A MODULAR APPROACH TO FERMAT EQUATIONS OF SIGNATURE 
\((p, p, 5)\) USING FREY HYPERELLIPTIC CURVES

IMIN CHEN AND ANGELOS KOUTSIANAS

Abstract. In this paper we carry out the steps of Darmon’s program for the generalized Fermat equation

\[ x^n + y^n = z^5. \]

In particular, we develop the machinery necessary to prove an optimal bound on the exponent \(n\) for solutions satisfying certain 2-adic and 5-adic conditions which are natural from the point of view of the method. We also reduce the problem of resolving this equation to a ‘big image conjecture’, completing a line of ideas suggested in his original program.

The above equation is an example of a generalized Fermat equation for which the predicted Frey abelian varieties have dimension \(> 1\) and thus it represents an interesting test case for Darmon’s program.

Contents

1. Introduction 2
2. Acknowledgements 4
3. Hyperelliptic equations 4
4. Abelian varieties 6
5. Darmon’s Frey hyperelliptic curve for signature \((p, p, r)\) 7
6. Modularity of \(\rho_{J^\pm, p}\) 9
7. Conductors of \(\bar{\rho}_{J^\pm, p}\) 12
8. Irreducibility of \(\bar{\rho}_{J^\pm, p}\) 23
9. Proof of Theorem 1.1 27
10. Proof of Theorem 1.2 29

References 30

Date: January 15, 2025.
2010 Mathematics Subject Classification. Primary 11D41, Secondary 11G10.
Key words and phrases. Fermat equations, modular method, Frey hyperelliptic curves, Darmon’s program.
I. Chen was supported by NSERC Discovery Grant RGPIN-2017-03892.
1. Introduction

This paper is motivated by the study of the generalized Fermat equation

\[(1.1) \quad x^r + y^q = z^p.\]

We say that a solution \((a, b, c) \in \mathbb{Z}^3\) to \((1.1)\) is \textit{primitive} if \(\gcd(a, b, c) = 1\), and \textit{trivial} if \(abc = 0\). It is an open conjecture that \((1.1)\) has no non-trivial primitive solutions if \(r, q, p \geq 3\) (see for instance, [3]).

The special case of \(r = q = p\) is Fermat’s Last Theorem which was proven in [63, 61] using Galois representations and modularity. In [16], Darmon described a program to show the generalized Fermat equation \((1.1)\) has no non-trivial solutions for one varying prime exponent \(p \geq 3\) using the approach of Galois representations and modularity.

Central to Darmon’s program is the construction of Frey representations of signature \((r, q, p)\), which is done explicitly in [16] for the case \((p, p, r)\) using Frey abelian varieties which are constructed as the Jacobians of Frey hyperelliptic curves. In order to carry out Darmon’s program for a specific \(r, q\), one needs to prove irreducibility and modularity of the 2-dimensional residual Galois representations attached to a putative solution, as well as distinguish them from those of the trivial solutions. Due to recent breakthroughs in modularity results, establishing modularity can be carried out in many cases, but we note for the main results of this paper, we do in fact need the multi-Frey method in order to avoid a case where a suitable modularity result is unknown.

Although irreducibility cannot be established in all cases, using local methods, it is possible to treat certain congruence classes. In addition, the trivial solution \((\pm 1, \mp 1, 0)\) presents an essential obstruction to the method because its associated Frey hyperelliptic curve is non-singular and the Jacobian of this hyperelliptic curve is modular at the Serre level.

Unlike signature \((r, r, p)\) where one still has Frey elliptic curves due to [29], signature \((p, p, r)\) for \(r \geq 5\) necessitates the consideration of Frey abelian varieties of dimension greater than 1 if the exponents are prime [18, §4.3]. For \(r = 2, 3\), signature \((p, p, r)\) equations were resolved in [19] using Frey elliptic curves which exist in these cases. The equation studied in this paper thus represents an interesting test case for Darmon’s program and develops some of the tools which in future studies of the case \(r > 5\).

In this paper, we consider the specific signature \((p, p, 5)\) and develop the necessary machinery to carry out Darmon’s program in all congruence classes mod 10 which avoid the two obstructions above. The method is sufficiently refined to establish optimal bounds on the exponents \(p\).

**Theorem 1.1.** For \(n \geq 3\), there are no non-trivial primitive solutions \((a, b, c) \in \mathbb{Z}^3\) to the equation

\[(1.2) \quad x^n + y^n = z^5,\]

in the cases

(I) \(2 \nmid ab\) and \(5 \mid ab\), or
(II) \(2 \mid ab\) and \(5 \nmid ab\).
We remark that the proof of the above theorem requires the use of both Frey abelian varieties $J_5^\pm(a, b, c)$ introduced in [16] for signature $(p, p, 5)$ in order to deal with a lack of a suitable modularity result for $J_5^+(a, b, c)$ in the case $5 \nmid ab$.

As a consequence of the tools developed, another theorem we prove distills the obstructions to resolving (1.2).

**Theorem 1.2.** For prime $p$ sufficiently large, any non-trivial primitive solution $(a, b, c) \in \mathbb{Z}^3$ to the equation (1.2) gives rise to a residual Frey representation $\bar{\rho}_{J_5^-(a, b, c), p}$ such that $\bar{\rho}_{J_5^-(a, b, c), p}$ is reducible, or is a quadratic twist of $\bar{\rho}_{J_5^-(\alpha, -\alpha, 0), p}$ for some non-zero integer $\alpha$, where $p$ is any choice of prime of $K = \mathbb{Q}(\zeta_5)$ above $p$.

Since any quadratic twist of $J_5(\alpha, -\alpha, 0)$ has CM by $\mathbb{Q}(\zeta_5)$, the residual representation has small image, so Darmon’s conjectural ideas can now kick in.

**Corollary 1.3.** Assuming Conjecture 4.1 in [16], there are no non-trivial primitive solutions to

$$x^p + y^p = z^5,$$

for prime $p$ sufficiently large.

The above corollary was not proven in [16] because modularity of $J_5^+(a, b, c)/K$ cannot be achieved for $5 \nmid ab$, while our study of $J_5^-(a, b, c)/K$ allows us to prove its modularity without any conditions. We also remark that we only need Conjecture 4.1 in the Borel case when $10 \mid ab$ as irreducibility in the other cases were established in the course of proving Theorem 1.1.

The obstruction to completely resolving (1.2) thus consists of proving irreducibility in the case $2 \mid ab, 5 \mid ab$ and eliminating the CM-form in the case $2 \nmid ab, 5 \nmid ab$. These are two fundamental obstructions in the study of generalized Fermat equations of signature $(p, p, r)$ that still remain.

The innovations needed to achieve the main results are:

1. We provide efficient and general local methods which can be used for establishing irreducibility of residual Galois representations attached to Frey abelian varieties.
2. The conductor at primes above 2 of a Frey abelian variety is generally more difficult to determine. For instance, the methods in [25, 26, 2] do not apply. We show that it can be read off easily up to twist by using the relation between odd Frey abelian varieties and the Legendre family of elliptic curves, thereby “propagating the computation of conductors” from the Legendre family. This differs from the approach in [5] where explicit computations with hyperelliptic models are performed to determine the inertial type.
3. We apply repeated elimination steps using several twists of the Frey abelian variety to minimize the conductor at primes above 2 and avoid the need for inertia arguments such as in [6].
4. We give a precise conductor calculation at the prime above 5 of the Frey abelian variety $J_5^-(a, b, c)$ by identifying extensions which achieve semistable reduction, giving first examples of such computations in the “wild case” for parameterized families of Frey abelian varieties of dimension $> 1$. 
The programs and output transcripts for the computations needed in this paper are described and posted at [14].

2. Acknowledgements

We thank Nicolas Billerey, Nuno Freitas, Luis Dieulefait, and Céline Maistret for helpful discussions and suggestions pertaining to the subject of this paper. We also thank Mohammad Sadek for discussions about [40, Théorème 1 (I)]. The second author is grateful to the Department of Mathematics of The University of British Columbia, especially to Michael Bennett, because part of this work was accomplished during his time in Vancouver.

3. Hyperelliptic equations

In this section, we summarize the basic theory of hyperelliptic equation, which is taken in part from [40, 41, 42, 43]. In this paper, a curve $C$ over $K$ is an integral scheme of dimension 1 which is proper over $K$.

Let $K$ be a finite extension of $\mathbb{Q}_\ell$ where $\ell$ is a rational prime. Denote by $\mathcal{O}$ the ring of integers of $K$, by $k$ the residue field of $\mathcal{O}$ and by $v$ the valuation of $K$. A hyperelliptic equation $E$ over $K$ is an equation of the form

$$y^2 + Q(x)y = P(x),$$

where $Q, P \in K[x]$, deg $Q \leq g + 1$, and deg $P \leq n = 2g + 2$ with

$$2g + 1 \leq \max(2 \deg Q, \deg P) \leq 2g + 2.$$

Let

$$R = 4P + Q^2,$$

and suppose $\kappa$ is the leading coefficient of $R$. The discriminant of $E$ [41] is given by

$$\Delta_E := \begin{cases} 2^{-4(g+1)}\Delta(R) & \text{if } \deg R = 2g + 2, \\ 2^{-4(g+1)}\kappa^2\Delta(R) & \text{if } \deg R = 2g + 1, \end{cases}$$

where $\Delta(H)$ denotes the discriminant of $H \in K[x]$. In particular, if $P$ is monic, $\deg P = 2g + 1$, and $\deg Q \leq g$, then

$$\Delta_E = 2^{4g}\Delta(P + Q^2/4),$$

using the fact that $\Delta(H)$ is homogeneous of degree $2n - 2$ in the coefficients of $H$.

A hyperelliptic equation $E$ over $K$ gives rise to a curve $C$ over $K$ by gluing the following two affine schemes over $K$

$$\text{Spec } K[x, y]/(y^2 + Q(x)y - P(x))$$

and

$$\text{Spec } K[u, z]/(z^2 + T(u)z - S(u))$$

along the open sets $x \neq 0$ and $u \neq 0$, respectively, by the relations

$$x = 1/u, \quad y = z/u^{g+1},$$

where

$$P(x) = u^{2g+2}S(u), \quad Q(x) = u^{g+1}T(u).$$
Definition 3.1. A curve $C$ over $K$ given by a hyperelliptic equation $E$ over $K$ such that $\Delta_E \neq 0$ is called a hyperelliptic curve over $K$. A hyperelliptic equation $F$ with coefficients in $\mathcal{O}$ which gives rise to a curve over $K$ which is isomorphic to $C$ over $K$ is a called a hyperelliptic model over $\mathcal{O}$ for $C$ over $K$.

The quantity $g$ is the genus of the curve $C$ over $K$. Two hyperelliptic equations $E, F$ for a hyperelliptic curve $C$ over $K$ are related by the transformations

$$
E : y^2 + Q(x)y = P(x),
F : z^2 + T(u)z = S(u),
$$

$$
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(K), \quad e \in K^*, \quad H(u) \in K[u], \quad \deg(H) \leq g + 1,
$$

(3.7) $\Delta_F = \Delta_E e^{4(g^2 + 1)}(ad - bc)^{n-1}.$

In particular, we note that the valuation of the discriminant modulo $\text{gcd}(4(n - 1), n(n - 1))$, is an invariant of the isomorphism class of $C$ over $K$.

We say a hyperelliptic equation has odd degree if $P(x)$ is monic and

$$
\deg P = 2g + 1, \quad \deg Q \leq g.
$$

An odd degree hyperelliptic curve over $K$ or model over $\mathcal{O}$ is one which is given by an odd degree hyperelliptic equation.

Two odd degree hyperelliptic equations $E : y^2 + Q(x)y = P(x)$ and $F : z^2 + T(u)z = S(u)$ for the same hyperelliptic curve $C$ over $K$ are related by a transformation of the shape

$$
x = e^2u + r, \quad y = e^{2g+1}z + t(u), \quad \text{where}
$$

$$
e \in K^*, \quad r \in K, \quad t \in K[u], \quad \deg(t) \leq g.
$$

The discriminants of the odd degree hyperelliptic equations are related by

$$
\Delta_F = \Delta_E e^{4g(2g+1)},
$$

hence the valuation of the discriminant modulo $4g(2g+1)$ is an invariant of the isomorphism class of the pointed hyperelliptic curve $(C, P)$ over $K$, where $P = \infty$ is the given $K$-rational Weierstrass point on $C$ as it is described by an odd degree hyperelliptic equation (see [43] for more details).

Definition 3.2. A model $\mathcal{C}$ over $\mathcal{O}$ for a curve $C$ over $K$ is a $\mathcal{O}$-scheme which is proper and flat over $\mathcal{O}$ such that $\mathcal{C}_K \cong C$ where $\mathcal{C}_K$ is the generic fiber of $\mathcal{C}$.

We note that a hyperelliptic model over $\mathcal{O}$ for $C$ over $K$ gives rise to a model over $\mathcal{O}$ for $C$ over $K$ as in (3.3)-(3.6).

---

$^1$An alternative definition is that $C$ is a smooth geometrically connected curve over $K$ with a finite separable morphism of degree 2 to $\mathbb{P}_K^1$ (see [42, Chapter 7, Definition 4.7]).
Definition 3.3. A model $C$ over $O$ for a curve $C$ over $K$ has good reduction if and only if its reduction mod $v$ is non-singular over $k$. In addition, we say that $C$ has bad semistable reduction if and only if its reduction mod $v$ is reduced, singular, and has only ordinary double points as singularities.

Definition 3.4. A curve $C$ over $K$ has good reduction (resp. bad semistable reduction) if and only if there is some model $C$ over $O$ for $C$ which has good reduction (resp. bad semistable reduction). We say that $C$ has semistable reduction if and only if it has good or bad semistable reduction.

Definition 3.5. Suppose $C : y^2 + Q(x)y = P(x)$ is a hyperelliptic model over $O$ of a hyperelliptic curve over $K$. If $Q(x) = b_{g+1}x^{g+1} + \cdots + b_0$ and $P(x) = a_nx^n + \cdots + a_0$, then we define the valuation vectors over $K$ of this hyperelliptic model as the pair of vectors $(v(a_0), \cdots, v(a_n))$ $(v(b_0), \cdots, v(b_{g+1}))$.

Proposition 3.6. Let $C$ be a hyperelliptic curve over $K$ with a $K$-rational point $P$. Then $C$ has good reduction if and only if $C$ has an odd degree hyperelliptic model $C$ over $O$ such that $v(\Delta(C)) = 0$.

Proof. If $C$ has an odd degree hyperelliptic model $C$ over $O$ such that $v(\Delta(C)) = 0$, then $C$ is a model with good reduction so $C$ has good reduction.

Suppose $C$ has good reduction, so there exists a model $C$ of $C$ with good reduction. By [42, Exercise 8.3.6], the hyperelliptic map

$$\pi : C \to \mathbb{P}_K^1,$$

extends to

$$\pi : C \to \mathbb{P}_O^1.$$

As a result, $C_k$ is a non-singular pointed hyperelliptic curve with a $k$-rational Weierstrass point $\tilde{P}$ where $\tilde{P}$ is the reduction of $P$ mod $v$, where $P$ is the $K$-Weierstrass point on $C$ over $K$, so using [43, Proposition 1.2] it follows that $C_k$ can be given by a non-singular odd degree hyperelliptic equation. We deduce that $C$ has an odd degree hyperelliptic model $C$ such that $v(\Delta(C)) = 0$. $\Box$

More generally, see [42, Chapter 7, Remark 4.25].

4. Abelian varieties

In this section, we recall definitions and results about $GL_2$-type abelian varieties and semistable reduction of abelian varieties that we use later in the paper. We recommend [48, Section II] for an introduction to $GL_2$-type abelian varieties.

Let $K$ be a number field and $G_K = \text{Gal}(\overline{K}/K)$ denotes the absolute Galois group of $K$, where $\overline{K}$ is an algebraic closure of $K$. Let $A$ be an abelian variety over $K$ of dimension $g$.

Let $E$ be a number field of degree $g$ over $\mathbb{Q}$. We say that $A$ is of $GL_2(E)$-type over $K$ if

$$E \leftrightarrow (\text{End}_K A) \otimes \mathbb{Q},$$

where $\text{End}_K(A)$ is the ring of endomorphisms of $A$ defined over $K$. 

6
Let $\ell$ be a rational prime and $T_\ell(A)$ the Tate module of $A$ with $V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}_\ell$. As $G_K$-modules we have that
\begin{equation}
V_\ell(A) \cong \bigoplus_{\lambda | \ell} V_{\lambda}(A),
\end{equation}
where $V_{\lambda}(A) = V_\ell(A) \otimes_{E_\lambda} E_\lambda$ is the $\lambda$-adic Tate module of $A$, $E_\ell = \bigoplus_{\lambda | \ell} E_\lambda$, and $E_\lambda$ is the completion of $E$ at $\lambda$. Because $G_K$ acts $E_\lambda$-linearly on $V_{\lambda}(A)$ and $V_\lambda(A)$ is an $E_\lambda$-vector space of dimension 2 we get a $\lambda$-adic Galois representation
\begin{equation}
\rho_{A,\lambda} : G_K \rightarrow \text{GL}_2(E_\lambda).
\end{equation}
For the system $(\rho_{A,\lambda})$ of Galois representations of $A$ we have the following theorem [55, Section 11.10].

**Theorem 4.1.** The system $(\rho_{A,\lambda})$ of Galois representations of $A$ is an $E$-rational weakly compatible system$^2$. In particular, the Frobenius polynomials associated with $(\rho_{A,\lambda})$ all have coefficients in the ring of integers of $E$.

Let $w$ be a prime in $K$ over $A$ has good reduction. We denote by $a_w$ the trace of Frobenius of $w$ and the system $(\rho_{A,\lambda})$. We define the Frobenius field $K_A$ of $A$ to be the field generated by the traces $a_w$. From Theorem 4.1, $K_A$ is a subfield of $E$.

At the end of this section, we recall the definition of semistable and multiplicative reduction of an abelian variety and how we can get this characterization when $A$ is the Jacobian of a curve $C$.

**Definition 4.2.** An abelian variety over $K$ has semistable reduction if and only if the linear part of the special fiber of the connected component of its Néron model is an algebraic torus. Furthermore, if its toric rank is positive, we say it has multiplicative reduction.

**Theorem 4.3.** Let $C$ be a curve over $K$ and let $J$ be the Jacobian of $C$. Then $C/K$ has semistable reduction if and only if $J/K$ has semistable reduction. Furthermore, if $C/K$ has bad semistable reduction with a model $C$ that has integral special fiber, then $J/K$ has multiplicative reduction.

**Proof.** See [21, Theorem 2.4] for the first assertion. Let $X$ be the special fibre of $C$. Then, by assumption $X$ is integral and has only ordinary double points as singularities. Therefore, with the notation in [50, Section 3.3], it holds that $X' = X_{\text{red}} = X$. If $\tilde{X}$ is the normalization of $X$ then $\tilde{X}$ is connected because $X$, and therefore $\tilde{X}$, is irreducible. Hence, $c = 1$ in [50, Lemma 3.3.5], so the toric rank of the reduction of $J$ is positive. Thus, $J$ has multiplicative reduction. \hfill \Box

5. **Darmon’s Frey hyperelliptic curve for signature $(p,p,r)$**

In this section, we briefly review from [16, 59] the construction of a suitable Frey hyperelliptic curve for the equation
\begin{equation}
x^p + y^p = z^r,
\end{equation}
where $r$ and $p$ are odd primes.

$^2$See [9] for the definition of $E$-rational weakly (strictly) compatible system of Galois representations.
Let $\zeta_r$ be a primitive $r$th root of unity, $\omega_j = \zeta_r^j + \zeta_r^{-j}$, and put
\[ g(x) = \prod_{j=1}^{r-1} (x + \omega_j). \]

From here on, we let $K = \mathbb{Q}(\zeta_r)^+$ and denote by $\mathfrak{p}$ the unique prime above $r$ in $K$. We also use the notation $\mathfrak{p}_q$ to denote a prime of $K$ above $q$ and in particular, $\mathfrak{p} = \mathfrak{p}_r$, where the former is used in the context of coefficients for representations, and the latter when completing $K$ at $\mathfrak{p}_r$.

**Proposition 5.1.** The quotient of the hyperelliptic curve
\[ Y^2 = X(X^{2r} + tX^r + 1), \]
by the involution $\tau : (X, Y) \mapsto (1/X, Y/X^r + 1)$ is given by the hyperelliptic curve
\[ y^2 = xg(x^2 - 2) + t. \]

Proof. See [59, Proposition 3]. □

**Proposition 5.2.** The quotient of the hyperelliptic curve
\[ Y^2 = X^{2r} + tX^r + 1, \]
by the involution $\tau : (X, Y) \mapsto (1/X, Y/X^r)$ is given by the hyperelliptic curve
\[ y^2 = (x + 2)(xg(x^2 - 2) + t). \]

Proof. See [59, Remark, p. 1058]. □

Consider the following hyperelliptic curves
\[ C^-_r(t) : y^2 = f^-_r(x) := f(x) + 2 - 4t, \]
\[ C^+_r(t) : y^2 = f^+_r(x) := (x + 2)(f(x) + 2 - 4t), \]
where $f(x) = xg(x^2 - 2)$.

**Theorem 5.3.** The discriminants of the polynomials $f^-_r(x)$ and $f^+_r(x)$ are given by
\[ \Delta(f^-_r) = (-1)^{r-1}2^{2(r-1)}r^r t^{\frac{r+1}{2}}(t - 1)^{\frac{r-1}{2}}, \]
\[ \Delta(f^+_r) = (-1)^{r-1}2^{2(r+1)}r^r t^{\frac{r+3}{2}}(t - 1)^{\frac{r-1}{2}}. \]

Proof. This is stated in slightly different form in the proof of [16, Proposition 1.15]. For further details on how such formulae can be justified, we refer the reader to [5]. □

**Theorem 5.4.** Let $J^\pm_r(t)$ be the Jacobian of the hyperelliptic curve $C^\pm_r(t)$. Then, the endomorphism algebra $\text{End}_K(J^\pm_r(t)) \otimes \mathbb{Q}$ contains the field $K$.

Proof. For $J^-_r(t)$, see [59, Theorem 1]. For $J^+_r(t)$, the result follows from [59, Remark, p. 1058] and modifying the argument in [59, §3.1]. □

Let $(a, b, c) \in \mathbb{Z}^3$ be a non-trivial primitive solution to (5.1). The following lemma is readily verified and appears in [16, p. 425].
Lemma 5.5. Let
\[ C_\tau^-(a, b, c) : \quad y^2 = c^\tau f(x/c) - 2(a^\tau - b^\tau), \]
\[ C_\tau^+(a, b, c) : \quad y^2 = (x + 2c)(c^\tau f(x/c) - 2(a^\tau - b^\tau)). \]

Then
1. \( C_\tau^-(a, b, c) \) is isomorphic to a twist of \( C_\tau^- (t) \) over \( \mathbb{Q} \) where \( t = a^\tau/c^\tau \),
2. \( C_\tau^+(a, b, c) \) is isomorphic to \( C_\tau^+ (t) \) over \( \mathbb{Q} \) where \( t = a^\tau/c^\tau \).

Some explicit examples are listed below.

\( C_\tau^- (a, b, c) \) for:
- \( r = 3 \): \( y^2 = x^3 - 3c^2x - 2(a^\tau - b^\tau) \),
- \( r = 5 \): \( y^2 = x^5 - 5c^2x^3 + 5c^4x - 2(a^\tau - b^\tau) \),
- \( r = 7 \): \( y^2 = x^7 - 7c^2x^5 + 14c^4x^3 - 7c^6x - 2(a^\tau - b^\tau) \),
- \( r = 11 \): \( y^2 = x^{11} - 11c^2x^9 + 44c^4x^7 - 77c^6x^5 + 55c^8x^3 - 11c^{10}x - 2(a^\tau - b^\tau) \).

\( C_\tau^+ (a, b, c) \) for:
- \( r = 3 \): \( y^2 = (x + 2c)(x^3 - 3c^2x - 2(a^\tau - b^\tau)) \),
- \( r = 5 \): \( y^2 = (x + 2c)(x^5 - 5c^2x^3 + 5c^4x - 2(a^\tau - b^\tau)) \),
- \( r = 7 \): \( y^2 = (x + 2c)(x^7 - 7c^2x^5 + 14c^4x^3 - 7c^6x - 2(a^\tau - b^\tau)) \),
- \( r = 11 \): \( y^2 = (x + 2c)(x^{11} - 11c^2x^9 + 44c^4x^7 - 77c^6x^5 + 55c^8x^3 - 11c^{10}x - 2(a^\tau - b^\tau)) \).

Remark 5.6. The curve \( C_\tau^+(a, b, c) \) corresponds to the (classical) Frey elliptic curve of the Fermat equation with signature \((p, p, 3)\) which has been studied in [19, 4].

From Theorem 5.3 and Lemma 5.5, the discriminants of the hyperelliptic curves \( C_\tau^- (a, b, c) \) and \( C_\tau^+ (a, b, c) \) are given by
\[
\Delta(C_\tau^-) = 2^{4(r-1)}r^r a^{p(r-1)/2}p^{(r-1)/2} \tag{5.2}
\]
\[
\Delta(C_\tau^+) = 2^{4r}r^r a^{p(r+3)/2}p^{(r-1)/2} \tag{5.3}
\]

We denote by \( J_\tau^\pm = J_\tau^\pm(a, b, c) \) the Jacobians of \( C_\tau^\pm (a, b, c) \). The abelian varieties \( J_\tau^\pm / K \) are of \( \text{GL}_2(K) \)-type [16].

Remark 5.7. \( C_\tau^+(1, -1, 0) \) is non-singular and \( J_\tau^+(1, -1, 0) \) has complex multiplication by \( \mathbb{Q}(\zeta_r) \) [16, Proposition 3.7].

6. Modularity of \( \rho_{J_\tau^\pm} \)

From this section onward, we specialize to the case \( r = 5 \). Let \((a, b, c) \in \mathbb{Z}^3\) be a non-trivial primitive solution to \((5.1)\) for \( r = 5 \), \( K = \mathbb{Q}(\zeta_5)^+ \) and \( p \) is an odd prime. For convenience, we denote \( C^\pm = C_5^\pm(a, b, c) \) and \( J^\pm = J_5^\pm(a, b, c) \).
Let $T_p(J^\pm)$ be the Tate module of $J^\pm$ and write $V_p(J^\pm) = T_p(J^\pm) \otimes \mathbb{Q}_p$. As $G_K$-modules from Section 4 and Theorem 5.4 we have that
\begin{equation}
V_p(J^\pm) \cong \oplus_{p|\mathfrak{p}} V_p(J^\pm),
\end{equation}
where $V_p(J^\pm) = V_p(J^\pm) \otimes K_p$ is the $p$-adic Tate module of $J^\pm$, $K_p = \oplus_{p|\mathfrak{p}} K_p$, and $K_p$ is the completion of $K$ at $p$.

Let $\rho_{J^\pm,p}$ be the Galois representation of $G_K$ on the $p$-adic Tate module of $J^\pm$, where $p$ is a prime of $K$ above $p$. We also denote by $\bar{\rho}_{J^\pm,p}$ the Galois representation of $G_K$ on the $p$-torsion of $J^\pm$.

Let $L$ be a totally real field and $n = [L : \mathbb{Q}]$. Let $f$ be a Hilbert newform over $L$ of weight $k = (k_1, \ldots, k_n) \in (\mathbb{Z}_{\geq 1})^n$, level $N_f$ an ideal of $\mathcal{O}_L$ and character $\chi$. We denote by $K_f$ the eigenvalue field of $f$. Then for any prime $\mathfrak{l}$ of $K_f$ above a rational prime $\ell$ there exists a continuous representation $\rho_{f,\mathfrak{l}} : G_L \to \text{GL}_2(K_{f,\mathfrak{l}})$ which is unramified outside $N_f\mathfrak{l}$ and for any prime $q \nmid N_f\mathfrak{l}$ it holds
\begin{align*}
\text{tr} \rho_{f,\mathfrak{l}}(\text{Frob}_q) &= a_q(f),
\text{det} \rho_{f,\mathfrak{l}}(\text{Frob}_q) &= \chi(q)N(q)^{k_0 - 1},
\end{align*}
where $k_0 = \max \{k_1, \ldots, k_n\}$ and $K_{f,\mathfrak{l}}$ is the completion of $K_f$ at $\mathfrak{l}$ (for the description of $k_0$, see [56]).

**Definition 6.1.** Let $A/L$ be an abelian variety of $\text{GL}_2(E)$-type where $L$ is totally real fields and $E$ is a number field. We say $A/L$ is modular if the weakly compatible system of representations $(\rho_{A,\lambda})$, as $\lambda$ varies over the finite primes of $E$, arises from the strictly compatible system of representations attached to a Hilbert newform $f$ over $L$. That is, the field of coefficients $K_f$ of $f$ is equal to the Frobenius field $L_A$ of $A$ and $\rho_{A,\lambda} \simeq \rho_{f,\mathfrak{l}}$ for all primes $\mathfrak{l}$ of $K_f$ and all primes $\lambda \mid \mathfrak{l}$ of $E$.

**Remark 6.2.** If $\rho_{A,\lambda} \simeq \rho_{f,\mathfrak{l}}$ for some pair of primes $(\lambda, \mathfrak{l})$, then in fact $\rho_{A,\lambda} \simeq \rho_{f,\mathfrak{l}}$ for all pairs $(\lambda, \mathfrak{l})$ by [48, Theorem (1.3.1)].

Suppose $A/L$ is a modular abelian variety of $\text{GL}_2(E)$-type. The conductor exponent at a prime $q$ of $L$ of $\rho_{A,\lambda}$ is independent of $\lambda \nmid N(q)$ which permits a definition of the conductor of a strictly compatible system of representations $(\rho_{A,\lambda})$. The conductor of the $\rho_{A,\lambda}$ coincides with the level of the Hilbert newform $f$ by [12, 60].

**Lemma 6.3.** The representations $\rho_{J^+,p}$ and $\rho_{J^-,p}$ have determinant the $p$-adic cyclotomic character $\chi_p$.

**Proof.** This follows from [64, Lemma 2.2.5, Corollary 2.2.10].

**Theorem 6.4.** Suppose $5 \mid ab$. Then $J^+/K$ is modular.

**Proof.** This is [16, Theorem 2.9].

---

3The existence of $\rho_{f,\lambda}$ is due to the work of many people; [57, Chapter 7] and [28, 54, 20, 22] for $L = \mathbb{Q}$ and [46, 49, 12, 62, 60, 8]. The form of these Galois representations after restriction to a decomposition group is provided by [39, 12, 62, 60, 51].
In the case $5 \nmid ab$, there is no currently known modularity result we can apply to prove that $\rho_{J^+,p}$ is modular in all cases. Therefore, we will work instead with $\rho_{J^-,p}$.

We denote by $\mathfrak{r}$ the unique prime ideal of $K$ above $5$ when $K$ is regarded as the coefficient field for a representation.

**Proposition 6.5.** The representation $\bar{\rho}_{J^-,\mathfrak{r}}$ extends to $G_Q$ and is absolutely irreducible when restricted to $G_{K(\zeta_5)}$.

**Proof.** The abelian variety $J^-/K$ is of $GL_2(K)$-type with $K \hookrightarrow \text{End}_K(J^-) \otimes \mathbb{Q}$. Thus, the 5-adic Tate module $T_5(J^-) \otimes \mathbb{Q}_5$ is a 2-dimensional $K \otimes \mathbb{Q}_5$-vector space. As 5 totally ramifies in $K$, we have that $K \otimes \mathbb{Q}_5 \cong K_5$.

Since $J^-$ is defined over $\mathbb{Q}$, as Darmon explains in [16, p. 443], the action of $G_K$ on $T_5(J^-) \otimes \mathbb{Q}_5$ as a $K_5$-vector space extends to a $G_Q$-action that is $G_K$-semilinear; it satisfies

$$\sigma(\alpha v) = \sigma(\alpha)\sigma(v),$$

where $\sigma \in G_Q$, $\alpha \in K_5$ and $v \in T_5(J^-)$. As $\mathfrak{r}$ is the unique prime above 5, the action of $G_Q$ on $T_5(J^-) \otimes_{\mathcal{O}_K} \mathbb{F}_5$, where the tensor product is taken with respect to the reduction map $\mathcal{O}_K \rightarrow \mathbb{F}_5$, is linear and restricts to the action of $G_K$ given by $\bar{\rho}_{J^-,\mathfrak{r}}$.

By [16, Theorem 2.6], we have that $\bar{\rho}_{J^-,\mathfrak{r}}$ arises up to quadratic twist from the Legendre family given by

$$\mathcal{L} : y^2 = x(x - 1)(x - t),$$

where $t = a^p/c^5$. More precisely, there is a character $\chi : G_K \rightarrow \mathbb{F}_5^\times$ of order dividing 2 such that

$$\bar{\rho}_{J^-,\mathfrak{r}} \cong \bar{\rho}_{\mathcal{L},5} \otimes \chi.$$

Suppose that $\bar{\rho}_{J^-,\mathfrak{r}}|_{G_{K(\zeta_5)}}$ is reducible; thus $\bar{\rho}_{\mathcal{L},5}|_{G_{K(\zeta_5)}}$ is reducible. We then obtain a non-cuspidal $K(\zeta_5)$-rational point in $X_0(20)$. A short Magma program allows one to verify the $K(\zeta_5)$-points on $X_0(20)$ are all cuspidal, a contradiction.

We have thus shown that $\bar{\rho}_{J^-,\mathfrak{r}}|_{G_{K(\zeta_5)}}$ is irreducible. To show absolute irreducibility, we need to check that $\bar{\rho}_{\mathcal{L},5}|_{G_{K(\zeta_5)}}$ cannot have image lying in a non-split Cartan subgroup $C'$, the only possible image for which the representation is irreducible, but becomes reducible after an extension of the coefficient field. The only possible image for $\bar{\rho}_{\mathcal{L},5}|_{G_K}$ is the normalizer of $C'$. Thus, for $\mathcal{L}$ to have this property we must have that

$$j_{\mathcal{L}}(t) - 1728 = j_{5N'}(s) - 1728,$$

where

$$j_{5N'}(s) = \frac{125s(2s + 1)^3(2s^2 + 7s + 8)^3}{(s^2 + s - 1)^5}$$

is the $j$-invariant of elliptic curves with normalizer of non-split Cartan structure on 5-torsion points [13, Corollary 5.3]. Since the left hand side is a square, $\mathcal{L}$ would give rise to a $K$-rational point on the hyperelliptic curve

$$y^2 = 2\left(\frac{7}{2}x + \frac{27}{8}\right)(x^2 + x - 1).$$
Using Magma, it can be checked that all $K$-rational points arise from cusps. □

**Theorem 6.6.** The $J^-/K$ is modular.

**Proof.** By Proposition 6.5, the representation $\bar{\rho}_{J^-}$ is absolutely irreducible and extends to a representation $\bar{\rho}$ of $G_{\mathbb{Q}}$. By Serre’s Conjecture over $\mathbb{Q}$, now proven in [34, 35, 36], $\bar{\rho}$ is modular, hence $\bar{\rho}_{J^-}$ is also modular by cyclic base change. Modularity of $\rho_{J^-}$ now follows from [33, Theorem 1.1] by checking its three hypotheses:

1. The representation $\rho_{J^-}$ is unramified outside the finite set of primes of $K$ dividing $10\Delta(C^-)$.
2. The abelian variety $J^-/K$ is potentially semi-stable so $\rho_{J^-}$ is deRham and hence Hodge-Tate. The Hodge-Tate weights of $\rho_{J^-}$ are $\{0, 1\}$.
3. The representation $\rho_{J^-} |_{G_K(\zeta_5)}$ is absolutely irreducible from Proposition 6.5.

Since $\rho_{J^-}$ is modular from Remark 6.2 we get that $\rho_{J^-,\lambda}$ is modular for every finite prime $\lambda$ of $K$. Hence, $J^-$ is modular. □

### 7. Conductors of $\bar{\rho}_{J^\pm, p}$

The discriminants of the hyperelliptic curves $C^\pm/K$ are given by

\[
\begin{align*}
\Delta(C^-) &= 2^{16}5^5(ab)^{2p}, \\
\Delta(C^+) &= 2^{20}5^5(a^2b)^{2p},
\end{align*}
\]

from (5.2)-(5.3) specialized to the case $r = 5$.

By Theorems 6.4 and 6.6, $J^\pm/K$ is modular, which implies the $\rho_{J^\pm,\lambda}$ over all primes $\lambda$ of $K$ form a strictly compatible system. Hence, the $\rho_{J^\pm,\lambda}$ all have isomorphic local Weil-Deligne representations at primes $q \nmid N(\lambda)$, and therefore have the same conductor exponent at $q$ independent of $\lambda \nmid N(q)$.

Let $K_{q_5}$ and $K_{q_2}$ denote the completions of $K$ at the unique primes $q_5$ and $q_2$ of $K$ above 5 and 2, with ring of integers $\mathcal{O}_{q_5}$ and $\mathcal{O}_{q_2}$, respectively. The notation $q_5$ is used when $K$ is regarded as the base field, in contrast to $r$ introduced earlier, which is used when $K$ is regarded as a coefficient field of a representation.

Let $m$ be a rational prime and $S$ a finite set of (finite) primes of $K$. We denote by

\[
K(S, m) = \{d \in K^*/K^{*m} : v_q(d) \equiv 0 \pmod{m} \text{ for all } q \not\in S\}
\]

the $m$-Selmer group of $K$ with respect to $S$. When $\zeta_m \in K$, let $K(S, m)^*$ denote the set of characters $\chi : G_K \to \mathbb{Z}/m\mathbb{Z}$ corresponding to the extensions $K(\sqrt[d]{d})/K$ where $d \in K(S, m)$.

In this section, we prove the following theorem on the conductors of $\bar{\rho}_{J^+, p}$ and a suitable twist of $\bar{\rho}_{J^-, p}$.

**Theorem 7.1.** Let $p > 5$ be a prime.

1. Suppose $2 \nmid ab$ and $5 \mid ab$. Then the Serre level of $\bar{\rho}_{J^+, p}$ divides $q_5$ when $5 \mid a$ and is equal to $q_5^2$ when $5 \mid b$. 

12
(2) Suppose $2 \mid a, b \equiv -1 \pmod{4}$ or $2 \mid c, a \equiv -1 \pmod{4}$. Then, for some character $\chi_0 \in K(S_2, 2)^*$, where $S_2 = \{q_2\}$, the Serre level of $\bar{\rho}_{J_{-p}} \otimes \chi_0$ is equal to $q_2^s \cdot q_3^t$ where $s = 0, 1, 2$ and $\epsilon = 2, 3$ if $5 \nmid ab$ and $\epsilon = 2$ if $5 \mid ab$. In particular, $s \leq 1$ when $2 \mid a, b \equiv -1 \pmod{4}$.

For every $p \mid q$ in $K$, the representations $\bar{\rho}_{J^+_{-p}}$ and $\bar{\rho}_{J^-_{-p}} \otimes \chi_0$ are finite at $p$.

Remark 7.2. The 2-Selmer group $K(S_2, 2)$ can be computed in Magma to be

$$K(S_2, 2) = \left\{ 1, -1, -2, 2, \frac{-\sqrt{5} + 1}{2}, \frac{\sqrt{5} - 1}{2}, \sqrt{5} - 1, -\sqrt{5} + 1 \right\}.$$ 

Remark 7.3. The work of Dokchitser-Dokchitser-Maistret-Morgan [25, 26] gives a method to compute the conductor of a fixed hyperelliptic curve over local fields of odd residual characteristic. Recently in [2], these methods have been applied to compute the conductors at odd primes of Frey hyperelliptic curves for signatures $(p, p, r)$ and $(r, r, p)$.

Remark 7.4. At the top of [16, p. 425], it is stated that the particular twists $J_r^+(a, b, c)$ and $J_r^-(a, b, c)$ taken are chosen to be as ‘little ramified’ as possible. We will explain in Remarks 7.8 and 7.22 corrections to which quadratic twist of $J_r^+(a, b, c)$ should be taken so the conductor exponent at $q_5$ is minimized, and in Remark 7.16 that a different twist of $J_r^-(a, b, c)$ is needed in some cases to minimize the conductor exponent at $q_2$.

Let $N(\rho_{J^+_{-p}})$ denote the conductor of the $p$-adic representation $\rho_{J^+_{-p}}$ (which by definition excludes the primes dividing $p$) and $N(\rho_{J^+_{-p}, \chi})$ be the conductor of the strictly compatible system of representations $(\rho_{J^+_{-p}, \chi})$. Away from the primes dividing $p$, the two conductors coincide.

To deal with the conductors of $(\rho_{J^+_{-p}, \chi})$ at primes $q$ above $q \neq 2, 5$, we first state and prove the following lemma.

Lemma 7.5. Let $q \neq 2, 5$ be a prime and $q$ a prime of $K$ above $q$. Then $C^+ / K$ and $J^+ / K$ are semistable at $q$. In particular, if $C^+ / K$ has bad semistable reduction at $q$, then $J^+ / K$ has multiplicative reduction at $q$.

Proof. We describe the proof for $C^+$ as similar arguments can be used to treat $C^+$ (a transcript of the computations in all cases can be found in [14]). Suppose $q$ is a prime of $K$ that does not divide 2 and 5. From Lemma 5.5 the curve $C^-$ is given by

$$C^- : y^2 = x^5 - 5c^2x^3 + 5c^4x - 2(a^p - b^p).$$

By Proposition 3.6 and (7.1) if $q \nmid ab$ then $C^- / K$ has good reduction at $q$. If $q \mid a$, the special fiber of the hyperelliptic model $C^- / O_K$ at $q$ is given by

$$y^2 = (x + 2\tilde{c})(x^2 - \tilde{c}x - \tilde{c}^2)^2,$$

where $c$ reduces to the element $\tilde{c}$ in the residue field $\mathbb{F}_q$ of $q$. As $\Delta(x^2 - \tilde{c}x - \tilde{c}^2) = 5\tilde{c}^2 \neq 0$ in $\mathbb{F}_q$, it follows that $C^- / O_K$ satisfies the double root criterion [10, Lemma 3.7]. Hence $C^- / K$ has bad semistable reduction at $q$, and therefore $C^- / K$ is semistable at $q$. The remaining case of $q \mid b$ is similar except that (7.5) is changed to

$$y^2 = (x - 2\tilde{c})(x^2 + \tilde{c}x - \tilde{c}^2)^2,$$

and so $C^- / K$ has good reduction at $q$. Therefore $C^- / K$ is semistable at $q$. Hence $C^- / K$ has semistable reduction at $q$.
The semistability of $J^+/K$ follows from the semistability of $C^+/K$ by Theorem 4.3. Using [10, Proposition 3.1] and the second part of Theorem 4.3, we obtain that $C^+/K$ having bad semistable reduction at $q$ implies that $J^+/K$ has multiplicative reduction at $q$. □

7.1. The conductor of $(\rho_{J^+,\lambda})$. We start by first determining an extension of semistable reduction for $C^+/K$ at $q_5$.

**Lemma 7.6.** Suppose $5 \mid ab$. Then the curve $C^+/K_{q_5}$ has potential multiplicative reduction. In particular, the curve has bad semistable reduction over $K_{q_5}$ when $5 \mid a$ and bad semistable reduction over $K_{q_5}(5^{1/4})$ when $5 \mid b$.

**Proof.** The initial model of $C^+$ is given by

$$y^2 = (x + 2c)(x^5 - 5c^2x^3 + 5c^4x - 2(a^p - b^p)).$$

Assume $5 \mid a$. Let $\tilde{c}$ be the reduction of $c$ modulo 5. We have one singular point of the special fibre which is $(-2\tilde{c},0)$ by noting that $c \equiv b^p \pmod{5}$. Making the substitutions

$$x \to \sqrt{5}x - 2c, \quad y \to 5^3y,$$

we obtain a model over $\mathcal{O}_{q_5}$ and the equation of the special fibre is given by

$$(7.7) \quad y^2 = x^6 + 2\tilde{c}^2x^4 + \tilde{c}^4x^2 = x^2(x - 2\tilde{c})^2(x + 2\tilde{c})^2.$$

The singular points are $(0,0)$ and $(\pm 2\tilde{c},0)$ and each satisfies the double root criterion. Otherwise $5 \mid b$. We have one singular point of the special fibre which is $(2\tilde{c},0)$ by noting that $c \equiv a^p \pmod{5}$. Making the substitutions

$$x \to \sqrt{5}x + 2c, \quad y \to \sqrt{5}^{5/2}y,$$

we obtain a model over $\mathcal{O}_{q_5}$ and the equation of the special fibre is given by

$$(7.8) \quad y^2 = 4\tilde{c}x^5 + 3\tilde{c}^3x^3 + 4\tilde{c}^5x = -\tilde{c}x(x - 2\tilde{c})^2(x + 2\tilde{c})^2.$$

The singular points are $(\pm 2\tilde{c},0)$ and each satisfies the double root criterion. This model is a quadratic twist of the initial model, therefore the curve $C^+$ has bad semistable reduction over the quadratic extension $K_{q_5}(5^{1/4})$ of $K_{q_5}$. □

The next theorem computes the conductor of $(\rho_{J^+,\lambda})$.

**Theorem 7.7.** Suppose $2 \nmid ab$ and $5 \mid ab$. Then the conductor $N(\rho_{J^+,\lambda}) = q_5^\epsilon \cdot q_{ab}$ where $q_{ab}$ is the square-free ideal of $K$ divisible by the primes $q \neq q_5$ and $q \mid ab$ and

$$\epsilon = \begin{cases} 1, & 5 \mid a, \\ 2, & 5 \mid b. \end{cases}$$

**Proof.** By the proof of [16, Proposition 1.15], $C^+/K$ has good reduction at the prime $q_2$. Applying Lemma 7.5, Lemma 7.6 and Theorem 4.3 shows that $J^+/K$ has multiplicative reduction at the primes $q \mid q_5 \cdot q_{ab}$ and good reduction for the other primes $q$. For the primes $q$ of potential multiplicative reduction, we conclude by Grothendieck’s inertial criterion [1, Exposé 9] that the compatible system $(\rho_{J^+,\chi} | q \lambda)$, where $\lambda$ runs through the primes of $K$ not lying above $N(q)$, is special type with respect to a character $\chi$. In particular, $\chi$ is trivial when $q \neq q_5$ or $q = q_5$ and $5 \mid a$, and the $\chi$ is a totally ramified quadratic character with
respect to the extension $K_{q_5}(5^{1/4})/K_{q_5}$ when $5 \mid b$. In the former case the conductor is $q_5^1$ at $q_5$ while in the latter case is $q_5^2$.

Remark 7.8. We point out that the statement in [16, Theorem 3.5(1)] for $J^+(a,b,c)$ is only true up to a quadratic twist when $r \mid b$. For instance, it would imply that $\rho_{J^+}$ has conductor $\leq 1$ at $q_5$ when $5 \mid b$, which is not true: we have shown that $\rho_{J^+}$ has special type and conductor exponent 2 at $q_5$ so using [31, Theorem 1.5] we conclude $\rho_{J^+}$ has conductor exponent $\leq 1$ at $q_5$. The twist of $\rho_{J^+}$ by the character $\chi$ has conductor exponent $\leq 1$ at $q_5$.

7.2. The conductor of $(\rho_{J^-}, \lambda)$. In this section we compute the conductor of $(\rho_{J^-} \otimes \chi_0)$ for some choice of $\chi_0 \in K(S_2, 2)^*$ which “minimizes” this conductor.

Theorem 7.9. Suppose $2 \mid a, b \equiv -1 \pmod{4}$ or $2 \mid c, a \equiv -1 \pmod{4}$, and $p > 5$. Then, for some choice of $\chi_0$, the conductor $N(\rho_{J^-} \otimes \chi_0)$ is of the form $q_2^s \cdot q_5^1 \cdot q_{ab}$ where $\epsilon = 2, 3$ if $5 \nmid ab$ and $\epsilon = 2$ if $5 \mid ab$,

$$s = \begin{cases} 1, & \text{if } 2 \mid a, \\ 1 \text{ or } 2, & \text{if } 2 \nmid a. \\ \end{cases}$$

and $q_{ab}$ is the square-free ideal of $K$ divisible by the primes $q \mid ab$ and $q \nmid 10$.

Proof. This will follow from Lemma 7.5 (for the conductor exponent at primes dividing $q_{ab}$ in the same way as the last paragraph of the proof of Theorem 7.7), Proposition 7.18 (for the conductor exponent at $q_2$), and Proposition 7.24 (for the conductor exponent at $q_5$) if $5 \nmid ab$ and Proposition 7.21 if $5 \mid ab$. □

7.2.1. The conductor of $(\rho_{J^-}, \lambda)$ at $q_2$. We have used (6.3) to “propagate modularity” from $L/K$ to $J^-/K$ in the previous section. In this section, we will use (6.3) to “propagate conductors” from $L/K$ to $J^-/K$.

Consider

$$E : y^2 = x(x + a^p)(x - b^p),$$

which is a certain quadratic twist of the Legendre family for $t = a^p/c^5$. The lemma below determines the conductor of $E/K$ at $q_2$.

Lemma 7.10. Suppose $p > 3$ and

(1) $2 \mid a, b \equiv -1 \pmod{4}$, or
(2) $2 \mid c, a \equiv -1 \pmod{4}$.

Then, the conductor at $q_2$ of the elliptic curve $E/K$ given by

$$(7.9) \quad E : y^2 = x(x + a^p)(x - b^p)$$

is $q_2$. Furthermore, $\rho_{E,5}$ has conductor at $q_2$ dividing $q_2$.

Proof. This can be proven using Tate’s algorithm, for instance in [17, §2.2], it is shown that if

$$(7.10) \quad A + B = C$$
where \((A, B, C) \in \mathbb{Z}^3\) are coprime, \(A \equiv -1 \pmod{4}\), \(B \equiv 0 \pmod{16}\), then the elliptic curve

\[
y^2 = x(x - A)(x + B)
\]

is semistable over \(\mathbb{Q}\) with conductor at 2 equal to 2, and

\[
\Delta_E = 2^{-8} A^2 B^2 C^2.
\]

If \(2 \mid a, b \equiv -1 \pmod{4}\) (resp. \(2 \mid c, a \equiv -1 \pmod{4}\)) then applying the above result with \(A = b^p, B = a^p\) (resp. \(A = a^p, B = -c^5\)) yields the conductor at 2 (and hence at \(q_2\)). The minimal discriminant of \(E\) is given by \(\Delta_E = 2^{-8}(ab)^2pC^{10}\) in both cases. \(\square\)

**Remark 7.11.** Note \(\bar{\rho}_{E,5}\) has conductor at \(q_2\) equal to \(q_2\) if and only if \(5 \nmid v_2(\Delta_E) = v_2((ab)^2pC^{10})\) = 8.

Our method of “propagating the conductor at \(q_2\)” of \(\mathcal{L}/K\) to \(J^-/K\) requires that we know the inertial type of \(J^-/K\) at \(q_2\) which is provided by the following result.

**Proposition 7.12.** Suppose \(2 \mid a, b \equiv -1 \pmod{4}\). Then \(C^-/K_{q_2}\) has potentially bad semistable reduction and \(\rho_{J^-,\lambda}|_{K_{q_2}}\) has special inertial type with \(\lambda \nmid N(q_2)\).

**Proof.** The Igusa invariants of \(C^-\) are given by

\[
J_2 = 700c^4,
\]

\[
J_4 = 13750c^8,
\]

\[
J_6 = 1280000a^2p^5c^2 - 1280000a^p c^7 + 312500c^{12},
\]

\[
J_8 = 224000000a^2p^6 - 224000000a^p c^{11} + 7421875c^{16},
\]

\[
J_{10} = 204800000a^4p - 409600000a^3p^5c^5 + 204800000a^2p^{10}
\]

According to [40, Théorème 1 (I)] the curve \(C^-/K_{q_2}\) has potential good reduction if and only if \(J_{2i}/J_{10}\) is integral for all \(1 \leq i \leq 5\). It holds that

\[
\frac{J_5^2}{J_{10}} = \frac{5^5 \tau_5 c^{20}}{2^6 a^{3p}(a^p - c^5)^2},
\]

which is not integral. Therefore, \(C^-/K_{q_2}\) has potential bad semistable reduction. \(\square\)

We need the following lemmas to determine a complete set of twists needed to minimize the conductor of \((\rho_{J^-,\lambda} \otimes \chi_0)\) at \(q_2\).

**Lemma 7.13.** Let \(K\) be an unramified extension of \(\mathbb{Q}_2\) with uniformizer \(\pi\) and ring of integers \(\mathcal{O}_K\). Suppose \(d \in \mathcal{O}_K^*\) satisfies \(d \equiv 1 \pmod{\pi^2}\). Then \(L = K(\sqrt{d})\) is unramified over \(K\).

**Proof.** Let \(\alpha = \sqrt{d}\) and \(\beta = \frac{1 + \alpha}{2}\). Then \(N_{L/K}(\beta) = \frac{1 - \alpha^2}{4} \in \mathcal{O}_K\) and \(T_{L/K}(\beta) = 1 \in \mathcal{O}_K\). Hence, \(\beta \in \mathcal{O}_L\). Now,

\[
\beta^2 = \frac{1 + 2\alpha + \alpha^2}{4} = \frac{1 + d}{4} + \frac{\alpha}{2}.
\]

\[
\beta^2 = \frac{1 + 2\alpha + \alpha^2}{4} = \frac{1 + d}{4} + \frac{\alpha}{2}.
\]
The relative discriminant of $\mathcal{O}_K[\beta] = \mathcal{O}_K + \mathcal{O}_K\beta$ over $\mathcal{O}_K$ is the determinant of

$$\begin{pmatrix} 2 & 1 + d \\ 1 & 2 \end{pmatrix}$$

which is $d$. It now follows that $\mathcal{O}_L = \mathcal{O}_K[\beta]$ and the relative discriminant of $L/K$ is $d\mathcal{O}_K$, which is not divisible by $\pi$. Hence, $L/K$ is unramified.

**Lemma 7.14.** Let $\chi : G_K \rightarrow \{\pm 1\}$ be a quadratic or the trivial character. Then there exists a character $\chi_0 \in K(S_2, 2)^*$ where $S_2 = \{q_2\}$ such that $\chi \chi_0$ is unramified at $q_2$.

**Proof.** If $\chi$ is the trivial character then we choose $\chi_0$ to be the trivial character as well. We now assume that $\chi$ is a non-trivial character and let $L = K(\sqrt{d})$ be the corresponding quadratic extension, where $d \in \mathcal{O}_K^*$ is square-free.

Since the class number of $K$ is 1, using the idelic definition of class group [45, Chapter VI, Proposition 1.3], there exists a $u \in K^\times$ such that

$$(7.15) \quad du^{-1} \in \hat{\mathcal{O}}_K^\times,$$

where $\hat{\mathcal{O}}_K^\times = \prod_{v \text{ finite}} \mathcal{O}_{K_v}^\times$. Let $\mathcal{O}_K^\times = \langle -1, \sqrt{5} + 1 \rangle$. It can be checked that reduction map $\mathcal{O}_K^\times$ to $\left(\mathcal{O}_K/q_2^2 \right)^\times$ is surjective. Hence, without loss of generality, we may assume that $u \equiv 1 \pmod{q_2^2}$.

Let $d_0 = du^{-1}$, then $d_0 \in K(S_2, 2)$ since $K(\sqrt{d_0})$ is unramified outside of $q_2$ by (7.15). Let $\chi_0 \in K(S_2, 2)^*$ and $\chi_u$ be the characters corresponding to $K(\sqrt{d_0})$ and $K(\sqrt{u})$, respectively. From $d_0 = du^{-1}$, we have the relation $\chi_u = \chi \chi_0^{-1} = \chi \chi_0$. As $u \in \mathcal{O}_K$ and $u \equiv 1 \pmod{q_2^2}$, by Lemma 7.13 we have that $\chi_u$ is unramified at $q_2$, therefore $\chi \chi_0$ is unramified at $q_2$. □

The next proposition propagates the conductor at $q_2$ of $\rho_{\mathcal{L},5}$ to $\rho_{J, -r} \otimes \chi_0$ for some choice of $\chi_0 \in K(S_2, 2)^*$ that minimizes this conductor.

**Proposition 7.15.** Suppose $2 \mid a$, $b \equiv -1 \pmod{4}$ or $2 \mid c$, $a \equiv -1 \pmod{4}$, and $p > 5$. Then there is a character $\chi_0 \in K(S_2, 2)^*$, where $S_2 = \{q_2\}$, such that the conductor at $q_2$ of $\rho_{J, -r} \otimes \chi_0$ is equal to $q_2^s$ where

$$s = \begin{cases} 1, & \text{if } 2 \mid a, \\ 1 \text{ or } 2, & \text{if } 2 \mid c. \end{cases}$$

**Proof.** To the solution $(a, b, c)$ we attach the elliptic curve

$$E : y^2 = x(x + a^p)(x - b^p).$$

The elliptic curve $E$ is a quadratic twist of $\mathcal{L}$ in (6.2) and hence by (6.3) we have that

$$(7.16) \quad \tilde{\rho}_{J, -r} \cong \tilde{\rho}_{E,5} \otimes \chi,$$

for some quadratic character $\chi$ of $G_K$. By Lemma 7.14 there exists a character $\chi_0 \in K(S_2, 2)^*$ such that $\chi \chi_0$ is unramified at $q_2$. Applying Lemma 7.13, the conductor at $q_2$ of $\tilde{\rho}_{J, -r} \otimes \chi_0 \simeq \tilde{\rho}_{E,5} \otimes \chi \chi_0$ divides $q_2$.

The representation $\tilde{\rho}_{J, -r}$ is absolutely irreducible by Proposition 6.5 and modular by Theorem 6.6. Therefore, as we explain below we can conclude that $\rho_{J, -r} \otimes \chi_0$ has conductor $q_2^s$ where $s = 1, 2$. 

17
If \(2 \mid a, b \equiv -1 \pmod{4}\), then by Proposition 7.12, \(\rho_{J^-} \otimes \chi_0\) has special type. If \(s \geq 2\), there is degeneration of the conductor under reduction and we are in case (2) of [31, Theorem 1.5]. But this cannot occur as \(N_{K/\mathbb{Q}}(q_2) - 1 = 3 < 5\). Hence, \(s \leq 1\), and by Proposition 7.12 again, \(s = 1\).

If \(2 \mid c, a \equiv -1 \pmod{4}\), then by the proof of Lemma 7.10 and Remark 7.11, \(\tilde{\rho}_{E,5}\) has conductor at \(q_2\) equal to \(q_2\) as \(5 \nmid v_2(\Delta_E)\). Hence, we cannot have \(s = 0\). Thus, we are either have \(s = 1\) or we are in cases (2) – (4) of [31, Theorem 1.5]. As \(N_{K/\mathbb{Q}}(q_2) - 1 = 3 < 5\), the only possibility is case (4) and \(s = 2\).

**Remark 7.16.** We point out the statement in [16, Theorem 1.17] for \(J^-_r(a, b, c)\) is only true up to a quadratic twist if \(2 \mid ab\). For instance, it would imply that \(\tilde{\rho}_{J^-}p\) has conductor exponent \(\leq 1\) at \(q_2\) when \(2 \mid ab\), which is not true: Consider \(a = 2, c = 1\) so that \(c^5 - a^7 = b^7\) for some \(b \in \mathbb{Z}_2\). Using [27], which applies for a fixed hyperelliptic curve of genus 2, we find that the conductor exponent at \(q_2\) of \(\rho_{J^-}p\) is 4. We have shown by Proposition 7.12 that \(\rho_{J^-}p\) has special type at \(q_2\) and by Proposition 7.15 some quadratic twist of \(\rho_{J^-}p\) has conductor exponent 1 at \(q_2\). We conclude from [31, Theorem 1.5] that the conductor exponent of \(\tilde{\rho}_{J^-}p\) at \(q_2\) is 4. Unlike Remarks 7.8 and 7.16, we do not have a precise description of which twist brings the conductor exponent of \(\tilde{\rho}_{J^-}p\) to 1.

**Remark 7.17.** There is less known about calculating conductors of hyperelliptic curves at primes above 2, in particular the recent methods of [25, 26, 2] do not cover this case. Our method of “propagating” conductor computations from the Legendre elliptic curve, though slightly weaker than an exact computation, avoids these difficulties and suffices for the purposes of Diophantine applications.

The final proposition which computes the conductor at \(q_2\) of \((\rho_{J^-} \otimes \chi_0)\) now follows from compatibility.

**Proposition 7.18.** Suppose \(2 \mid a, b \equiv -1 \pmod{4}\) or \(2 \mid c, a \equiv -1 \pmod{4},\) and \(p > 5\). Let \(\chi_0\) be a character as in Proposition 7.15. Then the conductor at \(q_2\) of \((\rho_{J^-} \otimes \chi_0)\) is equal to \(q_2^s\) where

\[
s = \begin{cases} 
1, & \text{if } 2 \mid a, \\
1 \text{ or } 2, & \text{if } 2 \mid c.
\end{cases}
\]

**Proof.** The conductor at \(q_2\) of the compatible system \((\rho_{J^-} \otimes \chi_0)\) is independent of \(\lambda\) for \(\lambda \nmid N(q_2)\) as we have shown \(J^-/K\) is modular, so by Proposition 7.15 we have the conclusion. \(\Box\)

**Remark 7.19.** As \(\chi_0\) is unramified outside of \(q_2\), the conductors of \(\rho_{J^-} \otimes \chi_0\) are equal away from \(q_2\).

### 7.2.2. The conductor of \((\rho_{J^-} \otimes \chi_0)\) at \(q_5\)

We state and prove two propositions, one which determines an extension of semistable reduction for \(C^-/K_{q_5}\) and another which uses this to determine the conductor of \((\rho_{J^-} \otimes \chi_0)\) at \(q_5\).

**Lemma 7.20.** Suppose \(5 \mid ab\). Then the curve \(C^-/K_{q_5}\) has potential bad semistable reduction. In particular, the curve has bad semistable reduction over \(K_{q_5}(5^{1/4})\).
\begin{proof}
The initial model of $C^-$ is given by 
\[ y^2 = x^5 - 5c^2x^3 + 5c^4x - 2(a^p - b^p). \]

Assume $5 \mid a$. Let $\tilde{c}$ be the reduction of $c$ modulo $5$. We have one singular point on the special fibre which is $(-2\tilde{c}, 0)$. Making the substitution 
\[ x \to \sqrt[5]{5} x - 2c, \quad y \to \sqrt[5]{5^2} y, \]
we obtain a model over $\mathcal{O}_{q_5}$ and the equation of the special fibre is given by 
\[ y^2 = x^5 + 2\tilde{c}^2x^3 + \tilde{c}^4x = x(x - 2\tilde{c})^2(x + 2\tilde{c})^2. \]

The singular points are $(\pm 2\tilde{c}, 0)$ which both satisfy the double root criterion. The new model is a quadratic twist of the initial model, thus $C^-$ attains multiplicative reduction over the extension $K_{q_5}(5^{1/4})$.

Otherwise $5 \mid b$. We have one singular point of the special fibre which is the point $(2\tilde{c}, 0)$. Using the substitution 
\[ x \to \sqrt[5]{5} x + 2c, \quad y \to \sqrt[5]{5^2} y, \]
we obtain a model over $\mathcal{O}_{q_5}$ and the equation of the special fibre is given by 
\[ y^2 = x^5 + 2\tilde{c}^2x^3 + \tilde{c}^4x = x(x - 2\tilde{c})^2(x + 2\tilde{c})^2. \]

The singular points are $(\pm 2\tilde{c}, 0)$ and each satisfies the double root criterion. The new model is a quadratic twist of the initial model again, thus $C^-$ attains multiplicative reduction over the extension $K_{q_5}(5^{1/4})$. \hfill \Box

\textbf{Proposition 7.21.} Suppose $5 \mid ab$. Then the conductor at $q_5$ of $(\rho_{J-\lambda})$ is equal to $q_5$. \hfill \Box

\textbf{Proof.} The proof is similar to the proof of Theorem 7.7. By Lemma 7.20 the curve $C^-$ attains multiplicative reduction over $K_{q_5}(5^{1/4})$. Hence, we conclude by Grothendieck’s inertial criterion \cite[Exposé 9]{1} that the compatible system $(\rho_{J+\lambda} |_{D_{q_5}})$, where $\lambda$ runs through the primes of $K$ not lying above $N(q)$, is special type with respect to the character $\chi$ associated to the extension $K_{q_5}(5^{1/4})/K_{q_5}$. We conclude that the conductor at $q_5$ is $q_5^2$. \hfill \Box

\textbf{Remark 7.22.} We point out that the statement in \cite[Theorem 3.5(1)]{16} for $J_r^-(a, b, c)$ is only true up to a quadratic twist for $r \mid ab$. For instance, it would imply that $\tilde{\rho}_{J-r}$ has conductor exponent $\leq 1$ at $q_5$ when $5 \mid ab$, which is not true: we have shown that $\rho_{J-r}$ has special type and conductor exponent $2$ at $q_5$ so using \cite[Theorem 1.5]{31} we conclude $\tilde{\rho}_{J-r}$ has conductor exponent $2$ at $q_5$. The twist of $\tilde{\rho}_{J-r}$ by the character $\chi$ has conductor exponent $\leq 1$ at $q_5$.

\textbf{Proposition 7.23.} Suppose $5 \nmid ab$. Let $M/K_{q_5}$ be a totally ramified extension of degree $4$ and 
\[ \phi(x) = x^5 - 5c^2x^3 + 5c^4x - 2(a^p - b^p). \]

Let $d(a, c)$ be the constant term of $g(x) = \phi(x - a^p - 2c)$.

(i) If $v_5(d(a, c)) \geq 2$, then $C^-/K_{q_5}$ attains good reduction over the extension $M/K_{q_5}$.

(ii) If $v_5(d(a, c)) = 1$, let $a_0, b_0, c_0 \in \mathbb{Z}$ be the least non-negative residues of $a, b, c$ modulo $25$, respectively. Then, there is an extension $L = L(a_0, b_0, c_0)$ of $K_{q_5}$ depending on $(a_0, b_0, c_0)$ such that $L/K_{q_5}$ is a degree $20$ totally ramified extension and $C^-/K_{q_5}$ attains good reduction over $L/K_{q_5}$. \hfill 19
Moreover, these extensions are minimal with respect to ramification index.

Proof. The initial model for $C^-$ is given by the equation $y^2 = \phi(x)$. The special fibre of $C^-$ has a singular point which is $(-\tilde{a}^5 - 2\tilde{c}, 0)$ where $\tilde{a}, \tilde{c}$ are the reductions of $a, c$ modulo 5. Hence we consider the transformation $x \to x - a^p - 2c$ which results in the hyperelliptic model $y^2 = g(x) = \phi(x - a^p - 2c)$ of $C^-$ which has valuation vectors over $M$ given by

\[ (7.19) \quad (8, 8, \geq 8, 8, \geq 8, 0, \infty) \quad (\infty, \infty, \infty, \infty), \quad \text{if } v_5(d(a, c)) = 1, \]

\[ (7.20) \quad (\geq 16, 8, \geq 8, \geq 8, 0, \infty) \quad (\infty, \infty, \infty, \infty), \quad \text{if } v_5(d(a, c)) \geq 2. \]

These valuations are determined by expanding the coefficients of $g(x)$ as power series in $a, c$.

**Case** $v_5(d(a, c)) \geq 2$: From (7.1) we have that $v_M(\Delta(C^-)) = 40$. From (7.20) and (3.9), the substitution $x \to \pi_M^2 x$, $y \to \pi_M^3 y$ gives us a model with good reduction over $M$, where $\pi_M$ is a uniformizer of $M$.

The extension $M/K_{q_5}$ has minimal ramification index with the property that $C^-/M$ has good reduction: Suppose $C^-$ attains good reduction over an extension $F/K_{q_5}$ with ring of integers $\mathcal{O}_F$. As $C^-$ attains good reduction over $F$, it has an odd degree hyperelliptic model over $\mathcal{O}_F$ by Proposition 3.6. Since $v_{K_{q_5}}(\Delta(C^-)) = 10$ from the hypothesis $5 \nmid ab$, it follows that the ramification index of $F/K_{q_5}$ must be divisible by 4 from (3.9).

**Case** $v_5(d(a, c)) = 1$: Let $\phi_0(x) = x^5 - 5c_1^2x^3 + 5c_0^2x^2 - 2(a_0^5 - b_0^5)$ and $g_0(x) = \phi_0(x - a_0^5 - 2c_0)$. The coefficients of $g(x)$ lie in $\mathbb{Q}$ and $M/\mathbb{Q}$ is a degree 8 totally ramified extension so Eisenstein’s criterion holds for $g(x)$ over $\mathbb{Q}_5$. As $g(x) \equiv g_0(x) \pmod{25}$, $g_0(x)$ also satisfies Eisenstein’s criterion over $\mathbb{Q}_5$.

Let $\theta_0$ be a root of $g_0(x)$ and $L = M(\theta_0)$. Then $L/K_{q_5}$ is a 20 degree totally ramified extension. Making the substitution $x \to x + \theta_0$ to the model $y^2 = g(x)$ of $C^-$, we obtain a model with valuation vectors over $L$

\[ (7.21) \quad (\geq 80, 40, \geq 40, 40, \geq 40, 0, \infty) \quad (\infty, \infty, \infty, \infty). \]

Again from (7.1) we have that $v_L(\Delta(C^-)) = 200$. From (7.21) and (3.9), the substitution $x \to \pi_L^{10} x$, $y \to \pi_L^{25} y$ gives us a model with good reduction over $L$, where $\pi_L$ is a uniformizer of $L$.

The extension $L/K_{q_5}$ has minimal ramification index with the property that $C^-/L$ has good reduction: Suppose $C^-$ attains good reduction over an extension $F/K_{q_5}$. Similar to the previous case, it follows that $4 \mid e(F/K_{q_5})$.

We know from [53] that $[K_{q_5}^{\text{ur}}(J^-[2]) : K_{q_5}^{\text{nr}}] \mid [F \cdot K_{q_5}^{\text{ur}} : K_{q_5}^{\text{nr}}]$, where $K_{q_5}^{\text{ur}}$ is the maximal unramified extension of $K_{q_5}$. As $g(x)$ is an Eisenstein polynomial over $\mathbb{Q}_5$, the extension $Q_5(\theta)/\mathbb{Q}_5$ is a totally ramified extension of degree 5, where $\theta$ is a root of $g(x)$. This in turn implies the extension $K_{q_5}(\theta)/K_{q_5}$ is a totally ramified extension of degree 5. Since $K_{q_5}^{\text{ur}}(\theta) \subset K_{q_5}^{\text{ur}}(J^-[2])$ it follows that $5 \mid [K_{q_5}^{\text{ur}}(J^-[2]) : K_{q_5}^{\text{ur}}]$, and hence $5 \mid [F \cdot K_{q_5}^{\text{ur}} : K_{q_5}^{\text{ur}}]$ so $5 \mid e(F/K_{q_5})$. We have thus shown $20 \mid e(F/K_{q_5})$. \(\square\)

By considering the Newton polygon of $g(x)$, it can be shown that the condition $v_5(d(a, c)) \geq 2$ is equivalent to the polynomial $g(x)$, and hence $\phi(x)$, being reducible in $\mathbb{Q}_5[x]$.
Proposition 7.24. Suppose $5 \nmid ab$. Then the conductor of $(\rho_{J^{-},\lambda})$ at $\mathfrak{q}_{5}$ is $\mathfrak{q}_{5}^{2}$ where

$$
\epsilon = \begin{cases} 
2, & \text{if } v_{5}(d(a,c)) \geq 2, \\
3, & \text{if } v_{5}(d(a,c)) = 1.
\end{cases}
$$

Proof. Let $F = M$ or $L$ as above. The field cut out by $\rho_{J^{-},\lambda} |_{I_{K_{q_{5}}}}$ corresponds to the extension $F \cdot K_{q_{5}}^{nr}/K_{q_{5}}^{nr}$ when $\lambda \nmid N(\mathfrak{q}_{5})$. This follows from [53] and the fact that

$$
\rho_{J^{-},\ell} \simeq \bigoplus_{\lambda|\ell} \rho_{J^{-},\lambda},
$$

where $\rho_{J^{-},\ell}$ is the representation of $G_{K}$ on the full Tate module $T_{\ell}(J^{-})$ and $\ell \neq 5$ a rational prime. Since $J^{-}/K$ is modular, the $\rho_{J^{-},\lambda}$ are strictly compatible and hence have the same associated Weil-Deligne representation. It follows that the field cut out by $\rho_{J^{-},\ell} |_{I_{K_{q_{5}}}}$ is the same as the field cut out by any one of the $\rho_{J^{-},\lambda} |_{I_{K_{q_{5}}}}$.

To ease notation set $K = K_{q_{5}}$, $G_{K} = G_{K_{q_{5}}}$, $I_{K} = I_{K_{q_{5}}}$ from here on until the end of this proof. There are finitely many possibilities for $F$. For each possible choice, we may compute the conductor of $\rho_{J^{-},\lambda} |_{I_{K}}$ in the following way.

Let $\rho : G_{K} \rightarrow GL_{2}(\mathbb{C})$ be a continuous Galois representations that factors through the Galois group of the normal closure $\bar{F}/K$ of $F/K$ with inertia group order equal to 4 if $F = M$ and 20 if $F = L$.

Using Magma’s function GaloisRepresentations, we compute all irreducible Galois representations of $G_{K}$ that factor through the Galois group of the normal closure $\bar{F}/K$ of $F/K$ with inertia group order equal to 4 if $F = M$ and 20 if $F = L$. Each such representation has dimension 1 and conductor $\mathfrak{q}_{5}$ when $F = M$, and dimension 2 and conductor $\mathfrak{q}_{5}^{2}$ when $F = L$.

Therefore, the conductor of $\rho$ is equal to $\mathfrak{q}_{5}^{2}$ when $F = M$ as the inertial type of $\rho$ in this case must be a principal series with characters that are inverses of each other on inertia; the conductor of $\rho$ is equal to $\mathfrak{q}_{5}^{3}$ when $F = L$ and the inertial type in this case is supercuspidal.

The above Magma command computes the conductor of Artin representations $\rho$ of $G_{K}$ whereas we want to compute the conductor of the $\lambda$-adic representation $\rho_{J^{-},\lambda} |_{G_{K}}$. To make the link between the two types of representations, we show that there is a continuous 2-dimensional representation $\rho : G_{K} \rightarrow GL_{2}(\mathbb{C})$ factoring through $\bar{F}/K$ associated to $\rho_{J^{-},\lambda} |_{G_{K}}$ and having the same conductor.

Let

$$
(\rho_{J^{-}}, N) = WD(\rho_{J^{-},\lambda} |_{G_{K}}),
$$

be the Weil-Deligne representation attached to $\rho_{J^{-},\lambda} |_{G_{K}}$. Since $N = 0$ in this case, $\rho_{J^{-}}$ is a representation of $W_{K}$ and we know that it is parametrized by quasicharacters $\chi_{1}, \chi_{2}$ of $W_{K}$ (principal series) or a quasicharacter $\psi$ of $W_{M_{v}}$ where $M_{v}/K$ is a quadratic extension (supercuspidal, odd residual characteristic).

Each quasicharacter $\chi_{i}$, $\psi$ can be multiplied by a (real) power of the (unramified) quasicharacter $| \cdot |_{\mathfrak{q}_{5}}, | \cdot |_{\nu}$ to obtain a character $\tilde{\chi}_{i}, \tilde{\psi}$ with finite image, respectively, and whose conductor is the same. Using $\tilde{\chi}_{1}, \tilde{\chi}_{2}$ in the principal series case, and $\tilde{\psi}$ in the supercuspidal case, we obtain a representation $\tilde{\rho}$ of $W_{K}$ with the same conductor as $\rho_{J^{-}}$ since by construction $\tilde{\rho} |_{I_{K}} \simeq \rho_{J^{-}} |_{I_{K}}$. 

21
By [58, Theorem (4.2.1)] the representation \(\tilde{\rho}\) gives a continuous representation \(W_K \to \text{GL}_2(\mathbb{Q}_p)\) with finite image, and hence \(\tilde{\rho}\) can be regarded as a continuous representation \(W_K \to \text{GL}_2(\mathbb{C})\). As it is explained in [58, Section 2.2] we can extend \(\tilde{\rho}\) to a continuous representation \(\rho : G_K \to \text{GL}_2(\mathbb{C})\).

Since the restrictions \(\tilde{\rho} |_{I_K} \simeq \rho_{J-} |_{I_K}\) cut out the same field, we deduce that \(\tilde{F} \cdot K^{ur}/K^{ur} = F \cdot K^{ur}/K^{ur}\) and both restrictions factor faithfully through \(I_{\tilde{F}/K} = I_K \cdot G_{\tilde{F}}/G_{\tilde{F}}\). In particular, \(#\rho(I_K)\) is equal to 4 if \(F = M\) and 20 if \(F = L\).

We have determined the conductor of every possible Artin representation \(\rho\) as above, and therefore deduce from this computation that the conductor of \(\rho_{J-} |_{G_K}\) is equal to \(q_5^2\) when \(F = M\), and \(q_3^3\) when \(F = L\). \(\square\)

**Remark 7.25.** With the notation in the last proof above, we may obtain an upper bound on the conductor exponent at \(q_5\) using the valuation of the relative different of \(F/K\) and [44, (18)]. Using Magma we get that the bound on the conductor exponent is \(\leq 3\) in case \(F = L\) and \(\leq 2\) in case \(F = M\). The inertial type of \(\rho_{J-} |_{I_K}\) cannot be unramified nor special so the conductor exponent is \(\geq 2\). When \(F = M\), we deduce the conductor exponent is exactly 2. When \(F = L\), we note that \(F\) is wildly ramified. If the inertial type is principal series with characters \(\chi_1, \chi_2\), then both \(\chi_1\) and \(\chi_2\) are wildly ramified, since we know that \(\chi_1 \chi_2 = 1\) on inertia. Thus, the conductor exponent of \(\chi_1\) and \(\chi_2\) are \(\geq 2\). It follows that the conductor exponent of \(\rho_{J-} |_{I_K}\) is \(\geq 4\). By the conductor formula for principal series, a contradiction. Hence, the inertial type is non-exceptional supercuspidal induced from a character \(\chi\) on a quadratic extension \(F'/F\). Since the wild inertia group lies in \(G_{F'}\), it follows that \(\chi\) is wildly ramified. Hence, the conductor exponent of \(\chi\) is \(\geq 2\) and the conductor exponent of \(\rho_{J-} |_{I_K}\) is \(\geq 3\) by the conductor formula for non-exceptional supercuspidal type (in fact, we are in the case when \(F'/F\) is ramified as the other case would predict a conductor exponent that is \(\geq 4\)). In summary, we deduce that the conductor exponent is exactly 3 when \(F = L\).

**Remark 7.26.** We also point out the statement in [16, Proposition 1.16] which covers general \(r\), but only gives a bound on the conductor exponent at \(r\).

### 7.3. Proof of Theorem 7.1.

For primes \(q\) of \(K\) not dividing 10, \(\tilde{\rho}_{J+} | p\) is unramified at \(q \nmid p\), and finite at \(q\) if \(q \mid p\) by [16, Proposition 1.15]. The same is true for \(\tilde{\rho}_{J-} \otimes \chi_0\) as \(\chi_0\) is unramified at \(q \nmid 10p\).

By Theorem 7.7 for \((\rho_{J+}, \lambda)\) we have that

\[
N(\rho_{J+}, \lambda) = q_5^\epsilon \cdot \prod_{q \neq q_5, q | ab} q,
\]

where \(\epsilon = 1\) when \(5 \mid a\) and \(\epsilon = 2\) when \(5 \mid b\). Suppose \(5 \mid b\) then the conductor of \(\rho_{J+} | p\) at \(q_5\) does not degenerate upon reduction mod \(p\) by applying [31, Theorem 1.5]. For the case \(5 \mid a\) we get that the Serre level of \(\tilde{\rho}_{J+} | p\) divides \(q_5\).

By Theorem 7.9 for \((\rho_{J-} \otimes \chi_0)\) we have that

\[
N(\rho_{J-} \otimes \chi_0) = q_5^\delta \cdot q_5^\epsilon \cdot \prod_{q \mid ab, \ q \neq q_2, q_3, q_5} q,
\]

22
where $\epsilon = 2, 3$ and $s = 1, 2$. Therefore, the Serre level of $\bar{\rho}_{J-\rho} \otimes \chi_0$ divides $q_2^s \cdot q_5^s$. The conductor of $\rho_{J-\rho} \otimes \chi_0$ at $q_5$ does not degenerate upon reduction mod $p$ by applying [31, Theorem 1.5], hence the conductor of $\bar{\rho}_{J-\rho} \otimes \chi_0$ at $q_5$ is still $q_5^s$. Finally, by Theorem 7.9 the conductor of $\bar{\rho}_{J-\rho} \otimes \chi_0$ at $q_2$ divides $q_2$ when $2 \mid a$ and $q_2^2$ when $2 \mid c$.

8. Irreducibility of $\bar{\rho}_{J-\rho}$

In this section, we provide general local results which are used to prove irreducibility of the representations $\bar{\rho}_{J-\rho}$ with efficient bounds on $p$. We refer the reader to [23, 7] for the general strategies for proving irreducibility using local methods with asymptotic bounds on $p$.

We start with $K$ being a finite extension of $\mathbb{Q}_p$, having ring of integers $\mathcal{O}$, uniformizer $\pi$, and residue field $k$. Fix embeddings $\mathbb{Q}_p \subseteq K \subseteq \mathbb{Q}_p$ and $\mathbb{F}_p \subseteq k \subseteq \overline{\mathbb{F}}_p$. For any integer $n \geq 1$, denote by $\mathbb{F}_p^n$ the subfield of $\overline{\mathbb{F}}_p$ with $p^n$ elements. Let $I_K$ denote the inertia subgroup of $G_K$ and $P_K \subseteq I_K$ the wild inertia subgroup. Let $I_{t,K} = I_K/P_K$ denote the tame inertia group of $K$. We denote by $G_{L/K}$ the Galois group of a Galois extension $L/K$. Let $I_{L/K}$ and $I_{t,L/K}$ the inertia and tame inertia subgroups of $G_{L/K}$.

The action of $I_{t,K}$ on $\pi_1/((p^n-1)$ gives a homomorphism $\psi : I_{t,K} \rightarrow \mathbb{F}_p^\times \subseteq \overline{\mathbb{F}}_p^\times$, denoted $\theta_{p^n-1}$ as in [52], which we refer to as the fundamental character of level $n$. In contrast, a fundamental character of level $n$ is any conjugate over $\mathbb{F}_p$ of $\psi = \theta_{p^n-1}$, that is, a character of the form $\sigma \circ \psi$, where $\sigma : \mathbb{F}_p^n \hookrightarrow \overline{\mathbb{F}}_p$ is an embedding. In particular, there are $n$ distinct fundamental characters of level $n$.

**Theorem 8.1.** We have

$$I_{t,K} \cong \lim_{\substack{\longrightarrow \atop (d,p)=1}} \mu_d \cong \lim_{\substack{\longrightarrow \atop m}} \mathbb{F}_p^{\times \cdot p^m},$$

where the projective limits are over the homomorphisms

$$\mu_{da} \longrightarrow \mu_d$$

$$\alpha \longmapsto \alpha^{d'}$$

and

$$\mathbb{F}_p^{\times \cdot p^m} \longrightarrow \mathbb{F}_p^{\times \cdot p^m}$$

$$\alpha \longmapsto \alpha^{1-p^m}.$$
Let \( r_{L/K} : K^\times \to G_{L/K} \) be the local reciprocity map, whose restriction to \( \mathcal{O}^\times \) factors through a map \( \bar{r}_{L/K} : k^\times \to G_{L/K} \).

Then we have that
\[
\psi_{L/K} \circ \bar{r}_{L/K}(\bar{x}) = \bar{x}^{-1}
\]
for all \( x \in \mathbb{F}_p^\times \).

**Proof.** From [52, Prop. 3], we have that
\[
\bar{r}_{L/K} \circ \psi(s^{-1}) = \alpha(s)
\]
for all \( s \in I_{t,K} \). Hence, we have
\[
\psi_{L/K} \circ \bar{r}_{L/K} \circ \psi(s^{-1}) = \psi_{L/K} \circ \alpha(s) = \psi(s)
\]
for all \( s \in I_{t,K} \). Putting \( x = \psi(s^{-1}) \) and noting that \( \psi \) is surjective to \( \mathbb{F}_p^\times \) yields the result. \( \square \)

**Corollary 8.3.** Suppose \( \varphi : G_K \to \mathbb{F}_p^\times \) is a continuous homomorphism. Then, we have that
\[
\varphi \circ r_K(x) = \prod_\sigma \sigma(\bar{x})^{n(\sigma)},
\]
where \( \bar{x} \in k^\times \) is the reduction of \( x \in \mathcal{O}^\times \), \( r_K : K^\times \to G_K^{ab} \) is the local reciprocity map, \( 0 \leq n(\sigma) \leq p - 1 \), and \( \sigma \) runs through the embeddings of \( k \hookrightarrow \mathbb{F}_p \).

**Proof.** Let \( p^n = |k| \). Firstly, we can write
\[
(8.1) \quad \varphi|_{I_K} = \prod_\sigma (\sigma \circ \psi)^{-n(\sigma)}
\]
where \( \psi = \theta_{p^n-1} \) and \( 0 \leq n(\sigma) \leq p - 1 \) as
\[
(8.2) \quad \varphi|_{I_K} = \psi^k
\]
for some \( 0 \leq -k \leq p^n - 2 \) as \( \psi \) has order \( p^n - 1 \). Write \( k \) in the form
\[
(8.3) \quad k = a_0 + a_1 p + \ldots + a_{n-1} p^{n-1}
\]
where \( 0 \leq -a_i \leq p - 1 \) for all \( 0 \leq i \leq n - 1 \), then the conjugates \( \sigma \circ \psi \) are of the form \( \psi^{p^i} \) where \( 0 \leq i \leq n - 1 \).

Taking \( L = K(\zeta_{p^n-1})(\pi^{1/(p^n-1)}) = K(\pi^{1/(p^n-1)}) \), which is a finite tamely ramified abelian extension over \( K \), we see from Lemma 8.2 that the fundamental character \( \psi \) of level \( n \) has the description
\[
(8.4) \quad \psi \circ r_K(x) = \bar{x}^{-1}.
\]
The desired result then follows from precomposing (8.1) with \( r_K \). \( \square \)

Now let \( K \) be a number field. The following result is a generalization of [38, Appendice A]. We provide additional details for the benefit of the reader.
**Proposition 8.4.** Let $K$ be a number field with ring of integers $\mathcal{O}_K$. Let $p$ be a prime number unramified in $K$ and $S_p$ the set of places in $K$ above $p$. Let $\varphi : G_K \to \mathbb{F}_p^\times$ be a continuous homomorphism satisfying the following conditions:

1. The Artin conductor of $\varphi$ is $m$, an ideal of $\mathcal{O}_K$ prime to $p$;
2. For all $p \in S_p$, the restriction $\varphi |_{I_{K_p}}$ is equal to $\prod_{\sigma \in \Omega_p} (\sigma \circ \psi_p)^{-n_p(\sigma)}$, where
   
   (a) $0 \leq n_p(\sigma) \leq p - 1$,
   (b) $k_p$ is the residue field of $p$,
   (c) $\Omega_p$ denotes the set of embeddings of $k_p$ into $\mathbb{F}_p$,
   (d) $\psi_p : I_{k_p} \to k_p^\times \subseteq \mathbb{F}_p^\times$ is the fundamental character, where $K_p$ is the completion of $K$ at $p$.

Then, for all totally positive units $u \in \mathcal{O}_K^\times$ such that $u \equiv 1 \pmod{m}$, we have that

$$\prod_{p \in S_p} \prod_{\sigma \in \Omega_p} \sigma(u + p)^{n_p(\sigma)} = 1.$$

**Proof.** Let $r_K : A_K^\times \to G_K^{ab}$ be the global reciprocity map, and let $K_p = (K \otimes \mathbb{Q}_p)^\times = \prod_{p \in S_p} K_p^\times$, which sits inside the idèle group $A_K^\times$. We also denote by

$$U_m = \{x \in A_K^\times : x_v \in \mathcal{O}_v^\times, x_v > 0 \text{ for all real } v \text{ and } x_q \equiv 1 \pmod{q^\nu(m)} \text{ for all } q \mid m\}.$$

We have that

1. $\varphi \circ r_K$ is trivial on $U_{m,v}$ for places $v \nmid p$,
2. $\varphi \circ r_K(x) = \prod_{p \in S_p} \prod_{\sigma \in \Omega_p} \sigma(x_p + p)^{n_p(\sigma)}$ for $x = \prod_{p} x_p \in K_p^\times$ by Corollary 8.3.

It follows that $\varphi \circ r_K$ is trivial on $E_m = U_m \cap K_p^\times$, that is, the group of totally positive units $u \in \mathcal{O}_K^\times$ such that $u \equiv 1 \pmod{m}$. \hfill $\square$

**Corollary 8.5.** With the notation and hypotheses of Proposition 8.4 in place, if $n_p(\sigma) = 0$ except for one pair $(p_0, \sigma_0)$, then we have that

$$\sigma_0(\nu_0, \sigma_0) \equiv 1 \pmod{p_0},$$

for every totally positive unit $u \in \mathcal{O}_K^\times$ such that $u \equiv 1 \pmod{m}$.

We now have all the ingredients to prove $\bar{\rho}_{J^+, p}$ and $\bar{\rho}_{J^-, p}$ are irreducible.

**Theorem 8.6.** Suppose $2 \nmid ab$ and $5 \mid ab$. Then, $\bar{\rho}_{J^+, p}$ is irreducible for $p > 5$.

**Proof.** Since $\bar{\rho}_{J^+, p}$ is odd and $K$ is totally real it is well known that $\bar{\rho}_{J^+, p}$ is absolutely irreducible if and only if it is irreducible.

From Lemma 6.3, we have that $\det \bar{\rho}_{J^+, p} = \chi_p$. Suppose $\bar{\rho}_{J^+, p}$ is reducible, that is, $\bar{\rho}_{J^+, p} \simeq \left(\begin{array}{cc} \theta & * \\ 0 & \theta' \end{array}\right)$ with $\theta, \theta' : G_K \to \mathbb{F}_p^\times$ satisfying $\theta \theta' = \chi_p,$

where $\mathbb{F}_p$ is the residual field of $K$ at $p$. As $\theta \theta' = \chi_p$, the characters $\theta$ and $\theta'$ have the same conductor exponents away from $p$. 

25
Let \( q \neq p \) be a prime of \( \mathcal{O}_K \). The semi-simplification \( \bar{\rho}_J^\text{ss}_{\mid p} \) of a reduction \( \bar{\rho}_J \mid p \) does not depend on the choice of lattice and its restriction to \( I_{K_q} \) is isomorphic to \( (\theta \oplus \theta') \mid I_{K_q} \). Suppose \( e_q \) is the conductor exponent of \( \theta \) and \( \theta' \) which is the same as mentioned above. Then, the conductor exponent at \( q \) of \( \bar{\rho}_{J,\mid p}^\text{ss} \) is \( 2e_q \). On the other hand, the conductor exponent at \( q \) of \( \bar{\rho}_{J,\mid p}^\text{ss} \) is bounded by the conductor exponent at \( q \) of \( \bar{\rho}_{J,\mid p}^\text{ss} \) which is 0 for \( q \neq q_5 \) and 0, 1, 2 for \( q = q_5 \) by Theorem 7.1. Thus, \( e_q = 0 \) for all \( q \neq q_5 \) and the conductor of \( \theta \) and \( \theta' \) away from \( p \) divides \( q_5 \).

By Theorem 7.1 again, the representation \( \bar{\rho}_J \mid p \) is finite at all primes \( p \mid q \), and as \( p \) is unramified in \( K \), it follows from [1, Corollaire 3.4.4] that the restriction to \( I_{K_q} \) of \( \theta \oplus \theta' \) is isomorphic to (up to switching \( \theta \) and \( \theta' \))

\[
\begin{align*}
1 & \oplus \chi_p \\
\text{or} & \\
\psi_p & \oplus \psi_p^p
\end{align*}
\]

where \( \chi_p \) is the \( p \)-th cyclotomic character and \( \psi_p \) is the fundamental character of level 2 of \( I_{t,K_p} \).

Suppose \( \theta \) is unramified at all primes \( p \mid q \). Then, \( \theta \) corresponds to a character of the Ray class group of modulus \( q_5 \infty_1 \infty_2 \) where \( \infty_i \) denote the two places at infinity, which is isomorphic to \( \mathbb{Z}/2\mathbb{Z} \). Hence, the Ray class group modulus \( q_5 \infty_1 \infty_2 \) corresponds to a quadratic character \( \psi \). It follows that \( \theta = \psi^t \) and \( \theta' = \psi^t \chi_p \) where \( t = 0,1 \). It holds \( \psi(Frob_{q_2}) = \pm 1 \) and \( \chi_p(Frob_{q_2}) = 2^2 \). As \( C^+ / K \) has good reduction at \( q_2 \), we have that

\[
\pm(1+2^2) \equiv a_{q_2}(J^+) \quad \text{(mod } p),
\]

where \( a_{q_2}(J^+) \) is the trace of \( \rho_{J,\mid p} \) evaluated at a Frobenius element at \( q_2 \). Using the change of variables in [16, Proposition 1.15] with a short Magma script, we check that \( a_{q_2}(J^+) = 0 \), so \( p \mid 5 \) which is a contradiction to the fact that \( p > 5 \).

Suppose that both \( \theta \) and \( \theta' \) ramify at some prime above \( p \). Applying Corollary 8.5 over \( K \) with \( \varphi \) equal to either \( \theta \) or \( \theta' \) implies that \( p \) divides the norm of \( u - 1 \) by (8.6), where \( u = \epsilon_1 \) is the fundamental unit in \( K \). However, this norm is \(-1 \), a contradiction. \( \square \)

**Theorem 8.7.** Suppose \( 2 \mid a, b \equiv -1 \text{ (mod } 4) \) or \( 2 \mid c, a \equiv -1 \text{ (mod } 4), \text{ and } 5 \nmid ab \). Then, \( \bar{\rho}_{J,\mid p} \) is irreducible for \( p > 5 \).

**Proof.** Since \( \rho_{J,\mid p} \) is odd and \( K \) is totally real, \( \bar{\rho}_{J,\mid p} \) is absolutely irreducible if and only if it is irreducible. To show \( \bar{\rho}_{J,\mid p} \) is irreducible, it suffices to show \( \bar{\rho}_{J,\mid p} \) is irreducible where \( J = J^- \otimes \chi_0 \) and \( \chi_0 \) is as in Theorem 7.9.

From Lemma 6.3, we have that \( \text{det} \bar{\rho}_{J,\mid p} = \chi_p \). Suppose \( \bar{\rho}_{J,\mid p} \) is reducible, that is,

\[
\bar{\rho}_{J,\mid p} \simeq \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix}
\]

with \( \theta, \theta' : G_K \to \mathbb{F}_p^\times \) satisfying \( \theta \theta' = \chi_p \),

where \( \mathbb{F}_p \) is the residual field of \( K \) at \( p \). As \( \theta \theta' = \chi_p \), the characters \( \theta \) and \( \theta' \) have the same conductor exponents away from \( p \).

Let \( q \neq p, q_2 \) and \( q_5 \). From Theorem 7.1 we know that \( \bar{\rho}_{J,\mid p} \) is unramified at \( q \). As in Theorem 8.6 we conclude that \( e_q = 0 \) where \( e_q \) is the conductor exponent of \( \theta \) and \( \theta' \) at \( q \).

The conductor at \( q_2 \) of the semi-simplification of \( \bar{\rho}_{J,\mid p} \), which is isomorphic to \( \theta \oplus \theta' \), divides the conductor at \( q_2 \) of the semi-simplification of \( \rho_{J,\mid p} \), which in turn divides the conductor at
$q_2$ of $\rho_{J,p}$, namely, $q_2^s$ where $s = 1, 2$. As $\theta$ and $\theta'$ have the same conductor at $q_2$, it follows that the conductors at $q_2$ of $\theta$ and $\theta'$ divide $q_2$.

From Proposition 7.23 we know that $\rho_{J,p}(I_{K_{q_5}})$ has order equal to 4 or 20, therefore $\bar{\rho}_{J,p}(I_{K_{q_5}})$ has order equal to 4 or 20, respectively. This holds because $\rho_{J,p}(I_{K_{q_5}})$ does not intersect the kernel of reduction (which is a pro-$p$ group) since $p > 5$ and $\chi_0$ is unramified at $q_5$.

Since $\bar{\rho}_{J,p}(I_{K_{q_5}})$ has order coprime to $p > 5$ by Proposition 7.23 and Maschke’s Theorem, we conclude that $\bar{\rho}_{J,p} |_{I_{K_{q_5}}} \simeq \theta \oplus \theta' |_{I_{K_{q_5}}}$. From Theorem 7.1, we know that the conductor exponent at $q_5$ of $\bar{\rho}_{J,p} |_{I_{K_{q_5}}}$ is 2, 3. As above we conclude that the conductors at $q_5$ of $\theta$ and $\theta'$ are the same and divide $q_5$.

In summary, the conductor of $\theta$ and $\theta'$ away from $p$ divides $q_2q_5$. By Theorem 7.1, the representation $\bar{\rho}_{J,-p} |_{I_{p}}$ is finite at all primes $p \mid p$, and as $p$ is unramified in $K$, it follows from [1, Corollaire 3.4.4] that the restriction to $I_{K_p}$ of $\theta \oplus \theta'$ is isomorphic to (up to switching $\theta$ and $\theta'$)

\[(8.7) \quad 1 \oplus \chi_p \quad \text{or} \quad \psi_p \oplus \psi_p^p,\]

where $\chi_p$ is the $p$-th cyclotomic character and $\psi_p$ is the fundamental character of level 2 of $I_{t,K_p}$.

Suppose $\theta$ is unramified at all primes $p \mid p$. Then, $\theta$ corresponds to a character of the Ray class group of modulus $q_2q_5\infty_1\infty_2$ where $\infty_i$ denote the two places of $K$ at infinity. The Ray class group with this modulus is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. From the above we have that $4 \mid \#\bar{\rho}_{J,-p}(I_{K_{q_5}})$ and $\bar{\rho}_{J,-p} |_{I_{K_{q_5}}} \simeq \theta \oplus \theta' |_{I_{K_{q_5}}}$, hence $\theta |_{I_{K_{q_5}}}$ has order divisible by 4, which is a contradiction.

Suppose that both $\theta$ and $\theta'$ ramify at some prime above $p$. Let $\epsilon_1$ be the fundamental unit in $K$. Applying Corollary 8.5 over $K$ with $\varphi$ equal to either $\theta$ or $\theta'$ implies that $p$ divides the norm of $u - 1$ by (8.7), where $u = \epsilon_1^{n_1}$ and $n_1 = 12$ is the smallest positive integer such that $u \equiv 1 \pmod{q_2q_5}$. This yields of bound of $p = 2, 5$, contradicting $p > 5$. \[\square\]

9. Proof of Theorem 1.1

Let $(a, b, c) \in \mathbb{Z}^3$ be a non-trivial primitive solution to (1.2). It is enough to prove Theorem 1.1 for the case $n = p$ an odd prime or 4. For the case $n = 3$ this is a result by Kraus [37], the case $n = 5$ is a special case of Fermat’s Last Theorem (see for instance, [24, Théorème IX]) while the case $n = 4$ has been proved in [11, Theorem 1.1]. The case $n = 7$ is treated in [15].

For the rest of the proof, we may now assume that $n = p \geq 11$ is a prime. Let $S_2(n)$ denote the space of Hilbert newforms over $K$ with parallel weight 2, trivial character, and level $n$.

9.1. Local comparison of traces. In the elimination step of the modular method using a Frey abelian variety $J$, we typically show that an isomorphism

\[(9.1) \quad \bar{\rho}_{J,p} \simeq \bar{\rho}_{g,p},\]

where \(g\) is a suitable element of $S_2(n)$.
where \( p \) is prime of \( K \) and \( \mathfrak{P} \) is a prime of field of coefficient \( K_g \) of a Hilbert newform \( g \), cannot occur by exhibiting a prime \( q \) not dividing \( p \) and the Artin conductor of \( \bar{\rho}_{J,p} \) such that
\[
\text{tr} \bar{\rho}_{J,p}(\text{Frob}_q) \neq \text{tr} \bar{\rho}_{g,\mathfrak{P}}(\text{Frob}_q).
\]
However, a subtlety occurs because in the definition of the isomorphism (9.1) we mean
\[
(9.2) \quad \bar{\rho}_{J,p} \otimes \mathbb{F}_p \simeq \bar{\rho}_{g,\mathfrak{P}} \otimes \mathbb{F}_p.
\]
Hence, the comparison (9.2) cannot be done until we have chosen an embedding of the residue fields of \( K_p \) and \( K_g,\mathfrak{P} \) into \( \mathbb{F}_p \). To rule out an isomorphism as in (9.1) by a local comparison of traces it is necessary to average out this ambiguity and instead use the condition
\[
(9.3) \quad p \nmid N_{L/\mathbb{Q}} \left( \prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} (a_q(g) - a_q(J)^{\sigma}) \right),
\]
where \( L \) is the compositum of \( K \) and \( K_g \) inside \( \mathbb{Q} \) (see [5] for more details). Here we define the quantities
\[
(9.4) \quad a_q(J) = \text{tr} \rho_{J,p}(\text{Frob}_q),
\]
\[
(9.5) \quad a_q(g) = \text{tr} \rho_{g,\mathfrak{P}}(\text{Frob}_q).
\]
Finally, we remark that this does not affect the computational time for the elimination step, since in practice \textsc{Magma} is only able to compute \( a_q(J) \) up to Galois conjugation over \( \mathbb{Q} \) in any case.

9.2. \textbf{Proof of Theorem 1.1 (I)}. We are under the assumption that \( p \nmid ab \) and \( 5 \mid ab \). By Theorems 8.6, 6.4, and Lemma 6.3, we have that \( \bar{\rho}_{J,p} \) is irreducible and modular with trivial character. Hence, by level lowering for Hilbert modular forms [30, 32, 47], we have that
\[
(9.7) \quad \bar{\rho}_{J,p} \simeq \bar{\rho}_{g,\mathfrak{B}},
\]
where \( g \) is a Hilbert newform of parallel weight 2, trivial character over \( K \) and level \( \mathcal{O}_K, q_5 \) or \( q_5^2 \) by Theorem 7.1, and \( \mathfrak{B} \) is a prime above \( p \) in the field of coefficients of \( g \). However, the spaces of Hilbert newforms \( S_2(1), S_2(q_5) \) and \( S_2(q_5^2) \) are empty which gives a contradiction.

9.3. \textbf{Proof of Theorem 1.1 (II)}. As before, we may assume that \( n = p \geq 11 \) is a prime. We may assume without loss of generality that \( 2 \mid a, b \equiv -1 \pmod{4} \) by switching the roles of \( a \) and \( b \) and negating \( (a,b,c) \), if necessary.

By Theorems 8.7, 6.6, and Lemma 6.3, we have that \( \bar{\rho}_{J,-p} \) is irreducible and modular with trivial character.

In what follows, we use the fact that
\[
\rho_{J^-,\chi,p} = \rho_{J^-,p} \otimes \chi,
\]
for any character \( \chi : G_K \to \{\pm 1\} \) of order dividing 2, where \( J^- \otimes \chi \) means the twist of \( J^- \) by \( \chi \), and \( \chi \) twists by the automorphism \(-1\) of \( J^- \).
Let \( J = J^- \otimes \chi_0 \) where \( \chi_0 \in K(S_2, 2)^* \) and \( S_2 = \{ q_2 \} \). By level lowering for Hilbert modular forms as in the proof of Theorem 1.1 (I), we have that

\[
(9.8) \quad \bar{\rho}_{J,p} \simeq \rho_{g,3},
\]

where \( g \) is a Hilbert newform of parallel weight 2, trivial character over \( K \) and level \( q_2 q_5^e \) where \( e = 2, 3 \), by Theorem 7.1, and \( 3 \) is a prime of \( K \) above \( p \) in the field of coefficients of \( g \). Note in level lowering, we can level lower prime by prime and choose not to strip \( q_2 \) from the level of \( \rho_{J,p} \) in case the Serre level of \( \bar{\rho}_{J,p} \) is not divisible by \( q_2 \).

Suppose \( q \neq p \) is a prime of \( K \) not above 2 and 5. Then we have that

\[
(9.9) \quad a_q(g) \equiv a_q(J) \pmod{p}, \quad \text{if } q \nmid ab,
\]

\[
(9.10) \quad a_q(g)^2 \equiv (N(q) + 1)^2 \pmod{p}, \quad \text{if } q \mid ab,
\]

where \( a_q(J) = \text{tr} \rho_f(\text{Frob}_q) \) and \( N(q) \) is the norm of \( q \). Thus, defining

\[
T(g, q) = N(q) \cdot (a_q(g)^2 - (N(q) + 1)^2) \cdot \prod_{a,b \in \mathbb{F}_q, ab \neq 0} N_{L/K}(\prod_{\sigma \in \text{Gal}(K/Q)} (a_q(g) - a_q(J)^\sigma)),
\]

we have that \( p \mid T(g, q) \), where \( L \) is the compositum of \( K \) and \( K_g \) inside \( \overline{Q} \). Taking the gcd of \( T(g, q) \) for a suitable choice of primes \( q \) above \( q_2 \), we typically obtain a small finite set of possible primes \( p \) (assuming one of the \( T(g, q) \) is non-zero).

For all choices of \( \chi_0 \in K(S_2, 2)^* \), using the auxiliary primes \( q = 3, 7, 11 \), we eliminate all newforms \( g \) except for the prime exponents \( p = 2, 3, 5, 7 \), which proves the desired conclusion.

**Remark 9.1.** Working with all the \( J^- \otimes \chi_0 \) instead of the \( J^- \) does have two important consequences. First of all, the level of the space of Hilbert newforms we have to compute is smaller, i.e. otherwise we would have to compute the space of Hilbert newforms of level \( q_2 q_5^e \) with \( e = 2, 3 \) for instance. Secondly, the spaces of Hilbert newforms of level \( q_2^2 q_5^e \) with \( e = 2, 3 \) contain additional forms with complex multiplication over \( \mathbb{Q}((\zeta_5)) \). The elimination step using a standard comparison of traces of Frobenius does not work on these forms and requires additional elimination techniques to prove Theorem 1.1.

### 10. Proof of Theorem 1.2

As before, we may assume that \( n = p \geq 11 \) is a prime.

The proof is similar to the proof of Theorem 1.1 (II) so we outline the differences according to the cases involved. Again, let \( J = J^- \otimes \chi_0 \).

If \( 2 \mid ab \) and \( 5 \mid ab \) and \( \bar{\rho}_{J,p} \) is irreducible, then \( \bar{\rho}_{J,p} \) arises from level \( q_2 q_5^2 \). There are two newforms at level \( q_2 q_5^2 \). We eliminate both newforms as in the case (II) above. So we conclude that \( \bar{\rho}_{J,p} \) is reducible, and hence \( \bar{\rho}_{J-,p} \) is reducible.

If \( 2 \nmid ab \) and \( 5 \nmid ab \), then we may assume without loss of generality that \( 2 \mid c, \ a \equiv -1 \pmod{4} \) by switching the roles of \( a \) and \( b \) and negating \( (a,b,c) \), if necessary. We now have the additional levels \( q_2^2 q_5^e \) for \( e = 2, 3 \) to consider. All forms except one at level \( q_2^2 q_5^2 \) and three at level \( q_2^2 q_5^3 \) can be eliminated for prime exponents \( p \) not equal to \( 2, 3, 5, 19 \). These forms are obtained from \( J^-((-8,8,0)) \otimes \chi_2 \), where \( \chi_2 \) corresponds to \( K(\sqrt{2})/K \), and \( J^-((a,b,c)) \) for
\((a, b, c) = (-1, 1, 0), (-4, 4, 0), (-16, 16, 0)\), respectively. This can be verified by computing the conductors for these specific Jacobians using [27] and noting they are modular at the correct levels.

**References**

[1] Groupes de monodromie en géométrie algébrique. I. Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, Berlin-New York, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim. 7.1, 7.2, 2, 8, 8

[2] Martin Azon, Mar Curo-Iranzo, Maleeha Khawaja, Céline Maistret, and Diana Mocanu. Conductor exponents for families of hyperelliptic curves. ArXiv preprint, arxiv.org/abs/21021134, 2024. 2, 7.3, 7.17

[3] M. Bennett, P. Mihăilescu, and S. Siksek. The generalized Fermat equation. In Open problems in mathematics, pages 173–205. Springer, 2016. 1

[4] M. Bennett, V. Vatsal, and S. Yazdani. Ternary Diophantine equations of signature \((p, p, 3)\). Compos. Math., 140(6):1399–1416, 2004. 5.6

[5] N. Billerey, I. Chen, L. Dieulefait, and N. Freitas. On Darmon’s program for the generalized Fermat equation, I. ArXiv preprint, arxiv.org/abs/2005.15861v2, 2022. 2, 5, 9.1

[6] Nicolas Billerey, Imin Chen, Lassina Dembélé, Luis Dieulefait, and Nuno Freitas. Some extensions of the modular method and Fermat equations of signature \((13, 13, n)\). Publ. Mat., 67(2):715–741, 2023. 3

[7] Nicolas Billerey, Imin Chen, Luis Dieulefait, and Nuno Freitas. A result on the equation \(x^p + y^p = z^r\) using Frey abelian varieties. Proc. Amer. Math. Soc., 145(10):4111–4117, 2017. 8

[8] D. Blasius and J. Rogawski. Galois representations. In Travaux mathématiques. Vol. XXIII, volume 23 of Trav. Math., pages 5–35. Fac. Sci. Technol. Commun. Univ. Luxemb., Luxembourg, 2013. 2

[9] G. Böckle. Galois representations. In Travaux mathématiques. Vol. XXIII, volume 23 of Trav. Math., pages 5–35. Fac. Sci. Technol. Commun. Univ. Luxemb., Luxembourg, 2013. 2

[10] M. Börner, I. Bouw, and S. Wewers. The functional equation for \(L\)-functions of hyperelliptic curves. Exp. Math., 26(4):396–411, 2017. 7, 7

[11] N. Bruin. Chabauty methods using elliptic curves. J. Reine Angew. Math., 562:27–49, 2003. 9

[12] H. Carayol. Sur les représentations \(l\)-adiques associées aux formes modulaires de Hilbert. Ann. Sci. École Norm. Sup. (4), 19(3):409–468, 1986. 6, 3

[13] I. Chen. On Siegel’s modular curve of level 5 and the class number one problem. J. Number Theory, 74(2):278–297, 1999. 6

[14] I. Chen and A. Koutsianas. Supporting files for this paper, github.com/akoutsianas/pp5. 1, 7

[15] S. R. Dahmen and S. Siksek. Perfect powers expressible as sums of five or seventh powers. Acta Arith., 164(1):65–100, 2014. 9

[16] H. Darmon. Rigid local systems, Hilbert modular forms, and Fermat’s Last Theorem. Duke Math. J., 102(3):413–449, 2000. 1, 1, 1.3, 1, 5, 5, 5, 5, 5, 5.7, 6, 6, 7.4, 7.1, 7.8, 7.16, 7.22, 7.26, 7.3, 8

[17] H. Darmon, F. Diamond, and R. 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. 7.2.1

[18] H. Darmon and A. Granville. On the equations \(z^m = F(x, y)\) and \(Ax^p + By^q = Cz^r\). Bull. London Math. Soc., 27(6):513–543, 1995. 1

[19] H. Darmon and L. Merel. Winding quotients and some variants of Fermat’s Last theorem. J. Reine Angew. Math., 490:81–100, 1997. 1, 5.6

[20] P. Deligne. Formes modulaires et représentations \(l\)-adiques. In Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, volume 175 of Lecture Notes in Math., pages No. 355, 139–172. Springer, Berlin, 1971. 3

[21] P. Deligne and D. Mumford. The irreducibility of the space of curves of given genus. Inst. Hautes Études Sci. Publ. Math., (36):75–109, 1969. 4

[22] P. Deligne and J.-P. Serre. Formes modulaires de poids 1. Ann. Sci. École Norm. Sup. (4), 7:507–530, 1974. 3
[23] M. Dimitrov. Galois representations modulo $p$ and cohomology of Hilbert modular varieties. *Ann. Sci. École Norm. Sup.* (4), 38(4):505–551, 2005. 8

[24] P. G. L. Dirichlet. Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré. *J. reine angew. Math.*, 3:354–375, 1828. 9

[25] T. Dokchitser, V. Dokchitser, C. Maistret, and A. Morgan. Semistable types of hyperelliptic curves. In *Algebraic curves and their applications*, volume 724 of *Contemp. Math.*, pages 73–135. Amer. Math. Soc., Providence, RI, 2019. 2, 7.3, 7.17

[26] T. Dokchitser, V. Dokchitser, C. Maistret, and A. Morgan. Arithmetic of hyperelliptic curves over local fields. *Math. Ann.*, 385(3-4):1213–1322, 2023. 2, 7.3, 7.17

[27] Tim Dokchitser and Christopher Doris. 3-torsion and conductor of genus 2 curves. *Math. Comp.*, 88(318):1913–1927, 2019. 7.16, 7.3, 7.17

[28] M. Eichler. Quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. *Arch. Math.*, 5:355–366, 1954. 3

[29] N. Freitas. Recipes to Fermat-type equations of the form $x^r + y^r = C z^p$. *Math. Z.*, 279(3-4):605–639, 2015. 1

[30] K. Fujiwara. Level optimization in the totally real case. ArXiv preprint, arxiv.org/abs/math/0602586, 2018. 9.2

[31] F. Jarvis. Level lowering for modular mod $\ell$ representations over totally real fields. *Math. Ann.*, 313(1):141–160, 1999. 7.8, 7.2.1, 7.16, 7.22, 7.3

[32] F. Jarvis. Correspondences on Shimura curves and Mazur’s principle at $p$. *Pacific J. Math.*, 213(2):267–280, 2004. 9.2

[33] C. Khare and J. Thorne. Automorphy of some residually $S_5$ Galois representations. *Math. Z.*, 286(1-2):399–429, 2017. 6

[34] C. Khare and J.-P. Wintenberger. Serre’s modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009. 6

[35] C. Khare and J.-P. Wintenberger. Serre’s modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009. 6

[36] M. Kisin. Modularity of 2-adic Barsotti-Tate representations. *Invent. Math.*, 178(3):587–634, 2009. 6

[37] A. Kraus. Courbes elliptiques semi-stables sur les corps de nombres. *Int. J. Number Theory*, 3(4):611–633, 2007. 8

[38] A. Kraus. Sur l’équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7(1):1–13, 1998. 9

[39] R. Langlands. Modular forms and $\ell$-adic representations. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, volume Vol. 349 of *Lecture Notes in Math.*, pages 361–500. Springer, Berlin-New York, 1973. 3

[40] Q. Liu. Courbes stables de genre 2 et leur schéma de modules. *Math. Ann.*, 295(2):201–222, 1993. 2, 3, 7.2.1

[41] Q. Liu. Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète. *Trans. Amer. Math. Soc.*, 348(11):4577–4610, 1996. 3, 3

[42] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications. 3, 1, 3

[43] P. Lockhart. On the discriminant of a hyperelliptic curve. *Trans. Amer. Math. Soc.*, 342(2):729–752, 1994. 3, 3, 3

[44] P. Lockhart, M. Rosen, and J. Silverman. An upper bound for the conductor of an abelian variety. *J. Algebraic Geom.*, 2(4):569–601, 1993. 7.25

[45] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. 7.2.1

[46] M. Ohta. On the zeta function of an abelian scheme over the Shimura curve. *Japan. J. Math. (N.S.)*, 9(1):1–25, 1983. 3

[47] A. Rajaei. On the levels of mod $\ell$ Hilbert modular forms. *J. Reine Angew. Math.*, 537:33–65, 2001. 9.2

[48] K. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976. 4, 6.2
J. Rogawski and J. Tunnell. On Artin L-functions associated to Hilbert modular forms of weight one. *Invent. Math.*, 74(1):1–42, 1983.

M. Romagny. Models of curves. In *Arithmetic and geometry around Galois theory*, volume 304 of *Progr. Math.*, pages 149–170. Birkhäuser/Springer, Basel, 2013.

T. Saito. Hilbert modular forms and p-adic Hodge theory. *Compos. Math.*, 145(5):1081–1113, 2009.

J.-P. Serre. Propriétés galoisienes des points d’ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

G. Shimura. Correspondances modulaires et les fonctions ζ de courbes algébriques. *J. Math. Soc. Japan*, 10:1–28, 1958.

G. Shimura. Algebraic number fields and symplectic discontinuous groups. *Ann. of Math. (2)*, 86:503–592, 1967.

G. Shimura. The special values of the zeta functions associated with Hilbert modular forms. *Duke Math. J.*, 45(3):637–679, 1978.

G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kano Memorial Lectures, 1.

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.

W. Tautz, J. Top, and A. Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math.*, 43(5):1055–1064, 1991.

R. Taylor. On Galois representations associated to Hilbert modular forms. *Invent. Math.*, 98(2):265–280, 1989.

R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

A. Wiles. On ordinary λ-adic representations associated to modular forms. *Invent. Math.*, 94(3):529–573, 1988.

A. Wiles. Modular elliptic curves and Fermat’s Last Theorem. *Annals of Mathematics*, 144:443–551, 1995.

C. Wu. *F-virtual Abelian Varieties of GL2-type and Rallis Inner Product Formula*. ProQuest LLC, Ann Arbor, MI, 2011. Thesis (Ph.D.)–Columbia University.

**Department of Mathematics, Simon Fraser University, Burnaby, BC V5A 1S6, Canada.**

*Email address: ichen@sfu.ca*

**Department of Mathematics, Aristotle University of Thessaloniki, 54124, Thessaloniki, Greece.**

*Email address: akoutsianas@math.auth.gr*