Rev. Mat. Iberoam. **31** (2015), no. 4, 1311–1332
DOI 10.4171/RMI/870

Division fields of elliptic curves with minimal ramification

Álvaro Lozano-Robledo

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$, let p be a prime number, and let $n \geq 1$. It is well-known that the p^n-th division field $\mathbb{Q}(E[p^n])$ of the elliptic curve E contains all the p^n-th roots of unity. It follows that the Galois extension $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is ramified above p, and the ramification index $e(p, \mathbb{Q}(E[p^n])/\mathbb{Q})$ of any prime $\wp$ of $\mathbb{Q}(E[p^n])$ lying above p is divisible by $\varphi(p^n)$. The goal of this article is to construct elliptic curves $E/\mathbb{Q}$ such that $e(p, \mathbb{Q}(E[p^n])/\mathbb{Q})$ is precisely $\varphi(p^n)$, and such that the Galois group of $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is as large as possible, i.e., isomorphic to $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$, let p be a prime number, and let $n \geq 1$. The central object of study of this article is the number field $\mathbb{Q}(E[p^n])$ that results by adjoining to $\mathbb{Q}$ the coordinates of all p^n-torsion points on $E(\overline{\mathbb{Q}})$, where $\overline{\mathbb{Q}}$ is a fixed algebraic closure of $\mathbb{Q}$. The existence of the Weil pairing ([24], III, Corollary 8.1.1) implies that $\mathbb{Q}(E[p^n])$ contains all the p^n-th roots of unity of $\overline{\mathbb{Q}}$, i.e., we have an inclusion $\mathbb{Q}(\zeta_{p^n}) \subseteq \mathbb{Q}(E[p^n])$, where ζ_{p^n} is a primitive p^n-th root of unity. It follows that the Galois extension $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is ramified above p, and the ramification index of any prime $\wp$ of $\mathbb{Q}(E[p^n])$ lying above p, denoted by $e(p, \mathbb{Q}(E[p^n])/\mathbb{Q})$, is divisible by $\varphi(p^n) = e(p, \mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$. The goal of this article is to construct elliptic curves $E/\mathbb{Q}$ such that $e(p, \mathbb{Q}(E[p^n])/\mathbb{Q})$ is *precisely* $\varphi(p^n)$. In other words, we are interested in finding elliptic curves such that the ramification index of the primes above p in $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is minimal (and equal to $\varphi(p^n)$). One such example is the curve $E/\mathbb{Q}$ with Cremona label "11a1" and Weierstrass model

$$E/\mathbb{Q} : y^2 + y = x^3 - x^2 - 10x - 20.$$

In this case $\mathbb{Q}(E[5])/\mathbb{Q}$ is rather small; in fact, $\mathbb{Q}(E[5]) = \mathbb{Q}(\zeta_5)$ and the ramification at 5 is indeed minimal as defined above (we will discuss this example

Mathematics Subject Classification (2010): Primary 11G05; Secondary 14H52.
Keywords: Elliptic curve, ramification, division field, torsion subgroup.

further in Question 4.7 and Example 8.4). Moreover, we know that in general $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q})$ is isomorphic to a subgroup of $\mathrm{GL}(2,\mathbb{Z}/p^n\mathbb{Z})$, so we are interested in constructing elliptic curves such that the extension $\mathbb{Q}(E[p^n])/\mathbb{Q}$ has minimal ramification above p, and it is as large as possible, i.e., $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}) \cong \mathrm{GL}(2,\mathbb{Z}/p^n\mathbb{Z})$. When this occurs, we have $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n})) \cong \mathrm{SL}(2,\mathbb{Z}/p^n\mathbb{Z})$, and the extension $\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n})$ is unramified at all primes above the rational prime p. For instance, this is the case for $p = 5$, $n = 5$, and the curve

$$E/\mathbb{Q} : y^2 + y = x^3 - 11x + 14.$$

Moreover, the extension $\mathbb{Q}(E[5^5])/\mathbb{Q}(\zeta_{5^5})$ is only ramified at primes above 2539. The main theorem of this article is as follows.

Theorem 1.1. *For every prime p and every integer $n \geq 1$, and for every ordinary j-invariant $\lambda \in \mathbb{F}_p$, with $\lambda \not\equiv 0, 1728 \bmod p$, there are infinitely many non-isomorphic, non-CM, elliptic curves E, defined over $\mathbb{Q}$, such that*

(a) *$j(E) \equiv \lambda \bmod p$ and $E/\mathbb{Q}$ has ordinary good reduction at p,*

(b) *the ramification index of p in the extension $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is exactly $\varphi(p^n)$, and*

(c) *$E[p]$ an irreducible $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module.*

Moreover, if $p \geq 17$ and E is such an elliptic curve, the representation $\rho_{E,p^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p^n]) \cong \mathrm{GL}(2,\mathbb{Z}/p^n\mathbb{Z})$ given by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[p^n]$ is surjective. In particular, $\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n})$ is a $\mathrm{SL}(2,\mathbb{Z}/p^n\mathbb{Z})$ extension, unramified at primes above p.

For example, let $p = 37$ and $n = 2$. Then, for each integer $k \geq 1$, the elliptic curve

$$E_{2,k} : y^2 + \beta_k xy = x^3 - 36\beta_k^3 x - \beta_k^5,$$

with $\beta_k = 9490 + 50653k$ and $j(E_{2,k}) = 11218 + 50653k$, satisfies that the extension $\mathbb{Q}(E_{2,k}[37^2])/\mathbb{Q}(\zeta_{37^2})$ has Galois group $\mathrm{SL}(2,\mathbb{Z}/37^2\mathbb{Z})$, and it is unramified at primes above 37 (see Examples 6.4 and 7.5 for similar infinite families of elliptic curves, for any $n \geq 1$).

The proof of Theorem 1.1 is as follows. The existence of infinitely many elliptic curves with minimal ramification is a consequence of Gross' work on companion forms ([6]; see Section 4), the classification of non-cuspidal rational points on the modular curves $X_0(N)$ (see for instance Section 9 of [14]), and Hilbert's irreducibility theorem (Section 5). The existence of infinitely many $\mathrm{SL}(2,\mathbb{Z}/p^n\mathbb{Z})$ extensions unramified above p is shown in Section 7 as an application of Serre's classification of maximal subgroups of $\mathrm{GL}(2,\mathbb{Z}/p\mathbb{Z})$ as in Theorem 7.2, and recent work of Bilu, Parent, and Rebolledo ([1], [2]) on the split case of Serre's uniformity question.

The first two sections discuss background material on Borel subgroups, and elliptic curves with ordinary good reduction, respectively. In order to apply Gross' criterion we need to calculate certain canonical lifts of j-invariants mod p. We explain how to do this in Section 4, and offer several examples (see Example 4.6). In Section 6 we provide examples of curves with minimal ramification for small primes p. In Section 8, we use the level 1 case of Serre's modularity conjecture [21] (now a theorem of Khare [9], and shown independently by Dieulefait [5]) to show the following theorem (the usual p-adic valuation of $\mathbb{Q}$ will be denoted by ν_p).

Theorem 1.2. *Let p be a prime, let $n \geq 1$, and let $E/\mathbb{Q}$ be an elliptic curve such that the Galois representation on the p-torsion $\overline{\rho}_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[p])$ is absolutely irreducible, and with either good reduction at p, or with multiplicative reduction at p and $\nu_p(j(E))$ divisible by p. Then, the extension $\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n})$ is always ramified at least at one prime ideal above a rational prime q distinct from p.*

As a corollary of Theorem 1.2, we see that any elliptic curve $E/\mathbb{Q}$ with good reduction at p, and such that the extension $\mathbb{Q}(E[p^n])/\mathbb{Q}$ has Galois group isomorphic to $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ and is minimally ramified at primes above p (i.e., elliptic curves whose existence we prove in Theorem 1.1), must also satisfy that $\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n})$ ramifies at least at one prime not above p.

Finally, at the end of Section 8 we calculate several examples of elliptic curves with Galois group $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n}))$ isomorphic to $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$, and such that $\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n})$ is ramified above exactly one prime $q \neq p$.

Acknowledgements. I would like to thank Kevin Buzzard, Fred Diamond, Benedict Gross, and Felipe Voloch for their help, and suggestions. I would like to give special thanks to Robert Pollack for pointing out that one can use Serre's conjecture to prove Theorem 1.2. Finally, I'd like to thank the two referees for their very helpful comments and suggestions.

2. Borel subgroups

In this section we discuss generalities on Borel subgroups.

Definition 2.1. Let p be a prime, and $n \geq 1$. We say that a subgroup B of $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is Borel if every matrix in B is upper triangular, i.e.,

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

We say that B is a non-diagonal Borel subgroup if none of the conjugates of B in $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is formed solely by diagonal matrices. If B is a Borel subgroup, we denote by B_1 the subgroup of B formed by those matrices in B whose diagonal coordinates are $1 \bmod p^n$, and we denote by B_d the subgroup of B formed by diagonal matrices, i.e.,

$$B_1 = B \cap \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}/p^n\mathbb{Z} \right\}, \quad B_d = B \cap \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} : a, c \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\}.$$

Lemma 2.2. *Let $p > 2$ be a prime, $n \geq 1$ and let $B \leq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ be a Borel subgroup, such that B contains a matrix $g = \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ with $a \not\equiv c \bmod p$. Let $B' = h^{-1}Bh$ with $h = \left(\begin{smallmatrix} 1 & b/(c-a) \\ 0 & 1 \end{smallmatrix}\right)$. Then, $B' \leq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is a Borel subgroup conjugated to B satisfying the following properties:*

(1) $B' = B'_d B'_1$, *i.e., for every* $M \in B'$ *there is* $U \in B'_d$ *and* $V \in B'_1$ *such that* $M = UV$*; and*

(2) $B/[B,B] \cong B'/[B',B']$ *and* $[B',B'] = B'_1$.

If follows that $[B,B] = B_1$, *and that* B_1 *is a cyclic subgroup of order* p^s *for some* $0 \leq s \leq n$.

Proof. Notice that $h^{-1}gh = \left(\begin{smallmatrix} a & 0 \\ 0 & c \end{smallmatrix}\right) \in B'$. If B' only contains diagonal matrices, then $B' = B'_d$ and the statement is trivial. Otherwise, let $v(B')$ be the smallest non-negative among all the top-right coordinates of matrices in B', and let $\left(\begin{smallmatrix} e & f \\ 0 & l \end{smallmatrix}\right) \in B'$ such that $f \not\equiv 0 \bmod p^n$ and the valuation of f is precisely $v(B')$. Then, the following commutator belongs to B':

$$k = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}\begin{pmatrix} e & f \\ 0 & l \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}^{-1}\begin{pmatrix} e & f \\ 0 & l \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \frac{f}{l}(\frac{a}{c}-1) \\ 0 & 1 \end{pmatrix}.$$

Since e, l are units and $a \not\equiv c \bmod p$, we conclude that $f(a/c-1)/l$ also has valuation $v(B')$. Let $m \in \mathbb{Z}$ be an integer such that $(f(a/c-1)/l)\cdot m \equiv p^{v(B')} \bmod p^n$. Then, $k^m = \left(\begin{smallmatrix} 1 & p^{v(B')} \\ 0 & 1 \end{smallmatrix}\right) \in B'$. Now, if $\beta \equiv 0 \bmod p^{v(B')}$, then there is some β' such that $\beta \equiv \beta' p^{v(B)} \bmod p^n$. Thus, if $M = \left(\begin{smallmatrix} \alpha & \beta \\ 0 & \gamma \end{smallmatrix}\right)$ is an arbitrary non-diagonal element of B', we have

$$\begin{aligned} M = \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} &= \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}(k^m)^{-\beta'/\alpha}(k^m)^{\beta'/\alpha} \\ &= \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}\begin{pmatrix} 1 & -\frac{\beta' p^{\nu(B')}}{\alpha} \\ 0 & 1 \end{pmatrix}(k^m)^{\beta'/\alpha} = \begin{pmatrix} \alpha & 0 \\ 0 & \gamma \end{pmatrix}(k^m)^{\beta'/\alpha}. \end{aligned}$$

Thus, we have shown that with $U = M(k^m)^{-\beta'/\alpha} \in B'_d$, $V = (k^m)^{\beta'/\alpha} \in B'_1$ we have $M = UV \in B'_d B'_1$. This shows (1). Moreover, it is clear that any commutator in $[B',B']$ has diagonal coordinates congruent to 1 modulo p^n and, therefore, $[B',B'] \leq B'_1$. Notice that if $M \in B'_1$, i.e., $\alpha \equiv \gamma \equiv 1 \bmod p^n$, and $m \in \mathbb{Z}$ as above, then U is the identity and $M = V = (k^m)^{\beta'} \in B'_1$. Since k is a commutator, this shows that $B'_1 \leq [B',B']$. Thus, $[B',B'] = B'_1$. Notice that $B_1 = hB'_1h^{-1}$. Hence, $[B,B] = h[B',B']h^{-1} = hB'_1h^{-1} = B_1$, as claimed in (2). Finally, $B \cong B'$, so

$$B/[B,B] \cong B'/[B',B'] \cong (B'_d B'_1)/B'_1 \cong B'_d \leq (\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

This shows (2) and concludes the proof of the lemma. □

Remark 2.3. The result of the previous lemma is simply false for $p = 2$, i.e., the assumption $p > 2$ is not just technical (the requirement $p > 2$ is needed for the existence of a matrix g as in the statement of the lemma). For instance, the Borel group

$$B = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in (\mathbb{Z}/4\mathbb{Z})^\times,\ b \equiv 0 \bmod 2\right\} \leq \mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$$

is *abelian*, so the commutator of B is trivial. The results of the lemma are also not necessarily true if the diagonal entries of each element in the Borel subgroup B are congruent modulo p (i.e., if there is no such element g as in the statement of the lemma). For instance, let B be the subgroup

$$B = \left\{ \begin{pmatrix} (1+p^{n-1})^t & t(1+p^{n-1})^{t-1}p^{n-1} \\ 0 & (1+p^{n-1})^t \end{pmatrix} \ : \ t = 1, \ldots, p \right\}$$

of $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. Suppose there is a subgroup B', which is a conjugate of B, such that $B' = B'_d B'_1$. Since B has order p, it follows that either $B \cong B'_d$ or $B \cong B'_1$. However, the matrices in B are not diagonalizable, and 1 is not a common eigenvalue so neither isomorphism can hold.

3. Ordinary good reduction

Let E be an elliptic curve defined over $\mathbb{Q}$, and let p be a prime such that $E/\mathbb{Q}$ has good reduction at p. Let us fix an embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Via ι, we may regard E as defined over $\mathbb{Q}_p$. We fix a minimal model of E over $\mathbb{Z}_p$ with good reduction, given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in \mathbb{Z} \subseteq \mathbb{Z}_p$. In particular, the discriminant Δ is a unit in $\mathbb{Z}_p$. Moreover, since $E/\mathbb{Z}_p$ has good reduction, we have an exact sequence

$$0 \to X_{p^n} \to E(\overline{\mathbb{Q}}_p)[p^n] \to \widetilde{E}(\overline{\mathbb{F}}_p)[p^n] \to 0,$$

where $\pi_n \colon E(\overline{\mathbb{Q}}_p)[p^n] \to \widetilde{E}(\overline{\mathbb{F}}_p)[p^n]$ is the homomorphism given by reduction modulo the maximal ideal of the ring of integers of $\overline{\mathbb{Q}}_p$, and X_{p^n} is the kernel of π_n (see [24], Ch. VII, Prop. 2.1).

From now on we assume that E has ordinary good reduction at a fixed prime p, i.e., the reduction of E mod p, denoted by $\widetilde{E}/\mathbb{F}_p$, is an elliptic curve and its Hasse invariant is non-zero. It follows that X_{p^n} and $\widetilde{E}(\overline{\mathbb{F}}_p)[p^n]$ are groups with p^n elements ([24], Ch. V, Thm. 3.1). The Galois group $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ fixes X_{p^n}. If we fix a $\mathbb{Z}/p^n\mathbb{Z}$-basis $\{P_n, Q_n\}$ of $E(\overline{\mathbb{Q}}_p)[p^n]$, such that $X_{p^n} = \langle P_n \rangle$, then $D_n = D_{p,n}$, the image of G_p in $\mathrm{Aut}(E[p^n]) = \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$, is a Borel subgroup, i.e.,

$$D_n \leq \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}.$$

Let $I \leq G_p$ be the inertia subgroup and let $I_n = I_{p,n}$ be the image of I in $\mathrm{Aut}(E[p^n]) \cong \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. Then, I acts on $\widetilde{E}(\overline{\mathbb{F}})[p^n]$ trivially (because I acts trivially on the residue field; see [24], Ch. VII, §4, or [18], Prop. 11, for details in the case when $n = 1$), and therefore I acts on X_{p^n} via $\chi_n \colon G_p \to (\mathbb{Z}/p^n\mathbb{Z})^\times$, the cyclotomic character modulo p^n, because the determinant of $\rho_{E,p^n} \colon G_p \to \mathrm{Aut}(E[p^n]) \cong \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is precisely χ_n. Thus,

$$I_n \leq \left\{ \begin{pmatrix} \chi_n & * \\ 0 & 1 \end{pmatrix} \right\}.$$

In what follows, we fix a prime $\overline{\Omega}$ of $\overline{\mathbb{Q}}$ over p, and let $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ be the embedding associated to $\overline{\Omega}$. Via ι, we may consider an elliptic curve $E/\mathbb{Q}$ as an elliptic curve defined over $\mathbb{Q}_p$. Let Ω be a prime of $\mathbb{Q}(E[p^n])$ lying under $\overline{\Omega}$, and let $D_{\Omega,n}$ and $I_{\Omega,n}$ be respectively the decomposition and inertia subgroups of $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q})$ associated to Ω. In this setting D_n, as above, can be identified with $D_{\Omega,n}$, and I_n is identified with $I_{\Omega,n}$.

Lemma 3.1. *If the decomposition group D_n is diagonalizable, then inertia I_n is diagonalizable. If $p > 2$, the converse is also true.*

Proof. One direction is trivial: if D_n is diagonalizable, then $I_n \leq D_n$ must be diagonalizable as well. Let us now suppose now that $p > 2$. By our remarks above, the decomposition group D_n is a Borel. Let us assume that I_n is diagonal, i.e., $I_n = \left\{\left(\begin{smallmatrix}\chi_n & 0\\ 0 & 1\end{smallmatrix}\right)\right\}$, with respect to a $\mathbb{Z}/p^n\mathbb{Z}$-basis $\{P_n, Q_n\}$ of $E[p^n]$. Let $D_{n,1}$ and $D_{n,d}$ be the subgroups of D_n defined as in Definition 2.1. Since $p > 2$ and since the cyclotomic character $\chi_n : I_n \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ is surjective (the base field here is $\mathbb{Q}_p$), there is a diagonal matrix $M = \left(\begin{smallmatrix}a & 0\\ 0 & 1\end{smallmatrix}\right)$ in $I_n \leq D_n$ with $a \not\equiv 1 \bmod p$. Hence, we can apply Lemma 2.2 with $B = D_n$, $g = M$, and $h = \mathrm{Id}$, and so $B = B' = D_n = D_{n,d}D_{n,1}$. Let L be the subfield of $\mathbb{Q}_p(E[p^n])$ fixed by $D_{n,1}$. It follows that $\mathrm{Gal}(\mathbb{Q}_p(E[p^n])/L) \cong D_{n,1}$, so the extension is cyclic, of degree p^s, for some $0 \leq s \leq n$, and it is unramified because $I_n \cap D_{n,1} = \{\mathrm{Id}\}$. Then, $\mathbb{Q}_p(E[p^n])/L$ is a finite unramified extension and, therefore, it is generated by a root of unity ζ of prime-to-p order ([8], p. 37). But, in this case, $\mathbb{Q}_p(E[p]) = L(\zeta)$ would be abelian over $\mathbb{Q}_p$. Since $\mathrm{Gal}(\mathbb{Q}_p(E[p])/\mathbb{Q}_p) \cong D_n$ and $D_{n,1}$ is the commutator subgroup of D_n, this is only possible if $D_{n,1}$ is trivial and $D_n = D_{n,d}$ is diagonalizable. $\square$

Remark 3.2. The converse part of Lemma 3.1 (i.e., if $p > 2$ and I_n is diagonalizable, then D_n is diagonalizable) is not used in the proof of our results, but we have included it here as it is interesting in itself.

Remark 3.3. The converse of the previous lemma is false for $p = 2$. For instance, let E be the curve with Cremona label "15a2", given by the model $y^2 + xy + y = x^3 + x^2 - 135x - 660$. The curve E has ordinary good reduction at $p = 2$. The 2-torsion of E is rational, so $\mathbb{Q}(E[2])/\mathbb{Q}$ is trivial and, therefore, $\mathbb{Q}_2(E[2])/\mathbb{Q}_2$ is trivial as well. Thus, $D_1 \cong \mathrm{Gal}(\mathbb{Q}_2(E[2])/\mathbb{Q}_2)$ and I_1 are trivially diagonalizable. However, even though D_2 is not, I_2 is diagonalizable.

The extension $\mathbb{Q}(E[4])/\mathbb{Q}$ is of degree 4, isomorphic to a subgroup of the linear group $\mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$ of the form

$$B = \left\{\begin{pmatrix} a & b\\ 0 & 1\end{pmatrix} : a \in (\mathbb{Z}/4\mathbb{Z})^\times,\ b \equiv 0 \bmod 2\right\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Thus, $K = \mathbb{Q}(E[4])$ is abelian over $\mathbb{Q}$ (see Remark 2.3) and, in fact, $K = \mathbb{Q}(i, \sqrt{5})$. Let $\mathcal{O}$ be the maximal order in $K = \mathbb{Q}(E[4])$. Since 2 remains prime in $\mathbb{Q}(\sqrt{5})$ and it ramifies in $\mathbb{Q}(i)$, it follows that $2\mathcal{O} = \wp^2$ is the square of a prime ideal $\wp$ of K above 2. Hence, $\mathbb{Q}_2(E[4])/\mathbb{Q}_2$ is also an extension of degree 4 (a ramified extension of degree 2 followed by an unramified extension also of degree 2), with Galois group $D_2 \cong B$ which is not diagonalizable. However, $I_2 \cong \left\{\left(\begin{smallmatrix}a & 0\\ 0 & 1\end{smallmatrix}\right) : a \in (\mathbb{Z}/4\mathbb{Z})^\times\right\}$ is diagonalizable.

Results of Serre ([22], A.2.4) and Lemma 3.1 show that, for $p > 2$, the inertia subgroup I_n is not diagonalizable for all $n \geq 1$ if and only if E is not a CM curve. We obtain:

Theorem 3.4. *Let $p > 2$. The following statements are equivalent:*

(1) *The elliptic curve E has CM (over an extension of $\mathbb{Q}_p$).*

(2) *The exact sequence*

$$0 \to X \to V_p(E) \to V_p(\widetilde{E}) \to 0$$

is split, where $X = (\varprojlim X_{p^n}) \otimes \mathbb{Q}_p$, and $V_p(E) = T_p(E) \otimes \mathbb{Q}_p$.

(3) *The decomposition subgroups $D_n \cong \mathrm{Gal}(\mathbb{Q}_p(E[p^n])/\mathbb{Q}_p)$ are diagonalizable for all $n \geq 1$.*

(4) *The inertia subgroups I_n are diagonalizable for all $n \geq 1$.*

Proof. The equivalence of (1), (2), and (3) is due to Serre. The equivalence between (3) and (4) follows from Lemma 3.1. □

Lemma 3.5. *Let $p > 2$ be a prime. Let $E/\mathbb{Q}$ be an elliptic curve with ordinary good reduction at p. With notation as above, suppose that I_m is diagonalizable but I_{m+1} is not, for some $m \geq 1$ (or $m = \infty$ if E has CM). Then there is a $\mathbb{Z}_p$-basis $\mathcal{B}$ of $T_p(E)$ such that the image of inertia, I, has the following structure:*

$$I = \left\{ \begin{pmatrix} \chi & b \\ 0 & 1 \end{pmatrix} : b \equiv 0 \bmod p^m \right\} \leq \mathrm{GL}(2, \mathbb{Z}_p),$$

where $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathbb{Z}_p^\times$ is the cyclotomic character.

Proof. By the remarks at the beginning of this section, we know that each I_n and $I = \varprojlim I_n$ are Borel subgroups of the form $\left\{\left(\begin{smallmatrix} \chi_m & * \\ 0 & 1 \end{smallmatrix}\right)\right\}$, with respect to some basis $\{P_n, Q_n\}$ of $E[p^n]$, respectively, where χ_m is the reduction of χ modulo p^m. Since $p > 2$ and χ_m is surjective, Lemma 2.2 implies the existence of a basis $\{P_n, Q'_n\}$ of $E[p^n]$ such that $I_n = (I_n)_d \cdot (I_n)_1$, where

$$(I_n)_d = \left\{ \begin{pmatrix} \chi_m & 0 \\ 0 & 1 \end{pmatrix} \right\}, \text{ and } (I_n)_1 = I_n \cap \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}.$$

Hence, if we put $P = (P_n)_{n=1}^\infty$ and $Q' = (Q'_n)_{n=1}^\infty \in T_p(E)$, then $\{P, Q'\}$ is a $\mathbb{Z}_p$-basis of $T_p(E)$ such that $I = (I)_d \cdot (I)_1$, where

$$(I)_d = \left\{ \begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix} \right\}, \text{ and } (I)_1 = I \cap \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}.$$

Since $(I)_1$ is an abelian subgroup of I, the top right coordinates of the matrices in $(I)_1$ form an additive subgroup H of $\mathbb{Z}_p$, say $H = p^t\mathbb{Z}_p$ for some $t \geq 0$. Thus,

$$(I)_1 = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in p^t\mathbb{Z}_p \right\}.$$

First, suppose that m is finite. Since $I_m \equiv I \bmod p^m$ is diagonalizable, we must have $t \geq m$, and since I_{m+1} is not diagonalizable, it follows $t = m$. This shows that

$$I = \left\{ \begin{pmatrix} \chi & b \\ 0 & 1 \end{pmatrix} : b \equiv 0 \bmod p^m \right\} \leq \mathrm{GL}(2, \mathbb{Z}_p),$$

as desired. If $m = \infty$, then t must be arbitrarily large, and so $b \in (0)$. □

The structure of the inertia subgroup described in the previous lemma has the following corollary on ramification indices.

Theorem 3.6. *Let $E/\mathbb{Q}$ be an elliptic curve without CM, and with ordinary good reduction at a prime p. If I_m is diagonalizable for some integer $m \geq 1$, then so is I_n for all integers $1 \leq n \leq m$. Moreover, if $p > 2$ and m is the largest integer such that I_m is diagonalizable, then the ramification index of p in the extension $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is given by $\varphi(p^n)$ if $1 \leq n \leq m$, and by $\varphi(p^n) \cdot p^{n-m}$ if $n > m$.*

Proof. Let Ω be a fixed prime of $\mathbb{Q}(E[p^n])$ above p. Suppose that there exists an integer n such that $I_n = I_n(\Omega|p)$ is diagonalizable, and let m be the largest such integer (a largest m exists by Theorem 3.4 because E does not have CM). Then, for every $1 \leq n \leq m$, there is a basis of $E[p^n]$ such that

$$I_n(\Omega|p) \cong \left\{ \begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix} \right\} \cong \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\} \leq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z}),$$

where $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ is the cyclotomic character (which is surjective). Since $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is Galois, the ramification index of any prime of $\mathbb{Q}(E[p^n])$ over p is the same, and it follows that the ramification index of p in $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is $\varphi(p^n)$ if $1 \leq n \leq m$, as claimed.

If $p > 2$, then Lemma 3.5 implies that the image of the inertia subgroup, $I_n(\Omega|p)$, is of the form

$$I_n(\Omega|p) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbb{Z}/p^n\mathbb{Z})^\times,\ b \equiv 0 \bmod p^m \right\} \leq \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z}).$$

Therefore, the ramification index of p in $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is $\varphi(p^n) \cdot p^{n-m}$ if $n \geq m$, as desired. □

4. Gross' criterion and canonical liftings

We now turn our attention to finding m such that I_m is diagonalizable, but I_{m+1} is not. A deep theorem of Gross provides the criterion we seek.

Theorem 4.1 (Gross; see [6], p. 514; see also §14-15). *Let p be a prime, and let $E/\mathbb{Q}$ be an elliptic curve with ordinary good reduction at p, with $j \neq 0, 1728$, and assume that $E[p]$ is an irreducible* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-module. Let $D_n \leq \mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}) \leq$ $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ be a decomposition group at p. Let $j_E = j(E)$ be the j-invariant* *of E and let j_0 be the j-invariant of the "canonical lifting" of the reduction of $j(E)$ modulo p, i.e., j_0 is the j-invariant of the unique elliptic curve $E_0/\mathbb{Q}_p$ which satisfies $E_0 \equiv E \bmod p$ and $\mathrm{End}_{\mathbb{Q}_p}(E_0) \equiv \mathrm{End}_{\mathbb{F}_p}(E)$. Then D_n is diagonalizable if and only if $j_E \equiv j_0 \bmod p^{n+1}$ if p is odd, and $j_E \equiv j_0 \bmod 2^{n+2}$ if $p = 2$.*

In order to use Gross' criterion (Theorem 4.1) we need to be able to calculate canonical liftings. In the rest of this section, we explain how to do so, and calculate a canonical lifting in several examples.

Theorem 4.2 (Deuring; see [15], §8). *Let $\mathbb{F}$ be a perfect field of characteristic $p > 0$, and let E be an elliptic curve with $j(E) \in \mathbb{F}$ and with Hasse invariant $\neq 0$ (i.e., having the maximum number of points of order p). Let $T_p(x, y)$ be the classical modular polynomial relating the j-invariants of elliptic curves that have isogenies of degree p between themselves. Let $W(\mathbb{F})$ be the ring of Witt vectors with coefficients in $\mathbb{F}$ and let $s : W(\mathbb{F}) \to W(\mathbb{F})$ be the Frobenius automorphism given by $(x_0, x_1, \dots) \to (x_0^p, x_1^p, \dots) \in W(\mathbb{F})$ in Witt vector coordinates. Then, there is a canonical lifting of $E/\mathbb{F}$ to $W(\mathbb{F})$, with j-invariant $j_0 \in W(\mathbb{F})$. Moreover,*

1. *one has $T_p(j_0, s(j_0)) = 0$ and $j_0 \equiv j(E) \bmod p$; and*
2. *if $j(E) \notin \mathbb{F}_{p^2}$, then there is a unique solution $j_0 \in W(\mathbb{F})$ with $T_p(j_0, s(j_0)) = 0$ and $j_0 \equiv j(E) \bmod p$.*

Corollary 4.3. *Let p be a prime and let $E/\mathbb{Q}$ be an elliptic curve with ordinary good reduction at p. Then, there is a canonical lifting of $E/\mathbb{F}_p$ to $\mathbb{Q}_p$, with j-invariant $j_0 \in \mathbb{Q}_p$. Moreover, j_0 satisfies $T_p(j_0, j_0) = 0$ and $j_0 \equiv j(E) \bmod p$.*

The proof of the corollary is clear, since $W(\mathbb{F}_p) = \mathbb{Q}_p$ and the Frobenius automorphism of Witt coordinates is the identity, as $x \mapsto x^p$ fixes $\mathbb{F}_p$.

Example 4.4. The classical modular polynomials $T_p(x, y)$ for $p = 2$ and 3 are given by

$$\begin{aligned}
T_2(x,y) &= x^3 - x^2y^2 + 1488x^2y - 162000x^2 + 1488xy^2 + 40773375xy \\
&\quad + 8748000000x + y^3 - 162000y^2 + 8748000000y - 157464000000000, \\
T_3(x,y) &= x^4 - x^3y^3 + 2232x^3y^2 - 1069956x^3y \\
&\quad + 36864000x^3 + 2232x^2y^3 + 2587918086x^2y^2 + 8900222976000x^2y \\
&\quad + 452984832000000x^2 - 1069956xy^3 + 8900222976000xy^2 \\
&\quad - 770845966336000000xy \\
&\quad + 1855425871872000000000x + y^4 + 36864000y^3 \\
&\quad + 452984832000000y^2 + 1855425871872000000000y,
\end{aligned}$$

and $T_2(x,x)$, $T_3(x,x)$ factor as

$$\begin{aligned} T_2(x,x) &= -x^4 + 2978x^3 + 40449375x^2 + 17496000000x - 157464000000000 \\ &= -(x-8000)(x-1728)(x+3375)^2. \\ T_3(x,x) &= -x^6 + 4464x^5 + 2585778176x^4 + 17800519680000x^3 \\ &\quad - 769939996672000000x^2 + 37108517437440000000000x \\ &= -x(x-54000)(x-8000)^2(x+32768)^2. \end{aligned}$$

Similarly, the polynomial $T_5(x,x)$ factors as

$$\begin{aligned} T_5(x,x) = (x-287496)^2 \cdot (x-1728)^2 \cdot (x+32768)^2 \cdot (x+884736)^2 \\ \cdot (x^2 - 1264000x - 681472000). \end{aligned}$$

Hence, if $E/\mathbb{Q}$ is an elliptic curve with ordinary good reduction at $p = 2$, 3, or 5, then the canonical lift of the reduction of E modulo p is the following:

- If $p = 2$ and $j(E) \equiv 1 \bmod 2$, then $j_0 = -3375 = -3^3 \cdot 5^3$.
- If $p = 3$, and $j(E) \equiv 1$ or $2 \bmod 3$, then $j_0 = -32768 = -2^{15}$ or $j_0 = 8000 = 2^6 \cdot 5^3$, respectively.
- If $p = 5$, and $j(E) \equiv 1, 2$ or $4 \bmod 5$, then $j_0 = 287496 = 2^3 3^3 11^3$, $j_0 = -32768 = -2^{15}$, or $j_0 = -884736 = -2^{15} \cdot 3^3$, respectively.

Example 4.5. Let $p = 37$. Let $T_{37}(x,y)$ be the classical modular polynomial, and put $f(x) = T_{37}(x,x) \in \mathbb{Z}[x]$. The degree of the polynomial $f(x)$ is 74 and it factors, over $\mathbb{Q}[x]$, as a product of 20 polynomials $f(x) = \prod_{i=1}^{20} p_i(x)^{m_i}$ of degree d_i and multiplicity m_i, as follows:

	1	2	3	4	5	6	7	8	9	10	11,...,16	17	18	19	20
d_i	1	1	1	1	1	1	1	1	1	2	2	3	4	4	4
m_i	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2

Notice that $f(x) \equiv -(x^{37} - x)^2 \bmod 37$. By the chart above, p_{10} is the only polynomial divisor of $f(x)$ whose multiplicity is not 2 over $\mathbb{Q}[x]$; however, $p_{10} \equiv (x-8)^2$ is a square over $(\mathbb{Z}/37\mathbb{Z})[x]$. It follows that there is a unique polynomial $p_i(x)$, for some $1 \le i \le 20$, such that one of the roots $j_0 \in \mathbb{Q}_{37}$ of $p_i(x)$ is congruent to 7 mod 37 (and j_0 is the unique root of $f(x)$ with this property). Indeed, direct computation reveals that the only polynomial $p_i(x)$ with 7 mod 37 as a root is $p_{20}(x)$. The polynomial $p_{20}(x)$ is given by

$$\begin{aligned} p_{20}(x) &= x^4 - 3196800946944x^3 - 5663679223085309952x^2 \\ &\quad + 88821246589810089394176x - 5133201653210986057826304 \\ &\equiv (x-2)(x-3)(x-7)(x-28) \bmod 37\mathbb{Z}[x], \end{aligned}$$

and its root $j_0 \in \mathbb{Q}_{37}$ has the following 37-adic expansion:

$$j_0 = \left(7,\ 266,\ 11218,\ 1632114 \bmod 37^4,\ 12877080 \bmod 37^5, \dots\right) \in \mathbb{Q}_{37}.$$

Example 4.6. In the table below, we list the first few primes ($p \leq 20$), together with those canonical lifts j_0 that are in $\mathbb{Z}_p$ (and not in some extension of $\mathbb{Z}_p$). If $j_0 \in \mathbb{Z}$, then we list the actual value of j_0 in the first line. If $j_0 \in \mathbb{Z}_p$, then we list a second (and third) line of values modulo p^5.

p	Canonical lifts
2	-3375, 1728, 8000
3	-32768, 0, 8000, 54000
5	-884736, -32768, 1728, 287496
7	-12288000, -884736, -3375, 0, 54000, 16581375, -7598, $2126 + O(7^5)$
11	-884736000, -884736, -32768, -3375, 8000, 16581375, 7665, 24243, 27342, 35982, $61340 + O(11^5)$
13	-884736000, -12288000, 0, 1728, 54000, 287496, -159805, -102235, -71051, 10643, 33871, $64521 + O(13^5)$
17	-147197952000, -884736000, -884736, 1728, 8000, 287496, -675116, -672317, -362937, -158485, $-126224 + O(17^5)$, -110190, 74802, 128731, $229973 + O(17^5)$
19	-147197952000, -12288000, -884736, 0, 8000, 54000 -752904, -695235, -605629, -570609, $-515098 + O(19^5)$, -118930, 318870, 414604, 526924, 710891, $1034963 + O(19^5)$, 1149479, $1187960 + O(19^5)$.

Question 4.7. In Gross' criterion (Theorem 4.1), it is assumed that $E[p]$ is an irreducible Galois module. Is this hypothesis necessary? I.e., suppose $E/\mathbb{Q}$ is ordinary good at $p > 2$, but $E[p]$ is reducible. Does Gross' criterion still work in this case? Indeed, we have verified that the criterion holds in many examples where $E[p]$ is reducible.

For instance, let $E/\mathbb{Q}$ be the curve with j-invariant $j(E) = -122023936/161051$ and Cremona label 11a1, given by a Weierstrass model

$$E : y^2 + y = x^3 - x^2 - 10x - 20.$$

The curve E has ordinary good reduction at $p = 5$, however, there is a 5-torsion point defined over $\mathbb{Q}$, namely $P = (16, 60)$. Hence, $\rho_{E,p}$ is reducible. Nonetheless,

$$j(E) = -122023936/161051 \equiv 14 \equiv -884736 \bmod 25,$$

where $j_0 = -884736$ is the canonical lift of $4 \in \mathbb{F}_5$. In particular, (if $E[5]$ was irreducible, then) Gross' criterion would imply that $\mathbb{Q}(E[5])/\mathbb{Q}(\zeta_5)$ is unramified at the prime above 5. This conclusion is indeed true because the extension is trivial, i.e., $\mathbb{Q}(E[5]) = \mathbb{Q}(\zeta_5)$ where $E[5]$ is generated by the 5-torsion points $P = (16, 60)$ and $Q = (4\zeta_5^3 + 2\zeta_5^2 + 3\zeta_5 + 2, 3\zeta_5^3 - 4\zeta_5^2 + 5\zeta_5)$.

5. Curves with minimal ramification at p

We begin with a summary of the definitions and the precise statement of Hilbert's irreducibility theorem (see [13], Chapter 9) that we will use in the proof of Theorem 5.4 (see [23], Chapter 3, for another flavor of Hilbert's irreducibility).

Definition 5.1 ([13], Ch. 9). Let K be a field of characteristic 0, and suppose that $f(t_1,\dots,t_r,X_1,\dots,X_s) = f(\mathbf{t},\mathbf{X}) \in K(\mathbf{t})[\mathbf{X}]$ is a polynomial in $X_1,\dots,X_s$ with coefficients in $K(\mathbf{t})$ which is irreducible as a polynomial in $\mathbf{X}$ variables. A *basic Hilbert set* is a subset $U_{f,K}$ of the affine space $\mathbb{A}^r(K)$ consisting of those points $\mathbf{t}' = (t_1',\dots,t_r') \in K^r$ at which the coefficients of f are defined, and such that $f(\mathbf{t}',\mathbf{X})$ is irreducible in $K[\mathbf{X}]$ over K. A *Hilbert subset* of $\mathbb{A}^r(K)$ is a set defined as the intersection of a finite number of basic Hilbert sets with a finite number of non-empty Zariski open subsets of $\mathbb{A}^r(K)$. A field K is called *hilbertian* if the Hilbert subsets of $\mathbb{A}^r(K)$ are not empty (and thus are infinite).

Theorem 5.2 ([13], Ch. 9). *A number field is hilbertian.*

Theorem 5.3 ([13], Ch. 9, Corollary 2.5). *A Hilbert subset of $\mathbb{Q}$ is dense for the ordinary topology and every p-adic topology on $\mathbb{Q}$.*

We are now ready to prove the first part of Theorem 1.1.

Theorem 5.4. *For every prime p and every $n \geq 1$, and for every ordinary j-invariant $\lambda \in \mathbb{F}_p$, with $\lambda \not\equiv 0, 1728 \bmod p$, there are infinitely many non isomorphic, non-CM, elliptic curves E, defined over $\mathbb{Q}$, with $j(E) \equiv \lambda \bmod p$ (and with ordinary good reduction at p) such that the ramification index of p in the extension $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is exactly $\varphi(p^n)$, and $E[p]$ is an irreducible $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. In particular, $\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n})$ is unramified at p.*

Proof. Let p be a fixed prime, and let U be the subset of $\mathbb{Q}$ formed by those j-invariants $\iota_0 \in \mathbb{Q}$ such that if $E/\mathbb{Q}$ is an elliptic curve with $j(E) = \iota_0$, then $E[p]$ is an irreducible $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. We claim that U contains a Hilbert set $V \subseteq U$. Indeed, if $E[p]$ is reducible, then $j(E)$ gives rise to a non-cuspidal rational point on the modular curve $X_0(p)$. We distinguish two cases:

- If $X_0(p)$ is a curve of genus ≥ 1 and $X_0(p)(\mathbb{Q})$ is non-empty, then Mazur's theorem on isogenies of prime degree ([16]) says that p is a prime in the list $11, 17, 19, 37, 43, 67, 163$, but in all these cases $X_0(p)(\mathbb{Q})$ has only finitely many points (see for example Section 9 and Table 4 of [14]). Hence, there are at most finitely many exceptions in $\iota_0 \in \mathbb{Q}$ such that $E[p]$ is reducible. Hence $V = U$ is a non-empty Zariski open set of $\mathbb{Q}$, and therefore a Hilbert set.
- If $X_0(p)$ is a curve of genus 0, then the set of j-invariants of elliptic curves over $\mathbb{Q}$ with $E[p]$ reducible is given by a one parameter family
$$S_{\mathrm{red},p} = \{\phi_p(h) : h \in \mathbb{Q}\}$$
where $\phi_p(h)$ is a rational function of degree ≥ 3 (see [14], Section 9, for the explicit rational function ϕ_p). Let $\phi_p(h) = u_p(h)/v_p(h)$, where u_p and v_p are relatively prime polynomials in $\mathbb{Q}[h]$. Then, $\iota_0 \in \mathbb{Q}$ is in U if and only if $\phi_p(h) = \iota_0$ has no root $h_0 \in \mathbb{Q}$ or, equivalently, if $u_p(h) - \iota_0 \cdot v_p(h) = 0$ has no root $h_0 \in \mathbb{Q}$. If we put $f_p(j,x) = u_p(x) - j v_p(x)$, then the basic Hilbert set $V = U_{f_p,\mathbb{Q}}$ is contained in U, since $\iota_0 \in U_{f_p,\mathbb{Q}}$ implies that $f_p(\iota_0, x)$ is irreducible over $\mathbb{Q}$, and therefore has no rational roots $x_0 \in \mathbb{Q}$.

Therefore, in all cases U contains a Hilbert set.

Let $\lambda \in \mathbb{F}_p$ be a fixed ordinary j-invariant, with $\lambda \not\equiv 0$ or $1728 \bmod p$. Notice that there is always at least one such ordinary j-invariant λ in $\mathbb{F}_p$: if $p = 2$, then $\lambda = 1$; if $p = 3$, we may pick $\lambda \equiv 1$ or $2 \bmod 3$; if $p = 5$, we may pick $\lambda \equiv 1, 2$ or $4 \bmod 5$; if $p > 5$, there are at least $p - ([p/12] + \varepsilon_p) \geq 11p/12 - 2 \geq 11 \cdot 7/12 - 2 \geq 4$ ordinary j-invariants in $\mathbb{F}_p$, where $\varepsilon_p = 0, 1, 1, 2$ if $p \equiv 1, 5, 7, 11 \bmod 12$, respectively (see [24], Ch. V, Theorem 4.1.(c)), so at least one of them is $\not\equiv 0$ or $1728 \bmod p$.

Let $E_0/\mathbb{Q}_p$ be the unique canonical lift to $\mathbb{Q}_p$ with j-invariant $j_0 = j(E_0) \equiv \lambda$ modulo p, and define

$$C_{\lambda,n} = \left\{ j \in \mathbb{Q} \cap \mathbb{Z}_p \ : \ j \equiv j_0 \bmod p^{n+1} \right\}$$

for $p > 2$, and $C_{\lambda,n} = \{ j \in \mathbb{Q} \cap \mathbb{Z}_2 : j \equiv j_0 \bmod 2^{n+2} \}$ when $p = 2$. By Theorem 5.2, the field $\mathbb{Q}$ is hilbertian and, by Theorem 5.3, the Hilbert set $V \subseteq U$ is dense for the p-adic topology. Since $C_{\lambda,n}$ is an open set p-adically, it follows that $C_{\lambda,n} \cap V$ is infinite and contained in U. Moreover, there are only 13 rational CM j-invariants (see [25], Appendix A, §3). Hence, the set $H_{\lambda,n}$ of j-invariants with $j \equiv j_0 \bmod p^{n+1}$ (with $j \equiv j_0 \bmod 2^{n+2}$ when $p = 2$), such that $E[p]$ is irreducible, and such that j has no complex multiplication, is infinite.

For each $j \in H_{\lambda,n}$ let E be the curve given by the Weierstrass equation

$$E : y^2 + (j - 1728)xy = x^3 - 36(j - 1728)^3 x - (j - 1728)^5$$

with j-invariant $j(E) = j$ and discriminant $\Delta_n = j^2(j - 1728)^9$. Since $j \equiv j_0 \equiv \lambda \bmod p$, and λ was chosen so that $\lambda \not\equiv 0, 1728 \bmod p$, it follows that $\Delta \in \mathbb{F}_p^\times$ and, in particular, $\Delta \neq 0$. Thus, $E/\mathbb{Q}$ is an elliptic curve with good reduction at p. Since $j(E) = j \equiv \lambda \bmod p$, and $\lambda \in \mathbb{F}_p$ is an ordinary j-invariant, we conclude that E has ordinary good reduction at p. Since $j \in H_{\lambda,n}$, the curve E is not a CM curve. Finally, $j(E) = j \equiv j_0 \bmod p^{n+1}$ if $p > 2$, and $j(E) \equiv j_0 \bmod 2^{n+2}$ if $p = 2$. Since $E[p]$ is an irreducible $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module, then by Theorem 4.1 the decomposition group D_n is diagonalizable, hence I_n is diagonalizable by Lemma 3.1. Therefore, we have $m \geq n$ in Theorem 3.6, and the ramification index in $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is exactly $\varphi(p^n)$, as claimed.

Hence, we have shown the existence of infinitely many non-isomorphic, non-CM curves, as in the statement of the theorem, one for each j in the infinite set $H_{\lambda,n}$. □

6. Examples

In the following examples we follow the recipe in the proof of Theorem 5.4 to find elliptic curves such that the ramification of p in $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is precisely $\varphi(p^n)$.

Example 6.1. Let $p = 2$, and let $\lambda = 1$. In Example 4.4 we have calculated the canonical lifting of λ, and it is $j_0 = -3375$. Now we can take $j_{n,k} = -3375 + 2^{n+2} \cdot k$, for each $n \geq 1$ and $k \geq 1$, and let $E_{n,k}$ be a curve with $j(E_{n,k}) = j_{n,k}$ given by a Weierstrass model as in the proof of 5.4, with discriminant $\Delta_{n,k} = j_{n,k}^2 (j_{n,k} - 1728)^9$. The curve $X_0(2)$ is of genus 0, and the function

$\phi_2(h) = (h+16)^3/h$ (see [14], Section 9). Let us define

$$f_2(j,x) = (x+16)^3 - j\cdot x = x^3 + 28x^2 + (768-j)x + 4096.$$

It follows that if $f_2(j_{n,k},x) \in \mathbb{Q}[x]$ has no rational roots $x \in \mathbb{Q}$, then $E_{n,k}[2]$ is irreducible, and therefore the ramification of any prime ideal above 2 in $\mathbb{Q}(E_{n,k}[2^n])/\mathbb{Q}$ will be precisely $\varphi(2^n)$. Using the software Magma, we have verified that, indeed, $f_2(j_{n,k},x)$ is irreducible over $\mathbb{Q}[x]$ for all $1 \leq n \leq 100$ and all $1 \leq k \leq 100$, and none of the j-invariants $j_{n,k}$ in this range has CM.

Example 6.2. Let $p = 3$, and let $\lambda = 2$. In Example 4.4 we have calculated that the canonical lifting of λ is $j_0 = 8000$. Now we can take $j_{n,k} = 8000 + 3^{n+1}\cdot k$, for each $n \geq 1$ and $k \geq 1$, and let $E_{n,k}$ be a curve with $j(E_{n,k}) = j_{n,k}$, and discriminant $\Delta_{n,k} = j_{n,k}^2(j_{n,k} - 1728)^9$. The curve $X_0(3)$ is of genus 0, and the function $\phi_3(h) = (h+27)(h+3)^3/h$. Let us define

$$f_3(j,x) = (x+27)(x+3)^3 - j\cdot x.$$

It follows that if $f_3(j_{n,k},x) \in \mathbb{Q}[x]$ has no rational roots $x \in \mathbb{Q}$, then $E_{n,k}[3]$ is irreducible, and therefore the ramification of any prime ideal above 3 in $\mathbb{Q}(E_{n,k}[3^n])/\mathbb{Q}$ will be precisely $\varphi(3^n)$. Using the software Magma, we have verified that, indeed, $f_3(j_{n,k},x)$ is irreducible over $\mathbb{Q}[x]$ for all $1 \leq n \leq 100$ and all $1 \leq k \leq 100$, and none of the j-invariants in this range has CM.

Example 6.3. Let $p = 5$, and let $\lambda = 2$. In Example 4.4 we have calculated that the canonical lifting of λ is $j_0 = -32768$. Now we can take $j_{n,k} = -32768 + 5^{n+1}\cdot k$, for each $n \geq 1$ and $k \geq 1$, and let $E_{n,k}$ be a curve with $j(E_{n,k}) = j_{n,k}$, and discriminant $\Delta_{n,k} = j_{n,k}^2(j_{n,k} - 1728)^9$. The curve $X_0(5)$ is of genus 0, and the function $\phi_5(h) = (h^2+10h+5)^3/h$. Let us define

$$f_5(j,x) = (x^2+10x+5)^3 - j\cdot x.$$

It follows that if $f_5(j_{n,k},x) \in \mathbb{Q}[x]$ has no rational roots $x \in \mathbb{Q}$, then $E_{n,k}[5]$ is irreducible, and therefore the ramification of any prime ideal above 5 in $\mathbb{Q}(E_{n,k}[5^n])/\mathbb{Q}$ will be precisely $\varphi(5^n)$. Using the software Magma, we have verified that, indeed, $f_5(j_{n,k},x)$ is irreducible over $\mathbb{Q}[x]$ for all $1 \leq n \leq 100$ and all $1 \leq k \leq 100$, and none of the j-invariants in this range has CM.

Example 6.4. Let $p = 37$, and let $\lambda = 7$. In Example 4.5 we have calculated that the canonical lifting of λ is $j_0 \in \mathbb{Q}_{37}$, with the following 37-adic expansion:

$$j_0 = \left(7,\ 266,\ 11218,\ 1632114 \bmod 37^4,\ 12877080 \bmod 37^5, \ldots\right) \in \mathbb{Q}_{37}.$$

Let α_n be a positive integer congruent to $j_0 \bmod 37^{n+1}$, e.g., $\alpha_1 = 266$, $\alpha_2 = 11218$, $\alpha_3 = 1632114$, etc. Now we take $j_{n,k} = \alpha_n + 37^{n+1}k$, for each $n \geq 1$ and $k \geq 1$, and let $E_{n,k}$ be a curve with $j(E_{n,k}) = j_{n,k}$, and discriminant $\Delta_{n,k} = j_{n,k}^2(j_{n,k} - 1728)^9$. The curve $X_0(37)$ is of genus 2, and it has only two rational non-cuspidal points, which correspond to the j-invariants $j_1 = -7\cdot 11^3$ and $j_2 = -7\cdot 137^3\cdot 2083^3$.

It follows that if $j_{n,k} \neq j_1$ or j_2, then $E_{n,k}[37]$ is irreducible, and therefore the ramification of any prime ideal above 37 in $\mathbb{Q}(E_{n,k}[37^n])/\mathbb{Q}$ will be precisely $\varphi(37^n)$. Since $j_{n,k}$ is always positive, and $j_1, j_2 < 0$, it follows that $j_{n,k} \neq j_1$ or j_2, for all $k \geq 0$, and all $n \geq 1$, and the ramification properties we seek actually hold for all curves $E_{n,k}$. Moreover, the only positive CM j-invariants are $\equiv 0, 6, 8, 10, 26, 33 \bmod 37$. Since none of them is $\equiv 7 \bmod 37$, we conclude that none of the $j_{n,k}$ have complex multiplication.

7. SL$_2$ extensions of cyclotomic fields

In this section we are interested to construct examples of $\mathrm{SL}(2, \mathbb{Z}/p^n\mathbb{Z})$ extensions of $\mathbb{Q}(\zeta_{p^n})$, that are unramified at primes above p.

Example 7.1. Let $p = 37$, as in the previous example, and consider the curve

$$E : y^2 = x^3 + x^2 + 17317393168x - 2056380789861728,$$

with j-invariant $j(E) = 266$ and ordinary good reduction at $p = 37$. Since 266 is not one of 13 rational CM j-invariants (see [25], Appendix A, §3), it follows that E is not a CM curve. Since $j(E) = 266$ is not one of two rational non-cuspidal points of $X_0(37)$, it follows that $E[37]$ is irreducible as a Galois module. Hence, Theorem 4.1 and Theorem 3.6 show that the ramification of any prime ideal above 37 in $\mathbb{Q}(E[37])/\mathbb{Q}$ is precisely $\varphi(37) = 36$. Since $\mathbb{Q}(\zeta_{37}) \subset \mathbb{Q}(E[37])$, it follows that $\mathbb{Q}(E[37])/\mathbb{Q}(\zeta_{37})$ is unramified at all the prime ideals above 37.

Let $\rho_{E,37} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/37\mathbb{Z})$ be the Galois representation associated to the natural action of Galois on $E[37]$. Using Proposition 19 of [18], one can verify that, in fact, $\rho_{E,37}$ is surjective (Serre's criterion is also implemented in the software package Sage). Hence, $\mathrm{Gal}(\mathbb{Q}(E[37])/\mathbb{Q}) \cong \mathrm{GL}(2, \mathbb{Z}/37\mathbb{Z})$, and $\mathrm{Gal}(\mathbb{Q}(E[37])/\mathbb{Q}(\zeta_{37})) \cong \mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$, because the determinant of $\rho_{E,37}$ is χ, the cyclotomic character. Hence, $\mathbb{Q}(E[37])$ is a Galois extension of $\mathbb{Q}(\zeta_{37})$, with Galois group $\mathrm{SL}(2, \mathbb{Z}/37\mathbb{Z})$, and unramified at the prime ideal above 37.

Notice, however, that the conductor of E is $N_E = 2^3 \cdot 7^2 \cdot 17^2 \cdot 19^2 \cdot 43^2$. By the criterion of Néron, Ogg, and Shafarevich, the extension $\mathbb{Q}(E[37])/\mathbb{Q}(\zeta_{37})$ may be ramified at primes above 2, 7, 17, 19, and 43.

Theorem 7.2 (Serre, [18], §2; [20], Lemme 18; Mazur, [16]). *Let $E/\mathbb{Q}$ be an elliptic curve. 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* $\mathrm{GL}(E[p])$*; or*

(2) *G is contained in the normalizer of a non-split Cartan subgroup of* $\mathrm{GL}(E[p])$*; 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* $\mathrm{GL}(E[p])$.

Moreover, option (3) *can only happen for $p \leq 13$, and option* (4) *can only happen for $p \leq 163$.*

Mazur [16] has shown that option (4) can only happen if $p \leq 163$, and $p \leq 37$ if E does not have CM. Building on [1] and some recent work of Gaudron and Rémond [7], the collaborators Bilu, Parent and Rebolledo [2] have shown the following result on curves whose image is of split Cartan type.

Theorem 7.3 (Bilu, Parent, Rebolledo, [2]). *Let $p \geq 11$, with $p \neq 13$, be a prime number. 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 $K/\mathbb{Q}$.*

As a corollary of the two previous theorems, and our Theorem 5.4, we obtain infinitely many examples of the SL_2 extensions we want.

Theorem 7.4. *For every prime $p \geq 17$ and every $n \geq 1$, and for every ordinary j-invariant $\lambda \in \mathbb{F}_p$, with $\lambda \not\equiv 0, 1728 \bmod p$, there are infinitely many non-isomorphic, non-CM, elliptic curves E, defined over $\mathbb{Q}$, with $j(E) \equiv \lambda \bmod p$ (and with ordinary good reduction at p) such that the ramification index of p in the extension $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is exactly $\varphi(p^n)$, and $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n})) \cong \mathrm{SL}(2, \mathbb{Z}/p^n\mathbb{Z})$. In particular, $\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n})$ is a $\mathrm{SL}(2, \mathbb{Z}/p^n\mathbb{Z})$ extension, unramified at primes above p.*

Proof. Let $p \geq 17$ be a prime, let $n \geq 1$ be fixed, and let $\lambda \in \mathbb{F}_p$ be an ordinary j-invariant with $j \not\equiv 0, 1728 \bmod p$. Let E be one of the infinitely many non-isomorphic, non-CM elliptic curves whose existence is proven by Theorem 5.4, and let G be the image of the representation $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$. If $G \neq \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$, then G falls in one of the four possibilities of Theorem 7.2:

(1) If G is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}(E[p])$, and $p \geq 17$, then Theorem 7.3 implies that E is CM. However, E as in Theorem 5.4 is not CM.

(2) Suppose G is contained in the normalizer of a non-split Cartan subgroup of $\mathrm{GL}(E[p])$. This case is impossible, because with respect to a certain basis, G contains the image of $I_1(\Omega|p)$, the inertia sugroup of Ω over p in $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$, which is a semi-split Cartan subgroup of the form

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in (\mathbb{Z}/p\mathbb{Z})^{\times} \right\}.$$

However, a normalizer of a non-split Cartan subgroup cannot contain a semi-split Cartan.

(3) If the projective image of G in $\mathrm{PGL}(E[p])$ is isomorphic to A_4, S_4 or A_5, then $p \leq 13$, but we have assumed that $p \geq 17$.

(4) If G is contained in a Borel subgroup of $\mathrm{GL}(E[p])$, then $E[p]$ is not irreducible, but the curves E were chosen so that the p-torsion was an irreducible Galois module, so that we could apply Gross' criterion.

Hence, the only possibility is that $G = \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$. Since $p \geq 17 \geq 5$, and our curves are defined over $\mathbb{Q}$, we can use [22], IV-23, Lemma 3, to conclude that $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is also surjective (in fact, the representation is surjective p-adically). Therefore, $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}) \cong \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$, and $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n})) \cong \mathrm{SL}(2, \mathbb{Z}/p^n\mathbb{Z})$. Moreover, $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n}))$ is unramified at primes above p by Theorem 5.4, and this concludes the proof of the theorem. □

Example 7.5. For each $n \geq 1$ and each $k \geq 1$, let $E_{n,k}/\mathbb{Q}$ be the elliptic curves described in Example 6.4. Then, these curves are non-isomorphic, non-CM, defined over $\mathbb{Q}$, with $j(E) \equiv 7 \bmod 37$ (and with ordinary good reduction at 37) such that the ramification index of 37 in the extension $\mathbb{Q}(E[37^n])/\mathbb{Q}$ is exactly $\varphi(37^n)$, and $E[37]$ is an irreducible $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. Hence, by the same argument as in the proof of Theorem 7.4, we conclude that $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n})) \cong \mathrm{SL}(2, \mathbb{Z}/p^n\mathbb{Z})$.

8. Ramification away from *p*

The goal of this section is to show that if $E/\mathbb{Q}$ is an elliptic curve such that the Galois representation on the p-torsion $\overline{\rho}_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[p])$ is absolutely irreducible, then the extension $\mathbb{Q}(E[p^n])$ over $\mathbb{Q}(\zeta_{p^n})$ has to ramify at some non-archimedian prime away from p. Later on, in the last part of this section, we will show examples of elliptic curves where the extension $\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n})$ is ramified above a single prime $q \neq p$. In order to show Theorem 1.2, we shall use Serre's modularity conjecture, which is now a theorem of Khare and Winterberger. Here, however, we only need the so-called level 1 case, which was shown independently by Dieulefait, and Khare.

Theorem 8.1 (Serre's modularity conjecture, [21], [9], [5], [10], [11]). *Let p be a prime, let $\mathbb{F}$ be a finite field of characteristic p, and let $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{F})$ be a continuous, absolutely irreducible, two-dimensional, odd (i.e., $\det(\overline{\rho}(\tau)) = -1$ for any complex conjugation τ) Galois representation. Let $k(\overline{\rho})$ be its optimal weight (as defined in [21]) and suppose that $N(\overline{\rho})$, the (prime-to-p) Artin conductor of $\overline{\rho}$, is identically 1. Then, $\overline{\rho}$ arises from $S_{k(\overline{\rho})}(\mathrm{SL}_2(\mathbb{Z}))$, i.e., there is a cusp form $f \in S_{k(\overline{\rho})}(\mathrm{SL}_2(\mathbb{Z}))$ and an integral model $\rho_f \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathcal{O})$ of its associated p-adic Galois representation, with $\mathcal{O}$ the ring of integers of a finite extension of $\mathbb{Q}_p$, such that the reduction of ρ_f modulo the maximal ideal of $\mathcal{O}$ is isomorphic to $\overline{\rho}$.*

Before we prove our theorem, we remind the reader about the definition of the Artin conductor of a representation, following [21], Section 1.2. Let V be a 2-dimensional vector space over $\overline{\mathbb{F}}_p$ and let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V)$ be a continuous Galois representation. Then, the Artin conductor of ρ is defined as

$$N = \prod_{\ell \neq p} \ell^{n(\ell,\rho)},$$

where $n(\ell,\rho) \geq 0$ are non-negative integers defined as follows. For each prime number $\ell \neq p$, let ν be an extension to $\overline{\mathbb{Q}}$ of the ℓ-adic valuation of $\mathbb{Q}$, and let

$$G_0 \supset G_1 \supset \cdots \supset G_i \supset \cdots$$

be the (higher) ramification groups of G with respect to ν. Let V_i be the subspace of V whose elements are fixed by G_i, and define

$$n(\ell,p) = \sum_{i=0}^{\infty} \frac{1}{[G_0 : G_i]} \dim V/V_i.$$

It is worth noting that:

1. $n(\ell,\rho) = 0$ if and only if $G_0 = \{1\}$, i.e., if and only if ρ is unramified at ℓ, and
2. $n(\ell,\rho) = \dim V/V_0$ if and only if $G_1 = \{1\}$, i.e., if and only if ρ is tamely ramified at ℓ.

We also need to recall some facts about the optimal weight $k(\overline{\rho})$, which is defined in [21], §2. In particular, we need the following result.

Proposition 8.2 (Serre, [21], §2.9, Prop. 5). *Let p be a prime, let $E/\mathbb{Q}_p$ be an elliptic curve, and let $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}(2,\mathbb{F}_p)$ be the representation attached to the natural action of Galois on the p-torsion $E[p]$ of E. Then,*

(1) *if $E/\mathbb{Q}_p$ has good reduction, then $k(\overline{\rho}) = 2$;*

(2) *if $E/\mathbb{Q}_p$ has multiplicative reduction, then $k(\overline{\rho}) = 2$ if $\nu_p(j(E))$ is divisible by p, and $k(\overline{\rho}) = p+1$ otherwise.*

We are now ready to prove Theorem 1.2. The idea of the proof is due to Robert Pollack.

Proof of Theorem 1.2. Let $E/\mathbb{Q}$ be an elliptic curve such that the Galois representation on the p-torsion $\overline{\rho}_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[p])$ is absolutely irreducible, and with either good reduction at p, or with multiplicative reduction at p and $\nu_p(j(E))$ divisible by p. Suppose for a contradiction that the extension $\mathbb{Q}(E[p^n])$ over $\mathbb{Q}(\zeta_{p^n})$ is unramified at all primes not above p. Then, the extension $\mathbb{Q}(E[p])/\mathbb{Q}(\zeta_p)$ is also unramified at all primes not above p, because of the multiplicativity of ramification indices in towers, and because $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}(\zeta_p)$ is only ramified above p.

Now, let $\overline{\rho}_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[p]) \cong \mathrm{GL}(2,\mathbb{F}_p)$ be the representation associated to the natural Galois action on $E[p]$. This representation is continuous, absolutely irreducible (by assumption), and odd (see, for instance, [17], Section 1.1.2). By our assumptions on the reduction type of E and Proposition 8.2, its weight is $k(\overline{\rho}_E) = 2$. Moreover, we have shown that $\mathbb{Q}(E[p])/\mathbb{Q}$ is only ramified above p and, thus, $\overline{\rho}_E$ is unramified outside p. It follows from our remarks above on the Artin conductor that $N(\overline{\rho}_E) = 1$. Hence, Theorem 8.1 implies that $\overline{\rho}_E$ arises from $S_2(\mathrm{SL}_2(\mathbb{Z}))$. However, $S_2(\mathrm{SL}_2(\mathbb{Z})) = \{0\}$ by Theorem 3.5.2 of [4] so this is impossible. □

We remark that if $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}(2,\mathbb{F}_p)$, then the Galois representation $\overline{\rho}_E$ is absolutely irreducible, therefore satisfying the hypothesis of Theorem 1.2. It follows that if $E/\mathbb{Q}$ has good reduction at p, and $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}(2,\mathbb{F}_p)$, then $\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_{p^n})$ must ramify (at least) at some prime above a rational prime $q \neq p$. In the rest of this section, we find examples where the ramification happens exactly at primes above one single rational prime $q \neq p$.

Theorem 8.3 (Kida, [12], Theorems 1.1 and 1.2). *Let q and $p \geq 2$ be distinct primes. Let $E/\mathbb{Q}$ be an elliptic curve. Then:*

(1) *The extension $\mathbb{Q}(E[p])/\mathbb{Q}$ is unramified at the primes above q if and only if $E/\mathbb{Q}$ has (a) good reduction at q, or (b) multiplicative reduction at q and $\nu_p(-\nu_q(j(E)))$ is a positive integer.*

(2) *Assume that $\mathbb{Q}(E[p])/\mathbb{Q}$ is unramified at q, and $E/\mathbb{Q}$ has multiplicative reduction at q. Then, $\mathbb{Q}(E[p^n])/\mathbb{Q}$ is unramified if and only if $1 \leq n \leq \nu_p(-\nu_q(j(E)))$.*

Example 8.4. Let $E/\mathbb{Q}$ be the curve with Cremona label 11a1. We saw in Question 4.7 that $\mathbb{Q}(E[5]) = \mathbb{Q}(\zeta_5)$, and therefore the extension $\mathbb{Q}(E[5])/\mathbb{Q}(\zeta_5)$ is trivially unramified at 5. Note however that E has bad reduction at 11, and $\mathbb{Q}(E[5])/\mathbb{Q}$ is unramified at 11. Kida's Theorem 8.3 says that the bad reduction at 11 must be multiplicative, and $\nu_5(-\nu_{11}(j(E)))$ must be positive. Indeed, the reduction is bad multiplicative ($\Delta = -11^5$, $c_4 = 2^4 \cdot 31$) and

$$j(E) = -\frac{122023936}{161051} = -\frac{2^{12}\cdot 31^3}{11^5},$$

and so $\nu_5(-\nu_{11}(j(E))) = 1 > 0$.

Example 8.5. In this example we find primes p, integers $n \geq 1$, and elliptic curves $E/\mathbb{Q}$ such that $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q}) \cong \mathrm{GL}(2,\mathbb{Z}/p^n\mathbb{Z})$ and such that $\mathbb{Q}(E[p^n])/\mathbb{Q}(\zeta_p^n)$ is unramified at primes above p, and only ramified at primes above at most one prime $q \neq p$. In order to find such examples, it suffices to find elliptic curves with the following properties:

(a) $E/\mathbb{Q}$ with ordinary good reduction at p;

(b) if $j(E) \equiv \lambda \in \mathbb{F}_p$, and j_0 is the canonical lift of λ, then $j(E) \equiv j_0 \bmod p^{n+1}$ if p is odd (and mod 2^{n+2} for $p = 2$);

(c) the representation $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2,\mathbb{Z}/p^n\mathbb{Z})$ must be surjective (one can be verify with Sage whether $\overline{\rho}_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2,\mathbb{F}_p)$ is surjective; if $p \geq 5$, then $\overline{\rho}_{E,p}$ is surjective if and only if $\rho_{E,p}$ is surjective);

(d) there is at most one prime of additive reduction q; and (e) every prime ℓ of multiplicative reduction satisfies $1 \leq n \leq \nu_p(-\nu_\ell(j(E)))$.

For instance, let $p = 5$, and let $E/\mathbb{Q}$ be the curve with Cremona reference "61a1" and j-invariant $j = -912673/61$, given by the model

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

The curve $E/\mathbb{Q}$ has bad multiplicative reduction at 61 (with Kodaira symbol I1), and good reduction elsewhere. Note that $j \equiv 7 \equiv -32768 \equiv j_0 \bmod 25$, where

$j_0 = -32768$ is the canonical lift of $\lambda = 2 \in \mathbb{F}_5$. With the help of Sage, we have verified that $\rho_{E,5} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{F}_5)$ is surjective. Finally, notice that there is only one prime of bad reduction, namely $q = 61$. Hence, all the necessary hypotheses are met, and $\mathbb{Q}(E[5])/\mathbb{Q}(\zeta_5)$ is a $\mathrm{SL}(2, \mathbb{F}_5)$ extension that is only ramified at primes above a unique rational prime, namely $q = 61$.

In the following table we give a few examples we have found using Cremona's tables (all curves with conductor ≤ 300000, a total of 1887909 curves) of primes p, integers $n \geq 1$, and curves $E/\mathbb{Q}$ with j-invariant $j(E)$ that verify conditions (a) through (e) as above. In all examples we have verified that $\overline{\rho}_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{F}_p)$ is surjective (with Sage). If $p \geq 5$, then the Galois representation $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is also surjective. In all cases, the Kodaira symbol at q is I1.

p	n	j_0	$j(E)$	Cremona	q
2	8	-3375	$-185193/114407$	114407a1	114407
3	6	-32768	$-5168743489/143729$	143729a1	143729
5	5	-32768	$-147197952/2539$	2539a1	2539
7	4	$2126 + O(7^5)$	$38272753/21283$	21283a1	21283
11	3	$7665 + O(11^5)$	$65597103937/110879$	110879c1	110879
13	2	-884736000	$-35937/1873$	1873a1	1873
17	2	$74802 + O(17^5)$	$-117649/89$	89a1	89
19	3	$-752904 + O(19^5)$	$49836032/57587$	57587a1	57587

We conclude with an example of an elliptic curve whose conductor is not prime. Let $E/\mathbb{Q}$ be the curve with label "309a1" and model

$$y^2 + xy = x^3 - 6x + 9.$$

The curve $E/\mathbb{Q}$ has bad multiplicative reduction at 3 and 103, with Kodaira symbols I5 and I1 respectively, and good reduction elsewhere. The j-invariant of E satisfies

$$j(E) = -\frac{24137569}{25029} = -17^6 \cdot 3^{-5} \cdot 103^{-1} \equiv 14 \bmod 25.$$

Thus, $j(E) \equiv j_0 \bmod 25$, where the canonical invariant in this case is $j_0 = -884736$ (see Example 4.4). With the help of Sage, we have verified that $\rho_{E,5} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{F}_5)$ is surjective. Hence, all the necessary hypotheses are met, and $\mathbb{Q}(E[5])/\mathbb{Q}(\zeta_5)$ is a $\mathrm{SL}(2, \mathbb{F}_5)$ extension that is only ramified at primes above a unique rational prime, namely $q = 103$. However, the extension $\mathbb{Q}(E[25])/\mathbb{Q}(\zeta_{25})$ also ramifies at primes above 3.

References

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

[2] Bilu, Y., Parent, P. and Rebolledo, M.: Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)* **63** (2013), no. 3, 957–984.

[3] Conrad, B. and Rubin, K.: *Arithmetic algebraic geometry.* IAS/Park City Mathematics Series 9, American Mathematical Society, Providence, RI, 2001.

[4] Diamond, F. and Shurman, J.: *A first course in modular forms.* Graduate Texts in Mathematics 228, Springer-Verlag, New York, 2005.

[5] Dieulefait, L.: The level 1 weight 2 case of Serre's conjecture. *Rev. Mat. Iberoam.* **23** (2007), no. 3, 1115–1124.

[6] Gross, B. H.: A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Math. J.* **61** (1990), no. 2, 445–517.

[7] Gaudron, É. and Rémond, G.: Théorème des périodes et degrés minimaux d'isogénies. *Comment. Math. Helv.* **89** (2014), no. 2, 343–403.

[8] Iwasawa, K.: *Local class field theory.* Oxford Science Publications, Oxford University Press, New York, 1986.

[9] Khare, C.: Serre's modularity conjecture: the level one case. *Duke Math. J.* **134** (2006), no. 3, 557–589.

[10] Khare, C. and Wintenberger, J-P.: Serre's modularity conjecture. I. *Invent. Math.* **178** (2009), no. 3, 485–504.

[11] Khare, C. and Wintenberger, J-P.: Serre's modularity conjecture. II. *Invent. Math.* **178** (2009), no. 3, 505–586.

[12] Kida, M.: Ramification in the division fields of an elliptic curve. *Abh. Math. Sem. Univ. Hamburg* **73** (2003), 195–207.

[13] Lang, S.: *Fundamentals of diophantine geometry.* Springer-Verlag, New York, 1983.

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

[15] Lubin, J., Serre, J-P. and Tate, J.: *Elliptic curves and formal groups.* Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts, July 6-31, 1964.

[16] Mazur, B.: Rational isogenies of prime degree. *Invent. Math.* **44** (1978), no. 2, 129–162.

[17] Ribet, K. A. and Stein, W. A.: Lectures on Serre's conjectures. In *Arithmetic algebraic geometry (Park City, UT, 1999),* 143–232. IAS/Park City Math. Ser. 9, Amer. Math. Soc., Providence, RI, 2001.

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

[19] Serre, J.-P. and Zagier, D. B.: *Modular functions of one variable V.* Lecture Notes in Mathematics 601, Springer-Verlag, Berlin-New York, 1977.

[20] Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401.

[21] Serre, J.-P.: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.* **54** (1987), no. 1, 179–230.

[22] Serre, J.-P.: *Abelian l-adic representations and elliptic curves.*, Research Notes in Mathematics 7, A K Peters, Wellesley, MA, 1998.

[23] Serre, J-P.: *Topics in Galois theory.* Research Notes in Mathematics 1, A K Peters, Wellesley, MA, 2008.

[24] Silverman, J. H.: *The arithmetic of elliptic curves.* Graduate Texts in Mathematics 106, Springer, Dordrecht, 2009.

[25] Silverman, J. H.: *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics 151, Springer-Verlag, New York, 1994

Received December 30, 2013; revised November 28, 2014.

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