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

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

In particular, we develop the machinery necessary to prove an optimal bound on the exponent p for solutions satisfying certain 2-adic and 5-adic conditions which are natural from the point of view of the method. The above equation is an example of a generalized Fermat equation for which higher dimensional Frey varieties are needed for the modular method to work and thus represents an interesting test case for Darmon's program.

CONTENTS

1

1. INTRODUCTION

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

$$(1.1) \qquad\qquad x^r + y^q = z^p.$$

We say that a solution $(a, b, c) \in \mathbb{Z}^3$ to (1.1) is *primitive* if $\gcd(a, b, c) = 1$, and *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 [43] [42] using Galois representations and modularity. In [12], Darmon described a program to show the generalized Fermat equations (1.1) have no non-trivial solutions for fixed primes $r, q \geq 3$ and 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 [12] for the case (p, p, r) using 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 is no longer the main difficulty.

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

Unlike signature (r, r, p) where one still has Frey elliptic curves due to [20], signature (p, p, r) for $r \geq 5$ necessitates consideration of Frey abelian varieties of dimension greater than 1 if the exponents are prime. For $r = 2, 3$, signature (p, p, r) equations were resolved in [14] 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.

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. In particular, we prove the following theorem.

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

$$(1.2) \qquad\qquad x^n + y^n = z^5$$

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 hyperelliptic curves introduced in [12] for signature $(p, p, 5)$ and necessitates the development of the following innovations:

(1) We provide more general local results which can be used for establishing irreducibility of residual Galois representations attached to Frey hyperelliptic curves.

(2) Typically, the conductor at 2 of a Frey hyperelliptic is more difficult to determine. We show that it can be read off up to twist by using the relation between odd Frey hyperelliptic curves and the Legendre family of elliptic curves. This allows us to apply repeated elimination steps using several twists of the Frey hyperelliptic curve to avoid an exact determination of conductors and delicate inertia arguments at primes above 2 such as in [4].

(3) We give a precise conductor calculation at the prime above 5 of the Frey hyperelliptic curves by identifying extensions which achieve semistable reduction.

The programs and output transcripts for the computations needed in this paper are described and posted at [10].

2. Acknowledgements

3. Hyperelliptic equations

In this section, we summarize the basic theory of hyperelliptic equations, which is taken in part from [31, 32, 33, 34].

Let K be a finite extension of $\mathbb{Q}_\ell$. 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

$$(3.1) \qquad y^2 + Q(x)y = P(x),$$

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

$$(3.2) \qquad 2g+1 \le \max(2\deg Q, \deg P) \le 2g+2.$$

Let

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

and suppose c is the leading coefficient of R. The *discriminant* of E [32] is given by

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

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

3

Definition 3.1. An algebraic curve C 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 $\mathcal{O}$ such that $K(F) \cong K(C) = K(E)$ is a called *a hyperelliptic model* for C.

Two hyperelliptic models E, F for a hyperelliptic curve C over K are related by the transformations

$$E : y^2 + Q(x)y = P(x),$$
$$F : z^2 + T(u)z = S(u),$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K), \quad e \in K^*, \quad H(u) \in K[u], \quad \deg(H) \leq g+1,$$

(3.3)
$$x = \frac{au+b}{cu+d}, \quad y = \frac{ez + H(u)}{(cu+d)^{g+1}},$$
$$\Delta_F = \Delta_E \, e^{-4(n-1)}(ad-bc)^{n(n-1)}.$$

In particular, we note that the valuation of the discriminant modulo

(3.4)
$$\gcd(4(n-1), n(n-1)),$$

is an invariant of the isomorphism class of C.

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

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

Two odd degree hyperelliptic models $E : y^2 + Q(x)y = P(x)$ 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

$$x = e^2 u + r, \quad y = e^{2g+1}z + t(u), \quad \text{where}$$
$$e \in K^*, \quad r \in K, \quad t \in K[u], \quad \deg(t) \leq g.$$

The discriminants of the odd degree hyperelliptic models are related by

(3.5)
$$\Delta_F = \Delta_E \, e^{-4g(2g+1)},$$

hence the valuation of the discriminant modulo $4g(2g+1)$ is an invariant of the isomorphism class of C among odd degree models.

Definition 3.2. A *model $\mathcal{C}$* over $\mathcal{O}$ for a hyperelliptic 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 $\mathcal{C}$.

Definition 3.3. A model $\mathcal{C}$ over $\mathcal{O}$ for a hyperelliptic 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 $\mathcal{C}$ 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 hyperelliptic curve C over K has *good reduction* (resp. *bad semistable reduction*) if and only if there is some model $\mathcal{C}$ over $\mathcal{O}$ 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 $y^2 + Q(x)y = P(x)$ is a hyperelliptic model over $\mathcal{O}$ of a hyperelliptic curve over K. If $Q(x) = b_{g+1}x^{g+1} + \cdots + b_0$ and $P(x) = a_n x^n + \cdots + a_0$, then we define the *valuation vectors over* K of this hyperelliptic model as the pair of vectors

$$(v(a_0), \cdots, v(a_n)) \qquad (v(b_0), \cdots, v(b_{g+1})).$$

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 $\mathcal{C}$ over $\mathcal{O}$ such that $v(\Delta(\mathcal{C})) = 0$.*

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

Suppose C has good reduction, so there exists a model $\mathcal{C}$ of C with good reduction. By [33, Exercise 8.3.6], the hyperelliptic map

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

extends to

$$\pi : \mathcal{C} \to \mathbb{P}^1_{\mathcal{O}}.$$

As a result, $\mathcal{C}_k$ is a non-singular pointed hyperelliptic curve with a k-rational point $\tilde{P}$ where $\tilde{P}$ is the reduction of P mod v, so using [34, Proposition 1.2] it follows that $\mathcal{C}_k$ can be given by a non-singular odd degree hyperelliptic equation. We deduce that C has an odd degree hyperelliptic model $\mathcal{C}$ such that $v(\Delta(\mathcal{C})) = 0$. $\qquad\qquad\square$

Definition 3.7. 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 3.8. *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 $\mathcal{C}$ that has integral special fiber, then J/K has multiplicative reduction.*

Proof. See [15, Theorem 2.4] for the first assertion. As the special fiber of the given model over $\mathcal{O}$ is integral, $X' = X_{\mathrm{red}} = X = \mathcal{C}$ and $c = 1$ in [38, Lemma 3.3.5] so the toric rank of J is positive. Thus, J has multiplicative reduction. $\qquad\qquad\square$

4. DARMON'S FREY HYPERELLIPTIC CURVE FOR SIGNATURE (p, p, r)

In this section, we briefly review from [12, 41] the construction of a suitable Frey hyperelliptic curve for the equation

$$(4.1) \qquad\qquad x^p + y^p = z^r,$$

where $r \geq 3$ and p are odd primes.

Let ζ be a primitive rth root of unity, $\omega_j = \zeta^j + \zeta^{-j}$, and put

$$g(X) = \prod_{j=1}^{\frac{r-1}{2}} (X + \omega_j).$$

From here on, we let $K = \mathbb{Q}(\zeta + \zeta^{-1})$ and denote by $\mathfrak{r}$ the unique prime above r in K. We also use the notation $\mathfrak{q}_q$ to denote a prime of K above q.

Proposition 4.1. *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 [41, Proposition 3]. $\qquad\square$

Proposition 4.2. *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 [41, Remark, p. 1058]. $\qquad\square$

Consider the following hyperelliptic curves
$$\begin{aligned} C_r^-(t): \quad y^2 &= f_t^-(x) := f(x) + 2 - 4t, \\ C_r^+(t): \quad y^2 &= f_t^+(x) := (x + 2)(f(x) + 2 - 4t), \end{aligned}$$
where $f(x) = xg(x^2 - 2)$.

Theorem 4.3. *The discriminants of the polynomials* $f_r^-(x)$ *and* $f_r^+(x)$ *are given by*
$$\Delta(f_t^-) = (-1)^{\frac{r-1}{2}} 2^{2(r-1)} r^r t^{\frac{r-1}{2}} (t - 1)^{\frac{r-1}{2}}$$
$$\Delta(f_t^+) = (-1)^{\frac{r+1}{2}} 2^{2(r+1)} r^r t^{\frac{r+3}{2}} (t - 1)^{\frac{r-1}{2}}.$$

Proof. This is stated in slightly different form in the proof of [12, Proposition 1.15]. For further details on how such formulae can be justified, we refer the reader to [6]. $\qquad\square$

Theorem 4.4. *Let* $J_r^\pm(t)$ *be the Jacobian of the hyperelliptic curve* $C_r^\pm(t)$. *Then, the endomorphism algebra* $\mathrm{End}_K(J_r^\pm(t)) \otimes \mathbb{Q}$ *contains the field* K.

Proof. For $J_r^-(t)$, see [41, Theorem 1]. For $J_r^+(t)$, the result follows from [41, Remark, p. 1058] and modifying the argument in [41, §3.1]. $\qquad\square$

Let $(a, b, c) \in \mathbb{Z}^3$ be a non-trivial primitive solution to (4.1). The following lemma is readily verified and appears in [12, p. 425].

Lemma 4.5. *Let*
$$\begin{aligned} C_r^-(a, b, c): \quad y^2 &= c^r f(x/c) - 2(a^p - b^p), \\ C_r^+(a, b, c): \quad y^2 &= (x + 2c)(c^r f(x/c) - 2(a^p - b^p)). \end{aligned}$$
Then

(1) $C_r^-(a, b, c)$ *is isomorphic to a twist of* $C_r^-(t)$ *over* $\mathbb{Q}$ *where* $t = \frac{a^p}{c^r}$,

(2) $C_r^+(a, b, c)$ *is isomorphic to* $C_r^+(t)$ *over* $\mathbb{Q}$ *where* $t = \frac{a^p}{c^r}$.

Some explicit examples are listed below.

$C_r^-(a, b, c)$ for:

$$
\begin{aligned}
r = 3: \quad & y^2 = (x^3 - 3c^2x - 2(a^p - b^p)) \\
r = 5: \quad & y^2 = (x^5 - 5c^2x^3 + 5c^4x - 2(a^p - b^p)) \\
r = 7: \quad & y^2 = (x^7 - 7c^2x^5 + 14c^4x^3 - 7c^6x - 2(a^p - b^p)) \\
r = 11: \quad & y^2 = (x^{11} - 11c^2x^9 + 44c^4x^7 - 77c^6x^5 + 55c^8x^3 - 11c^{10}x - 2(a^p - b^p)).
\end{aligned}
$$

$C_r^+(a, b, c)$ for:

$$
\begin{aligned}
r = 3: \quad & y^2 = (x + 2c)(x^3 - 3c^2x - 2(a^p - b^p)) \\
r = 5: \quad & y^2 = (x + 2c)(x^5 - 5c^2x^2 + 5c^4x - 2(a^p - b^p)) \\
r = 7: \quad & y^2 = (x + 2c)(x^7 - 7c^2x^5 + 14c^4x^3 - 7c^6x - 2(a^p - b^p)) \\
r = 11: \quad & y^2 = (x + 2c)(x^{11} - 11c^2x^9 + 44c^4x^7 - 77c^6x^5 + 55c^8x^3 - 11c^{10}x - 2(a^p - b^p)).
\end{aligned}
$$

From Theorem 4.3 and Lemma 4.5, the discriminants of the hyperelliptic curves $C_r^-(a, b, c)$ and $C_r^+(a, b, c)$ are given by

(4.2) $$\Delta(C_r^-) = (-1)^{(r-1)/2} 2^{2(r-1)} r^r a^{p(r-1)/2} b^{p(r-1)/2}$$

(4.3) $$\Delta(C_r^+) = (-1)^{(r-1)/2} 2^{2(r+1)} r^r a^{p(r+3)/2} b^{p(r-1)/2}.$$

We denote by $J_r^\pm = J_r^\pm(a, b, c)$ the Jacobians of $C_r^\pm(a, b, c)$.

Remark 4.6. $C_r^\pm(1, -1, 0)$ is non-singular and $J_r^\pm(1, -1, 0)$ has complex multiplication by $\mathbb{Q}(\zeta)$ [12, Proposition 3.7].

5. MODULARITY OF $\rho_{J^\pm, \mathfrak{p}}$

Let $G_M = \mathrm{Gal}(\overline{M}/M)$ denote the absolute Galois group of a number field M, where $\overline{M}$ is an algebraic closure of M.

From this section onward, we specialize to the case $r = 5$. For convenience, we denote $C^\pm = C_5^\pm$ and $J^\pm = J_5^\pm$.

Let $(a, b, c) \in \mathbb{Z}^3$ be a non-trivial primitive solution to (4.1).

Theorem 5.1. *Suppose* $5 \mid ab$. *Then* $\rho_{J^+, \mathfrak{p}}$ *is modular.*

Proof. This is [12, Theorem 2.9]. $\qquad\square$

In the case $5 \nmid ab$, there is no currently known modularity result we can apply to prove that $\rho_{J^+, \mathfrak{p}}$ is modular in all cases. Therefore, we will work instead with $\rho_{J^-, \mathfrak{p}}$.

Lemma 5.2. *Suppose $2 \mid a$, $b \equiv c \equiv -1 \pmod 4$, and $p > 3$. Then, the conductor at $\mathfrak{q}_2$ of the elliptic curve E/K given by*

$$E : y^2 = x(x + a^p)(x - b^p) \tag{5.1}$$

is $\mathfrak{q}_2$. Furthermore, $\bar{\rho}_{E,5}$ has conductor at $\mathfrak{q}_2$ dividing $\mathfrak{q}_2$.

Proof. This can be proven using Tate's algorithm, for instance [13, §2.2]. Under the conditions on a, b, c and p, the minimal discriminant of E is given by $\Delta_E = 2^{-8}(ab)^{2p}c^{10}$. Note $\bar{\rho}_{E,5}$ has conductor at $\mathfrak{q}_2$ equal to $\mathfrak{q}_2$ if and only if $5 \nmid v_2(\Delta_E) = 2pv_2(a) - 8$. □

Proposition 5.3. *The representation $\bar{\rho}_{J^-,\mathfrak{r}}$ extends to $G_\mathbb{Q}$ and is absolutely irreducible when restricted to $G_{K(\zeta_r)}$.*

Proof. The abelian variety J^-/K is of GL$_2$-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 $K \otimes \mathbb{Q}_5 \simeq K_{\mathfrak{q}_r}$.

Since J^- is defined over $\mathbb{Q}$, as Darmon explains in [12, p. 443], the action of G_K on $T_5(J^-) \otimes \mathbb{Q}_5$ as a $K_{\mathfrak{q}_r}$-vector space extends to a $G_\mathbb{Q}$-action that is G_K-semilinear; it satisfies

$$\sigma(av) = \sigma(a)\sigma(v),$$

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

By [12, Theorem 2.6], we have that $\bar{\rho}_{J^-,\mathfrak{r}}$ arises up to quadratic twist from the Legendre family given by

$$L : y^2 = x(x - 1)(x - t), \tag{5.2}$$

where $t = a^p/c^r$. More precisely, there is a quadratic character χ of G_K such that

$$\bar{\rho}_{J^-,\mathfrak{r}} \simeq \bar{\rho}_{L,5} \otimes \chi. \tag{5.3}$$

Suppose that $\bar{\rho}_{J^-,\mathfrak{r}}|_{G_{K(\zeta_5)}}$ is reducible; thus $\bar{\rho}_{L,5}|_{G_{K(\zeta_5)}}$ 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 $\bar{\rho}_{L,5}|_{G_{K(\zeta_5)}}$ 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 $\bar{\rho}_{L,5}|_{G_K}$ is the normalizer of C'. Thus, for L to have this property we must have that

$$j_L(t) - 1728 = j_{5N'}(s) - 1728. \tag{5.4}$$

where

$$j_{5N'}(s) = \frac{125s(2s + 1)^3(2s^2 + 7s + 8)^3}{(s^2 + s - 1)^5} \tag{5.5}$$

8

is the j-invariant of elliptic curves with normalizer of non-split Cartan structure on 5-torsion points [9, Corollary 5.3]. Since the left hand side is a square, L would give rise to a K-rational point on the hyperelliptic curve

$$(5.6) \qquad y^2 = 2 \left(x^2 + \frac{7}{2}x + \frac{27}{8} \right) (x^2 + x - 1).$$

Using `Magma`, it can be checked that all K-rational points arise from cusps. $\qquad \square$

Theorem 5.4. *Suppose* $2 \mid a$, $b \equiv c \equiv -1 \pmod 4$. *Then* $\rho_{J^-,\mathfrak{p}}$ *is modular.*

Proof. By Proposition 5.3, the representation $\bar\rho_{J^-,\mathfrak{r}}$ is absolutely irreducible and extends to a representation $\bar\rho$ of $G_{\mathbb{Q}}$. By Serre's Conjecture over $\mathbb{Q}$, now proven in [25, 26, 27], $\bar\rho$ is modular, hence $\bar\rho_{J^-,\mathfrak{r}}$ is also modular by cyclic base change. Modularity of J^-/K now follows from [24, Theorem 1.1] by checking its three hypotheses:

(1) The representation $\rho_{J^-,\mathfrak{r}}$ 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 $\rho_{J^-,\mathfrak{r}}$ is deRham and hence Hodge-Tate. The Hodge-Tate weights of $\rho_{J^-,\mathfrak{r}}$ are $\{0,1\}$.
(3) The representation $\bar\rho_{J^-,\mathfrak{r}} \mid_{G_{K(\zeta_5)}}$ is absolutely irreducible from Proposition 5.3.

Since J^- is modular, $\rho_{J^-,\mathfrak{p}}$ is modular for every prime $\mathfrak{p}$ of K. $\qquad \square$

6. Conductors of $\bar\rho_{J^\pm,\mathfrak{p}}$

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

$$(6.1) \qquad\qquad \Delta(C^-) = 2^8 5^5 (ab)^{2p},$$
$$(6.2) \qquad\qquad \Delta(C^+) = 2^{12} 5^5 (a^2 b)^{2p},$$

from (4.2)-(4.3) in the case $r = 5$.

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 we have that

$$(6.3) \qquad\qquad V_p(J^\pm) \cong \oplus_{\mathfrak{p}|p} V_{\mathfrak{p}}(J^\pm)$$

where $V_{\mathfrak{p}}(J^\pm) = V_p(J^\pm) \otimes K_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic Tate module of $J^\pm$, $K_p = \oplus_{\mathfrak{p}|p} K_{\mathfrak{p}}$, and $K_{\mathfrak{p}}$ is the completion of K at $\mathfrak{p}$.

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

By Theorems 5.1 and 5.4, $J^\pm/K$ is modular, which implies the $\rho_{J^\pm,\mathfrak{p}}$ over all primes $\mathfrak{p}$ of K form a strictly compatible system of $\mathfrak{p}$-adic representations. Hence, the $\rho_{J^\pm,\mathfrak{p}}$ all have isomorphic local Weil-Deligne representations at primes $\mathfrak{q}$ not dividing p, and therefore have the same conductor exponent at $\mathfrak{q}$ independent of $\mathfrak{p} \mid p$.

Remark 6.1. The work of Dokchitser-Dokchitser-Maistret-Morgan [19, 18] gives a method to compute the conductor of a fixed hyperelliptic curve over local fields of odd residual characteristic. Anni-Dokchitser [2] have made this explicit in the case when the defining polynomial involves factors with shifted t-Eisenstein polynomials.

Let $K_{\mathfrak{q}_r}$ and $K_{\mathfrak{q}_2}$ denote the completions of K at the unique primes $\mathfrak{q}_r$ and $\mathfrak{q}_2$ of K above r and 2, respectively.

Lemma 6.2. *Let $q \neq 2, 5$ be a prime and $\mathfrak{q}$ a prime of K above q. Then $C^{\pm}/K$ and $J^{\pm}/K$ are semistable at $\mathfrak{q}$. In particular, if $C^{\pm}/K$ has bad semistable reduction, then $J^{\pm}/K$ has multiplicative reduction.*

Proof. Suppose $\mathfrak{q}$ is a prime of K that does not divide 2 and 5. From Lemma 4.5 the curve C^- is given by
$$C^- : \ y^2 = x^5 - 5c^2 x^3 + 5c^4 x - 2(a^p - b^p).$$
By (4.2) we recall that
$$\Delta(C_r^-) = (-1)^{(r-1)/2} 2^{2(r-1)} r^r a^{p(r-1)/2} b^{p(r-1)/2}.$$
By Proposition 3.6 if $\mathfrak{q} \nmid ab$ then C^-/K has good reduction at $\mathfrak{q}$.

Suppose $\mathfrak{q} \mid ab$. We treat the case $\mathfrak{q} \mid a$, as the case $\mathfrak{q} \mid b$ is similar. The special fiber of C^- in the case $\mathfrak{q} \mid a$ 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 $\mathbb{F}_{\mathfrak{q}}$ of $\mathfrak{q}$. As $\Delta(x^2 - \tilde{c}x - \tilde{c}^2) = 5\tilde{c}^2 \neq 0$ in $\mathbb{F}_{\mathfrak{q}}$, it follows that C^- satisfies the double root criterion [7, Lemma 3.7]. Hence C^- has bad semistable reduction at $\mathfrak{q}$, and therefore C^- is semistable at $\mathfrak{q}$. A similar argument can be given for C^+.

Finally, the statement for $J^{\pm}$ follows from the statement about $C^{\pm}$, [7, Proposition 3.1], and Theorem 3.8. $\qquad\square$

Let m be a rational prime and S a finite set of primes of K. We denote by $K(S, m)$ 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 $K(\sqrt[m]{d})/K$ where $d \in K(S, m)$.

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

Theorem 6.3. *Let $p \neq 2, 5$ be a prime.*

(1) *Suppose $2 \nmid ab$ and $5 \mid ab$. Then the Serre level of $\bar{\rho}_{J^+, \mathfrak{p}}$ divides $\mathfrak{q}_r$.*
(2) *Suppose $2 \mid a$, $b \equiv c \equiv -1 \pmod 4$, and $5 \nmid ab$. Then, for some character $\chi_0 \in K(S_2, 2)^*$, where $S_2 = \{\mathfrak{q}_2\}$, the Serre level of $\bar{\rho}_{J^-, \mathfrak{p}} \otimes \chi_0$ is equal to $\mathfrak{q}_2^s \cdot \mathfrak{q}_r^t$ where $s = 0, 1$ and $t = 2, 3$.*

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

Proof. For primes $\mathfrak{q}$ of K not dividing 10, $\bar{\rho}_{J^{\pm}, \mathfrak{p}}$ is unramified at $\mathfrak{q} \nmid p$, and finite at $\mathfrak{q}$ if $\mathfrak{q} \mid p$ by [12, Proposition 1.15].

By Theorem 6.5 for $\rho_{J^+,\mathfrak{p}}$ we have that

$$N(\rho_{J^+,\mathfrak{p}}) = \mathfrak{q}_r \cdot \prod_{\mathfrak{q} \neq \mathfrak{q}_r, \mathfrak{q}|ab} \mathfrak{q}$$

Therefore the Serre level of $\bar{\rho}_{J^+,\mathfrak{p}}$ divides $\mathfrak{q}_r$ (see also [12, Theorem 3.5]).

By Theorem 6.7 for $\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ we have that

$$N(\rho_{J^-,\mathfrak{p}} \otimes \chi_0) = \mathfrak{q}_2 \cdot \mathfrak{q}_r^t \cdot \prod_{\mathfrak{q} \neq \mathfrak{q}_2, \mathfrak{q}_r, \mathfrak{q}|ab} \mathfrak{q}$$

where $t = 2, 3$. Therefore, the Serre level of $\bar{\rho}_{J^-,\mathfrak{p}} \otimes \chi_0$ divides $\mathfrak{q}_2 \cdot \mathfrak{q}_r^t$. As the image of inertia of $\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ at $\mathfrak{q}_r$ has order coprime to $p \neq 2, 5$ by the proof of Proposition 6.14, the conductor of $\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ at $\mathfrak{q}_r$ does not degenerate upon reduction mod $\mathfrak{p}$ by applying [22, Theorem 1.5]. We conclude the conductor of $\bar{\rho}_{J^-,\mathfrak{p}} \otimes \chi_0$ at $\mathfrak{q}_r$ is still $\mathfrak{q}_r^t$. Finally, by Proposition 6.12 the conductor of $\bar{\rho}_{J^-,\mathfrak{p}} \otimes \chi_0$ at $\mathfrak{q}_2$ divides $\mathfrak{q}_2$. $\square$

Remark 6.4. The 2-Selmer group $K(S_2, 2)$ can be computed in `Magma` to be

$$(6.4) \qquad K(S_2, 2) = \left\{ 1, -1, -2, 2, \frac{-\sqrt{5}+1}{2}, \frac{\sqrt{5}-1}{2}, \sqrt{5}-1, -\sqrt{5}+1 \right\}.$$

6.1. **The conductor exponent of $\rho_{J^+,\mathfrak{p}}$.** In this section we compute the conductor of $\rho_{J^+,\mathfrak{p}}$.

Theorem 6.5. *Suppose $2 \nmid ab$ and $5 \mid ab$. Then $N(\rho_{J^+,\mathfrak{p}}) = \mathfrak{q}_r \cdot \mathfrak{q}_{ab}$ where $\mathfrak{q}_{ab}$ is the square-free ideal of K divisible by the primes $\mathfrak{q} \neq \mathfrak{q}_5$ and $\mathfrak{q} \mid ab$.*

Proof. By the proof of [12, Proposition 1.15], C^+/K has good reduction at the prime $\mathfrak{q}_2$. Applying Lemma 6.2, Lemma 6.6 and Theorem 3.8 show that J^+/K has multiplicative reduction at the primes $\mathfrak{q} \mid \mathfrak{q}_r \cdot \mathfrak{q}_{ab}$ and good reduction for the other primes $\mathfrak{q}$. The argument in [6, Theorem 9.15(d)] using Grothendieck's inertial criterion then allows us to conclude the conductor exponents of $\rho_{J^+,\mathfrak{p}}$ at the primes $\mathfrak{q} \mid \mathfrak{q}_r \cdot \mathfrak{q}_{ab}$ are 1. $\square$

Lemma 6.6. *Suppose $5 \mid ab$. Then the curve $C^+/K_{\mathfrak{q}_r}$ has bad semistable reduction.*

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

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

Assume $5 \mid a$. Making the substitution $x \to \sqrt{5}x - a^p - 2c$ and $y \to \sqrt{5}^3 y$ we obtain a model with valuation vectors over $K_{\mathfrak{q}_r}$

$$(\geq 1, \geq 1, 0, 1, 0, 1, 0) \qquad (\infty, \infty, \infty, \infty),$$

which satisfies the double root criterion.

Otherwise $5 \mid b$. Making the substitution $x \to \sqrt{5}x + a^p - 2c$ and $y \to \sqrt{5}^3 y$ we obtain a model with valuation vectors over $K_{\mathfrak{q}_r}$

$$(\geq 1, \geq 1, 0, 1, 0, 1, 0) \qquad (\infty, \infty, \infty, \infty).$$

$\square$

6.2. **The conductor exponent of $\rho_{J^-,\mathfrak{p}}$.** In this section we compute the conductor of $\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ where $\chi_0 \in K(S_2, 2)^*$ with $S_2 = \{\mathfrak{q}_2\}$.

Theorem 6.7. *Suppose* $2 \mid a$, $b \equiv c \equiv -1 \pmod 4$, $5 \nmid ab$, *and* $p > 5$. *Then, for some choice of* χ_0, *the conductor of* $\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ *is of the form* $\mathfrak{q}_2 \cdot \mathfrak{q}_r^t \cdot \mathfrak{q}_{ab}$ *where* $t = 2, 3$ *and* $\mathfrak{q}_{ab}$ *is the square-free ideal of* K *divisible by the primes* $\mathfrak{q} \mid ab$ *and* $\mathfrak{q} \nmid 10$.

Proof. This will follow from Lemma 6.2, and Propositions 6.12 and 6.15. □

6.2.1. *The conductor exponent of* $\rho_{J^-,\mathfrak{p}}$ *at* $\mathfrak{q}_2$.

Proposition 6.8. *Suppose* $2 \mid a$, $b \equiv c \equiv -1 \pmod 4$, *and* $p > 5$. *Then* C^-/K_2 *has potentially bad semistable reduction and* $\rho_{J^-,\mathfrak{p}} \mid_{I_{\mathfrak{q}_2}}$ *has special inertial type.*

Proof. This can be verified using [31, Théorème 1 (I)] and Magma. □

We need the following lemma.

Lemma 6.9. *Let* K *be an unramified extension of* $\mathbb{Q}_2$ *with uniformizer* π *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,

$$(6.5) \qquad \beta^2 = \frac{1 + 2\alpha + \alpha^2}{4}$$

$$(6.6) \qquad = \frac{1 - \alpha^2}{4} + \frac{\alpha}{2}$$

The relative discriminant of $\mathcal{O}_K[\beta] = \mathcal{O}_K + \mathcal{O}_K\beta$ over $\mathcal{O}_K$ is the determinant of

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

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 π. Hence, L/K is unramified. □

Lemma 6.10. *Let* $\chi: G_K \to \{\pm 1\}$ *be a quadratic or the trivial character. Then there exists a character* $\chi_0 \in K(S_2, 2)^*$ *where* $S_2 = \{\mathfrak{q}_2\}$ *such that* $\chi\chi_0$ *is unramified at* $\mathfrak{q}_2$.

Proof. If χ is the trivial character then we choose χ_0 to be the trivial character as well. We now assume that χ 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 [36, Chapter VI, Proposition 1.3], there exists a $u \in K^\times$ such that

$$(6.7) \qquad du^{-1} \in \hat{\mathcal{O}}_K^\times$$

where $\hat{\mathcal{O}}_K^\times = \prod_{v \text{ finite}} \mathcal{O}_{K_v}^\times$. Let $\mathcal{O}_K^\times = \langle -1, \frac{\sqrt{5}+1}{2} \rangle$. It can be checked that reduction map $\mathcal{O}_K^\times$ to $(\mathcal{O}_K/\mathfrak{q}_2^2)^\times$ is surjective. Hence, without loss of generality, we may assume that $u \equiv 1 \pmod{\mathfrak{q}_2^2}$.

Let $d_0 = du^{-1}$, then $d_0 \in K(S_2, 2)$ since $K(\sqrt{d_0})$ is unramified outside of $\mathfrak{q}_2$ by (6.7). Let $\chi_0 \in K(S_2, 2)^*$ and χ_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 $u \equiv 1 \pmod{\mathfrak{q}_2^2}$, by Lemma 6.9 we have that χ_u is unramified at $\mathfrak{q}_2$, therefore $\chi\chi_0$ is unramified at $\mathfrak{q}_2$. $\square$

Proposition 6.11. *Suppose $2 \mid a$, $b \equiv c \equiv -1 \pmod 4$ and $p > 3$. Then there is a character $\chi_0 \in K(S_2, 2)^*$, where $S_2 = \{\mathfrak{q}_2\}$, such that the conductor at $\mathfrak{q}_2$ of $\rho_{J^-,\mathfrak{r}} \otimes \chi_0$ is equal to $\mathfrak{q}_2$.*

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

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

is a quadratic twist of L in (5.2) and hence by (5.3) we have that

(6.8) $$\bar{\rho}_{J^-,\mathfrak{r}} \cong \bar{\rho}_{E,5} \otimes \chi$$

for some quadratic character χ of G_K. By (6.8) we have that $\bar{\rho}_{J^-,\mathfrak{r}} \simeq \bar{\rho}_{E,5} \otimes \chi$ where χ is a character of G_K of order dividing 2. By Lemma 6.10 there exists a character $\chi_0 \in K(S_2, 2)^*$ such that $\chi\chi_0$ is unramified at $\mathfrak{q}_2$. By Lemma 5.2, the conductor at $\mathfrak{q}_2$ of $\bar{\rho}_{J^-,\mathfrak{r}} \otimes \chi_0 \simeq \bar{\rho}_{E,5} \otimes \chi\chi_0$ divides $\mathfrak{q}_2$.

The representation $\bar{\rho}_{J^-,\mathfrak{r}}$ is absolutely irreducible by Proposition 5.3 and modular by Theorem 5.4. Therefore, we conclude that $\rho_{J^-,\mathfrak{r}} \otimes \chi_0$ has conductor $\mathfrak{q}_2$ by applying [22, Theorem 1.5 (2)]. In particular, if the conductor of $\rho_{J^-,\mathfrak{r}} \otimes \chi_0$ is $\mathfrak{q}_2^t$ for $t \geq 2$, degeneration of the conductor occurs under reduction. Since $\rho_{J^-,\mathfrak{r}} \otimes \chi_0 \mid_{I_{\mathfrak{q}_2}}$ has inertial special type associated to a character χ, it follows that the reduction of χ is trivial and $N_{K/\mathbb{Q}}(\mathfrak{q}_2) \equiv 1 \pmod p$, which cannot happen as $N_{K/\mathbb{Q}}(\mathfrak{q}_2) - 1 = 3 < p$. We conclude $t \leq 1$ and hence $t = 1$. $\square$

Proposition 6.12. *Suppose $2 \mid a$, $b \equiv c \equiv -1 \pmod 4$ and $p > 3$. Let χ_0 be a character as in Proposition 6.11. Then the conductor at $\mathfrak{q}_2$ of $\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ is equal to $\mathfrak{q}_2$.*

Proof. The conductor at $\mathfrak{q}_2$ of the compatible system $\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ is independent of $\mathfrak{p}$ for $\mathfrak{p} \nmid 2$, so by Proposition 6.11 we have the conclusion. $\square$

Remark 6.13. As χ_0 is unramified outside of $\mathfrak{q}_2$, the conductors of $\rho_{J^-,\mathfrak{p}}$ and $\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ are equal away from $\mathfrak{q}_2$.

6.2.2. *The conductor exponent of $\rho_{J^-,\mathfrak{p}}$ at $\mathfrak{q}_r$.*

Proposition 6.14. *Suppose $5 \nmid ab$. Let $M/K_{\mathfrak{q}_r}$ be a totally ramified extension of degree 4 and*

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

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

   (i) *If $v_5(d(a, c)) \geq 2$, then $C^-/K_{\mathfrak{q}_r}$ attains good reduction over the extension $M/K_{\mathfrak{q}_r}$.*
   (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 $K_{\mathfrak{q}_r}$ depending on (a_0, b_0, c_0) such that $L/K_{\mathfrak{q}_r}$ is a degree 20 totally ramified extension and $C^-/K_{\mathfrak{q}_r}$ attains good reduction over $L/K_{\mathfrak{q}_r}$.*

Moreover, these extensions are minimal with respect to ramification index.

Proof. The initial model for C^- is given by the equation $y^2 = f(x)$. The hyperelliptic model $y^2 = g(x)$ of C^- has valuation vectors over M

$$(8, 8, \geq 8, 8, \geq 8, 0, \infty) \qquad (\infty, \infty, \infty, \infty), \qquad \text{if } v_5(d(a,c)) = 1,$$
$$(\geq 10, 8, \geq 8, 8, \geq 8, 0, \infty) \qquad (\infty, \infty, \infty, \infty), \qquad \text{if } v_5(d(a,c)) \geq 2.$$

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

Case $v_5(d(a,c)) \geq 2$: The substitution $x \to \pi_M^2 x$, $y \to \pi_M^5 y$ gives us a model with good reduction over M, where π_M is a uniformizer of M.

The extension $M/K_{\mathfrak{q}_r}$ has minimal ramification index with the property that C^-/M has good reduction: Suppose C^- attains good reduction over an extension $F/K_{\mathfrak{q}_r}$ 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 $v_{K_{\mathfrak{q}_r}}(\Delta(C^-)) = 10$, it follows that the ramification index of $F/K_{\mathfrak{q}_r}$ must be divisible by 4 from (3.5).

Case $v_5(d(a,c)) = 1$: Let $g_0(x) = f_0(x - a_0^p - 2c_0)$. From the fact that the coefficients of $g(x)$ lie in $\mathbb{Q}_5$ and $M/\mathbb{Q}_5$ is a degree 8 totally ramified extension, we have that 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 θ be a root of $g_0(x)$ and $L = M(\theta)$. Then $L/K_{\mathfrak{q}_r}$ is a 20 degree totally ramified extension. Making the substitution $x \to x + \theta$ to the model $y^2 = g(x)$ of C^-, we obtain a model with valuation vectors over L

$$(\geq 80, 40, \geq 40, 40, \geq 40, 0, \infty) \qquad (\infty, \infty, \infty, \infty).$$

Making the substitution $x \to \pi_L^{10} x$, $y \to \pi_L^{25} y$, we get a model with good reduction over L, where π_L is a uniformizer of L.

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

We know from [40] that $[K_{\mathfrak{q}_r}^{\mathrm{nr}}(J^-[2]) : K_{\mathfrak{q}_r}^{\mathrm{nr}}] \mid [F \cdot K_{\mathfrak{q}_r}^{\mathrm{nr}} : K_{\mathfrak{q}_r}^{\mathrm{nr}}]$, where $K_{\mathfrak{q}_r}^{\mathrm{nr}}$ is the maximal unramified extension of $K_{\mathfrak{q}_r}$. As $g_0(x)$ is an Eisenstein polynomial over $\mathbb{Q}_5$, the extension $\mathbb{Q}_5(\theta)/\mathbb{Q}_5$ is a totally ramified extension of degree 5, which in turn implies the extension $K_{\mathfrak{q}_r}(\theta)/K_{\mathfrak{q}_r}$ is a totally ramified extension of degree 5. Since $K_{\mathfrak{q}_r}(\theta) \subset K_{\mathfrak{q}_r}(J^-[2])$ it follows that $5 \mid [K_{\mathfrak{q}_r}^{\mathrm{nr}}(J^-[2]) : K_{\mathfrak{q}_r}^{\mathrm{nr}}]$, and hence $5 \mid [F \cdot K_{\mathfrak{q}_r}^{\mathrm{nr}} : K_{\mathfrak{q}_r}^{\mathrm{nr}}]$ so $5 \mid e(F/K_{\mathfrak{q}_r})$. We have thus shown $20 \mid e(F/K_{\mathfrak{q}_r})$. $\qquad \square$

Proposition 6.15. *Suppose $5 \nmid ab$. Then the conductor of $\rho_{J^-,\mathfrak{p}}$ at $\mathfrak{q}_r$ is $\mathfrak{q}_r^2$ or $\mathfrak{q}_r^3$ accordingly as $v_5(d(a,c)) \geq 2$ or $v_5(d(a,c)) = 1$, respectively.*

Proof. Let $F = M$ or L as above. The field cut out by $\rho_{J^-,\mathfrak{p}} \mid_{I_{\mathfrak{q}_r}}$ corresponds to the extension $F \cdot K_{\mathfrak{q}_r}^{\mathrm{nr}}/K_{\mathfrak{q}_r}^{\mathrm{nr}}$.

There are finitely many possibilities for F. For each possible choice, we may compute the conductor exponent of $\rho_{J^-,\mathfrak{p}} \mid_{I_{\mathfrak{q}_r}}$ using the Magma. In particular, using Magma's function *GaloisRepresentations* we compute all possible irreducible Galois representations that factor

through the Galois group of $F/K_{\mathfrak{q}_r}$ faithfully. For each Galois representation we compute the conductor which is always equal to $\mathfrak{q}_r^2$ when $F = M$ and $\mathfrak{q}_r^3$ when $F = L$. Therefore, we conclude that the conductor of $\rho_{J^-,\mathfrak{p}}$ is equal to $\mathfrak{q}_r^2$ and $\mathfrak{q}_r^3$ when $F = M$ and L, respectively.

Alternatively, we may obtain a bound on the conductor exponent at $\mathfrak{q}_r$ using the valuation of the relative different of $F/K_{\mathfrak{q}_r}$ and [35, (18)]. The bound on the conductor exponent is ≤ 3 in case $F = L$ and ≤ 2 in case $F = M$. Since we know the reduction type is potentially good reduction, the conductor exponent is 2 or 3, though we do not have an explicit criterion to determine which is the case, unlike the proof above. $\qquad\square$

Remark 6.16. We also point out [12, Proposition 1.16] which covers general r but does not give the exact conductor at $\mathfrak{r}$.

7. IRREDUCIBILITY OF $\bar{\rho}_{J^\pm,\mathfrak{p}}$

We start with K being a finite extension of $\mathbb{Q}_p$, having ring of integers $\mathcal{O}$, uniformizer π, and residue field k. Fix embeddings $\mathbb{Q}_p \subseteq K \subseteq \overline{\mathbb{Q}}_p$ 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 $\psi : I_{t,K} \to \mathbb{F}_{p^n}^\times \subseteq \overline{\mathbb{F}}_p^\times$, denoted θ_{p^n-1} as in [39], 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 7.1. *We have*
$$I_{t,K} \cong \varprojlim_{(d,p)=1} \mu_d \cong \varprojlim_m \mathbb{F}_{p^m}^\times,$$
where the projective limits are over the homomorphisms
$$\mu_{dd'} \longrightarrow \mu_d$$
$$\alpha \longmapsto \alpha^{d'}$$
and
$$\mathbb{F}_{p^{mn}}^\times \longrightarrow \mathbb{F}_{p^m}^\times$$
$$\alpha \longmapsto \alpha^{\frac{1-p^{mn}}{1-p^m}}.$$

Proof. See [39, Section 1.2]. $\qquad\square$

Lemma 7.2. *Suppose $k \cong \mathbb{F}_{p^n}$. Let $\psi = \theta_{p^n-1}$ be the fundamental character of level n.*

- *Suppose L is a finite tamely ramified abelian extension of K such that ψ factors as $\psi = \psi_{L/K} \circ \alpha$ where*
$$\psi_{L/K} : I_{t,L/K} \cong I_K \cdot G_L/G_L \cong I_K/(I_K \cap G_L) \to \mathbb{F}_{p^n}^\times$$

and

$$\alpha : I_{t,K} \to I_{t,L/K}$$

is the natural homomorphism.

- *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 $x \in \mathbb{F}_{p^n}^\times$.

Proof. From [39, 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 ψ is surjective to $\mathbb{F}_{p^n}^\times$ yields the result. $\qquad\square$

Corollary 7.3. *Suppose $\varphi : G_K \to \overline{\mathbb{F}}_p^\times$ 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 $x \in \mathcal{O}^\times$, $r_K \colon K^\times \to G_K^{ab}$ is the local reciprocity map, $0 \le n(\sigma) \le p - 1$, and σ runs through the embeddings of $k \hookrightarrow \overline{\mathbb{F}}_p$.

Proof. Let $p^n = |k|$. Firstly, we can write

$$(7.1) \qquad \varphi \mid_{I_K} = \prod_\sigma (\sigma \circ \psi)^{-n(\sigma)}$$

where $\psi = \theta_{p^n-1}$ and $0 \le n(\sigma) \le p - 1$ as

$$(7.2) \qquad \varphi \mid_{I_K} = \psi^k$$

for some $0 \le -k \le p^n - 2$ as ψ has order $p^n - 1$. Write k in the form

$$(7.3) \qquad k = a_0 + a_1 p + \ldots + a_{n-1} p^{n-1}$$

where $0 \le -a_i \le p - 1$ for all $0 \le i \le n - 1$, then the conjugates $\sigma \circ \psi$ are of the form ψ^{p^i} where $0 \le i \le n - 1$.

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 7.2 that the fundamental character ψ of level n has the description

$$(7.4) \qquad \psi \circ r_K(x) = \bar{x}^{-1}.$$

The desired result then follows from precomposing (7.1) with r_K.

$\qquad\square$

Now let K be a number field. The following result is a generalization of [29, Appendice A] [16, 30]. We provide additional details for the benefit of the reader.

Proposition 7.4. *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 $\varphi : G_K \to \overline{\mathbb{F}}_p^{\times}$ be a continuous homomorphism satisfying the following conditions:*

(1) The Artin conductor of φ is $\mathfrak{m}$, an ideal of $\mathcal{O}_K$ prime to p;
(2) For all $\mathfrak{p} \in S_p$, the restriction $\varphi \mid_{I_\mathfrak{p}}$ is equal to $\prod_{\sigma \in \Omega_\mathfrak{p}} (\sigma \circ \psi_\mathfrak{p})^{-n_\mathfrak{p}(\sigma)}$, where
  (a) $0 \le n_\mathfrak{p}(\sigma) \le p - 1$,
  (b) $k_\mathfrak{p}$ is the residue field of $\mathfrak{p}$,
  (c) $\Omega_\mathfrak{p}$ denotes the set of embeddings of $k_\mathfrak{p}$ into $\overline{\mathbb{F}}_p$,
  (d) $\psi_\mathfrak{p} : I_{t,K_\mathfrak{p}} \to k_\mathfrak{p}^{\times} \subseteq \overline{\mathbb{F}}_p^{\times}$ is the fundamental character, where $K_\mathfrak{p}$ is the completion of K at $\mathfrak{p}$.

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

$$\prod_{\mathfrak{p} \in S_p} \prod_{\sigma \in \Omega_\mathfrak{p}} \sigma(u + \mathfrak{p})^{n_\mathfrak{p}(\sigma)} = 1.$$

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

$$U_\mathfrak{m} = \{ x \in \mathbb{A}_K^{\times} : x_v \in \mathcal{O}_v^{\times}, \ x_v > 0 \text{ for all real } v \text{ and } x_\mathfrak{q} \equiv 1 \pmod{\mathfrak{q}^{v_\mathfrak{q}(\mathfrak{m})}} \text{ for all } \mathfrak{q} \mid \mathfrak{m} \}.$$

We have that

(1) $\varphi \circ r_K$ is trivial on $U_{\mathfrak{m},v}$ for places $v \nmid p$,
(2) $\varphi \circ r_K(x) = \prod_{\mathfrak{p} \in S_p} \prod_{\sigma \in \Omega_\mathfrak{p}} \sigma(\bar{x}_\mathfrak{p})^{n_\mathfrak{p}(\sigma)}$ for $x = \prod_\mathfrak{p} x_\mathfrak{p} \in K_p^{\times}$ by Corollary 7.3.

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

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

Theorem 7.5. *Suppose $2 \nmid ab$ and $5 \mid ab$. Then, $\bar{\rho}_{J^+,\mathfrak{p}}$ is irreducible for $p > 5$.*

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

Suppose $\bar{\rho}_{J_r^+,\mathfrak{p}}$ is reducible, that is,

$$\bar{\rho}_{J^+,\mathfrak{p}} \sim \begin{pmatrix} \theta & h \\ 0 & \theta' \end{pmatrix} \quad \text{with} \quad \theta, \theta' : G_K \to \mathbb{F}_\mathfrak{p}^{*} \quad \text{satisfying} \quad \theta\theta' = \chi_p,$$

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

Let $\mathfrak{q} \neq \mathfrak{p}$ be a prime of $\mathcal{O}_K$. The semi-simplification $\bar{\rho}_{J^+,\mathfrak{p}}^{\mathrm{ss}}$ of the reduction $\bar{\rho}_{J^+,\mathfrak{p}}$ does not depend on the choice of lattice and its restriction to $I_\mathfrak{q}$ is isomorphic to $(\theta \oplus \theta') \mid_{I_\mathfrak{q}}$. Suppose $e_\mathfrak{q}$ is the conductor exponent of θ and θ' which is the same as mentioned above. Then, the

17

conductor exponent at $\mathfrak{q}$ of $\bar{\rho}_{J^+,\mathfrak{p}}^{ss}$ is $2e_{\mathfrak{q}}$. On the other hand, the conductor exponent at $\mathfrak{q}$ of $\bar{\rho}_{J^+,\mathfrak{p}}^{ss}$ is bounded by the conductor exponent at $\mathfrak{q}$ of $\bar{\rho}_{J^+,\mathfrak{p}}$ which is 0 for $\mathfrak{q} \neq \mathfrak{q}_r$ and 0 or 1 for $\mathfrak{q} = \mathfrak{q}_r$ by Theorem 6.3. Thus, $e_{\mathfrak{q}} = 0$ for all $\mathfrak{q}$ and the conductor of θ and θ' away from p is $\mathcal{O}_K$.

By Theorem 6.3 again, the representation $\bar{\rho}_{J^+,\mathfrak{p}}$ is finite at all primes $\mathfrak{p} \mid p$, and as p is unramified in K, it follows from [1, Corollaire 3.4.4] that the restriction to $I_{\mathfrak{p}}$ of $\theta \oplus \theta'$ is isomorphic to

(7.5) $$\chi_p \oplus 1 \qquad \text{or} \qquad \psi_{\mathfrak{p}} \oplus \psi_{\mathfrak{p}}^p$$

where χ_p is the pth cyclotomic character and $\psi_{\mathfrak{p}}$ is a fundamental character of level 2.

Suppose that one of θ and θ' is unramified at all primes $\mathfrak{p} \mid p$. We can assume it is θ (after relabeling if needed). Then, θ corresponds to a character of the Ray class group of modulus $\infty_1 \infty_2$ where ∞_i denote the two places at infinity, which is trivial. It follows that $\theta = 1$ and $\theta' = \chi_p$. As C^+/K has good reduction at $\mathfrak{q}_2$, we have that

$$1 + 2^2 \equiv a_{\mathfrak{q}_2}(J^+) \pmod{\mathfrak{p}},$$

where $a_{\mathfrak{q}_2}(J^+)$ is the trace of $\rho_{J^+,\mathfrak{p}}$ evaluated at a Frobenius element at $\mathfrak{q}_2$. Using the change of variables in [12, Proposition 1.15] with a short `Magma` script, we check that $a_{\mathfrak{q}_2} = 0$, so $\mathfrak{p} \mid 5$ which is a contradiction to the fact that $p > 5$.

Suppose that both θ and θ' ramify at some prime above p. Applying Lemma 7.4 over K with ϕ equal to either θ or θ' implies that p divides the norm of $u - 1$ by (7.5), where $u = \epsilon_1$ is the fundamental unit in K. However, this norm is -1, a contradiction. $\square$

Theorem 7.6. *Suppose $2 \mid a$, $b \equiv c \equiv -1 \pmod 4$, and $5 \nmid ab$. Then, $\bar{\rho}_{J^-,\mathfrak{p}}$ is irreducible for $p > 5$.*

Proof. Since $\bar{\rho}_{J^-,\mathfrak{p}}$ is odd and K is totally real it is well known that $\bar{\rho}_{J,\mathfrak{p}}$ is absolutely irreducible if and only if it is irreducible. To show $\bar{\rho}_{J^-,\mathfrak{p}}$ is irreducible, it suffices to show $\bar{\rho}_{J,\mathfrak{p}}$ is irreducible where $J = J^- \otimes \chi_0$ and χ_0 is as in Theorem 6.7.

Suppose $\bar{\rho}_{J,\mathfrak{p}}$ is reducible, that is,

$$\bar{\rho}_{J,\mathfrak{p}} \sim \begin{pmatrix} \theta & h \\ 0 & \theta' \end{pmatrix} \quad \text{with} \quad \theta, \theta' : G_K \to \mathbb{F}_{\mathfrak{p}}^* \quad \text{satisfying} \quad \theta\theta' = \chi_p,$$

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

By Propositions 6.8 and 6.12 we know that $\rho_{J,\mathfrak{p}} \mid_{I_{\mathfrak{q}_2}}$ is of special type attached to a character χ and the conductor at $\mathfrak{q}_2$ of $\rho_{J,\mathfrak{p}}$ does not degenerate under reduction mod $\mathfrak{p}$ with conductor exponent of $\rho_{J,\mathfrak{p}} \mid_{I_{\mathfrak{q}_2}}$ and $\bar{\rho}_{J,\mathfrak{p}} \mid_{I_{\mathfrak{q}_2}}$ equal to 1. If χ is ramified then the conductor exponent of $\rho_{J,\mathfrak{p}} \mid_{I_{\mathfrak{q}_2}}$ is twice the conductor exponent of $\chi \mid_{I_{\mathfrak{q}_2}}$ which contradicts the fact that the conductor exponent at $\mathfrak{q}_2$ of $\rho_{J,\mathfrak{p}} \mid_{I_{\mathfrak{q}_2}}$ is equal to 1. Hence, χ is unramified at $\mathfrak{q}_2$.

The semi-simplification of the reduction $\bar{\rho}_{J,\mathfrak{p}}$ does not depend on the choice of lattice and its restriction to $I_{\mathfrak{q}_2}$ is isomorphic to $\bar{\chi} \oplus \bar{\chi}$ (where $\bar{\chi}$ is the reduction of χ mod $\mathfrak{p}$) which in turn is isomorphic to $(\theta \oplus \theta') \mid_{I_{\mathfrak{q}_2}}$. Thus, the conductor at $\mathfrak{q}_2$ of θ and θ' is $\mathcal{O}_K$.

18

Alternatively, we show the conductor at $\mathfrak{q}_2$ of θ and θ' is $\mathcal{O}_K$ without knowing that $\rho_{J,\mathfrak{p}}\mid_{I_{\mathfrak{q}_2}}$ is of special type. The conductor at $\mathfrak{q}_2$ of the semi-simplification of $\bar{\rho}_{J,\mathfrak{p}}$, which is isomorphic to $\theta \oplus \theta'$, divides the conductor at $\mathfrak{q}_2$ of the semi-simplification of $\rho_{J,\mathfrak{p}}$, which in turn divides the conductor at $\mathfrak{q}_2$ of $\rho_{J,\mathfrak{p}}$, namely, $\mathfrak{q}_2$. From above θ and θ' have the same conductor at $\mathfrak{q}_2$, it follows that the conductor of θ and θ' is $\mathcal{O}_K$.

From Proposition 6.14 we know that $\rho_{J^-,\mathfrak{p}}(I_{\mathfrak{q}_r})$ has order equal to 4 or 20, therefore $\bar{\rho}_{J,\mathfrak{p}}(I_{\mathfrak{q}_r})$ has order equal to 4 or 20, respectively. This holds because $\rho_{J,\mathfrak{p}}(I_{\mathfrak{q}_r})$ does not intersect the kernel of reduction (which is a pro-p group) since $p > 5$ and χ_0 is unramified at $\mathfrak{q}_r$.

Since $\bar{\rho}_{J,\mathfrak{p}}(I_{\mathfrak{q}_r})$ has order coprime to $p > 5$ by Proposition 6.14 and Maschke's Theorem, we conclude that $\bar{\rho}_{J,\mathfrak{p}}\mid_{I_{\mathfrak{q}_r}} \cong \theta \oplus \theta'\mid_{I_{\mathfrak{q}_r}}$. From Theorem 6.3, we know that the conductor exponent at $\mathfrak{q}_r$ of $\bar{\rho}_{J,\mathfrak{p}}\mid_{I_{\mathfrak{q}_r}}$ is $2, 3$. As above we conclude that the conductor at $\mathfrak{q}_r$ of θ and θ' is the same and divides $\mathfrak{q}_r$.

In summary, the conductor of θ and θ' away from p divides $\mathfrak{q}_r$. By Theorem 6.3, the representation $\bar{\rho}_{J^-,\mathfrak{p}}$ is finite at all primes $\mathfrak{p} \mid p$, and as p is unramified in K, it follows from [1, Corollaire 3.4.4] that the restriction to $I_{\mathfrak{p}}$ of $\theta \oplus \theta'$ is isomorphic to

$$(7.6) \qquad\qquad \chi_p \oplus 1 \qquad \text{or} \qquad \psi_{\mathfrak{p}} \oplus \psi_{\mathfrak{p}}^p,$$

where χ_p is the p-th cyclotomic character and $\psi_{\mathfrak{p}}$ is a fundamental character of level 2.

Suppose that one of θ, θ' is unramified at every prime dividing p. We can assume it is θ (after relabeling if needed). It follows that θ corresponds to a character of the Ray class group of modulus $\mathfrak{q}_r \infty_1 \infty_2$ where ∞_i denote the two places at infinity. The Ray class group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. From the above we have that $4 \mid \#\bar{\rho}_{J,\mathfrak{p}}(I_{\mathfrak{q}_r})$ and $\bar{\rho}_{J,\mathfrak{p}}\mid_{I_{\mathfrak{q}_r}} \cong \theta \oplus \theta'\mid_{I_{\mathfrak{q}_r}}$, hence $\theta\mid_{I_{\mathfrak{q}_r}}$ has order divisible by 4 which is a contradiction.

Suppose that both θ and θ' ramify at some prime above p. Let ϵ_1 be the the fundamental unit in K. Applying Proposition 7.4 to either θ or θ' implies that p divides the norm of $u - 1$ by (7.6), where $u = \epsilon_1^{n_1}$ and $n_1 = 4$ is the smallest positive integer such that $u \equiv 1 \pmod{\mathfrak{q}_r}$. This yields of bound of $p = 5$, contradicting $p > 5$. $\qquad\square$

8. 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 [28], the case $n = 5$ is a special case of Fermat's Last Theorem (see for instance, [17, Théorème IX]) while the case $n = 4$ has been proved in [8, Theorem 1.1]. The case $n = 7$ is treated in [11].

For the rest of the proof, we may now assume that $n = p \geq 11$ is a prime. Let $S_2(\mathfrak{n})$ denote the space of Hilbert newforms over K with parallel weight 2, trivial character, and level $\mathfrak{n}$. We may assume without loss of generality in the second case that $2 \mid a$, $b \equiv c \equiv -1 \pmod 4$ by switching the roles of a and b and negating (a, b, c), if necessary.

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

$$(8.1) \qquad\qquad \bar{\rho}_{J,\mathfrak{p}} \simeq \bar{\rho}_{g,\mathfrak{P}},$$

where $\mathfrak{p}$ 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 $\mathfrak{q}$ such that

$$(8.2) \qquad \operatorname{tr} \bar{\rho}_{J,\mathfrak{p}}(\operatorname{Frob}_\mathfrak{q}) \neq \operatorname{tr} \bar{\rho}_{g,\mathfrak{P}}(\operatorname{Frob}_\mathfrak{q}).$$

However, a subtlety occurs because in the definition of the isomorphism (8.1) we mean

$$(8.3) \qquad \bar{\rho}_{J,\mathfrak{p}} \otimes \overline{\mathbb{F}}_p \simeq \bar{\rho}_{g,\mathfrak{P}} \otimes \overline{\mathbb{F}}_p.$$

Hence, the comparison (8.2) cannot be done until we have chosen an embedding of the residue fields of $K_\mathfrak{p}$ and $K_{g,\mathfrak{P}}$ into $\overline{\mathbb{F}}_p$. The correct condition to rule out an isomorphism as in (8.1) by a local comparison of traces is

$$(8.4) \qquad p \nmid N_{L/\mathbb{Q}} \left(\prod_{\sigma \in \operatorname{Gal}(K/\mathbb{Q})} (a_\mathfrak{q}(g) - a_\mathfrak{q}(J)^\sigma) \right),$$

where L is the compositum of K and K_g inside $\overline{\mathbb{Q}}$ (see [5] for more details).

Finally, we remark that this does not affect the computational time for the elimination step, since in practice `Magma` is only able to compute $a_\mathfrak{q}(J)$ up to Galois conjugation over $\mathbb{Q}$ in any case.

8.2. **Proof of Theorem 1.1 (I).** We are under the assumption that $2 \nmid ab$ and $5 \mid ab$. By Theorems 7.5 and 5.1, we have that $\bar{\rho}_{J^+,\mathfrak{p}}$ is irreducible and modular. Hence, by level lowering for Hilbert modular forms [21, 23, 37], we have that

$$(8.5) \qquad \bar{\rho}_{J^+,\mathfrak{p}} \simeq \bar{\rho}_{g,\mathfrak{B}}$$

where g is a Hilbert newform of parallel weight 2, trivial character over K and level $\mathcal{O}_K$ or $\mathfrak{q}_r$ by Theorem 6.3, and $\mathfrak{B}$ is a prime above p in the field of coefficients of g. However, both spaces of Hilbert newforms $S_2(1)$ and $S_2(\mathfrak{q}_r)$ are empty which gives a contradiction.

8.3. **Proof of Theorem 1.1 (II).** As before, we may assume that $n = p \geq 11$ is a prime. We are under the assumption that $2 \mid a$, $b \equiv c \equiv -1 \pmod 4$, and $5 \nmid ab$. By Theorems 7.6 and 5.4, we have that $\bar{\rho}_{J^-,\mathfrak{p}}$ is irreducible and modular.

In what follows, we use the fact that

$$\rho_{J \otimes \chi, \mathfrak{p}} = \rho_{J,\mathfrak{p}} \otimes \chi,$$

for any character $\chi : G_K \to \{\pm 1\}$ of order dividing 2, where $J \otimes \chi$ means the twist of J by χ, and χ twists by the automorphism -1 of J.

Let $J = J^- \otimes \chi_0$ where $\chi_0 \in K(S_2, 2)^*$ where $S_2 = \{\mathfrak{q}_2\}$. By level lowering for Hilbert modular forms as above, we have that

$$(8.6) \qquad \bar{\rho}_{J,\mathfrak{p}} \simeq \bar{\rho}_{g,\mathfrak{B}}$$

where g is a Hilbert newform of parallel weight 2, trivial character over K and level $\mathfrak{q}_2 \mathfrak{q}_r^t$ for $t = 2, 3$ (by Theorem 6.3) and $\mathfrak{B}$ 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 $\mathfrak{q}_2$ from the level of $\rho_{J,\mathfrak{p}}$ in case the Serre level of $\bar{\rho}_{J,\mathfrak{p}}$ is not divisible by $\mathfrak{q}_2$.

Suppose $\mathfrak{q} \neq \mathfrak{p}$ is a prime of K not above 2 and 5. Then we have that

$$a_{\mathfrak{q}}(g) \equiv a_{\mathfrak{q}}(J) \pmod{\mathfrak{p}}, \qquad\qquad \text{if } q \nmid ab, \tag{8.7}$$

$$a_{\mathfrak{q}}(g)^2 \equiv (N(\mathfrak{q}) + 1)^2 \pmod{\mathfrak{p}}, \qquad\qquad \text{if } q \mid ab, \tag{8.8}$$

where $a_{\mathfrak{q}}(J) = \operatorname{tr}\rho_J(\operatorname{Frob}_{\mathfrak{q}})$ and $N(\mathfrak{q})$ is the norm of $\mathfrak{q}$. Thus, defining

$$T(g, \mathfrak{q}) = N(\mathfrak{q}) \cdot \left(a_{\mathfrak{q}}(g)^2 - (N(\mathfrak{q}) + 1)^2 \right) \cdot \prod_{a,b \in \mathbb{F}_q, ab \neq 0} N_{L/\mathbb{Q}} \left(\prod_{\sigma \in \operatorname{Gal}(K/\mathbb{Q})} (a_{\mathfrak{q}}(g) - a_{\mathfrak{q}}(J)^\sigma) \right),$$

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

For all choices of χ_0, 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 8.1. 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. For J^- we also have to compute the space of Hilbert newforms of level $\mathfrak{q}_2^4 \mathfrak{q}_r^t$ with $t = 2, 3$ which have bigger dimension and thus make the computations slower. Secondly, the spaces of Hilbert newforms of level $\mathfrak{q}_2^4 \mathfrak{q}_r^t$ with $t = 2, 3$ have forms with complex multiplication over $\mathbb{Q}(\zeta_5)$. The elimination step using standard comparison of traces of Frobenius does not work on these forms and requires additional elimination techniques to prove Theorem 1.1.

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, 7

[2] S. Anni and V. Dokchitser. Constructing hyperelliptic curves with surjective Galois representations. *Trans. Amer. Math. Soc.*, 373(2):1477–1500, 2020. 6.1

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

[4] N. Billerey, I. Chen, L. Dembélé, L. Dieulefait, and N. Freitas. Some extensions of the modular method and Fermat equations of signature $(13, 13, n)$. 2022. Accepted, Publicacions Matemàtiques, 22 pages. 2

[5] N. Billerey, I. Chen, L. Dieulefait, and N. Freitas. A multi-Frey approach to Fermat equations of signature (r, r, p). *Trans. Amer. Math. Soc. (to appear)*. 8.1

[6] N. Billerey, I. Chen, L. Dieulefait, N. Freitas, and F. Najman. On Darmon's program for the generalized fermat equation. 2022. ArXiv, arxiv.org/abs/2205.15861. 4, 6.1

[7] M. Börner, I. Bouw, and S. Wewers. The functional equation for L-functions of hyperelliptic curves. *Exp. Math.*, 26(4):396–411, 2017. 6

[8] N. Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003. 8

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

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

[11] S. R. Dahmen and S. Siksek. Perfect powers expressible as sums of two fifth or seventh powers. *Acta Arith.*, 164(1):65–100, 2014. 8

[12] H. Darmon. Rigid local systems, Hilbert modular forms, and Fermat's Last Theorem. *Duke Math. J.*, 102(3):413–449, 2000. 1, 1, 4, 4, 4, 4.6, 5, 5, 6, 6.1, 6.16, 7

[13] 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. 5

[14] H. Darmon and L. Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997. 1

[15] 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. 3

[16] M. Dimitrov. Galois representations modulo p and cohomology of Hilbert modular varieties. *Ann. Sci. École Norm. Sup. (4)*, 38(4):505–551, 2005. 7

[17] P. G. L. Dirichlet. Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré. *J. reine angew. Math.*, 3:354–375, 1828. 8

[18] T. Dokchitser, V. Dokchitser, C. Maistret, and A. Morgan. Arithmetic of hyperelliptic curves over local fields. *Math. Ann. (to appear)*. ArXiv preprint, arXiv:1808.02936. 6.1

[19] 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. 6.1

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

[21] K. Fujiwara. Level optimization in the totally real case. *ArXiv Mathematics e-prints*, February 2006. 8.2

[22] F. Jarvis. Level lowering for modular mod l representations over totally real fields. *Math. Ann.*, 313(1):141–160, 1999. 6, 6.2.1

[23] F. Jarvis. Correspondences on Shimura curves and Mazur's principle at p. *Pacific J. Math.*, 213(2):267–280, 2004. 8.2

[24] C. Khare and J. A. Thorne. Automorphy of some residually S_5 Galois representations. *Math. Z.*, 286(1-2):399–429, 2017. 5

[25] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009. 5

[26] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009. 5

[27] M. Kisin. Modularity of 2-adic Barsotti-Tate representations. *Invent. Math.*, 178(3):587–634, 2009. 5

[28] A. Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7(1):1–13, 1998. 8

[29] A. Kraus. Courbes elliptiques semi-stables sur les corps de nombres. *Int. J. Number Theory*, 3(4):611–633, 2007. 7

[30] E. Larson and D. Vaintrob. Determinants of subquotients of Galois representations associated with abelian varieties. *J. Inst. Math. Jussieu*, 13(3):517–559, 2014. With an appendix by Brian Conrad. 7

[31] Q. Liu. Courbes stables de genre 2 et leur schéma de modules. *Math. Ann.*, 295(2):201–222, 1993. 2, 3, 6.2.1

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

[33] 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, 3

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

[35] P. Lockhart, M. Rosen, and J.H. Silverman. An upper bound for the conductor of an abelian variety. *J. Algebraic Geom.*, 2(4):569–601, 1993. 6.2.2

[36] 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. 6.2.1

[37] A. Rajaei. On the levels of mod ℓ Hilbert modular forms. *J. Reine Angew. Math.*, 537:33–65, 2001. 8.2

[38] M. Romagny. Models of curves. In *Arithmetic and geometry around Galois theory*, volume 304 of *Progr. Math.*, pages 149–170. Birkhäuser/Springer, Basel, 2013. 3

[39] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972. 7, 7, 7

[40] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968. 6.2.2

[41] W. Tautz, J. Top, and A. Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math.*, 43(5):1055–1064, 1991. 4, 4, 4, 4

[42] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995. 1

[43] Andrew Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, 144:443–551, 1995. 1

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