ON THE FIELD OF DEFINITION OF p-TORSION POINTS ON ELLIPTIC CURVES OVER THE RATIONALS

ÁLVARO LOZANO-ROBLEDO

Abstract. Let $S_{\mathbb{Q}}(d)$ be the set of primes p for which there exists a number field K of degree $\leq d$ and an elliptic curve $E/\mathbb{Q}$, such that the order of the torsion subgroup of $E(K)$ is divisible by p. In this article we give bounds for the primes in the set $S_{\mathbb{Q}}(d)$. In particular, we show that, if $p \geq 11$, $p \neq 13, 37$, and $p \in S_{\mathbb{Q}}(d)$, then $p \leq 2d+1$. Moreover, we determine $S_{\mathbb{Q}}(d)$ for all $d \leq 42$, and give a conjectural formula for all $d \geq 1$. If Serre's uniformity problem is answered positively, then our conjectural formula is valid for all sufficiently large d. Under further assumptions on the non-cuspidal points on modular curves that parametrize those j-invariants associated to Cartan subgroups, the formula is valid for all $d \geq 1$.

1. Introduction

Let K be a number field of degree $d \geq 1$ and let E/K be an elliptic curve. The Mordell-Weil theorem states that $E(K)$, the set of K-rational points on E, can be given the structure of a finitely generated abelian group. Thus, there is an integer $R \geq 0$ such that $E(K) \cong E(K)_{\text{tors}} \oplus \mathbb{Z}^R$ and the torsion subgroup $E(K)_{\text{tors}}$ is finite. Here, we will focus on the order of $E(K)_{\text{tors}}$. In particular, we are interested in the following question: if we fix $d \geq 1$, what are the possible prime divisors of the order of $E(K)_{\text{tors}}$, for E and K as above?

Definition 1.1. *We define $S(d)$ as the set of primes p for which there exists a number field K of degree $\leq d$ and an elliptic curve E/K such that $|E(K)_{tors}|$ is divisible by p. We also define $\Phi(d)$ as the set of all possible isomorphism types for $E(K)_{tors}$, over all K and E as above.*

The following list represents some highlights (in chronological order) of what is known about the sets $S(d)$ and $\Phi(d)$:

- (Mazur, [33]) $S(1) = \{2, 3, 5, 7\}$ and $\Phi(1)$ is determined, with 15 types.
- (Kamienny, Mazur, [21]; see also [11]) $S(2) = \{2, 3, 5, 7, 11, 13\}$ and $\Phi(2)$ has 26 types.
- (Faltings, Frey, [16], [17]) If $S(d)$ is finite, then $\Phi(d)$ is finite.
- (Merel, [36]) For all $d \geq 1$, the set $S(d)$ is always finite; thus, $\Phi(d)$ is also finite. Moreover, if $d > 1$ and $p \in S(d)$, then $p \leq d^{3d^2}$.
- (Osterlé, unpublished work but mentioned in [36]) If $p \in S(d)$, then $p \leq (3^{d/2}+1)^2$.
- (Parent, [39]) $S(3) = \{2, 3, 5, 7, 11, 13\}$.

In addition, Derickx, Kamienny, Stein, and Stoll ([9]) have recently shown using a computational method that $S(4) = S(3) \cup \{17\}$, $S(5) = S(4) \cup \{19\}$, and $S(6) \subseteq S(5) \cup \{37, 73\}$.

In this article, we restrict our study to the simpler case of elliptic curves E/K that arise from elliptic curves defined over $\mathbb{Q}$ whose base field has been extended to K.

1991 *Mathematics Subject Classification.* Primary: 11G05, Secondary: 14H52.

Definition 1.2. *Let $S_{\mathbb{Q}}(d)$ be the set of primes p for which there exists a number field K of degree $\leq d$ and an elliptic curve $E/\mathbb{Q}$, such that $|E(K)_{tors}|$ is divisible by p.*

Clearly $S_{\mathbb{Q}}(d) \subseteq S(d)$ and $S_{\mathbb{Q}}(1) = S(1)$ but, as we shall see, $S_{\mathbb{Q}}(2) = S(1) \subsetneq S(2)$. Our first theorem provides an upper bound for the primes in $S_{\mathbb{Q}}(d)$.

Theorem 1.3. *Let $p \geq 11$ with $p \neq 13$ or 37, and such that $p \in S_{\mathbb{Q}}(d)$. Then $p \leq 2d+1$.*

In order to show Theorem 1.3, we will prove the following. Let $E/\mathbb{Q}$ be an elliptic curve and $p \geq 11$ be a prime, other than 13. Let K be a number field of degree $d \geq 1$ such that $|E(K)_{\mathrm{tors}}|$ is divisible by p. Then $d \geq (p-1)/2$ unless $j(E) = -7 \cdot 11^3$ and $p = 37$, in which case $d \geq (p-1)/3 = 12$. We will also show that $13 \in S_{\mathbb{Q}}(3)$ and $37 \in S_{\mathbb{Q}}(12)$.

The bounds of Theorem 1.3, together with the refined bounds of Theorem 2.1 below, will allow us to determine $S_{\mathbb{Q}}(d)$ for small values of d. We will also provide a conjectural formula for $S_{\mathbb{Q}}(d)$. If a question of Serre is answered positively, then our formula holds for all sufficiently large d. Under further assumptions, the formula holds for all $d \geq 1$.

Let $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[p])$ be the representation induced by the action of Galois on $E[p]$. In [43] §4.3, Serre asked whether there is a constant N, that does not depend on E, and such that $\rho_{E,p}$ is surjective for all elliptic curves $E/\mathbb{Q}$ without CM, and for all $p > N$. Serre actually asks whether $N = 37$ works. This question, usually known as "Serre's uniformity problem", has generated great interest (see [2], [6], [7], [27], [32], [40]). It has been solved by Mazur in the Borel case ([33]), by Serre in the exceptional case ([46]) and by Bilu and Parent in the split Cartan case ([2]). Only the non-split Cartan case remains to be solved. For more details on this topic, see the introduction of [2], or [35], §2.

Theorem 1.4. *Let $d \geq 1$ and define sets of primes $A = \{2,3,5,7\} \cup \{13, \text{ if } d \geq 3\} \cup \{37, \text{ if } d \geq 12\}$, and sets B, C, D, F by:*

$$\begin{aligned} B &= \{\text{primes } p = 11, 17, 19, 43, 67, \text{ or } 163 \text{ and such that } p \leq 2d+1\}, \\ C &= \{\text{primes } p \text{ such that } p \leq \sqrt{d+1}\},\ D = \{\text{primes } p \text{ such that } p \leq d+1\} \end{aligned}$$

and let F be the set of all primes $11 \leq p \leq d/2+1$ such that there is a quadratic imaginary field of class number 1 in which p splits. Then:

1. *$A \cup B \cup C \cup F \subseteq S_{\mathbb{Q}}(d) \subseteq A \cup B \cup D$, and*
2. *Suppose that there is a constant $M \geq 11$ such that, for all primes $p > M$ either $E/\mathbb{Q}$ is CM, or $\rho_{E,p}$ is surjective, or its image is a Borel. Then $A \cup B \cup C \cup F = S_{\mathbb{Q}}(d)$ for all $d \geq M^2 - 1$.*

We note that, if $d \leq 21$ and $p \in S_{\mathbb{Q}}(d) \cap D$, then $p \in A \cup B$. It follows that $S_{\mathbb{Q}}(d) = A \cup B \cup C \cup F$ for all $d \leq 21$. This allows us to give an explicit description of $S_{\mathbb{Q}}(d)$ for $d \leq 21$.

Corollary 1.5. *Let $S_{\mathbb{Q}}(d)$ be the set of Definition 1.2.*

- $S_{\mathbb{Q}}(d) = \{2,3,5,7\}$ *for $d = 1$ and 2;*
- $S_{\mathbb{Q}}(d) = \{2,3,5,7,13\}$ *for $d = 3$ and 4;*
- $S_{\mathbb{Q}}(d) = \{2,3,5,7,11,13\}$ *for $d = 5$, 6, and 7;*
- $S_{\mathbb{Q}}(d) = \{2,3,5,7,11,13,17\}$ *for $d = 8$;*
- $S_{\mathbb{Q}}(d) = \{2,3,5,7,11,13,17,19\}$ *for $d = 9$, 10, and 11;*
- $S_{\mathbb{Q}}(d) = \{2,3,5,7,11,13,17,19,37\}$ *for $12 \leq d \leq 20$.*
- $S_{\mathbb{Q}}(d) = \{2,3,5,7,11,13,17,19,37,43\}$ *for $d = 21$.*

Question 1.6. Does the formula for $S_{\mathbb{Q}}(d) = A \cup B \cup C \cup F$ hold for all $d \geq 1$?

The answer to this question, as well as Serre's uniformity problem, hinges in a deeper understanding of non-cuspidal points on the modular curves that classify those elliptic curves whose representations $\rho_{E,p}$ have an image contained in the normalizer of a split or non-split Cartan subgroup. In the following theorem we show that recent work of Bilu, Parent and Rebolledo, and further assumptions on the Cartan cases imply better bounds, or even a positive answer to Question 1.6.

Theorem 1.7. *Let $d \geq 1$ be fixed, let A, B, C, F be the sets of primes defined above, and let F' be the set of all primes $p \leq d/2 + 1$. Then*

$$A \cup B \cup C \cup F \subseteq S_{\mathbb{Q}}(d) \subseteq A \cup B \cup F'.$$

Moreover, suppose that the following hypothesis is verified for all primes $13 < p < d/2 + 1$ that do not belong to $A \cup B$:

- (H) *If $E/\mathbb{Q}$ is an elliptic curve such that the image of $\rho_{E,p}$ is contained in a normalizer of a non-split Cartan subgroup, then the image is either a full non-split Cartan subgroup or its normalizer.*

Then, $A \cup B \cup C \cup F = S_{\mathbb{Q}}(d)$.

Remark 1.8. Theorem 1.7 relies on recent progress towards Serre's uniformity problem. Let p be a prime and let (H') be the following condition for p:

- (H') If $E/\mathbb{Q}$ is an elliptic curve such that the image of $\rho_{E,p}$ is contained in a normalizer of a split Cartan subgroup, then the curve $E/\mathbb{Q}$ has CM by a quadratic imaginary field K and p splits in $K/\mathbb{Q}$.

Here is a brief history of the recent developments on our understanding of hypothesis (H'). Rebolledo showed in her thesis ([42], a corollary of Thm. (0.12)) that hypothesis (H') holds for all $13 < p < 1873$ (see also the work of Momose [37]). As part of his thesis, Daniels [8] has shown that (H') holds for $p = 11$. Furthermore, in their groundbreaking paper [2], Bilu and Parent have shown that there is a constant N such that (H') holds for all $p \geq N$. Finally, building on [2] and some recent work of Gaudron and Rémond [14], the collaborators Bilu, Parent and Rebolledo [3] have shown that (H') holds for all $p \geq 11$ except for $p = 13$. If Serre's uniformity problem is answered positively in the non-split case for all $p > 13$, this would imply condition (H), by Theorem 7.6.

Corollary 1.9. *The formula $S_{\mathbb{Q}}(d) = A \cup B \cup C \cup F$ is valid for all $1 \leq d \leq 42$.*

The proof of Theorem 1.3 will be summarized in Section 2 and completed in Sections 3 through 9. The proofs of Theorems 1.4, 1.7, and Corollary 1.9 will be given in Section 2. Our results rest on the work of Serre ([43]; see Section 3) and the classification of non-cuspidal rational point on the modular curves $X_0(N)$. For the convenience of the reader, we have collected all non-cuspidal $\mathbb{Q}$-points on $X_0(N)$, for all $N \geq 1$, in Tables 3 and 4 of Subsection 9.1.

2. Refined Bounds

In this section we discuss bounds for the field of definition of a p-torsion point on an elliptic curve $E/\mathbb{Q}$. The proof of Theorem 2.1 also serves as a table of contents for the organization of the rest of the paper.

Theorem 2.1. *Let $E/\mathbb{Q}$ be an elliptic curve and let $p \geq 11$ be a prime, other than 13. Let $R \in E[p]$ be a torsion point of exact order p and let $\mathbb{Q}(R) = \mathbb{Q}(x(R), y(R))$ be the field of definition of R. Then*

$$[\mathbb{Q}(R) : \mathbb{Q}] \geq \frac{p-1}{2}$$

unless $j(E) = -7 \cdot 11^3$ and $p = 37$, in which case $[\mathbb{Q}(R) : \mathbb{Q}] \geq (p-1)/3 = 12$. More concretely, suppose $j(E) \neq -7 \cdot 11^3$:

1. *If the image of $\rho_{E,p}$, with respect to an $\mathbb{F}_p$-basis $\{P, Q\}$ of $E[p]$, is a Borel subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$, then $p = 11$, 17, 19, 37, 43, 67 or 163. Moreover, if $R \in \langle P \rangle$, then $\mathbb{Q}(R)/\mathbb{Q}$ is Galois, cyclic and $[\mathbb{Q}(R) : \mathbb{Q}] = (p-1)/2$ or $(p-1)$. Otherwise, $[\mathbb{Q}(R) : \mathbb{Q}] \geq p$.*
2. *If the image of $\rho_{E,p}$ is not a Borel (in any basis), then $[\mathbb{Q}(R) : \mathbb{Q}] \geq p - 1$.*

Proof. Let E, $p \geq 11$ but $p \neq 13$, and $\rho_{E,p}$ be as in the statement of the theorem, and let R be an arbitrary torsion point in $E(\overline{\mathbb{Q}})$ of exact order p. Let G be the image of $\rho_{E,p}$ in $\mathrm{GL}(E[p])$. By the work of Serre (see Section 3), either G is all of $\mathrm{GL}(2, \mathbb{F}_p)$, or it is contained in one of 4 types of maximal subgroups (Theorem 3.2), so we break the proof into 5 cases:

1. If $G = \mathrm{GL}(E[p])$, then $[\mathbb{Q}(R) : \mathbb{Q}] = p^2 - 1$ by Theorem 5.1;
2. If G is contained in a split Cartan subgroup of $\mathrm{GL}(E[p])$, then $p \leq 5$ by Theorem 6.2. If G is contained in the normalizer of a split Cartan, then $[\mathbb{Q}(R) : \mathbb{Q}] \geq p - 1$ by Theorem 6.5;
3. If G is contained in the normalizer of a non-split Cartan subgroup, then $[\mathbb{Q}(R) : \mathbb{Q}] \geq 2(p-1)$ by Theorem 7.3;
4. If the projective image of G in $\mathrm{PGL}(E[p])$, call it $\overline{G}$, is isomorphic to A_4, S_4 or A_5, then $p \leq 13$ and $\overline{G} \cong S_4$, by Theorem 8.1. Moreover, if $p = 11$ then $[\mathbb{Q}(R) : \mathbb{Q}] \geq 60 > 10 = p - 1$ by Theorem 8.3;
5. Finally, if the image of $\rho_{E,p}$, with respect to an $\mathbb{F}_p$-basis $\{P, Q\}$ of $E[p]$, is a Borel subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$, then $p = 11$, 17, 19, 37, 43, 67 or 163 by the classification of all non-cuspidal $\mathbb{Q}$-points on the modular curves $X_0(N)$, when N is prime (see Subsection 9.1 and, in particular, Table 4). The results on $[\mathbb{Q}(R) : \mathbb{Q}]$ are shown in Theorems 9.3 and 9.4.

Thus, the proof of Theorem 2.1 is complete. □

Theorem 1.3 is an immediate consequence of Theorem 2.1. We can also deduce Theorem 1.4.

Proof of Theorem 1.4. Let us begin by discussing the cases of $p = 13$ and $p = 37$. The prime $13 \in S_{\mathbb{Q}}(d)$ if and only if $d \geq 3$. Indeed, by the work of Laska, Lorenz, and Fujita, $13 \notin S_{\mathbb{Q}}(2) = S(1)$, but as the following example (due to Elkies) demonstrates, 13 belongs to $S_{\mathbb{Q}}(3)$: let E be the elliptic curve defined by $y^2 + y = x^3 + x^2 - 114x + 473$. Then E has a torsion point of order 13 defined over $K/\mathbb{Q}$, a cubic Galois extension, where $K = \mathbb{Q}(\alpha)$ and $\alpha^3 - 48\alpha^2 + 425\alpha - 1009 = 0$. A point $P \in E$ of order 13 is $(\alpha, 7\alpha - 39)$.

By Theorem 2.1, if $p = 37$ belongs to $S_{\mathbb{Q}}(d)$, then $d \geq 12$. Moreover, $37 \in S_{\mathbb{Q}}(12)$. Indeed, the elliptic curve $y^2 + xy + y = x^3 + x^2 - 8x + 6$ has a point of order 37 defined over the number field of degree 12 over $\mathbb{Q}$ (see the proof of Theorem 9.4 for more details).

Now we can show that $S_{\mathbb{Q}}(d) \subseteq A \cup B \cup D$. Suppose $p \in S_{\mathbb{Q}}(d) \setminus A$ and let K be a number field of degree d and $E/\mathbb{Q}$ an elliptic curve with $|E(K)_{\mathrm{tors}}|$ divisible by p. By Theorem 2.1, if the image of $\rho_{E,p}$ is a Borel (and $p \notin A$), then $p = 11$, 17, 19, 43, 67 or 163 and $d \geq (p-1)/2$. Thus, $p \leq 2d + 1$ and $p \in B$. If the image of $\rho_{E,p}$ is not a Borel, then $d \geq p - 1$, so $p \in D$. Hence, $S_{\mathbb{Q}}(d) \subseteq A \cup B \cup D$. This shows the containment of $S_{\mathbb{Q}}(d)$ in (1).

We know that $S_{\mathbb{Q}}(1) = S(1)$, which was determined by Mazur, [33]. The fact that $S_{\mathbb{Q}}(2) = S(1)$ follows from a theorem of Laska, Lorenz and Fujita (see [19]). Together with the facts about $p = 13$ and 37, this shows $A \subseteq S_{\mathbb{Q}}(d)$.

By Theorem 2.1, if $p = 17$ belongs to $S_{\mathbb{Q}}(d)$, then $d \geq 8$. The following example shows that $17 \in S_{\mathbb{Q}}(8)$. The elliptic curve $y^2 + xy = x^3 + x^2 - 660x - 7600$ with $j = -17 \cdot 373^3/2^{17}$ has a 17-torsion point defined over $\mathbb{Q}(\alpha)$ where α is a root of

$$x^8 - 30x^7 + 23620x^6 - 694800x^5 + 174568000x^4 - 3730176000x^3$$
$$+472522624000x^2 - 5238622720000x + 343420835840000 = 0.$$

Moreover, for each $p = 11$, 19, 43, 67, or 163, there is an elliptic curve $E/\mathbb{Q}$ with CM by $\mathbb{Q}(\sqrt{-p})$ and a non-trivial point $P \in E[p]$ such that $[\mathbb{Q}(P) : \mathbb{Q}] = (p-1)/2$ (this will be shown below in Corollary 9.8). Hence, if $p \in B$, then $p \in S_{\mathbb{Q}}(d)$. We have shown that $A \cup B \subseteq S_{\mathbb{Q}}(d)$.

Let $E/\mathbb{Q}$ be an elliptic curve with CM by an order $\mathcal{O}$ in a quadratic imaginary field K and $p \geq 11$. By Theorem 7.6, there is a non-trivial point $R' \in E[p]$ such that, if p splits in $K/\mathbb{Q}$, then $[\mathbb{Q}(R') : \mathbb{Q}] = 2(p-1)$. In particular, if $d \geq 2(p-1)$, or equivalently, if $p \leq d/2 + 1$, then $p \in S_{\mathbb{Q}}(d)$. This shows that $F \subset S_{\mathbb{Q}}(d)$. Moreover, if p is inert, then $[\mathbb{Q}(R') : \mathbb{Q}] = p^2 - 1$. For any $7 \leq p \leq \sqrt{d+1}$ (i.e., $p^2 - 1 \leq d$), one can find an elliptic curve $E/\mathbb{Q}$ with CM by K and such that p is unramified in $K/\mathbb{Q}$ (notice that either E with CM by $\mathbb{Q}(\sqrt{-7})$ or E with CM by $\mathbb{Q}(\sqrt{-11})$ must work). Whether p splits or remains inert in K, in both cases we have $[\mathbb{Q}(R') : \mathbb{Q}] \leq p^2 - 1 \leq d$ and, hence, $p \in S_{\mathbb{Q}}(d)$. This shows that $C \subseteq S_{\mathbb{Q}}(d)$. This concludes the proof of (1).

To show (2), let us assume there is a constant $M \geq 11$ as in the statement of the theorem, assume that $d \geq M^2 - 1$ and let $p \in S_{\mathbb{Q}}(d) \setminus A \cup B$. Let $E/\mathbb{Q}$ be an elliptic curve with a non-trivial p-torsion point R defined in an extension of degree $\leq d$. If $p \leq M$, then $p^2 - 1 \leq M^2 - 1 \leq d$ and therefore $p \in C$. If $p > M \geq 11$ and $p \notin A \cup B$, then $\rho_{E,p}$ is either surjective, in which case by Theorem 5.1 we have that $[\mathbb{Q}(R) : \mathbb{Q}] = p^2 - 1 \leq d$ and $p \in C$, or $E/\mathbb{Q}$ has CM by a quadratic imaginary field K and p is unramified in K (if it was ramified, then $\rho_{E,p}$ would be in a Borel). By Theorem 7.6, if p is inert in $K/\mathbb{Q}$ then $p \in C$ and, if p splits, then $p \in F$. This shows that $S_{\mathbb{Q}}(d) \subseteq A \cup B \cup C \cup F$ and concludes the proof of the theorem. □

Next, we shall prove Theorem 1.7.

Proof of Theorem 1.7. Let $d \geq 1$ be fixed. By Theorem 1.4 we know that $A \cup B \cup C \cup F \subseteq S_{\mathbb{Q}}(d) \subseteq A \cup B \cup D$. By Corollary 1.5 we may assume that $d \geq 22$. Let $p \in S_{\mathbb{Q}}(d)$ with $p \notin A \cup B$. In particular, $p > 13$. We shall show that $p \in F'$. Let $E/\mathbb{Q}$ be an elliptic curve with a non-trivial p-torsion point R defined in an extension of degree $\leq d$ and let G be the image of $\rho_{E,p}$. By Serre's classification of maximal subgroups of $\mathrm{GL}(E[p])$, as in Section 3, here are the only possibilities:

(1) If $\rho_{E,p}$ is surjective, i.e., $G = \mathrm{GL}(E[p])$, then $d \geq [\mathbb{Q}(R) : \mathbb{Q}] = p^2 - 1$ by Theorem 5.1, thus $p \in C \subseteq F'$;
(2) If G is an exceptional subgroup, then $p \leq 13$ (by Theorem 8.1). If G is a Borel subgroup, then $p \in B$ as we have seen above (and in Subsection 9.1). Since we have assumed that $p \notin A \cup B$, these cases cannot occur;
(3) Suppose G is contained in $\mathcal{C}_{\mathrm{sp}}^+$, the normalizer of a split Cartan subgroup $\mathcal{C}_{\mathrm{sp}}$. Recall that $p > 13$. By the work of Bilu, Parent and Rebolledo (see Remark 1.8), hypothesis (H') is satisfied and $E/\mathbb{Q}$ must have CM by a quadratic imaginary field K, and p splits in K. By Theorem 7.6, the group G must be the full normalizer of a split Cartan subgroup, i.e.,

$G = \mathcal{C}_{\rm sp}^+$. Lemma 7.5 tell us that $[\mathbb{Q}(R) : \mathbb{Q}] = 2(p-1)$ or $(p-1)^2$ and both possibilities occur. Hence $d \geq 2(p-1)$ and $p \in F'$;

(4) Finally, suppose that G is contained in $\mathcal{C}_{\rm nsp}^+$, the normalizer of a non-split Cartan subgroup $\mathcal{C}_{\rm nsp}$. By Theorem 7.3 we have $[\mathbb{Q}(R) : \mathbb{Q}] \geq 2(p-1)$, so $d \geq 2(p-1)$ and $p \leq d/2+1$. Thus $p \in F'$.

This shows $S_{\mathbb{Q}}(d) \subseteq A \cup B \cup F'$ and concludes the first part of Theorem 1.7. If in addition we assume that (H) holds for all p in the range $13 < p < d/2+1$, then only cases (3) and (4) above need to be modified.

Suppose first that we are in case (3) and G is contained in $\mathcal{C}_{\rm sp}^+$. By Remark 1.8, the prime $p > 13$ satisfies (H') and by Theorem 7.6, we have that $p \in F$. If instead we are in case (4) and G is contained in $\mathcal{C}_{\rm nsp}^+$, then we have seen that $p \leq d/2+1$. By (H), the group G must contain $\mathcal{C}_{\rm nsp}$ and, therefore, $G = \mathcal{C}_{\rm nsp}$ or $\mathcal{C}_{\rm nsp}^+$. By Lemma 7.5, there is some $R' \in E[p]$ with $[\mathbb{Q}(R') : \mathbb{Q}] = p^2-1$, so $d \geq p^2-1$. Thus $p \in C$.

Hence, in all cases, if $p \notin A \cup B$ then $p \in C \cup F$. Thus $S_{\mathbb{Q}}(d) \subseteq A \cup B \cup C \cup F$ and the desired equality holds. □

To finish this section, we show Corollary 1.9 as an application of Theorem 1.7.

Proof of Corollary 1.9. Let $d \leq 42$. By Corollary 1.5, we may assume that $d \geq 22$. In order to prove the corollary, we will use Theorem 1.7.

The fact that $22 \leq d \leq 42$ implies that all the primes below 19 are in $A \cup B \subseteq S_{\mathbb{Q}}(d)$, by Theorem 1.4. Thus, hypothesis (H) is trivially satisfied since it only pertains to primes $p \leq d/2+1 \leq 22$ which do not belong to $A \cup B$, but they all do. Hence, $S_{\mathbb{Q}}(d) = A \cup B \cup C \cup F$ for all $d \leq 42$, as claimed. □

3. On Serre's results

In this section we summarize several results of Serre [43], and we specialize these results to the particular case of elliptic curves defined over $\mathbb{Q}$. Serre concentrates on the semi-stable case; for our purposes, we shall need to be more explicit about the case of additive reduction.

Let E be an elliptic curve defined over $\mathbb{Q}$ and let $p \geq 5$ be a prime. Let K be an extension of $\mathbb{Q}_p$, of the least possible degree such that E/K has good or multiplicative reduction ([48], Ch. VII, Prop. 5.4). Let e be the ramification index of $K/\mathbb{Q}_p$, and let ν be a valuation on K such that $\nu(p) = e$. Let A be the ring of elements of K with valuation ≥ 0.

If E/K has multiplicative reduction, then $[K : \mathbb{Q}_p] \leq 2$ (see [43], §1.12). If E/K has good reduction, then the ramification index e at p in the extension $K/\mathbb{Q}_p$ is $e = 1, 2, 3, 4$ or 6 ([43], §5.6). Let $\mathbb{F}_q$ be the residue field of K, where $q = p^n$. Let us fix an algebraic closure $\overline{K}$ of K and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{K}$. This induces an embedding of Galois groups $\iota : \mathrm{Gal}(\overline{K}/K) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $K_{\rm nr}$ be the largest subextension of $\overline{K}$ that is unramified over K, and let K_t be the largest subextension of $\overline{K}$ that is tamely ramified over K. We write $I_K = \iota(\mathrm{Gal}(\overline{K}/K_{\rm nr}))$ and $I_{K,p} = \iota(\mathrm{Gal}(\overline{K}/K_t))$ for the corresponding inertia subgroups in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, via the embedding ι of absolute Galois groups. Notice that $I_{K,p}$ is the largest pro-p-subgroup of I_K. The quotient $I_K/I_{K,p} = \mathrm{Gal}(K_t/K_{\rm nr})$ will be denoted by $I_{K,t}$.

Let π be a uniformizer for $K_{\rm nr}$. For any d relatively prime to p, we write $K_d = K_{\rm nr}(\pi^{1/d})$ and μ_d for the group of d-th roots of unity. We have an isomorphism $\mathrm{Gal}(K_d/K_{\rm nr}) \cong \mu_d$ given by the map that sends σ to a d-th root of unity ζ_σ, such that $\sigma(\pi^{1/d}) = \zeta_\sigma \pi^{1/d}$. The field K_t is the union of all K_d, with $\gcd(d,p) = 1$, and $I_{K,t} = \mathrm{Gal}(K_t/K_{\mathrm{nr}})$ can be identified with the inverse limit $\varprojlim \mathrm{Gal}(K_d/K_{\mathrm{nr}})$ over all d relatively prime to p. We define a character θ_d of I_K (which factors through $I_{K,t}$) by restricting to K_d, i.e., $\theta_d : I_{K,t} \to \mathrm{Gal}(K_d/K_{\mathrm{nr}}) \cong \mu_d \cong \mathbb{Z}/d\mathbb{Z}$, as defined in [43], §1.3; see also §1.7. Each θ_d is surjective, since it is given by restriction from K_t to K_d. In what follows we will be particularly interested in $\theta_{p-1} : I_{K,t} \to \mathbb{F}_p^\times$ and $\theta_{p^2-1} : I_{K,t} \to \mathbb{F}_{p^2}^\times$.

In the following theorem, we describe the image of I_K via the map $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[p])$, according to the type of reduction of E/K and the ramification index e of $K/\mathbb{Q}_p$. First, we introduce some notation. A *semi-Cartan* subgroup $\mathcal{D}$ of $\mathrm{GL}(2,\mathbb{F}_p)$ is a subgroup of the form

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_p^\times \right\}.$$

The precise definitions of split Cartan, non-split Cartan and Borel subgroups will appear in Definitions 6.1, 7.1 and 9.1, respectively. For general results about these types of groups, see [43], §2.

Theorem 3.1 (Serre, [43])**.** *With notation as above, let $f = \gcd(p-1,e)$, and let $\mathcal{D}^f$ be the f-th power of a semi-Cartan subgroup.*

(1) *If E/K has good ordinary reduction or multiplicative reduction, then there is an $\mathbb{F}_p$-basis $\{P,Q\}$ of $E[p]$ such that $\rho_{E,p}(I_K)$ contains $\mathcal{D}^f$;*
(2) *If E/K has good supersingular reduction, then there is an $\mathbb{F}_p$-basis $\{P,Q\}$ of $E[p]$ such that:*
   (a) *$\rho_{E,p}(I_K)$ is the e-th power of a non-split Cartan subgroup; or*
   (b) *$\rho_{E,p}(I_{K,p})$ is non-trivial, i.e., $\rho_{E,p}(I_{K,p})$ contains a non-trivial element of order p, and the image of I_K is a Borel subgroup.*

Proof. The good ordinary case is treated in Proposition 11 of [43], §1.11. Similarly, the multiplicative case is in Proposition 13 of §1.12. In both cases, the image of $I_{K,t}$ contains a subgroup of the form

$$\left\{ \begin{pmatrix} \theta_{p-1}^e & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Since $\theta_{p-1} : I_{K,t} \to \mathbb{F}_p^\times$ is surjective, the image of θ_{p-1}^e is the subgroup formed by all f-th powers in $\mathbb{F}_p^\times$, where $f = \gcd(p-1,e)$.

The good supersingular case is treated in Proposition 12 of §1.11, but some additional remarks are necessary when $e > 1$ (see the *Remarque* after Prop. 12, and also §1.10).

If E/K has good supersingular reduction (i.e., the formal group $\widehat{E}/K$ associated to E has height 2), then the size of the residue field of K is $q = p^2$. Let $[p](X) = \sum_{i=1}^\infty a_i X^i$ be the multiplication-by-p map in $\widehat{E}$. Then $a_i \in A$, $a_1 = p$, $\nu(a_i) \geq 1$ if $i < q = p^2$ and $\nu(a_q) = 0$. Let N be the part of the Newton polygon of $[p](X)$ that describes the roots of valuation > 0. Let $P_i = (q_i, e_i)$, for $i = 0, \ldots, m$, be the different vertices of the Newton polygon N, such that $1 = q_0 < \cdots < q_m = q$, and $e_i = \nu(a_{q_i})$. In particular $e_0 = \nu(a_1) = \nu(p) = e$ and $e_m = \nu(a_q) = 0$. Since $q = p^2$ and every q_i is a power of p ([43], p. 272), we have that $m = 1$ or 2.

Let us first suppose that the Newton polygon N of $[p](X)$ has only one segment (i.e., $m = 1$), between $P_0 = (1,e)$ and $P_1 = (p^2, 0)$. The slope between P_0 and P_1 is $-\alpha = -e/(p^2-1)$. By the properties of Newton polygons ([1], Ch. 2, §5), the series $[p](X)$ has $p^2 - 1$ roots with valuation α, i.e., every non-zero element of $E[p]$ has valuation α. Thus, $E[p]$ can be given a structure of a 1-dimensional $\mathbb{F}_{p^2}$-vector space. Moreover, Proposition 10 of [43] tells us that the action of I_t on

$E[p]$ is given by the e-th power of a fundamental character of level 2, $\theta_{p^2-1}^e : I_{K,t} \to (\mathbb{F}_{p^2}^\times)^e$, and $I_{K,p}$ acts trivially. Since $\theta_{p^2-1} : I_{K,t} \to \mathbb{F}_{p^2}^\times$ is surjective, the image of I_K in $\mathrm{GL}(E[p])$ is the e-th power of a non-split Cartan subgroup (see Remark 7.2 below).

Finally, suppose instead that the Newton polygon N has two segments (i.e., $m = 2$), with vertices $P_0 = (1, e)$, $P_1 = (p, e')$ and $P_2 = (p^2, 0)$. The slopes between points are $-\alpha_1 = -(e - e')/(p - 1)$ and $-\alpha_2 = -e'/(p^2 - p)$. Let $V^0 = \{0\}$, and V^i be the space formed by those elements $x \in E[p]$ with valuation $\geq \alpha_i$. Then (as in [43], §1.10), there is a filtration $\{0\} = V^0 \subsetneq V^1 \subsetneq V^2 = E[p]$, with $\mathrm{card}(V^1) = p$ and $\mathrm{card}(V^2) = p^2$, and $\mathrm{Gal}(\overline{K}/K)$ respects this filtration. It follows that the action of $\mathrm{Gal}(\overline{K}/K)$ on $E[p]$ is upper triangular when we fix a first basis vector in $V^1 \setminus V^0$ and a second basis vector in $V^2 \setminus V^1$. By Proposition 10 of [43], when we restrict to the action of I_K on $E[p]$, the character that appears in the upper left corner, i.e., the action on V^1, is given by $\theta_{p-1}^{e-e'}$. By the properties of Newton polygons, there are $p^2 - p = p(p-1)$ elements in $E[p]$ with valuation $\alpha_2 = e'/(p^2 - p)$. Hence, the ramification index in $K(E[p])/K$ is divisible by p. It follows that the image of $I_{K,p}$ under $\rho_{E,p}$ is non-trivial. Thus, $\rho_{E,p}(I_K)$ is contained in a Borel subgroup, and it has an element of order p. □

As a result of the previous theorem, and using the classification of maximal subgroups of $\mathrm{GL}(2, \mathbb{F}_p)$ that Serre describes in [43], §2 (in particular, see §2.6, and Prop. 17 in §2.7), one deduces the following theorem.

Theorem 3.2 (Serre, [43])**.** *Let $e = 1, 2, 3, 4$ or 6 be the ramification index of $K/\mathbb{Q}_p$, as before. 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 the normalizer of a split Cartan subgroup of $\mathrm{GL}(E[p])$ and contains the f-th power of a semi-Cartan subgroup, i.e., $\mathcal{D}^f \leq G$, where $f = \gcd(e, p-1)$; or*
2. *G is contained in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}(E[p])$ and contains the e-th power of a non-split Cartan subgroup; or*
3. *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; or*
4. *G is contained in a Borel subgroup of $\mathrm{GL}(E[p])$ and the order of G is divisible by $p(p-1)$.*

The main theorem of [43] is the following.

Theorem 3.3 (Serre)**.** *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication (CM). Then $\rho_{E,p}$ is surjective for all but finitely many primes p.*

4. Preliminaries

In this section we establish some notation and preliminary results that we shall use repeatedly in the rest of the paper. Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime. Fix an $\mathbb{F}_p$-basis of $E[p]$ and let $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}(2, \mathbb{F}_p)$ be the Galois representation induced by the action of Galois on $E[p]$. The image of $\rho_{E,p}$ will be denoted by G. Since the kernel of $\rho_{E,p}$ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[p]))$, we deduce that $G \cong \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$.

Lemma 4.1. *Let $G \leq \mathrm{GL}(2, \mathbb{F}_p)$ be as above. Then the determinant map $G \to \mathbb{F}_p^\times$ is surjective.*

Proof. It is well-known that the determinant of $\rho_{E,p}$ is the cyclotomic character $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_p^\times$, thus $\det(\rho_{E,p}) : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_p^\times$ is surjective. Since $\rho_{E,p}$ factors through $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$, the map $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \hookrightarrow \mathrm{GL}(2, \mathbb{F}_p) \to \mathbb{F}_p^\times$ is surjective as well. □

Let $R = (x(R), y(R)) \in E[p]$ be a torsion point. The (minimal) field of definition of R, i.e., the number field $\mathbb{Q}(x(R), y(R))$, will be denoted by $\mathbb{Q}(R)$. Since $\mathbb{Q}(R) \subseteq \mathbb{Q}(E[p])$, it follows that there is a subgroup $H \le G$ such that $\mathbb{Q}(R)$ is the fixed field of $\mathbb{Q}(E[p])$ by H, i.e., $\mathbb{Q}(R) = \mathbb{Q}(E[p])^H$. Moreover, by Galois theory, we know that $[\mathbb{Q}(R) : \mathbb{Q}] = |G/H|$. In order to give a lower bound on $[\mathbb{Q}(R) : \mathbb{Q}]$ it suffices to bound the quotient $|G|/|H|$.

Also, we can deduce that $H \le G \le \mathrm{GL}(2, \mathbb{F}_p)$ fixes each element of a 1-dimensional $\mathbb{F}_p$-subspace V of $E[p] \cong \mathbb{F}_p^2$, namely $V = \langle R \rangle$. Therefore, each matrix in H has an eigenvalue $\lambda = 1$, and V is contained in the corresponding λ-eigenspace.

5. Full image

Theorem 5.1. *Let p be a prime and let $E/\mathbb{Q}$ be an elliptic curve. Suppose that $\rho_{E,p}$ is surjective, i.e., its image is $\mathrm{GL}(E[p])$. Then, for every non-trivial torsion point $R \in E[p]$, the degree of the field of definition of R satisfies $[\mathbb{Q}(R) : \mathbb{Q}] = p^2 - 1$.*

Proof. Let E, p and R be as in the statement of the theorem. Let $Q \in E[p]$ such that $\{R, Q\}$ is an $\mathbb{F}_p$-basis of $E[p]$. With respect to this basis, the field of definition $\mathbb{Q}(R)$ is the fixed field of the subgroup

$$H = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{F}_p,\ b \in \mathbb{F}_p^\times \right\} \le \mathrm{GL}(2, \mathbb{F}_p).$$

Since $|\mathrm{GL}(2, \mathbb{F}_p)| = (p^2 - 1)(p^2 - p)$ and $|H| = p^2 - p$, we conclude that

$$[\mathbb{Q}(R) : \mathbb{Q}] = |G/H| = (p^2 - 1)(p^2 - p)/(p^2 - p) = p^2 - 1,$$

as claimed. □

As a consequence of Theorems 3.3 and 5.1, we obtain the following corollary.

Corollary 5.2. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then, for all but finitely many primes p, the field of definition of any non-trivial torsion point $R \in E[p]$ has degree $p^2 - 1$ over $\mathbb{Q}$.*

6. Normalizer of a split Cartan

Definition 6.1. *Let $p \ge 3$ be a prime. The split Cartan subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$ is the subgroup*

$$\mathcal{C}_{sp} = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{F}_p^\times \right\}.$$

In order to abbreviate matrix notation, we define diagonal and anti-diagonal matrices:

$$D(a, b) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \quad A(c, d) = \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix},$$

for any $a, b, c, d \in \mathbb{F}_p^\times$. With this notation, $\mathcal{C}_{sp} = \{D(a, b) : a, b \in \mathbb{F}_p^\times\}$.

Theorem 6.2. *Let p be a prime and let $E/\mathbb{Q}$ be an elliptic curve. Suppose that there is an $\mathbb{F}_p$-basis $\{P, Q\}$ of $E[p]$ such that the image of $\rho_{E,p}$ is a subgroup of $\mathcal{C}_{sp}$. Then $p \le 5$.*

Proof. Let p, $E/\mathbb{Q}$ and $\{P, Q\}$ be as in the statement of the theorem. Then, $\langle P\rangle$ and $\langle Q\rangle$ are distinct subgroups of E, cyclic of order p, which are stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. By Prop. 4.12 of [48], Ch. III, there are *unique* elliptic curves $E' = E/\langle P\rangle$ and $E'' = E/\langle Q\rangle$, and isogenies $\phi' : E \to E'$ and $\phi'' : E \to E''$ with kernel $\langle P\rangle$ and $\langle Q\rangle$, respectively. Moreover, E and E' are elliptic curves defined over $\mathbb{Q}$ (see [48], Ch. III, Remark 4.13.2). Since $|\langle P\rangle| = |\langle Q\rangle| = p$, the curve E is p-isogenous (over $\mathbb{Q}$) to E' and E'', and each one of these curves is in a different $\mathbb{Q}$-isomorphism class. Hence, there are at least 3 non-$\mathbb{Q}$-isomorphic elliptic curves (over $\mathbb{Q}$) in the p-isogeny class of E. Let $C_p(E)$ be the number of $\mathbb{Q}$-isomorphism classes of elliptic curves that are isogenous to E via an isogeny whose degree is a non-negative power of p. By Theorem 2 of [26], the number $C_p(E)$ is bounded as in Table 1.

Table 1: Bounds for $C_p(E)$

p	2	3	5	7	11	13	17	19	37	43	67	163	else
$C_p(E) \leq$	8	4	3	2	2	2	2	2	2	2	2	2	1

Note: $C = \prod_p C_p \leq 8$, and $C = 8$ iff $C_2 = 8$, or $C_2 = 4$ and $C_3 = 2$.

References: [26]; see also [4], [35], [45].

Hence the prime p must be less than or equal to 5. ☐

Example 6.3. Let E be the elliptic curve given by $y^2 + y = x^3 - x^2 - 10x - 20$. Let P and Q be points defined by

$$P = (5, 5), \quad \text{and} \quad Q = (4\zeta_5^3 + 2\zeta_5^2 + 3\zeta_5 + 2, 3\zeta_5^3 - 4\zeta_5^2 + 5\zeta_5),$$

where ζ_5 is a primitive 5th root of unity. Then, the image of $\rho_{E,5}$ with respect to the basis $\{P, Q\}$ is the subgroup

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} : b \in \mathbb{F}_5^\times \right\} \leq \mathcal{C}_{\mathrm{sp}}.$$

Indeed, $\mathrm{Gal}(\mathbb{Q}(E[5])/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong \mathbb{F}_5^\times$. The elliptic curve E is 5-isogenous to $E' = E/\langle P\rangle : y^2 + y = x^3 - x^2 - 7820x - 263580$ and $E'' = E/\langle Q\rangle : y^2 + y = x^3 - x^2$. The $\mathbb{Q}$-isogeny class of E consists precisely of E, E' and E''.

Next we treat the case when the Galois group $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ embeds into the normalizer of the split Cartan subgroup. It is easy to show that the normalizer of the split Cartan subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$ is the subgroup

$$\mathcal{C}_{\mathrm{sp}}^+ = \{D(a, b),\ A(c, d) : a, b, c, d \in \mathbb{F}_p^\times\}.$$

Remark 6.4. Serre's uniformity problem (see our remarks before Theorem 1.4) has been proved by Bilu and Parent [2] in the case of the normalizer of a split Cartan: there is a constant N, that does not depend on the elliptic curve $E/\mathbb{Q}$, such that if $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ embeds into the normalizer of the split Cartan subgroup and E is not CM, then $p \leq N$.

In the rest of this section, we shall prove the following result.

Theorem 6.5. *Let $E/\mathbb{Q}$ be an elliptic curve and let $p \geq 11$ be a prime. Let $R \in E[p]$ be a point of exact order p. Suppose that there is an $\mathbb{F}_p$-basis of $E[p]$ such that the image of $\rho_{E,p}$ lies in the normalizer of the split Cartan subgroup, but it is not contained in the split Cartan. Then $[\mathbb{Q}(R) : \mathbb{Q}] \geq p - 1$.*

Lemma 6.6. *Let H be a non-trivial subgroup of $\mathcal{C}_{sp}^+$ that fixes each element in a 1-dimensional $\mathbb{F}_p$-subspace V of $\mathbb{F}_p^2$. Then:*

(1) $H \leq \left\{D(1,b) : b \in \mathbb{F}_p^\times\right\}$ *and* $V = \langle(1,0)\rangle$*; or*
(2) $H \leq \left\{D(a,1) : a \in \mathbb{F}_p^\times\right\}$ *and* $V = \langle(0,1)\rangle$*; or*
(3) $H = \left\{D(1,1),\ A(c,c^{-1})\right\}$ *for some* $c \in \mathbb{F}_p^\times$ *and* $V = \langle(c,1)\rangle$.

Proof. Clearly, the eigenvectors of a diagonal matrix $D(a,b)$ are $(1,0)$ and $(0,1)$, with eigenvalues a and b, respectively. Also, an anti-diagonal matrix $A(c,d)$ has eigenvalues $\pm\lambda$ such that $\lambda^2 = cd$. Thus, if $\lambda = 1$, then $d = c^{-1}$. Finally, notice that $A(c,c^{-1})^2 = D(1,1)$. ☐

Proof of Theorem 6.5. Let $G = \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$. By assumption, there exists an $\mathbb{F}_p$-basis $\{P,Q\}$ of $E[p]$ such that G is isomorphic to a subgroup of $\mathcal{C}_{\mathrm{sp}}^+$. By abuse of notation, we will say $G \leq \mathcal{C}_{\mathrm{sp}}^+$. Our assumptions also include that $G \not\leq \mathcal{C}_{\mathrm{sp}}$. By Lemma 4.1, $\det : G \to \mathbb{F}_p^\times$ is surjective. In particular, the order of G is divisible by $p-1$. For the remainder of the proof, we fix a matrix $M_g \in G$ such that $\det(M_g) = g$, where $g \in \mathbb{F}_p^\times$ is a primitive root modulo p (i.e., the order of g is exactly $p-1$). By Theorem 3.2, G contains $\mathcal{D}^f$, the f-th power of the semi-Cartan subgroup of $\mathrm{GL}(2,\mathbb{F}_p)$, where $f = \gcd(p-1,e)$, and $e = 1,2,3,4$ or 6. In our notation, $\mathcal{D}^f = \{D(a,1) : a \in J_f\}$, where $J_f = (\mathbb{F}_p^\times)^f \leq \mathbb{F}_p^\times$ is the subgroup formed by all f-th powers. Thus, $|\mathcal{D}^f| = |J_f| = (p-1)/f$. Since $f \leq e \leq 6$ and $p \geq 11$, the group J_f has order ≥ 2. Let α be a generator of J_f (in particular $\alpha \not\equiv 1 \bmod p$), and let $D(\alpha,1)$ be the corresponding generator matrix of $\mathcal{D}^f$.

Since $G \leq \mathcal{C}_{\mathrm{sp}}^+$ but $G \not\leq \mathcal{C}_{\mathrm{sp}}$, there is a matrix $A = A(c,d) \in G$, for some $c,d \in \mathbb{F}_p^\times$, and since G is a group, $A^{-1} = A(d^{-1},c^{-1}) \in G$ as well. We also remark on the following equation:

$$\begin{pmatrix} 0 & d^{-1} \\ c^{-1} & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix}. \tag{1}$$

In particular, this shows that if $D(a,b) \in G$ then $D(b,a)$ is also in G and, therefore, $D(a,b)D(b,a) = D(ab,ab) \in G$ as well. We will use this remark several times below.

Let H be as in Section 4. Hence, we can use Lemma 6.6. Let us assume first that $H = \left\{D(1,1),\ A(c,c^{-1})\right\}$ and so, H is a subgroup of order 2. Thus, one immediately obtains that $|G/H| \geq (p-1)/2$. In order to improve this bound, we need to consider two cases according to the shape of M_g. If $M_g = D(a,b)$ with $ab = g$, then $D(ab,ab) = D(g,g) \in G$ by Eq. (1) and the remark that followed it. Hence, $D(g^k,g^k)A(c,c^{-1}) = A(cg^k,c^{-1}g^k) \in G$ and the set

$$\{D(g^k,g^k) : k = 1,\ldots,p-1\} \cup \{A(cg^k,c^{-1}g^k) : k = 1,\ldots,p-1\}$$

is contained in G. Thus, $|G| \geq 2(p-1)$ and $|G/H| \geq p-1$. The other possibility is that $M_g = A(m,n)$ with $-mn = g$. In this case, $M_g^2 = D(mn,mn) = D(-g,-g)$. The element $h = -g \in \mathbb{F}_p^\times$ has order $p-1$ or $(p-1)/2$ according to whether $p \equiv 1$ or $3 \bmod 4$, respectively.

- Suppose $p \equiv 1 \bmod 4$. Since $h = -g$ has order $p-1$, we have that $D(a,a) \in G$, for all $a \in \mathbb{F}_p^\times$ and, therefore, $\{D(a,a), A(ca,c^{-1}a) : a \in \mathbb{F}_p^\times\} \subseteq G$. Thus, $|G| \geq 2(p-1)$ and $|G/H| \geq p-1$.
- Suppose $p \equiv 3 \bmod 4$. We need to consider two additional cases, according to whether α, a generator of $J_f = (\mathbb{F}_p^\times)^f$, is a quadratic residue.
  - If $\alpha \in J_f$ is a quadratic non-residue, then αh is a quadratic non-residue as well, because $h = -g$ is a square. Since the order of h is $(p-1)/2$, the set $\{h^k, \alpha h^k : k = 1,\ldots,(p-1)/2\} = \mathbb{F}_p^\times$. Since $D(\alpha,1) \in \mathcal{D}^f \leq G$, we also have $D(\alpha,\alpha) \in G$ by Eq. (1), and

$D(\alpha,\alpha)D(h^k,h^k) = D(\alpha h^k, \alpha h^k) \in G$ as well. Hence,

$$\{D(h^k,h^k), D(\alpha h^k,\alpha h^k) : k = 1,\ldots,(p-1)/2\} = \{D(a,a) : a \in \mathbb{F}_p^\times\}$$

is contained in G. Thus, $\{D(a,a), A(ca,c^{-1}a) : a \in \mathbb{F}_p^\times\} \subseteq G$ and we can conclude that $|G/H| \geq p-1$.

– If $\alpha \in J_f$ is a quadratic residue, recall that we have shown above that $|J_f| \geq 2$. Since α is a generator of J_f, then the order of α is at least 2. Since $p \equiv 3 \bmod 4$, it follows that $-1 \bmod p$ is not a quadratic residue, so $\alpha \not\equiv \pm 1 \bmod p$. Now, each of the matrices in the following set K belong to G:

$$K = \{D(t\alpha,t), D(t,\alpha t), A(ct\alpha, c^{-1}t), A(ct, c^{-1}t\alpha) : t \in (\mathbb{F}_p^\times)^2\}.$$

Notice that, if $D(t\alpha,t) \equiv D(s,\alpha s)$ where t,s are squares modulo p, then $\alpha \equiv s/t \equiv t/s \bmod p$ and this would imply that $\alpha \equiv \pm 1 \bmod p$, which we have shown is impossible. Similarly, the congruence $A(ct\alpha,c^{-1}t) \equiv A(cs,c^{-1}s\alpha)$ is impossible for squares t,s. Thus, K has size $4\cdot(p-1)/2 = 2(p-1)$ and $K \subseteq G$. Hence $|G/H| \geq p-1$, as desired.

Having taking care of the case when $|H| = 2$, and according to Lemma 6.6, to finish the proof of the theorem it suffices to consider the case when $H = \{D(1,b) : b \in J\}$, where J is an arbitrary subgroup of $\mathbb{F}_p^\times$ (the same proof will apply to case (2) of Lemma 6.6, by symmetry).

Once again, we divide the proof into two cases: when $M_g = D(a,b)$ for some $a,b \in \mathbb{F}_p^\times$, or $M_g = A(m,n)$, for some $m,n \in \mathbb{F}_p^\times$:

If M_g is of the form $D(a,b) \in G$, then $ab = g$ and $D(ab,ab) = D(g,g) \in G$ by Eq. (1). By taking powers of $D(g,g)$ we deduce that $D(a,a) \in G$ for all $a \in \mathbb{F}_p^\times$, and the fact that $H \leq G$ implies that the product $D(a,a)D(1,b) \in G$ for all $a \in \mathbb{F}_p^\times$ and all $b \in J$. This shows that $|G| \geq (p-1)|J|$ and

$$|G/H| = \frac{|G|}{|H|} = \frac{|G|}{|J|} \geq \frac{(p-1)|J|}{|J|} = p-1.$$

It remains to consider the case when $M_g = A(m,n)$, with $-mn = g$. Then $M_g^2 = A(m,n)^2 = D(mn,mn) = D(-g,-g)$. If $p \equiv 1 \bmod 4$, the element $-g$ is also a primitive root and, proceeding as in the case when M_g was diagonal, we reach $|G/H| \geq p-1$. If $p \equiv 3 \bmod 4$, then G contains

$$L = \{D(tj,t), A(tmj,tn) : t \in (\mathbb{F}_p^\times)^2,\ j \in J\}.$$

Since $|G| \geq |L| = 2\cdot|J|\cdot(p-1)/2 = (p-1)|J|$, we conclude that $|G/H| \geq p-1$, as desired. This finishes the proof of the theorem. □

7. Normalizer of a non-split Cartan

Definition 7.1. *Let $p \geq 3$ be a prime. The non-split Cartan subgroup of* $\mathrm{GL}(2,\mathbb{F}_p)$ *is the subgroup*

$$\mathcal{C}_{nsp} = \left\{ \begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix} : a,b \in \mathbb{F}_p,\ (a,b) \not\equiv (0,0) \bmod p \right\},$$

where ε is a fixed quadratic non-residue of $\mathbb{F}_p$. In order to abbreviate matrix notation, we define two types of matrices:

$$M(a,b) = \begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix}, \quad N(c,d) = \begin{pmatrix} c & \varepsilon d \\ -d & -c \end{pmatrix},$$

for any $a,b,c,d \in \mathbb{F}_p$, such that $(a,b),(c,d) \not\equiv (0,0) \bmod p$. With this notation, $\mathcal{C}_{nsp} = \{M(a,b) : a,b \in \mathbb{F}_p,\ (a,b) \not\equiv (0,0) \bmod p\}$.

Remark 7.2. The group $\mathcal{C}_{\rm nsp}$ is isomorphic to $\mathbb{F}_{p^2}^\times$. Indeed, let ε be a fixed quadratic non-residue of $\mathbb{F}_p^\times$. Then $\mathbb{F}_{p^2} \cong \mathbb{F}_p[X]/(X^2-\varepsilon)$. We define a map $\psi : (\mathbb{F}_p[X]/(X^2-\varepsilon))^\times \to \mathrm{GL}(2,p)$ so that $\psi(a+bX)$ is the matrix of the linear multiplication-by-$(a+bX)$ map in $\mathbb{F}_p[X]/(X^2-\varepsilon)$, with respect to the basis $\{1, X\}$. The map ψ is an isomorphism between $\mathbb{F}_{p^2}^\times$ and $\mathcal{C}_{\rm nsp}$. Notice that $\mathcal{C}_{\rm nsp}$ is abelian, cyclic of order p^2-1.

It is easy to show that the normalizer of the non-split Cartan subgroup of $\mathrm{GL}(2,\mathbb{F}_p)$ is the subgroup

$$\mathcal{C}_{\rm nsp}^+ = \{M(a,b),\ N(c,d) : a,b,c,d \in \mathbb{F}_p,\ (a,b),(c,d) \not\equiv (0,0) \bmod p\}.$$

In this section we prove the following result.

Theorem 7.3. *Let $E/\mathbb{Q}$ be an elliptic curve and let $p \geq 3$ be a prime. Let $R \in E[p]$ be a point of exact order p. Suppose that there is an $\mathbb{F}_p$-basis of $E[p]$ such that the image of $\rho_{E,p}$ lies in the normalizer of the non-split Cartan subgroup. Then $[\mathbb{Q}(R):\mathbb{Q}] \geq (p^2-1)/e$, where $e \leq 6$ is the ramification index of the extension $K/\mathbb{Q}_p$ defined in Section 3. In particular, $[\mathbb{Q}(R):\mathbb{Q}] \geq 2(p-1)$ for all $p \geq 11$.*

Lemma 7.4. *Let H be a non-trivial subgroup of $\mathcal{C}_{nsp}^+$ that fixes each element in a 1-dimensional $\mathbb{F}_p$-subspace V of $\mathbb{F}_p^2$. Then:*

$$H = \{D(1,1),\ N(c,d)\}$$

for some $c, d \in \mathbb{F}_p$ with $c^2 - \varepsilon d^2 = 1$.

Proof. A simple calculation reveals that the eigenvalues of a matrix of the form $M(a,b)$, with $a,b \in \mathbb{F}_p$ and $(a,b) \not\equiv (0,0) \bmod p$, are precisely $a \pm b\sqrt{\varepsilon} \in \overline{\mathbb{F}_p}$. Since ε is a quadratic non-residue modulo p, we conclude that the only matrix $M(a,b)$ that fixes a non-trivial vector in $\mathbb{F}_p^2$ is the identity $M(1,0) = D(1,1)$.

Similarly, the matrix $N(c,d)$ has eigenvalues $\pm\lambda$ with $\lambda^2 = c^2 - \varepsilon d^2$. If $c^2 - \varepsilon d^2 = 1$, then $\det(N(c,d)) = -1$ and $N(c,d)^2 = D(1,1)$ is the identity matrix. The eigenvectors of $N(c,d)$ with eigenvalue 1 are the multiples of $(-\varepsilon d, c-1)$ if $c \not\equiv 1$, or the multiples of $(1,0)$ if $c \equiv 1$, $d \equiv 0 \bmod p$. Thus $N(c,d)$ and $N(c',d')$ have the same eigenvector (with eigenvalue 1) if and only if the vector $(-\varepsilon d, c-1)$ is in the kernel of the matrix $(N(c,d) - N(c',d')) = N(c-c', d-d')$. In particular, its determinant, $-(c-c')^2 + \varepsilon(d-d')^2$, vanishes. Since ε is a quadratic non-residue, the determinant of $N(c-c', d-d')$ vanishes if and only if $c \equiv c'$ and $d \equiv d' \bmod p$, i.e., if $N(c,d) \equiv N(c',d') \bmod p$. ☐

Proof of Theorem 7.3. Let $G = \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$. By assumption, there exists an $\mathbb{F}_p$-basis $\{P,Q\}$ of $E[p]$ such that G is isomorphic to a subgroup of $\mathcal{C}_{\rm nsp}^+$. By abuse of notation, we will say $G \leq \mathcal{C}_{\rm nsp}^+$.

Let H be as in Section 4. Hence, we can use Lemma 7.4. Thus, H is trivial or H has two elements, i.e., $H = \{D(1,1),\ N(c,d)\}$, with with $c^2 - \varepsilon d^2 = 1$.

By Theorem 3.2, G contains the e-th power of the non-split Cartan subgroup, $\mathcal{C}_{\rm nsp}^e$. Hence,

$$|G| \geq (p^2-1)/e \geq (p^2-1)/6 = (p+1)(p-1)/6 \geq 12(p-1)/6 = 2(p-1)$$

for all $p \geq 11$. If H is trivial, then $|G/H| \geq (p^2-1)/e \geq 2(p-1)$, as claimed. Let us suppose now that H is of order 2, and let $M \in G$ be an element of exact order $(p^2-1)/e$, that generates the e-th power of the non-split Cartan subgroup $\mathcal{C}_{\rm nsp}^e$. Then, the set

$$\{M^k, N(c,d)M^k : k = 1, \ldots, (p^2-1)/e\}$$

has size $2(p^2-1)/e$. Hence,

$$|G/H| \geq |G|/2 \geq (2(p^2-1)/e)/2 \geq (p^2-1)/e \geq 2(p-1)$$

for all $p \geq 11$. This finishes the proof of the theorem. $\square$

Putting together our results in this section and those of Section 6, we can prove the following results about elliptic curves over $\mathbb{Q}$ whose image of $\rho_{E,p}$ contains a Cartan subgroup.

Lemma 7.5. *Let $E/\mathbb{Q}$ be an elliptic curve, p a prime, and let G be the image of $\rho_{E,p}$.*

(1) *Suppose $G \cong \mathcal{C}_{sp}^+$. If $R \in E[p]$ is non-trivial, then $[\mathbb{Q}(R):\mathbb{Q}] = 2(p-1)$ or $(p-1)^2$ and both possibilities occur.*
(2) *Suppose $G \cong \mathcal{C}_{nsp}$ or $\mathcal{C}_{nsp}^+$. if $R \in E[p]$ is non-trivial, then $[\mathbb{Q}(R):\mathbb{Q}] = p^2-1$ or $2(p^2-1)$. Moreover, there is some $R' \in E[p]$ with $[\mathbb{Q}(R'):\mathbb{Q}] = p^2-1$.*

Proof. Suppose first that $G \cong \mathcal{C}_{\mathrm{sp}}^+$. By Lemma 6.6, if $R \in E[p]$ is non-trivial, and R belongs to $\langle P\rangle$ or $\langle Q\rangle$, then $[\mathbb{Q}(R):\mathbb{Q}] = 2(p-1)$. Otherwise, $[\mathbb{Q}(R):\mathbb{Q}] = (p-1)^2$.

If $G = \mathcal{C}_{\mathrm{nsp}}$, Lemma 7.4 tells us that $\mathbb{Q}(R) = \mathbb{Q}(E[p])$ and $[\mathbb{Q}(R):\mathbb{Q}] = p^2-1$. If $G = \mathcal{C}_{\mathrm{nsp}}^+$, then $|G| = 2(p^2-1)$ and $\mathbb{Q}(R) = \mathbb{Q}(E[p])^H$ with $|H| = 1$ or 2. Thus $[\mathbb{Q}(R):\mathbb{Q}] = p^2-1$ or $2(p^2-1)$. Moreover, Lemma 7.4 shows that there are points $R' \in E[p]$ for which $|H| = 2$. $\square$

Theorem 7.6. *Let $E/\mathbb{Q}$ be an elliptic curve with CM by an order $\mathcal{O}$ of a quadratic imaginary field K. Let $p \geq 7$ be an unramified prime in $K/\mathbb{Q}$. Let G be the image of the representation $\rho_{E,p}$.*

(1) *If p is split in K, then G is the normalizer of a full split Cartan subgroup $\mathcal{C}_{sp}^+$.*
(2) *If p is inert in K, then G is either a non-split Cartan subgroup $\mathcal{C}_{nsp}$ or its normalizer $\mathcal{C}_{nsp}^+$.*

In particular, the field of definition of any $R \in E[p]$ satisfy the conclusions of Lemma 7.5.

Proof. Notice that the discriminant of $\mathcal{O}$ and the discriminant of K only differ by a power of 2 or a power of 3 (see the Table in Appendix A.3 of [49]). Since $p \geq 7$ and p is unramified in $K/\mathbb{Q}$, then $\gcd(p, \operatorname{disc}(\mathcal{O})) = \gcd(p, \operatorname{disc}(E/\mathbb{Q})) = 1$, and p is a prime of good reduction for $E/\mathbb{Q}$ (thus, $e = 1$).

By the theory of complex multiplication, G is contained in the normalizer of a Cartan subgroup. If $p \geq 7$ splits in K, then G is contained in the normalizer of a non-split Cartan $\mathcal{C}_{\mathrm{sp}}^+$ with respect to some basis $\{P, Q\}$. By Theorems 6.2 and 3.2, respectively, the group G cannot be contained in $\mathcal{C}_{\mathrm{sp}}$, and G contains a semi-Cartan group $\mathcal{D}$, of order $p-1$. By Eq. (1), the group G must also contain the lower semi-Cartan $\{D(1,b) : b \in \mathbb{F}_p^\times\}$, and, therefore, $\mathcal{C}_{\mathrm{sp}} \lneq G \leq \mathcal{C}_{\mathrm{sp}}^+$. Thus, $G = \mathcal{C}_{\mathrm{sp}}^+$ and $|G| = 2(p-1)^2$.

If p is inert in K, then G is contained in the normalizer of a non-split Cartan with respect to some basis $\{P, Q\}$, and by Theorem 3.2, the group G contains a non-split Cartan subgroup $\mathcal{C}_{\mathrm{nsp}}$ of order p^2-1. Hence $G \cong \mathcal{C}_{\mathrm{nsp}}$ or $\mathcal{C}_{\mathrm{nsp}}^+$. $\square$

8. Exceptional Subgroups

Let S_n be the symmetric group on n letters and A_n the alternating group.

Theorem 8.1. *Let $E/\mathbb{Q}$ be an elliptic curve, and $p \geq 3$ a prime number, such that the image of $\rho_{E,p}$ in $\mathrm{PGL}(E[p])$ is isomorphic to $\overline{G} = A_4$, S_4, or A_5. Then $p \leq 13$ and $\overline{G} = S_4$.*

Proof. Serre has shown that this situation does not occur for $p \geq 17$ ([46], *Lemme* 18). Moreover, the cases of A_4 and A_5 cannot occur for an elliptic curve over $\mathbb{Q}$. Indeed, for $H = A_4, A_5$ or S_4, let

$X_H(p)$ be the modular curve that parametrizes all elliptic curves E such that the projective image of $G = \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ in $\mathrm{PGL}(E[p])$ is H. For details on the construction of X_H and its properties, see [35], §2. The modular curves $X_{A_4}(p)$ and $X_{A_5}(p)$ are defined over the unique quadratic subfield of $\mathbb{Q}(\mu_p)$ (see [35], §2, MAZ-10, p. 116) and, therefore, cannot have $\mathbb{Q}$-rational points ([35], §2, MAZ-15, p.121, Remark 4(d)). $\square$

Remark 8.2. The curve $X_{S_4}(p)$ is defined over $\mathbb{Q}$ when $p \equiv \pm 3 \bmod 8$, and is defined over the quadratic subfield of $\mathbb{Q}(\mu_p)$ otherwise. Serre has exhibited $\mathbb{Q}$-rational points on $X_{S_4}(p)$ for $p = 11$ and 13 using elliptic curves with complex multiplication by $\mathbb{Q}(\sqrt{-3})$.

By Theorem 8.1, and since we will exclude $p = 2, 3, 5, 7$ and 13 for our purposes in our main result, Theorem 2.1, we only need to deal with the case $p = 11$.

Theorem 8.3. *Let $E/\mathbb{Q}$ be an elliptic curve and let $p = 11$. Let $R \in E[p]$ be a point of exact order p. Suppose that the image of $\rho_{E,p}$ in $\mathrm{PGL}(2, \mathbb{F}_p)$ is isomorphic to S_4. Then $[\mathbb{Q}(R) : \mathbb{Q}] \geq 60 > 10 = p-1$.*

Proof. Let $p = 11$ and let $G = \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$. By assumption, $\overline{G}$, the projective image of G in $\mathrm{PGL}(2, \mathbb{F}_p)$, is isomorphic to S_4. Let ZG be the subgroup of G formed by those matrices in G that are scalar matrices, i.e., $ZG = G \cap \{D(\lambda, \lambda) : \lambda \in \mathbb{F}_p^\times\}$. Then $\overline{G} = G/ZG \cong S_4$. In particular, $|G|$ is divisible by 24. Also, by Lemma 4.1, $|G|$ is divisible by 10. Hence, $|G|$ is divisible by $\mathrm{lcm}(24, 10) = 120$. Since 5 is not a divisor of $|S_4|$, we conclude that every element of order 5 in G belongs to ZG, i.e., it is a scalar matrix in G.

Let H be as in Section 4. Let $Q \in E[p]$ be another point such that $\{R, Q\}$ is an $\mathbb{F}_p$-basis of $E[p]$. With respect to this basis, H is a subgroup of a Borel

$$B = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{F}_p,\ b \in \mathbb{F}_p^\times \right\}.$$

Since $|G|$ is not divisible by 11, then $|H|$ is a divisor of $|\mathbb{F}_p^\times| = 10$. Moreover, $B \cap ZG = \{D(1, 1)\}$, so H cannot contain elements of order 5. Hence $|H| = 1$ or 2. Therefore, $[\mathbb{Q}(R) : \mathbb{Q}] = |G/H| \geq 120/2 = 60$, as claimed. $\square$

9. Borel Subgroups

Definition 9.1. *Let $p \geq 2$ be a prime. Let J be a subgroup of $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ such that the map $J \to \mathbb{F}_p^\times$, defined by $(u, v) \mapsto uv$, is surjective. A Borel subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$ is a subgroup of the form:*

$$B = B(J) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : (a, c) \in J,\ b \in \mathbb{F}_p \right\}.$$

In order to abbreviate matrix notation, we define a type of matrix:

$$B(a, b, c) = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

for any $a, c \in \mathbb{F}_p^\times$ and any $b \in \mathbb{F}_p$.

Lemma 9.2. *Let H be a non-trivial subgroup of a Borel subgroup $B(J)$ that fixes each element in a 1-dimensional $\mathbb{F}_p$-subspace V of $\mathbb{F}_p^2$. Then:*

(1) *$H \leq \{B(1, b, c) : b \in \mathbb{F}_p,\ c \in \mathbb{F}_p^\times\}$ and $V = \langle (1, 0) \rangle$; or*

(2) *There is some* $\lambda \in \mathbb{F}_p$ *such that* H *is a subgroup of*

$$B_\lambda = \{B(1-b, \lambda b, 1) : b \in \mathbb{F}_p,\ b \not\equiv 1 \bmod p\}$$

and $V = \langle (\lambda, 1) \rangle$.

Proof. Clearly, the eigenvalues of a matrix $B(a,b,c)$ are a and c. A matrix $B(a,b,c)$ fixes each element in the subspace $\langle (1,0) \rangle$ if and only if $a \equiv 1 \bmod p$. If $V \neq \langle (1,0) \rangle$, then there is $\lambda \in \mathbb{F}_p$ such that $V = \langle (\lambda, 1) \rangle$. We claim that the matrices of the form $B(a,b,c)$ that fix $v_\lambda = (\lambda, 1)$ are those in the subgroup B_λ in the statement of the lemma. This is clear if $\lambda \equiv 0 \bmod p$, so we will assume λ is a unit. It is also clear that, if $B(a,b,c)$ fixes $(\lambda, 1)$ then c must be $1 \bmod p$. Moreover, a simple calculation shows that $B(1-b, \lambda b, 1)v_\lambda = v_\lambda$, for any $b \not\equiv 1 \bmod p$, so the matrices in B_λ fix v_λ.

Now, suppose that $B(a', b', 1)$, with $a' \in \mathbb{F}_p^\times$ and $b' \in \mathbb{F}_p$, fixes v_λ. Then the vector $v_\lambda = (\lambda, 1)$ is in the kernel of the matrix

$$M = B(1 - b'/\lambda, b', 1) - B(a', b', 1) \equiv B(1 - b'/\lambda - a', 0, 0) \bmod p.$$

Thus, $a' \equiv 1 - b'/\lambda \bmod p$. Hence, $B(a', b', 1) \equiv B(1 - b'/\lambda, b', 1) \in B_\lambda$, and this concludes the proof of the lemma. □

Theorem 9.3. *Let* $E/\mathbb{Q}$ *be an elliptic curve and let* p *be a prime such that the image of* $\rho_{E,p}$ *is a Borel subgroup* $B(J)$*, with respect to some basis* $\{P, Q\}$ *of* $E[p]$*. Then:*

(1) *The extension* $\mathbb{Q}(P)/\mathbb{Q}$ *is Galois, cyclic, of degree* $\leq p-1$*;*
(2) *If* $R \in E[p]$ *but* $R \notin \langle P \rangle$*, then* $[\mathbb{Q}(R) : \mathbb{Q}] \geq p$.

Proof. Let $G = \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$. By assumption, there exists an $\mathbb{F}_p$-basis $\{P, Q\}$ of $E[p]$ such that G is isomorphic to a Borel subgroup $B(J)$. By abuse of notation, we will say $G = B(J)$. Let R and H be as in Section 4. Hence, we can use Lemma 9.2 and there are two possibilities:

- $R \in \langle P \rangle$. Then $H = G \cap \left\{B(1, b, c) : b \in \mathbb{F}_p,\ c \in \mathbb{F}_p^\times\right\}$. A simple calculation shows that H is normal in $B(J)$ and, hence, $\mathbb{Q}(P)/\mathbb{Q}$ is Galois. Moreover, $G/H \hookrightarrow B(J)/\{B(1,b,c)\} \leq \mathbb{F}_p^\times$. Therefore $\mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ is cyclic and of degree $\leq p-1$.
- $R \notin \langle P \rangle$. Then $R \in \langle \lambda P + Q \rangle$ and $H = G \cap B_\lambda$. Thus $|H|$ is a divisor of $|B_\lambda| = p - 1$. Since $G = B(J)$, the order of G is divisible by p, and so $|G| \geq p \cdot |H| = p \cdot |G \cap B_\lambda|$. Hence,

$$|G/H| = |G|/|H| \geq p \cdot |G \cap B_\lambda| / |G \cap B_\lambda| \geq p.$$

The proof of the theorem is complete. □

In the rest of this section, our goal is to prove the following theorem.

Theorem 9.4. *Let* $E/\mathbb{Q}$ *be an elliptic curve and let* $p = 11$ *or* $p \geq 17$ *be a prime. Suppose that there is an* $\mathbb{F}_p$*-basis* $\{P, Q\}$ *of* $E[p]$ *such that the image of* $\rho_{E,p}$ *is a Borel subgroup. Let* $R \in E[p]$ *be non-trivial. Then* $[\mathbb{Q}(R) : \mathbb{Q}] \geq (p-1)/2$*, except if* $j = -7 \cdot 11^3$ *and* $p = 37$*, in which case* $[\mathbb{Q}(R) : \mathbb{Q}] \geq (p-1)/3 = 12$.

In order to prove Theorem 9.4, we shall use the classification of all $\mathbb{Q}$-rational points on the modular curves $X_0(N)$, which we discuss in the next subsection. We will tackle the proof of the theorem in Subsection 9.2.

9.1. **Rational points on the modular curve $X_0(N)$.** Let $\mathbb{H}$ be the complex upper half-plane, let $N \geq 1$ and let $\Gamma_0(N)$ be the usual congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$ given by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : c \equiv 0 \bmod N \right\}.$$

The group $\mathrm{SL}(2,\mathbb{Z})$ acts on $\mathbb{H}$ by linear fractional transformations, i.e., if $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ then we define an action $Mz = \frac{az+b}{cz+d}$, for any $z \in \mathbb{H}$. Let $Y_0(N) = \mathbb{H}/\Gamma_0(N)$ and let $X_0(N)$ be the compactification of $Y_0(N)$. The finite set of points in $X_0(N) \setminus Y_0(N)$ are called the cusps of $X_0(N)$, and can be identified with $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N)$. Thus constructed, $X_0(N)$ is a compact algebraic curve defined over $\mathbb{C}$, but it has a model defined over $\mathbb{Q}$ (see [35], §2, or [10], Ch. 7). Moreover, $X_0(N)$ is a moduli space of isomorphism classes of ordered pairs (E, C), where E is a complex elliptic curve and C is a cyclic subgroup of E of order N (see [10], Section 1.5). The non-cuspidal $\mathbb{Q}$-rational points of $X_0(N)$ have the following equivalent moduli interpretations:

- Isomorphism classes of pairs $(E/\mathbb{Q}, C/\mathbb{Q})$, where $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational cyclic subgroup C of E of order N.
- Isomorphism classes of pairs $(E/\mathbb{Q}, \langle P \rangle)$, where $E/\mathbb{Q}$ is an elliptic curve, and P is a torsion point of order N such that $\mathbb{Q}(P)$ is Galois over $\mathbb{Q}$.
- Isomorphism classes of elliptic curves $E/\mathbb{Q}$ such that the image of $\rho_{E,N}$ is contained in a Borel subgroup of $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ with respect to some $\mathbb{Z}/N\mathbb{Z}$-basis of $E[n]$.
- Isomorphism classes of pairs $(E/\mathbb{Q}, E'/\mathbb{Q}, \phi)$ of elliptic curves over $\mathbb{Q}$ and an isogeny $\phi : E \to E'$ with cyclic kernel of size N.

The $\mathbb{Q}$-rational points on $X_0(N)$ have been described completely in the literature, for all N. One of the most important milestones in the classification was [33], where Mazur dealt with the case when N is prime. The complete classification of $\mathbb{Q}$-rational points on $X_0(N)$, for any N, was completed due to work of Fricke, Kenku, Klein, Kubert, Ligozat, Mazur and Ogg, among others (see the references at the bottom of Tables 2, 3 and 4).

Theorem 9.5. *Let $N \geq 2$ be a number such that $X_0(N)$ has a non-cuspidal $\mathbb{Q}$-rational point. Then:*

(1) $N \leq 10$*, or* $N = 12, 13, 16, 18$ *or* 25*. In this case $X_0(N)$ is a curve of genus 0 and, hence, the is a 1-parameter family with infinitely many different $\mathbb{Q}$-rational points; or*

(2) $N = 11, 14, 15, 17, 19, 21, 27, 37, 43, 67$ *or* 163*. In this case $X_0(N)$ is a curve of genus ≥ 1 and there are only finitely many $\mathbb{Q}$-rational points.*

About Tables 2, 3 and 4. For the convenience of the reader, we have collected in Tables 3 and 4 a complete list of all non-cuspidal $\mathbb{Q}$-rational points on the modular curves $X_0(N)$. These points are well-known, but seem to be spread out accross the literature. Our main references are [4], [33] and [26], but we have consulted many other references, which we list at the bottom of each table.

When $X_0(N)$ is a curve of genus zero, its function field is generated over $\mathbb{C}$ by a single function $h = h_N$ (usually called the Hauptmodul of $X_0(N)$). In other words, the function field $\mathbb{C}(X_0(N))$ is of the form $\mathbb{C}(h)$. Since the modular j-invariant function is a Hauptmodul for $X_0(1) = X(1)$, the function field $\mathbb{C}(h)$ is a finite extension of $\mathbb{C}(j)$ and, therefore, h is algebraic over $\mathbb{C}(j)$. For each N such that $X_0(N)$ has genus 0, we have listed in Table 2 a choice of Hauptmodul $h = h_N$ in terms of the η function. In Table 3, we have listed an algebraic relation between h and j. For each N we have also listed a function j', in terms of h with the following property: for every elliptic curve E

with $j(E) = j$ there is an elliptic curve E' with $j(E') = j'$ and an isogeny $\phi : E \to E'$ with cyclic kernel of size N.

When $X_0(N)$ is a curve of genus ≥ 1, there are only finitely many $\mathbb{Q}$-points for each N, and these correspond to finitely many rational j-invariants. In Table 4, we list all the j-invariants and we also list the Cremona label of a representative for each class, with the least possible conductor. Finally, we indicate whether the j-invariant has complex multiplication. If it does, we list the associated quadratic discriminant.

Table 2: Hauptmoduln for the function field of $X_0(N)$, genus 0 case

N	Hauptmodul	N	Hauptmodul
2	$h = 2^{12} \cdot \left(\frac{\eta(2\tau)}{\eta(\tau)}\right)^{24}$	9	$h = 3 + 3^3 \cdot \left(\frac{\eta(9\tau)}{\eta(\tau)}\right)^{3}$
3	$h = 3^{6} \cdot \left(\frac{\eta(3\tau)}{\eta(\tau)}\right)^{12}$	10	$h = 4 + 2^2 5 \cdot \frac{\eta(2\tau)\eta(10\tau)^3}{\eta(\tau)^3\eta(5\tau)}$
4	$h = 2^{8} \cdot \left(\frac{\eta(4\tau)}{\eta(\tau)}\right)^{8}$	12	$h = 3 + 2^3 3 \cdot \frac{\eta(2\tau)^2\eta(3\tau)\eta(12\tau)^3}{\eta(\tau)^3\eta(4\tau)\eta(6\tau)^2}$
5	$h = 5^{3} \cdot \left(\frac{\eta(5\tau)}{\eta(\tau)}\right)^{6}$	13	$h = 13 \cdot \left(\frac{\eta(13\tau)}{\eta(\tau)}\right)^{2}$
6	$h = 2^3 3^2 \cdot \frac{\eta(2\tau)\eta(6\tau)^5}{\eta(\tau)^5\eta(3\tau)}$	16	$h = 2 + 2^3 \cdot \frac{\eta(2\tau)\eta(16\tau)^2}{\eta(\tau)^2\eta(8\tau)}$
7	$h = 7^{2} \cdot \left(\frac{\eta(7\tau)}{\eta(\tau)}\right)^{4}$	18	$h = 2 + 2 \cdot 3 \cdot \frac{\eta(2\tau)\eta(3\tau)\eta(18\tau)^2}{\eta(\tau)^2\eta(6\tau)\eta(9\tau)}$
8	$h = 4 + 2^5 \cdot \frac{\eta(2\tau)^2\eta(8\tau)^4}{\eta(\tau)^4\eta(4\tau)^2}$	25	$h = 1 + 5 \cdot \left(\frac{\eta(25\tau)}{\eta(\tau)}\right)$

Notation: $\eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$, and $q = e^{2\pi i\tau}$.

References: [12] eq. (80); [13]; [15], [18] pp. 370 - 458; [20] p. 1889; [31].

Table 3: All non-cuspidal rational points on $X_0(N)$, genus 0 case

N	j and j'-invariants such that E and E' are N-isogenous	
2	$j = \frac{(h+16)^3}{h}$	$j' = \frac{(h+256)^3}{h^2}$
3	$j = \frac{(h+27)(h+3)^3}{h}$	$j' = \frac{(h+27)(h+243)^3}{h^3}$
4	$j = \frac{(h^2+16h+16)^3}{h(h+16)}$	$j' = \frac{(h^2+256h+4096)^3}{h^4(h+16)}$
5	$j = \frac{(h^2+10h+5)^3}{h}$	$j' = \frac{(h^2+250h+5^5)^3}{h^5}$
6	$j = \frac{(h+6)^3(h^3+18h^2+84h+24)^3}{h(h+8)^3(h+9)^2}$	$j' = \frac{(h+12)^3(h^3+252h^2+3888h+15552)^3}{h^6(h+8)^2(h+9)^3}$
7	$j = \frac{(h^2+13h+49)(h^2+5h+1)^3}{h}$	$j' = \frac{(h^2+13h+49)(h^2+245h+2401)^3}{h^7}$
8	$j = \frac{(h^4-16h^2+16)^3}{(h^2-16)h^2}$	$j' = \frac{(h^4+240h^3+2144h^2+3840h+256)^3}{(h-4)^8h(h+4)^2}$
9	$j = \frac{h^3(h^3-24)^3}{h^3-27}$	$j' = \frac{(h+6)^3(h^3+234h^2+756h+2160)^3}{(h-3)^8(h^3-27)}$
10	$j = \frac{(h^6-4h^5+16h+16)^3}{(h+1)^2(h-4)h^5}$	$j' = \frac{(h^6+236h^5+1440h^4+1920h^3+3840h^2+256h+256)^3}{(h-4)^{10}h^2(h+1)^5}$
12	$j = \frac{(h^2-3)^3(h^6-9h^4+3h^2-3)^3}{h^4(h^2-9)(h^2-1)^3}$	$j' = \frac{(h^2+6h-3)^3(h^6+234h^5+747h^4+540h^3-729h^2-486h-243)^3}{(h-3)^{12}(h-1)h^3(h+1)^4(h+3)^3}$
13	$j = \frac{(h^2+5h+13)(h^4+7h^3+20h^2+19h+1)^3}{h}$	$j' = \frac{(h^2+5h+13)(h^4+247h^3+3380h^2+15379h+28561)^3}{h^{13}}$
16	$j = \frac{(h^8-16h^4+16)^3}{h^4(h^4-16)}$	
	$j' = \frac{(h^8+240h^7+2160h^6+6720h^5+17504h^4+26880h^3+34560h^2+15360h+256)^3}{(h-2)^{16}h(h+2)^4(h^2+4)}$	
18	$j = \frac{(h^3-2)^3(h^9-6h^6-12h^3-8)^3}{h^9(h^3-8)(h^3+1)^2}$	
	$j' = \frac{(h^3+6h^2+4)^3(h^9+234h^8+756h^7+2172h^6+1872h^5+3024h^4+48h^3+3744h^2+64)^3}{(h-2)^{18}h^2(h+1)^9(h^2-h+1)(h^2+2h+4)^2}$	
25	$j = \frac{(h^{10}+10h^8+35h^6-12h^5+50h^4-60h^3+25h^2-60h+16)^3}{h^5+5h^3+5h-11}$	
	$j' = \frac{(h^{10}+240h^9+2170h^8+8880h^7+34835h^6+83748h^5+206210h^4+313380h^3+503545h^2+424740h+375376)^3}{(h-1)^{25}(h^4+h^3+6h^2+6h+11)}$	

References: [12] eq. (80); [13]; [15], [18] pp. 370 - 458; [20] p. 1889; [31].

Table 4: All non-cuspidal rational points on $X_0(N)$, genus > 0 case

N, genus($X_0(N)$)	j-invariants	Cremona Labels	Conductor	CM?
11, $g = 1$	$j = -11 \cdot 131^3$	121A1, 121C2	11^2	No
	$j = -2^{15}$	121B1, 121B2	11^2	-11
	$j = -11^2$	121C1, 121A2	11^2	No
14, $g = 1$	$j = -3^3 \cdot 5^3$	49A1, 49A3	7^2	-7
	$j = 3^3 \cdot 5^3 \cdot 17^3$	49A2, 49A4	7^2	-28
15, $g = 1$	$j = -5^2/2$	50A1, 50B3	$2 \cdot 5^2$	No
	$j = -5^2 \cdot 241^3/2^3$	50A2, 50B4	$2 \cdot 5^2$	No
	$j = -5 \cdot 29^3/2^5$	50A3, 50B1	$2 \cdot 5^2$	No
	$j = 5 \cdot 211^3/2^{15}$	50A4, 50B2	$2 \cdot 5^2$	No
17, $g = 1$	$j = -17^2 \cdot 101^3/2$	14450P1	$2 \cdot 5^2 \cdot 17^2$	No
	$j = -17 \cdot 373^3/2^{17}$	14450P2	$2 \cdot 5^2 \cdot 17^2$	No
19, $g = 1$	$j = -2^{15} \cdot 3^3$	361A1, 361A2	19^2	-19
21, $g = 1$	$j = -3^2 \cdot 5^6/2^3$	162B1, 162C2	$2 \cdot 3^4$	No
	$j = 3^3 \cdot 5^3/2$	162B2, 162C1	$2 \cdot 3^4$	No
	$j = -3^2 \cdot 5^3 \cdot 101^3/2^{21}$	162B3, 162C4	$2 \cdot 3^4$	No
	$j = -3^3 \cdot 5^3 \cdot 383^3/2^7$	162B4, 162C3	$2 \cdot 3^4$	No
27, $g = 1$	$j = -2^{15} \cdot 3 \cdot 5^3$	27A2, 27A4	3^3	-27
37, $g = 2$	$j = -7 \cdot 11^3$	1225H1	$5^2 \cdot 7^2$	No
	$j = -7 \cdot 137^3 \cdot 2083^3$	1225H2	$5^2 \cdot 7^2$	No
43, $g = 3$	$j = -2^{18} \cdot 3^3 \cdot 5^3$	1849A1, 1849A2	43^2	-43
67, $g = 5$	$j = -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	4489A1, 4489A2	67^2	-67
163, $g = 13$	$j = -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	26569A1, 26569A2	163^2	-163

Remark: the Cremona labels are the representatives in this class of least conductor.

References: [4], pp. 78-80; [33]; [26]; [29], [38], [28], [34], [22], [23], [24], [25].

9.2. **Proof of Theorem 9.4.** Now that we have described all non-cuspidal $\mathbb{Q}$-rational point on $X_0(N)$, we can continue towards the proof of Theorem 9.4.

Lemma 9.6. *Let $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ be isomorphic elliptic curves (over $\mathbb{C}$) with $j(E) \neq 0$ or 1728, and let $\phi : E \to E'$ be an isomorphism. Then:*

(1) *E and E' are isomorphic over $\mathbb{Q}$ or E' is a quadratic twist of E.*
(2) *For all $R \in E(\overline{\mathbb{Q}})$, we have $\mathbb{Q}(x(R)) = \mathbb{Q}(x(\phi(R)))$.*

(3) *Moreover, if* $\mathbb{Q}(R)/\mathbb{Q}$ *is Galois, cyclic, and* $[\mathbb{Q}(x(R)):\mathbb{Q}]$ *is even, then the quotient* $[\mathbb{Q}(\phi(R)):\mathbb{Q}]/[\mathbb{Q}(R):\mathbb{Q}] = 1$ *or* 2.

Proof. Let E and E', respectively, be given by Weierstrass equations $y^2 = x^3 + Ax + B$ and $y^2 = x^3 + A'x + B'$, with coefficients in $\mathbb{Z}$. Since $j(E) = j(E') \neq 0, 1728$, none of the coefficients is zero. By [48], Ch. III, Prop. 3.1, the isomorphism $\phi : E \to E'$ is given by $(x, y) \mapsto (u^2x, u^3y)$ for some $u \in \overline{\mathbb{Q}} \setminus \{0\}$. Hence $A' = u^4A$ and $B' = u^6B$, and so $u^2 \in \mathbb{Q}$. Thus, either $E \cong_{\mathbb{Q}} E'$ or E' is the quadratic twist of E by u.

Let $R \in E(\overline{\mathbb{Q}})$. If $E \cong_{\mathbb{Q}} E'$ then $\mathbb{Q}(R) = \mathbb{Q}(\phi(R))$ and the same holds for the subfields of the x-coordinates, so (2) and (3) are immediate. Let us assume for the rest of the proof that E' is the quadratic twist of E by $\sqrt{d}$, for some square-free $d \in \mathbb{Z}$. It follows that $\phi((x, y)) = (dx, d\sqrt{d}\cdot y)$ and, therefore, $\mathbb{Q}(x(\phi(R))) = \mathbb{Q}(d \cdot x(R)) = \mathbb{Q}(x(R))$. This proves (2).

Let $x = x(R)$ and $y = y(R)$. Then $\mathbb{Q}(R) = \mathbb{Q}(x, y)$ and $\mathbb{Q}(\phi(R)) = \mathbb{Q}(x, \sqrt{d}\cdot y)$. The degree of $\mathbb{Q}(x, y)/\mathbb{Q}(x)$ is 1 or 2 because y is given by the Weierstrass equation $y^2 = x^3 + Ax + B$.

- If $\mathbb{Q}(x) = \mathbb{Q}(x, y) = \mathbb{Q}(R)$, then $y \in \mathbb{Q}(x)$ and $\mathbb{Q}(x, \sqrt{d}\cdot y) = \mathbb{Q}(x, \sqrt{d})$. Thus, we have $[\mathbb{Q}(\phi(R)) : \mathbb{Q}] = [\mathbb{Q}(x, \sqrt{d}) : \mathbb{Q}(x)] \cdot [\mathbb{Q}(x) : \mathbb{Q}]$ and hence $[\mathbb{Q}(\phi(R)) : \mathbb{Q}]/[\mathbb{Q}(R) : \mathbb{Q}] = 1$ or 2.
- Suppose $\mathbb{Q}(x, y)/\mathbb{Q}(x)$ is quadratic. If $\mathbb{Q}(x, \sqrt{d}\cdot y)/\mathbb{Q}(x)$ is also quadratic, then we have $[\mathbb{Q}(\phi(R)) : \mathbb{Q}]/[\mathbb{Q}(R) : \mathbb{Q}] = 1$. Otherwise, assume that $\mathbb{Q}(x, \sqrt{d}\cdot y) = \mathbb{Q}(x)$ and we will reach a contradiction. Indeed, in this case $\sqrt{d}\cdot y \in \mathbb{Q}(x)$. Hence, there is $z \in \mathbb{Q}(x)$ such that $y = \sqrt{d}\cdot z$ and we may conclude that $\mathbb{Q}(x, y) = \mathbb{Q}(x, \sqrt{d})$. It follows that $\sqrt{d} \in \mathbb{Q}(R)$. Let $K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(R)$. Since $\mathbb{Q}(R)/\mathbb{Q}$ is Galois and cyclic, K is the unique quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(R)$. Moreover, $\mathbb{Q}(x)/\mathbb{Q}$ is of even degree by assumption, and Galois, cyclic because $\mathbb{Q}(x) \subseteq \mathbb{Q}(R)$. Thus, $K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(x)$. It would follow that $\mathbb{Q}(x, y) = \mathbb{Q}(x, \sqrt{d}) = \mathbb{Q}(x)$ which is a contradiction, since we have assumed that $\mathbb{Q}(R)/\mathbb{Q}(x)$ is quadratic.

This proves (3) and concludes the proof of the lemma. □

In the proof of Theorem 9.4, we will also use the following result about the field of definition of torsion points for elliptic curves with complex multiplication.

Theorem 9.7 (Silverberg [47], Prasad-Yogananda [41]; see also [5])**.** *Let F be a number field of degree d, and let E/F be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in the imaginary quadratic field K. Let $w = w(\mathcal{O}) = \#\mathcal{O}^\times$ (so $w = 2, 4$ or 6) and let e be the maximal order of an element of $E(F)_{tors}$. Then:*

(1) $\varphi(e) \leq wd$ *(φ is Euler's totient function).*
(2) *If $K \subseteq F$, then $\varphi(e) \leq \frac{w}{2}d$.*
(3) *If F does not contain K, then $\varphi(\#E(F)_{tors}) \leq wd$.*

Corollary 9.8. *Let $p = 11$, 19, 43, 67, or 163. There is an elliptic curve $E/\mathbb{Q}$ with CM by $\mathbb{Q}(\sqrt{-p})$ and a non-trivial point $P \in E[p]$ such that $[\mathbb{Q}(P) : \mathbb{Q}] = (p-1)/2$.*

Proof. Let $E/\mathbb{Q}$ be the elliptic curve with CM by $\mathbb{Z}[\sqrt{-p}]$ and conductor $N_E = p^2$, whose j-invariant and Cremona label are listed in Table 4. Let $E/\mathbb{Q}$ be given by a Weierstrass equation $y^2 = x^3+Ax+B$. It is well known that $E/\mathbb{Q}$ has a $\mathbb{Q}$-rational p-isogeny (see, for example, [33]) and, therefore, there is a basis $\{P, Q\}$ of $E[p]$ such that the image G of $\rho_{E,p}$ is a Borel subgroup and, more concretely, for all

$\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have $\rho_{E,p}(\sigma) = B(\psi(\sigma), b, c)$, where $b, c \in \mathbb{F}_p$ and ψ is a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. By Theorems 9.3 and 9.7, we have that $[\mathbb{Q}(P) : \mathbb{Q}] = (p-1)/2$ or $p-1$.

Suppose that $[\mathbb{Q}(P) : \mathbb{Q}] = p-1$. Then the character $\psi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_p^\times$ is surjective. Let χ be the quadratic character $\left(\frac{\psi}{p}\right)$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol, and let $E' = E^\chi$ be the quadratic twist of E by χ. Then, $j(E') = j(E)$, so E' also has CM by $\mathbb{Q}(\sqrt{-p})$. Moreover, the image of $\rho_{E',p}$ is also a Borel, with respect to some basis $\{P', Q'\}$ and for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have $\rho_{E',p}(\sigma) = B(\chi(\sigma)\psi(\sigma), b', c')$ for some $b', c' \in \mathbb{F}_p$ (see [48], Ch. X, §3, Example 2.4). Since $p \equiv 3 \bmod 4$, the image of the character $\chi\psi$ has size $(p-1)/2$ and, therefore, $[\mathbb{Q}(P') : \mathbb{Q}] = (p-1)/2$ as desired. □

Now we are ready to prove our theorem.

Proof of Theorem 9.4. Let $E/\mathbb{Q}$ be an elliptic curve and let $p = 11$ or $p \geq 17$ be a prime. Suppose that there is an $\mathbb{F}_p$-basis $\{P, Q\}$ of $E[p]$ such that the image of $\rho_{E,p}$ is a Borel subgroup. Let $R \in E[p]$ be non-trivial.

By Theorem 9.3, if $R \in E[p]$ but $R \notin \langle P \rangle$, then $[\mathbb{Q}(R) : \mathbb{Q}] \geq p$. Hence, we may assume for the rest of the proof that $R = P$. Moreover, by the classification of all non-cuspidal $\mathbb{Q}$-points on $X_0(p)$, as in Subsection 9.1, the prime p is 11, 17, 19, 37, 43, 67 or 163, and $j(E)$ is one of the j-invariants in Table 4.

When $N = p$ is prime, every j-invariant in Table 4 with CM has complex multiplication by the maximal order $\mathcal{O}_j$ in a quadratic imaginary field K_j, with discriminant $\neq -3, -4$. Therefore, $w_j = \#\mathcal{O}_j^\times = 2$. By setting $F = \mathbb{Q}(R)$ in Theorem 9.7, we deduce that $[\mathbb{Q}(R) : \mathbb{Q}] \geq \varphi(p)/w_j = (p-1)/2$, as claimed.

It remains to treat the cases in Table 4, where $N = p$ is prime and j does not have CM. Such j-invariants are listed in Table 5, and we have also listed a polynomial $q(x) \in \mathbb{Q}[x]$ that has $x(R)$ as a root, where we have taken E to be the first Cremona label listed for each j in Table 4. Each polynomial was calculated using the computer package Sage: $q(x)$ is an irreducible factor of the p-th division polynomial with smallest positive degree. By Lemma 9.6, the field $\mathbb{Q}(x(R))$ is well-defined up to isomorphism of $E/\mathbb{Q}$. Hence, the degrees of the polynomials in Table 5 show that

$$[\mathbb{Q}(P) : \mathbb{Q}] \geq [\mathbb{Q}(x(P)) : \mathbb{Q}] \geq (p-1)/2$$

when $p = 11$ (any j), or $p = 17$ and $j = -17^2 \cdot 101^3/2$, or $p = 37$ and $j = -7 \cdot 137^3 \cdot 2083^3$.

Only two cases are left to consider:

- Let $p = 17$ and $j = -17 \cdot 373^3/2^{17}$. The degree of $\mathbb{Q}(x(R))/\mathbb{Q}$ is 4 and, using Sage, one can show that $\mathbb{Q}(R) = \mathbb{Q}(x(R), y(R))$ is of degree 8, Galois over $\mathbb{Q}$, cyclic, and generated by a root of

$$\begin{aligned}&x^8 - 478x^7 + 114898348x^6 - 55311970256x^5 + 4018578903430720x^4\\&-1445438002496889856x^3 + 519706420623863049748 48x^2\\&-98106828426813091216097 28x + 18827444206339859302794631577 6 = 0.\end{aligned}$$

  Since $[\mathbb{Q}(x(R)) : \mathbb{Q}] = 4$ is even, by Lemma 9.6, part (3), the degree of $\mathbb{Q}(R)/\mathbb{Q}$ is 8 or 16 for all elliptic curves with j-invariant $j = -17 \cdot 373^3/2^{17}$. Hence $[\mathbb{Q}(R) : \mathbb{Q}] \geq (p-1)/2 = 8$.
- Finally, let $p = 37$ and $j = -7 \cdot 11^3$. The degree of $\mathbb{Q}(x(R))/\mathbb{Q}$ is 6 and, using Sage, one can show that $\mathbb{Q}(R) = \mathbb{Q}(x(R), y(R))$ is of degree 12,Galois over $\mathbb{Q}$, cyclic, and generated by a

root of

$$x^{12}+91x^{11}-510286x^{10}-5285035x^{9}-13216280x^{8}+29005256x^{7}+166375776x^{6}$$
$$+155428049x^{5}-180670105x^{4}-273432740x^{3}-9522366x^{2}+10706059x+1010821=0.$$

Since $[\mathbb{Q}(x(R)):\mathbb{Q}]=6$ is even, by Lemma 9.6, part (3), the degree of $\mathbb{Q}(R)/\mathbb{Q}$ is 12 or 24 for all elliptic curves with j-invariant $j=-7\cdot 11^3$. Hence $[\mathbb{Q}(R):\mathbb{Q}]\geq (p-1)/3=12$.

This concludes the proof of Theorem 9.4. □

Table 5: Non-cuspidal $\mathbb{Q}$-points on $X_0(p)$, genus >0, $p\geq 11$ prime, non-CM

N	j-invariants	Irreducible polynomial with root $x=x(P)$
11	$j=-11\cdot 131^3$	$x^5+14x^4+63x^3+62x^2-230x-439$
	$j=-11^2$	$x^5+14x^4+30x^3-37x^2-76x+1$
17	$j=-17^2\cdot 101^3/2$	$x^8-226x^7+18372x^6-543828x^5-9242705x^4+1127218758x^3$ $-33006143963x^2+437271444481x-2252576338909$
	$j=-17\cdot 373^3/2^{17}$	$x^4+482x^3+1144x^2-15809842x-958623689$
37	$j=-7\cdot 11^3$	$x^6-85x^5+435x^4-750x^3+400x^2+125x-125$
	$j=-7\cdot 137^3\cdot 2083^3$	

$$\begin{gathered}x^{18}+4540x^{17}+9432590x^{16}+11849891575x^{15}+9976762132800x^{14}\\ +5848587595725875x^{13}+2353459307197093375x^{12}+568092837455595073750x^{11}\\ +104971669015525170187 50x^{10}-58167719763827256503515625x^{9}\\ -29123957981672764259404562500x^{8}-86425348744787339517475903125 00x^{7}\\ -1813067882488802075989763827437500x^{6}\\ -2805306298032756694345875261417968 75x^{5}\\ -320923174592951987009017556294203906 25x^{4}\\ -265364776129956997628028623910045664 0625x^{3}\\ -1505123571836944993538892424156400152 34375x^{2}\\ -525141102271763847437919446615343235 7421875x\\ -3148881707222283483037230006935969560314453125/37\end{gathered}$$

Acknowledgements. This work was motivated by an earlier collaboration with Benjamin Lundell, where we described bounds on fields of definition in terms of ramification indices [30]. The author would like to thank Benjamin Lundell, Robert Pollack, Jeremy Teitelbaum, Ravi Ramakrishna, and the anonymous referee for their helpful suggestions and comments. In addition, my thanks to Tyler Genao for alerting me to an issue in the proof of Theorem 6.5 which has now been corrected in this version of the paper.

References

[1] E. Artin, *Algebraic Numbers and Algebraic Functions*, American Mathematical Society Chelsea Publishing, 2006.
[2] Y. Bilu, P. Parent, *Serre's uniformity problem in the split Cartan case*, Annals of Mathematics, Volume 173 (2011), Issue 1, pp. 569-584.

[3] Y. Bilu, P. Parent, M. Rebolledo, *Rational points on $X_0^+(p^r)$*, arXiv:1104.4641v1

[4] B. J. Birch, W. Kuyk (Editors), *Modular functions of one variable IV*, Lecture Notes in Mathematics 476, Berlin-Heidelberg-New York, Springer 1975.

[5] P. L. Clark, B. Cook, J. Stankewicz, *Torsion points on elliptic curves with complex multiplication*, preprint.

[6] A. C. Cojocaru, *On the surjectivity of the Galois representations associated to non-CM elliptic curves (with an appendix by Ernst Kani)*, Canad. Math. Bull. 48 (2005), pp. 16-31.

[7] A. C. Cojocaru, C. Hall, *Uniform results for Serre's theorem for elliptic curves*, Int. Math. Res. Not. 2005, pp. 3065-3080.

[8] H. Daniels, *Siegel functions, modular curves, and Serre's uniformity problem*, Ph.D. Thesis (in preparation), University of Connecticut.

[9] M. Derickx, S. Kamienny, W. Stein, M. Stoll, *Torsion points on elliptic curves over number fields of small degree*, in preparation (private communication).

[10] F. Diamond, J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics 228, Springer-Verlag, 2nd Edition, New York, 2005.

[11] B. Edixhoven, *Rational torsion points on elliptic curves over number fields (after Kamienny and Mazur)*. Séminaire Bourbaki, Vol. 1993/94. Astérisque No. 227 (1995), Exp. No. 782, 4, 209-227.

[12] N. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, in Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin (D.A. Buell and J.T. Teitelbaum, eds.; AMS/International Press, 1998), pp. 21-76.

[13] N. Elkies, *Explicit Modular Towers*, in Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing (1997, T. Basar, A. Vardy, eds.), Univ. of Illinois at Urbana-Champaign 1998, pp. 23-32 (math.NT/0103107 on the arXiv).

[14] É. Gaudron, G. Rémond, *Théorème des périodes et degrés minimaux d'isogénies*, manuscript (2011), arXiv:1105.1230v1.

[15] R. Fricke, F. Klein, *Vorlesungen ъber die Theorie der elliptischen Modulfunctionen* (Volumes 1 and 2), B. G. Teubner, Leipzig 1890, 1892.

[16] G. Faltings, *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), 175-182, Perspect. Math., 15, Academic Press, San Diego, CA, 1994.

[17] G. Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. 85 (1994), no. 1-3, 79-83.

[18] R. Fricke, *Die elliptischen Funktionen und ihre Anwendungen*. Leipzig-Berlin: Teubner 1922.

[19] Y. Fujita, *Torsion subgroups of elliptic curves in elementary abelian 2-extensions of* $\mathbb{Q}$, J. Number Theory 114 (2005), 124-134.

[20] N. Ishii, *Rational Expression for J-invariant Function in Terms of Generators of Modular Function Fields*, International Mathematical Forum, 2, 2007, no. 38, pp. 1877 - 1894.

[21] S. Kamienny, B. Mazur, *Rational torsion of prime order in elliptic curves over number fields. With an appendix by A. Granville*. Columbia University Number Theory Seminar (New York, 1992). Astйrisque No. 228 (1995), 3, 81-100.

[22] M. A. Kenku, *The modular curve $X_0(39)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. 85 (1979), pp. 21 - 23.

[23] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. 87 (1980), pp. 15 - 20.

[24] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) 22 (1980), 239 - 244.

[25] M. A. Kenku, *The modular curve $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) 23 (1981), 415 - 427.

[26] M. A. Kenku, *On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class*, J. Number Th. 15 (1982), 199-202.

[27] A. Kraus, *Une remarque sur les points de torsion des courbes elliptiques*, C. R. Acad. Sci. Paris Sr. I Math. 321 (1995), pp. 1143-1146.

[28] S. D. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3), 33 (1976), pp. 193 - 237.

[29] G. Ligozat, *Courbes Modulaires de genre 1*, Bull. Soc. Math. France (1975), pp. 1 - 80.

[30] Á. Lozano-Robledo, B. Lundell, *Bounds for the torsion of elliptic curves over extensions with bounded ramification*, International Journal of Number Theory, Volume: 6, Issue: 6 (2010), pp. 1293-1309.

[31] R. Maier, *On Rationally Parametrized Modular Equations*, J. Ramanujan Math. Soc. 24 (2009), pp. 1 - 73.

[32] D. W. Masser, G. Wüstholz, *Galois properties of division fields of elliptic curves*, Bull. London Math. Soc. 25 (1993), pp. 247-254.
[33] B. Mazur, *Rational isogenies of prime degree*, Inventiones Math. 44 (1978), pp. 129 - 162.
[34] B. Mazur, J. Vélu, *Courbes de Weil de conducteur 26*, C. R. Acad. Sc. Paris, t. 275 (1972), série A, pp. 743-745.
[35] B. Mazur, *Rational points on modular curves* (in [44]), Proceedings of Conference on Modular Functions held in Bonn, Lecture Notes in Math. 601, Springer-Verlag, Berlin-Heiderberg-New York (1977), pp. 107-148.
[36] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. 124 (1996), no. 1-3, 437-449.
[37] F. Momose, *Rational points on the modular curves $X_{split}(p)$*, Compositio Math., 52 (1984),115-137.
[38] A. Ogg, *Rational points on certain elliptic modular curves*, Proc. Symp. Pure Math. XXIX, AMS, (1973) pp. 221 - 231.
[39] P. Parent, *No* 17*-torsion on elliptic curves over cubic number fields*, Journal de Théorie des Nombres de Bordeaux 15 (2003), 831-838.
[40] F. Pellarin, *Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques*, Acta Arith. 100 (2001), pp. 203-243.
[41] D. Prasad, C. S. Yogananda, *Bounding the torsion in CM elliptic curves*. C. R. Math. Acad. Sci. Soc. R. Can. 23 (2001), 1-5.
[42] M. Rebolledo, *Module supersingulier et points rationnels des courbes modulaires*, Thèse, Universié Pierre et Marie Curie, 2004.
[43] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), pp. 259-331.
[44] J.-P. Serre, D. B. Zagier (Editors), *Modular Functions of One Variable V: Proceedings International Conference*, University of Bonn, Sonderforschungsbereich Theoretische Mathematik, July 2-14, 1976: No. V (Lecture Notes in Mathematics 601).
[45] J.-P. Serre, *Points rationnels des courbes modulaires $X_0(N)$*, Seminaire Bourbaki, 1977/1978, No. 511.
[46] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. IHES 54 (1981), pp. 123-201.
[47] A. Silverberg, *Torsion points on abelian varieties of CM-type*. Compositio Math. 68 (1988), no. 3, 241-249.
[48] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 2nd Edition, New York, 2009.
[49] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York.

Dept. of Mathematics, Univ. of Connecticut, Storrs, CT 06269, USA
E-mail address: alozano@math.uconn.edu