Math. Res. Lett.
Volume 24, Number 4, 1067–1096, 2017

On the minimal degree of definition of p-primary torsion subgroups of elliptic curves

Enrique González-Jiménez and Álvaro Lozano-Robledo

In this article, we study the minimal degree $[K(T):K]$ of a p-subgroup $T \subseteq E(\overline{K})_{\text{tors}}$ for an elliptic curve E/K defined over a number field K. Our results depend on the shape of the image of the p-adic Galois representation $\rho_{E,p^\infty}: \operatorname{Gal}(\overline{K}/K) \to \operatorname{GL}(2,\mathbb{Z}_p)$. However, we are able to show that there are certain uniform bounds for the minimal degree of definition of T. When the results are applied to $K=\mathbb{Q}$ and $p=2$, we obtain a divisibility condition on the minimal degree of definition of any subgroup of $E[2^n]$ that is best possible.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$, let p be a prime number, and let $N \geq 1$. Let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$, and let $E[p^N]$ be the subgroup of algebraic points on $E(\overline{\mathbb{Q}})$ that are torsion points of order dividing p^N. In other words, $E[p^N]$ is the kernel of the multiplication-by-p^N map $[p^N]: E \to E$. Let $T \subseteq E[p^N]$ be a p-subgroup. The central object of study of this article is the field of definition of T, namely $\mathbb{Q}(T) := \mathbb{Q}(\{x(P), y(P) : P = (x(P), y(P)) \in T\})$.

It is well-known that a torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ may contain points of prime-power order 8, 9, 5, or 7, but no points of order 16, 27, 25, 49, or $p > 7$. This follows for example from a theorem of Mazur (Theorem 2.1 below). Similarly, a theorem of Kamienny, Kenku, and Momose (Theorem 2.2), shows that there are quadratic fields K and elliptic curves E/K such that $E(K)$ contains a point of order 16. However, one cannot find points of order 32 in $E(K)$, for a curve E/K and a quadratic extension $K/\mathbb{Q}$. Points of order 16 also may appear starting from an elliptic curve $E/\mathbb{Q}$ and considering $E(K)$,

2010 Mathematics Subject Classification: Primary: 11G05, Secondary: 14H52.

The first author was partially supported by the grant MTM2012–35849.

where $K/\mathbb{Q}$ is quadratic (see Theorem 2.3). More generally, the second author has shown that if $E/\mathbb{Q}$ is an elliptic curve over $\mathbb{Q}$, and $R \in E(\overline{\mathbb{Q}})$ is a point of order $p = 11$ or $p > 13$, then $[\mathbb{Q}(P) : \mathbb{Q}] \geq (p-1)/2$ (see [12], Theorem 2.1).

In this article, we fix a number field K and we study the minimal degree $[K(T) : K]$ of a subgroup $T \subseteq E(\overline{K})_{\text{tors}}$ with $T \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z}$ for an elliptic curve E/K defined over K. Our results depend on the shape of the image of the p-adic Galois representation $\rho_{E,p^\infty} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2, \mathbb{Z}_p)$. However, we are able to show that there are certain uniform bounds for the minimal degree of definition of T.

Theorem 1.1. *Let p be a prime, let K be a number field, and let E/K be an elliptic curve defined over K without complex multiplication. Let $0 \leq s \leq N$ be integers, and let $T_{s,N} \subseteq E(\overline{K})_{tors}$ with $T_{s,N} \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z}$. Then:*

1) *There are positive integers $n = n(K,p)$, $g_{s,M}(K,p)$, and $m_{s,M}(K,p)$, for $0 \leq s \leq n$ and $M = \min\{n, N\}$, that depend on K and p but not on the choice of E/K or $T_{s,N}$, such that the degree $[K(T_{s,N}) : K]$ is divisible by $g_{s,M}(K,p) \cdot \max\{1, p^{2N-2n}\}$, and $[K(T_{s,N}) : K] \geq m_{s,M}(K,p) \cdot \max\{1, p^{2N-2n}\}$ if $s < n$, and the degree is divisible by $g_{n,n}(K,p) \cdot p^{2N+2s-4n}$, and $[K(T_{s,N}) : K] \geq m_{n,n}(K,p) \cdot p^{2N+2s-4n}$ if $n \leq s \leq N$.*
2) *For a fixed E/K, and for all but finitely many primes p, we have*

$$[K(T_{s,N}) : K] = \begin{cases} (p^2-1)p^{2N-2} & , \text{ if } s = 0, \\ (p-1)(p^2-1)p^{2N+2s-3} & , \text{ if } s \geq 1. \end{cases}$$

The integer $n(K,p)$ that appears in Theorem 1.1 is the smallest integer such that the image of the p-adic Galois representation ρ_{E,p^∞} is completely defined modulo $p^{n(K,p)}$ for all elliptic curves E/K without complex multiplication. The existence of $n(K,p)$ is shown in Theorem 2.5.

We apply the uniform results of Theorem 1.1 to the case of $K = \mathbb{Q}$. For instance, we show that the minimal degree of a point of order 32 for elliptic curves over $\mathbb{Q}$ is 8. In fact, we show the following uniform divisibility result about the degree of the extension $\mathbb{Q}(P)/\mathbb{Q}$, for a point of arbitrary order 2^N, for $N \geq 4$.

Theorem 1.2. *Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ without CM, and let $P \in E[2^N]$ be a point of exact order 2^N, with $N \geq 4$. Then, the degree $[\mathbb{Q}(P) : \mathbb{Q}]$ is divisible by 2^{2N-7}. Moreover, this bound is best possible, in the sense that there is a one-parameter family E_t of elliptic curves over $\mathbb{Q}$ such* *that, for each $t \in \mathbb{Q}$, there is a points $P_{t,N} \in E_t(\overline{\mathbb{Q}})$ of exact order 2^N, such that*

$$[\mathbb{Q}(P_{t,N}) : \mathbb{Q}] = 2^{2N-7}.$$

The family mentioned in the statement of Theorem 1.2 is $\mathcal{X}_{235l}$, which parametrizes all elliptic curves over $\mathbb{Q}$ with 2-adic image `X235l` in the notation of [16] (see Section 4). One concrete member of the family is the curve with Cremona label [7] `210e1`, given in Weierstrass form by

$$E : y^2 + xy = x^3 + 210x + 900.$$

As a corollary of Theorem 1.2, we obtain the following bound on two-torsion points.

Corollary 1.3. *Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let $F/\mathbb{Q}$ be an extension of degree $d \geq 1$. Then $E(F)$ can only contain points of order 2^N with $N \leq (\log_2(d) + 7)/2$. More precisely, if ν_2 is the usual 2-adic valuation, then $E(F)$ can only contain points of order 2^N with $N \leq \lfloor \frac{\nu_2(d)+7}{2} \rfloor$.*

Exploiting recent work of Rouse and Zureick-Brown [16] that classifies all possible 2-adic images for elliptic curves over $\mathbb{Q}$, one can calculate explicitly the constants $g_{s,N}(\mathbb{Q}, 2)$ of Theorem 1.1 and calculate the minimal degree of definition of various subgroups of $E[2^N]$, for an elliptic curve E defined over $\mathbb{Q}$. As before, Mazur's theorem implies that the 2-primary component of any torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to a subgroup of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, while the theorems of Kenku, Kamienny, and Momose imply that the 2-primary components defined over a quadratic field are isomorphic to subgroups of $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Our second main theorem, gives the best possible (divisibility) bound for the degree of definition of any torsion subgroup $T \cong \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$, for any $0 \leq s \leq N$, for an elliptic curve over $\mathbb{Q}$ without CM.

Theorem 1.4. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $1 \leq s \leq N$ be fixed integers, and let $T \subseteq E[2^N]$ be a subgroup isomorphic to $\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$. Then, $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by 2 if $s = N = 2$, and otherwise by $2^{2N+2s-8}$ if $N \geq 3$, unless $s \geq 4$ and $j(E)$ is one of the two values*

$$-\frac{3 \cdot 18249920^3}{17^{16}} \quad or \quad -\frac{7 \cdot 1723187806080^3}{79^{16}}$$

in which case $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $3 \cdot 2^{2N+2s-9}$. Moreover, this bound is best possible, in the sense that there are one-parameter families $E_{s,N}(t)$

of elliptic curves over $\mathbb{Q}$ such that, for each $s, N \geq 0$ and each $t \in \mathbb{Q}$, and subgroups $T_{s,N} \in E_{s,N}(t)(\overline{\mathbb{Q}})$ isomorphic to $\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$, such that $[\mathbb{Q}(T_{s,N}) : \mathbb{Q}]$ is equal to the bound given above.

We remark here that the 2-torsion subgroups that are not covered by Theorems 1.2 and 1.4, namely those that correspond to pairs $(s, N) = (0, 1)$, $(0, 2)$, $(0, 3)$, $(1, 1)$, and $(1, 2)$, are known to appear infinitely many times as defined over $\mathbb{Q}$, by Mazur's theorem (Theorem 2.1). Also, it is worth pointing out that the two j-invariants that appear in the statement of Theorem 1.4 are two of the j-invariants that appear in Theorem 1.1 and Table 1 of [16].

Example 1.5. As a consequence of Corollary 3.5, we can calculate the first degree d where a certain 2-primary torsion structure appears for some elliptic curve $E/\mathbb{Q}$ without CM. We do this in Table 1 for $d \leq 16$, i.e., for each $d \leq 16$, we list all the possible torsion structures $\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$, such that there exists an elliptic curve E defined over $\mathbb{Q}$ with $T_{s,N} \subseteq E_{s,N}(\overline{\mathbb{Q}})$ isomorphic to $\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$ and $[\mathbb{Q}(T_{s,N}) : \mathbb{Q}] = d$, and such that d is smallest with this property.

d				
1	2	4	8	16
$\mathbb{Z}/2\mathbb{Z}$ $\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/8\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/16\mathbb{Z}$ $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/32\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}$ $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$

Table 1: 2-primary torsion subgroups that appear in degree d for the first time.

For $p > 2$, the classification of all possible p-adic images of Galois representations associated to elliptic curves $E/\mathbb{Q}$ is not known. In fact, the classification of all possible mod-p images is not known, since we do not know whether there are elliptic curves without CM such that the mod-p image is contained in a normalizer of a non-split Cartan subgroup of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ when $p \geq 13$ (see the introduction of [12] for a discussion of this topic). However, Sutherland and Zywina ([20], [21]) have a list of 63 mod-p images that do occur for non-CM curves $E/\mathbb{Q}$, and that would be the complete list if the answer to Serre's uniformity question is positive. Using this list of images, we can show the following theorem about p-adic representations that are defined modulo p, i.e., for those p-adic images that are the full inverse image of their mod-p image.

Theorem 1.6. *Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let p be a prime such that*

(A) the image G_1 of $\rho_{E,p} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}(2, \mathbb{Z}/p\mathbb{Z})$ is not contained in the normalizer of a non-split Cartan subgroup.

In addition, let us assume that either (B) or (C) occurs, where

(B) p is not in the set $S = \{2, 3, 5, 7, 11, 13, 17, 37\}$, or

(C) if $p \in S$, we suppose that the p-adic image G of ρ_{E,p^∞} is defined modulo p, i.e., the image G of ρ_{E,p^∞} is the full inverse image of $G_1 = \rho_{E,p}(\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ under mod-p reduction.

Let $T = T_{s,N} \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z} \subseteq E[p^N]$ be a subgroup. Then,

1) For a fixed $G_1 = \rho_{E,p}(\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, the degree $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $g_{0,1}(G_1) \cdot p^{2N-2}$, and $[\mathbb{Q}(T) : \mathbb{Q}] \geq m_{0,1}(G_1) \cdot p^{2N-2}$ if $s = 0$, and $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $g_{1,1}(G_1) \cdot p^{2N+2s-4}$, and $[\mathbb{Q}(T) : \mathbb{Q}] \geq m_{1,1}(G_1) \cdot p^{2N+2s-4}$ if $s \geq 1$, where the constants $g_{k,1}(G_1)$ and $m_{k,1}(G_1)$ are given in Tables 5 and 6 for $k = 0, 1$.

2) In general, $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $g_{0,1}(\mathbb{Q}, p) \cdot p^{2N-2}$, and $[\mathbb{Q}(T) : \mathbb{Q}] \geq m_{0,1}(\mathbb{Q}, p) \cdot p^{2N-2}$ if $s = 0$, and divisible by $g_{1,1}(\mathbb{Q}, p) \cdot p^{2N+2s-4}$, and $[\mathbb{Q}(T) : \mathbb{Q}] \geq m_{1,1}(\mathbb{Q}, p) \cdot p^{2N+2s-4}$ if $s \geq 1$, where the constants $g_{k,1}(\mathbb{Q}, p)$ and $m_{k,1}(\mathbb{Q}, p)$ are given in Table 2 for $k = 0, 1$.

For example, let $E/\mathbb{Q}$ be the elliptic curve

$$y^2 + xy + y = x^3 + x^2 - 3x + 1$$

and Cremona label `50b1`. This is an elliptic curve without complex multiplication, such that $B = \rho_{E,3}(\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is conjugate to a full Borel subgroup of $\operatorname{GL}(2, \mathbb{Z}/3\mathbb{Z})$. In the notation of [20], the image is `3B`. Moreover, the 3-adic image $\rho_{E,3^\infty}(\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is the full inverse image of B in $\operatorname{GL}(2, \mathbb{Z}_3)$, as we will see in Section 4.1. Thus, $\rho_{E,3^\infty}$ is defined modulo 3, so $E/\mathbb{Q}$ satisfies (A) and (C) of Theorem 1.6. It is easy to see that $g_{0,1}(\texttt{3B}) = m_{0,1}(\texttt{3B}) = 2$ and

p	$g_{0,1}(\mathbb{Q},p)$	$m_{0,1}(\mathbb{Q},p)$	$g_{1,1}(\mathbb{Q},p)$	$m_{1,1}(\mathbb{Q},p)$
2	1	1	1	1
3	1	1	2	2
5	1	1	4	4
7	1	1	6	18
11	5	5	10	110
13	1	3	12	288
17	8	8	1088	1088
37	12	12	15984	15984
else	p^2-1	p^2-1	$(p-1)p(p^2-1)$	$(p-1)p(p^2-1)$

Table 2: $g_{k,1}(\mathbb{Q},p)$ and $m_{k,1}(\mathbb{Q},p)$, for $k=0,1$.

$g_{1,1}(\texttt{3B}) = m_{1,1}(\texttt{3B}) = 12$. Therefore, for every $0 \le s \le N$, and every subgroup $T_{s,N} \cong \mathbb{Z}/3^s\mathbb{Z} \oplus \mathbb{Z}/3^N\mathbb{Z} \subseteq E[3^N]$, we have that $[\mathbb{Q}(T_{s,N}) : \mathbb{Q}]$ is divisible by

$$\begin{cases} 2^{2N-1} & , \text{ if } s = 0, \\ 3 \cdot 2^{2N+2s-2} & , \text{ if } s \ge 1, \end{cases}$$

and these divisibility bounds are best possible, in the sense that, for each pair of s, N, there is a choice of $T'_{s,N} \subseteq E[3^N]$ such that $[\mathbb{Q}(T'_{s,N}) : \mathbb{Q}]$ is equal to the bound.

Remark 1.7. All our results in this article are for elliptic curves without complex multiplication. In the CM case, there are known divisibility bounds for the field of definition of a point of order N (and for p-primary torsion structures when the field of definition does not contain the quadratic field of complex multiplication) given by Silverberg [19], and Prasad and Yogananda [15]. More generally, Bourdon, Clark, and Pollack [6], have recently shown divisibility bounds for p-primary torsion structures, similar to those of our Theorem 1.6.

The article is organized as follows. In Section 2 we record previous results in the literature related to our work, which will be used in Section 3 to prove our main Theorem 3.1. Then, we will deduce a number of corollaries, which include Theorems 1.1, 1.2, and 1.4 from the introduction. In particular, Theorem 1.1 follows from Corollaries 3.2 and 3.3, while 1.2, and 1.4 follow from Corollary 3.4 (and they are equivalent to Corollary 3.5). Theorem 1.6 will be shown at the very end of Section 3. Finally, in Section 4, we show examples of families of elliptic curves that achieve the minimal degrees of definition.

2. Prior Results in the Literature

The first three results that we quote describe the possible torsion subgroups for elliptic curves over $\mathbb{Q}$ or quadratic fields.

Theorem 2.1 (Mazur, [13], Theorem 2). *Let $E/\mathbb{Q}$ be an elliptic curve. Then*

$$E(\mathbb{Q})_{tors} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \textit{with } 1 \leq M \leq 10 \textit{ or } M = 12, \textit{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \textit{with } 1 \leq M \leq 4. \end{cases}$$

Theorem 2.2 (Kenku, Momose, [11]; Kamienny, [10]). *Let $K/\mathbb{Q}$ be a quadratic field and let E/K be an elliptic curve. Then*

$$E(K)_{tors} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \textit{with } 1 \leq M \leq 16 \textit{ or } M = 18, \textit{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \textit{with } 1 \leq M \leq 6, \textit{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \textit{with } M = 1 \textit{ or } 2, \textit{ only if } K = \mathbb{Q}(\sqrt{-3}), \textit{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \textit{only if } K = \mathbb{Q}(\sqrt{-1}). \end{cases}$$

Theorem 2.3 (Najman, [14], Theorem 2). *Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$, and let F be a quadratic number field. Then,*

$$E(F)_{tors} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \textit{with } 1 \leq M \leq 10, \textit{ or } M = 12, 15, \textit{ or } 16, \textit{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \textit{with } 1 \leq M \leq 6, \textit{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \textit{with } M = 1 \textit{ or } 2, \textit{ only if } F = \mathbb{Q}(\sqrt{-3}), \textit{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \textit{only if } F = \mathbb{Q}(\sqrt{-1}). \end{cases}$$

As we mentioned in the introduction, our results depend on the image of the p-adic Galois representation $\rho_{E,p^\infty} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2, \mathbb{Z}_p)$ associated to the natural action of Galois on the Tate module $T_p(E)$ with respect to a fixed $\mathbb{Z}_p$-basis. In [17], Serre showed that the image of ρ_{E,p^∞} is as large as possible for all but finitely many prime numbers, as long as E/K does not have complex multiplication.

Theorem 2.4 (Serre, [17]). *Let K be a number field, and let E/K be an elliptic curve without complex multiplication. Then, $\rho_{E,p^\infty}(\mathrm{Gal}(\overline{K}/K))$ is an* *open subgroup of* $\mathrm{GL}(2,\mathbb{Z}_p)$*, and* ρ_{E,p^∞} *is surjective for all but finitely many primes.*

Serre's open image theorem implies that there is a number $n = n(E/K,p)$ such that $1 + p^n M_2(\mathbb{Z}_p) \subseteq \rho_{E,p^\infty}(\mathrm{Gal}(\overline{K}/K))$. The following result shows that $n(E/K,p)$ can be made independent of the curve.

Theorem 2.5 (Arai, [1]). *Let* K *be a number field, and let* p *be a prime. Then, there exists an integer* $n = n(K,p) \geq 1$ *depending on* K *and* p *such that for any elliptic curve* E *over* K *with no complex multiplication, we have* $1 + p^n M_2(\mathbb{Z}_p) \subseteq \rho_{E,p^\infty}(\mathrm{Gal}(\overline{K}/K))$*. In other words,* $\rho_{E,p^\infty}(\mathrm{Gal}(\overline{K}/K))$ *is the full inverse image of* $\rho_{E,p^n}(\mathrm{Gal}(\overline{K}/K))$ *under reduction modulo* p^n*.*

As a corollary of Arai's theorem, the image of ρ_{E,p^∞} is determined modulo $p^{n(K,p)}$, and so, the number of possible p-adic images (up to conjugation) is bounded above by the number of subgroups of $\mathrm{GL}(2,\mathbb{Z}/p^n\mathbb{Z})$. Thus, we obtain that there are only finitely many possible p-adic images of ρ_{E,p^∞} over K up to conjugation.

Corollary 2.6. *Let* K *be a number field, and let* p *be a prime. Then, there is only a finite number* $a(K,p) \geq 1$ *of possibilities (up to conjugation) for the image of* $\rho_{E,p^\infty} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2,\mathbb{Z}_p)$*, for any elliptic curve* E/K *without complex multiplication. In other words, there are subgroups* G^i *of* $\mathrm{GL}(2,\mathbb{Z}_p)$*, for* $1 \leq i \leq a(K,p)$*, such that for any elliptic curve* E/K *there is a number* j *such that* $\rho_{E,p^\infty}(\mathrm{Gal}(\overline{K}/K))$ *is a conjugate of* G^j *in* $\mathrm{GL}(2,\mathbb{Z}_p)$*.*

Rouse and Zureick-Brown have classified all the possible 2-adic images of $\rho_{E,2} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2,\mathbb{Z}_2)$, and have shown that $n(\mathbb{Q},2) = 5$ and $a(\mathbb{Q},2) = 1208$, with notation as in Arai's theorem and its corollary.

Theorem 2.7 (Rouse, Zureick-Brown, [16]). *Let* E *be an elliptic curve over* $\mathbb{Q}$ *without complex multiplication. Then, there are exactly* 1208 *possibilities for the* 2*-adic image* $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$*, up to conjugacy in* $\mathrm{GL}(2,\mathbb{Z}_2)$*. Moreover:*

1) *The index of* $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ *in* $\mathrm{GL}(2,\mathbb{Z}_2)$ *divides* 64 *or* 96*.*
2) *The image* $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ *is the full inverse image of* $\rho_{E,2^5}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ *under reduction modulo* 2^5*.*

Remark 2.8. The 1208 distinct possibilities for 2-adic images that are found in [16] are described in a few text files that can be found on the website listed in the references of this article. Each image has a label `Xk` or `Xkt` where `k` is a number and `t` is a letter (e.g., `X2` or `X58i`). In particular, the files `curvelist1.txt` and `curvelist2.txt` are lists of examples of elliptic curves with each type of image, and the files `gl2data.gz` and `gl2finedata.gz` contain the descriptions of each image. The curves with each type of image come in 1-parameter families which are given in the file `finemodels.tar.gz`. See the article and website [16] for more info on how to interpret the files and notations. In addition, the website [16] contains links to individual websites with data about each 2-adic image. For instance, `http://users.wfu.edu/rouseja/2adic/X441.html` is the site for the image `X441`.

For $p > 2$, we know that the image of $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[p])$ is contained in one of the maximal subgroups of $\mathrm{GL}(E[p]) \cong \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$. The best results known are summarized in the following result.

Theorem 2.9 (Serre, [17], §2; [18], Lemme 18; Mazur, [13]; Bilu, Parent, Rebolledo [3], [4]). *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let G be the image of $\rho_{E,p}$, and suppose $G \neq \mathrm{GL}(E[p])$. Then one of the following possibilities holds:*

1) *G is contained in a Borel subgroup of $\mathrm{GL}(E[p])$, and $p = 2, 3, 5, 7, 11, 13, 17$, or 37; or*
2) *The projective image of G in $\mathrm{PGL}(E[p])$ is isomorphic to A_4, S_4 or A_5, where S_n is the symmetric group and A_n the alternating group, and $p \leq 13$; or*
3) *G is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}(E[p])$ and $p \leq 13$, with $p \neq 11$; or*
4) *G is contained in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}(E[p])$.*

Sutherland has computed the mod-p image of all the non-CM elliptic curves in Cremona's tables and the Stein-Watkins database, some 140 million curves with conductors ranging up to 10^{12}, and Zywina has described all known (and conjecturally all) proper subgroups of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ that occur as the image of $\rho_{E,p}$.

Conjecture 2.10 (Sutherland, [20]; Zywina, [21]). *Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let p be a prime. Then, there is a set S_p formed by $s_p = |S_p|$ isomorphism types of subgroups of $\mathrm{GL}(2, \mathbb{F}_p)$, where*

p	2	3	5	7	11	13	17	37	*else*
s_p	3	7	15	16	7	11	2	2	0,

such that if G *is the image of* $\rho_{E,p}$*, then* G *is conjugate to one of the subgroups in* S*, or* $G \cong \mathrm{GL}(2, \mathbb{F}_p)$.

The list of images in the sets S_p appears in our Tables 5 and 6 and are described in [21], and Tables 3 and 4 of [20].

3. Proofs

We begin by calculating a general formula for $[K(T) : K]$ in terms of the sizes of subgroups of the Galois group of $\mathbb{Q}(E[p^N])/\mathbb{Q}$.

Theorem 3.1. *Let* p *be a prime number, let* K *be a number field, let* E/K *be an elliptic curve without CM, let* $G = \rho_{E,p^\infty}(\mathrm{Gal}(\overline{K}/K))$*, and suppose that* G *is defined at level* p^d*, for some* $d \geq 1$ *(i.e.,* G *is the full inverse image of* $G_d \equiv G \bmod p^d$ *under reduction modulo* p^d*). Let* $0 \leq s \leq N$ *be fixed integers, and let* $T \subseteq E[p^N]$ *be a subgroup isomorphic to* $\mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z}$*, and write* H_T *for the subgroup of* $G_N \cong \mathrm{Gal}(K(E[p^N])/K)$ *that fixes* $K(T)$*, so that if* $s > 0$ *we have*

$$H_T = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + p^s \cdot \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}/p^N\mathbb{Z} \right\} \cap G_N \subseteq \mathrm{GL}(2, \mathbb{Z}/p^N\mathbb{Z}),$$

where the chosen basis of $E[p^N]$ *is* $\{P, Q\}$ *and* $P \in T$ *is a point of order* p^N*, and if* $s = 0$*, then*

$$H_T = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{Z}/p^N\mathbb{Z},\ b \in (\mathbb{Z}/p^N\mathbb{Z})^\times \right\} \cap G_N \subseteq \mathrm{GL}(2, \mathbb{Z}/p^N\mathbb{Z}).$$

Then, the index $[K(T) : K]$ *is computed as follows:*

(i) If $0 < s \leq N \leq d$*, then* $[K(T) : K] = |G_N|/|H_T|$ *where* $G_N \equiv G \equiv G_d \bmod p^N$.

(ii) If $s \leq d \leq N$*, then*

$$[K(T) : K] = \frac{|G_N|}{|H_T|} = \frac{|G_d|}{|H_{T_d}|} \cdot p^{2(N-d)},$$

where H_{T_d} *is the subgroup of* G_d *that fixes* $T_d = T \cap E[p^d]$.

(iii) If $d \leq s \leq N$, then

$$[K(T):K] = \frac{|G_N|}{|H_T|} = |G_d| \cdot p^{2N+2s-4d}.$$

Proof. Let p be a prime number, let E/K be an elliptic curve without CM, and let ρ_{E,p^∞} be the Galois representation $\operatorname{Gal}(\overline{K}/K) \to \operatorname{GL}(2,\mathbb{Z}_p)$ associated to the action of Galois on the Tate module $T_p(E)$ after fixing a $\mathbb{Z}_p$-basis $\{P,Q\}$ of $T_p(E)$, and suppose that G is defined at level p^d, for some $d \geq 1$ (i.e., G is the full inverse image of $G_d \equiv G \bmod p^d$ under reduction modulo p^d). For each $m \geq 1$, let $\rho_{E,p^m} : \operatorname{Gal}(\overline{K}/K) \to \operatorname{GL}(2,\mathbb{Z}/p^m\mathbb{Z})$ be the Galois representations obtained as reduction of $\rho_{E,p}$ modulo p^m, and let G_m be the image of ρ_{E,p^m}. Then, $G_m \cong \operatorname{Gal}(K(E[p^m])/K)$.

Let s, N, and T be as in the statement of the theorem. Let H_T be the subgroup of $G_N \cong \operatorname{Gal}(K(E[p^N])/K)$ that fixes $K(T)$. In particular,

$$[K(T):K] = \frac{|\operatorname{Gal}(K(E[p^N])/K)|}{|H_T|} = \frac{|G_N|}{|H_T|}.$$

Since T contains a point P_N of order p^N, we can choose $Q_N \in E[p^N]$ that forms a $\mathbb{Z}/p^N\mathbb{Z}$-basis $\{P_N, Q_N\}$ of $E[p^N]$. With respect to this basis, the subgroup H_T fixing T must be the subgroup of matrices in $G_N \subseteq \operatorname{GL}(2,\mathbb{Z}/p^N\mathbb{Z})$ that (a) fix P_N, and (b) reduce to the identity modulo p^s (since $E[p^s] \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^s\mathbb{Z}$ is a subgroup of T). Hence, if $s > 0$, the group H_T must be given by

$$H_T = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + p^s \cdot \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}/p^N\mathbb{Z} \right\} \cap G_N \subseteq \operatorname{GL}(2,\mathbb{Z}/p^N\mathbb{Z}),$$

and if $s = 0$, then

$$H_T = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{Z}/p^N\mathbb{Z},\ b \in (\mathbb{Z}/p^N\mathbb{Z})^\times \right\} \cap G_N \subseteq \operatorname{GL}(2,\mathbb{Z}/p^N\mathbb{Z}).$$

We distinguish three cases according to whether (i) $s \leq N \leq d$, or (ii) $s \leq d \leq N$, or (iii) $d \leq s \leq N$:

(i) Suppose $s \leq N \leq d$. Then, $[K(T):K] = |G_N|/|H_T|$ can be calculated directly, where $G_N \equiv G_d \bmod p^N$, and H_T is defined as before.

(ii) Suppose $s \leq d \leq N$. Since $N \geq d$, the subgroup G_N is the full inverse image of G_d. In particular, since $\operatorname{Ker}(\operatorname{GL}(2,\mathbb{Z}/p^{d+1}\mathbb{Z}) \to \operatorname{GL}(2,\mathbb{Z}/p^d\mathbb{Z}))$

is the subgroup

$$\left\langle \begin{pmatrix} 1 & p^d \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ p^d & 1 \end{pmatrix}, \begin{pmatrix} 1+p^d & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1+p^d \end{pmatrix} \right\rangle,$$

of order p^4, it follows that $\operatorname{Ker}(\mathrm{GL}(2,\mathbb{Z}/p^N\mathbb{Z}) \to \mathrm{GL}(2,\mathbb{Z}/p^d\mathbb{Z}))$ is a subgroup of order $p^{4(N-d)}$. Hence:

$$\begin{aligned} |G_N| &= |\operatorname{Gal}(K(E[p^N])/K)| \\ &= |\operatorname{Gal}(K(E[p^d])/K)| \cdot p^{4(N-d)} = |G_d| \cdot p^{4(N-d)}. \end{aligned}$$

Let H_{T_d} be the subgroup of G_d that fixes $T_d = T \cap E[p^d] \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^d\mathbb{Z}$, where a fixed point of order p^d is $P_d = p^{N-d}P_N$. If we write $Q_d = p^{N-d}Q_N$, and we assume $s > 0$ for now, then H_{T_d} is the subgroup

$$H_{T_d} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + p^s \cdot \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}/p^d\mathbb{Z} \right\} \cap G_d \subseteq \mathrm{GL}(2,\mathbb{Z}/p^d\mathbb{Z}),$$

and if $s = 0$, then

$$H_{T_d} = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{Z}/p^d\mathbb{Z},\ b \in (\mathbb{Z}/p^d\mathbb{Z})^\times \right\} \cap G_d \subseteq \mathrm{GL}(2,\mathbb{Z}/p^d\mathbb{Z}).$$

In either case, $H_{T_d} \equiv H_T \bmod p^d$, and $|H_T|/|H_{T_d}| = p^{2(N-d)}$. Hence,

$$[K(T):K] = \frac{|G_N|}{|H_T|} = \frac{|G_d| \cdot p^{4(N-d)}}{|H_{T_d}| \cdot p^{2(N-d)}} = \frac{|G_d|}{|H_{T_d}|} \cdot p^{2N-2d}.$$

We remark here that this formula is the same for any subgroup $T \subseteq E[p^N]$ such that $T_d = T \cap E[p^d]$. Thus, it only depends on the size of $|G_d|/|H_{T_d}|$, for each possible $T_d \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^d\mathbb{Z}$.

(iii) Suppose that $d \leq s \leq N$. As before, G_N is the full inverse image of G_d, and so $|G_N| = |G_d| \cdot p^{4(N-d)}$. In this case, $d \leq s$, and so, by the definition of $H_T \subseteq G_N$, every $M \in H_T$ reduces to the identity modulo s and thus modulo d. Since $N \geq s \geq d \geq 1$, it follows that

$$H_T = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + p^s \cdot \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z}/p^N\mathbb{Z} \right\}$$

and, therefore,

$$|H_T| = p^{2(N-s)},$$

and

$$[K(T):K] = \frac{|G_N|}{|H_T|} = \frac{|G_d| \cdot p^{4(N-d)}}{p^{2(N-s)}} = |G_d| \cdot p^{2N+2s-4d}.$$

□

In the following corollary, we apply Theorem 3.1 to the case of full $\mathrm{GL}(2,\mathbb{Z}_p)$ image. We remind the reader that the order

$$|\,\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})| = \varphi(N) \cdot N^3 \prod_{p|N} (1-1/p^2)$$

for any $N \geq 1$. In particular,

$$|\,\mathrm{GL}(2,\mathbb{Z}/p^N\mathbb{Z})| = (p-1)p^{N-1} \cdot p^{3N} \cdot (1-1/p^2) = (p-1)(p^2-1)p^{4N-3}.$$

Corollary 3.2. *Let K be a number field, and let E/K be an elliptic curve. Then:*

1) Suppose $G = \rho_{E,p^\infty}(\mathrm{Gal}(\overline{K}/K)) \cong \mathrm{GL}(2,\mathbb{Z}_p)$ for some prime p. Let $0 \leq s \leq N$ be fixed integers, let $T_{s,N} \subseteq E[p^N]$ be a subgroup isomorphic to $\mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z}$. Then:

$$[K(T_{s,N}):K] = \begin{cases} (p^2-1)p^{2N-2} & , \text{ if } s=0, \\ (p-1)(p^2-1)p^{2N+2s-3} & , \text{ if } s \geq 1. \end{cases}$$

2) For a fixed elliptic curve E/K without CM the degree $[K(T_{s,N}):K]$ is given by the formula in (1) for all but finitely many primes p.

Proof. First, let $s=0$ and let $N \geq 1$ be arbitrary. Let $T = \langle P \rangle$ and let $\{P,Q\}$ be a basis of $E[p^N]$, and write H_T for the subgroup of $G_N \cong \mathrm{Gal}(K(E[p^N])/K)$ that fixes $K(T)$. Then, the formulae of Theorem 3.1 says that $|H_T| = \varphi(p^N) \cdot p^N = (p-1)p^{N-1}p^N$, while $|G_N| = |\,\mathrm{GL}(2,\mathbb{Z}/p^N\mathbb{Z})| = (p-1)(p^2-1)p^{4N-3}$. Thus,

$$[K(T):K] = [K(P):K] = \frac{|G_N|}{|H_T|} = \frac{(p-1)(p^2-1)p^{4N-3}}{(p-1)p^{2N-1}} = (p^2-1)p^{2N-2}.$$

Otherwise, $N \geq s \geq 1 = d$, and we are in case (iii) of Theorem 3.1. Hence,

$$\begin{aligned}[K(T):K] &= |G_1| \cdot p^{2N+2s-4} \\ &= (p-1)(p^2-1)p \cdot p^{2N+2s-4} = (p-1)(p^2-1)p^{2N+2s-3}.\end{aligned}$$

This shows (1). Now (2) is a direct consequence of Serre's open image theorem (Theorem 2.4). □

Corollary 2.6 says that there is a finite number of possible p-adic images of the form $\rho_{E,p^\infty}(\mathrm{Gal}(\overline{K}/K))$, up to conjugation, for any elliptic curve E/K. Thus, there are divisibility bounds as in Theorem 3.1 that are uniform over all elliptic curves over K.

Corollary 3.3. *Let p be a prime, let K be a number field, and let $n(K,p) \geq 1$ be the number given by Theorem 2.5. Let G^i, for $i = 1, \dots, a(K,p)$, be the possible p-adic images for ρ_{E,p^∞}, given by Corollary 2.6. Let E/K be an elliptic curve without CM. Let $0 \leq s \leq N$ be fixed integers, let $T \subseteq E[p^N]$ be any subgroup isomorphic to $\mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z}$, and put $M = \min\{N, n(K,p)\}$. Then:*

1) *Suppose $\rho_{E,p^\infty}(\mathrm{Gal}(\overline{K}/K)) = G^i$, for a fixed $1 \leq i \leq a(K,p)$. Then, if $s < n(K,p)$, $[K(T):K]$ is divisible by $g_{s,M}(G^i) \cdot \max\{1, p^{2N-2n(K,p)}\}$ and if $s \geq n(K,p)$, $[K(T):K]$ is divisible by*

$$g_{n(K,p),n(K,p)}(G^i) \cdot p^{2N+2s-4n(K,p)},$$

where

$$g_{s,M}(G^i) = \gcd\left(\left\{\frac{|G^i_M|}{|H^i_{T'}|} : T' \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^M\mathbb{Z} \subseteq \langle P^i_M, Q^i_M\rangle\right\}\right),$$

the group G^i_M is defined by $G^i_M \equiv G^i_{n(K,p)} \equiv G^i \bmod p^M$ as a subgroup of $\mathrm{GL}(2,\mathbb{Z}/p^M\mathbb{Z})$, and $H^i_{T'}$ is the subgroup of G^i_M that fixes T'.

2) *More generally, if $s < n(K,p)$ the degree $[K(T):K]$ is divisible by $g_{s,M}(K,p) \cdot \max\{1, p^{2N-2n(K,p)}\}$ and if $s \geq n(K,p)$, by $g_{n(K,p),n(K,p)}(K,p) \cdot p^{2N+2s-4n(K,p)}$, where*

$$g_{s,M}(K,p) = \gcd(\{g_{s,M}(G^i) : 1 \leq i \leq a(K,p)\}).$$

Finally, if we define $m_{s,N}(G^i)$ and $m_{s,N}(K,p)$ like $g_{s,N}$ replacing gcd *by* min, *then $[K(T):K] \geq$*

$$m_{s,M}(G^i) \cdot \max\{1, p^{2N-2n(K,p)}\} \geq m_{s,M}(K,p) \cdot \max\{1, p^{2N-2n(K,p)}\},$$

if $s < n(K,p)$, and

$$m_{n(K,p),n(K,p)}(G^i) \cdot p^{2N+2s-4n(K,p)} \geq m_{n(K,p),n(K,p)}(K,p) \cdot p^{2N+2s-4n(K,p)},$$

if $s \geq n(K,p)$.

Proof. The result follows from the divisibility bounds of Theorem 3.1. Clearly part (2) is a direct consequence of (1) and the fact that there are only $a(K,p)$ possible p-adic images (Corollary 2.6), so we will just prove (1). By Theorem 2.5 for every elliptic curve E/K without CM, the image $G = \rho_{E,p^\infty}(\mathrm{Gal}(\overline{K}/K))$ is defined at most modulo $p^{n(K,p)}$ so, for our purposes, we will define every representation exactly modulo $p^{n(K,p)}$, i.e., the value of d in Theorem 3.1 will be always $d = n(K,p)$. Each image G^i is then defined by $G^i_d \equiv G^i \bmod p^d$ as a subgroup of $\mathrm{GL}(2,\mathbb{Z}/p^d\mathbb{Z})$, with respect to a basis $\{P^i_d, Q^i_d\}$ of $E^i[p^d]$, where E^i is an elliptic curve with $G = \rho_{E,p^\infty}(\mathrm{Gal}(\overline{K}/K)) = G^i$. We also fix a compatible basis $\{P^i_n, Q^i_n\}$ of $E^i[p^n]$ for each $n \geq 1$.

There are three possibilities according to the values of s, N, and $d = n(K,p)$.

(i) Suppose $s \leq N \leq n(K,p)$. Then, Theorem 3.1, part (i) shows that $[K(T) : K]$ is divisible by the quantity $g_{s,N}(G^i)$, where

$$g_{s,N}(G^i) = \gcd\left(\left\{\frac{|G^i_N|}{|H^i_{T'}|} : T' \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z} \subseteq \langle P^i_N, Q^i_N\rangle\right\}\right),$$

where $H^i_{T'}$ is the subgroup of G^i_N that fixes T', and $G^i_N \equiv G^i_{n(K,p)} \equiv G^i \bmod p^N$.

(ii) Suppose $s \leq n(K,p) \leq N$. Then, Theorem 3.1, part (ii) shows that $[K(T) : K]$ is divisible by $g_{s,n(K,p)}(G^i) \cdot p^{2N-2n(K,p)}$, where

$$g_{s,n(K,p)}(G^i) = \gcd\left(\left\{\frac{|G^i_{n(K,p)}|}{|H^i_{T'}|} : T' \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^{n(K,p)}\mathbb{Z} \subseteq \langle P^i_{n(K,p)}, Q^i_{n(K,p)}\rangle\right\}\right),$$

where $H^i_{T'}$ is the subgroup of $G^i_{n(K,p)}$ that fixes T'.

(iii) Suppose $n(K,p) \leq s \leq N$. Then, Theorem 3.1, part (iii) shows that $[K(T) : K]$ is divisible by $g_{n(K,p),n(K,p)}(G^i) \cdot p^{2N+2s-4n(K,p)}$, where $g_{n(K,p),n(K,p)}(G^i) = |G^i_{n(K,p)}|$.

Hence, in all cases, $[K(T) : K]$ is divisible by $g_{s,M}(G^i) \cdot \max\{1, p^{2N-2n(K,p)}\}$ if $s < n(K,p)$ and by $g_{n(K,p),n(K,p)}(G^i) \cdot p^{2N+2s-4n(K,p)}$ if $s \geq n(K,p)$, as claimed. □

By the results of [16], we know that $n(\mathbb{Q},2) = 5$ and $a(\mathbb{Q},2) = 1208$, so we can specialize the previous result to $p = 2$ and $K = \mathbb{Q}$, as follows.

Corollary 3.4. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $0 \leq s \leq N$ be fixed integers, let $T \subseteq E[2^N]$ be a subgroup isomorphic to $\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$, and put $M = \min\{N, 5\}$. Then:*

1) *Suppose that $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = G^i$. Then, $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by the number $g_{s,M}(G^i) \cdot \max\{1, 2^{2N-10}\}$ if $s < 5$ and by $g_{5,5}(G^i) \cdot 2^{2N+2s-20}$ if $s \geq 5$, where the numbers $g_{s,M}(G^i)$ are defined as in Corollary 3.3.*
2) *More generally, $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $g_{s,M}(\mathbb{Q}, 2) \cdot \max\{1, 2^{2N-10}\}$ if $s < 5$ and by the number $g_{5,5}(\mathbb{Q}, 2) \cdot 2^{2N+2s-20}$ if $s \geq 5$, where $g_{s,M}(\mathbb{Q}, 2) = \gcd(\{g_{s,M}(G^i) : 1 \leq i \leq 1208\})$, and the values $g_{s,M}(\mathbb{Q}, 2)$ are given by Table 3.*

$g_{s,M}(\mathbb{Q},2)$		M				
		1	2	3	4	5
s	0	1	1	1	2	2^3
	1	1	1	1	2^2	2^4
	2		2	2^2	2^4	2^6
	3			2^4	2^6	2^8
	4				2^7	2^9
	5					2^{11}

Table 3: $g_{s,M}(\mathbb{Q}, 2)$, for $0 \leq s \leq M \leq 5$.

Furthermore:

(a) *The values $g_{s,M}(\mathbb{Q}, 2)$ are best possible for $0 \leq s \leq 3$, i.e., there is a type of representation G^i such that $g_{s,M}(\mathbb{Q}, 2) = g_{s,M}(G^i) = m_{s,M}(G^i)$ (with notation as in Cor. 3.3).*

(b) *For any $1 \leq i \leq 1208$, and if $s \geq 4$, then $g_{s,M}(G^i)$ is divisible by $2 \cdot g_{s,M}(\mathbb{Q}, 2)$ or $3 \cdot g_{s,M}(\mathbb{Q}, 2)$, and both cases occur with equality for certain 2-adic images.*

(c) *Let $s \geq 4$. The image G^i is such that $g_{s,M}(G^i)$ is divisible by $3 \cdot g_{s,M}(\mathbb{Q}, 2)$ but not by $2 \cdot g_{s,M}(\mathbb{Q}, 2)$ if and only if G^i corresponds to the 2-adic image with label* `X441`.

(d) *The minimal values* $m_{s,M}(\mathbb{Q},2)$ *are equal to* $g_{s,M}(\mathbb{Q},2)$ *for* $0 \leq s \leq 3$, *and equal to* $2 \cdot g_{s,M}(\mathbb{Q},2)$ *for* $s \geq 4$.

Proof. The first part is immediate from Corollary 3.3. The values $g_{s,N}(G^i)$ and $g_{s,N}(\mathbb{Q},2)$ have been calculated using Magma [5] for each possible image group G^i as described by [16]. In our calculations we have found all possible values of $|G^i_N|/|H^i_{T'}|$ for each $N \leq 5$, for each choice of $T' \subseteq E[2^N]$, and for all $1 \leq i \leq a(\mathbb{Q},2) = 1208$. The Magma scripts used in this computation can be found at the research website of either author. In particular, the file `2primary_Ss.txt` contains the values of $g_{s,t}(G^i)$, for $0 \leq s \leq 5$ and $1 \leq t \leq 5$, for each of the possible 2-adic images that occur for elliptic curves over $\mathbb{Q}$. In other words, in the file `2primary_Ss.txt` the reader can find an analogue of Table 4 for each of the 1208 possible 2-adic images for non-CM curves. We shall outline here the computation for a given image.

For instance, say $G^i = G$ corresponds to the 2-adic image `X235l` (as always, following the notation of [16]), which is defined modulo 16, and is generated in $\mathrm{GL}(2,\mathbb{Z}/16\mathbb{Z})$ by

$$G_4 = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 12 & 1 \end{pmatrix}, \begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 14 & 1 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 15 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 9 & 0 \\ 8 & 9 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix} \right\rangle.$$

In our notation G_N acts on $E[2^N]$ on the left, i.e., $M \in G_N$ acts on $R \in E[2^N]$ by $M \cdot R$, so our matrices are transposed from those that appear in [16]. Then, the values $g_{s,M}(G)$ are given in Table 4. We shall work out two cases in detail: $(s,N) = (0,1)$ and $(s,N) = (1,5)$.

Let $s = 0$ and $N = 1$. We first compute G_1 which is the reduction of G modulo 2, so it is generated by the reduction of every generator of G_4 modulo 2. Thus,

$$G_1 = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle \subset \mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z}).$$

As T' runs over the three subgroups $T'_1 = \langle (1,0) \rangle$, $T'_2 = \langle (0,1) \rangle$, and $T'_3 = \langle (1,1) \rangle$ of order 2 of $E[2]$ (where the points are given in the same coordinates chosen to represent the matrices), we obtain

$$\frac{|G_1|}{|H_{T'_1}|} = \frac{|G_1|}{|\{\mathrm{Id}\}|} = 2, \quad \frac{|G_1|}{|H_{T'_2}|} = \frac{|G_1|}{|G_1|} = 1, \quad \frac{|G_1|}{|H_{T'_3}|} = \frac{|G_1|}{|\{\mathrm{Id}\}|} = 2.$$

$g_{s,M}(G)$		M				
		1	2	3	4	5
s	0	1	1	1	2	2^3
	1	2	2	2	2^2	2^4
	2		2^3	2^3	2^4	2^6
	3			2^5	2^6	2^8
	4				2^8	2^{10}
	5					2^{12}

Table 4: Values $g_{s,M}(G)$, for $0 \leq s \leq M \leq 5$, where G is the image with label `X2351`.

Hence, $g_{0,1}(G) = \gcd(1,2) = 1$, as it should be, for an elliptic curve $E/\mathbb{Q}$ with 2-adic image `X2351` has a 2-torsion point defined over $\mathbb{Q}$ (in fact, $E(\mathbb{Q})[2^\infty] \cong \mathbb{Z}/8\mathbb{Z}$).

Let now $(s,N) = (1,5)$. Since G is defined modulo 16, the image modulo 2^5 is the full inverse image of G_4 in $\mathrm{GL}(2,\mathbb{Z}/32\mathbb{Z})$. We compute G_5, then, as the subgroup mod 32 generated by the lift of generators of G_4, together with generators of the kernel of reduction $\mathrm{GL}(2,\mathbb{Z}/32\mathbb{Z}) \to \mathrm{GL}(2,\mathbb{Z}/16\mathbb{Z})$. We obtain that G_5 is generated by

$$G_5 = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 12 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix}, \begin{pmatrix} 17 & 0 \\ 0 & 1 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 1 & 16 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 16 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 17 \end{pmatrix} \right\rangle,$$

which is a subgroup of order 4096. Now we need to parametrize subgroups $T' \subset E[5]$ such that $T' \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^5\mathbb{Z}$. Equivalently, we are parametrizing structures $T' = \langle E[2], Q \rangle$ where Q is a point of exact order 2^5. For each such choice of Q, we first find H_Q, the stabilizer of Q in G_5. Then,

$$H_{T'} = H_Q \cap \{M \in \mathrm{GL}(2,\mathbb{Z}/2^5\mathbb{Z}) : M \equiv \mathrm{Id} \bmod 2\}.$$

For instance, let $Q=(1,0)$. Then,

$$H_Q=\left\langle \begin{pmatrix}1 & 16\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & 25\end{pmatrix}\right\rangle,$$

and $H_{T'}=H_Q$ because every matrix in H_Q already fixes $E[2]$ as well. Thus,

$$\frac{|G_5|}{|H_{T'}|}=\frac{4096}{8}=512.$$

Similarly, let $Q=(0,1)$. Then,

$$H_Q=\left\langle \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 12 & 1\end{pmatrix}, \begin{pmatrix}9 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 14 & 1\end{pmatrix}, \begin{pmatrix}5 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}15 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 8 & 1\end{pmatrix}, \begin{pmatrix}17 & 0\\ 0 & 1\end{pmatrix}\right\rangle,$$

while

$$H_{T'}=\left\langle \begin{pmatrix}1 & 0\\ 12 & 1\end{pmatrix}, \begin{pmatrix}9 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 14 & 1\end{pmatrix}, \begin{pmatrix}5 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}15 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 8 & 1\end{pmatrix}, \begin{pmatrix}17 & 0\\ 0 & 1\end{pmatrix}\right\rangle,$$

because every matrix in H_Q already fixes $E[2]$ as well, except for $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$. Thus,

$$\frac{|G_5|}{|H_{T'}|}=\frac{4096}{256}=16.$$

It follows that $g_{1,5}(G)$ is a divisor of $16=2^4$. In fact, the calculation for all possible T' reveals that $g_{1,5}(G)=2^4$, and in fact, $g_{1,5}(G^k)$ is divisible by 2^4, for all $1\leq k\leq 1208$. Hence, $g_{1,5}(\mathbb{Q},2)=2^4$ as it appears in Table 3. Since the value 2^4 is in fact achieved for a specific 2-adic image that occurs over $\mathbb{Q}$, it follows that $g_{1,5}(\mathbb{Q},2)=2^4=m_{1,5}(\mathbb{Q},2)$ as well. Similarly, our calculations show that, in all cases, the values $g_{s,M}(\mathbb{Q},2)$ are best possible for $0\leq s\leq 3$, i.e., there is a type of representation G^i such that $g_{s,M}(\mathbb{Q},2)=g_{s,M}(G^i)=m_{s,M}(G^i)$. This shows (a).

Moreover, for any $1\leq i\leq 1208$, and if $s\geq 4$, then the data computed in `2primary_Ss.txt` shows that $g_{s,M}(G^i)$ is divisible by $2\cdot g_{s,M}(\mathbb{Q},2)$ or

$3\cdot g_{s,M}(\mathbb{Q},2)$. And $g_{s,M}(G^i)$ is divisible by $3\cdot g_{s,M}(\mathbb{Q},2)$ but not by $3\cdot g_{s,M}(\mathbb{Q},2)$ only in one case, that of `X441`. This shows (b) and (c).

Finally, it follows from (b) that the minimal values $m_{s,M}(\mathbb{Q},2)$ are equal to the values $g_{s,M}(\mathbb{Q},2)$ for $0\le s\le 3$, and equal to $2\cdot g_{s,M}(\mathbb{Q},2)$ for $s\ge 4$. This shows (d). □

We remark that the values computed for Table 3 are fairly regular. Indeed, for $1\le s\le 3$ and $3\le N\le 5$, we have $g_{s,N}(\mathbb{Q},2)=2^{2(s+N-4)}$. Thus, the formulas can be simplified as follows.

Corollary 3.5. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $0\le s\le N$ be fixed integers, and let $T\subseteq E[2^N]$ be a subgroup isomorphic to $\mathbb{Z}/2^s\mathbb{Z}\oplus\mathbb{Z}/2^N\mathbb{Z}$. Then, $[\mathbb{Q}(T):\mathbb{Q}]$ is divisible by 2 if $s=N=2$, and otherwise by*

$$\begin{cases} 2^{2N-7} & \textit{if } s=0 \textit{ and } N\ge 4, \textit{ or}\\ 2^{2N+2s-8} & \textit{if } s\ge 1 \textit{ and } N\ge \max\{3,s\},\end{cases}$$

unless $s\ge 4$ and $j(E)$ is one of the two values

$$-\frac{3\cdot 18249920^3}{17^{16}} \quad \textit{or} \quad -\frac{7\cdot 1723187806080^3}{79^{16}}$$

in which case $[\mathbb{Q}(T):\mathbb{Q}]$ is divisible by $3\cdot 2^{2N+2s-9}$. Furthermore, these divisibility properties are best possible, in the sense that for each s,N there exists an elliptic curve $E/\mathbb{Q}$ and a subgroup $T\subseteq E[2^N]$ such that $[\mathbb{Q}(T):\mathbb{Q}]$ equals the bound above.

Proof. By Corollary 3.4, and specifically parts (2) and (b), it follows that $[\mathbb{Q}(T):\mathbb{Q}]$ is divisible by

$$\begin{cases} 2^{2N-7} & \text{if } s=0 \text{ and } N\ge 4, \text{ or}\\ 2^{2N+2s-8} & \text{if } 1\le s\le 3 \text{ and } N\ge 3,\\ 2^{2N+2s-8} \text{ or } 3\cdot 2^{2N+2s-9} & \text{if } 4\le s\le N.\end{cases}$$

However, part (c) says that the divisibility by $3\cdot 2^{2N+2s-9}$ and not by $2^{2N+2s-8}$ only occurs when the image is `X441`. By the work of [16], Section 8.3, the elliptic curves with 2-adic image `X441` are parametrized by a modular curve $\mathcal{X}_{441}$ which, in turn, is isomorphic to $X_{ns}^{+}(16)$, whose noncuspidal points classify elliptic curves whose mod 16 image of Galois is contained in the normalizer of a non-split Cartan subgroup (see Remarks 1.4 and 7.1, and Section 8.3 in [16]), and it is given by a model

$$X_{ns}^{+}(16) : y^2 = x^6 - 3x^4 + x^2 + 1.$$

The non-cuspidal rational points on $X_{ns}^{+}(16)$ were first computed by Baran [2] (and calculated again in [16], Section 8.3), and the only two non-CM associated j-invariants are

$$-\frac{3 \cdot 18249920^3}{17^{16}} \text{ or } -\frac{7 \cdot 1723187806080^3}{79^{16}}.$$

Hence, Corollary 3.4, part (c), implies that if $j(E)$ is not one of these two values, and $s \geq 4$, then $[\mathbb{Q}(T) : \mathbb{Q}]$ is actually divisible by $2^{2N+2s-8}$, as claimed.

Finally, the assertion that the divisibilities are best possible follows from Corollary 3.4, parts (a) and (b). □

We finish this section with a proof of Theorem 1.6 from the introduction.

Proof of Theorem 1.6. Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication, and let us first assume that p is a prime satisfying (A) and (B). In particular, Theorem 2.9 says that the representation $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ must be surjective (for $p > 13$ and $p \neq 17$ or 37). By [18], IV-24, Lemma 3, if $\rho_{E,p}$ is surjective and $p \geq 5$, then the p-adic representation ρ_{E,p^∞} must be surjective as well. Thus, Corollary 3.2 gives an exact value for $[\mathbb{Q}(T) : \mathbb{Q}]$ in this case, which coincide with the bounds stated in Theorem 1.6.

Otherwise, assume that p is a prime satisfying (A) and (C). Then, if we denote by $G = \rho_{E,p^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, we have that G is defined modulo p. Moreover, the mod-p image is either surjective, or the image is contained in one of the maximal subgroups of type (1), (2), or (3) of Theorem 2.9. In [20] and [21] such types of images have been completely classified, and there are only 63 possibilities of non-surjective mod-p images $G_1^i \cong \rho_{E,p}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, $1 \leq i \leq 63$. For each G^i defined to be the full inverse p-adic image of G_1^i, the bounds of Cor. 3.3 apply, where $n(K,p)$ can be taken to be 1 because these representations are defined modulo p. Thus, only $g_{k,1}(G^i)$, and $m_{k,1}(G^i)$, for $k = 0, 1$ play a role here. Each of these constants have been calculated with Magma, and recorded in Tables 5 and 6 below. Finally, in Table 2 we have calculated and recorded $g_{k,1}(\mathbb{Q}, p)$ and $m_{k,1}(\mathbb{Q}, p)$, for $k = 0, 1$. □

4. Examples

In Table 3 we have given the values of $g_{s,N}$, for $0 \leq s \leq N \leq 5$, which played an important role in the bounds given by Corollary 3.5, and as claimed in the statement, for each pair s, N there is an elliptic curve $E_{s,N}$ over $\mathbb{Q}$, and a subgroup $T_{s,N} \subseteq E_{s,N}(\overline{\mathbb{Q}})$ isomorphic to $\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$, such that $[\mathbb{Q}(T_{s,N}) : \mathbb{Q}]$ equals the bound given by Corollary 3.5. In fact, there are infinitely many non-isomorphic curves over $\mathbb{Q}$ with this property, given by one-parameter families (except for the two exceptional j-invariants mentioned in the statement of Corollary 3.5). In particular, the elliptic curves with 2-adic images `X193n` and `X441` up to conjugation (following the notation of [16]), which are parametrized by the elliptic surface $\mathcal{X}_{193n}$ and the modular curve $\mathcal{X}_{441}$, achieve the bound in all cases except for $s = 0$ and $N \geq 1$, or $s = N = 2$, which are achieved by the 2-adic images `X235l` or `X58i` up to conjugation, respectively (and parametrized by the surfaces $\mathcal{X}_{235l}$ or $\mathcal{X}_{58i}$ which we will give below). Here are the models of the modular curves (note that we have simplified the models of $\mathcal{X}_{58i}$, $\mathcal{X}_{193n}$, and $\mathcal{X}_{235l}$ given in [16], by changing variables so that $(0, 0)$ belongs to the elliptic surface).

$$\begin{aligned}
\mathcal{X}_{58i} &: y^2 = x^3 - 2(t^4 + 1)x^2 + (t^8 - 2t^4 + 1)x,\\
\mathcal{X}_{193n} &: y^2 = x^3 + (256t^8 - 256t^6 + 352t^4 - 16t^2 + 1)x^2 + 256t^4(4t^2 - 1)^4x,\\
\mathcal{X}_{235l} &: y^2 = x^3 + (t^8 - 4t^6 - 2t^4 - 4t^2 + 1)x^2 + 16t^8x,\\
\mathcal{X}_{441} &: y^2 = x^6 + x^4 - 3x^2 + 1.
\end{aligned}$$

As mentioned in the proof of Corollary 3.5, the curve $\mathcal{X}_{441} = X_{ns}^+(16)$, a modular curve of genus 2, contains only two non-cuspidal rational points that correspond to non-CM elliptic curves, whose j-invariants are given in the statement of the corollary.

In this section we show explicitly, as an example, the field of definition of $T = \mathbb{Z}/2^N\mathbb{Z}$ for $N \leq 5$ (with T chosen so that $[\mathbb{Q}(T) : \mathbb{Q}]$ is minimal) in the elliptic surface $\mathcal{X}_{235l}$ and points of order 2^N for $N = 3, 4, 5$. The 2-adic image `X235l` (as always, following the notation of [16]) is defined modulo 16. For each elliptic curve E with image `X235l` (up to conjugation) there is a subgroup $T \cong \mathbb{Z}/2^N\mathbb{Z} \subseteq E[2^N]$, for $N \geq 4$, such that $[\mathbb{Q}(T) : \mathbb{Q}] = 2^{2N-7}$. Indeed, let us show that

$$g_{0,4}(\texttt{X235l}) = g_{0,4}(\mathbb{Q}, 2) = 2, \quad \text{and} \quad g_{0,5}(\texttt{X235l}) = g_{0,5}(\mathbb{Q}, 2) = 2^3.$$

In order to do this, we show explicitly that the curves with image `X235l` (up to conjugation) have a 16-torsion point defined over a quadratic extension of $\mathbb{Q}$, and a 32-torsion point defined over an extension of degree 8. As shown in [16], the curves with 2-adic image `X235l` are parametrized by the surface $\mathcal{X}_{235l}$ that appears above (see also our Remark 2.8 to find the model in their database). The torsion structure and generators of $\mathcal{X}_{235l}$ over $\mathbb{Q}(t)$ can be computed with Magma, and it is isomorphic to $\mathbb{Z}/8\mathbb{Z}$ with the following generator:

$$P_8 = (4t^2, -4t^2(t^4-1)).$$

Over the quadratic extension $K = \mathbb{Q}(\sqrt{(t^4-1)(t^2+2t-1)})$ the point:

$$P_{16} = (2t(t^4-1)+2t\alpha, 2t(t^8-4t^6+2t^5-2t^4-2t+1)+2t(t^4+2t-1)\alpha),$$

where $\alpha = 2t+(t-1)\sqrt{(t^4-1)(t^2+2t-1)}$, is of order 16.

To obtain a point of order 32 it is necessary to go to $L = \mathbb{Q}(t)(\beta)$, a degree 4 extension of K, where β satisfies:

$$\begin{aligned}&\beta^4 + (-12t\alpha - 2t^8 + 8t^6 - 12t^5 + 4t^4 + 8t^2 + 12t - 2)\beta^2\\ &+ ((-16t^5 - 32t^2 + 16t)\alpha - 16t^9 + 64t^7 - 32t^6 + 32t^5 + 32t^2 - 16t)\beta\\ &+ (-4t^9 + 16t^7 - 24t^6 + 8t^5 - 32t^3 + 24t^2 - 4t)\alpha + t^{16} - 8t^{14} - 4t^{13}\\ &+ 12t^{12} + 16t^{11} - 16t^{10} + 12t^9 + 22t^8 - 48t^7 + 56t^6 - 12t^5 + 12t^4 + 32t^3\\ &- 32t^2 + 4t + 1 = 0\end{aligned}$$

and the point of order 32 is:

$$\begin{aligned}P_{32} = (&1/2\beta^2 - t\alpha - 1/2t^8 + 2t^6 - t^5 + t^4 + 2t^2 + t - 1/2,\\ &1/2\beta^3 + (-3t\alpha - 1/2t^8 + 2t^6 - 3t^5 + t^4 + 2t^2 + 3t - 1/2)\beta\\ &+ (-2t^5 - 4t^2 + 2t)\alpha - 2t^9 + 8t^7 - 4t^6 + 4t^5 + 4t^2 - 2t).\end{aligned}$$

Remark 4.1. In the example above we have $2P_{32} = P_{16}$, and $2P_{16} = P_8$. We have halved these points using the 2-divisibility method (cf. [9], or [8, Prop. 12]). This method establishes that if E is an elliptic curve defined over a field K and $P \in E(K)[N]$ then there exists $Q \in E(L)[2N]$ where $[L : K] \leq 4$ [9, Theorem 3.1]. We note here that while [8] or [9] use the 2-divisibility method over number fields, the same method applies to function fields as well.

4.1. Examples of p-adic representations defined modulo p

In this section we give examples of elliptic curves $E/\mathbb{Q}$ and primes p such that the condition (C) of Theorem 1.6 is verified, i.e., p-adic representations attached to elliptic curves that are defined modulo p. We have also calculated the constants $g_{k,1}$ and $m_{k,1}$, for $k = 0, 1$, for each of the examples that appear in this section, and they are listed in Table 5.

For $p = 2$, the classification of [16] of all possible 2-adic images (for non-CM elliptic curves) includes the level of definition of the image. In particular, the images X1, X2, X6, and X8 are the only images defined modulo 2, and these correspond to $\mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z})$, 2Cn, 2B, and 2Cs (in the notation of [20]) for X1, X2, X6, and X8, respectively. The following elliptic curves are examples in each image defined modulo 2:

- 2-adic image X1, corresponds to all of $\mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z})$ modulo 2, and 11a1 is an example.
- 2-adic image X2, corresponds to image 2Cn modulo 2, and 196a1 is an example.
- 2-adic image X6, corresponds to image 2B modulo 2, and 69a1 is an example.
- 2-adic image X8, corresponds to image 2Cs modulo 2, and 315b2 is an example.

For $p > 2$, in order to check that an image is defined modulo p, it suffices to check that the image modulo p^2 is the full inverse image of the mod-p image, by the following result.

Lemma 4.2 ([1], Lemma 2.2). *Let $n \geq 1$ be an integer and let $p > 2$ be a prime. Let H be a closed subgroup of $\mathrm{GL}(2, \mathbb{Z}_p)$. Then H contains $1 + p^n M(2, \mathbb{Z}_p)$ if and only if $H \bmod p^{n+1}$ contains $1 + p^n M(2, \mathbb{Z}/p^{n+1}\mathbb{Z})$.*

We have used the previous Lemma, to find examples where $\rho_{E,9}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is the full inverse image of $\rho_{E,3}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$. In order to show this, we used Magma to verify that

$$|\operatorname{Gal}(\mathbb{Q}(E[9])/\mathbb{Q})|/|\operatorname{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})| = 3^4.$$

We obtained the following examples of each of the images defined modulo 3:

- Image $\mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z})$ modulo 3, the curve 11a1 is an example.
- Image 3Cs.1.1 modulo 3, the curve 14a1 is an example.
- Image 3Cs modulo 3, the curve 98a3 is an example.
- Image 3B.1.1 modulo 3, the curve 30a1 is an example.
- Image 3B.1.2 modulo 3, the curve 20a3 is an example.

- Image 3Ns modulo 3, the curve 338d1 is an example.
- Image 3B modulo 3, the curve 50b1 is an example.
- Image 3Nn modulo 3, the curve 245a1 is an example.

Let us verify, for instance, that if E is the curve with Cremona label 11a1, then $\rho_{E,3^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathrm{GL}(2, \mathbb{Z}_3)$. Either by looking up the mod 3 image in the Cremona database [7], or by direct computation (using the 3-division polynomial and checking that $[\mathbb{Q}(E[3]) : \mathbb{Q}] = 48 = (3-1) \cdot 3 \cdot (3^2 - 1) = |\,\mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z})|$), we verify first that $\rho_{E,3}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z})$. We note here that $[\mathbb{Q}(x(E[3])) : \mathbb{Q}] = 24$. Now we compute $[\mathbb{Q}(E[9]) : \mathbb{Q}(E[3])]$. The 9-th division polynomial for $E/\mathbb{Q}$ factors as $\psi_9(x) = \psi_3(x)f(x)$ over $\mathbb{Q}[x]$, where the degrees of ψ_3 and f are 4 and 36, respectively. Here $\psi_3(x)$ is the 3-rd division polynomial, whose splitting field is $\mathbb{Q}(x(E[3]))$, and the splitting field of $f(x)$ is $\mathbb{Q}(x(E[9]))$. The extension $L/\mathbb{Q}$ generated by a root of $f(x)$, thus, is a number field of degree 36, and Magma tells us that the Galois group of f has degree 1944. Hence, the Galois closure of L, i.e., $\mathbb{Q}(x(E[9]))$ is of degree $1944 = 24 \cdot 3^4$ over $\mathbb{Q}$, and the extension $\mathbb{Q}(x(E[9]))/\mathbb{Q}(x(E[3]))$ is of degree 3^4. Therefore

$$[\mathbb{Q}(E[9]) : \mathbb{Q}(E[3])] = [\mathbb{Q}(x(E[9])) : \mathbb{Q}(x(E[3]))] = 3^4.$$

Hence, by Lemma 4.2, we conclude that $\rho_{E,3^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \mathrm{GL}(2, \mathbb{Z}_3)$, as desired.

Unfortunately, we have not been able to verify $\rho_{E,p^2}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is the full inverse image of the mod-p image, for any elliptic curve with non-surjective image modulo $p > 3$.

4.2. About the Tables 5 and 6

As mentioned in Conjecture 2.10, Sutherland and Zywina ([20], [21]) have found a list of 63 exceptional mod-p images that do occur for non-CM curves $E/\mathbb{Q}$, and that, together with $\mathrm{GL}(2, \mathbb{F}_p)$, would be the complete list if the answer to Serre's uniformity question is positive. We list all such possible images in Tables 5 and 6, together with the values of the prime p, the label of the type of mod p representation, and the constants $g_{0,1}(G)$, $m_{0,1}(G)$, and $g_{1,1}(G) = m_{1,1}(G)$ that appear in Theorem 1.6. In other words, if $E/\mathbb{Q}$ is an elliptic curve such that $\rho_{E,p^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is the full inverse image of its mod p representation, then Theorem 1.6 applies with the constants as given in these tables. In addition to the constants we have added an example of an elliptic curve whose mod p representation is the group indicated in the second column. However, as explained in the previous section, for $p > 3$ we have not been able to verify that, for each of the examples $E/\mathbb{Q}$ we give, the representation ρ_{E,p^∞} is indeed defined modulo p.

Finally, we note that $m_{0,1}(G)$ and $m_{1,1}(G)$ appear listed in [20], Tables 3 and 4, as d_1 and d, respectively. The tables in [20] also give generators for each type of image.

p	G	$g_{0,1}(G)$	$m_{0,1}(G)$	$g_{1,1}(G) = m_{1,1}(G)$	Example $E/\mathbb{Q}$
2	2Cs	1	1	1	315b2
2	2B	1	1	2	69a1
2	2Cn	3	3	3	196a1
2	$\mathrm{GL}(2,\mathbb{F}_2)$	3	3	6	11a1
3	3Cs.1.1	1	1	2	14a1
3	3Cs	2	2	4	98a3
3	3B.1.1	1	1	6	30a1
3	3B.1.2	1	2	6	20a3
3	3Ns	4	4	8	338d1
3	3B	2	2	12	50b1
3	3Nn	8	8	16	245a1
3	$\mathrm{GL}(2,\mathbb{F}_3)$	8	8	48	11a1
5	5Cs.1.1	1	1	4	11a1
5	5Cs.1.3	2	2	4	275b2
5	5Cs.4.1	2	2	8	99d2
5	5Ns.2.1	8	8	16	6975a1
5	5Cs	4	4	16	18176b2
5	5B.1.1	1	1	20	11a3
5	5B.1.2	1	4	20	11a2
5	5B.1.3	2	4	20	50a1
5	5B.1.4	2	2	20	50a3
5	5Ns	8	8	32	608b1
5	5B.4.1	2	2	40	99d1
5	5B.4.2	2	4	40	99d3
5	5Nn	24	24	48	675b1
5	5B	4	4	80	338d1
5	5S4	24	24	96	324b1
5	$\mathrm{GL}(2,\mathbb{F}_5)$	24	24	480	14a1

Table 5: $g_{k,1}(G)$ and $m_{k,1}(G)$, for $k = 0, 1$, and example curves.

p	G	$g_{0,1}(G)$	$m_{0,1}(G)$	$g_{1,1}(G) = m_{1,1}(G)$	Example $E/\mathbb{Q}$
7	7Ns.2.1	3	6	18	2450ba1
7	7Ns.3.1	6	12	36	2450a1
7	7B.1.1	1	1	42	26b1
7	7B.1.2	3	3	42	637a1
7	7B.1.3	1	6	42	26b2
7	7B.1.4	1	3	42	294a1
7	7B.1.5	3	6	42	637a2
7	7B.1.6	1	2	42	294a2
7	7Ns	12	12	72	9225a1
7	7B.6.1	2	2	84	208d1
7	7B.6.2	6	6	84	5733d1
7	7B.6.3	2	6	84	208d2
7	7Nn	48	48	96	15341a1
7	7B.2.1	3	3	126	162b1
7	7B.2.3	3	6	126	162b3
7	7B	6	6	252	162c1
7	$\mathrm{GL}(2, \mathbb{F}_7)$	48	48	2016	11a1
11	11B.1.4	5	5	110	121a2
11	11B.1.5	5	5	110	121c2
11	11B.1.6	5	10	110	121a1
11	11B.1.7	5	10	110	121c1
11	11B.10.4	10	10	220	1089f2
11	11B.10.5	10	10	220	1089f1
11	11Nn	120	120	240	232544f1
11	$\mathrm{GL}(2, \mathbb{F}_{11})$	120	120	13200	11a1
13	13S4	24	72	288	152100g1
13	13B.3.1	3	3	468	147b1
13	13B.3.2	3	12	468	147b2
13	13B.3.4	6	6	468	24843o1
13	13B.3.7	6	12	468	24843o2
13	13B.5.1	4	4	624	2890d1
13	13B.5.2	4	12	624	2890d2
13	13B.5.4	12	12	624	216320i1
13	13B.4.1	6	6	936	147c1
13	13B.4.2	6	12	936	147c2
13	13B	12	12	1872	2450l1
13	$\mathrm{GL}(2, \mathbb{F}_{13})$	168	168	26208	11a1
17	17B.4.2	8	8	1088	14450n1
17	17B.4.6	8	16	1088	14450n2
17	$\mathrm{GL}(2, \mathbb{F}_{17})$	288	288	78336	11a1
37	37B.8.1	12	12	15984	1225e1
37	37B.8.2	12	36	15984	1225e2
37	$\mathrm{GL}(2, \mathbb{F}_{37})$	1368	1368	1822176	11a1
else	$\mathrm{GL}(2, \mathbb{F}_p)$	$p^2 - 1$	$p^2 - 1$	$(p-1)p(p^2-1)$	11a1

Table 6: $g_{k,1}(G)$ and $m_{k,1}(G)$, for $k = 0, 1$, and example curves.

Acknowledgements

We would like to thank Andrew Sutherland and David Zywina for several helpful references and remarks. The second author would like to thank the Universidad Autónoma de Madrid, where much of this work was completed during a sabbatical visit, for its hospitality. Finally, we would like to thank the editors and the referee(s) for a very efficient and helpful editorial and review process.

References

[1] Keisuke Arai, *On uniform lower bound of the Galois images associated to elliptic curves*, J. Théor. Nombres Bordeaux **20** (2008), no. 1, 23–43.

[2] Burcu Baran, *Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem*, J. Number Theory **130** (2010), no. 12, 2753–2772.

[3] Yuri Bilu and Pierre Parent, *Serre's uniformity problem in the split Cartan case*, Ann. of Math. (2) **173** (2011), no. 1, 569–584.

[4] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on* $X_0^+(p^r)$, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984.

[5] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993).

[6] Abbey Bourdon, Pete L. Clark, and Paul Pollack, *Anatomy of torsion in the cm case*, Math. Z. **285** (2017), no. 3, 795–820..

[7] John E. Cremona, *Elliptic curve data for conductors up to 350.000*, available at `http://homepages.warwick.ac.uk/~masgaj/ftp/data/`, 2015.

[8] Enrique González-Jiménez and José M. Tornero, *Torsion of rational elliptic curves over quadratic fields II*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM **110** (2016), no. 1, 121–143.

[9] Daeyeol Jeon, Chang Heon Kim, and Yoonjin Lee, *Infinite families of elliptic curves over dihedral quartic number fields*, J. Number Theory **133** (2013), no. 1, 115–122.

[10] Sheldon Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229.

[11] M. A. Kenku and Fumiyuki Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.

[12] Álvaro Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Math. Ann. **357** (2013), no. 1, 279–305.

[13] Barry C. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[14] Filip Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Lett. **23** (2016), 245–272.

[15] Dipendra Prasad and Chalya S. Yogananda, *Bounding the torsion in CM elliptic curves*, C. R. Math. Acad. Sci. Soc. R. Can. **23** (2001), no. 1, 1–5.

[16] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of galois*, Research in Number Theory 1:12 (data files and subgroup descriptions available at `http://users.wfu.edu/rouseja/2adic/`, 2015.

[17] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[18] Jean-Pierre Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401.

[19] Alice Silverberg, *Torsion points on abelian varieties of CM-type*, Compositio Math. **68** (1988), no. 3, 241–249.

[20] Andrew Sutherland, *Computing images of galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), e4

[21] David Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*, `arXiv:1508.07660`.

Departamento de Matemáticas
Universidad Autónoma de Madrid
Madrid, Spain
E-mail address: `enrique.gonzalez.jimenez@uam.es`

Department of Mathematics
University of Connecticut
Storrs, CT 06269, USA
E-mail address: `alvaro.lozano-robledo@uconn.edu`

Received May 10, 2015