ON GALOIS INERTIAL TYPES OF ELLIPTIC CURVES OVER $\mathbb{Q}_\ell$

LASSINA DEMBÉLÉ, NUNO FREITAS, AND JOHN VOIGHT

1. Introduction

Let ℓ be a prime, and $F/\mathbb{Q}_\ell$ a finite extension. Let $G_F = \mathrm{Gal}(\overline{F}/F)$ be the absolute Galois group of F, and $I_F \subset G_F$ the inertia subgroup. An *inertial type* is a homomorphism $\tau : I_F \to \mathrm{GL}_2(\mathbb{C})$, with open kernel, which extends to a representation of G_F. We say that τ is a *discrete series* if it is scalar or can be extended to an irreducible representation of G_F, in which case, we say that τ is *special* or *supercuspidal* accordingly.

There is an inertial Langlands correspondence between 2-dimensional Galois inertial types of F and smooth representations of $\mathrm{GL}_2(\mathcal{O}_F)$, where $\mathcal{O}_F$ denotes the ring of integers of F, (see [20] for definitions, and [5, Appendix] for this correspondence). This in fact justifies the above terminology. In an upcoming paper, we discuss an explicit/algorithmic version of this correspondence as well as arithmetic applications.

Inertial types were introduced in [8, 4] in the study of deformation rings. Since then, they have played a prominent role in the mod p and p-adic Langlands Programme. For example, the Breuil-Mézard Conjecture [5] for $\mathbb{Q}_\ell$ can be seen as a refinement of the Serre Conjecture over $\mathbb{Q}$ where inertial types are a crucial input.

In a different direction, the work of Bennett-Skinner [2] can be seen as a precursor of the use of inertial types in the study of Diophantine equations. Further refinements and new applications of those ideas are due to the second author and his collaborators [3, 13]. It is important to note that all of this is predated by work of Diamond and Kramer in [10, Appendix]. Indeed, motivated by Diophantine and modularity applications, they described (in the sense of [10, Section 2]) the structure of $\overline{\rho}_{E,p}$, the mod p representation attached to an elliptic curve $E/\mathbb{Q}_\ell$, in terms of the j-invariant of E. In [13], using a blend of the approaches in [16] and [10, Appendix], the authors describe, for $E/\mathbb{Q}_\ell$ with certain reduction types at $\ell = 2, 3$ (see [13, Theorem 3.1]), the possible fixed fields of the restriction to inertia $\overline{\rho}_{E,p}|_{I_\ell}$. They then use this to study the Generalized Fermat equation $x^2 + y^3 = z^p$.

In light of these applications, the goal of this paper is to give a complete description of the inertial types for all elliptic curves $E/\mathbb{Q}_\ell$, where ℓ is an arbitrary prime. Our results have recently been applied to the determination of the symplectic type of isomorphisms between the p-torsion of elliptic curve [14].

Date: October 2, 2019.

Freitas is supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 747808 and the grant *Proyecto RSME-FBBVA* 2015 *José Luis Rubio de Francia*.

2. A review of 2-dimensional Weil-Deligne representations

In this section, we will recall the necessary background for Galois representations of local fields. Our main references for the section are [18], [7] and [6].

We start by establishing some notation. As in the introduction, ℓ is a prime and $F/\mathbb{Q}_\ell$ a finite extension. Let π_F be a uniformizer of F, $\mathfrak{p} = (\pi_F)$ the unique prime of F, and write q_F for the cardinality of the residue field of F. Let v denote a valuation of F satisfying that $v(\pi_F) = 1$. Let $G_F = \mathrm{Gal}(\overline{F}/F)$ for the absolute Galois group of F, and W_F the Weil group of F. We denote the inertia subgroup of W_F by I_F. When $F = \mathbb{Q}_\ell$ we will write simply I_ℓ, W_ℓ and ℓ.

Let W_F^{ab} denote the maximal abelian quotient of W_F, and write $\mathrm{Art}_F : F^\times \to W_F^{ab}$ for the Artin reciprocity map from local class field theory, sending π_F to an inverse Frobenius element. The map Art_F allows to identify a character χ of W_F with the character $\chi^A = \chi \circ \mathrm{Art}_F$ of $F^\times$. We recall that, if $\chi : W_F \to \mathbb{C}^\times$ is a character, the conductor of χ is the ideal $\mathfrak{p}^m$, where m is the smallest integer such that $\chi^A|_{U_m}$ is trivial, where $U_m = 1 + \mathfrak{p}^m$. We will write $\mathrm{cond}(\chi) = \mathfrak{p}^m$ and, by abuse of notation, we will also write $\mathrm{cond}(\chi)$ to denote the conductor exponent m.

Denote by ω the unramified quasi-character giving the action of W_F on the roots of unity, which corresponds to the norm quasi-character $|\cdot|$ via class field theory.

We are interested in 2-dimensional complex Weil-Deligne representations of the local field F (see [18, Section 3] for definitions). We recall that a Weil-Deligne representation consists of a pair (σ, N) such that

(1) σ is a representation $\sigma : W_F \to \mathrm{GL}_2(\mathbb{C})$ of the Weil group of F; and
(2) N is a nilpotent endomorphism of $\mathbb{C}^2$ satisfying
$$\sigma(g)N\sigma(g)^{-1} = \omega(g)N \quad \text{for all } g \in W_F.$$

We will now briefly describe the types of 2-dimensional Weil-Deligne representations.

2.1. Principal series.

Let $\chi : W_F \to \mathbb{C}^\times$ be a character. The *principal series* representation attached to χ is given by the pair $(\sigma, 0)$, where
$$\sigma = \mathrm{PS}(\chi) = \chi \oplus \chi^{-1}\omega^{-1}.$$
Its conductor exponent is given by
$$\mathrm{cond}(\mathrm{PS}(\chi)) = 2\,\mathrm{cond}(\chi) \tag{2.1}$$

2.2. Special series.

Let $\chi : W_F \to \mathbb{C}^\times$ be a character whose restriction to I_F is quadratic. The *special series* representation attached to χ is given by the pair (σ, N), where
$$\sigma = \mathrm{Sp}(\chi) = \chi \otimes \begin{pmatrix} \omega & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$
Its conductor exponent is given by
$$\mathrm{cond}(\mathrm{Sp}(\chi)) = \begin{cases} 2\,\mathrm{cond}(\chi) & \text{if } \chi \text{ is ramified} \\ 1 & \text{otherwise.} \end{cases} \tag{2.2}$$

2.3. **Supercuspidal representations.** Irreducible Weil-Deligne representations $(\sigma, 0)$, with $\sigma : W_F \to \mathrm{GL}_2(\mathbb{C})$, are classified by their projective images in $\mathrm{PGL}_2(\mathbb{C})$ (see [6, Sections 41 and 42] or [7, Section 12]). We say that σ is *imprimitive* (resp. *primitive*) if its projective image is the dihedral group D_n (resp. A_4 or S_4). We also use the term *non-exceptional* (resp. *exceptional*) to describe imprimitive (resp. primitive) representations. It is known that primitive representations only exists when the residual characteristic $\ell = 2$. (We note that, since W_F is totally disconnected, the case when σ has projective image A_5 cannot occur.)

2.3.1. **Imprimitive supercuspidal representations.** Let M/F be a quadratic extension and write ϵ_M for the quadratic character corresponding to M. Write $s \in G_F$ for a lift of the non-trivial element in $\mathrm{Gal}(M/F)$. Let $\chi : W_M \to \mathbb{C}^\times$ be a character. Define its s-conjugate character $\chi^s : W_M \to \mathbb{C}^\times$ by the formula $\chi^s(g) := \chi(s^{-1}gs)$ for $g \in W_M$. We note that $\chi = \chi^s$ if and only if the character $\chi^A = \chi \circ \mathrm{Art}_F$ factors through the norm map of M/F, that is, if and only if there exists a character $\theta : F^\times \to \mathbb{C}^\times$ such that

$$\chi^A(x) = (\theta \circ \mathrm{Nm}_{M/F})(x), \text{ for all } x \in M^\times.$$

Suppose that $\chi \neq \chi^s$; then the *imprimitive supercuspidal* representation attached to χ is given by $(\sigma, 0)$, where

$$\sigma = \mathrm{BC}(\chi) = \mathrm{Ind}_{W_M}^{W_F} \chi, \quad \text{in which case} \quad (\chi^A|_{F^\times}) \cdot \epsilon_M^A = |\cdot|^{-1} \text{ as characters of } F^\times. \tag{2.3}$$

Its conductor exponent is given by

$$\mathrm{cond}(\mathrm{BC}(\chi)) = \begin{cases} 2\,\mathrm{cond}(\chi) & \text{if } M/F \text{ is unramified} \\ \mathrm{cond}(\chi) + \mathrm{cond}(\epsilon_M) & \text{otherwise.} \end{cases} \tag{2.4}$$

The condition $\chi \neq \chi^s$ above is necessary to ensure that σ is irreducible.

For our calculations below, we will need to check if characters of the form χ^A factor through the norm map. For that we will often use the following lemma.

Lemma 2.5. *Let M/F be quadratic and $\chi : M^\times \to \mathbb{C}^\times$ a character. Let $s \in \mathrm{Gal}(M/F)$ be non-trivial and define $\chi^s(x) := \chi(x^s)$. If χ factors through the norm map then $\chi = \chi^s$.*

Proof. Suppose that $\chi(x) = (\theta \circ \mathrm{Nm}_{M/F})(x)$ for some character $\theta : F^\times \to \mathbb{C}^\times$. Then,

$$\chi^s(x) = \chi(s(x)) = \theta(\mathrm{Nm}_{M/F}(s(x))) = \theta(\mathrm{Nm}_{M/F}(x)) = \chi(x).$$

□

2.3.2. **Primitive supercuspidal representations.** Let $\sigma : W_F \to \mathrm{GL}_2(\mathbb{C})$ be a primitive supercuspidal representation σ. From [6, p. 261], it follows that there is a cubic extension K/F (unique up to F-isomorphism) such that $\sigma|_{W_K}$ is imprimitve. So, there exists a quadratic extension M/K, and a character $\chi : W_M \to \mathbb{C}^\times$, which doesn't factor through the norm map $\mathrm{Nm}_{M/K}(x)$, such that

$$\sigma|_{W_K} = \mathrm{BC}(\chi) = \mathrm{Ind}_{W_M}^{W_K} \chi.$$

Furthermore, if $\sigma' : W_F \to \mathrm{GL}_2(\mathbb{C})$ is another primitive representation such that $\det \sigma = \det \sigma'$ and $\sigma|_{W_K} \sim \sigma'|_{W_K}$, then σ and σ' are isomorphic. This shows that a primitive representation $\sigma : W_F \to \mathrm{GL}_2(\mathbb{C})$ is determined by a triple (K, M, χ), where K/F is a cubic extension, M/K quadratic extension, and $\chi : W_M \to \mathbb{C}^\times$ a character such that $\chi^s \neq \chi$.

For a triple (K, M, χ) as above, we define the associated *primitive supercuspidal* Weil-Deligne representation to be the pair $(\sigma, 0)$.

3. **Inertial types**

We recall that an *inertial type* is a representation $\tau : I_F \to \mathrm{GL}_2(\mathbb{C})$, with open kernel, which extends to a representation $\sigma : W_F \to \mathrm{GL}_2(\mathbb{C})$. We will say that τ is a *principal series* (resp. *special series* or *supercuspidal type*) if σ is a principal series (resp. special series or supercuspidal representation). If σ is supercuspidal, we will say that τ is *imprimitive* (resp. *primitive*) if σ is imprimitive (resp. primitive).

Lemma 3.1. *Let $\sigma = \mathrm{Ind}_{W_M}^{W_F} \chi$ be an imprimitive supercuspidal representation and $\tau = \sigma|_{I_F}$ the corresponding supercuspidal type. Then τ is given by*

$$\tau = \chi|_{I_F} \oplus \chi^s|_{I_F} \qquad \textit{or} \qquad \tau = \mathrm{Ind}_{I_M}^{I_F} \chi|_{I_M}$$

according as to whether the quadratic extension M/F is unramified or ramified.

Proof. There is an unramified character μ of W_F such that the twist $\sigma \otimes \mu$ has finite image (cf. 2.2.1 in [21]). Since $(\sigma \otimes \mu)|_{I_F} = \sigma|_{I_F} \otimes \mu|_{I_F} = \tau$, we can assume that σ has finite image.

We now follow the notation in [19, Section 7.3]. Let G be the Galois group of the fixed field of σ, and write the double coset decomposition

$$G = \coprod_{h \in S} I_F \cdot h \cdot W_M.$$

Since W_M has index 2 inside W_F, we have the following two possibilities for S:

(i) $S = \{1, s\}$ if $I_F \subset W_M$; or
(ii) $S = \{1\}$ if $I_F \not\subset W_M$.

We now apply [19, Proposition 22] to determine the shape of $\tau = \sigma|_{I_F}$. This gives that $\tau = \chi|_{I_F} \oplus \chi^s|_{I_F}$ in case (i), and $\tau = \mathrm{Ind}_{I_M}^{I_F} \chi|_{I_M}$ in case (ii). Finally, we note that $I_F \subset W_M$ if and only if M/F is unramified. $\square$

The following proposition gives a complete classification of all inertial types, which are *not* primitive (compare with [5, Lemme 2.1.1.2]).

Proposition 3.2. *Let $\tau : I_F \to \mathrm{GL}_2(\mathbb{C})$ be an inertial type, which is not primitive. Then, we have one of the followings:*

(i) τ is the restriction of a principal series, i.e. there exists $\chi : W_F \to \mathbb{C}^\times$ such that

$$\tau = \mathrm{PS}(\chi)|_{I_F};$$

(ii) τ is the restriction of a special series, i.e. there exists $\chi : W_F \to \mathbb{C}^\times$ such that

$$\tau = \mathrm{Sp}(\chi)|_{I_F};$$

(iii) There exists a character $\chi : W_M \to \mathbb{C}^\times$, where M/F is the unramified quadratic extension, which does not *extend to W_F such that $\chi \neq \chi^s$ and*

$$\tau = \chi|_{I_F} \oplus \chi^s|_{I_F};$$

(iv) There exist a ramified quadratic extension M/F, and a character $\chi : W_M \to \mathbb{C}^\times$ such that

$$\tau = \operatorname{Ind}_{I_M}^{I_F} \chi|_{I_M}.$$

Proof. This follows from the above discussion together with Lemma 3.1. □

We see that τ is reducible in Cases (i)–(iii), and irreducible in Case (iv). Also, in Cases (iii) and (iv), we see that τ is a supercuspidal series type. We say τ is an *exceptional type (or primitive type)* if it is the restriction to I_F of an exceptional representation.

It is clear from the definitions of $\mathrm{PS}(\chi)$ and $\mathrm{Sp}(\chi)$ that principal series and special types are determined by $\chi|_{I_F}$, the restriction of χ to inertia. Similarly, it follows from Propostion 3.1 and the discussion in Section 2.3.2 that $(K, M, \chi|_{I_M})$ completely determines $\tau = \sigma|_{I_F}$ where σ is the exceptional representation corresponding to (K, M, χ).

4. Background on elliptic curves

In this section we will recall some well know facts about elliptic curves and give a couple of preliminary results on their inertial types.

For an elliptic curve E defined over a global or local field we will write N_E for its conductor.

Let $F/\mathbb{Q}_\ell$ be a finite extension and E/F an elliptic curve. There is $\sigma_E \colon W_F \to \mathrm{GL}_2(\mathbb{C})$, a representation of conductor N_E attached to E (see [18, Section 13] and [9, Remark 2.14]).

We call the restriction $\tau := \sigma_E|_{I_F}$ *the inertial type of E*. When E is defined over a global field whose completion at a prime ℓ is F we say *inertial type of E at ℓ*.

The following statement is a consequence of Tate's algorithm.

Lemma 4.1. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Then,*

(i) $0 \leq \upsilon_\ell(N_E) \leq 2$ *for* $\ell \geq 5$*;*
(ii) $0 \leq \upsilon_\ell(N_E) \leq 5$ *for* $\ell = 3$*;*
(iii) $0 \leq \upsilon_\ell(N_E) \leq 8$ *for* $\ell = 2$*.*

Moreover, if E has additive reduction at ℓ then $\ell^2 \parallel N_E$;

Assume that E has potentially good reduction. Let $m \in \mathbb{Z}_{\geq 3}$ be coprime to ℓ, and consider the field $L_E = F^{un}(E[m])$. It is well known (see [16]) that the extension L_E/F^{un} is independent of m, and is the minimal extension of F^{un} where E achieves good reduction. Note that L_E is the field fixed by $\tau = \sigma_E|_{I_F}$; we call it *the inertial field of E*. Write $\Phi = \mathrm{Gal}(L_E/F^{un})$ and denote by e the order of Φ. We call e the *semistability defect of E*. The following lemma, which describes the possibilities for Φ, can be found in [16].

Lemma 4.2. *Let $F/\mathbb{Q}_\ell$ be a finite extension and E/F an elliptic curve with potentially good reduction. Then,*

(i) *if* $\ell \geq 5$ *then* Φ *is cyclic of order* $2, 3, 4$ *or* 6;
(ii) *if* $\ell = 3$ *then* Φ *is cyclic of order* $2, 3, 4, 6$ *or isomorphic to the non-abelian semi-direct product* $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ *of order* 12;
(iii) *if* $\ell = 2$ *then* Φ *is cyclic of order* $2, 3, 4, 6$ *or of order* 8 *and isomorphic to the quaternion group* H_8 *or of order* 24 *and isomorphic to* $\mathrm{SL}_2(\mathbb{F}_3)$.

From Lemma 4.2, one gets the following partial descriptions of the inertial types of $E/\mathbb{Q}_\ell$ in the extremal cases when $e = 2$ or $e = 24$.

Proposition 4.3. *Let* $E/\mathbb{Q}_\ell$ *be an elliptic curve with potentially good reduction with semistability defect* $e = 2$ *and inertial type* τ. *Then* τ *is trivial after a quadratic twist.*

Proof. Since L_E is fixed by τ and $e = 2$, then $L_E/\mathbb{Q}_\ell^{un}$ is a quadratic extension. Twisting τ by the quadratic character corresponding to L_E will trivialize τ, as desired. □

Proposition 4.4. *Let* $E/\mathbb{Q}_2$ *be an elliptic curve with additive potentially good reduction, semistability defect* e *and inertial type* τ. *Then* τ *is exceptional if and only if* $e = 24$.

Proof. Suppose $\tau := \sigma_E|_{I_2}$ is exceptional. From the group structure of $\overline{G}$ in [6, Section 42.3] it follows that e is at least 12, so we must have $e = 24$ by Lemma 4.2.

Conversely, suppose $e = 24$. From [12, Lemma 1] there is an unramified twist of σ_E factoring via the field $K = \mathbb{Q}_2(E[3])$, so the images of $\mathbb{P}(\sigma_E)$ and $\mathbb{P}(\overline{\rho}_{E,3})$ are isomorphic as abstract groups. Since τ is irreducible with image isomorphic to $\Phi \simeq \mathrm{SL}_2(\mathbb{F}_3)$, we have that $\overline{\rho}_{E,3}(G_{\mathbb{Q}_2}) = \mathrm{GL}_2(\mathbb{F}_3)$ (see [12, Table 1]). Thus $\mathbb{P}(\sigma_E) \simeq \mathrm{GL}_2(\mathbb{F}_3)/\{\pm 1\} \simeq S_4$, so that σ_E is an exceptional representation, hence τ is an exceptional type, as desired. □

5. Special inertial types for $E/\mathbb{Q}$

In this section, we focus on elliptic curves with potentially multiplicative reduction at a prime ℓ. If $E/\mathbb{Q}_\ell$ is an elliptic curve with potentially multiplicative reduction at ℓ, then the type $\tau_E = \sigma_E|_{I_\ell}$ is a special inertial type. Write $\tau_{sp} := \mathrm{Sp}(1)|_{I_\ell}$.

Proposition 5.1. *Let* $E/\mathbb{Q}_\ell$ *be an elliptic curve with potentially multiplicative reduction with conductor* N_E *and inertial type* τ.

Then, $\tau = \mathrm{Sp}(\chi)|_{I_\ell}$ *for some character* χ *of* W_ℓ. *Moreover,*

(1) If E *has multiplicative reduction then* $\ell \parallel N_E$ *and* $\tau = \tau_{sp}$.

(2) Suppose E *has additive reduction, that is* $\ell^2 \mid N_E$.

(i) *If* $\ell \geq 3$ *then* $\ell^2 \parallel N_E$ *and* $\tau = \tau_{sp} \otimes \epsilon_\ell$.
(ii) *If* $\ell = 2$ *then* $\ell^4 \parallel N_E$ *and* $\tau = \tau_{sp} \otimes \epsilon_{-1}$ *or* $\ell^6 \parallel N_E$ *and* $\tau = \tau_{sp} \otimes \epsilon_2$ *or* $\tau_{sp} \otimes \epsilon_{-2}$.

Proof. Let $\tau = \sigma_E|_{I_\ell}$ be the type of E. We have $\tau = \mathrm{Sp}(\chi)|_{I_\ell}$ for some character χ of W_ℓ since this is the only kind of type arising from a representation (σ, N) where $N \neq 0$.

(1) If E has multiplicative reduction, then $N_E = \mathrm{cond}(\tau) = \ell$ and by the conductor formula it follows that χ is unramified. In that case,

$$\tau = (\chi \otimes \mathrm{Sp}(1))|_{I_\ell} = \chi|_{I_\ell} \otimes \mathrm{Sp}(1)|_{I_\ell} = \mathrm{Sp}(1)|_{I_p} = \tau_{sp},$$

as desired.

(2) Suppose E as additive reduction, so that $\ell^2 \mid N_E$. Then, the conductor formula gives $N_E = \mathrm{cond}(\tau) = \ell^{2m}$, with χ ramified and $\mathrm{cond}(\chi) = \ell^m$.

Since $\det \sigma_E = \omega^{-1}$, we conclude that $(\chi|_{I_\ell})^2 = 1$.

If $\ell \geq 3$, then any character $\chi : W_\ell \to \mathbb{C}^\times$ such that $\chi|_{I_\ell}$ is quadratic must have conductor ℓ, and satisfies that $\chi|_{I_\ell} = \epsilon_\ell$. Thus $m = 1$, $\ell^2 \parallel N_E$ and $\tau = \tau_{sp} \otimes \epsilon_\ell$. This proves (i).

If $\ell = 2$, then character $\chi : W_2 \to \mathbb{C}^\times$ such that $\chi|_{I_2}$ is quadratic must be of either of the following types:

- χ has conductor 2^2 and satisfies $\chi|_{I_\ell} = \epsilon_{-1}$; or
- χ has conductor 2^3 and $\chi|_{I_\ell} = \epsilon_{-2}$ or ϵ_2.

We conclude that either $\tau = \tau_{sp} \otimes \epsilon_{-1}$ and $2^4 \parallel N_E$ or $2^6 \parallel N_E$ and $\tau = \tau_{sp} \otimes \epsilon_2$ or $\tau_{sp} \otimes \epsilon_{-2}$. This proves (ii). □

This proposition covers all the cases of potentially multiplicative reduction. So, the rest of this paper is concerned with elliptic curves with potentially good reduction.

6. Inertial types at $\ell \geq 5$

Let $\ell \geq 5$ be a prime, and M the unique unramified quadratic extension of $\mathbb{Q}_\ell$. Let $\mathfrak{p}$ be the unique prime in M, and $s \in G_{\mathbb{Q}_\ell}$ a lift of the non-trivial element of $\mathrm{Gal}(M/\mathbb{Q}_\ell)$.

We first define the possible types for an elliptic curve $E/\mathbb{Q}_\ell$ with potentially good reduction and then prove the list is correct. Recall from Section 4 that the semistability defect of E is $e = 2, 3, 4, 6$.

(1) Suppose $e \in \{3, 4, 6\}$ satisfies $e \mid \ell - 1$. Let χ_e be any character of W_ℓ given on I_ℓ by $\chi_e(\mu) = \zeta_e$, where μ is a generator of $(\mathbb{Z}_\ell/\ell)^\times$, and define the type $\tau_{\ell,e}$ of conductor ℓ^2 by

$$\tau_{\ell,e} = \mathrm{PS}(\chi_e)|_{I_\ell}$$

(2) Suppose $e \in \{3, 4, 6\}$ satisfies $e \mid \ell + 1$. Let χ'_e be a character of W_M of conductor given on I_M by $\chi'_e(\mu) = \zeta_e$, where μ is a generator of $(\mathcal{O}_M/\mathfrak{p})^\times$. Define the inertial type $\tau'_{\ell,e}$ of conductor ℓ^2 by

$$\tau'_{\ell,e} = \mathrm{BC}(\chi'_e)|_{I_\ell}.$$

Proposition 6.1. *Let $\ell \geq 5$. Let $E/\mathbb{Q}_\ell$ be an elliptic curve with additive potentially good reduction, semistability defect e and inertial type τ. Then,*

(a) *if $e = 2$ then τ is trivial after a quadratic twist;*
(b) *if $e = 3, 4, 6$ and $e \mid \ell - 1$ then $\tau \simeq \tau_{\ell,e}$ is a principal series;*
(c) *if $e = 3, 4, 6$ and $e \mid \ell + 1$ then $\tau \simeq \tau'_{\ell,e}$ is supercuspidal.*

Proof. Part (a) is Proposition 4.3, so we can suppose $e \neq 2$.

Lemma 4.1 implies that τ has conductor ℓ^2. And, from Lemma 4.2, it follows that $\Phi := \mathrm{Gal}(L_E/\mathbb{Q}_\ell^{un})$ is cyclic of order $e = 3, 4, 6$. Therefore, τ is a reducible type with finite image, hence it is either principal series or (imprimitive) supercuspidal induced from the unramified quadratic extension M.

Case 1: τ is a principal series.

Then, $\tau = \chi|_{I_\ell} \oplus \chi^{-1}|_{I_\ell}$, where χ is a character of W_ℓ of conductor ℓ and order e. Thus, $\chi|_{I_\ell}$ factors through

$$\mathbb{Z}_\ell^\times / U_1 \simeq (\mathbb{Z}_\ell/\ell)^\times \simeq \mathbb{F}_\ell^\times \simeq \mathbb{Z}/(\ell-1)\mathbb{Z}.$$

Hence, e divides $\ell - 1$. Let μ be a lift of the generator μ of $(\mathbb{Z}_\ell/\ell)^\times$ given in (1) above. We have $\chi(\mu) = \zeta_e^c$ with $1 \leq c \leq e$ and $(c, e) = 1$. Clearly, for the three possible values of e there are only two choices for $\chi|_{I_\ell}$ which correspond to χ_e and χ_e^{-1}. Both give $\tau \simeq \tau_{\ell,e}$.

Case 2: τ is supercuspidal.

Since τ has conductor ℓ^2, it follows that χ is a character of $M^\times$ of conductor $\mathfrak{p}$ satisfying $\chi|_{\mathbb{Z}_\ell^\times} = 1$. We have that $\chi|_{I_\ell}$ factors through

$$\mathcal{O}_M^\times / U_1 \simeq (\mathcal{O}_M/\mathfrak{p})^\times \simeq \mathbb{F}_{\ell^2}^\times \simeq \mathbb{Z}/(\ell^2 - 1)\mathbb{Z},$$

hence e divides $\ell^2 - 1 = (\ell+1)(\ell-1)$. Let μ be a lift of the generator μ of $(\mathcal{O}_M/\mathfrak{p})^\times$ in (2) above. Observe that $\mu^{\ell+1}$ generates $(\mathbb{Z}_\ell/\ell)^\times \subset (\mathcal{O}_M/\mathfrak{p})^\times$. So, the condition $\chi|_{\mathbb{Z}_\ell^\times} = 1$ implies that $e \mid \ell + 1$. We have $\chi(\mu) = \zeta_e^c$, with $1 \leq c \leq e$ and $(c, e) = 1$. Again, as above, the possibilities for $\chi|_{I_M}$ are χ'_e or $(\chi'_e)^{-1}$.

Note that χ does not factor through the norm map. Otherwise, we would have

$$\zeta_e^c = \chi(\mu) = \chi(s(\mu)) = \chi(\mu^\ell) = \zeta_e^{c\ell}$$

which would imply that $e \mid \ell - 1$, a contradiction with $e \mid \ell + 1$ (since $e \neq 2$).

We conclude that $\chi^s \neq \chi$ and so we have either $\chi|_{I_M} = \chi'_e$ and $\chi^s|_{I_M} = (\chi'_e)^{-1}$ or vice-versa. In both cases, we obtain $\tau \simeq \tau'_{\ell,e}$. Parts (b) and (c) now follow. □

7. Inertial types at $\ell = 3$

Let $M = \mathbb{Q}_3(d)$, for $d = \sqrt{-1}, \sqrt{\pm 3}$, denote a quadratic extension of $\mathbb{Q}_3$, and write $\mathfrak{p}$ for the prime in M. Also write $\mathcal{O}_M = \mathbb{Z}_3[w]$ for the ring of integers. Let $s \in G_{\mathbb{Q}_3}$ be a lift of the non-trivial element of $\mathrm{Gal}(M/\mathbb{Q}_\ell)$.

Recall that ϵ_3 is the unique quadratic character of I_3 with conductor 3; it can be obtained by restricting to inertia the quadratic character fixing $\mathbb{Q}_3(\sqrt{-3})$.

In Tables 1 and 2 we list the possible types for an elliptic curve $E/\mathbb{Q}_3$ with potentially good reduction. The propositions in this section will show that list is correct. Recall that the semistability defect of E is $e = 2, 3, 4, 6, 12$ with Φ non-abelian when $e = 12$.

Proposition 7.1. *Let $E/\mathbb{Q}_3$ be an elliptic curve with potentially good reduction, conductor $N_E = 3^2$ and inertial type τ. Then $\tau \simeq \tau'_{3,4}$.*

Proof. Since the conductor exponent is 2, we are in the case of tame reduction. Hence, $e = 4$ and Φ is cyclic by Lemma 4.2.

Table 1. Conductors and group structures for $(\mathcal{O}_M/\mathfrak{f})^\times$ for quadratic extension of $\mathbb{Q}_3$

M	$\mathfrak{f}$	$(\mathcal{O}_M/\mathfrak{f})^\times$	Group structure
$\mathbb{Q}_3$	3^2	$\langle -1\rangle \times \langle 4\rangle$	$\mathbb{Z}/2\times\mathbb{Z}/3$
$\mathbb{Q}_3(\sqrt{-1})$	$\mathfrak{p}$	$\langle w-1\rangle$	$\mathbb{Z}/8$
$\mathbb{Q}_3(\sqrt{-1})$	$\mathfrak{p}^2$	$\langle -2w+2\rangle \times \langle 3w+1\rangle \times \langle 4\rangle$	$\mathbb{Z}/8\times\mathbb{Z}/3\times\mathbb{Z}/3$
$\mathbb{Q}_3(\sqrt{3})$	$\mathfrak{p}^2$	$\langle -1\rangle \times \langle w+1\rangle$	$\mathbb{Z}/2\times\mathbb{Z}/3$
$\mathbb{Q}_3(\sqrt{-3})$	$\mathfrak{p}^2$	$\langle -1\rangle \times \langle -w\rangle$	$\mathbb{Z}/2\times\mathbb{Z}/3$
$\mathbb{Q}_3(\sqrt{3})$	$\mathfrak{p}^4$	$\langle -1\rangle \times \langle w+1\rangle \times \langle 4\rangle$	$\mathbb{Z}/2\times\mathbb{Z}/9\times\mathbb{Z}/3$
$\mathbb{Q}_3(\sqrt{-3})$	$\mathfrak{p}^4$	$\langle -1\rangle \times \langle -3w-2\rangle \times \langle 4w+1\rangle \times \langle 4\rangle$	$\mathbb{Z}/2\times\mathbb{Z}/3\times\mathbb{Z}/3\times\mathbb{Z}/3$

Suppose τ is a principal series. Then $\tau = \chi|_{I_3} \oplus \chi^{-1}|_{I_3}$, where χ is a character of W_3 of conductor 3 and order 4, which is impossible. So, τ must be imprimitive supercuspidal since we are in odd characteristic. Noting that $e = 4 \mid (3+1)$, we conclude that $\tau \simeq \tau'_{3,4}$ using a similar argument as in the proof of Part (c) of Proposition 6.1. □

Proposition 7.2. *Let $E/\mathbb{Q}_3$ be an elliptic curve of conductor N_E, with inertial type τ and additive potentially good reduction. Assume that E as semistability defect $e \neq 2$. Then, τ is given by one of the following cases:*

1. *if $N_E = 3^2$ then $e = 4$ and $\tau = \tau'_{3,4}$;*
2. *if $N_E = 3^4$ then $e = 3$ and $\tau \simeq \tau_3$, $\tau_{\sqrt{-1}}$ or $e = 6$ and $\tau \simeq \tau_3 \otimes \epsilon_3$, $\tau_{\sqrt{-1}} \otimes \epsilon_3$;*
3. *if $N_E = 3^3$ then $e = 12$ and $\tau = \tau_{\sqrt{3}}$ or $\tau = \tau_{\sqrt{-3}}$;*
4. *if $N_E = 3^5$ then $e = 12$ and $\tau = \tau_{\sqrt{-3},j}$ for some $j = 0, 1, 2$;*

Proof. Part (1) follows from Proposition 7.1.

We will now prove (2). Suppose $N_E = 3^4$.

Assume τ is a principal series. Then $\tau = \chi|_{I_3} \oplus \chi^{-1}|_{I_3}$, where χ is a character of W_3 with conductor 3^2. Thus $\chi|_{I_3}$ factors through $\mathbb{Z}_3^\times/U_3 \simeq \langle -1\rangle \times \langle 4\rangle$ (see Table 1), and must be primitive. This means that $\chi(4) = \zeta_3^c$ with $c = 1$ or 2. Twisting by ϵ_3, we can assume that $\chi(-1) = 1$. Thus, there are two possibilities for $\chi|_{I_3}$, which are $\chi_{3,2}$ and $\chi_{3,2}^{-1}$. Thus $\tau \simeq \tau_3$ (hence $e = 3$) or $\tau \simeq \tau_3 \otimes \epsilon_3$ (hence $e = 6$).

Assume τ is supercuspidal, hence is an induction of χ from a quadratic extension $M = \mathbb{Q}_3(d)$.

Suppose first that $d = \sqrt{-1}$, so that M is unramified. Then χ has conductor $\mathfrak{p}^2$ and $\chi|_{I_\mathfrak{p}}$ factors through $\mathcal{O}_M^\times/U_2 \simeq \langle -2w+2\rangle \times \langle 3w+1\rangle \times \langle 4\rangle$ (see Table 1). The condition $\chi|_{\mathbb{Z}_3^\times} = 1$ implies $\chi^4(-2w+2) = 1$ and $\chi(4) = 1$; Since χ is primitive, we must have $\chi(1+3w) = \zeta_3^c$ with $c = 1$ or 2. This also implies that χ does not factor through the norm map. We must have $\chi(-2w+2) = \pm 1$ since τ has an abelian image. Otherwise, we would have $e = 12$ and Φ would be non-abelian. Therefore, up to twisting by ϵ_3, we can assume that $\chi(-2w+2) = 1$. So, again, we have two possibilities for $\chi|_{I_3}$, which are $\chi_{\sqrt{-1}}$ and its conjugate; hence $\tau \simeq \tau_{\sqrt{-1}}$ (and $e = 3$).

Table 2. Galois inertial types attached to characters at $\ell = 3$; in the bottom row $j = 0, 1, 2$.)

M	$\mathfrak{f}$	χ	χ on generators	τ	cond(τ)
$\mathbb{Q}_3$	3^2	$\chi_{3,2}$	$1,\ \zeta_3$	$\tau_3 = \mathrm{PS}(\chi_{3,2})\|_{I_3}$	3^4
$\mathbb{Q}_3(\sqrt{-1})$	$\mathfrak{p}$	χ_4	ζ_4	$\tau'_{3,4} = \mathrm{BC}(\chi_4)\|_{I_3}$	3^2
$\mathbb{Q}_3(\sqrt{-1})$	$\mathfrak{p}^2$	$\chi_{\sqrt{-1}}$	$1,\ \zeta_3,\ 1$	$\tau_{\sqrt{-1}} = \mathrm{BC}(\chi_{\sqrt{-1}})\|_{I_3}$	3^4
$\mathbb{Q}_3(\sqrt{3})$	$\mathfrak{p}^2$	$\chi_{\sqrt{3}}$	$-1,\ \zeta_3$	$\tau_{\sqrt{3}} = \mathrm{BC}(\chi_{\sqrt{3}})\|_{I_3}$	3^3
$\mathbb{Q}_3(\sqrt{-3})$	$\mathfrak{p}^2$	$\chi_{\sqrt{-3}}$	$-1,\ \zeta_3$	$\tau_{\sqrt{-3}} = \mathrm{BC}(\chi_{\sqrt{-3}})\|_{I_3}$	3^3
$\mathbb{Q}_3(\sqrt{-3})$	$\mathfrak{p}^4$	$\chi_{\sqrt{-3},j}$	$-1,\ \zeta_3,\ \zeta_3^j,\ 1$	$\tau_{\sqrt{-3},j} = \mathrm{BC}(\chi_{\sqrt{-3},j})\|_{I_3}$	3^5

The last sentence in [17, Corollary 3.1] shows that τ cannot be induced from a ramified quadratic extension $M/\mathbb{Q}_3$ in this case. This completes the proof of (2).

Suppose $3^k \parallel N_E$ with $k = 3, 5$. Then, it follows from the conductor formula that τ is obtained from an induction of a character χ for one of ramified quadratic extensions $M/\mathbb{Q}_3$. It follows from Propositions 3.1 and 3.2 that τ is irreducible; hence, $e = 12$ by Lemma 4.2. Moreover, since $k = \upsilon_{\mathfrak{p}}(\mathrm{cond}(\chi)) + \upsilon_3(\mathrm{disc}(M))$ and $\upsilon_3(\mathrm{disc}(M)) = 1$, χ has conductor $\mathfrak{p}^2$ for $k = 3$, and $\mathfrak{p}^4$ for $k = 5$.

Suppose $k = 3$. Then, we have $(\mathcal{O}_M/\mathfrak{p}^2)^\times \simeq \langle -1 \rangle \times \langle u \rangle$, where $u = w + 1$ for $M = \mathbb{Q}_3(\sqrt{3})$, and $u = -w$ for $M = \mathbb{Q}_3(\sqrt{-3})$ (see Table 1). The condition $\chi|_{\mathbb{Z}_3^\times} = \epsilon_M$ implies $\chi(-1) = -1$. Again, since χ is primitive, we must have $\chi(u) = \zeta_3^c$ with $c = 1$ or 2. This means that χ doesn't factor through the norm. Therefore, there are two choices for $\chi|_{I_M}$ which are χ_d and χ_d^s, with $d = \sqrt{\pm 3}$. Both give that $\tau \simeq \tau_d$. This proves (3).

Suppose now that $k = 5$ and $d = \sqrt{3}$. The character $\chi|_{I_M}$ factors through $(\mathcal{O}_M/\mathfrak{p}^4)^\times \simeq \langle -1 \rangle \times \langle w + 1 \rangle \times \langle 4 \rangle = \mathbb{Z}/2 \times \mathbb{Z}/9 \times \mathbb{Z}/3$. The condition $\chi|_{\mathbb{Z}_3^\times} = \epsilon_M$ implies $\chi(-1) = -1$. Since χ has conductor $\mathfrak{p}^4$, we must have $\chi(w + 1) = \zeta_9^c$ with $(c, 3) = 1$; thus $9 \mid e$, which is a contradiction.

We conclude that $k = 5$ and $d = \sqrt{-3}$. The character $\chi|_{I_M}$ factors through $(\mathcal{O}_M/\mathfrak{p}^4)^\times \simeq \langle -1 \rangle \times \langle -3w - 2 \rangle \times \langle 4w + 1 \rangle \times \langle 4 \rangle$ (see Table 1). The condition $\chi|_{\mathbb{Z}_3^\times} = \epsilon_M$ implies $\chi(-1) = -1$ and $\chi(4) = 1$. The primitivity of χ implies that $\chi(-3w + 2) = \zeta_3^c$ with $c = 1$, or 2. Hence, χ does not factor via the norm. There are no constraints on the generator $4w + 1$, so $\chi(4w + 1) = \zeta_3^j$ with $j = 0, 1$, or 2. Thus, we have six possible choices for $\chi|_{I_M}$, which group into three pairs of conjugated characters (χ, χ^s). Since each pair contains one character for which $c = 1$, and conjugated characters give the same type, we can assume that $c = 1$. Hence, $\chi|_{I_M} = \chi_{d,j}$ and $\tau \simeq \tau_{\sqrt{-3},j}$ for $j = 0, 1$, or 2. This proves (4). □

8. Non-exceptional inertial types at $\ell = 2$

Let $M = \mathbb{Q}_2(d)$ for $d = \sqrt{-1}$, $\sqrt{\pm 2}$, $\sqrt{\pm 5}$, $\sqrt{\pm 10}$ be one of the seven quadratic extensions of $\mathbb{Q}_2$. Also write $\mathcal{O}_M = \mathbb{Z}_2[w]$ for the ring of integers of M, and $\mathfrak{p}$ for the prime of M. Let

TABLE 3. Conductors and group structures for $(\mathcal{O}_M/\mathfrak{f})^\times$ for quadratic extension of $\mathbb{Q}_2$

M	$\mathfrak{f}$	$(\mathcal{O}_M/\mathfrak{f})^\times$	Group structure
$\mathbb{Q}_2$	2^4	$\langle -1\rangle \times \langle 5\rangle$	$\mathbb{Z}/2 \times \mathbb{Z}/4$
$\mathbb{Q}_2(\sqrt{5})$	$\mathfrak{p}$	$\langle w\rangle$	$\mathbb{Z}/3$
$\mathbb{Q}_2(\sqrt{5})$	$\mathfrak{p}^2$	$\langle -w+2\rangle \times \langle -1\rangle \times \langle 2w+1\rangle$	$\mathbb{Z}/3 \times \mathbb{Z}/2 \times \mathbb{Z}/2$
$\mathbb{Q}_2(\sqrt{5})$	$\mathfrak{p}^3$	$\langle 3w+2\rangle \times \langle 4w+1\rangle \times \langle 3\rangle \times \langle 2w+1\rangle$	$\mathbb{Z}/3 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/4$
$\mathbb{Q}_2(\sqrt{5})$	$\mathfrak{p}^4$	$\langle -5w+2\rangle \times \langle 4w+1\rangle \times \langle 8w-1\rangle \times \langle 2w+1\rangle$	$\mathbb{Z}/3 \times \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/8$
$\mathbb{Q}_2(\sqrt{\pm 2})$	$\mathfrak{p}^5$	$\langle -3\rangle \times \langle w+1\rangle \times \langle 2w+1\rangle$	$\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/2$
$\mathbb{Q}_2(\sqrt{\pm 10})$	$\mathfrak{p}^5$	$\langle -3\rangle \times \langle w+1\rangle \times \langle 2w+1\rangle$	$\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/2$
$\mathbb{Q}_2(\sqrt{-1})$	$\mathfrak{p}^3$	$\langle w+2\rangle$	$\mathbb{Z}/4$
$\mathbb{Q}_2(\sqrt{-1})$	$\mathfrak{p}^4$	$\langle w+2\rangle \times \langle 2w-1\rangle$	$\mathbb{Z}/4 \times \mathbb{Z}/2$
$\mathbb{Q}_2(\sqrt{-1})$	$\mathfrak{p}^6$	$\langle -3\rangle \times \langle w+2\rangle \times \langle 2w-1\rangle$	$\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/4$
$\mathbb{Q}_2(\sqrt{-5})$	$\mathfrak{p}^3$	$\langle w+2\rangle$	$\mathbb{Z}/4$
$\mathbb{Q}_2(\sqrt{-5})$	$\mathfrak{p}^4$	$\langle w+2\rangle \times \langle 2w-1\rangle$	$\mathbb{Z}/4 \times \mathbb{Z}/2$
$\mathbb{Q}_2(\sqrt{-5})$	$\mathfrak{p}^6$	$\langle -3\rangle \times \langle w+2\rangle \times \langle -2w+3\rangle$	$\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/4$

$s \in G_{\mathbb{Q}_2}$ be a lift of the non-trivial element of $\mathrm{Gal}(M/\mathbb{Q}_\ell)$. For an integer d denote by ϵ_d the restriction to inertia of the character of $G_{\mathbb{Q}_2}$ fixing $\mathbb{Q}_2(\sqrt{d})$.

The objective of this section is to prove Theorem 8.1. All the relevant inertial types are defined in Tables 3 and 4.

From Lemma 4.2, we know that the semistability defect of an elliptic curve $E/\mathbb{Q}_2$, with potentially good reduction, is $e = 2, 3, 4, 6, 8, 24$, and that Φ is non-abelian if and only if $e = 8$ or 24. The following proposition shows that E has an exceptional inertial type if and only if $e = 24$.

Let us recall the explicit definition of some characters ϵ_d that we shall need.

ϵ_{-1} : has conductor 2^2 and is defined on $(\mathbb{Z}_2/2^2)^\times$ by

$$\epsilon_{-1}(-1) = -1.$$

ϵ_2 : has conductor 2^3 and is defined on $(\mathbb{Z}_2/2^3)^\times$ by

$$\epsilon_2(-1) = 1, \quad \epsilon_2(5) = -1.$$

ϵ_{-2} : has conductor 2^3, satisfies $\epsilon_{-2} = \epsilon_{-1}\epsilon_2$ and is defined on $(\mathbb{Z}_2/2^3)^\times$ by

$$\epsilon_2(-1) = -1, \quad \epsilon_2(5) = -1.$$

Note also that $\epsilon_2 = \epsilon_{10}$ and $\epsilon_{-2} = \epsilon_{-10}$.

Theorem 8.1. *Let $E/\mathbb{Q}_2$ be an elliptic curve with additive potentially good reduction, conductor N_E, semistability defect e and inertial type τ. Suppose further that $e \neq 24$, so that τ is not exceptional. Then,*

(1) if $e = 2$ then τ is trivial after a quadratic twist;
(2) if $N_E = 2^2$ then $e = 3$ and $\tau = \tau_{\sqrt{5},2}$;
(3) if $N_E = 2^4$ then $e = 6$ and $\tau = \tau_{\sqrt{5},2} \otimes \epsilon_{-1}$;
(4) if $N_E = 2^5$ then $e = 8$ and $\tau = \tau_{\sqrt{-1},5}$ or $\tau = \tau_{\sqrt{-5},5}$;
(5) if $N_E = 2^6$ then $e = 6$ or $e = 8$ and, moreover, we have
 - if $e = 6$ then $\tau = \tau_{\sqrt{5},2} \otimes \epsilon_2$ or $\tau_{\sqrt{5},2} \otimes \epsilon_{-2}$;
 - if $e = 8$ then $\tau = \tau_{\sqrt{-1},5} \otimes \epsilon_2$ or $\tau_{\sqrt{-5},5} \otimes \epsilon_2$;
(6) if $N_E = 2^8$ then $e = 4$ or $e = 8$ and, moreover, we have
 - if $e = 4$ then τ_2, $\tau_2 \otimes \epsilon_{-1}$, $\tau_{\sqrt{5},8}$, $\tau_{\sqrt{5},8} \otimes \epsilon_{-1}$;
 - if $e = 8$ then $\tau_{\sqrt{-5},8}$ or $\tau_{\sqrt{-5},8} \otimes \epsilon_2$

8.1. **Principal Series.**

Proposition 8.2. *Let $E/\mathbb{Q}_2$ be an elliptic curve with additive potentially good reduction, semistability defect $e \neq 2$, conductor N_E and inertial type τ. Suppose further that τ is a principal series. Then $N_E = 2^8$, $e = 4$ and $\tau \simeq \tau_2$ or $\tau_2 \otimes \epsilon_{-1}$.*

Proof. We have $\mathrm{cond}(\tau) = 2^{2m}$ with $1 \leq m \leq 4$ by Lemma 4.1 and the conductor formula for principal series. Thus $\tau = \chi|_{I_2} \oplus \chi^{-1}|_{I_2}$, where $\chi|_{I_2}$ factors through $(\mathbb{Z}_2/2^m)^\times$.

If $m = 1, 2$ or 3, then $\chi|_{I_2}$ is at most quadratic. Hence $e = 1$ or 2, which is a contradiction; thus $m = 4$. Since $(\mathbb{Z}_2/2^4)^\times = \langle -1 \rangle \times \langle 5 \rangle = \mathbb{Z}/2 \times \mathbb{Z}/4$ (see Table 1), we must have $\chi(5) = \pm i$. If $\chi(-1) = 1$, then $\chi|_{I_2} = \chi_{4,4}$ or $\chi_{4,4}^{-1}$, yielding that $\tau = \tau_2$. If $\chi(-1) = -1$, then $\tau = \tau_2 \otimes \epsilon_{-1}$. ☐

8.2. **Inductions from $M/\mathbb{Q}_2$ of conductor 2^3.** Let $M = \mathbb{Q}_2(\sqrt{d})$ with $d = \sqrt{\pm 2}, \sqrt{\pm 10}$, so that $M/\mathbb{Q}_2$ is quadratic ramified of conductor 2^3. (These are the four quadratic extensions $M/\mathbb{Q}_2$ with that conductor.) Let $s \in G_{\mathbb{Q}_2}$ be a lift of the non-trivial element of $\mathrm{Gal}(M/\mathbb{Q}_2)$.

From [17, Corollary 4.1] and Lemma 4.1, it follows that an elliptic curve $E/\mathbb{Q}_2$ with a supercuspidal type τ induced from one of these M must have conductor $N_E = 2^8$. The following proposition shows this cannot happen if E has additive potentially good reduction.

Proposition 8.3. *Let $E/\mathbb{Q}_2$ be an elliptic curve with additive potentially good reduction, semistability defect e, conductor $N_E = 2^8$ and inertial type τ. Suppose further that τ is imprimitive supercuspidal induced from a quadratic extension $M/\mathbb{Q}_2$.*

Then M does not have conductor 2^3.

Proof. Suppose that $\rho_E = \mathrm{Ind}_{W_M}^{W_2} \chi$ for a character $\chi : W_M \to \mathbb{C}^\times$, where $M/\mathbb{Q}_2$ has conductor 2^3. This means that $M = \mathbb{Q}_2(d)$ with $d = \sqrt{\pm 2}, \sqrt{\pm 10}$. Write $\mathfrak{p}$ for the prime ideal in M. Since $\mathrm{cond}(\rho_E) = 2^8$, the conductor formula (2.4) implies $\mathrm{cond}(\chi) = \mathfrak{p}^5$.

For $M = \mathbb{Q}_2(d)$, with $d = \pm 2, \pm 10$, we have

$$(\mathcal{O}_M/\mathfrak{p}^5)^\times = \langle -3 \rangle \times \langle w + 1 \rangle \times \langle 2w + 1 \rangle \simeq \mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/2.$$

Recall that $\chi|_{\mathbb{Z}_2^\times} = \epsilon_d$.

Suppose $d = \sqrt{-2}$ or $\sqrt{-10}$. Since χ has conductor $\mathfrak{p}^5$, we must have $\chi(-3) = -1$. Note that $(\mathbb{Z}_2/2^3)^\times = \langle -1 \rangle \times \langle 5 \rangle \subset (\mathcal{O}_M/\mathfrak{p}^5)^\times$; therefore $\chi|_{\mathbb{Z}_2^\times} = \epsilon_d$ implies

$$\chi(5) = \chi(-3) = -1 \qquad \text{and} \qquad \chi(-1) = \chi(w+1)^2\chi(2w+1) = -1$$

which can be restated as the following two cases

$$(i) \quad \begin{cases} \chi(-3) = -1 \\ \chi(1+w) = \pm i \\ \chi(1+2w) = 1 \end{cases} \qquad \text{or} \qquad (ii) \quad \begin{cases} \chi(-3) = -1 \\ \chi(1+w) = \pm 1 \\ \chi(1+2w) = -1. \end{cases}$$

For $d = 2, 10$, the same conclusion holds. Indeed, the conductor implies that $\chi(-3) = -1$ and from $\chi|_{\mathbb{Z}_2^\times} = \epsilon_d$ we get $\chi(5) = \chi(-3) = -1$ and $\chi(-1) = \chi(-3)\chi(1+w)^2\chi(1+2w) = 1$, leading to the same cases (i) and (ii) above.

Suppose now that $M = \mathbb{Q}_2(d)$, with $d = \sqrt{-2}$, and that χ satisfies case (i). One verifies that

$$(\chi/\chi^s)(-3) = (\chi/\chi^s)(2w+1) = 1, \text{ and } (\chi/\chi^s)(w+1) = -1,$$

so χ does not factor via the norm. In particular, σ_E is irreducible and since $\tau = \sigma_E|_{I_M}$ it follows from Proposition 3.1 and Lemma 4.2 that $e = 8$.

Moreover, we have that d is an uniformizer in M and $\chi^s(d) = \chi(-d) = \chi(-1)\chi(d) = -\chi(d)$, therefore $(\chi/\chi^s)(d) = -1$ and it now is easy to check that

$$(\chi/\chi^s)(x) = (\epsilon_{-5} \circ \mathrm{Nm}_{M/\mathbb{Q}_2})(x).$$

We conclude that σ_E is triply imprimitive by [6, Section 41.3] and it follows from [15, Section 2.7] that σ_E has projective image $\mathbb{P}(\sigma_E) \simeq D_2 \simeq C_2 \times C_2$.

On the other hand, from [12, Lemma 1] there is a twist of σ_E factoring via $K = \mathbb{Q}_2(E[3])$, so $\mathbb{P}(\sigma_E) \simeq \mathbb{P}(\overline{\rho}_{E,3})$. From [12, Table 1] we see that if $e = 8$ (hence $\Phi \simeq H_8$) then $\overline{\rho}_{E,3}(G_{\mathbb{Q}_2}) \subset \mathrm{GL}_2(\mathbb{F}_3)$ is the 2-Sylow subgroup which does not satisfy $\mathbb{P}(\overline{\rho}_{E,3}) \simeq C_2 \times C_2$, giving a contradiction.

A similar argument leads to contradictions also for $d = \sqrt{2}, \sqrt{\pm 10}$ when χ satisfies (i). Finally, when χ is given by (ii), one verifies that, for all d, $\chi|_{I_M} = (\chi|_{I_M})^s$. So, χ factors through the norm map and does not give rise to a supercuspidal type. $\square$

8.3. **Inductions from $M/\mathbb{Q}_2$ unramified.** Let $M = \mathbb{Q}_2(\sqrt{5})$, so that M is quadratic unramified, and $s \in G_{\mathbb{Q}_2}$ be a lift of the non-trivial element of $\mathrm{Gal}(M/\mathbb{Q}_2)$.

Proposition 8.4. *Let $E/\mathbb{Q}_2$ be an elliptic curve with additive potentially good reduction, semistability defect $e \neq 2$, conductor N_E and inertial type τ. Suppose further that τ is supercuspidal obtained by inducing a character χ of W_M, where $M = \mathbb{Q}_2(\sqrt{5})$. Then,*

1. *if $N_E = 2^2$ then $e = 3$ and $\tau = \tau_{\sqrt{5},2}$,*
2. *if $N_E = 2^4$ then $e = 6$ and $\tau = \tau_{\sqrt{5},2} \otimes \epsilon_{-1}$,*
3. *if $N_E = 2^6$ then $e = 6$ and $\tau = \tau_{\sqrt{5},2} \otimes \epsilon_2$ or $\tau = \tau_{\sqrt{5},2} \otimes \epsilon_{-2}$,*
4. *if $N_E = 2^8$ then $e = 4$ and τ is $\tau_{\sqrt{5},8}$ or $\tau_{\sqrt{5},8} \otimes \epsilon_{-1}$.*

Table 4. Galois inertial types attached the characters at $\ell = 2$

M	$\mathfrak{f}$	χ	χ on generators	τ	cond(τ)
$\mathbb{Q}_2$	2^4	$\chi_{4,4}$	$1,\ i$	$\tau_2 = \mathrm{PS}(\chi_{4,4})\|_{I_2}$	2^8
$\mathbb{Q}_2(\sqrt{5})$	$\mathfrak{p}$	$\chi_{d,1}$	ζ_3	$\tau_{d,2} = \mathrm{BC}(\chi_{d,1})\|_{I_2}$	2^2
	$\mathfrak{p}^4$	$\chi_{d,4}$	$1,\ i,\ -1,\ i$	$\tau_{d,8} = \mathrm{BC}(\chi_{d,4})\|_{I_2}$	2^8
$\mathbb{Q}_2(\sqrt{\pm 2})$	$\mathfrak{p}^5$	$\chi_{d,5}$	$-1,\ i,\ 1$	$\tau_{d,8} = \mathrm{BC}(\chi_{d,5})\|_{I_2}$	2^8
	$\mathfrak{p}^5$	$\chi'_{d,5}$	$-1,\ 1,\ -1$	$\tau'_{d,8} = \mathrm{BC}(\chi'_{d,5})\|_{I_2}$	2^8
$\mathbb{Q}_2(\sqrt{\pm 10})$	$\mathfrak{p}^5$	$\chi_{d,5}$	$-1,\ i,\ 1$	$\tau_{d,8} = \mathrm{BC}(\chi_{d,5})\|_{I_2}$	2^8
	$\mathfrak{p}^5$	$\chi'_{d,5}$	$-1,\ 1,\ -1$	$\tau'_{d,8} = \mathrm{BC}(\chi'_{d,5})\|_{I_2}$	2^8
$\mathbb{Q}_2(\sqrt{-1})$	$\mathfrak{p}^3$	$\chi_{d,3}$	i	$\tau_{d,5} = \mathrm{BC}(\chi_{d,3})\|_{I_2}$	2^5
	$\mathfrak{p}^6$	$\chi_{d,6}$	$1,\ 1,\ i$	$\tau_{d,8} = \mathrm{BC}(\chi_{d,6})\|_{I_2}$	2^8
$\mathbb{Q}_2(\sqrt{-5})$	$\mathfrak{p}^3$	$\chi_{d,3}$	i	$\tau_{d,5} = \mathrm{BC}(\chi_{d,3})\|_{I_2}$	2^5
	$\mathfrak{p}^6$	$\chi_{d,6}$	$1,\ 1,\ i$	$\tau_{d,8} = \mathrm{BC}(\chi_{d,6})\|_{I_2}$	2^8
	$\mathfrak{p}^6$	$\chi'_{d,6}$	$1,\ -1,\ i$	$\tau'_{d,8} = \mathrm{BC}(\chi'_{d,6})\|_{I_2}$	2^8

Proof. Since $M/\mathbb{Q}_2$ is unramified then $I_2 \subset W_M$ and we are in case Proposition 3.2 (iii). So τ has abelian image and $e = 3, 4$ or 6. The conductor of τ is 2^{2m}, which means that χ has conductor $\mathfrak{p}^m$ with $m \leq 4$. We will now determine the possibilities for $\chi|_{\mathcal{O}_M^\times}$.

Suppose $m = 1$; then $N_E = 2^2$, and the reduction is tame, hence $e = 3$. Since $(\mathcal{O}_M/\mathfrak{p})^\times = \langle w \rangle = \mathbb{Z}/3$, we must have $\chi(w) = \zeta_3^c$ with $c = 1$ or 2. Therefore, $\chi|_{I_2} = \chi_{\sqrt{5},1}$ or $\chi_{\sqrt{5},1}^s$ since it doesn't factor through the norm. Thus $\tau \simeq \tau_{\sqrt{5},2}$, proving (1).

Suppose $m = 2$. Then, from Table 3, we have

$$(\mathbb{Z}_2/2^2)^\times \subset (\mathcal{O}_M/\mathfrak{p}^2)^\times = \langle -w+2 \rangle \times \langle -1 \rangle \times \langle 2w+1 \rangle \simeq \mathbb{Z}/3 \times \mathbb{Z}/2 \times \mathbb{Z}/2.$$

Since $\chi|_{\mathbb{Z}_2^\times} = 1$, we must have $\chi(-1) = 1$. Also, $\chi(2w+1) = -1$ since χ has conductor $\mathfrak{p}^2$. Therefore $\chi(-w+2) = \zeta_3^c$ with $c = 1$ or 2; otherwise, χ would factor through the norm. We conclude there are two choices for $\chi|_{I_2}$, which must be conjugate. They give rise to the same type τ' of conductor 2^4. But, twisting an elliptic curve with inertial type $\tau_{\sqrt{5},2}$ by -1, gives an elliptic curve of conductor 2^4 and inertial type $\tau_{\sqrt{5},2} \otimes \epsilon_{-1}$. Since τ' is the unique inertial type of conductor 2^4, we must have $\tau' = \tau_{\sqrt{5},2} \otimes \epsilon_{-1}$. This proves (2).

Suppose $m = 3$. Then, from Table 3, we have

$$(\mathbb{Z}_2/2^3)^\times \subset (\mathcal{O}_M/\mathfrak{p}^3)^\times = \langle 3w+2 \rangle \times \langle 4w+1 \rangle \times \langle 3 \rangle \times \langle 2w+1 \rangle \simeq \mathbb{Z}/3 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/4.$$

Since $\chi|_{\mathbb{Z}_2^\times} = 1$, it follows that

$$\chi(-1) = \chi(3)\chi(2w+1)^2 = 1 \quad \text{and} \quad \chi(5) = \chi(2w+1)^2 = 1.$$

Hence $\chi(2w+1) = \pm 1$. Since χ has conductor $\mathfrak{p}^3$, we must have $\chi(4w+1) = -1$ or $\chi(2w+1) = \pm i$. But, the latter is incompatible, thus $\chi(4w+1) = -1$. Since χ doesn't factor through the norm, we see that $\chi(3w+2) = \zeta_3^c$ with $c = 1$ or 2. This gives four possibilities for $\chi|_{I_2}$ yielding two pairs of conjugate characters, and hence two possible inertial types τ of conductor 2^6. But, twisting an elliptic curve with inertial type $\tau_{\sqrt{5},2}$ by 2 (resp. -2) gives an elliptic curve of conductor 2^6 and inertial type $\tau_{\sqrt{5},2} \otimes \epsilon_2$ (resp. $\tau_{\sqrt{5},2} \otimes \epsilon_{-2}$). So, $\tau_{\sqrt{5},2} \otimes \epsilon_2$ and $\tau_{\sqrt{5},2} \otimes \epsilon_{-2}$ must correspond to the two inertial types described above. This proves (3).

Suppose $m = 4$. Then, from Table 3, we have

$(\mathbb{Z}_2/2^4)^\times \subset (\mathcal{O}_M/\mathfrak{p}^4)^\times = \langle -5w+2\rangle \times \langle 4w+1\rangle \times \langle 8w-1\rangle \times \langle 2w+1\rangle = \mathbb{Z}/3\times\mathbb{Z}/4\times\mathbb{Z}/2\times\mathbb{Z}/8.$

So, from $\chi|_{\mathbb{Z}_2^\times} = 1$, it follows $\chi(-1) = \chi(5) = 1$. A little calculation then shows that

$$\chi(4w+1)^2 = \chi(8w-1) = \chi(2w+1)^2 = \pm 1.$$

Hence, in particular, $\chi(2w+1)^4 = 1$. Since, χ has conductor $\mathfrak{p}^4$, we must $\chi(4w+1) = \pm i$ or $\chi(2w+1)$ has order 8. But the latter is impossible, so $\chi(4w+1) = \pm i$. From the above equalities, it then follows that $\chi(8w-1) = -1$ and $\chi(2w+1) = \pm i$.

One checks further that $\chi(4\bar{w}+1) = \chi(4w+1)\chi(2w+1)^2 = -\chi(4w+1)$, where $\bar{w}$ denotes the Galois conjugate of w, hence χ does not factor via the norm. Therefore, $\chi(-5w+2) = \zeta_3^c$ with $c = 0, 1$ or 2. If $c \neq 0$, then the image of $\chi|_{I_2}$ has size $e = 12$ which is a contradiction, so $c = 0$. This shows that there are four possibilites for $\chi|_{I_2}$ which are

$$\chi_{\sqrt{5},4}, \quad \chi_{\sqrt{5},4}^s = \chi_{\sqrt{5},4}\epsilon_{-2}, \quad \chi_{\sqrt{5},4}\epsilon_{-1}, \quad (\chi_{\sqrt{5},4}\epsilon_{-1})^s = \chi_{\sqrt{5},4}\epsilon_2$$

and we conclude $\tau \simeq \tau_{\sqrt{5},8}$ or $\tau_{\sqrt{5},8} \otimes \epsilon_{-1}$, as desired. □

8.4. **Inductions from $M/\mathbb{Q}_2$ of conductor 2^2.** Let $M = \mathbb{Q}_2(\sqrt{d})$ with $d = \sqrt{-1}, \sqrt{-5}$, so that $M/\mathbb{Q}_2$ is quadratic ramified of conductor 2^2. Let $s \in G_{\mathbb{Q}_2}$ be a lift of the non-trivial element of $\mathrm{Gal}(M/\mathbb{Q}_2)$.

Proposition 8.5. *Let $E/\mathbb{Q}_2$ be an elliptic curve with additive potentially good reduction, semistability defect $e \neq 2$, conductor N_E and inertial type τ. Suppose further that τ is supercuspidal obtained by inducing a character χ of W_M, where M has conducotr 2^2.*

Then,

1. *if $N_E = 2^5$ then $e = 8$ and $\tau = \tau_{\sqrt{-1},5}$ or $\tau_{\sqrt{-5},5}$;*
2. *if $N_E = 2^6$ then $e = 8$ and $\tau = \tau_{\sqrt{-1},5} \otimes \epsilon_2$ or $\tau_{\sqrt{-5},5} \otimes \epsilon_2$;*
3. *if $N_E = 2^8$ then τ is $\tau_{\sqrt{-1},8}$ or $\tau_{\sqrt{-1},8} \otimes \epsilon_2$.*

Proof. From Lemma 4.1 and [17, Corollary 4.1] it follows that $\mathrm{cond}(\tau) = N_E = 2^k$ with $k = 5, 6, 8$, thus χ is of conductor $\mathfrak{p}^m$ with $m = k - 2 = 3, 4, 6$, respectively. We will now determine the possibilities for $\chi|_{\mathcal{O}_M^\times}$.

Case: $d = \sqrt{-1}$

Note that $\chi|_{\mathbb{Z}_2^\times} = \epsilon_d$ implies $\chi(-1) = -1$, so that χ does not factor through the norm.

Suppose $m = 3$. We have that $(\mathcal{O}_M/\mathfrak{p}^3)^\times = \langle w+2\rangle \simeq \mathbb{Z}/4$. Since χ has conductor $\mathfrak{p}^3$, we must have $\chi(2+d) = \pm i$; this gives two conjugate characters, hence $\tau = \tau_{\sqrt{-1},5}$.

Suppose $m = 4$. Then, we have that $(\mathcal{O}_M/\mathfrak{p}^4)^\times = \langle w+2\rangle \times \langle 2w-1\rangle \simeq \mathbb{Z}/4\times\mathbb{Z}/2$. Since χ has conductor $\mathfrak{p}^4$, we must have $\chi(2w-1) = -1$. From $\chi|_{\mathbb{Z}_2^\times} = \epsilon_d$, it follows $\chi(-1) = \chi(w+2)^2 = -1$, hence $\chi(w+2) = \pm i$. So, we again have two conjugate choices, leading to one possible type τ'. But, twisting an elliptic curve with inertial type $\tau_{\sqrt{-1},5}$ by 2, we obtain an elliptic curve with conductor 2^6 and inertial type $\tau_{\sqrt{-1},5} \otimes \epsilon_2$. So by uniqueness, we must have $\tau' = \tau_{\sqrt{-1},5} \otimes \epsilon_2$. This proves (2).

Suppose $m = 6$. Then, we have that $(\mathcal{O}_M/\mathfrak{p}^6)^\times = \langle -3 \rangle \times \langle w+2 \rangle \times \langle 2w-1 \rangle \simeq \mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/4$. Since χ is primitive, we must have $\chi(2w-1) = \pm i$. From $\chi|_{\mathbb{Z}_2^\times} = \epsilon_d$ it follows that $\chi(5) = \chi(-3) = 1$ and

$$\chi(-1) = \chi(w+2)^2 \chi(2w-1)^2 = \chi(w+2)^2 \cdot (-1) = -1$$

hence $\chi(w+2) = \pm 1$. There are four possible characters which are

$$\chi_{\sqrt{-1},6}, \quad \chi^s_{\sqrt{-1},6}, \quad \chi_{\sqrt{-1},6} \cdot \epsilon_2, \quad (\chi_{\sqrt{-1},6} \cdot \epsilon_2)^s,$$

hence $\tau = \tau_{\sqrt{-1},8}$ or $\tau_{\sqrt{-1},8} \otimes \epsilon_2$.

Case: $d = \sqrt{-5}$

Note that $\chi|_{\mathbb{Z}_2^\times} = \epsilon_d$ implies $\chi(-1) = -1$, hence χ does not factor through the norm. For $m = 3, 4$, the same argument as for $d = -1$ applies (see Table 3 for group structures).

Suppose $m = 6$. Then, we have that

$$(\mathcal{O}_M/\mathfrak{p}^6)^\times = \langle -3 \rangle \times \langle w+2 \rangle \times \langle -2w+3 \rangle \simeq \mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/4.$$

Since χ is primitive, we must have $\chi(-2w+3) = \pm i$. From $\chi|_{\mathbb{Z}_2^\times} = \epsilon_d$, we get $\chi(5) = \chi(-3) = 1$ and

$$\chi(-1) = \chi(-3)\chi(w+2)^2 \chi(-2w+3)^2 = \chi(w+2)^2 \cdot (-1) = -1$$

hence $\chi(w+2) = \pm 1$. Again, there are four possible characters $\chi|_{I_M}$, which can be written as

$$\chi_1, \quad \chi_1^s = \chi_1 \cdot \epsilon_2, \quad \chi_2, \quad \chi_2^s = \chi_2 \cdot \epsilon_2,$$

where we have fixed certain choice for χ_1 and χ_2 among the four possibilities.

In particular, χ/χ^s factors through the norm, so σ_E is triply imprimitive. This leads to a contradiction similarly to the proof of Proposition 8.3. We conclude there are no types arising from an elliptic curve for $m = 6$ and $d = \sqrt{-5}$. ☐

8.5. **Proof of Main Theorem.** We now combine the results of the section to prove Theorem 8.1.

Proof of Theorem 8.1. We have $e \neq 24$ by Proposition 4.4.

Part (1) is Proposition 4.3, so we can assume also $e \neq 2$.

We know that τ is either principal series or imprimitive supercuspidal.

Suppose τ is principal series. From Proposition 8.2 it follows that $N_E = 2^8$, $e = 4$ and $\tau \simeq \tau_2$ or $\tau_2 \otimes \epsilon_{-1}$. Suppose now τ is supercuspidal and $N_E = 2^8$. Then Proposition 8.3 implies it is induced from a quadratic extension $M/\mathbb{Q}_2$ with M unramified or of conductor 2^2. In the former case we have $e = 4$ and $\tau \simeq \tau_{\sqrt{5},8}$ or $\tau_{\sqrt{5},8} \otimes \epsilon_{-1}$; in the latter case we have $e = 8$ and $\tau \simeq \tau_{\sqrt{-1},8}$, $\tau_{\sqrt{-1},8} \otimes \epsilon_2$. This concludes the proof of part (6).

The above also shows that, for the remaining cases, we can asume τ is imprimitive supercuspidal with conductor $\neq 2^8$. Thus from [17, Corollary 4.1] we know that τ is induced from M with conductor 2^0 or 2^2 and, in particular, we are under the hypothesis of either Proposition 8.4 or Proposition 8.5. The remaining cases now follow directly from these two propositions. □

9. Exceptional inertial types for $E/\mathbb{Q}_2$

Let $r = \pm 1, \pm 2$ and define the following elliptic curves over $\mathbb{Q}_2$

$$E_{1,r} : ry^2 = x^3 + 3x + 2 \qquad \text{and} \qquad E_{2,r} : ry^2 = x^3 - 3x + 1. \tag{9.1}$$

We define $\tau_{ex,1}$ and $\tau_{ex,2}$ to be the inertial types of $E_{1,1}$ and $E_{2,-1}$, more precisely,

$$\tau_{ex,1} = \sigma_{E_{1,1}}|_{I_2} \quad \text{and} \quad \tau_{ex,2} = \sigma_{E_{2,-1}}|_{I_2}.$$

Theorem 9.2. *Let $E/\mathbb{Q}_2$ be an elliptic curve with additive potentially good reduction, semistability defect $e = 24$, conductor N_E and inertial type τ. Then,*

(1) if $N_E = 2^3$ then $\tau = \tau_{ex,2}$;
(2) if $N_E = 2^4$ then $\tau = \tau_{ex,2} \otimes \epsilon_{-1}$;
(3) if $N_E = 2^6$ then $\tau = \tau_{ex,2} \otimes \epsilon_2$ or $\tau = \tau_{ex,2} \otimes \epsilon_{-2}$;
(4) if $N_E = 2^7$ then τ is one of $\tau_{ex,1}$, $\tau_{ex,1} \otimes \epsilon_{-1}$, $\tau_{ex,1} \otimes \epsilon_2$, $\tau_{ex,1} \otimes \epsilon_{-2}$;

Proof. Let $K = \mathbb{Q}_2(E[3])$, $G = \mathrm{Gal}(K/\mathbb{Q}_2)$ and $L = \mathbb{Q}_2^{un}K$ be the inertial field of E. From the proof of Proposition 4.4, we know that $G \simeq \mathrm{GL}_2(\mathbb{F}_3) \simeq \tilde{S}_4$ which is a double cover of $\mathbb{P}(\overline{\rho}_{E,3}) \simeq S_4$. From [1, Table 10] we see that all the $\tilde{S}_4$ extensions $K/\mathbb{Q}_2$ are of the form $K = \mathbb{Q}_2(E_{i,r}[3])$, where $E_{i,r}$ is one of the curves defined in (9.1). Thus both τ and $\tau_{i,r} = \rho_{E_{i,r}}|_{I_2}$ fix the extension $L/\mathbb{Q}_2^{un}$. We have $\mathrm{Gal}(L/\mathbb{Q}_2^{un}) \simeq \Phi \simeq \mathrm{SL}_2(\mathbb{F}_3)$ by Lemma 4.2, and since there is only one irreducble $\mathrm{GL}_2(\mathbb{C})$-representation of $\mathrm{SL}_2(\mathbb{F}_3)$ whose image is contained in $\mathrm{SL}_2(\mathbb{C})$, we conclude that $\tau \simeq \tau_{i,r}$.

Finally, note that, for $r = -1, 2, -2$, the curve $E_{2,-r}$ is the quadratic twist of $E_{2,-1}$ by r, so that the inertial type of $E_{2,-r}$ is $\tau_{ex,2} \otimes \epsilon_r$. Similarly, the inertial type of $E_{1,r}$ is $\tau_{ex,1} \otimes \epsilon_r$. Moreover, the conductor of $E_{1,1}$ is 2^7 and that of $E_{2,-1}$ is 2^3, thus the eight types split in the 4 cases of the theorem according to their conductors. □

Recall that, as in previous sections, we aim for an explicit description of the types in Theorem 9.2 in terms of characters. As explained in Section 2.3.2, an exceptional type is determined by a triple (K, M, χ), where $K/\mathbb{Q}_2$ is a cubic extension, M/K a quadratic and $\chi : W_M \to \mathbb{C}^\times$ a character that we only need to specify on I_M. We now define two inertial types this way.

Let $M_i = \mathbb{Q}_2(b_i)$ for $i = 1, 2$ be the degree 6 extensions defined by the Eisenstein polynomials

$$f_1 := x^6 - 6x^5 + 18x^4 - 32x^3 + 36x^2 - 24x + 10;$$
$$f_2 := x^6 - 198x^5 + 10728x^4 - 88434x^3 + 249264x^2 - 9882x + 918.$$

We recall that b_i is a uniformizer in M_i, and that $\mathcal{O}_{M_i} = \mathbb{Z}_2[b_i]$, and write $\mathfrak{p}_i = (b_i)$ for the unique prime ideal of $\mathcal{O}_{M_i}$.

Let $\chi_2 : W_{M_2} \to \mathbb{C}^\times$ be a character, with conductor $\mathfrak{p}_2^3$, whose restriction $\chi_2|_{I_{M_2}}$ is given by $\chi_2(1+b_2) = i$. Also let $\chi_1 : W_{M_1} \to \mathbb{C}^\times$ be a character of conductor $\mathfrak{p}_1^{11}$ such that $\chi_1|_{I_{M_1}}$ is given by

$$\chi_1(u_3) = i, \quad \chi_1(u_1) = \chi_1(u_2) = \chi_1(u_4) = \chi_1(u_5) = -1.$$

where

$$(\mathcal{O}_{M_1}/\mathfrak{p}_1^{11})^\times = \langle u_1 \rangle \times \langle u_2 \rangle \times \langle u_3 \rangle \times \langle u_4 \rangle \times \langle u_5 \rangle \simeq \mathbb{Z}/16 \times \mathbb{Z}/4 \times \mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2,$$

and

$$\begin{array}{ll} u_1 := b_1 + 1, & \\ u_2 := b_1^3 + 1, & u_4 := 2b_1 + 1, \\ u_3 := b_1^5 + 1, & u_5 := 2b_1^3 + 1. \end{array}$$

Note that, for $i = 1, 2$, $M_i/\mathbb{Q}_2(u)$, where u is a root of $x^3 - 2$, is a quadratic extension. We let $K_1 = K_2 = \mathbb{Q}_2(u)$, and define $\tau_{1,1}$ and $\tau_{2,-1}$ to be the inertial types determined by (K_1, M_1, χ_1) and (K_2, M_2, χ_2), respectively.

Lemma 9.3. *The following equalities of inertial types are satisfied:*

$$\tau_{ex,1} = \tau_{1,1} \qquad \textit{and} \qquad \tau_{ex,2} = \tau_{2,-1}.$$

Proof. We will write E for $E_{1,1}$ or $E_{2,-1}$. Let τ be the inertial type of E and $(K, M, \chi|_{I_M})$ be the triple determining τ, so that $K/\mathbb{Q}_2$ is cubic, M/K is quadratic and $\sigma_E|_{W_K}$ is an imprimitive representation.

From [12, Lemma 1] there is an unramified twist $\sigma = \sigma_E \otimes \mu$ which factors via $L = \mathbb{Q}_2(E[3])$; since $\tau = (\sigma_E \otimes \mu)|_{I_2} = \sigma|_{I_2}$ we can work with σ. Note also that $\mathbb{P}(\sigma_E) = \mathbb{P}(\sigma)$.

Write $L_x \subset L$ for the subfield generated by the x-coordinates of the 3-torsion points of E. From the proof Theorem 9.2, we have that $G := \mathrm{Gal}(L/\mathbb{Q}_2) \simeq \mathrm{GL}_2(\mathbb{F}_3) \simeq \tilde{S}_4$ and $\mathbb{P}(\sigma_E)$ factors via $G_x := \mathrm{Gal}(L_x/\mathbb{Q}_2) \simeq S_4$.

The above shows that the image of σ has order 48, $\sigma|_{W_K}$ is an imprimitive supercuspidal representation and $\sigma|_{W_M} = \chi \oplus \chi^s$, where s is conjugation in M/K and $\chi \neq \chi^s$.

Let $H \subset G$ be the subgroup fixing M. Since M is of degree 6 and $\sigma|_{W_M} = \chi \oplus \chi^s$, it follows that H is cyclic of order 8. Up to conjugation, there is only one cyclic subgroup of $\tilde{S}_4$ of order 8, which must correspond to H. Since $e = 24$, $|H| = 8$ and $M/\mathbb{Q}_2$ is totally ramified of degree 6, we see that χ is of order 8; but $\chi|_{I_M}$ has order 4.

Case: $E = E_{2,-1}$

This means that $\tau = \tau_{ex,2}$. From [11, Proposition 2] we obtain that $L/\mathbb{Q}_2$ is the splitting field of the Eisenstein polynomial

$$h_1 = x^8 - 8x^7 + 26x^6 - 46x^5 + 50x^4 - 38x^3 + 22x^2 - 8x + 2.$$

One checks that f_2 splits completely over L. Thus, L contains the field M_2 in particular. In fact, one verifies that M_2 is the fixed field of H inside L. Since, h_1 is irreducible over M_2 and $K_2 \subset M_2$ is the unique cubic subfield, we conclude $K = K_2 \subset M = M_2$. To finish this case we need to show $\chi|_{I_M} = \chi_2|_{I_M}$.

Let $\mathfrak{p}$, $\mathfrak{p}_K$ be the primes in M, K; we have $\upsilon_{\mathfrak{p}_K}(\Delta(M/K)) = 2$ and the curve E/K has conductor $\mathfrak{p}_K^5$, hence χ has conductor $\mathfrak{p}^3$ by the conductor formula. We note that $(\mathcal{O}_M/\mathfrak{p}^3)^\times$ is generated by $b_2 + 1$. Since χ has conductor $\mathfrak{p}^3$, we must have $\chi(b_2 + 1) = \pm i$. This gives two choices for $\chi|_{I_M}$ which are conjugated by s, so we can take $\chi|_{I_M} = \chi_2|_{I_M}$ hence $\tau = \tau_{2,-1}$, as desired.

Case: $E = E_{1,1}$

This means that $\tau = \tau_{ex,1}$. From [11, Proposition 2], we obtain that $L/\mathbb{Q}_2$ is the splitting field of the Eisenstein polynomial

$$h_2 = x^8 - 28x^7 + 236x^6 - 280x^5 - 104x^4 - 392x^3 - 164x^2 - 112x + 2,$$

and $L_x/\mathbb{Q}_2$ is the splitting field of $g_2 := x^4 - 4x^3 + 4x + 2$ (obtained from the 3-division polynomial of E). As above, one checks that f_1 splits completely over L, and that M_1 is the fixed field of H inside L. Furthermore, h_2 and g_2 are irreducible over M_1 and $K_1 \subset M_1$ is the unique cubic subfield. We conclude $K = K_1 \subset M = M_1$. So, it remains to show that $\chi|_{I_M} = \chi_1|_{I_M}$.

Let $\mathfrak{p}, \mathfrak{p}_K$ be the primes in M, K. We have $\upsilon_{\mathfrak{p}_K}(\Delta(M/K)) = 6$ and the curve E/K has conductor $\mathfrak{p}_K^{17}$, hence χ has conductor $\mathfrak{p}^{11}$ by the conductor formula.

We recall that $(\mathcal{O}_M/\mathfrak{p}^{11})^\times$ is generated by u_1, u_2, u_3, u_4, u_5 of orders 16, 4, 4, 2, 2, respectively. Since χ is primitive, we must have $\chi(u_3) = \pm i$. Also, since χ fixes L and has order 4 on inertia, it follows that χ^2 fixes L_x and $\chi^2|_{I_M}$ has order 2.

From local class field theory, we know that χ^2 fixes L_x if and only if it is trivial on the norm group $\mathrm{Norm}_{L_x/M}(L_x)$. Using the `Magma` routine `NormEquation` we check which u_i are norms from elements in L_x and we conclude that

$$\chi^2(u_1) = \chi^2(u_2) = \chi^2(u_4) = \chi^2(u_5) = 1, \quad \chi^2(u_3) = -1.$$

Similarly, we check which u_i are norms from L/M to conclude that $\chi(u_i) \neq 1$ for all i. It follows that

$$\chi(u_1) = \chi(u_2) = \chi(u_4) = \chi(u_5) = -1, \quad \chi(u_3) = \pm i$$

where the two options are s-conjugated characters. Therefore, we can take $\chi|_{I_M} = \chi_1|_{I_M}$ hence $\tau = \tau_{1,1}$, as desired. ∎

References

[1] Pilar Bayer and Anna Rio. Dyadic exercises for octahedral extensions. *J. Reine Angew. Math.*, 517:1–17, 1999. 9

[2] Michael A. Bennett and Chris M. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004. 1

[3] N. Billerey, I. Chen, L. Dieulefait, and N. Freitas. A multi-frey approach to fermat equations of signature (r, r, p). Preprint, 2017. 1

[4] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001. 1

[5] Christophe Breuil and Ariane Mézard. Multiplicités modulaires et représentations de $\mathrm{GL}_2(\mathbf{Z}_p)$ et de $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ en $l = p$. *Duke Math. J.*, 115(2):205–310, 2002. With an appendix by Guy Henniart. 1, 3

[6] Colin J. Bushnell and Guy Henniart. *The local Langlands conjecture for* GL(2), volume 335 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2006. 2, 2.3, 2.3.2, 4, 8.2

[7] Henri Carayol. Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)*, 19(3):409–468, 1986. 2, 2.3

[8] Brian Conrad, Fred Diamond, and Richard Taylor. Modularity of certain potentially Barsotti-Tate Galois representations. *J. Amer. Math. Soc.*, 12(2):521–567, 1999. 1

[9] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140. Int. Press, Cambridge, MA, 1997. 4

[10] Fred Diamond. An extension of Wiles' results. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 475–489. Springer, New York, 1997. 1

[11] Tim Dokchitser and Vladimir Dokchitser. Root numbers of elliptic curves in residue characteristic 2. *Bull. Lond. Math. Soc.*, 40(3):516–524, 2008. 9

[12] Tim Dokchitser and Vladimir Dokchitser. Local invariants of isogenous elliptic curves. *Trans. Amer. Math. Soc.*, 367(6):4339–4358, 2015. 4, 8.2, 9

[13] N. Freitas, B. Naskręcki, and M. Stoll. The generalized fermat equation with exponents $2, 3, n$. Preprint, 2017. 1

[14] Nuno Freitas and Alain Kraus. On the symplectic type of isomorphisms of the p-torsion of elliptic curves. Preprint, 2017. 1

[15] Paul Gérardin. Facteurs locaux des algèbres simples de rang 4. I. In *Reductive groups and automorphic forms, I (Paris, 1976/1977)*, volume 1 of *Publ. Math. Univ. Paris VII*, pages 37–77. Univ. Paris VII, Paris, 1978. 8.2

[16] Alain Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta Math.*, 69(4):353–385, 1990. 1, 4

[17] Ariel Pacetti. On the change of root numbers under twisting and applications. *Proc. Amer. Math. Soc.*, 141(8):2615–2628, 2013. 7, 8.2, 8.4, 8.5

[18] David E. Rohrlich. Elliptic curves and the Weil-Deligne group. In *Elliptic curves and related topics*, volume 4 of *CRM Proc. Lecture Notes*, pages 125–157. Amer. Math. Soc., Providence, RI, 1994. 2, 4

[19] Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. 3, 3

[20] Alexander Stasinski. The smooth representations of $\mathrm{GL}_2(\mathfrak{o})$. *Comm. Algebra*, 37(12):4416–4430, 2009. 1

[21] J. Tate. Number theoretic background. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 3–26. Amer. Math. Soc., Providence, R.I., 1979. 3

Mathematics Institute, University of Warwick, CV4 7AL, United Kingdom

Email address: nunobfreitas@gmail.com