_1(3^k)$ associated to an elliptic curve in $\mathcal{E}$ has degree divisible by $3^{\max(0,2k-3)}$. By Proposition 3·2, any point of even degree must be divisible by $2 \cdot 3^{\max(0,2k-4)}$. Since there exists $x \in X_1(3)$ of degree 1 associated to E', this strengthens the lower bound in Proposition 3·2 by a factor of 2 or 3, respectively.

6·1. *Preliminary results*

The goal of this section is to prove Proposition 6·6, which obtains the divisibility condition of Proposition 6·1 in the case where $\mathcal{E}$ contains $E'/\mathbb{Q}$ with $\mathrm{im}\rho_{E',3^\infty} = 9.36.0.6$ or $9.36.0.8$. We start by proving two lemmas.

LEMMA 6·4 *Suppose F is a number field of odd degree and E/F is a non-CM elliptic curve with $P \in E(F)$ of order 3^k for $k \in \mathbb{Z}^+$. Let $\varphi : E \to E'$ be an F-rational isogeny, where there exists $E_0/\mathbb{Q}$ of with $j(E_0) = j(E')$ and $d := \mathrm{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \mathrm{im}\rho_{E_0,3^\infty}])$. If $3^{\max(0,2k-1-d)} \nmid [F : \mathbb{Q}]$, then with respect to the basis $\{P, Q\}$ of $E[3^k]$ we have*

$$\mathrm{im}\rho_{E/F,3^k} = \left\{ \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \mid x \in \mathbb{Z}/3^k\mathbb{Z}, y \in (\mathbb{Z}/3^k\mathbb{Z})^\times \right\}$$

and $\mathrm{im}\rho_{E/F,3^\infty} = \pi^{-1}(\mathrm{im}\rho_{E/F,3^k})$.

Proof. Suppose $3^{\max(0,2k-1-d)} \nmid [F : \mathbb{Q}]$, so in particular $2k - 1 - d > 0$. Let $\{P, Q\}$ be a basis of $E[3^k]$. Replacing F with at worst a quadratic extension L/F, we may view φ as an L-isogeny from E to E_0/L. Then $\mathrm{im}\rho_{E/L,3^k}$ is contained in

$$H := \left\{ \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \mid x \in \mathbb{Z}/3^k\mathbb{Z}, y \in (\mathbb{Z}/3^k\mathbb{Z})^\times \right\},$$

which has order $3^k \cdot \varphi(3^k) = 3^{2k-1} \cdot 2$. If $\mathrm{ord}_3(\#\mathrm{im}\rho_{E/L,3^k}) < 2k - 1$, then the index of the mod 3^k Galois representation of E/L is divisible by 3^{2k-1}. Thus

$$3^{2k-1} \mid [\mathrm{GL}_2(\mathbb{Z}_3) : \mathrm{im}\rho_{E/L,3^\infty}].$$

By [**11**, lemma 4·5], we have $3^{2k-1} \mid [\mathrm{GL}_2(\mathbb{Z}_3) : \mathrm{im}\rho_{E_0/\mathbb{Q},3^\infty}] \cdot [L \cap \mathbb{Q}(E_0[3^\infty]) : \mathbb{Q}]$. Since

$$\mathrm{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \mathrm{im}\rho_{E_0/\mathbb{Q},3^\infty}]) = d,$$

it follows that $3^{2k-1-d} \mid [L \cap \mathbb{Q}(E_0[3^\infty]) : \mathbb{Q}]$. Since L is at most a quadratic extension of F, then $3^{2k-1-d} \mid [F : \mathbb{Q}]$, contradicting our assumption. So we may assume $\mathrm{ord}_3(\#\mathrm{im}\rho_{E/L,3^k}) = 2k - 1$.

Note $\mathrm{im}\rho_{E/F,3^k}$ contained in H as well, and since L/F is at worst a quadratic extension, we have $\mathrm{ord}_3(\#\mathrm{im}\rho_{E/F,3^k}) = 2k - 1$. If $\mathrm{im}\rho_{E/F,3^k}$ is properly contained in H, then $\#\mathrm{im}\rho_{E/F,3^k} = 3^{2k-1}$. Since $\mathbb{Q}(\zeta_{3^k}) \subseteq F(E[3^k])$, it follows that 2 must divide $[F : \mathbb{Q}]$. This contradicts F having odd degree. Hence $\mathrm{im}\rho_{E/F,3^k} = H$.

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

If $\mathrm{im}\rho_{E/F,3^\infty} \neq \pi^{-1}(\mathrm{im}\rho_{E/F,3^k})$, then $[F(E[3^{k+1}]) : F(E[3^k])]$ divides 3^3; see, for example, [**9**, proposition 3·5]. Since $\#\mathrm{Gal}(F(E[3^k])/F) = 3^{2k-1} \cdot 2$, we have

$$\#\mathrm{Gal}(F(E[3^{k+1}])/F) \mid 3^3 \cdot 3^{2k-1} \cdot 2 = 3^{2k+2} \cdot 2.$$

It follows that $\#\mathrm{Gal}(L(E[3^{k+1}])/L) \mid 3^{2k+2} \cdot 2$, and so the index of the 3-adic Galois representation of E/L is divisible by at least $3^{2k-1} \cdot 8$. By [**11**, lemma 4·5], we have $3^{2k-1} \cdot 8 \mid [\mathrm{GL}_2(\mathbb{Z}_3) : \mathrm{im}\rho_{E_0/\mathbb{Q},3^\infty}] \cdot [L \cap \mathbb{Q}(E_0[3^\infty]) : \mathbb{Q}]$. It follows that $3^{2k-1-d} \mid [L \cap \mathbb{Q}(E_0[3^\infty]) : \mathbb{Q}]$. Since L is at worst a quadratic extension of F, then $3^{2k-1-d} \mid [F : \mathbb{Q}]$, contradicting our assumption. Thus, $\mathrm{im}\rho_{E/F,3^\infty} = \pi^{-1}(\mathrm{im}\rho_{E/F,3^k})$.

LEMMA 6·5 *Suppose F is a number field of odd degree and E/F is a non-CM elliptic curve with $P \in E(F)$ of order 3^k, $k \geq 2$. Let $\varphi : E \to E'$ be an F-rational isogeny of degree 3^r for $r \in \mathbb{Z}^+$, where there exists $E_0/\mathbb{Q}$ with $j(E_0) = j(E')$ and $d := \mathrm{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \mathrm{im}\rho_{E_0,3^\infty}])$. If $3^{\max(0,2k-1-d)} \nmid [F : \mathbb{Q}]$, then $r \leq k$ and $\ker(\varphi) \subseteq \langle P \rangle$.*

Proof. Suppose $3^{\max(0,2k-1-d)} \nmid [F : \mathbb{Q}]$, so $2k - 1 - d > 0$. First, suppose for the sake of contradiction that $r > k$. Then

$$\mathrm{im}\rho_{E,3^r} \neq \pi^{-1}(\mathrm{im}\rho_{E,3^k}),$$

and by Lemma 6·4 we have $3^{2k-1-d} \mid [F : \mathbb{Q}]$. We have reached a contradiction. So $r \leq k$.

By assumption there exists $R \in E$ of order 3^r such that $\ker(\varphi) = \langle R \rangle$. With respect to the basis $\{3^{k-r}P, Q\}$ of $E[3^r]$, by Lemma 6·4 we may assume

$$\mathrm{im}\rho_{E/F,3^r} = \left\{ \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \mid x \in \mathbb{Z}/3^r\mathbb{Z}, y \in (\mathbb{Z}/3^r\mathbb{Z})^\times \right\}.$$

With respect to this basis, $R = \alpha 3^{k-r}P + \beta Q$ for some $\alpha, \beta \in \mathbb{Z}/3^r\mathbb{Z}$. We will show $\beta = 0$, from which we may conclude that $R \in \langle P \rangle$.

Since R has order 3^r, we must have $3 \nmid \alpha$ or $3 \nmid \beta$. First suppose $3 \nmid \alpha$. The F-rationality of $\langle R \rangle$ and description of $\mathrm{im}\rho_{E/F,3^r}$ as above implies there exists $\sigma \in \mathrm{Gal}_F$ and $\gamma_1 \in (\mathbb{Z}/3^r\mathbb{Z})^\times$ such that

$$\sigma(R) = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ 2\beta \end{pmatrix} = \begin{pmatrix} \gamma_1\alpha \\ \gamma_1\beta \end{pmatrix}.$$

So $\gamma_1 = 1$, which implies $\beta = 0$. Now suppose $3 \nmid \beta$. As before, there must exist $\gamma_2 \in (\mathbb{Z}/3^r\mathbb{Z})^\times$ such that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha + \beta \\ \beta \end{pmatrix} = \begin{pmatrix} \gamma_2\alpha \\ \gamma_2\beta \end{pmatrix}.$$

Again $\gamma_2 = 1$ and $\beta = 0$.

PROPOSITION 6·6. *Suppose F is a number field of odd degree and E/F is an elliptic curve with $P \in E(F)$ of order 3^k, $k \geq 2$. Let $\varphi : E \to E'$ be an F-rational isogeny, where there exists $E_0/\mathbb{Q}$ of with $j(E_0) = j(E')$ and $\mathrm{im}\rho_{E_0,3^\infty} = 9.36.0.6$ or $9.36.0.8$. Then $3^{2k-3} \mid [F : \mathbb{Q}]$.*

Proof. By [**18**, lemma A·1], we may assume φ is cyclic and generated by a point of order $3^r \cdot n$ where $3 \nmid n$. If $n > 1$, then by replacing E with an n-isogenous curve if necessary, we may assume φ has degree 3^r. If $\mathrm{im}\rho_{E_0,3^\infty} = 9.36.0.6$ or $9.36.0.8$, then

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

$\mathrm{ord}_3([\mathrm{GL}_2(\mathbb{Z}_3) : \mathrm{im}\rho_{E_0,3^\infty}]) = 2$. Suppose for the sake of contradiction that $3^{2k-3} \nmid [F : \mathbb{Q}]$. By Lemma 6·5, we have $r \leq k$ and $\ker(\varphi) \subseteq \langle P \rangle$.

First, suppose $r = k-1$ or k. Set $t = r+2$, and let $\{R, S\}$ be a basis of $E[3^t]$ such that $3^{t-k}R = P$ and $3^{t-k}S = Q$. Then we will show $\{\varphi(R), 3^{k-2}\varphi(Q)\}$ is a basis of $E'[\mathbf{9}]$. Suppose there exist $\alpha, \beta \in \mathbb{Z}/9\mathbb{Z}$ such that $\alpha\varphi(R) = \beta 3^{k-2}\varphi(Q)$. This implies $\alpha R - \beta 3^{k-2}Q \in \ker(\varphi) \subseteq \langle P \rangle = \langle 3^{t-k}R \rangle$. Thus $\beta 3^{t-s}S$ is in the cyclic subgroup generated by R, and so $3^2 \mid \beta$ since $\{R, S\}$ is a basis of $E[3^t]$. Thus $\alpha\varphi(R) = \beta 3^{k-2}\varphi(Q) = \mathcal{O}$, as desired.

By Lemma 6·4 with respect to the basis $\{P, Q\}$, there exists $\sigma \in \mathrm{Gal}_F$ such that

$$\rho_{E/F,3^k}(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}.$$

Also by Lemma 6·4 we have $\mathrm{im}\rho_{E/F,3^\infty} = \pi^{-1}(\mathrm{im}\rho_{E/F,3^k})$, so with respect to the basis $\{R, S\}$ of $E[3^t]$, we know there exists $\sigma' \in \mathrm{Gal}_F$ such that

$$\rho_{E/F,3^t}(\sigma') = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}.$$

Under the basis $\{\varphi(R), 3^{k-2}\varphi(Q)\}$ of $E'[\mathbf{9}]$,

$$\sigma'(\varphi(R)) = \varphi(\sigma'(R)) = \varphi(R)$$

$$\sigma'(3^{k-2}\varphi(Q)) = 3^{k-2}\varphi(\sigma'(Q)) = 4 \cdot 3^{k-2}\varphi(Q).$$

So

$$\rho_{E'/F,9}(\sigma') = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}.$$

After at worst a quadratic extension L/F, we have $E'/L \cong_L E_0/L$. Since the matrix above has order 3,

$$\rho_{E_0/L,9}(\sigma') = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}.$$

This means that the group generated by $\rho_{E_0/L,9}(\sigma')$ is conjugate to an order 3 subgroup of 9.36.0.6 or 9.36.0.8 mod 9, and a Magma computation shows no such subgroup exists.

Now, suppose $r \leq k-2$. Then $\{3^{k-r-2}\varphi(P), 3^{k-2}\varphi(Q)\}$ is a basis of $E'[\mathbf{9}]$ since $\ker(\varphi) \subseteq \langle P \rangle$. Since $P \in E(F)$, we have $3^{k-r-2}\varphi(P) \in E'(F)$. Moreover, for $\sigma \in \mathrm{Gal}_F$ as above,

$$\sigma(3^{k-2}\varphi(Q)) = 3^{k-2}\varphi(\sigma(Q)) = 4 \cdot 3^{k-2}\varphi(Q),$$

so

$$\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \in \mathrm{im}\rho_{E'/F,9}.$$

We reach a contradiction as before.

6·2. *Proof of Proposition 6·1*

Let $F = \mathbb{Q}(x)$. By Lemma 3·1, there is a model of E/F where $P \in E(F)$ and such that there exists an F-rational cyclic isogeny $\varphi : E \to E'$ with $j(E') \in \mathbb{Q}$. Replacing E with an isogenous curve if necessary, we may assume φ has degree 3^r. Since E has a 3-isogeny over

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

F, so does E' by [**18**, proposition 3·2]. It follows from [**18**, proposition 3·3] that any $E_0/\mathbb{Q}$ with $j(E_0) = j(E')$ has a $\mathbb{Q}$-rational cyclic 3-isogeny, and E_0 gives a degree 1 closed point on $X_1(3)$ by Proposition 2·3. By [**41**, corollary 1·3.1], the 3-adic image is one of the following groups, and we will consider each separately. Since we are interested in closed points on modular curves, and the degree of these points is not altered by taking quadratic twists, we may restrict to cases where $-I$ is contained in the 3-adic image.

(1) $\mathrm{im}\rho_{E_0,3^\infty} = 3.4.0.1$: since $d = 0$ and $\deg(X_1(3^k) \to X_1(3)) = 3^{2k-2}$, the divisibility condition of Proposition 3.2 is best possible for all $k \in \mathbb{Z}^+$, and one can take $j_{min} = j(E_0)$.

(2) $\mathrm{im}\rho_{E_0,3^\infty} = 3.12.0.1$ or $9.12.0.1$: if $\mathrm{im}\rho_{E_0,3^\infty} = 3.12.0.1$, then E_0 is 3-isogenous to an elliptic curve $E'/\mathbb{Q}$ with a rational cyclic 49-isogeny. By Proposition 3·5, the 3-adic Galois representation of E' is completely determined by $\rho_{E_0,3^\infty}$, and so it suffices to check a specific example. By viewing isogeny class 175.b in the LMFDB, we see that $\mathrm{im}\rho_{E',3^\infty} = 9.12.0.1$. Replacing E_0 with E' if necessary, we are free to assume E_0 has image 9.12.0.1. Thus E_0 corresponds to closed points on $X_1(3)$ and $X_1(9)$ of degree 1 and 3, respectively. Since $d = 1$ and $\deg(X_1(3^k) \to X_1(3)) = 3^{2k-2}$ for $k \geq 2$, the divisibility condition of Proposition 3.2 is best-possible for $k \in \mathbb{Z}^+$ and we can take $j_{min} = j(E_0)$.

(3) $\mathrm{im}\rho_{E_0,3^\infty} = 9.12.0.2$: a Magma computation shows that for $E_0/\mathbb{Q}$ with this image, there exists a cubic extension L such that E_0/L has an L-rational 9-isogeny and an independent 3-isogeny. Thus over L, the curve E_0 is 3-isogenous to E_1/L with a rational cyclic 27-isogeny. Thus E_1 gives a closed point on $X_1(27)$ of degree at most 27 by Proposition 2.3. Since $d = 1$ and $\deg(X_1(3^k) \to X_1(27)) = 3^{2k-6}$, the divisibility conditions of Proposition 3.2 are best-possible for all $k \geq 3$ with $j_{min} = j(E_1)$. No elliptic curve in $\mathcal{E}$ with $j \in \mathbb{Q}$ has a point of order 27 in this degree or lower.

(4) $\mathrm{im}\rho_{E_0,3^\infty} = 9.36.0.2$ or $27.36.0.1$: as in case (2), the isogeny class 304.c in the LMFDB shows we are free to assume E_0 has image 27.36.0.1. A Magma computation shows that for $E_0/\mathbb{Q}$ with this image, there exists a cubic extension L such that E_0/L has an L-rational 27-isogeny and an independent 3-isogeny. Thus over L, the curve E_0 is 3-isogenous to E_1/L with a rational cyclic 81-isogeny. Thus E_1 gives a closed point on $X_1(81)$ of degree at most 81 by Proposition 2.3. Since $d = 2$ and $\deg(X_1(3^k) \to X_1(81)) = 3^{2k-8}$, the divisibility conditions of Proposition 3.2 are best-possible for all $k \geq 4$ with $j_{min} = j(E_1)$. No elliptic curve in $\mathcal{E}$ with j-invariant in $\mathbb{Q}$ has a point of order 81 in this degree or lower.

(5) $\mathrm{im}\rho_{E_0,3^\infty} = 9.36.0.3$ or $9.36.0.6$: as in case (2), the isogeny class 22491.u in the LMFDB shows we are free to assume E_0 has image 9.36.0.6. Then $3^{\max(0,2k-3)} \mid [F{:}\mathbb{Q}]$ by Proposition 6.6. The conclusion follows with $j_{min} = j(E_0)$.

(6) $\mathrm{im}\rho_{E_0,3^\infty} = 9.36.0.1$, $9.36.0.4$ or $9.36.0.5$: as in case (2), the isogeny class 432.b in the LMFBD shows we are free to assume E_0 has image 9.36.0.4. A twist of E_0 has a rational point of order 9 and $d = 2$, so divisibility conditions of Proposition 3.2 are best possible for all $k \in \mathbb{Z}^+$ with $j_{min} = j(E_0)$.

(7) $\mathrm{im}\rho_{E_0,3^\infty} = 9.36.0.7$ or $9.36.0.9$: as in case (2), the isogeny class 1734.k in the LMFDB shows we are free to assume E_0 has image 9.36.0.7. A Magma computation shows that there exists a cubic extension L such that a twist E_0^t of E_0/L has an L-rational point of order 9 (say Q) and an independent 3-isogeny (say, with kernel

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

generated by R). Then $\psi : E_0^t \to E_1 = E_0^t/\langle R\rangle$ is a degree 3 isogeny, where E_1 has an L-rational cyclic 27-isogeny and $\psi(Q) \in E_1(F)$ is a point of order 9. Moreover, $\psi(Q)$ is in the kernel of the rational 27-isogeny. Thus the image of the 27-isogeny character χ associated to E_1/L lands in $\{1, 10, 19\}$ and E_1 attains a point of order 27 in $\overline{L}^{\ker(\chi)}$, an extension of L of degree dividing 3. Hence E_1 corresponds to a point on $X_1(27)$ of degree dividing 9. Since $d = 2$, the divisibility conditions of Proposition 3.2 are best-possible for $k \geq 3$ with $j_{min} = j(E_1)$. No elliptic curve in $\mathcal{E}$ with j-invariant in $\mathbb{Q}$ has a point of order 27 in this degree or lower.

(8) $\mathrm{im}\rho_{E_0,3^\infty} = 9.36.0.8$: by Proposition 6.6, we have $3^{\max(0,2k-3)} \mid [F : \mathbb{Q}]$. A Magma computation shows that for $E_0/\mathbb{Q}$ with this image, there exists a cubic extension L such that E_0/L has an L-rational 9-isogeny and an independent 3-isogeny. As in case (3), there exists E_1 which is 3-isogenous to E_0 and gives a closed point on $X_1(27)$ of degree at most 27. Thus the divisibility conditions of Proposition 6.6 are best-possible for $k \geq 3$ with $j_{min} = j(E_1)$. No elliptic curve in $\mathcal{E}$ with j-invariant in $\mathbb{Q}$ has a point of order 27 in this degree or lower.

It remains to consider $k = 2$ if $\mathrm{im}\rho_{E_0,3^\infty} = 9.12.0.2, 9.36.0.2, 9.36.0.7$ or $9.36.0.8$ and $k = 3$ if $\mathrm{im}\rho_{E_0,3^\infty} = 9.36.0.2$. By Corollary 3.6, results can be obtained by choosing a particular elliptic curve $E_0/\mathbb{Q}$ with this Galois image and computing the degrees of closed points on $X_1(3^k)$ for elliptic curves 3^r-isogenous to E_0, where the j-invariants of the isogenous curves are roots of the modular polynomial $\Phi_{3^r}(X, j(E_0))$. For r sufficiently large, any odd degree point on $X_1(3^k)$ associated to an elliptic curve 3^r-isogenous to E_0 will have degree divisible by 3δ, so there are only finitely many curves to test. We do this computation in Magma.

7. *Results for non-CM classes and $\ell = 2$*

Any non-CM $\mathbb{Q}$-curve defined over a number field of odd degree is geometrically isogenous to an elliptic curve with rational j-invariant, by work of Cremona and Najman [**18**, theorem 2·7]. Thus the following can be viewed as a strengthening of [**11**, proposition 4·1], which shows that if a non-CM $\mathbb{Q}$-curve has a point of order 2^k over a field of odd degree then $k \leq 4$. There exist non-CM elliptic curves over $\mathbb{Q}$ with a rational point of order 8, so the following gives the best possible bound. The following proposition proves Theorem 1·4 in the case of $\ell = 2$.

PROPOSITION 7·1. *Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves. If $E \in \mathcal{E}$ and $x = [E, P] \in X_1(2^k)$ is a point of odd degree, then $k \leq 3$. Moreover*:

(i) *the least odd degree of a point on $X_1(2)$ associated to $\mathcal{E}$ is* 1 *or* 3*, depending on whether there exists $E'/\mathbb{Q} \in \mathcal{E}$ with a rational point of order* 2;

(ii) *if there exists an odd degree point on $X_1(4)$ associated to $\mathcal{E}$, then the least such degree is* 1 *or* 3*. The least degree is* 1 *if and only if there exists $E'/\mathbb{Q} \in \mathcal{E}$ with a rational point of order* 4*. The least odd degree is 3 if and only if there exists $E'/\mathbb{Q} \in \mathcal{E}$ full* 2*-torsion over a cubic field or with* $\mathrm{im}\rho_{E',2^\infty} = 4.8.0.2$;

(iii) *if there exists an odd degree point on $X_1(8)$ associated to $\mathcal{E}$, then the least such degree is* 1*. This occurs if and only if there exists $E'/\mathbb{Q} \in \mathcal{E}$ with a rational point of order* 8.

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

We can take $j_{min} \in \mathbb{Q}$ unless there exists $E'/\mathbb{Q} \in \mathcal{E}$ full 2-torsion over a cubic field, in which case j_{min} is 2-isogenous to a rational j-invariant and defines a cubic extension.

Proof. Suppose for the sake of contradiction that $x \in X_1(16)$ is a point of odd degree, and let $F := \mathbb{Q}(x)$. By Lemma 3·1, there exists a model of E/F for which $P \in E(F)$ and such that there exists a rational cyclic isogeny $\varphi : E \to E'$ with $j(E') \in \mathbb{Q}$. If $\deg(\varphi) = 2^r \cdot n$ for $n > 1$ odd, we replace E with an n-isogenous elliptic curve so we may assume φ has degree 2^r.

The dual isogeny $\hat{\varphi} : E' \to E$ is also cyclic of degree 2^r, and so E' possesses an F-rational cyclic subgroup of order 2^r. Rational subgroups are twist-invariant, so any elliptic curve $E_0/\mathbb{Q}$ with $j(E_0) = j(E')$ will possess an F-rational subgroup of order 2^r, say generated by Q. It follows that $2^{r-1}Q$ is F-rational. Since F has odd degree, it must be that $[\mathbb{Q}(2^{r-1}Q) : \mathbb{Q}] = 1$ or 3. If $r = 1$, then it follows $\mathbb{Q}(\langle Q \rangle) = \mathbb{Q}(2^{r-1}Q)$. Otherwise, by [**18**, proposition 3·6],

$$[\mathbb{Q}(\langle Q \rangle) : \mathbb{Q}(\langle 2Q \rangle)] \leq 2.$$

Since $\mathbb{Q}(\langle Q \rangle)$ is contained if F, it must be of odd degree, and so $\mathbb{Q}(\langle Q \rangle) = \mathbb{Q}(\langle 2^{r-1}Q \rangle) = \mathbb{Q}(2^{r-1}Q)$. In either case, $\mathbb{Q}(\langle Q \rangle)$ is of degree 1 or 3. If $\mathbb{Q}(\langle Q \rangle) = \mathbb{Q}$, then $j(E) \in \mathbb{Q}$ and this contradicts [**10**, theorem 3]. Thus $\mathbb{Q}(\langle Q \rangle)$ is of degree 3.

Next, we will show $r = 1$. If not, then both $\langle 2^{r-2}Q \rangle$ and $2^{r-1}Q$ generate the same degree 3 extension of $\mathbb{Q}$. By Proposition 2·3, the elliptic curve E_0 has a closed point of degree 3 on $X_1(4)$ lying above a degree 3 point on $X_1(2)$. By the classification of 2-adic images due to Rouse and Zureick-Brown [**42**], this implies E_0 has 2-adic image X20b, X20a, or X20; see the data file associated to Corollaries 3·4 and 3·5 of [**29**]. These groups have RSZB labels 4.16.0.2, 8.16.0.3 and 4.8.0.2, respectively. Thus $\mathrm{ord}_2([\mathrm{GL}_2(\mathbb{Z}_2) : \mathrm{im}\rho_{E_0,2^\infty}]) = 3$ or 4. However, this implies the degree of F is even by Proposition 3·2. Therefore $r = 1$ and Q has order 2.

Thus φ is of degree 2, and $\varphi(P)$ is a point of order at least 8 defined over F. This guarantees the existence of a closed point $y \in X_1(4)$ associated to E' with $\deg(y)$ odd. Since E_0 gives a degree 3 point on $X_1(2)$, so does E', and so $\deg(y)$ is an odd multiple of 3. As $\deg(X_1(4) \to X_1(2)) = 2$, this implies $\deg(y) = 3$. But then we are again in the case where E_0 gives a closed point of degree 3 on $X_1(4)$ lying above a degree 3 point on $X_1(2)$. As above, $\mathrm{ord}_2([\mathrm{GL}_2(\mathbb{Z}_2) : \mathrm{im}\rho_{E_0,2^\infty}]) = 3$ or 4 and we reach a contradiction via Proposition 3·2.

Finally, we will prove the refined degree bounds for each $k \leq 3$. As above, suppose $x \in X_1(2^k)$ is a point of odd degree associated to $E \in \mathcal{E}$ and $F := \mathbb{Q}(x)$. We may assume there is an F-rational cyclic isogeny $\varphi : E \to E'$ of degree 2^r with $j(E') \in \mathbb{Q}$, where $E(F)$ has a point of order 2^k. Let $E_0/\mathbb{Q}$ with $j(E_0) = j(E')$. By the second paragraph, if E_0 has a rational point of order 2, then $j(E) \in \mathbb{Q}$ and E gives a closed point of degree 1 on $X_1(2)$ by [**18**, proposition 3·2]. By [**30**, proposition 4·6], the only odd degree closed points on $X_1(2^k)$ associated to E have degree 1. So it suffices to consider the case when E_0 has no rational point of order 2.

The results for $X_1(2)$ are immediate, so suppose $2 \leq k \leq 3$. By [**11**, lemma 6·3], the curve $E_0/\mathbb{Q} \in \mathcal{E}$ has full 2-torsion or a 4-isogeny defined over a number field of odd degree. Since $E_0(\mathbb{Q})$ has no point of order 2, these conditions occur if E_0 has $\mathrm{im}\rho_{E_0,2} = 2\mathrm{Cn}$ or if $\mathrm{im}\rho_{E_0,2^\infty} \in \{4.16.0.2, 8.16.0.3, 4.8.0.2\}$, respectively, as above. In either case, E_0 or an elliptic curve 2-isogenous to E_0 has a cyclic 4-isogeny defined over a cubic field. This gives a degree 3 closed point on $X_1(4)$ by Proposition 2·3. However, we will show no point on $X_1(8)$ associated to $\mathcal{E}$ has odd degree.

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

By replacing E_0 by a quadratic twist if necessary, we may assume the 2-adic image contains $-I$. Thus we may assume $\mathrm{im}\rho_{E_0,2^\infty} = 2.2.0.1$ or $4.8.0.2$; see [**42**] for curves that minimally cover X2 and X20. In the first, there are no odd degree points on $X_1(8)$ associated to $\mathcal{E}$ by Proposition 3·2, so assume $\mathrm{im}\rho_{E_0,2^\infty} = 4.8.0.2$. By Corollary 36, results can be obtained by choosing a particular elliptic curve with this Galois image and computing the degrees of points on $X_1(8)$ for elliptic curves 2^r-isogenous to E_0, where the j-invariants of the isogenous curves are roots of the modular polynomial $\Phi_{2^r}(X, j(E_0))$. A Magma computation shows that 2 divides the degree of a point on $X_1(8)$ associated to any elliptic curve 2^r-isogenous to E_0 for $r \in \mathbb{Z}^+$, as desired.

8. *ℓ-adic images of level ℓ*

PROPOSITION 8·1. *Let $\mathcal{E}$ be a rational $\overline{\mathbb{Q}}$-isogeny class of non-CM elliptic curves and let ℓ be prime. Suppose there exists $E_0/\mathbb{Q} \in \mathcal{E}$ with ℓ-adic Galois representation of level ℓ. Among points on $X_1(\ell^k)$ associated to $\mathcal{E}$, a point of least degree can always be associated to $j_{min} \in \mathcal{E}$ which is at most ℓ-isogenous to a rational j-invariant.*

Proof. If $\mathrm{im}\rho_{E_0,\ell}$ is surjective, this follows from Proposition 3·2 and the formula for $\deg(X_1(\ell^k) \to X_1(\ell))$; see Proposition 2·6. Suppose ℓ is odd. If $E_0/\mathbb{Q}$ has a rational ℓ-isogeny, then the result follow from Lemma 5·3 if $\ell \geq 5$ and the proof of Proposition 6·1 if $\ell = 3$; see cases (i) and (ii).

If $E_0/\mathbb{Q}$ has no rational ℓ-isogeny and $\mathrm{im}\rho_{E_0,\ell}$ is not surjective, then $\mathrm{im}\rho_{E_0,\ell^\infty}$ is the complete preimage of one of the following groups (see Section 2.2). One may check that $\mathrm{ord}_\ell([\mathrm{GL}_2(\mathbb{Z}_\ell) : \mathrm{im}\rho_{E_0,\ell^\infty}]) = 1$. We will consider each case separately. We will see $j_{min} \notin \mathbb{Q}$ in each case.

(i) $C_{ns}^+(\ell)$: this is a subgroup of order $2(\ell^2 - 1)$, and up to a choice of basis it contains all matrices

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \not\equiv 0 \pmod{\ell},$$

$$\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}, a \not\equiv 0 \pmod{\ell}.$$

Since ℓ is odd, these matrices form a group of order $2(\ell - 1)$. Its fixed field has size $\ell + 1$, so over an extension of degree $\ell + 1$, the curve E_0 attains two independent ℓ-isogenies with kernels C_1 and C_2. Then by Proposition 2·3, the curve E_0/C_1 attains a closed point on $X_1(\ell)$ in degree dividing $(\ell + 1) \cdot \varphi(\ell)/2 = (\ell^2 - 1)/2$ and a closed point on $X_1(\ell^2)$ in degree dividing $(\ell + 1) \cdot \varphi(\ell^2)/2 = (\ell^2 - 1) \cdot \ell/2$. Since all closed points on $X_1(\ell)$ associated to E_0 have degree $(\ell^2 - 1)/2$, the claim holds by Propositions 3·2 and 2·6 with $j_{min} = j(E_0/C_1)$.

(ii) 13S4, 5S4: a Magma computation shows the curve E_0 attains two independent ℓ-isogenies in degree 6 with kernels C_1 and C_2. By Proposition 2·3, the curve E_0/C_1 attains a closed point on $X_1(\ell)$ in degree dividing $6 \cdot (\varphi(\ell)/2) = 3(\ell - 1)$ and a closed point on $X_1(\ell^2)$ in degree dividing $6 \cdot (\varphi(\ell^2)/2) = 3\ell(\ell - 1)$. The claim holds by Propositions 3·2 and 2·6 with $j_{min} = j(E_0/C_1)$.

(iii) 7Ns, 7Ns.2.1, 7Ns.3.1, 5Ns, 5Ns.2.1, 3Ns: the curve E_0 picks up 2 independent ℓ-isogenies in degree 2 with kernels C_1 and C_2. By Proposition 2·3, the curve

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

E_0/C_1 attains a closed point on $X_1(\ell)$ in degree dividing $2 \cdot (\varphi(\ell)/2) = \ell - 1$ and a closed point on $X_1(\ell^2)$ in degree dividing $2 \cdot (\varphi(\ell^2)/2) = \ell(\ell - 1)$. The claim holds by Propositions 3·2 and 2·6 with $j_{min} = j(E_0/C_1)$.

Now suppose $\ell = 2$. If $\mathrm{im}\rho_{E_0,2} = 2\mathrm{Cs}$, then E_0 has full 2-torsion over $\mathbb{Q}$. Hence it is isogenous over $\mathbb{Q}$ to an elliptic curve $E'/\mathbb{Q}$ with a $\mathbb{Q}$-rational cyclic 4-isogeny. By Proposition 2·3, there is a degree 1 closed point on $X_1(4)$ associated to E', and the claim follows from Proposition 3·2 and the formula for $\deg(X_1(2^k) \to X_1(4))$. If $\mathrm{im}\rho_{E_0,2} = 2\mathrm{B}$ or $2\mathrm{Cn}$, then E_0 has full 2-torsion over an extension K of degree 2 or 3, respectively. There is E'/K with a K-rational cyclic 4-isogeny, and the claim follows as in the previous case.

Remark 8·2. The expression for the least degree does not necessarily divide all degrees. For example, the proof of Proposition 8·1 shows that the least degree of a point on $X_1(7^k)$ associated to $\mathcal{E}$ containing $E_0/\mathbb{Q}$ with $\mathrm{im}\rho_{E_0,7^\infty} = 7.28.0.1$ is $7^{\max(0,2k-3)} \cdot 6$. However, there is a closed point on $X_1(7)$ associated to E_0 of degree 9, and points on $X_1(7^k)$ lying above this point will not have degree divisible by $7^{\max(0,2k-3)} \cdot 6$.

The next result shows that working with curves in a non-CM rational geometric isogeny class $\mathcal{E}$ can yield points of strictly lower degree than those associated with any rational non-CM j-invariant. This relies on recent work of Furio [**24**], as applied in work of the first author with Ejder [**12**].

COROLLARY 8·3. *The least degree of a point on* $X_1(49)$ *associated to any non-CM rational* $\overline{\mathbb{Q}}$*-isogeny class* $\mathcal{E}$ *is at most* 42*, whereas the least degree of a non-CM point* $x \in X_1(49)$ *with* $j(x) \in \mathbb{Q}$ *is* 49.

Proof. The first claim follows from the previous proposition: consider, for example, an elliptic curve over $\mathbb{Q}$ with mod 7 image 7Ns. For the second claim, note that all known non-surjective 7-adic images for non-CM elliptic curves $E/\mathbb{Q}$ have level 7; see [**42**]. Thus any point on $X_1(49)$ associated to such an E has degree at least 49. Equality holds for any elliptic curve over $\mathbb{Q}$ with a rational point of order 7. If $E/\mathbb{Q}$ has surjective 7-adic image, then E gives a single closed point on $X_1(49)$ of degree 1176. By [**41**, theorem 1·1·6] and [**25**, theorem 1·4], other groups which could occur as 7-adic images for non-CM elliptic curves over $\mathbb{Q}$ would give rise to rational points on the modular curves with RSZB label 49.147.9.1 or 49.196.9.1. In the first case, such an $E/\mathbb{Q}$ would have mod 7 image landing in the normaliser of a non-split Cartan subgroup. Possible 7-adic images for E are given in [**24**, theorem 1·9], and the last paragraph of the proof of Theorem 6 in [**12**] shows E gives a point on $X_1(49)$ of degree at least 168. Finally, if $E/\mathbb{Q}$ corresponds to a rational point on the modular curve labeled 49.196.9.1, then $\mathrm{im}\rho_{E,7^\infty} = 49.196.9.1$ by [**12**, corollary 3]. Such an image gives points on $X_1(49)$ of degree at least 294.

9. *CM elliptic curves*

Let $\mathcal{E}$ be a $\overline{\mathbb{Q}}$-isogeny class of CM elliptic curves. The endomorphism algebra $K = \mathrm{End}(E) \otimes \mathbb{Q}$ is an isogeny invariant, so all elliptic curves in $\mathcal{E}$ have CM by an order in the imaginary quadratic field K. In fact, since any CM elliptic curve is isogenous to one with CM by the maximal order (see, for example, [**13**, proposition 2·2]), the class $\mathcal{E}$ contains elliptic

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

curves with CM by any possible order in K. In this section, we study the isogeny distance from a minimal torsion curve to an elliptic curve E with CM by the full ring of integers in K, since $[\mathbb{Q}(j(E)):\mathbb{Q}]$ is minimal for $\mathcal{E}$. This builds on work of the first author and Clark [6, 7]. A key first step is to establish sharp lower bounds on the least degree of a point on $X_1(\ell^k)$ associated to $\mathcal{E}$. These appear as Propositions 9·1, 9·2 and 9·3. Taken together they imply Theorem 1·1. Preliminary results about CM elliptic curves are summarised in Section 2·5.

Throughout this section $w_K = \#\mathcal{O}_K^\times$ and h_K denotes the class number of K.

9·1. *ℓ split in K*

PROPOSITION 9·1. *Let $\mathcal{E}$ be a $\overline{\mathbb{Q}}$-isogeny class of elliptic curves with CM by orders in the imaginary quadratic field K, and let ℓ be a prime split in K. Then the least degree of a point on $X_1(\ell^n)$ associated to $\mathcal{E}$ is*

$$2 \cdot h_K \cdot \ell^{n-1}(\ell - 1)/w_K,$$

and this is attained by $E \in \mathcal{E}$ with CM by the maximal order in K. Thus $[\mathbb{Q}(j_{min}) : \mathbb{Q}] = h_K$.

Proof. That such an E gives a point on $X_1(\ell^n)$ in this degree follows from [7, theorem 6.2] and $[\mathbb{Q}(j(E)) : \mathbb{Q}] = h_K$ by Section 2·5; note that $\ell > 3$ if $\Delta = -3, -4$ by the assumption that ℓ is split in K. It remains to show this is the least possible degree among all $E' \in \mathcal{E}$. We may assume $\ell^n > 2$. Since the endomorphism algebra is an isogeny invariant, any $E' \in \mathcal{E}$ has CM by an order in K. Since we already have the least degree for a point with CM by the maximal order, we will henceforth assume E' has CM by an order in K of conductor $\mathfrak{f} > 1$. For any point $x = [E', P'] \in X_1(\ell^n)$, by [6, theorem 6·2] we have

$$h_K \cdot \frac{\ell^{n-1}(\ell - 1)}{2} \mid \deg(x).$$

If $\deg(x) = h_K \cdot (\ell^{n-1}(\ell - 1)/2) \cdot d < 2 \cdot h_K \cdot (\ell^{n-1}(\ell - 1)/w_K)$ for some $d \in \mathbb{Z}^+$, it must be that $d = 1$ and $w_K = 2$. This implies $[\mathbb{Q}(j(E')) : \mathbb{Q}] = h_K$. The degree of this extension is equal to the class number of the order $\mathcal{O}$; see Equation 2·1 in Section 2·5. Since $w_K = 2$, then $[\mathbb{Q}(j(E')) : \mathbb{Q}] = h_K$ implies E' has CM by an order in K of conductor dividing 2. Since we have assumed E' has CM by an order of conductor $\mathfrak{f} > 1$, we will suppose E' has CM by the order in K of conductor 2. By Equation 2·1, this can happen only if 2 is split in K. But this contradicts [7, theorem 6·2] if ℓ is odd and [7, theorem 6·6] if $\ell = 2$.

9·2. *ℓ inert in K*

PROPOSITION 9·2. *Let $\mathcal{E}$ be a $\overline{\mathbb{Q}}$-isogeny class of elliptic curves with CM by orders in the imaginary quadratic field K, and let ℓ be a prime inert in K. The least degree of a point on $X_1(\ell^n)$ associated to $\mathcal{E}$ is*

$$\delta := \begin{cases} h_K \cdot \ell^{\lfloor 3(n-1)/2 \rfloor + 1}(\ell^2 - 1)/w_K \text{ if } \ell = 2, \\ h_K \cdot \ell^{\lfloor 3(n-1)/2 \rfloor}(\ell^2 - 1)/w_K \text{ if } \ell \geq 3. \end{cases}$$

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

This is attained by $E \in \mathcal{E}$ with CM by an order in K of conductor $\mathfrak{f} = \ell^{\lfloor n/2 \rfloor}$. Moreover, if j_{min} is the j-invariant of a minimal torsion curve of level ℓ^n and $n \geq 5$, then

$$[\mathbb{Q}(j_{min}) : \mathbb{Q}] \geq h_K \cdot \frac{\ell^{(n-5)/2}}{3}(\ell + 1).$$

Thus $[\mathbb{Q}(j_{min}) : \mathbb{Q}] \to \infty$ as $n \to \infty$.

Proof. Suppose E has CM by the order in K of conductor $\mathfrak{f} = \ell^{\lfloor n/2 \rfloor}$. Note we can find such an $E \in \mathcal{E}$ by the first paragraph of Section 9. Then by [7, theorem 6·1, Theorem 6·6], the point $x \in X_1(\ell^n)$ of least degree associated to such an E has

$$\deg(x) = 2^{\epsilon} \cdot T(\mathcal{O}, \ell^n) \cdot h(\mathcal{O}),$$

where $T(\mathcal{O}, \ell^n)$ is as defined in [7, theorem 4·1] and $\epsilon = 1$ if $\ell = 2$, $n > 1$ and $\epsilon = 0$ otherwise. Evaluating $T(\mathcal{O}, \ell^n)$ via [7, theorem 4·1] and $h(\mathcal{O})$ with Equation 2·1 shows $\deg(x) = \delta$.

Now we will justify that this is the least possible degree of a point on $X_1(\ell^n)$ associated to $\mathcal{E}$. Suppose $E' \in \mathcal{E}$ has CM by the order of conductor $\ell^c \mathfrak{f}'$ in $\mathcal{O}_K$ where $\ell \nmid \mathfrak{f}'$. By [7, theorem 4·1, Theorem 6·1] and Equation (2·1), the least degree of a point on $X_1(\ell^n)$ associated to E' is at least δ, and this inequality is strict if $c < (n-3)/2$. Thus, any minimal torsion curve of level ℓ^n must have $c \geq (n-3)/2$. If $n \geq 5$, then $[\mathbb{Q}(j_{min}) : \mathbb{Q}] \geq h_K \cdot ((\ell^{(n-5)/2})/3)(\ell + 1)$ by Equation 2·1 in Section 2·5. The conclusion follows.

9·3. *ℓ ramified in K*

PROPOSITION 9·3. *Let $\mathcal{E}$ be a $\overline{\mathbb{Q}}$-isogeny class of elliptic curves with CM by orders in the imaginary quadratic field K, and let ℓ be a prime ramified in K. Then the least degree of a point on $X_1(\ell^n)$ associated to $\mathcal{E}$ is*

$$\delta := \begin{cases} h_K \text{ if } \ell^n \leq 3, \\ h_K \cdot \ell^{\lfloor 3(n-1)/2 \rfloor + 1}(\ell - 1)/w_K \text{ if } \ell = 2, n > 1, \operatorname{ord}_2(\Delta_K) = 2, \\ h_K \cdot \ell^{\lfloor 3n/2 \rfloor - 1}(\ell - 1)/w_K \text{ otherwise.} \end{cases}$$

The least degree is attained by $E \in \mathcal{E}$ with CM by an order in K of conductor $\mathfrak{f} = \ell^{\lfloor n/2 \rfloor}$. Also, for any j-invariant j_{min} of a minimal torsion curve of level ℓ^n and $n \geq 5$, one has

$$[\mathbb{Q}(j_{min}) : \mathbb{Q}] \geq h_K \cdot \frac{\ell^{(n-3)/2}}{3}.$$

Thus $[\mathbb{Q}(j_{min}) : \mathbb{Q}] \to \infty$ as $n \to \infty$.

Proof. Suppose E has CM by an order in K of conductor $\mathfrak{f} = \ell^{\lfloor n/2 \rfloor}$; we can find such an $E \in \mathcal{E}$ by the first paragraph of Section 9. Then by [7, theorem 6·6] the least degree $x \in X_1(\ell^n)$ associated to E is

$$\deg(x) = 2^{\epsilon} \cdot T(\mathcal{O}, \ell^n) \cdot h(\mathcal{O}),$$

where $T(\mathcal{O}, \ell^n)$ is as defined in [7, theorem 4·1] and $\epsilon = 1$ if $\operatorname{ord}_2(\Delta_K) = 2$, $\ell = 2$, n an odd integer greater than 1 and $\epsilon = 0$ otherwise. Evaluating $T(\mathcal{O}, \ell^n)$ via [7, theorem 4·1] and replacing $h(\mathcal{O})$ with the formula in Equation 2·1 of Section 2.5 shows $\deg(x) = \delta$.

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

Now we will justify that this is the least possible degree of a point on $X_1(\ell^n)$ associated to $\mathcal{E}$. Suppose $E' \in \mathcal{E}$ has CM by the order of conductor $\ell^c \mathfrak{f}'$ in $\mathcal{O}_K$ where $\ell \nmid \mathfrak{f}'$. By [7, theorem 4·1, Theorem 6·6] and Equation (2·1), the least degree of a point on $X_1(\ell^n)$ associated to E' is at least δ, and this inequality is strict if $c < (n-3)/2$. Thus any minimal torsion curve of level ℓ^n must have $c \geq (n-3)/2$, meaning $[\mathbb{Q}(j_{min}) : \mathbb{Q}] \geq h_K \cdot (\ell^{(n-3)/2}/3)$ by Equation (2·1) in Section 2·5. The conclusion follows.

Acknowledgements. We thank John Cremona, Álvaro Lozano-Robledo, Jeremy Rouse, Parker Schwartz and Andrew Sutherland for helpful conversations. We thank John Cremona, Michael Eddy, Tyler Genao and Filip Najman for helpful comments on an earlier version of this paper. We are especially grateful to the anonymous referee, who made many comments and suggestions with greatly improved the exposition. All authors were supported by NSF grant DMS-2137659. The first author was partially supported by an A. J. Sterge Faculty Fellowship and NSF grant DMS-2145270.

REFERENCES

[1] N. ADZAGA, T. KELLER, P. MICHAUD-JACOBS, F. NAJMAN, E. OZMAN and B. VUKOREPA. Computing quadratic points on modular curves $X_0(N)$. *Math. Comp.* **93**(347) (2024), 1371–1397.
[2] 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.
[3] J. S. BALAKRISHNAN and B. MAZUR. Ogg's torsion conjecture: fifty years later. Bull. Amer. Math. Soc. (N.S.) **62**(2) (2025), 235–268.
[4] Y. BILU, P. PARENT and M. REBOLLEDO. Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)* **63**(3) (2013), 957–984.
[5] W. BOSMA, J. CANNON and C. PLAYOUST. *The Magma algebra system. I. The user language*, vol. 24 (1997). Computational algebra and number theory (London, 1993), pp. 235–265.
[6] A. BOURDON and P. L. CLARK. Torsion points and Galois representations on CM elliptic curves. *Pacific J. Math.* **305**(1) (2020), 43–88.
[7] A. BOURDON and P. L. CLARK. Torsion points and isogenies on CM elliptic curves. *J. London Math. Soc. (2)* **102**(2) (2020), 580–622.
[8] A. BOURDON, P. L. CLARK and J. STANKEWICZ. Torsion points on CM elliptic curves over real number fields. *Trans. Amer. Math. Soc.* **369**(12) (2017), 8457–8496.
[9] A. BOURDON, O. EJDER, Y. LIU, F. ODUMODU and B. VIRAY. On the level of modular curves that give rise to isolated j-invariants. *Adv. Math.* **357** (2019), 106824, 33.
[10] A. BOURDON, D. R. GILL, J. ROUSE and L. D. WATSON. Odd degree isolated points on $X_1(N)$ with rational j-invariant. *Res. Number Theory* 10(1) (2024), paper no. 5, 32.
[11] A. BOURDON and F. NAJMAN. Sporadic points of odd degree on $X_1(N)$ coming from $\mathbb{Q}$-curves. *Preprint:* arXiv:2107.10909, to appear in Algebra & Number Theory.
[12] A. BOURDON and ÖZLEM EJDER. Rational isolated j-invariants from $X_1(\ell^n)$ and $X_0(\ell^n)$. *Preprint:* arXiv:2506.19560, to appear in Res. Number Theory.
[13] A. BOURDON and P. POLLACK. Torsion subgroups of CM elliptic curves over odd degree number fields. *Int. Math. Res. Not. IMRN* (2017), no. 16, 4923–4961.
[14] P. L. CLARK. CM elliptic curves: volcanoes, reality, and applications. *Preprint:* arXiv:2212.13316.
[15] P. L. CLARK, T. GENAO, P. POLLACK and F. SAIA. The least degree of a CM point on a modular curve. *J. Lond. Math. Soc.* (2) **105**(2) (2022), 825–883.
[16] The LMFDB Collaboration. The L-functions and modular forms database, (2023). Available at lmfdb.org.
[17] D. A. COX. *Primes of the Form $x^2 + ny^2$*. (A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989). Fermat, class field theory and complex multiplication.
[18] J. E. CREMONA and F. NAJMAN. $\mathbb{Q}$-curves over odd degree number fields. *Res. Number Theory* **7**(4) (2021), paper no. 62, 30.

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

[19] P. DELIGNE and M. RAPOPORT. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*. Lecture Notes in Math., vol. 349, (Springer, Berlin 1973), pp. 143–316.
[20] M. DERICKX, A. ETROPOLSKI, M. VAN HOEIJ, J. S. MORROW and D. ZUREICK-BROWN. Sporadic cubic torsion. *Algebra Number Theory* **15**(7) (2021), 1837–1864.
[21] M. DERICKX and F. NAJMAN. Classification of torsion of elliptic curves over quartic fields. *Preprint:* arXiv:2412.16016.
[22] F. DIAMOND and J. IM. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994). CMS Conf. Proc.*, vol. 17 (Amer. Math. Soc., Providence, RI, 1995), pp 39–133.
[23] F. DIAMOND and J. SHURMAN. *A first course in modular forms*. Graduate Texts in Math., vol. 228 (Springer-Verlag, New York, 2005).
[24] L. FURIO. Effective bounds for adelic galois representations attached to elliptic curves over the rationals. *Preprint:* arXiv:2412.10340.
[25] L. FURIO and D. LOMBARDO. On 7-adic Galois representations for elliptic curves over $\mathbb{Q}$. *Preprint:* arXiv:2507.17967.
[26] L. FURIO and D. LOMBARDO. Serre's uniformity question and proper subgroups of $C_{ns}^{+}(p)$. *Preprint:* arXiv:2305.17780, to appear in Algebra & Number Theory.
[27] T. GENAO. Typically bounding torsion on elliptic curves isogenous to rational j-invariant. *Proc. Amer. Math. Soc.* **151**(5) (2023), 1907–1914.
[28] T. GENAO. Polynomial bounds on torsion from a fixed geometric isogeny class of elliptic curves. *J. Théor. Nombres Bordeaux* **36**(2) (2024), 661–670.
[29] E. GONZÁLEZ-JIMÉNEZ and A. LOZANO-ROBLEDO. On the minimal degree of definition of p-primary torsion subgroups of elliptic curves. *Math. Res. Lett.* **24**(4) (2017), 1067–1096.
[30] E. GONZÁLEZ-JIMÉNEZ and F. NAJMAN. Growth of torsion groups of elliptic curves upon base change. *Math. Comp.* **89**(323) (2020), 1457–1485.
[31] R. GREENBERG, K. RUBIN, A. SILVERBERG and M. STOLL. On elliptic curves with an isogeny of degree 7. *Amer. J. Math.* **136**(1) (2014), 77–109.
[32] R. GREENBERG. The image of Galois representations attached to elliptic curves with an isogeny. *Amer. J. Math.* **134**(5) (2012), 1167–1196.
[33] H. HEILBRONN. On the class-number in imaginary quadratic fields. *Quart. J. Math.* **os-5**(1) (1934), 150–160.
[34] S. KAMIENNY. Torsion points on elliptic curves over all quadratic fields. *Duke Math. J.* **53**(1) (1986), 157–162.
[35] S. KAMIENNY. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.* **109**(2) (1992), 221–229.
[36] M. A. KENKU and F. MOMOSE. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.* **109** (1988), 125–149.
[37] 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.
[38] A. LOZANO-ROBLEDO. Galois representations attached to elliptic curves with complex multiplication. *Algebra Number Theory* **16**(4) (2022), 777–837.
[39] B. MAZUR. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.* (1977), **33–186** (1978).
[40] B. MAZUR. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.* **44**(2) (1978), 129–162.
[41] 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), paper no. e62, 63. With an appendix with John Voight.
[42] J. ROUSE and D. ZUREICK-BROWN. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Res. Number Theory* **1** (2015), Art. 12, 34.
[43] J.-P. SERRE. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), 259–331.
[44] J.-P. SERRE. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.* (1981), 323–401.

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press

[45] G. SHIMURA. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, no. 11. (Iwanami Shoten, Publishers, Tokyo, 1971). Kanô Memorial Lectures, no. 1.

[46] J. H. SILVERMAN. *The arithmetic of elliptic curves*, second ed. Graduate Texts in Math., vol. 106 (Springer, Dordrecht, 2009).

[47] A. V. SUTHERLAND. A local-global principle for rational isogenies of prime degree. *J. Théor. Nombres Bordeaux* **24**(2) (2012), 475–485.

[48] A. V. SUTHERLAND. Computing images of Galois representations attached to elliptic curves. *Forum Math. Sigma* **4** (2016), e4, 79.

[49] 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.

[50] D. ZYWINA. On the possible image of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. *Preprint:* arXiv:1508.07660.

https://doi.org/10.1017/S030500412610200X Published online by Cambridge University Press