# THE GENERALIZED FERMAT EQUATION $x^{11} + y^{11} = z^5$

MANVIR JASWAL

ABSTRACT. We prove that $x^{11} + y^{11} = z^5$ has no solution in nonzero coprime integers, and that for every prime $p \geq 11$ the solutions of $x^p + y^p = z^5$ in nonzero coprime integers with $xy$ prime to 10 have $xy \equiv -1 \pmod 5$. To a solution Darmon attaches a Frey abelian surface over $\mathbb{Q}(\sqrt{5})$, a twist of the member at $t = x^p/z^5$ of a one-parameter family. For $p = 11$, results of Chen and Koutsianas and of Billerey, Chen, Dieulefait and Freitas leave only the solutions with $10 \mid xy$ and $11 \nmid z$. For these, $t$ gives a point on a quotient of Darmon's modular curve $X_0(\mathfrak{p})$, $\mathfrak{p} \mid 11$, that is an elliptic curve of rank 1 over $\mathbb{Q}(\sqrt{5})$, and Chabauty's method in the restriction of scalars excludes such points. For general $p$ and $xy$ prime to 10, Chen and Koutsianas show that the Frey surface is congruent modulo $p$, up to a quadratic twist, to one of four surfaces with complex multiplication (or, for $p = 19$, to one more modular form); we test this congruence at the prime $\sqrt{5}$. When $xy \equiv \pm 2 \pmod 5$, the fields cut out by inertia there differ or, in one subcase, a Frobenius trace does. When $xy \equiv 1 \pmod 5$, the reduction at 2 determines the twist, and Frobenius traces exclude the congruence: at an auxiliary prime, and on the special fiber over $\mathbb{F}_5$ that the genus-2 curves defining these surfaces share over a totally ramified extension of $\mathbb{Q}_5(\sqrt{5})$. For $10 \mid xy$, a uniform bound on rational points of order $p$ on abelian surfaces over $\mathbb{Q}(\sqrt{5})$ with real multiplication would exclude this class for large $p$.

## 1. INTRODUCTION

Let $p$ be an odd prime. We study the generalized Fermat equation of signature $(p, p, 5)$,

$$x^p + y^p = z^5, \tag{1.1}$$

and call a triple $(a, b, c)$ of coprime integers with $abc \neq 0$ and $a^p + b^p = c^5$ a *solution*. For $p = 3$ there is no solution: Bruin proved that the integer solutions of $x^3 + y^3 = z^5$ with $xyz \neq 0$ have $\gcd(x, y, z) > 1$ [11], and Dahmen gave a second proof by the modular method [19, §3.3.2]. For $p = 5$ the equation is a case of Fermat's Last Theorem, for $p = 7$ it was solved by Dahmen and Siksek [20], and for $p = 13$ by Best, Dahmen and Freitas [4]. We take $p \geq 11$ in the results below. Darmon [21] proposed a program for the equations $x^p + y^p = z^r$ with $r$ fixed: attach to a solution a Frey abelian variety over the real cyclotomic field $\mathbb{Q}(\zeta_r)^+$, of dimension $(r-1)/2$, with real multiplication by the integers of that field, and carry out the modular method with it. For $r = 5$ the field is $K = \mathbb{Q}(\sqrt{5})$ and the Frey varieties are Jacobians of curves of genus 2. Chen and Koutsianas [15] carried out this program for $r = 5$ with Darmon's two Frey Jacobians $J^{\pm}$. We use $J^-$, the Jacobian of the curve

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

Chen and Koutsianas showed that (1.1) has no solution with $2 \nmid ab$, $5 \mid ab$, nor with $2 \mid ab$, $5 \nmid ab$, for every odd prime $p$ [15, Theorem 1.1]. Billerey, Chen, Dieulefait and Freitas treat

2020 *Mathematics Subject Classification.* Primary 11D41; Secondary 11F80, 11G10, 11F41.

*Key words and phrases.* Generalized Fermat equation, Frey hyperelliptic curves, real multiplication, Hilbert modular forms, inertia at $\sqrt{5}$, modular method.

How AI was used in this work is described under Declarations, p. 40.

the signatures $(r, r, p)$ with several Frey curves [7], and develop Darmon's program further in [8]. The local behavior of the Frey curves of the program at the primes above 2 and $r$, their conductors in particular, is studied by Azon [1], by Azon, Curcó-Iranzo, Khawaja, Maistret and Mocanu [2], by Cazorla García and Villagra Torcomian [13], and by Chen and Villagra Torcomian [17].

In the case $2 \nmid ab$, $5 \nmid ab$ the elimination step of [15] leaves a congruence between $J^-$ and one of four Hilbert newforms over $K$ with complex multiplication by $\mathbb{Q}(\zeta_5)$, up to a quadratic character unramified outside 2 that this step does not determine. These forms come from trivial solutions: they are attached to the Jacobians of the curves $y^2 = x^5 + D$, $D \in \{1, 4, 16, 64\}$, and $C^-$ becomes $y^2 = x^5 + 4\alpha$ when $a^p = -\alpha$, $b^p = \alpha$ and $c = 0$ (for $p = 19$ a newform without complex multiplication also survives). Chen and Koutsianas describe the elimination of these forms in the case $2 \nmid ab$, $5 \nmid ab$, and the irreducibility of the residual representation in the case $10 \mid ab$, as the two obstructions that remain for signature $(p, p, 5)$ [15, p. 3], and they discuss the obstruction from trivial solutions in their survey of Darmon's program [14, §2]. One known way to separate a Frey representation from such a form is to compare the fields cut out by inertia at a prime of bad reduction [7, §3], [5, §5]. We do this at the prime $\mathfrak{q}_5 = (\sqrt{5})$ of $K$.

1.1. **Results.** The theorems below use the following results of [15], recalled in Section 2: the modularity of $J^-$, its conductor at the primes above 2 and 5, level lowering, and the elimination of all newforms but the four with complex multiplication (and one more at $p = 19$).

**Theorem A.** *Let $p \geq 11$ be a prime. Then $x^p + y^p = z^5$ has no solution $(a, b, c)$ in coprime integers with $abc \neq 0$ and $ab \equiv \pm 2 \pmod 5$.*

**Theorem B.** *Let $p \geq 11$ be a prime and $(a, b, c)$ a solution of $x^p + y^p = z^5$ in coprime integers with $abc \neq 0$.*

*(a) Either $10 \mid ab$, or $2 \nmid ab$ and $ab \equiv -1 \pmod 5$.*

*(b) Let $2 \nmid ab$, so that $ab \equiv -1 \pmod 5$ by (a). If $p \equiv \pm 2 \pmod 5$, then $a \equiv \pm 1 \pmod 8$. If $a \equiv -1 \pmod 4$ (which exchanging $a$ and $b$ always achieves), then for every prime $\mathfrak{p}$ of $K$ above $p$ the $G_K$-modules $J^-[\mathfrak{p}]$ and $\mathcal{J}_D[\mathfrak{p}]$ are isomorphic, compatibly with the action of $\mathcal{O}_K$, for $D = 4$ or $D = 16$, where $\mathcal{J}_D$ is the Jacobian of $y^2 = x^5 + D$.*

Theorem A is Theorem 5.3, and Theorem B is Corollary 6.8 and Theorem 6.7. Theorem 6.7 also says which of $D = 4, 16$ occurs, and part (a) uses [15, Theorem 1.1] as well. Table 1 shows where each case is treated.

**Theorem C.** *The equation $x^{11} + y^{11} = z^5$ has no solution $(a, b, c)$ in coprime integers with $abc \neq 0$.*

Theorem C is Theorem 7.1. Part of it was already known. Billerey, Chen, Dieulefait and Freitas proved that $x^{11} + y^{11} = z^n$, for every $n \geq 2$, has no solution $(a, b, c)$ in coprime integers with $abc \neq 0$ and $2 \mid a + b$ or $11 \mid a + b$ [9, Theorem 1.5], and Chen and Koutsianas excluded the class $2 \mid ab$, $5 \nmid ab$ [15, Theorem 1.1]. In terms of $ab$ and $c$: for coprime $a$ and $b$, $2 \mid a + b$ exactly when $2 \nmid ab$, and for a solution, $11 \mid a + b$ exactly when $11 \mid c$, as $a^{11} + b^{11} \equiv a + b \pmod{11}$. So these results leave exactly the solutions with $10 \mid ab$ and $11 \nmid c$, and this class is what Theorem C adds to them.

We treat the whole class $10 \mid ab$. The curve $C^-$ is a quadratic twist of the member $y^2 = x^5 - 5x^3 + 5x + 2 - 4t$ of Darmon's family at the rational value $t = a^{11}/c^5$, which we

call the *Frey parameter* of the solution (Section 7.1). For a prime $\mathfrak{p}$ of $K$ above 11, Darmon's modular curve $X_0(\mathfrak{p})$ [21, §4] classifies the members of the family together with a subgroup of order 11 of the $\mathfrak{p}$-torsion of the Jacobian that is stable under the real multiplication. When $10 \mid ab$ the representation of $G_K$ on $J^-[\mathfrak{p}]$ is reducible (Lemma 7.2): if it were irreducible, level lowering would make it congruent, up to a quadratic twist, to one of the two Hilbert newforms of level (10) over $K$, and a comparison of traces at the prime (3) excludes both. So $t$ gives a point of $X_0(\mathfrak{p})$ over $K$. The quotient of $X_0(\mathfrak{p})$ by an involution over $t \mapsto 1-t$ is an elliptic curve $E$ over $K$ of rank 1, on which the function $v = 4t(1-t)$ takes a rational value at this point. Such points are the rational points of a curve in the restriction of scalars of $E$ to $\mathbb{Q}$, of dimension $[K:\mathbb{Q}] = 2$; as the rank 1 of $E$ is less than 2, Chabauty's method applies, and it shows that $v$ is rational only at the two points of $E(K)$ over $v = 0$, which come from no solution (Proposition 7.9). The involution comes from the isomorphism $(x, y) \mapsto (-x, \sqrt{-1}\, y)$ from the member at $t$ of Darmon's family to the member at $1-t$ (Section 7.1). That the quotient is the elliptic curve $E$, for one of the two primes $\mathfrak{p}$ above 11, is shown by comparing $v$ with an explicit function on $E$ of degree 12: as covers of the projective line, both have monodromy group $\mathrm{PSL}_2(\mathbb{F}_{11})$, the same ramification and conjugate local monodromies (Propositions 7.4 and 7.7). The curve $E$ has rank 1 by Zhang's theorem, as its analytic rank is 1 (Proposition 7.8). The same argument over $\mathbb{Q}(\zeta_5)$, where the rank is $2 < [\mathbb{Q}(\zeta_5):\mathbb{Q}] = 4$, together with Theorem B, gives a second proof that there is no solution with $2 \nmid ab$ (Proposition 7.10 and Remark 7.11). For comparison, Best, Dahmen and Freitas [4] solve $x^{13} + y^{13} = z^5$ by removing the solutions with $13 \mid c$ with the modular method, and the others by a descent and sieves (one of them using the modular method) that lead to a curve of genus 2 over the cubic subfield of $\mathbb{Q}(\zeta_{13})$, all of whose points they determine by Chabauty's method over number fields. Here the modular method is followed instead by a study of the points of a modular curve, and only those over rational values of $t$ are needed.

TABLE 1. Solutions with $p \geq 11$, by the class of $ab$, and the case $p = 11$.

| class of $ab$ | status | reference |
|---|---|---|
| $2 \mid ab$, $5 \nmid ab$ | no solution | [15, Theorem 1.1] |
| $2 \nmid ab$, $5 \mid ab$ | no solution | [15, Theorem 1.1] |
| $2 \nmid ab$, $ab \equiv \pm 2 \pmod 5$ | no solution | Theorem 5.3 |
| $2 \nmid ab$, $ab \equiv 1 \pmod 5$ | no solution | Theorem 6.7 |
| $2 \nmid ab$, $ab \equiv -1 \pmod 5$ | open; for $a \equiv -1 \pmod 4$, $J^-[\mathfrak{p}] \cong \mathcal{J}_4[\mathfrak{p}]$ or $\mathcal{J}_{16}[\mathfrak{p}]$ | Theorem 6.7 and Proposition 6.9 |
| $10 \mid ab$ | open; reduced to a torsion bound | Proposition 8.1 |
| $p = 11$ | | |
| $2 \nmid ab$, or $11 \mid c$ | no solution | [9, Theorem 1.5] |
| $10 \mid ab$ | no solution | Proposition 7.9 |

The two Jacobians $\mathcal{J}_4$ and $\mathcal{J}_{16}$ that remain in Theorem B are the Frey Jacobians of the triples $(-2^k, 2^k, 0)$, $k \geq 0$ (trivial solutions, not coprime when $k > 0$), so no test at an auxiliary prime (in the sense of Section 6), Kraus's included [36], can remove them (Proposition 6.9). For the case $10 \mid ab$ we show that the input from Darmon's conjecture used in [15, Corollary 1.3] can be replaced by a uniform bound on rational points of order $p$ on abelian surfaces over $K$ with real multiplication by $\mathcal{O}_K$ (Proposition 8.1). For this we carry out, with the conductors of [15], Darmon's reduction to rational torsion [21, Theorem 3.13 and §4], an argument that turns the reducibility of the representation of $G_K$ on $J^-[\mathfrak{p}]$ into

a rational point of order $p$ on a twist of $J^-$ or on a quotient of it (Section 8). For $p \equiv 1 \pmod 5$ the representation $\bar\rho_{J^-,\mathfrak{p}}$ restricted to $G_{\mathbb{Q}(\zeta_5)}$ is reducible in both remaining cases (Proposition 8.2), in the case $10 \mid ab$ by the results of [15]. So, for Frey Jacobians whose endomorphism algebra over $\overline{\mathbb{Q}}$ is $K$, these cases are instances of the Borel case of Darmon's conjecture [21, Conjecture 4.1] over $\mathbb{Q}(\zeta_5)$, the assertion that for $p$ large the image of the residual representation is not contained in a Borel subgroup (Remark 8.3).

1.2. **The idea.** When $5 \nmid ab$, the Frey surface $J^-$ and the surfaces $\mathcal{J}_D$ with complex multiplication, the Jacobians of the curves $H_D\colon y^2 = x^5 + D$, have bad reduction at the prime $\mathfrak{q}_5 = (\sqrt{5})$ of $K$ that becomes good over a finite extension. Over the maximal unramified extension of $F = \mathbb{Q}_5(\sqrt{5})$, the least such extension is the field cut out by the action of inertia on the torsion points of order prime to 5. For $p \geq 7$, inertia acts on both sides through a finite group of order prime to $p$, so an isomorphism between the $p$-torsion modules, even up to a quadratic twist unramified at $\mathfrak{q}_5$, forces the fields of $J^-$ and of $\mathcal{J}_D$ to coincide. Over a finite extension of $F$ over which both then have good reduction, the isomorphism also makes the traces of Frobenius on the two reductions congruent modulo $p$, up to the value of the twist. So there are two local tests at $\mathfrak{q}_5$: the fields over which the reduction becomes good and, where these agree, the traces of Frobenius over them.

In the case $2 \nmid ab$, $5 \nmid ab$ we apply these tests to $J^-$ and the $\mathcal{J}_D$. When $ab \equiv \pm 2 \pmod 5$ a congruence between $J^-$ and $\mathcal{J}_D$ already fails locally at $\mathfrak{q}_5$: in general the fields cut out by inertia differ, as the Weierstrass points of $C^-$ show, and in one subcase a Frobenius trace differs. When $ab \equiv \pm 1 \pmod 5$ the local representations at $\mathfrak{q}_5$ agree up to an unramified quadratic twist. We then use the reduction at 2, which determines the quadratic character left undetermined in [15], and compare Frobenius traces at both primes above an auxiliary prime and, when the conductor exponent of $J^-$ at $\mathfrak{q}_5$ is 3, on the special fiber that $C^-$ shares with the curves $H_D$ over one totally ramified extension of $F$.

The roots of $\Phi(x) = x^5 - 5c^2x^3 + 5c^4x - 2(a^p - b^p)$ have de Moivre's closed form $v\zeta^k + c^2v^{-1}\zeta^{-k}$ ($\zeta = \zeta_5$, $k \in \mathbb{Z}/5$), where $v^5 = \beta$ and $\beta = (\sqrt{a^p} + \sqrt{-b^p})^2$ [22], [2], [13]. So over $\mathcal{M} = \mathbb{Q}_5^{\mathrm{ur}}(\zeta_5)$ the Weierstrass points of $C^-$ (the point at infinity and the points with $y = 0$) generate the Kummer extension $\mathcal{M}(\beta^{1/5})$, which is $\mathcal{M}$ or cyclic of degree 5 over $\mathcal{M}$. Its class in $\mathcal{M}^\times/\mathcal{M}^{\times 5}$ is given by an element $\kappa(\beta)$ of $\overline{\mathbb{F}}_5$, the residue of $(\beta/\beta_0 - 1)/5$ for the root of unity $\beta_0 \equiv \beta \pmod 5$ of order prime to 5. Two such extensions of degree 5 coincide exactly when their elements $\kappa$ differ by a factor in $\mathbb{F}_5^\times$, that is, span the same $\mathbb{F}_5$-line of $\overline{\mathbb{F}}_5$, viewed as a vector space over $\mathbb{F}_5$ (Lemma 3.2). For the curves $y^2 = x^5 + D$ with complex multiplication this element lies on the line $\mathbb{F}_5$. When $ab \equiv \pm 2 \pmod 5$, $\beta$ lies in the unramified quadratic extension of $\mathbb{Q}_5$ and not in $\mathbb{Q}_5$, its norm is a fifth power, and, when $\kappa(\beta) \neq 0$, $\kappa(\beta)$ lies on a different line. Then the fields cut out by inertia at $\mathfrak{q}_5$ differ, which a congruence modulo a prime $p \geq 7$ forbids (Lemmas 3.1 and 3.6). The case $\kappa(\beta) = 0$ is the one in which the conductor exponent of $J^-$ at $\mathfrak{q}_5$ is 2 and $C^-$ acquires good reduction over a tamely ramified extension. We call it the *tame case*. There $C^-$ has good reduction over $\mathbb{Q}_5(5^{1/8})$, with special fiber $y^2 = x^5 - x$ when $ab \equiv \pm 2 \pmod 5$, on which Frobenius has trace $\pm 2\sqrt{5}$. A Frobenius element over this field does not fix $\zeta_5$, so its trace on the forms with complex multiplication by $\mathbb{Q}(\zeta_5)$ is 0, and the two cannot be congruent modulo $p \nmid 20$ (Proposition 5.2).

When $ab \equiv \pm 1 \pmod 5$ the classes lie on the same line, and the local representations at $\mathfrak{q}_5$ agree up to an unramified quadratic character (Proposition 6.1). Three further inputs then decide the case. First, at the place 2 the Frey curve acquires good reduction over $\mathbb{Q}_2^{\mathrm{ur}}(2^{1/5})$, with the same special fiber $w^2 + w = X^5$ as the curve $y^2 = x^5 + 4$ of a trivial

solution. This forces the quadratic character of [15] to be trivial, and it fixes, for each form with complex multiplication, which of the two identifications of its coefficient field with $K$ matches the real multiplication of $J^-$ (Proposition 4.1). Second, Chen and Koutsianas compare traces of Frobenius only up to sign and up to the automorphism of $K$, since the twist and the identification are unknown to them [15, §§9.1, 9.3, 10]. With both fixed, the traces themselves can be compared at both primes above an auxiliary prime $q \equiv 1 \pmod 5$, $q \neq p$, as in [9, (9.5), Remark 9.12]: we use $q = 11$, and for $p = 11$ the primes 31, 61 and 101. This removes two of the four forms and the extra form at $p = 19$ (Proposition 4.3). Third, when the conductor exponent $\varepsilon$ of $J^-$ at $\mathfrak{q}_5$ is 3, the curve $C^-$ and the curves $H_D$, $D = 4, 16, 64$, acquire good reduction over the totally ramified extension $L_1 = \mathbb{Q}_5((-5)^{1/8}, 6^{1/5})$ of $F$, of degree 20, which contains a fifth root of every element of $\mathbb{Z}_5^\times$, since every such element is a power of 6 times a fifth power. The models with good reduction over $L_1$ come from a change of variables that uses both radicals. As $(1-\zeta)^4$ is $-5$ times a fourth power, $\mathbb{Q}_5((-5)^{1/4}) = \mathbb{Q}_5(\zeta)$, and the eighth root of $-5$ makes the valuation of $1-\zeta$ even. The fifth root of 6 gives the fifth roots of $\beta$ and of $-D$: here $\beta \in \mathbb{Z}_5^\times$, and as $\kappa(6) = 1$, $\beta$ is a power of 6 times a fifth power in $\mathbb{Z}_5$, so $L_1$ contains a fifth root of $\beta$ for every solution, and likewise of $-D$. The special fibers are the same curve $Y^2 = h(X^5 - X)$ over $\mathbb{F}_5$, with the same constant $h \in \mathbb{F}_5^\times$, and the endomorphism $\omega = \zeta + \zeta^{-1}$ of the real multiplication reduces to $T_e + T_e^{-1}$, where $T_e$ is the translation $X \mapsto X + e$, with $e = \bar{\delta}$ for $C^-$ ($\delta^2 = -a^p b^p$) and $e = \bar{D}$ for $H_D$. The trace of Frobenius on this curve is $\pm 2\sqrt{5}$, and replacing $e$ by $je$ multiplies it by $(\frac{j}{5})$. So the traces for $C^-$ and $H_D$ are equal or opposite according to $(\frac{\bar{\delta}\bar{D}}{5})$, which is $+1$ exactly when $ab \equiv -1 \pmod 5$. As the place 2 and the second input leave only $\mathcal{J}_4$ and $\mathcal{J}_{16}$, and not the surfaces $\mathcal{J}_4^\sigma$, $\mathcal{J}_{16}^\sigma$ on which $K$ acts through its nontrivial automorphism $\sigma$, this removes $ab \equiv 1 \pmod 5$ (Proposition 6.3). For $p \equiv \pm 2 \pmod 5$, comparing the multipliers of the Weil pairings at 2 and $\sqrt{5}$, as in the symplectic method of Halberstadt and Kraus [31], gives $a \equiv \pm 1 \pmod 8$ (Proposition 6.6).

1.3. **Relation to earlier work.** For every $r$, the analogue of $\Phi$ for $x^p + y^p = z^r$ is the polynomial of degree $r$ that defines the analogue of $C^-$ in Darmon's program. Its roots are given in closed form in [2, Definitions 4.1, 4.4 and Proposition 4.6] and [13, Proposition 2.2], and Azon describes the splitting field over $\mathbb{Q}_r(\zeta_r)$ as a Kummer extension [1, Theorem 4.36, proof of Theorem 4.48] and computes the conductor exponents 2 and 3 at the prime above $r$ [1, Table 2]. Azon also gives the model of the Frey curve at the even place [1, Proposition 4.28]. These results describe the Frey curve alone, and do not compare it with the curves $y^2 = x^5 + D$. In [7, §3] and [5, §5] the fields cut out by inertia are compared for Frey elliptic curves, and Chen and Suozer give a criterion for two local representations to have isomorphic reductions [16, Theorem 3.5]. When $\varepsilon = 3$, Chen and Koutsianas show that $C^-$ acquires good reduction over a totally ramified extension of $F$ of degree 20 that depends on $a$, $b$, $c$ modulo 25 [15, Proposition 7.23(ii)], and the proof of [15, Proposition 7.24] identifies the field cut out by inertia with the field over which $J^-$ acquires good reduction. What this paper adds is the comparison of the Kummer class of the Weierstrass points of $C^-$ with that of $y^2 = x^5 + D$ and the Frobenius trace in the tame case (Section 5); the determination of the quadratic character and of the identification of coefficient fields from the reduction at 2 (Proposition 4.1), which makes the two-prime comparison of [9, (9.5)] available; the extension $L_1$, the same for all solutions with $ab \equiv \pm 1 \pmod 5$ and $\varepsilon = 3$ and for the curves $H_D$, and the Frobenius trace on their common special fiber over it (Proposition 6.3); and the symplectic argument at 2 and $\sqrt{5}$ (Proposition 6.6). Section 8

follows Darmon [21, Theorem 3.13], using a totally positive unit congruent to 1 modulo $\mathfrak{q}_2\mathfrak{q}_5$, as in [15, proof of Theorem 8.7], and the ray class group of modulus $\mathfrak{q}_5\infty_1\infty_2$, as in [15, proof of Theorem 8.6]. A companion paper compares the fields cut out by inertia at $\sqrt{5}$ in the same way for the genus-2 Frey curves of $x^5+y^3=z^p$, whose Jacobians also have real multiplication by $\mathcal{O}_K$ [35].

1.4. **Plan.** Section 2 fixes notation and lists the results of [15] that we use. Section 3 computes the fields cut out by inertia at $\mathfrak{q}_5$, Section 4 treats the place 2 and the auxiliary primes, and Sections 5 and 6 treat the two cases modulo 5. Section 7 proves Theorem C, and Section 8 concerns the remaining cases. Appendix A lists the computations on which the proofs depend. The programs and their outputs are in [34].

1.5. **Notation.**

| | |
|---|---|
| $K$, $\mathcal{O}_K$, $\sigma$ | $\mathbb{Q}(\sqrt{5})$, its ring of integers, its nontrivial automorphism |
| $\zeta$, $\omega$ | $\zeta_5$, and $\omega=\zeta+\zeta^{-1}=(-1+\sqrt{5})/2$, so $\mathcal{O}_K=\mathbb{Z}[\omega]$ |
| $\mathfrak{q}_2$, $\mathfrak{q}_5$ | the primes of $K$ above 2 and 5 |
| $F$, $F^{\mathrm{ur}}$, $I_F$ | $K_{\mathfrak{q}_5}=\mathbb{Q}_5(\sqrt{5})$, its maximal unramified extension, its inertia group |
| $F'$, $\mathcal{M}$, $N_0$ | $\mathbb{Q}_5(\zeta_5)$, $F^{\mathrm{ur}}(\zeta_5)$, $\mathcal{M}(6^{1/5})$ |
| $(a,b,c)$, $A$, $B$ | a solution, and $A=a^p$, $B=b^p$ |
| $C^-$, $J^-$, $\Phi$ | the Frey curve $y^2=\Phi(x)$ of [15] and its Jacobian |
| $d$ | the number $\Phi(-A-2c)$, called $d(a,c)$ in [15] |
| $H_D$, $\mathcal{J}_D$ | the curve $y^2=x^5+D$ and its Jacobian |
| $\varepsilon$ | the conductor exponent of $J^-$ at $\mathfrak{q}_5$ |
| $\chi_0$ | the quadratic character of [15] unramified outside 2 |
| $\kappa(u)$ | the Kummer class of a unit $u$ of $\mathbb{Q}_5^{\mathrm{ur}}$ (before Lemma 3.2) |
| $g_1, g_4, g_{16}, g_{64}$ | the newforms with complex multiplication left by [15] (Table 2) |
| $\mathfrak{f}(\cdot)$ | the conductor exponent of a local character or representation |

## 2. Notation and the results of Chen and Koutsianas

Here $p$ is an odd prime, and solutions $(a,b,c)$ and $A=a^p$, $B=b^p$ are as in Section 1 and the table in Section 1.5. We have $\left(\frac{AB}{5}\right)=\left(\frac{ab}{5}\right)$, and for $5\nmid ab$ the condition $ab\equiv\pm2 \pmod 5$ means $\left(\frac{ab}{5}\right)=-1$. A solution with $2\nmid ab$ (so $2\mid c$) is *normalized* if $a\equiv-1 \pmod 4$. Exchanging $a$ and $b$, which keeps $ab$, reaches a normalized solution, since $a+b\equiv a^p+b^p=c^5\equiv0 \pmod 4$ [15, §10].

We use the rest of the notation of that table, with $F^{\mathrm{ur}}$ taken in a fixed algebraic closure. Write $G_E$ for the absolute Galois group of a field $E$, so that $I_F=G_{F^{\mathrm{ur}}}$, and $I_E=G_{EF^{\mathrm{ur}}}$ for $E/F$ finite. The field $F'$ is the completion of $\mathbb{Q}(\zeta_5)$ above 5, ramified quadratic over $F$, and $[\mathcal{M}:F^{\mathrm{ur}}]=2$.

The Frey curve of [15, Lemma 5.5] is $C^-\colon y^2=\Phi(x)$, $\Phi(x)=x^5-5c^2x^3+5c^4x-2(A-B)$, with Jacobian $J^-$, also written $J^-(a,b,c)$. By [15, Theorem 5.4], $K\subseteq\mathrm{End}_K(J^-)\otimes\mathbb{Q}$, with $\omega=\zeta+\zeta^{-1}$ acting by the correspondence of Tautz, Top and Verberkmoes [46]: writing $x=c(u+u^{-1})$, it sends $(x,y)$ to $(x',y)+(x'',y)$, where $x',x''=c(\zeta^{\pm1}u+\zeta^{\mp1}u^{-1})$ are the roots of $x'^2-\omega xx'+x^2+c^2(\omega^2-4)=0$. For an abelian surface $\mathcal{B}/K$ with $K$ acting by endomorphisms defined over $K$ and a prime $\lambda\mid\ell$ of $K$, $\rho_{\mathcal{B},\lambda}$ is the action of $G_K$ on $V_\ell(\mathcal{B})\otimes_{K\otimes\mathbb{Q}_\ell}K_\lambda$, and, for a prime $\mathfrak{p}$ of $K$ above $p$, $\bar\rho_{\mathcal{B},\mathfrak{p}}$ a reduction of $\rho_{\mathcal{B},\mathfrak{p}}$. Frobenius elements are arithmetic. With $x_0=-A-2c$,

$$\Phi(x+x_0)=x^5+5x_0x^4+(10x_0^2-5c^2)x^3+(10x_0^3-15c^2x_0)x^2+a_1x+d,\quad a_1=5(x_0^4-3c^2x_0^2+c^4),$$

and $d=\Phi(x_0)$ is the number $d(a,c)$ of [15, Proposition 7.23].

For $D\in\mathbb{Z}\smallsetminus\{0\}$ let $H_D\colon y^2=x^5+D$ and $\mathcal{J}_D=\operatorname{Jac}H_D$, with $K$ acting by $\zeta+\zeta^{-1}\mapsto[\zeta]+[\zeta^{-1}]$, $[\zeta](x,y)=(\zeta x,y)$; $\mathcal{J}_D^\sigma$ is the same surface with $K$ acting through $\sigma$, whose traces in $K$ are the $\sigma$-conjugates of those of $\mathcal{J}_D$. For $c=0$ the correspondence above is $[\zeta]+[\zeta^{-1}]$, and if moreover $(A,B)=(-\alpha,\alpha)$ the curve $C^-$ is $H_{4\alpha}$. As in [15, §10] we call it the curve of the trivial solution $(-\alpha,\alpha,0)$ and write its Jacobian $J^-(-\alpha,\alpha,0)$. For a Hilbert newform $g$ over $K$ and a prime $\mathfrak{B}$ of its coefficient field, $\rho_{g,\mathfrak{B}}$ is the attached $\mathfrak{B}$-adic representation of $G_K$. The form $g$ has *complex multiplication by* $\mathbb{Q}(\zeta_5)$ if $\rho_{g,\mathfrak{B}}\cong\rho_{g,\mathfrak{B}}\otimes\chi_{\mathbb{Q}(\zeta_5)/K}$; then $\rho_{g,\mathfrak{B}}\cong\operatorname{Ind}_{G_{\mathbb{Q}(\zeta_5)}}^{G_K}\psi$ for a character $\psi$ of $G_{\mathbb{Q}(\zeta_5)}$.

Let $K(S_2,2)\subseteq K^\times/K^{\times2}$ be the group of classes $\Delta$ with $K(\sqrt{\Delta})/K$ unramified at every finite prime not dividing 2 (equivalently, $v_\mathfrak{q}(\Delta)$ even for every prime $\mathfrak{q}\neq\mathfrak{q}_2$), and $K(S_2,2)^*$ the group of the corresponding characters of $G_K$ of order dividing 2, the class $\Delta$ giving the character that cuts out $K(\sqrt{\Delta})$. Both groups have order 8: $K$ has class number 1, its units are generated by $-1$ and $(1+\sqrt{5})/2$, and $\mathfrak{q}_2=(2)$, so $K(S_2,2)=\langle-1,(1+\sqrt{5})/2,2\rangle$. We use the version arXiv:2210.02316v2 of [15], from which we take:

(CK1) [15, Theorem 1.1]: for $n\geq3$, $x^n+y^n=z^5$ has no solution with $2\nmid ab$, $5\mid ab$ (part (I)), nor with $2\mid ab$, $5\nmid ab$ (part (II)).

(CK2) [15, Propositions 7.23, 7.24]: if $5\nmid ab$, $C^-$ has potentially good reduction at $\mathfrak{q}_5$, and the conductor exponent $\varepsilon$ of $\rho_{J^-,\lambda}$ ($\lambda\nmid5$) at $\mathfrak{q}_5$ is 2 if $v_5(d)\geq2$ and 3 if $v_5(d)=1$.

(CK3) [15, Lemma 6.3, Theorems 6.6, 7.1(2), 7.9, 8.7, §7.3]: if $2\nmid ab$, $5\nmid ab$, $2\mid c$, $a\equiv-1\pmod4$ and $p>5$, then there is $\chi_0\in K(S_2,2)^*$ such that $\bar\rho=\bar\rho_{J^-,\mathfrak{p}}\otimes\chi_0$ is irreducible and modular with cyclotomic determinant. The character $\chi_0$ cuts out $K(\sqrt{\Delta_0})$, where $\Delta_0$ is one of the classes listed in [15, Remark 7.2]. The representation $\rho_{J^-,\lambda}\otimes\chi_0$ has conductor $\mathfrak{q}_2^s\mathfrak{q}_5^\varepsilon\mathfrak{q}_{ab}$, where $s\in\{1,2\}$ and $\mathfrak{q}_{ab}$ is the product of the primes dividing $ab$ and prime to 10 [15, Theorem 7.9]. The Serre level of $\bar\rho$ is $\mathfrak{q}_2^{s'}\mathfrak{q}_5^\varepsilon$ with $s'\in\{0,1,2\}$ by [15, Theorem 7.1(2)], and it divides $\mathfrak{q}_2^s\mathfrak{q}_5^\varepsilon$. Finally, $J^-$ has multiplicative reduction at the primes dividing $\mathfrak{q}_{ab}$ [15, Lemma 7.5 and its proof].

(CK4) [15, §§9.3, 10]: then level lowering prime by prime, keeping $\mathfrak{q}_2$, gives $\bar\rho\cong\bar\rho_{g,\mathfrak{B}}$ for a newform $g$ of parallel weight 2, trivial character and level $\mathfrak{q}_2^s\mathfrak{q}_5^\varepsilon$. Traces at the primes above $3,7,11$ exclude every newform of level $\mathfrak{q}_2\mathfrak{q}_5^\varepsilon$ for $p\notin\{2,3,5,7\}$; for $p=11$, those above 3 and 7 suffice (item A1). Traces at the primes above $3,7,11$ also exclude every newform of level $\mathfrak{q}_2^2\mathfrak{q}_5^\varepsilon$ for $p\notin\{2,3,5,19\}$ except four: $g_1$, of level $\mathfrak{q}_2^2\mathfrak{q}_5^2$, and $g_4,g_{16},g_{64}$, of level $\mathfrak{q}_2^2\mathfrak{q}_5^3$. The form $g_1$ is attached to $\mathcal{J}_{1024}\cong\mathcal{J}_1$, the twist of $J^-(-8,8,0)$ by $K(\sqrt{2})/K$, and $g_4,g_{16},g_{64}$ are attached to $\mathcal{J}_4,\mathcal{J}_{16},\mathcal{J}_{64}$.

These statements hold for every prime $p\geq11$. (CK1) is proved for every exponent $n\geq3$, and (CK2) is local at $\mathfrak{q}_5$ and does not involve $p$. In (CK3), the modularity of $J^-$ [15, Theorem 6.6] holds for every $p$, and the conductors and the Serre level [15, Theorem 7.1] and the irreducibility [15, Theorem 8.7] need $p>5$. The level lowering and the trace comparisons in (CK4) are those of [15, §§9.3, 10], which assume $p\geq11$ and apply level lowering for Hilbert modular forms, as cited in [15, §9.2], to the irreducible representation of (CK3); the only primes $p\geq11$ they leave out are those stated in (CK4), so [15, §10] does not cover $p=19$, which Remark 5.4 treats. Section 8 uses in addition the case $10\mid ab$ of the proof of [15, Theorem 1.2]; that theorem is stated for $p$ sufficiently large, but its proof in the case $10\mid ab$ [15, §10] assumes only $p\geq11$. Of [15, §10] we use the level lowering and the list of forms left by the trace comparison in (CK4). That comparison, made at the primes above 3, 7 and 11, uses squared traces, which do not change under twisting by any $\chi_0\in K(S_2,2)^*$,

so it covers all eight characters at once. Applied to every newform of level $\mathfrak{q}_2^s\mathfrak{q}_5^\varepsilon$, $s \in \{1,2\}$, $\varepsilon \in \{2,3\}$, it leaves exactly the forms of (CK4), with the Hecke eigenvalues of the LMFDB [48] as with those of the Brandt module of the icosian ring (items A1 and A10).

As $\Delta_0$ is a unit times a power of 2, $\chi_0|_{G_F}$ is unramified. The $g_D$ have complex multiplication by $\mathbb{Q}(\zeta_5)$, as $\mathcal{J}_D$ does. They are the LMFDB newforms of Table 2: their Hecke eigenvalues equal the Frobenius traces of $\mathcal{J}_D$ at the primes above the 40 rational primes $q \equiv 1 \pmod 5$ below 1000 (item A1).

TABLE 2. The newforms left by [15, §10]; labels from [48].

| form | Jacobian | level | exponent at $\mathfrak{q}_5$ | LMFDB label |
|---|---|---|---|---|
| $g_1$ | $\mathcal{J}_1 \cong \mathcal{J}_{1024}$ | $\mathfrak{q}_2^2\mathfrak{q}_5^2$ | 2 | 2.2.5.1-400.1-b |
| $g_4$ | $\mathcal{J}_4$ | $\mathfrak{q}_2^2\mathfrak{q}_5^3$ | 3 | 2.2.5.1-2000.1-e |
| $g_{16}$ | $\mathcal{J}_{16}$ | $\mathfrak{q}_2^2\mathfrak{q}_5^3$ | 3 | 2.2.5.1-2000.1-d |
| $g_{64}$ | $\mathcal{J}_{64}$ | $\mathfrak{q}_2^2\mathfrak{q}_5^3$ | 3 | 2.2.5.1-2000.1-b |

**Lemma 2.1** (Reduction and descent data)**.** *Let $E$ be a field complete for a discrete valuation, with perfect residue field of characteristic $q_0$, let $\overline{E}$ be an algebraic closure of $E$ and $\overline{\mathbb{F}}$ its residue field, and for $g \in G_E$ let $\bar{g}$ be the automorphism of $\overline{\mathbb{F}}$ induced by $g$. Let $C$ be a curve of genus 2 over $E$ with affine coordinates $x, y$, and $E' \subseteq \overline{E}$ a finite Galois extension of $E$. Suppose that $C_{E'}$ is the generic fiber of a smooth proper model $\mathcal{C}$ over $\mathcal{O}_{E'}$, the closure in the weighted projective plane $\mathbb{P}(1,3,1)$ of a curve $Y^2 + Q_1(X)Y = Q_0(X)$ with $Q_0, Q_1 \in \mathcal{O}_{E'}[X]$, $\deg Q_0 = 5$, $\deg Q_1 \le 2$, where $x \in E' + E'^{\times}X$ and $y \in E'^{\times}Y + E'[X]$. Let $\tilde{C}$ be its special fiber. Then for $g \in G_E$ there are $u_g, v_g \in E'^{\times}$, $t_g \in E'$ and $s_g \in E'[X]$ such that, for every $P \in C(\overline{E})$,*

$$X(gP) = u_g\, g(X(P)) + t_g, \qquad Y(gP) = v_g\, g(Y(P)) + s_g(g(X(P))).$$

*Assume that this change of coordinates and its inverse are integral, that is, $u_g, v_g \in \mathcal{O}_{E'}^{\times}$, $t_g \in \mathcal{O}_{E'}$ and $s_g \in \mathcal{O}_{E'}[X]$, for every $g \in G_E$. The* reduced descent datum *of $g$ is the map $\tilde{g}$ of $\tilde{C}(\overline{\mathbb{F}})$ that fixes the point at infinity and sends $(\bar{X}, \bar{Y})$ to $(\bar{u}_g\bar{g}(\bar{X}) + \bar{t}_g,\ \bar{v}_g\bar{g}(\bar{Y}) + \bar{s}_g(\bar{g}(\bar{X})))$, bars denoting reduction. Then:*

- *(a) for $P \in C(\overline{E})$ with reduction $\tilde{P}$, the reduction of $gP$ is $\tilde{g}(\tilde{P})$;*
- *(b) for every prime $\ell \neq q_0$, reduction is an isomorphism $T_\ell(\operatorname{Jac} C) \to T_\ell(\operatorname{Jac} \tilde{C})$ that is compatible with the Weil pairings, carries the action of each $g \in G_E$ to the map induced by $\tilde{g}$ on divisor classes, and carries each endomorphism of $\operatorname{Jac} C_{E'}$ to its reduction, an endomorphism of $\operatorname{Jac} \tilde{C}$;*
- *(c) if $C_1$, $C_2$ are two such curves, with the same $E'$, and $\varphi\colon \operatorname{Jac} \tilde{C}_1 \to \operatorname{Jac} \tilde{C}_2$ is a homomorphism over $\overline{\mathbb{F}}$ that commutes with the maps induced by $\tilde{g}_1$ and $\tilde{g}_2$ for every $g \in G_E$, then $\varphi$ induces, through (b), a homomorphism of $\mathbb{Z}_\ell[G_E]$-modules $T_\ell(\operatorname{Jac} C_1) \to T_\ell(\operatorname{Jac} C_2)$. This homomorphism multiplies the Weil pairings by $m$ if $\varphi^\dagger\varphi = m$, where $\varphi^\dagger$ is the adjoint of $\varphi$ for the canonical principal polarizations. If $\varphi$ is an isogeny of degree prime to $\ell$, the homomorphism is an isomorphism, and so is the map it induces on $\ell$-torsion. If $\varphi = \alpha_*$ for an isomorphism of curves $\alpha\colon \tilde{C}_1 \to \tilde{C}_2$ over $\overline{\mathbb{F}}$, it suffices that $\alpha \circ \tilde{g}_1 = \tilde{g}_2 \circ \alpha$ for every $g \in G_E$; then $m = 1$, and $\varphi$ carries an endomorphism of $\operatorname{Jac} C_{1,E'}$ to one of $\operatorname{Jac} C_{2,E'}$ whenever $\alpha_*$ carries the reduction of the first to that of the second.*

*Proof.* The displayed formulas follow by applying $g$ to the coordinates and changing coordinates; the coefficients lie in $E'$ as $E'/E$ is Galois. (a) If $X(P)$ is integral, so is $Y(P)$, and the formulas show that $gP$ has integral coordinates reducing to $\tilde{g}(\tilde{P})$. Otherwise $v(X(gP)) = v(X(P)) < 0$, and $P$ and $gP$ both reduce to the point at infinity, the only point of $\tilde{C}$ outside the affine chart. As every point of $\tilde{C}(\overline{\mathbb{F}})$ is a reduction (Hensel's lemma), $\tilde{g}$ maps $\tilde{C}(\overline{\mathbb{F}})$ to itself. (b) By [10, §9.4, Proposition 4], $\mathrm{Pic}^0_{\mathcal{C}/\mathcal{O}_{E'}}$ is an abelian scheme with fibers $\operatorname{Jac} C_{E'}$ and $\operatorname{Jac}\tilde{C}$; so reduction is a bijection on $\ell^n$-torsion [43, §1, Lemma 2]. Sections of the smooth model through points of $C$ (over finite extensions of $E'$) are Cartier divisors, so the class of a divisor reduces to the class of its reduction, and (a) gives the compatibility of $g$ with $\tilde{g}$. An endomorphism of $\operatorname{Jac} C_{E'}$ extends to the abelian scheme, which is the Néron model of its generic fiber [10, §1.2, Proposition 8], so it commutes with reduction. For the Weil pairing $e_{\ell^n}([\mathfrak{d}_1],[\mathfrak{d}_2]) = f_1(\mathfrak{d}_2)/f_2(\mathfrak{d}_1)$, where $\ell^n\mathfrak{d}_i = \operatorname{div} f_i$, move $\mathfrak{d}_1, \mathfrak{d}_2$ by divisors of functions so that their reductions have disjoint supports, and scale $f_1, f_2$ to have nonzero reductions $\tilde{f}_1, \tilde{f}_2$; then $\operatorname{div}\tilde{f}_i = \ell^n\tilde{\mathfrak{d}}_i$, and $f_1(\mathfrak{d}_2)/f_2(\mathfrak{d}_1)$ reduces to $\tilde{f}_1(\tilde{\mathfrak{d}}_2)/\tilde{f}_2(\tilde{\mathfrak{d}}_1)$, the Weil pairing of the reductions. The divisors can be moved in this way because every function on $\tilde{C}$ is a quotient of two sections of $\mathcal{O}(n\infty)$ for some $n \geq 3$, and these sections lift after a finite unramified extension of $E'$, as $H^0(\mathcal{C}, \mathcal{O}(n\infty)) \to H^0(\tilde{C}, \mathcal{O}(n\infty))$ is onto for $n \geq 3$. (c) Compose $\varphi$ with the isomorphisms of (b); $e(\varphi z_1, \varphi z_2) = e(z_1, \varphi^\dagger \varphi z_2)$ for the Weil pairings, and $\alpha_*$, coming from an isomorphism of curves, preserves the canonical principal polarizations. □

We use Lemma 2.1 with $E'/E$ equal to $\mathbb{Q}_2(\zeta_5, 2^{1/5})/\mathbb{Q}_2$ (Propositions 4.1 and 6.6), $\mathbb{Q}_5(5^{1/8})/F$ (Proposition 6.1), $L_1/L_1$ (Proposition 6.3), $L_1/F$ (Proposition 6.4) and $L_1(\zeta_8)/\mathbb{Q}_5$ (Lemma 6.5), where $L_1 = \mathbb{Q}_5((-5)^{1/8}, 6^{1/5})$.

## 3. Inertia at $\sqrt{5}$ and the Weierstrass points

The roots of $\Phi$ have a closed form, and over $\mathcal{M}$ they generate a Kummer extension of degree 1 or 5 (Proposition 3.4). Its Kummer class is an element of $\overline{\mathbb{F}}_5$ up to $\mathbb{F}_5^\times$, and comparing it with the class for the curves $H_D$ is how inertia at $\mathfrak{q}_5$ separates $J^-$ from the forms with complex multiplication.

**Lemma 3.1.** *Let $\mathcal{B} = \operatorname{Jac} C$, $C/K$ of genus 2 with potentially good reduction at $\mathfrak{q}_5$ and Weierstrass points $W$, with $K \subseteq \operatorname{End}_K(\mathcal{B}) \otimes \mathbb{Q}$. Let $L_\mathcal{B}$ be the fixed field of $\ker(\rho_{\mathcal{B},\lambda}|_{I_F})$, $\lambda \nmid 5$.*

*(a) $L_\mathcal{B}$ does not depend on $\lambda$; on $I_F$, the traces of $\rho_{\mathcal{B},\lambda}$ lie in $K$ and do not depend on $\lambda$, and the determinant is 1.*

*(b) $L_\mathcal{B}$ contains the field $F^{\mathrm{ur}}(W)$ generated over $F^{\mathrm{ur}}$ by the coordinates of the points of $W$, which we call the* Weierstrass field *of $C$, and $|\rho_{\mathcal{B},\lambda}(I_F)| = [L_\mathcal{B} : F^{\mathrm{ur}}]$ divides $2 \cdot 6!$.*

*(c) For $p \geq 7$ and $\mathfrak{p} \mid p$, $\ker(\bar{\rho}_{\mathcal{B},\mathfrak{p}}|_{I_F}) = I_{L_\mathcal{B}}$.*

*Proof.* Over a finite extension of $F^{\mathrm{ur}}$ where $C$ has good reduction $\tilde{C}$, $I_F$ acts on $V_\ell(\mathcal{B})$ through automorphisms of $\tilde{C}$ commuting with $K$ [43, §2], the reduced descent data of Lemma 2.1. For such an automorphism $\gamma$ the characteristic polynomial on $V_\lambda$ lies in $K[x]$ and does not depend on $\lambda$ (the traces of $t\gamma$, $t \in K$, on $V_\ell$ are rational and independent of $\ell$, and the trace form of $K \otimes \mathbb{Q}_\ell$ is nondegenerate); the determinant is cyclotomic. If $\gamma$ is trivial on one $V_\lambda$, then, as $\gamma$ has finite order and the same characteristic polynomial on every $V_\lambda$, it is trivial on all, so on $H^1(\tilde{C})$, and $\gamma = 1$ by the Lefschetz formula. So $I_{L_\mathcal{B}}$ is the kernel

of $I_F \to \operatorname{Aut}\tilde{C}$, which gives (a). Reduction maps $W$ bijectively, compatibly with $I_F$, onto the Weierstrass points of $\tilde{C}$, so $I_{L_\mathcal{B}}$ fixes $W$; and $\operatorname{Aut}\tilde{C}/\langle\iota\rangle$, $\iota$ the hyperelliptic involution, acts faithfully on those six points, giving (b). For (c), the kernel of reduction on $\mathrm{GL}_2(\mathcal{O}_{K_\mathfrak{p}})$ is pro-$p$ and $p \nmid 2\cdot 6!$. □

For a unit $u$ of $\mathbb{Q}_5^{\mathrm{ur}}$ let $\hat{u}$ be the root of unity of order prime to 5 with $u \equiv \hat{u} \pmod 5$, and $\kappa(u) \in \overline{\mathbb{F}}_5$ the residue of $(u/\hat{u}-1)/5$; so $\kappa(6)=1$. By an $\mathbb{F}_5$-*line* in $\overline{\mathbb{F}}_5$ we mean a set $\mathbb{F}_5 x$ with $x \neq 0$.

**Lemma 3.2.** *Let $u, u'$ be units of $\mathbb{Q}_5^{\mathrm{ur}}$.*

*(a) $u \in \mathcal{M}^{\times 5}$ if and only if $\kappa(u)=0$; if $\kappa(u),\kappa(u') \neq 0$, then $\mathcal{M}(u^{1/5}) = \mathcal{M}(u'^{1/5})$ if and only if $\kappa(u') \in \mathbb{F}_5^\times \kappa(u)$.*

*(b) If $u \in \mathbb{Z}_5^\times$, then $\kappa(u) \in \mathbb{F}_5$, and $\kappa(u)=0$ if and only if $u^4 \equiv 1 \pmod{25}$.*

*(c) If $u$ is a unit of the unramified quadratic extension $\mathbb{Q}_{25}$ of $\mathbb{Q}_5$ and $N_{\mathbb{Q}_{25}/\mathbb{Q}_5}(u) \in \mathbb{Z}_5^{\times 5}$, then $\kappa(u) \in \zeta_8\mathbb{F}_5$, where $\zeta_8 \in \mathbb{F}_{25}$ has order 8.*

*Proof.* Let $\pi_\mathcal{M}$ be a uniformizer of $\mathcal{M}$ and $v$ its normalized valuation, so that $v(5)=4$. Let $\mathcal{O}$ be the ring of integers of $\mathcal{M}$, put $U_n = 1+\pi_\mathcal{M}^n\mathcal{O}$, and let $\eta = 5/\pi_\mathcal{M}^4$, a unit. Then $1+5y \mapsto \bar{y}$ gives $U_4/U_5 \cong \overline{\mathbb{F}}_5$, and $U_1^5 \subseteq U_5$. We show that $U_5 \subseteq \mathcal{M}^{\times 5}$. For $t \in \mathcal{O}$, $(1+\pi_\mathcal{M} t)^5 \equiv 1+\pi_\mathcal{M}^5(t^5+\eta t) \pmod{\pi_\mathcal{M}^6}$, and the map $\bar{t} \mapsto \bar{t}^5 + \bar{\eta}\bar{t}$ of $\overline{\mathbb{F}}_5$ is onto, so every element of $U_5$ is a fifth power times an element of $U_6$. For $j \geq 2$, $(1+\pi_\mathcal{M}^j t)^5 \equiv 1+\eta\pi_\mathcal{M}^{j+4}t \pmod{\pi_\mathcal{M}^{j+5}}$, so every element of $U_{j+4}$ is a fifth power times an element of $U_{j+5}$. Together these reduce $U_5$ to $U_9$, and every element of $U_9$ is a fifth power by Hensel's lemma, as $9 > 2v(5)$. Conversely, if $(\xi_0 x_1)^5 \in U_4$ with $x_1 \in U_1$ and $\xi_0$ a root of unity of order prime to 5, then $\xi_0^5 \equiv 1 \pmod{\pi_\mathcal{M}^4}$, so $\xi_0 = 1$. Hence $U_4 \cap \mathcal{M}^{\times 5} = U_5$ and $U_4/U_5 \hookrightarrow \mathcal{M}^\times/\mathcal{M}^{\times 5}$, the class of $u$ being that of $\kappa(u)$. Kummer theory gives (a); (b) holds as $(1+5\mathbb{Z}_5)^5 = 1+25\mathbb{Z}_5$. For (c), with $\mathrm{Fr}_5$ the Frobenius of $\mathbb{Q}_{25}/\mathbb{Q}_5$ and $u = \hat{u}(1+5y)$, $N(u)/\widehat{N(u)} \equiv 1+5(y+\mathrm{Fr}_5 y) \pmod{25}$ lies in $(1+5\mathbb{Z}_5)^5 = 1+25\mathbb{Z}_5$, so $\kappa(u)^5 = -\kappa(u)$. □

**Lemma 3.3.** *Let $(a,b,c)$ be a solution with $5 \nmid abc$ and $v_5(d) \geq 2$, and $L = \mathbb{Q}_5(\pi)$, $\pi^8 = 5$; then $F = \mathbb{Q}_5(\pi^4)$ and $L/F$ is cyclic, totally ramified of degree 4. The curve $C^-$ has good reduction over $L$, with special fiber $y^2 = x^5 + (abc)^2 x$ over $\mathbb{F}_5$.*

*Proof.* Write $\Phi(x+x_0) = x^5 + \sum_{k\leq 4} a_k x^k$ as in Section 2, so that $a_0 = d$. Modulo 5, $c \equiv A+B$, $x_0 \equiv 2A+3B$, $a_1/5 \equiv (x_0^2+c^2)^2$ and $x_0^2+c^2 \equiv (2A+3B)^2+(A+B)^2 \equiv -AB$, so $u = a_1/5 \equiv (abc)^{2p} \equiv (abc)^2$. Put $x = x_0 + \pi^2 X$, $y = \pi^5 Y$: the coefficient of $X^k$, $k \leq 4$, becomes $a_k \pi^{2k-10}$, of $\pi$-valuation $8v_5(a_k)+2k-10$, which is $\geq 6, \geq 4, \geq 2, 0, \geq 6$ for $k = 4, \ldots, 0$. The reduction $Y^2 = X^5 + uX$ is smooth. □

**Proposition 3.4.** *Let $(a,b,c)$ be a solution with $5 \nmid abc$, and $W$ the Weierstrass points of $C^-$.*

*(a) There is $\delta \in \mathbb{Q}_5^{\mathrm{ur}}$, $\delta^2 = -AB$, with $\beta = A-B+2\delta = (\sqrt{A}+\sqrt{-B})^2$ a unit; $\beta' = A-B-2\delta$ has $\beta\beta' = c^{10}$. With $v^5 = \beta$ the roots of $\Phi$ are $v\zeta^k + c^2 v^{-1}\zeta^{-k}$ ($k \in \mathbb{Z}/5$), and $\mathcal{M}F^{\mathrm{ur}}(W) = \mathcal{M}(\beta^{1/5})$.*

*(b) $\kappa(\beta) \neq 0$ if and only if $v_5(d)=1$, if and only if $\varepsilon = 3$.*

*(c) If $\left(\frac{abc}{5}\right) = +1$ and $\varepsilon = 3$, then $\mathcal{M}F^{\mathrm{ur}}(W) = N_0$.*

*(d) If $\left(\frac{abc}{5}\right) = -1$, then $5 \nmid c$; if also $\varepsilon = 3$, $\mathcal{M}F^{\mathrm{ur}}(W)$ is cyclic quintic over $\mathcal{M}$ and different from $N_0$.*

*(e) If $D \in \mathbb{Z}_5^\times$ is not a fifth power, the Weierstrass points $W_D$ of $H_D$ have $\mathcal{M}F^{\mathrm{ur}}(W_D) = N_0$; this holds for $D = 4, 16, 64$.*

*Proof.* (a) $\beta+\beta'=2(A-B)$ and $\beta\beta'=(A+B)^2=c^{10}$; if $5\mid c$, $A-B\equiv 2A$ is a unit, so the sign of $\delta$ can be chosen with $\beta$ a unit. The identity $(v+w)^5-5vw(v+w)^3+5(vw)^2(v+w)=v^5+w^5$ with $w=c^2/v$ gives $\Phi(v+w)=\beta+\beta'-2(A-B)=0$, and likewise for $(v\zeta^k, w\zeta^{-k})$; two of these roots coincide only if $\beta=\beta'$, i.e. $AB=0$. They lie in $\mathcal{M}(v)$, and if $v\notin\mathcal{M}$ the generator $v\mapsto\zeta v$ of $\mathrm{Gal}(\mathcal{M}(v)/\mathcal{M})$ moves each root, so each generates $\mathcal{M}(v)$.

(b) By Lemma 3.2(a), $\kappa(\beta)\neq 0$ if and only if $5\mid[F^{\mathrm{ur}}(W):F^{\mathrm{ur}}]$. Modulo 5, $c\equiv A+B$ and $x_0\equiv 2A+3B$, so $d\equiv x_0-2(A-B)\equiv 0$, and the other nonleading coefficients of $\Phi(x+x_0)$ are divisible by 5. If $v_5(d)=1$ it is Eisenstein over $\mathbb{Z}_5$, so $5\mid[F^{\mathrm{ur}}(W):F^{\mathrm{ur}}]$. If $v_5(d)\geq 2$, $C^-$ has good reduction over the tame extension $L$ of Lemma 3.3 (see also [15, Proposition 7.23(i)]); then $F^{\mathrm{ur}}(W)\subseteq L_{J^-}\subseteq LF^{\mathrm{ur}}$ by Lemma 3.1(b). Conclude by (CK2).

(c) $-AB$ is a square mod 5, so $\beta\in\mathbb{Z}_5^\times$, $\kappa(\beta)\in\mathbb{F}_5^\times=\mathbb{F}_5^\times\kappa(6)$; apply Lemma 3.2(a).

(d) If $5\mid c$, $-AB\equiv A^2$ would be a square. So $\delta\in\mathcal{O}_{\mathbb{Q}_{25}}\smallsetminus\mathbb{Z}_5$, $\mathrm{Fr}_5(\beta)=\beta'$, and $N(\beta)=(c^2)^5$; by Lemma 3.2(c) and part (b), $\kappa(\beta)\in\zeta_8\mathbb{F}_5^\times$, a line other than $\mathbb{F}_5$.

(e) The roots of $x^5+D$ generate $\mathcal{M}((-D)^{1/5})$, and $\kappa(-D)\in\mathbb{F}_5^\times$ by Lemma 3.2(b). For $D=4,16,64$: $D^4\equiv 6,11,16 \pmod{25}$, and $\kappa(-4),\kappa(-16),\kappa(-64)=4,3,2$. □

*Remark* 3.5. For each sign of $\left(\frac{ab}{5}\right)$, 32 classes ($A$ mod 25, $c$ mod 5) have $\varepsilon=3$, 8 have $\varepsilon=2$ (item A2), so both values of $\varepsilon$ occur in each case.

**Lemma 3.6.** *Let $g$ have complex multiplication by $\mathbb{Q}(\zeta_5)$, $\mathfrak{B}\nmid 5$, and $L_g$ the fixed field of* $\ker(\rho_{g,\mathfrak{B}}|_{I_F})$.

*(a)* $\mathrm{tr}\,\rho_{g,\mathfrak{B}}(\gamma)=0$ *for* $\gamma\in G_F\smallsetminus G_{F'}$.

*(b) If $g$ has conductor exponent 3 at $\mathfrak{q}_5$, then $|\rho_{g,\mathfrak{B}}(I_F)|$ divides 40 and $L_g\supseteq N_0$.*

*Proof.* (a) $G_F\cap G_{\mathbb{Q}(\zeta_5)}=G_{F'}$, so $\chi_{\mathbb{Q}(\zeta_5)/K}(\gamma)=-1$.

(b) Let $w$ be the prime of $\mathbb{Q}(\zeta_5)$ above 5, so that $G_{F'}$ is its decomposition group, and $\psi_w=\psi|_{G_{F'}}$ ($\psi$ as in Section 2). By Mackey, $\rho_{g,\mathfrak{B}}|_{G_F}\cong\mathrm{Ind}_{G_{F'}}^{G_F}\psi_w$; as $F'/F$ is tamely ramified quadratic, the conductor exponent is $3=\mathfrak{f}(\psi_w)+1$. So, with $U_n=1+\mathfrak{m}_{F'}^n$ and rec the reciprocity map of $F'$, $\psi_w\circ\mathrm{rec}$ is trivial on $U_2$ and not on $U_1$. On $I_{F'}$ the representation is $\psi_w\oplus\psi_w^\tau$, where $\psi_w^\tau(x)=\psi_w(\tau x\tau^{-1})$ for a fixed $\tau\in G_F\smallsetminus G_{F'}$, through $\mathcal{O}_{F'}^\times/U_2\cong\mathbb{Z}/4\times\mathbb{Z}/5$, so the order divides 40; elements of $I_F\smallsetminus I_{F'}$ swap the two lines, so $I_{L_g}\subseteq\ker\psi_w$. The group $H=\{u\in\mathcal{O}_{F'}^\times:\psi_w(\mathrm{rec}\,u)=1\}$ meets $U_1$ in $U_2$, so $H\subseteq\mu_4\times U_2$, and $L_g$ contains the field cut out over $\mathcal{M}=F'^{\mathrm{ur}}$ by $\mathrm{rec}(\mu_4\times U_2)$. This field is $N_0$: $E=F'(6^{1/5})$ is cyclic of degree 5 and totally ramified (Lemma 3.2); writing $6^{1/5}=1+z$, $(1+z)^5=6$ forces $v_E(z)=4$, and $v_E((\zeta-1)(1+z))=5$, so the break is 1 and the conductor 2; hence $\mathcal{O}_{F'}^\times\cap N_{E/F'}E^\times$, of index 5, contains $U_2$ and $\mu_4$, so equals $\mu_4\times U_2$, and $\mathcal{M}E=N_0$. □

## 4. The place 2 and the primes above 11

Chen and Koutsianas obtain some $\chi_0$ in (CK3) without saying which [15, Proposition 7.15], and compare traces up to the action of $\sigma$ and up to sign [15, §§9.1, 9.3, 10]. The model and the inertial type of $C^-$ at $\mathfrak{q}_2$ are known up to a quadratic twist [1, Propositions 4.28, 5.18(1), Corollary 4.32, Theorem 5.11 and Table 2], [17, Propositions 2.15, 4.3, Corollary 4.6]; comparing with the curves $H_D$ fixes the twist and the action of $K$. Write $\mathbb{Q}_4=K_{\mathfrak{q}_2}=\mathbb{Q}_2(\sqrt{5})$, the unramified quadratic extension of $\mathbb{Q}_2$, $t_2=2^{1/5}$, and $P_k(\omega)=\zeta^k+\zeta^{-k}\in\mathcal{O}_K$; so $P_1(\omega)=\omega$ and $P_2(\omega)=\sigma(\omega)$.

**Proposition 4.1.** *Let $p\geq 7$ and $(a,b,c)$ a normalized solution with $2\nmid abc$.*

(a) *For every prime $\lambda \nmid 2$ of $K$, $\rho_{J^-,\lambda}|_{G_{\mathbb{Q}_4}} \cong \rho_{\mathcal{J}_4,\lambda}|_{G_{\mathbb{Q}_4}}$, compatibly with the actions of $K$; inertia acts through a cyclic group of order 5, as $\theta_2 \oplus \theta_2^{-1}$ for a character $\theta_2$ of order 5, and the conductor exponent is 2.*

(b) *For $D = 2^j$, $j = 0, 2, 4, 6$, $\mathcal{J}_D$ has good reduction over $\mathbb{Q}_4^{\mathrm{ur}}(t_2)$ with special fiber $w^2 + w = X^5$, and an element $\gamma$ of the inertia group of $\mathbb{Q}_4$ acting with order 5 acts on $J^-$, $\mathcal{J}_4$, $\mathcal{J}_{16}$ with the same trace in $K$, and on $\mathcal{J}_{64}$, $\mathcal{J}_1$ with its $\sigma$-conjugate.*

(c) *Hence, if $\bar{\rho}_{J^-,\mathfrak{p}} \otimes \chi_0 \cong \bar{\rho}_{g,\mathfrak{B}}$ with $\chi_0 \in K(S_2, 2)^*$ and $g$ a newform whose level has $\mathfrak{q}_2$-exponent at most 2, then $\chi_0 = 1$; and if $\bar{\rho}_{J^-,\mathfrak{p}} \cong \bar{\rho}_{\mathcal{A},\mathfrak{p}}$ with $\mathcal{A} \in \{\mathcal{J}_D, \mathcal{J}_D^\sigma\}$, then $\mathcal{A} = \mathcal{J}_D$ for $D = 4, 16$ and $\mathcal{A} = \mathcal{J}_D^\sigma$ for $D = 64, 1$.*

*Proof.* (a) *The model.* As $A \equiv a \equiv -1 \pmod 4$, $-A \equiv 1$ or $5 \pmod 8$ is a square in $\mathbb{Q}_4$; let $\varsigma^2 = -A$, $\varsigma \in \mathcal{O}_{\mathbb{Q}_4}^\times$, and $n_2 = v_2(c) \geq 1$. The substitution $x = t_2^4 X$, $y = 2(\varsigma + 2w)$ gives

$$y^2 - \Phi(x) = 16\big(w^2 + \varsigma w - X^5 - c_3 X^3 - c_1 X - c_0\big), \qquad c_3 = -\tfrac{5c^2 t_2^{12}}{16}, \quad c_1 = \tfrac{5c^4 t_2^4}{16}, \quad c_0 = \tfrac{c^5}{8},$$

of 2-adic valuations $2n_2 - \frac{8}{5}$, $4n_2 - \frac{16}{5}$, $5n_2 - 3 > 0$. So over $\mathbb{Q}_2(\zeta_5, t_2)$, which is finite and Galois over $\mathbb{Q}_2$ and contains $\mathbb{Q}_4$, the model $w^2 + \varsigma w = X^5 + c_3 X^3 + c_1 X + c_0$ is integral with smooth special fiber $\tilde{C}\colon w^2 + w = X^5$ ($\bar{\varsigma} = 1$). The same substitution turns $C_0^-\colon y^2 = x^5 - 4A$, the curve $C^-$ read with $(A, B, c) = (A, -A, 0)$, into $w^2 + \varsigma w = X^5$ exactly.

*The descent data.* For $g \in G_{\mathbb{Q}_2}$ let $\zeta_g = g(t_2)/t_2 \in \mu_5$. Since $X = x/t_2^4$ and $w = (y/2 - \varsigma)/2$, on points

$$X(gP) = \frac{g(t_2^4 X(P))}{t_2^4} = \zeta_g^4\, g(X(P)), \qquad w(gP) = g(w(P)) + \frac{g(\varsigma) - \varsigma}{2},$$

for both curves, with the same $t_2$ and $\varsigma$, and $g(\varsigma) = \varsigma$ for $g \in G_{\mathbb{Q}_4}$. These changes of coordinates and their inverses are integral, so the two curves have the same reduced descent data (Lemma 2.1): $g \in G_{\mathbb{Q}_4}$ acts on $\tilde{C}$ by $P \mapsto [\bar{\zeta}_g^4](\mathrm{Frob}^{n(g)} P)$, where $\mathrm{Frob}^{n(g)}$ is the power of the Frobenius of $\overline{\mathbb{F}}_2$ induced by $g$. Hence reduction identifies $T_\ell$ of both Jacobians ($\ell \neq 2$) with $T_\ell(\mathrm{Jac}\,\tilde{C})$, $G_{\mathbb{Q}_4}$-equivariantly.

*The real multiplication.* In the coordinate $X$ the correspondence reads $X'^2 - \omega X X' + X^2 + c^2 t_2^{-8}(\omega^2 - 4) = 0$; the constant has valuation $2n_2 - \frac{8}{5} > 0$ ($\omega^2 - 4$ has norm 5), so it reduces to $(X' - \bar{\zeta} X)(X' - \bar{\zeta}^{-1} X) = 0$, that is to $[\bar{\zeta}] + [\bar{\zeta}^{-1}]$, which is also the reduction for $C_0^-$. Hence $\rho_{J^-,\lambda}|_{G_{\mathbb{Q}_4}} \cong \rho_{\mathrm{Jac}\, C_0^-,\lambda}|_{G_{\mathbb{Q}_4}}$, $K$-linearly.

*From $C_0^-$ to $H_4$.* Every unit of $\mathbb{Q}_4$ is a fifth power; with $\varrho^5 = -A$, $x = \varrho x'$ turns $C_0^-$ into $y^2 = -A(x'^5 + 4)$, the twist of $H_4$ by $-A$, a square in $\mathbb{Q}_4$, and commutes with $[\zeta]$. So $\rho_{J^-,\lambda}|_{G_{\mathbb{Q}_4}} \cong \rho_{\mathcal{J}_4,\lambda}|_{G_{\mathbb{Q}_4}}$.

*Inertia.* Inertia acts through $\langle[\bar{\zeta}]\rangle$, of order 5; since the quotient of $\tilde{C}$ by $X \mapsto \bar{\zeta} X$ has genus 0, there are no inertia invariants, so $\rho|_I = \theta_2 \oplus \theta_2^{-1}$ with $\theta_2$ of order 5, and the conductor exponent is 2.

(b) For $D = 2^j$, $x = t_2^{j+2} X$, $y = 2^{j/2}(1 + 2w)$ turns $H_D$ into $w^2 + w = X^5$ exactly, and $[\zeta]$ reduces to $X \mapsto \bar{\zeta} X$. An element $\gamma$ of the inertia group acts on $X$ by $\zeta_\gamma^{j+2}$ for $\mathcal{J}_D$ and by $\zeta_\gamma^4$ for $J^-$. Fix $\gamma$ with $\bar{\zeta}_\gamma^4 = \bar{\zeta}^k$, $k \not\equiv 0 \pmod 5$. As $\omega$ acts by $[\bar{\zeta}] + [\bar{\zeta}^{-1}]$ on the special fiber, the trace of $\gamma$ is $P_k(\omega)$ for $J^-$ and $P_{km}(\omega)$ for $\mathcal{J}_D$, $m \equiv (j+2)/4 \pmod 5$. Now $m \equiv 1, 4, 2, 3$ for $D = 4, 16, 64, 1$, so the traces agree with those of $J^-$ for $D = 4, 16$ and are their $\sigma$-conjugates for $D = 64, 1$.

(c) For $p \geq 7$, $\bar{\rho}_{J^-,\mathfrak{p}}|_{I_{\mathfrak{q}_2}} = \bar{\theta}_2 \oplus \bar{\theta}_2^{-1}$ with $\bar{\theta}_2$ of order 5. If $\chi_0|_{I_{\mathfrak{q}_2}} \neq 1$, then $\mathfrak{f}(\chi_0|_{G_{\mathbb{Q}_4}}) \in \{2, 3\}$: $K(S_2, 2) = \langle -1, (1 + \sqrt{5})/2, 2\rangle$, and each of the seven nontrivial classes $\Delta$ gives $K(\sqrt{\Delta})/K$

ramified at $\mathfrak{q}_2$ with discriminant exponent 2 or 3 (item A5), and this exponent is the conductor exponent of the character. So $\mathfrak{f}(\bar\theta_2\chi_0)=\mathfrak{f}(\chi_0)\ge 2$, as $\bar\theta_2$ is tamely ramified, and the Serre conductor of $\bar\rho_{J^-,\mathfrak{p}}\otimes\chi_0$ at $\mathfrak{q}_2$ is at least $\mathfrak{q}_2^4$, which no newform of $\mathfrak{q}_2$-exponent at most 2 can match (the conductor of $\rho_{g,\mathfrak{B}}$ at $\mathfrak{q}_2$ is the $\mathfrak{q}_2$-exponent of the level of $g$, and reduction modulo $\mathfrak{B}$ does not raise the conductor exponent at $\mathfrak{q}_2\nmid p$). So $\chi_0$ is unramified at $\mathfrak{q}_2$, hence at every finite prime, hence trivial: $K$ has narrow class number 1. For the second statement, an isomorphism matches the traces of $\bar\rho(\gamma)$ ($\bar\rho(\gamma)$ has order 5, prime to $p$, so it is semisimple), and $P_1(\omega)-P_2(\omega)=\pm\sqrt{5}$ is not 0 modulo any prime above $p\ne 5$; apply (b). □

At a prime $\mathfrak{q}\nmid 10$ of $K$ where $J^-$ has good reduction we write $a_\mathfrak{q}(J^-)=\operatorname{tr}\rho_{J^-,\lambda}(\mathrm{Frob}_\mathfrak{q})\in\mathcal{O}_K$ ($\lambda\nmid q$), and likewise for $\mathcal{J}_D$; then $a_\mathfrak{q}(\mathcal{J}_D^\sigma)=\sigma(a_\mathfrak{q}(\mathcal{J}_D))$, and $a_{\sigma(\mathfrak{q})}=\sigma(a_\mathfrak{q})$ as the curves are defined over $\mathbb{Q}$.

**Lemma 4.2.** *Let $q\equiv 1\pmod 5$ be prime, $\mathfrak{q}\mid q$, $\bar\zeta\in\mathbb{F}_q$ of order 5 with $\omega\equiv\bar\zeta+\bar\zeta^{-1}\pmod{\mathfrak{q}}$, and $u_j\in\mathbb{F}_q^\times$ with $u_j^{(q-1)/5}=\bar\zeta^j$. Let $q\nmid AB$.*

*(a) If $q\nmid c$, let $\mathcal{D}\colon W^2=c^5X(X^{10}+\tau X^5+1)$ over $\mathbb{F}_q$, $\tau=-2(A-B)/c^5$, $[\bar\zeta](X,W)=(\bar\zeta X,\bar\zeta^3W)$, and $\nu_j=\#\{P\in\mathcal{D}(\overline{\mathbb{F}}_q):\mathrm{Frob}(P)=[\bar\zeta]^jP\}$. Then $a_\mathfrak{q}(J^-)=((\nu_2-\nu_0)+(\nu_2-\nu_1)\omega)/5$.*

*(b) If $q\mid c$, or for $\mathcal{J}_D$ with $q\nmid D$, let $\mu_j=q-\#\{(x,y)\in\mathbb{F}_q^2:y^2=u_jx^5+D\}$ with $D=-4A$ in the first case. Then $a_\mathfrak{q}=(2\mu_0+\omega(\mu_1+\mu_4)-(1+\omega)(\mu_2+\mu_3))/5$.*

*Proof.* (a) The curve $\mathcal{D}$ is a double cover of $C^-$ modulo $\mathfrak{q}$ with an automorphism $[\bar\zeta]$ of order 5 that lifts the real multiplication, so its point counts twisted by powers of $[\bar\zeta]$ separate the eigenspaces of $[\bar\zeta]$. The map $x=c(X+X^{-1})$, $y=W/X^3$ exhibits $C^-$ modulo $\mathfrak{q}$ as the quotient $\pi\colon\mathcal{D}\to C^-$ by $\upsilon(X,W)=(X^{-1},W/X^6)$, and $\omega$ acts as $\pi_*[\bar\zeta]\pi^*$ (it moves $c(X+X^{-1})$ to $c(\bar\zeta X+\bar\zeta^{-1}X^{-1})$). Over $\overline{\mathbb{Q}}_\ell$, $H^1(\mathcal{D})$ is the sum of the invariants $H^1_1$ of $[\bar\zeta]^*$ and of its eigenspaces $H^1_\xi$, $\xi\ne 1$, each of dimension 2; $\pi^*$ identifies $H^1(C^-)$ with $\{v+\upsilon^*v:v\in H^1_\xi\oplus H^1_{\xi^2}\}$, and $\omega$ acts on the image of $H^1_\xi$ by $\xi+\xi^{-1}$. Hence $\operatorname{tr}(\mathrm{Frob}^*|H^1_\xi)=\jmath_\xi(a_\mathfrak{q}(J^-))$, where $\jmath_\xi\colon K\to\overline{\mathbb{Q}}_\ell$ is the embedding with $\jmath_\xi(\omega)=\xi+\xi^{-1}$, and $H^1_\xi$, $H^1_{\xi^{-1}}$ give the same trace ($\upsilon$ exchanges them). The Lefschetz formula $q+1-\nu_j=\sum_\xi\xi^{-j}\operatorname{tr}(\mathrm{Frob}^*|H^1_\xi)$ for $[\bar\zeta]^{-j}\circ\mathrm{Frob}$ and Fourier inversion give, for $a_\mathfrak{q}(J^-)=s+t\omega$, $\nu_2-\nu_1=5t$ and $\nu_2-\nu_0=5s$. (b) The curve is $y^2=x^5+D$, with $\omega$ acting by $[\bar\zeta]+[\bar\zeta^{-1}]$. Its $H^1$ is the sum of lines $L_\xi$, $\xi\ne1$, on which $[\bar\zeta]^*$ acts by $\xi$; the fixed points of $[\bar\zeta]^{-j}\circ\mathrm{Frob}$ other than $\infty$ correspond to the affine points of $y^2=u_jx^5+D$ over $\mathbb{F}_q$, so $\mu_j=\sum_\xi\xi^{-j}\operatorname{tr}(\mathrm{Frob}^*|L_\xi)$, and $\jmath_\xi(a_\mathfrak{q})=\operatorname{tr}(\mathrm{Frob}^*|L_\xi)+\operatorname{tr}(\mathrm{Frob}^*|L_{\xi^{-1}})=\frac15\sum_j(\xi^j+\xi^{-j})\mu_j$, which is the formula ($P_2(\omega)=-1-\omega$). □

**Proposition 4.3.** *Let $(a,b,c)$ be a normalized solution with $2\nmid ab$, $5\nmid ab$, and $\mathfrak{p}\mid p$.*

*(a) If $p\ge 7$, $\bar\rho_{J^-,\mathfrak{p}}$ is isomorphic neither to $\bar\rho_{\mathcal{J}_{64}^\sigma,\mathfrak{p}}$ nor to $\bar\rho_{\mathcal{J}_1^\sigma,\mathfrak{p}}$.*

*(b) If $p\ge 11$, $\bar\rho_{J^-,\mathfrak{p}}\ncong\bar\rho_{f,\mathfrak{B}}$ for the newform $f=$ 2.2.5.1-2000.1-h [48] and every prime $\mathfrak{B}\mid p$ of its coefficient field.*

*Proof.* We use both primes above an auxiliary prime, as in [9, (9.5), Remark 9.12]. Let $q\equiv1\pmod5$, $q\nmid 10p$, $\mathfrak{q}\mid q$ and $\mathfrak{q}'=\sigma(\mathfrak{q})$. (a) Let $\bar\rho_{J^-,\mathfrak{p}}\cong\bar\rho_{\mathcal{A},\mathfrak{p}}$, $\mathcal{A}\in\{\mathcal{J}_{64}^\sigma,\mathcal{J}_1^\sigma\}$. If $q\nmid AB$, the traces at $\mathrm{Frob}_\mathfrak{q}$ and $\mathrm{Frob}_{\mathfrak{q}'}$ give $x=a_\mathfrak{q}(J^-)-a_\mathfrak{q}(\mathcal{A})\in\mathfrak{p}$ and $\sigma(x)\in\mathfrak{p}$, so $x\in\mathfrak{p}\cap\sigma(\mathfrak{p})=p\mathcal{O}_K$. If $q\mid AB$, $J^-$ has multiplicative reduction at $\mathfrak{q}$ and $\mathfrak{q}'$ [15, Lemma 7.5 and its proof], and

likewise $a_{\mathfrak{q}}(\mathcal{A})^2-(q+1)^2\in p\mathcal{O}_K$. Let $r=(A \bmod q, c \bmod q)$ be the residue of the solution; by Lemma 4.2 it determines $x$. Let $m_r$ be the content (the greatest common divisor of the coordinates in $\mathbb{Z}[\omega]$) of $x$ if $q\nmid AB$, and of $a_{\mathfrak{q}}(\mathcal{A})^2-(q+1)^2$ if $q\mid AB$. Then $p\mid m_r$, so $p$ divides $B_q=\operatorname{lcm}_r m_r$, the least common multiple over all residues $r$. Replacing $\mathfrak{q}$ by $\sigma(\mathfrak{q})$ replaces $x$, and $a_{\mathfrak{q}}(\mathcal{A})^2-(q+1)^2$, by their images under $\sigma$, which have the same contents, so $B_q$ does not depend on the choice of $\mathfrak{q}$. The values computed with Lemma 4.2 (item A8) are in Table 3. As $q\nmid 10p$ is needed, $q=11$ serves for $p\neq 11$, and $q=61$, 101 for $p=11$.

TABLE 3. The integers $B_q$ of Proposition 4.3(a).

| $q$ | form | $B_q$ | used for |
|---|---|---|---|
| 11 | $\mathcal{J}_{64}^{\sigma}$ | $90=2\cdot 3^2\cdot 5$ | $p\geq 7$, $p\neq 11$ |
| 11 | $\mathcal{J}_{1}^{\sigma}$ | $240=2^4\cdot 3\cdot 5$ | $p\geq 7$, $p\neq 11$ |
| 61 | $\mathcal{J}_{64}^{\sigma}$ | $24360=2^3\cdot 3\cdot 5\cdot 7\cdot 29$ | $p=11$ |
| 101 | $\mathcal{J}_{1}^{\sigma}$ | $20160=2^6\cdot 3^2\cdot 5\cdot 7$ | $p=11$ |

(b) The coefficient field $K_f$ of $f$ has degree 4 and contains $K$. An isomorphism gives an embedding $\jmath\colon K\to K_f$ with $a_{\mathfrak{q}}(f)-\jmath(a_{\mathfrak{q}}(J^-))$, $a_{\mathfrak{q}'}(f)-\jmath(\sigma(a_{\mathfrak{q}}(J^-)))\in\mathfrak{B}$ if $q\nmid AB$, and $a_{\mathfrak{q}}(f)\mp(q+1)$, $a_{\mathfrak{q}'}(f)\mp(q+1)\in\mathfrak{B}$, with independent signs, if $q\mid AB$; so $p$ divides the norm of the ideal of $\mathcal{O}_{K_f}$ generated by these two elements, for one $\jmath$ and the residue of the solution. Table 4 gives the eigenvalues of $f$ at the primes above 11 and 31. They are those of the LMFDB, which names each prime by a generator; the Brandt module of item A10 confirms this matching of primes and eigenvalues (item A9). The other identification of the LMFDB's $w$, namely $w=-\omega$ instead of $w=\omega+1$, exchanges the two primes above each $q$, which amounts to replacing $\jmath$ by $\jmath\circ\sigma$, and the condition above is tested for both embeddings. As these four eigenvalues lie in $\jmath_0(K)$, with $a_{\sigma(\mathfrak{q})}(f)=\jmath_0(\sigma(\alpha))$ when $a_{\mathfrak{q}}(f)=\jmath_0(\alpha)$, the two elements of this condition lie in $\jmath_0(\mathcal{O}_K)$ for both $\jmath$, and the primes $p$ can be read off in $\mathcal{O}_K$.

TABLE 4. Hecke eigenvalues of $f=$ 2.2.5.1-2000.1-h [48] at the primes above 11 and 31. The LMFDB writes $K=\mathbb{Q}(w)$ with $w^2=w+1$; we take $w=\omega+1=(1+\sqrt{5})/2$, where $\sqrt{5}=2\omega+1$. The coefficient field is $K_f=\mathbb{Q}(e)$ with $e^4-10e^3-13e^2+190e+241=0$; the element $\theta=-(4e^3-30e^2-36e+215)/91$ satisfies $\theta^2=5$, and $\jmath_0\colon K\to K_f$ is the embedding with $\jmath_0(\sqrt{5})=\theta$. (Also $K_f=\mathbb{Q}(\theta,\eta)=\mathbb{Q}(\sqrt{5},\sqrt{6})$ with $\eta=(2e-5+\theta)/4$, $\eta^2=6$.)

| LMFDB prime | $\mathfrak{q}$ | $\omega \bmod \mathfrak{q}$ | $a_{\mathfrak{q}}(f)$ in the LMFDB | $a_{\mathfrak{q}}(f)$ |
|---|---|---|---|---|
| $[11,11,-3w+2]$ | $(3\omega+1)$ | 7 | $(-2e^3+15e^2+18e+120)/91$ | $(5+\theta)/2=\jmath_0(3+\omega)$ |
| $[11,11,-3w+1]$ | $(3\omega+2)$ | 3 | $(2e^3-15e^2-18e+335)/91$ | $(5-\theta)/2=\jmath_0(2-\omega)$ |
| $[31,31,-5w+2]$ | $(5\omega+3)$ | 18 | $(2e^3-15e^2-18e+426)/91$ | $(7-\theta)/2=\jmath_0(3-\omega)$ |
| $[31,31,-5w+3]$ | $(5\omega+2)$ | 12 | $(-2e^3+15e^2+18e+211)/91$ | $(7+\theta)/2=\jmath_0(4+\omega)$ |

With the Hecke eigenvalues of $f$ (item A10), the primes that occur, over all residues and both $\jmath$, are $\{2,3,5,7\}$ at $q=11$ and $\{2,3,5,13\}$ at $q=31$ (item A9). For $p=11$ we use $q=31$. □

## 5. The case $ab \equiv \pm 2 \pmod 5$

When $\varepsilon = 3$ the Kummer class of the Weierstrass field of $C^-$ lies off the $\mathbb{F}_5$-line of the curves $H_D$ (Proposition 3.4(d)), so inertia at $\mathfrak{q}_5$ separates $J^-$ from every form with complex multiplication by $\mathbb{Q}(\zeta_5)$ and exponent 3 at $\mathfrak{q}_5$. When $\varepsilon = 2$ a Frobenius trace over a tamely ramified extension of $F$ does the same.

**Proposition 5.1.** *Let $p \geq 7$, $(a,b,c)$ a solution with $5 \nmid ab$, $\left(\frac{ab}{5}\right) = -1$, $\varepsilon = 3$, $g$ a newform with complex multiplication by $\mathbb{Q}(\zeta_5)$ and exponent 3 at $\mathfrak{q}_5$, $\mathfrak{p}, \mathfrak{B} \mid p$, and $\chi$ a finite-order character of $G_K$ unramified at $\mathfrak{q}_5$. Then $(\bar\rho_{J^-,\mathfrak{p}} \otimes \bar\chi)|_{I_F}$ and $\bar\rho_{g,\mathfrak{B}}|_{I_F}$ are not isomorphic over any common extension of their residue fields.*

*Proof.* $\chi$ is trivial on $I_F$. By Lemmas 3.1 and 3.6 both residual kernels on $I_F$ equal the $\lambda$-adic ones (for $g$ as $|\rho_{g,\mathfrak{B}}(I_F)|$ divides 40, which is prime to $p$, and the kernel of reduction is pro-$p$), with fixed fields $L_{J^-} \supseteq F^{\mathrm{ur}}(W)$ and $L_g \supseteq N_0$, and the 5-part of $[L_{J^-} : F^{\mathrm{ur}}]$ is at most 5. An isomorphism gives $L_{J^-} = L_g \supseteq \mathcal{M}(\beta^{1/5})N_0$, of degree 25 over $\mathcal{M}$ by Proposition 3.4(d): a contradiction. □

**Proposition 5.2.** *Let $(a,b,c)$ be a solution with $5 \nmid ab$ and $\varepsilon = 2$, and $L = \mathbb{Q}_5(\pi)$, $\pi^8 = 5$; then $F = \mathbb{Q}_5(\pi^4)$ and $L/F$ is cyclic, totally ramified of degree 4.*

- *(a) $C^-$ has good reduction over $L$, with special fiber $y^2 = x^5 + (ab)^2 x$ over $\mathbb{F}_5$.*
- *(b) For $\lambda \nmid 5$ and any Frobenius element $\mathrm{Frob}_L \in G_L$, $\operatorname{tr}\rho_{J^-,\lambda}(\mathrm{Frob}_L)$ is 0 if $\left(\frac{ab}{5}\right) = +1$ and $\pm 2\sqrt{5}$ if $\left(\frac{ab}{5}\right) = -1$.*
- *(c) $\operatorname{tr}\rho_{g,\mathfrak{B}}(\mathrm{Frob}_L) = 0$ if $g$ has complex multiplication by $\mathbb{Q}(\zeta_5)$ and $\mathfrak{B} \nmid 5$.*
- *(d) If $\left(\frac{ab}{5}\right) = -1$, $p \nmid 10$, $\mathfrak{p}, \mathfrak{B} \mid p$ and $\chi$ has finite order, then $\bar\rho_{J^-,\mathfrak{p}} \otimes \bar\chi \ncong \bar\rho_{g,\mathfrak{B}}$ on $G_L$ for every such $g$.*

*Proof.* (a) As $\varepsilon = 2$, $v_5(d) \geq 2$ by (CK2); apply Lemma 3.3.

(b) $\mathrm{Frob}_L$ acts on $V_\ell(J^-)$ as Frobenius on the Jacobian of the special fiber [43, §2]. The curves $y^2 = x^5 \pm x$ have 6 points over $\mathbb{F}_5$; over $\mathbb{F}_{25}$, $y^2 = x^5 + x$ has 46 points and $y^2 = x^5 - x$ has 6, so their Frobenius polynomials are $(x^2+5)^2$ and $(x^2-5)^2$. The two eigenvalues on $V_\lambda$ are roots of the Frobenius polynomial of the special fiber with product 5 (cyclotomic determinant, [15, Lemma 6.3]): $\pm i\sqrt{5}$ if $(ab)^2 \equiv 1$, and $\sqrt{5}, \sqrt{5}$ or $-\sqrt{5}, -\sqrt{5}$ if $(ab)^2 \equiv -1$.

(c) $(1-\zeta)^4 = -5u$ with $u$ a unit congruent to 1 modulo $1-\zeta$, hence a fourth power, so $F' = \mathbb{Q}_5((-5)^{1/4})$ and $LF' = L(\zeta_8)$ is unramified quadratic over $L$. So $\mathrm{Frob}_L \notin G_{F'}$; apply Lemma 3.6(a).

(d) Comparing traces at $\mathrm{Frob}_L$ gives $\bar\chi(\mathrm{Frob}_L)(\pm 2\sqrt{5}) \equiv 0$ modulo a prime above $p$, but $(2\sqrt{5})^2 = 20$. □

**Theorem 5.3.** *Let $p \geq 11$ be a prime. Then $x^p + y^p = z^5$ has no solution $(a,b,c)$ in coprime integers with $abc \neq 0$ and $ab \equiv \pm 2 \pmod 5$.*

*Proof.* Here $5 \nmid ab$ and $\left(\frac{ab}{5}\right) = -1$. If $2 \mid ab$, apply (CK1). Otherwise $a$ and $b$ are odd, so $2 \mid c$ and $a + b \equiv a^p + b^p = c^5 \equiv 0 \pmod 4$; exchanging $a$ and $b$ if necessary, which keeps $ab$, we may assume $a \equiv -1 \pmod 4$, as in Section 2. By (CK3), (CK4) and $p \notin \{2,3,5,7\}$, $\bar\rho_{J^-,\mathfrak{p}} \otimes \chi_0 \cong \bar\rho_{g,\mathfrak{B}}$ with $g \in \{g_4, g_{16}, g_{64}\}$ if $\varepsilon = 3$ and $g = g_1$ if $\varepsilon = 2$, or $p = 19$ and $g$ is the form of Remark 5.4. Proposition 5.1 with $\chi = \chi_0$, resp. Proposition 5.2(d), excludes the first case, and Remark 5.4 the second. □

*Remark* 5.4. For $p = 19$ the trace comparison of [15, §10] leaves, besides $g_1, g_4, g_{16}, g_{64}$, the newform 2.2.5.1-2000.1-h [48], without complex multiplication, of level $\mathfrak{q}_2^2\mathfrak{q}_5^3$ (items A1

and A10). By Proposition 4.1(c) the twist is then $\chi_0 = 1$, and Proposition 4.3(b), which compares the traces themselves at both primes above 11, excludes it. For $p = 7$, the elimination of [15, §9.3] at level $\mathfrak{q}_2\mathfrak{q}_5^{\varepsilon}$ fails, but $x^7 + y^7 = z^5$ is solved by Dahmen and Siksek [20]. The proof follows [15, §9.3] in keeping $\mathfrak{q}_2$ in the level; lowering to the Serre level instead adds only the levels $\mathfrak{q}_5^2$, with no newform [15, §9.2], and $\mathfrak{q}_5^3$, whose only newform orbit in the LMFDB, 2.2.5.1-125.1-a [48], has complex multiplication by $\mathbb{Q}(\zeta_5)$ and is covered by Proposition 5.1.

## 6. The case $ab \equiv \pm 1 \pmod 5$

Here $J^-$ and one of the Jacobians $\mathcal{J}_D$, $\mathcal{J}_D^\sigma$ have the same restriction to $G_F$ up to an unramified quadratic character (Proposition 6.1), so inertia at $\mathfrak{q}_5$ alone cannot separate them. With the place 2 (Proposition 4.1) and the auxiliary primes (Proposition 4.3), a Frobenius trace over a totally ramified extension of $F$ (Proposition 6.3) leaves the class $ab \equiv -1 \pmod 5$ and the two forms $g_4$, $g_{16}$, which come from trivial solutions (Proposition 6.9).

**Proposition 6.1.** *Let $(a, b, c)$ be a solution with $5 \nmid ab$ and $\left(\frac{ab}{5}\right) = +1$ (this includes $5 \mid c$), and $\lambda \nmid 5$.*

*(a) Let $\varepsilon = 3$, $D \in \{4, 16, 64\}$. Then $\rho_{J^-,\lambda}(I_F)$ and $\rho_{\mathcal{J}_D,\lambda}(I_F)$ are binary dihedral of order 20 with the same fixed field. Exactly one $\mathcal{A} \in \{\mathcal{J}_D, \mathcal{J}_D^\sigma\}$ has $\rho_{\mathcal{A},\lambda}|_{I_F} \cong \rho_{J^-,\lambda}|_{I_F}$, and then $\rho_{J^-,\lambda}|_{G_F} \cong \rho_{\mathcal{A},\lambda}|_{G_F} \otimes \mu$ with $\mu$ unramified, $\mu^2 = 1$. For $p \geq 7$, $\bar\rho_{J^-,\mathfrak{p}}|_{I_F}$ is isomorphic to $\bar\rho_{\mathcal{A},\mathfrak{p}}|_{I_F}$ and not to the restriction of the other element of $\{\bar\rho_{\mathcal{J}_D,\mathfrak{p}}, \bar\rho_{\mathcal{J}_D^\sigma,\mathfrak{p}}\}$.*

*(b) Let $\varepsilon = 2$. Then $\rho_{J^-,\lambda}|_{G_F} \cong \rho_{\mathcal{J}_1,\lambda}|_{G_F} \otimes \mu$ with $\mu$ unramified, $\mu^2 = 1$.*

*So for $p \geq 7$ and every $\chi_0 \in K(S_2, 2)^*$, $(\bar\rho_{J^-,\mathfrak{p}} \otimes \chi_0)|_{G_F}$ is the restriction of $\bar\rho_{\mathcal{A},\mathfrak{p}}$, resp. $\bar\rho_{\mathcal{J}_1,\mathfrak{p}}$, twisted by an unramified character of order at most 2.*

*Proof.* (a) By Proposition 3.4(c),(e), $\mathcal{M}F^{\mathrm{ur}}(W) = \mathcal{M}F^{\mathrm{ur}}(W_D) = N_0$. A lift of the generator of $\mathrm{Gal}(\mathcal{M}/F^{\mathrm{ur}})$ inverts $\zeta$, so $\mathrm{Gal}(N_0/F^{\mathrm{ur}}) \cong D_5$, which has no normal subgroup of order 2; so $F^{\mathrm{ur}}(W) = F^{\mathrm{ur}}(W_D) = N_0$. For $\mathcal{B} \in \{J^-, \mathcal{J}_D\}$ let $G_{\mathcal{B}} = \mathrm{Gal}(L_{\mathcal{B}}/F^{\mathrm{ur}})$. Elements fixing $N_0$ fix the six Weierstrass points of the special fiber, so act as 1 or $\iota$ (proof of Lemma 3.1); hence $[L_{\mathcal{B}} : N_0] \leq 2$. As $G_{\mathcal{B}} \subset \mathrm{SL}_2$ has $-1$ as its only involution and $D_5$ has five, $[L_{\mathcal{B}} : N_0] = 2$ and $G_{\mathcal{B}}/\{\pm 1\} \cong D_5$. The rotations lift to a cyclic group $\langle \mathsf{r} \rangle$ of order 10, and a lift $\mathsf{s}$ of a reflection has $\mathsf{s}^2 = -1 = \mathsf{r}^5$ and $\mathsf{srs}^{-1} = \mathsf{r}^{-1}$ (the only element of order 10 in $\{\pm \mathsf{r}^{-1}\}$): $G_{\mathcal{B}} \cong \mathrm{Dic}_5$. As $N_0$ has a unique quadratic extension (its residue field is algebraically closed of odd characteristic), $L_{J^-} = L_{\mathcal{J}_D}$, with group $G \cong \mathrm{Dic}_5$ acting faithfully in both.

$\mathrm{Dic}_5 = \langle \mathsf{r}, \mathsf{s} \mid \mathsf{r}^{10} = 1, \mathsf{s}^2 = \mathsf{r}^5, \mathsf{srs}^{-1} = \mathsf{r}^{-1} \rangle$ has two faithful irreducible characters of degree 2, induced from $\mathsf{r} \mapsto \zeta_{10}^j$, $j = 1, 3$, with values $\zeta + \zeta^{-1} = (-1 + \sqrt{5})/2$ and $\zeta^2 + \zeta^{-2} = (-1 - \sqrt{5})/2$ at $\mathsf{r}^2$, exchanged by $\sigma$. The characters of $\rho_{J^-,\lambda}|_{I_F}$ and $\rho_{\mathcal{J}_D,\lambda}|_{I_F}$ are $K$-valued, independent of $\lambda$ (Lemma 3.1(a)) and faithful, and that of $\mathcal{J}_D^\sigma$ is the $\sigma$-conjugate of that of $\mathcal{J}_D$; this gives $\mathcal{A}$. For $p \geq 7$ the two values at $\mathsf{r}^2$ differ by $\pm\sqrt{5} \not\equiv 0$ modulo $\mathfrak{p}$, and the image has order prime to $p$, which gives the residual statement. As $\rho_{J^-,\lambda}|_{I_F}$ is irreducible, $\mathrm{Hom}_{I_F}(\rho_{\mathcal{A},\lambda}, \rho_{J^-,\lambda})$ is a line on which $G_F$ acts through an unramified character $\mu$; so $\rho_{J^-,\lambda}|_{G_F} \cong \rho_{\mathcal{A},\lambda}|_{G_F} \otimes \mu$, and the cyclotomic determinants give $\mu^2 = 1$.

(b) Here $u = (ab)^2 \equiv 1$, so $C^-$ and $H_1$ (with $x = -1 + \pi^2 X$, $y = \pi^5 Y$) both reduce over $L$ to $Y^2 = X^5 + X$. An element $\gamma \in I_F$ mapping to $\pi \mapsto i\pi$ in $\mathrm{Gal}(L/F)$ acts on both fibers by $(X, Y) \mapsto (-X, iY)$, whose square is the hyperelliptic involution $\iota$. So for $\mathcal{B} \in \{J^-, \mathcal{J}_1\}$, $\rho_{\mathcal{B},\lambda}(\gamma)$ has determinant 1 and square $-1$: $\rho_{\mathcal{B},\lambda}|_{I_F} = \chi \oplus \chi^{-1}$, $\chi \colon I_F \to \mathrm{Gal}(LF^{\mathrm{ur}}/F^{\mathrm{ur}}) \to \mu_4$, $\gamma \mapsto i$, and as $\chi^5 = \chi$, $\rho_{\mathcal{B},\lambda}|_{G_F} = \mu_1^{\mathcal{B}} \oplus \mu_2^{\mathcal{B}}$ over $\overline{K}_\lambda$ with $\mu_1^{\mathcal{B}}|_{I_F} = \chi$. The unramified

$\nu=\mu_1^{J^-}/\mu_1^{\mathcal{J}_1}$ has $\nu(\mathrm{Frob}_F)=\nu(\mathrm{Frob}_L)=\pm1$, both Frobenius polynomials over $L$ being $x^2+5$ by Proposition 5.2(b), whose proof applies to $\mathcal{J}_1$, which has the same special fiber; the determinants give $\mu_2^{J^-}=\mu_2^{\mathcal{J}_1}\nu$.

For $p\ge7$, take $\lambda=\mathfrak{p}$ and reduce. The relations above hold for the $\bar\rho_{\mathcal{B},\mathfrak{p}}|_{G_F}$ by Brauer–Nesbitt, as these are semisimple. In (a) they are irreducible on $I_F$, whose image $\mathrm{Dic}_5$ has order prime to $p$. In (b) $I_F$ acts through $\mu_4$ and $p\nmid4$, so every stable lattice, after adjoining $i$, is the sum of its $\chi$- and $\chi^{-1}$-lines. Finally, $\chi_0|_{G_F}$ is unramified of order at most 2 (Section 2), which gives the last assertion. □

*Remark* 6.2. By (CK4), $g_D$ has the representations of $\mathcal{J}_D$ or $\mathcal{J}_D^\sigma$. So for $(\frac{ab}{5})=+1$ the two sides of $\bar\rho_{J^-,\mathfrak{p}}\otimes\chi_0\cong\bar\rho_{g_D,\mathfrak{P}}$ agree on $G_F$ up to the unramified character $\mu\cdot\chi_0|_{G_F}$. Every invariant unchanged by such a twist (the inertia field, the inertial type, the conductor) takes the same value on both, and so do the squared traces compared in [15], which ignore every quadratic twist. A test at $\sqrt5$ needs $\mu$ and $\chi_0$, which are left undetermined in [15]. The place 2 fixes $\chi_0=1$ (Proposition 4.1), and Proposition 6.3 compares Frobenius traces over a totally ramified extension of $F$.

For $(\frac{ab}{5})=+1$, $\delta$ in Proposition 3.4(a) lies in $\mathbb{Z}_5$ ($-AB$ is a square modulo 5); write $\bar\delta=\delta \bmod 5$, $\bar D=D \bmod 5$, and $T_e\colon X\mapsto X+e$ for $e\in\mathbb{F}_5$.

**Proposition 6.3.** *Let $(a,b,c)$ be a solution with $5\nmid abc$, $(\frac{ab}{5})=+1$ and $\varepsilon=3$, and $D\in\{4,16,64\}$. Let $L_1=\mathbb{Q}_5(\varpi,6^{1/5})$, $\varpi^8=-5$, totally ramified of degree 20 over $F$ and containing $F'$ ([15, Proposition 7.23(ii)] gives such an extension for each class of $a,b,c$ modulo 25). Over $L_1$, $J^-$ and $\mathcal{J}_D$ have good reduction, the special fibers are the same curve $Y^2=h(X^5-X)$ over $\mathbb{F}_5$ ($h\in\mathbb{F}_5^\times$ the same for both), and $\omega$ reduces to $T_e+T_e^{-1}$, with $e=\bar\delta$ for $J^-$ and $e=\bar D$ for $\mathcal{J}_D$. Consequently the traces in $K$ of a Frobenius element of $G_{L_1}$ are $t_{J^-}=(\frac{\bar\delta\bar D}{5})t_{\mathcal{J}_D}$ with $t_{\mathcal{J}_D}=\pm2\sqrt5\ne0$. Since $(\frac45)=(\frac{16}{5})=(\frac{64}{5})=1$, for $p\ne2,5$ an isomorphism $\bar\rho_{J^-,\mathfrak{p}}\cong\bar\rho_{\mathcal{J}_D,\mathfrak{p}}$ needs $(\frac{\bar\delta}{5})=+1$, that is $ab\equiv-1 \pmod5$, and an isomorphism $\bar\rho_{J^-,\mathfrak{p}}\cong\bar\rho_{\mathcal{J}_D^\sigma,\mathfrak{p}}$ needs $ab\equiv+1 \pmod5$.*

*Proof. The field.* Let $j=\kappa(\beta)\in\mathbb{F}_5^\times$ (Proposition 3.4(b)). Then $u=\beta/6^j\in\mathbb{Z}_5^\times$ has $\kappa(u)=0$, so $u$ is a root of unity of order dividing 4 times an element of $1+25\mathbb{Z}_5=(1+5\mathbb{Z}_5)^5$, and $u\in\mathbb{Z}_5^{\times5}$; so $\beta$ has a fifth root $v\in L_1$, and likewise $-D$ ($\kappa(-D)\ne0$, Proposition 3.4(e)), giving $v_D\in L_1$. As $x^8+5$ and $(x+1)^5-6$ are Eisenstein, $L_1$ is totally ramified of degree 40 over $\mathbb{Q}_5$; it contains $\sqrt5=\varpi^4\sqrt{-1}$, and $\mathbb{Q}_5(\varpi^2)=\mathbb{Q}_5((-5)^{1/4})=F'$ (proof of Proposition 5.2(c)), so $\zeta\in L_1$.

*The model.* $\Lambda=1-\zeta$ has even valuation 10 in $L_1$; choose $\Theta\in L_1$ and $e_0\in\{1,2\}$ with $\Theta^2=e_0\Lambda$. With the roots $r_k=v\zeta^k+c^2v^{-1}\zeta^{-k}$ ($k\in\mathbb{Z}/5$) of $\Phi$ (Proposition 3.4(a)), $x=r_0+\Lambda X$ and $y=\Lambda^2\Theta Y$ turn $y^2=\Phi(x)$ into $e_0Y^2=\prod_k(X-X_k)$, $X_k=(r_k-r_0)/\Lambda=-(1+\zeta+\cdots+\zeta^{k-1})(v-c^2v^{-1}\zeta^{-k})$. So $X_k$ is integral, $\bar X_k=k\bar X_1$, and $\bar X_1=(\bar c^2-\bar v^2)/\bar v$. In $\mathbb{F}_5$, $\bar v=\bar v^5=\bar\beta$, $\bar c^2=\bar c^{10}=\bar\beta\bar\beta'$ ($\beta'=A-B-2\delta$, $\beta\beta'=c^{10}$) and $\bar\beta'-\bar\beta=-4\bar\delta=\bar\delta$, so $\bar X_1=\bar\delta\ne0$ ($\bar\delta^2=-\bar A\bar B$). The special fiber is $Y^2=h(X^5-\bar\delta^4X)=h(X^5-X)$ with $h=e_0^{-1}$, a smooth curve. For $\mathcal{J}_D$ the same substitution, with the same $\Lambda,\Theta$ and $r_0=v_D$, gives $X_k=-(1+\cdots+\zeta^{k-1})v_D$, $\bar X_1=-\bar v_D=\bar D$, and the same special fiber.

*The real multiplication.* The correspondence of Section 2 sends a point $(x,y)$ to the two points $(x',y)$ whose $x'$ satisfy $x'^2-\omega xx'+x^2+c^2(\omega^2-4)=0$. With $x=r_0+\Lambda X$ and $x'=r_0+\Lambda X'$ this equation, divided by $\Lambda^2$, reads

$$X^2+X'^2-\omega XX'+\frac{(2-\omega)r_0}{\Lambda}(X+X')+\frac{(2-\omega)r_0^2+c^2(\omega^2-4)}{\Lambda^2}=0.$$

Since $2-\omega = -\zeta^{-1}\Lambda^2$ and $\omega^2-4=(\omega-2)(\omega+2)$, the linear term vanishes modulo the maximal ideal, and the constant term is

$$\frac{(2-\omega)(r_0^2-c^2(\omega+2))}{\Lambda^2} = -\zeta^{-1}(r_0^2-c^2(\omega+2)) = X_1X_{-1},$$

as $r_0^2-c^2(\omega+2) = v^2-c^2\omega+c^4v^{-2} = (v-c^2\zeta/v)(v-c^2\zeta^{-1}/v) = -\zeta X_1X_{-1}$. It reduces to $\bar{X}_1\bar{X}_{-1} = -\bar{X}_1^2$, and $\bar{\omega}=2$. So the two image points of a point $P$ of $C^-$ with integral coordinates $(X,Y)$ are $(X',Y)$ with $X'$ a root of a monic quadratic with integral coefficients, hence integral, reducing to a root of $(\bar{X}-X')^2=\bar{X}_1^2$: they reduce to $T(\tilde{P})$ and $T^{-1}(\tilde{P})$, where $\tilde{P}$ is the reduction of $P$ and $T=T_{\bar{X}_1}$, an automorphism of $\tilde{C}\colon Y^2=h(X^5-X)$ with $T^2\neq 1$.

*The closure of the correspondence.* Let $\mathcal{C}$ be the smooth model over $\mathcal{O}_{L_1}$, $Z\subset C^-\times C^-$ the curve of the correspondence, which is symmetric and has bidegree $(2,2)$, and $\mathcal{Z}$ its closure in the product $\mathcal{C}\times_{\mathcal{O}_{L_1}}\mathcal{C}$. As this product is regular and $\mathcal{Z}$, the closure of a divisor of the generic fiber, has pure codimension 1, $\mathcal{Z}$ is a Cartier divisor; it is flat over $\mathcal{O}_{L_1}$, so its special fiber $\mathcal{Z}_s$ is an effective divisor on $\tilde{C}\times\tilde{C}$ (over $\overline{\mathbb{F}}_5$). We show that $\mathcal{Z}_s=\Gamma_T+\Gamma_{T^{-1}}$, where $\Gamma$ denotes a graph, so that the correspondence itself reduces to $T+T^{-1}$; the next paragraph shows this for $\omega$ directly. (i) Lift an affine point $\tilde{P}$ of $\tilde{C}$ to a point $P$ (Hensel's lemma). The closures in $\mathcal{C}\times_{\mathcal{O}_{L_1}}\mathcal{C}$ of the two points of $Z$ above $P$ lie in $\mathcal{Z}$ and meet the special fiber in $(\tilde{P},T\tilde{P})$ and $(\tilde{P},T^{-1}\tilde{P})$. As $\tilde{P}$ varies, these points are dense in $\Gamma_T$ and $\Gamma_{T^{-1}}$, which are distinct as $T^2\neq 1$; so $\mathcal{Z}_s=\Gamma_T+\Gamma_{T^{-1}}+R$ with $R$ effective. (ii) Let $\mathcal{P}$ be the section of $\mathcal{C}$ through the Weierstrass point $(r_0,0)$. The restrictions of $\mathcal{O}(\mathcal{Z})$ to $\mathcal{P}\times_{\mathcal{O}_{L_1}}\mathcal{C}$ and to $\mathcal{C}\times_{\mathcal{O}_{L_1}}\mathcal{P}$ are flat over $\mathcal{O}_{L_1}$, so each has the same Euler characteristic on both fibers [32, III, Theorem 9.9 and its proof], hence, by Riemann–Roch, the same degree. So $\mathcal{Z}_s$ has intersection number 2 with each of the two fibers through the reduction of $(r_0,0)$, as $Z$ has with $\{(r_0,0)\}\times C^-$ and with $C^-\times\{(r_0,0)\}$. As fibers over different points are algebraically equivalent, $\mathcal{Z}_s$ also has intersection number 2 with each fiber $\{\tilde{P}\}\times\tilde{C}$ and $\tilde{C}\times\{\tilde{P}\}$. (iii) Each graph meets each such fiber once, so $R$ meets both fiber classes trivially. Every prime divisor meets both fiber classes nonnegatively, and one that meets the fibers $\{\tilde{P}\}\times\tilde{C}$ trivially is one of them and meets $\tilde{C}\times\{\tilde{P}\}$ once. So $R=0$.

*The reduction of $\omega$.* The endomorphism $\omega$ extends to the abelian scheme $\mathrm{Pic}^0_{\mathcal{C}/\mathcal{O}_{L_1}}$ (Lemma 2.1(b)), and the extension commutes with reduction of points. For affine points $\tilde{P},\tilde{Q}$ of $\tilde{C}$ lifted to $P,Q$, with image points $P',P''$ and $Q',Q''$, the class $[P-Q]$ reduces to $[\tilde{P}-\tilde{Q}]$, and $\omega[P-Q]=[P'+P''-Q'-Q'']$ reduces to $[T\tilde{P}+T^{-1}\tilde{P}-T\tilde{Q}-T^{-1}\tilde{Q}]$ by the reduction of the image points above (the class of a divisor reduces to the class of its reduction, proof of Lemma 2.1(b)). The classes $[\tilde{P}-\tilde{Q}]$ generate $\mathrm{Jac}\,\tilde{C}(\overline{\mathbb{F}}_5)$, as every divisor class of degree 0 has a representative supported on the affine chart; so $\omega$ reduces to $T+T^{-1}$. The same holds for $\mathcal{J}_D$ with $T_{\bar{D}}$.

*The traces.* Let $\bar{C}\colon Y^2=h(X^5-X)$ over $\mathbb{F}_5$, $e\in\mathbb{F}_5^\times$ and $T=T_e$. Then $H^1(\bar{C})\otimes\overline{\mathbb{Q}}_\ell = \bigoplus_{i\in(\mathbb{Z}/5)^\times}L_i$ with $T^*=\xi^i$ on $L_i$, $\xi$ a primitive fifth root of unity (the quotient by $\langle T\rangle$ has genus 0, and the characteristic polynomial of $T^*$ is rational, so each primitive fifth root of unity occurs once). Frobenius commutes with $T^*$ and acts on $L_i$ by $\pi_i$. $\#\bar{C}(\mathbb{F}_5)=\#\bar{C}(\mathbb{F}_{25})=6$, so the Weil polynomial is $(x^2-5)^2$, all $\pi_i=\pm\sqrt{5}$ and $\sum\pi_i=0$; the Weil pairing pairs $L_i$ with $L_{-i}$, so $\pi_i\pi_{-i}=5$, $\pi_{-i}=\pi_i$, and $\pi_2=-\pi_1$. As $\omega$ acts by $T+T^{-1}$, on $L_{\pm i}$ by $\xi^i+\xi^{-i}$, the trace $t_e\in K$ is $2\pi_1$ under the embedding with $\omega\mapsto\xi+\xi^{-1}$ and $-2\pi_1$ under the other: $t_e=\pm2\sqrt{5}$. For $e'=je$, $T_{e'}=T^j$, so $t_{e'}=t_e$ if $j=\pm1$ and $t_{e'}=\sigma(t_e)=-t_e$ if $j=\pm2$: $t_{e'}=\left(\frac{j}{5}\right)t_e$.

*Conclusion.* $G_{L_1}$ acts on $V_\ell(J^-)$ and $V_\ell(\mathcal{J}_D)$ through the Frobenius of these special fibers [43, §2], compatibly with $K$. So for a Frobenius element of $G_{L_1}$, $t_{J^-}=t_{\bar\delta}=(\frac{\bar\delta\bar D}{5})t_{\bar D}=(\frac{\bar\delta\bar D}{5})t_{\mathcal{J}_D}$. An isomorphism $\bar\rho_{J^-,\mathfrak{p}}\cong\bar\rho_{\mathcal{J}_D,\mathfrak{p}}$ gives $t_{J^-}\equiv t_{\mathcal{J}_D}\pmod{\mathfrak{p}}$, and an isomorphism $\bar\rho_{J^-,\mathfrak{p}}\cong\bar\rho_{\mathcal{J}_D^\sigma,\mathfrak{p}}$ gives $t_{J^-}\equiv\sigma(t_{\mathcal{J}_D})=-t_{\mathcal{J}_D}\pmod{\mathfrak{p}}$. If the sign differs from $(\frac{\bar\delta\bar D}{5})$, then $2t_{\mathcal{J}_D}\in\mathfrak{p}$, so $p\mid \mathrm{N}(4\sqrt{5})=-80$. Finally $\bar\delta^2\equiv -AB\equiv -ab\pmod 5$ ($AB\equiv(ab)^p\equiv ab$ as $ab\equiv\pm1$) and $(\frac{\bar\delta}{5})\equiv\bar\delta^2$, so $(\frac{\bar\delta}{5})=+1$ if and only if $ab\equiv -1\pmod 5$. □

**Proposition 6.4.** *Let $(a,b,c)$ be a solution with $5\nmid abc$, $(\frac{ab}{5})=+1$ and $\varepsilon=3$, and $D\in\{4,16,64\}$. Then $\rho_{J^-,\lambda}|_{I_F}\cong\rho_{\mathcal{J}_D,\lambda}|_{I_F}$ compatibly with $K$, and, for $p\neq 2,5$, the same for the residual representations, if and only if $\kappa(\beta)\equiv\pm\kappa(-D)$; and with $\mathcal{J}_D^\sigma$ in place of $\mathcal{J}_D$ if and only if $\kappa(\beta)\equiv\pm2\kappa(-D)\pmod 5$.*

*Proof.* Let $\gamma\in I_{\mathcal{M}}$ fix $\Theta$ and move $6^{1/5}$ (it exists, as $\Theta^2\in\mathcal{M}$); so $\gamma(\zeta)=\zeta$, $\gamma(\Lambda)=\Lambda$, $\gamma(\Theta)=\Theta$ and $\gamma(6^{1/5})=\zeta^k6^{1/5}$, $k\neq 0$. With $v=(6^{1/5})^{\kappa(\beta)}w$ and $v_D=(6^{1/5})^{\kappa(-D)}w_D$, $w,w_D\in\mathbb{Z}_5^\times$ (proof of Proposition 6.3), $\gamma(v)=\zeta^m v$ and $\gamma(v_D)=\zeta^{m_D}v_D$ with $m=\kappa(\beta)k$, $m_D=\kappa(-D)k$. Then $\gamma(r_0)=r_m$, and on points $X(\gamma P)=\gamma(X(P))+X_m$, which reduces to $\bar X+m\bar X_1$; $\bar Y$ is fixed (this is the reduced descent datum of $\gamma$ in Lemma 2.1, with $E=F$ and $E'=L_1$, which is Galois over $F$). So $\gamma$ acts on the special fiber of $J^-$ as $T_{\bar\delta}^m$ and on that of $\mathcal{J}_D$ as $T_{\bar D}^{m_D}$. As $\omega$ acts by $T_{\bar\delta}+T_{\bar\delta}^{-1}$ on the first and by $T_{\bar D}+T_{\bar D}^{-1}$ on the second, the traces of $\gamma$ are $P_m(\omega)$ and $P_{m_D}(\omega)$. They are equal if and only if $m\equiv\pm m_D$, and $\sigma$-conjugate if and only if $m\equiv\pm2m_D$, and $m/m_D=\kappa(\beta)/\kappa(-D)$. By Proposition 6.1(a) and its proof, $\rho_{J^-,\lambda}|_{I_F}$ is isomorphic to exactly one of $\rho_{\mathcal{J}_D,\lambda}|_{I_F}$, $\rho_{\mathcal{J}_D^\sigma,\lambda}|_{I_F}$, the one with the same trace at $\gamma$. Residually the image of $I_F$ has order 20, prime to $p\neq 2,5$, and the two possible traces at $\gamma$ differ by $\pm\sqrt{5}\notin\mathfrak{p}$. □

**Lemma 6.5.** *In Proposition 6.4, let $\kappa(\beta)\equiv\pm\kappa(-D)$ and $(\frac{\bar\delta\bar D}{5})=+1$. Then $\alpha(X,Y)=(s_0X,\sqrt{s_0}Y)$, with $s_0=\kappa(-D)\bar D/(\kappa(\beta)\bar\delta)$, a square in $\mathbb{F}_5^\times$, is an automorphism of the common special fiber that intertwines the actions of $G_{\mathbb{Q}_5}$ and of $K$. So for $p\neq 2,5$ the $G_{\mathbb{Q}_5}$-isomorphism $J^-[p]\to\mathcal{J}_D[p]$, unique up to $\mathbb{F}_p^\times$, multiplies the Weil pairings by a square in $\mathbb{F}_p^\times$.*

*Proof.* The field $L_1$ is Galois over $F$, being the splitting field over $F$ of $(X^4-\varpi^4)(X^5-6)$ (as $\sqrt{-1}\in\mathbb{Q}_5$ and $\zeta\in L_1$), but not over $\mathbb{Q}_5$, as the conjugate $\zeta_8\varpi$ of $\varpi$ is not in $L_1$ ($\zeta_8$ generates the unramified quadratic extension of $\mathbb{Q}_5$, and $L_1$ is totally ramified). Let $L_1'=L_1(\zeta_8)=L_1(\sqrt{2})$, the Galois closure of $L_1$ over $\mathbb{Q}_5$, unramified of degree 2 over $L_1$, with residue field $\mathbb{F}_{25}$; over $\mathcal{O}_{L_1'}$ the models of the proof of Proposition 6.3 are still smooth, with the same special fiber $Y^2=h(X^5-X)$. For $g\in G_{\mathbb{Q}_5}$ let $g(\zeta)=\zeta^{r(g)}$ and $g(6^{1/5})=\zeta^{k_6(g)}6^{1/5}$. With $v,v_D$ as in the proof of Proposition 6.4, $g(r_0)=r_{\kappa(\beta)k_6(g)}$. From $x=r_0+\Lambda X$ and $y=\Lambda^2\Theta Y$,

$$X(gP)=\frac{g(\Lambda)}{\Lambda}\,g(X(P))+\frac{g(r_0)-r_0}{\Lambda},\qquad Y(gP)=\frac{g(\Lambda^2\Theta)}{\Lambda^2\Theta}\,g(Y(P)),$$

with $g(\Lambda)/\Lambda=1+\zeta+\cdots+\zeta^{r(g)-1}$ a unit congruent to $r(g)$, and $(g(r_0)-r_0)/\Lambda=X_{\kappa(\beta)k_6(g)}$ integral, reducing to $\kappa(\beta)k_6(g)\bar\delta$. As $(g(\Theta)/\Theta)^2=g(\Lambda)/\Lambda$, the factor $g(\Lambda^2\Theta)/(\Lambda^2\Theta)$ is a unit of $L_1'$, which lies in $L_1$ only if $r(g)=\pm1$ ($\pm2$ is not a square in $\mathbb{F}_5$); its reduction $\bar v_g\in\mathbb{F}_{25}^\times$ has $\bar v_g^2=r(g)$. So Lemma 2.1 applies with $E=\mathbb{Q}_5$ and $E'=L_1'$, and the reduced descent data are

$$\bar X\mapsto r(g)\bar g(\bar X)+\kappa(\beta)k_6(g)\bar\delta\ \text{ for } J^-,\qquad \bar X\mapsto r(g)\bar g(\bar X)+\kappa(-D)k_6(g)\bar D\ \text{ for } \mathcal{J}_D,$$

and $\bar{Y} \mapsto \bar{v}_g \bar{g}(\bar{Y})$ for both, with the same $\bar{v}_g$, since both models use $y = \Lambda^2 \Theta Y$ with the same $\Lambda$ and $\Theta$. Now $\alpha$ is an automorphism of $Y^2 = h(X^5 - X)$, $\alpha T_{\bar{\delta}} \alpha^{-1} = T_{s_0 \bar{\delta}} = T_{\pm \bar{D}}$, and $\alpha \circ g_{J^-} = g_{\mathcal{J}_D} \circ \alpha$ for every $g \in G_{\mathbb{Q}_5}$: the $X$-parts agree because $s_0 \kappa(\beta) \bar{\delta} = \kappa(-D) \bar{D}$ and $\bar{g}$ fixes $s_0$, and the $Y$-parts, both equal to $\sqrt{s_0}\, \bar{v}_g\, \bar{g}(\bar{Y})$, because $\bar{g}$ fixes $\sqrt{s_0} \in \mathbb{F}_5$. So $\alpha$ induces a $G_{\mathbb{Q}_5}$-isomorphism $J^-[p] \to \mathcal{J}_D[p]$ compatible with $K$; an automorphism of a curve preserves the principal polarization and reduction preserves Weil pairings, so its multiplier is 1. It is unique up to $\mathbb{F}_p^\times$: over $\overline{\mathbb{F}}_p$, $J^-[p] \otimes \overline{\mathbb{F}}_p \cong \mathrm{Ind}_{G_F}^{G_{\mathbb{Q}_5}} V$, where $V$ is irreducible already on $I_F$ (Proposition 6.1(a), the image having order prime to $p$) and not isomorphic on $I_F$ to its conjugate $V'$ (their traces at the element $\gamma$ of the proof of Proposition 6.4 differ by $\pm\sqrt{5}$, which is nonzero modulo $p$). So by Frobenius reciprocity

$$\mathrm{End}_{G_{\mathbb{Q}_5}}(J^-[p] \otimes \overline{\mathbb{F}}_p) = \mathrm{Hom}_{G_F}(V, V \oplus V') = \overline{\mathbb{F}}_p. \qquad \square$$

**Proposition 6.6.** *Let $p \geq 11$ be a prime with $p \equiv \pm 2 \pmod 5$, $(a, b, c)$ a normalized solution with $2 \nmid abc$, $abc \equiv -1 \pmod 5$ and $\varepsilon = 3$, and $D \in \{4, 16\}$ with $\kappa(\beta) \equiv \pm\kappa(-D)$ and $\bar{\rho}_{J^-,p} \cong \bar{\rho}_{\mathcal{J}_D,p}$ as $G_K$-modules over $\mathcal{O}_K/p$. Then $a \equiv -1 \pmod 8$.*

*Proof.* This is the symplectic argument of Halberstadt and Kraus [31], used by Freitas [24] for $x^3 + y^3 = z^p$, here for abelian surfaces at the places 2 and $\sqrt{5}$, over $\mathbb{Q}$.

*The descent.* Here $\mathcal{O}_K/p = \mathbb{F}_{p^2}$. Let $\vartheta \colon J^-[p] \to \mathcal{J}_D[p]$ be the $\mathbb{F}_{p^2}$-linear $G_K$-isomorphism. For $\tau \in G_{\mathbb{Q}} \smallsetminus G_K$, $\tau$ acts $\sigma$-semilinearly on both (the real multiplications are defined over $K$ and conjugated by $\tau$), so $\tau\vartheta\tau^{-1}$ is again an $\mathbb{F}_{p^2}$-linear $G_K$-isomorphism. The image of $I_F$ under $\bar{\rho}_{\mathcal{J}_D,p}$ is $\mathrm{Dic}_5$ (Proposition 6.1(a) and Lemma 3.1(c)), a nonabelian group of order prime to $p$, so $\bar{\rho}_{\mathcal{J}_D,p}$ is absolutely irreducible, and by Schur's lemma $\tau\vartheta\tau^{-1} = \xi_\tau \vartheta$ with $\xi_\tau \in \mathbb{F}_{p^2}^\times$. Applying this twice, as $\tau^2 \in G_K$, gives $\mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\xi_\tau) = 1$; by Hilbert's Theorem 90 some $\Psi = u\vartheta$, $u \in \mathbb{F}_{p^2}^\times$, is $G_{\mathbb{Q}}$-equivariant. The 4-dimensional $\mathbb{F}_p[G_{\mathbb{Q}}]$-module $J^-[p]$ is absolutely irreducible. Indeed, over $\overline{\mathbb{F}}_p$ it is $V_\jmath \oplus V_{\jmath'}$, one summand for each embedding $\jmath, \jmath'$ of $\mathcal{O}_K/p$ in $\overline{\mathbb{F}}_p$. These summands are irreducible and nonisomorphic for $G_K$, since their inertia characters at $\mathfrak{q}_2$ are $\bar{\theta}_2^{\pm 1}$ and $\bar{\theta}_2^{\pm 2}$ (Proposition 4.1(b)), and $\tau$ exchanges them. So $\Psi$ is unique up to $\mathbb{F}_p^\times$, and $\Psi^* e_{\mathcal{J}_D} = c_\Psi e_{J^-}$ for the $\mathbb{F}_p$-valued Weil pairings, with a well-defined class $[c_\Psi] \in \mathbb{F}_p^\times / \mathbb{F}_p^{\times 2}$.

*At 2.* Inertia at 2 acts on $w^2 + w = X^5$ by $X \mapsto \zeta X$, so on $J^-[p] \otimes \overline{\mathbb{F}}_p$ through the four distinct characters $\bar{\theta}_2^i$, $i \in (\mathbb{Z}/5)^\times$, which the Frobenius of $\mathbb{F}_2$ permutes transitively (it squares $\zeta$); so $J^-[p]$ is absolutely irreducible over $G_{\mathbb{Q}_2}$ and the $G_{\mathbb{Q}_2}$-intertwiners form a line over $\mathbb{F}_p$. Over $\mathbb{Q}_2$ the model of the proof of Proposition 4.1(a) identifies $J^-$ with $\mathrm{Jac}\, C_0^-$, $C_0^- \colon y^2 = x^5 - 4A$, as the two models have the same special fiber (and the same descent data for all of $G_{\mathbb{Q}_2}$: $w(gP) = g(w(P)) + (g(\varsigma) - \varsigma)/2$ for both), with multiplier 1. With $\varrho^5 = -A$ in $\mathbb{Z}_2^\times$, $C_0^-$ is the quadratic twist of $H_4$ by $-A$ over $\mathbb{Q}_2$: for $-A \equiv 1 \pmod 8$ it is $H_4$ itself (multiplier 1), for $-A \equiv 5 \pmod 8$ it gives $\mathcal{J}_4 \otimes \eta_2$, $\eta_2$ the unramified quadratic character of $\mathbb{Q}_2$.

*The twist by $\eta_2$.* A $G_{\mathbb{Q}_2}$-intertwiner $(\mathcal{J}_4 \otimes \eta_2)[p] \to \mathcal{J}_4[p]$ commutes with $G_{\mathbb{Q}_4}$, whose commutant on $\mathcal{J}_4[p]$ is $\mathcal{O}_K/p = \mathbb{F}_{p^2}$ (the two pieces have inertia characters $\bar{\theta}_2^{\pm 1}$ and $\bar{\theta}_2^{\pm 2}$, distinct as $p \neq 5$), so it is some $u \in \mathbb{F}_{p^2}$. For $\tau \in G_{\mathbb{Q}_2} \smallsetminus G_{\mathbb{Q}_4}$, $\eta_2(\tau) = -1$ and $\tau$ acts $\sigma$-semilinearly, so $u$ must satisfy $-u\tau = \tau u = \sigma(u)\tau$, and $u \in \sqrt{5}\, \mathbb{F}_p^\times$. Conversely, $u = \sqrt{5}$ gives such an intertwiner. Let $\mathcal{J}_4^{(5)}$ be the Jacobian of $5y^2 = x^5 + 4$, the quadratic twist of $H_4$ by 5, with $K$ acting through $[\zeta](x, y) = (\zeta x, y)$, and let $j_5 \colon \mathcal{J}_4^{(5)} \to \mathcal{J}_4$ be the isomorphism induced by $(x, y) \mapsto (x, \sqrt{5}\, y)$. It is defined over $\mathbb{Q}_4$, commutes with $K$ and preserves the

Weil pairings, and $\tau(j_5)=\iota\circ j_5=-j_5$, $\iota$ the hyperelliptic involution; so $j_5$ identifies $\mathcal{J}_4^{(5)}$ with $\mathcal{J}_4\otimes\eta_2$. As $\tau(\omega)=\sigma(\omega)=-1-\omega$, the endomorphism $\sqrt{5}=2\omega+1$ has $\tau(\sqrt{5})=-\sqrt{5}$, so $\sqrt{5}\circ j_5$ is defined over $\mathbb{Q}_2$. As $u=r\sqrt{5}$, $r\in\mathbb{F}_p^\times$, is fixed by the Rosati involution, $e(ux,uy)=e(x,u^2y)=5r^2e(x,y)$, so this intertwiner multiplies the Weil pairings by $5r^2$, of class [5].

*From $\mathcal{J}_{16}$ to $\mathcal{J}_4$.* Let Fr be the $\mathbb{F}_2$-Frobenius endomorphism of $w^2+w=X^5$ and of its Jacobian. Then $\mathrm{Fr}\circ[\bar\zeta]=[\bar\zeta^2]\circ\mathrm{Fr}$, so $\mathrm{Fr}^2$ carries $[\bar\zeta_\gamma^6]$, the action of an inertia element $\gamma$ on the special fiber of $\mathcal{J}_{16}$ (Proposition 4.1(b)), to $[\bar\zeta_\gamma^{24}]=[\bar\zeta_\gamma^4]$, its action on that of $\mathcal{J}_4$; and $\mathrm{Fr}^2$ commutes with the $\mathbb{F}_2$-Frobenius. So $\mathrm{Fr}^2$ gives a $G_{\mathbb{Q}_2}$-isomorphism $\mathcal{J}_{16}[p]\to\mathcal{J}_4[p]$. Since $\mathrm{Fr}^\dagger\mathrm{Fr}=2$, its multiplier is 4, a square.

As $A\equiv a \pmod 8$, together these give the class of $\Psi$ at 2: it is [5] if $a\equiv 3 \pmod 8$ and [1] if $a\equiv 7 \pmod 8$.

*At 5.* As $ab\equiv -1 \pmod 5$, $(\frac{\bar\delta}{5})=+1$ (proof of Proposition 6.3) and $(\frac{\bar D}{5})=1$, so $(\frac{\bar\delta\bar D}{5})=+1$, and Lemma 6.5 gives the class [1].

*Conclusion.* $\Psi$ is a $G_{\mathbb{Q}_2}$- and a $G_{\mathbb{Q}_5}$-intertwiner, so $[c_\Psi]$ is the class found at each place: $[5^{e_2}]=[1]$, with $e_2=1$ if and only if $a\equiv 3 \pmod 8$. As $(\frac{5}{p})=-1$, $a\equiv 7 \pmod 8$. □

Recall (Section 2) that a solution with $2\nmid ab$ is normalized if $a\equiv -1 \pmod 4$. Exchanging $a$ and $b$ reaches a normalized solution and changes neither $ab$ nor $\pm\kappa(\beta)$.

**Theorem 6.7.** *Let $p\geq 11$ be prime and $(a,b,c)$ a normalized solution of $x^p+y^p=z^5$ in coprime integers with $abc\neq 0$, $2\nmid ab$ and $5\nmid ab$. Then $ab\equiv -1 \pmod 5$, $\kappa(\beta)\neq 0$, and, for every prime $\mathfrak{p}$ of $K$ above $p$, either $\kappa(\beta)\equiv\pm\kappa(4) \pmod 5$ and $\bar\rho_{J^-,\mathfrak{p}}\cong\bar\rho_{\mathcal{J}_4,\mathfrak{p}}$, or $\kappa(\beta)\equiv\pm\kappa(16)$ and $\bar\rho_{J^-,\mathfrak{p}}\cong\bar\rho_{\mathcal{J}_{16},\mathfrak{p}}$. If $p\equiv\pm 2 \pmod 5$, also $a\equiv -1 \pmod 8$ in this normalization, that is $a\equiv\pm 1 \pmod 8$ for every solution with $2\nmid ab$ and $5\nmid ab$.*

*Proof.* By Theorem 5.3, $(\frac{ab}{5})=+1$. By (CK3), (CK4), $\bar\rho_{J^-,\mathfrak{p}}\otimes\chi_0\cong\bar\rho_{g,\mathfrak{B}}$ for a newform $g$ of level $\mathfrak{q}_2^s\mathfrak{q}_5^\varepsilon$, $s\in\{1,2\}$. By Proposition 4.1(c), $\chi_0=1$, and then $s=2$ by Proposition 4.1(a). By (CK4) and Remark 5.4, $g\in\{g_1,g_4,g_{16},g_{64}\}$, or $p=19$ and $g$ is 2.2.5.1-2000.1-h, which Proposition 4.3(b) excludes. As $g_D$ has the representations of $\mathcal{J}_D$ or $\mathcal{J}_D^\sigma$ (Remark 6.2), $\bar\rho_{J^-,\mathfrak{p}}\cong\bar\rho_{\mathcal{A},\mathfrak{p}}$ with $\mathcal{A}\in\{\mathcal{J}_D,\mathcal{J}_D^\sigma\}$; by Proposition 4.1(c), $\mathcal{A}$ is $\mathcal{J}_4$, $\mathcal{J}_{16}$, $\mathcal{J}_{64}^\sigma$ or $\mathcal{J}_1^\sigma$, and Proposition 4.3(a) excludes the last two. So $\mathcal{A}=\mathcal{J}_D$ with $D\in\{4,16\}$, of exponent 3 at $\mathfrak{q}_5$; so $\varepsilon=3$ and $\kappa(\beta)\neq 0$ (Proposition 3.4(b)). Proposition 6.3 gives $ab\equiv -1 \pmod 5$, and Proposition 6.4 gives $\kappa(\beta)\equiv\pm\kappa(-D)=\pm\kappa(D)$. For $p\equiv\pm 2 \pmod 5$, Proposition 6.6 gives $a\equiv -1 \pmod 8$. Since $2\mid c$, $v_2(a+b)=5v_2(c)\geq 5$ (the cofactor $(a^p+b^p)/(a+b)$ is a sum of $p$ odd terms), so $b\equiv -a \pmod{32}$; a solution with $a\equiv 1 \pmod 4$ is normalized by exchanging $a$ and $b$, so in general $a\equiv\pm 1 \pmod 8$. □

**Corollary 6.8.** *Let $p\geq 11$ be prime. Every solution $(a,b,c)$ of $x^p+y^p=z^5$ in coprime integers with $abc\neq 0$ has $10\mid ab$, or $2\nmid ab$ and $ab\equiv -1 \pmod 5$.*

*Proof.* (CK1) excludes $2\nmid ab$, $5\mid ab$ and $2\mid ab$, $5\nmid ab$. If $2\nmid ab$ and $5\nmid ab$, apply Theorem 6.7 to the normalized solution obtained by exchanging $a$ and $b$ if necessary. □

Let $q\nmid 10p$ be prime. A *test at the auxiliary prime $q$* removes a form $g$ if no residue $(A \bmod q, c \bmod q)$ with $A$ and $c^5-A$ congruent to $p$-th powers is compatible with the traces of $g$ at the primes above $q$, as in the proof of Proposition 4.3. Kraus [36, Théorème 3.1] uses such tests at primes $q\equiv 1 \pmod p$; here they are adapted to $J^-$ over $K$. The forms $g_4$ and $g_{16}$ left by Theorem 6.7 pass every such test, because they come from trivial solutions [15, Theorem 1.2, §10]:

**Proposition 6.9.** *Let $p \neq 5$ be an odd prime and $k \geq 0$. The trivial solution $(-2^k, 2^k, 0)$ (not coprime if $k > 0$) has Frey curve $C^-\colon y^2 = x^5 + 2^{kp+2}$, isomorphic over $\mathbb{Q}$, compatibly with $(x, y) \mapsto (\zeta x, y)$, to $H_{2^j}$, where $j \in \{0, 1, \dots, 9\}$ and $j \equiv kp + 2 \pmod{10}$; for instance to $H_4$, $H_{16}$, $H_{64}$, $H_1$ when $kp \equiv 0, 2, 4, 8 \pmod{10}$ respectively. Hence at every auxiliary prime $q \nmid 10p$ the residue $(A, 0)$ of this trivial solution, $A \equiv -2^{kp} \pmod{q}$, has $A$ and $c^5 - A$ congruent to $p$-th powers, namely to $(-2^k)^p$ and $(2^k)^p$. Moreover $-A$ is a 10th power modulo $q$ if $kp \equiv 0 \pmod{10}$, and $-A/4$ is one if $kp \equiv 2 \pmod{10}$, so this residue is compatible with the traces of $g_4$ at the primes above $q$ in the first case, and with those of $g_{16}$ in the second: no test at an auxiliary prime, Kraus's included, can remove $g_4$ or $g_{16}$.*

*Proof.* Here $A = -2^{kp}$, $B = 2^{kp}$, $c = 0$, so $\Phi(x) = x^5 + 2^{kp+2}$. With $j$ as in the statement and $D = 2^j$, $2^{kp+2}/D = w^{10}$ with $w = 2^{(kp+2-j)/10} \in \mathbb{Z}$, and $(x, y) \mapsto (w^2 x, w^5 y)$ is an isomorphism from $H_D$ to $C^-$ commuting with $(x, y) \mapsto (\zeta x, y)$. Let $D = 4$ or 16, and choose $k$ with $kp \equiv 0$ or $2 \pmod{10}$ accordingly (possible as $\gcd(p, 10) = 1$); then $-4A/D = 2^{kp+2}/D$ is a 10th power. At $q \nmid 10p$ the residue $(A, 0)$, $A \equiv -2^{kp}$, has $A$ and $c^5 - A$ congruent to $p$-th powers, and its curve $y^2 = x^5 - 4A$ is isomorphic over $\mathbb{F}_q$ to $H_D$, compatibly with $[\zeta]$; so its traces at the primes above $q$ are those of $\mathcal{J}_D$, that is of $g_D$ (Proposition 4.1(c)). □

## 7. The exponent $p = 11$

For $p = 11$, Corollary 6.8 leaves two classes of solutions: $10 \mid ab$, where $\bar{\rho}_{J^-,\mathfrak{p}}$ is reducible (Lemma 7.2), and $2 \nmid ab$, $ab \equiv -1 \pmod{5}$, where $\bar{\rho}_{J^-,\mathfrak{p}} \cong \bar{\rho}_{\mathcal{J}_D,\mathfrak{p}}$ with $D \in \{4, 16\}$ for the normalized solution (Theorem 6.7). So $J^-[\mathfrak{p}]$ has a line stable under $G_K$ in the first class, and, as $11 \equiv 1 \pmod{5}$, a line stable under $G_{\mathbb{Q}(\zeta_5)}$ in the second (Proposition 8.2(a)). Such a line is a point of the curve $X_0(\mathfrak{p})$ that parametrizes the lines in the $\mathfrak{p}$-torsion of Darmon's family of Jacobians over the $t$-line, and this point lies over the Frey parameter $t = a^p/c^5$ of the solution, a rational number. We show that for $\mathfrak{p} \mid 11$ the quotient of $X_0(\mathfrak{p})$ by the involution over $t \mapsto 1 - t$ is an elliptic curve $E$ over $K$ of rank 1, and that its points over $K$ and over $\mathbb{Q}(\zeta_5)$ at which $4t(1 - t)$ is rational are the images of cusps and of points over $t = \infty$. The rank exceeds 0, so Mazur's argument does not apply to $E$; but the points we need are the rational points of a curve in the restriction of scalars of $E$ from $K$ or from $\mathbb{Q}(\zeta_5)$, which has dimension 2 or 4, larger than the rank; so Chabauty's method applies, as in elliptic Chabauty [23, 12]. This gives the following theorem.

**Theorem 7.1.** *The equation $x^{11} + y^{11} = z^5$ has no solution $(a, b, c)$ in coprime integers with $abc \neq 0$.*

Darmon proposed to study the curves $X_0^{\pm}(\mathfrak{p})$, which classify the Jacobians of his family with a rational subgroup of the $\mathfrak{p}$-torsion, toward his Conjecture 4.3, and asked whether the Jacobian of $X_0^+(\mathfrak{p})$ always has a nonzero quotient with finite Mordell–Weil group over $\mathbb{Q}(\zeta_r)^+$, at least for $\mathfrak{p}$ large enough [21, §4]. For $r = 5$ the curve $X_0(\mathfrak{p})$ below is his $X_0^-(\mathfrak{p})$; the quotient of it used here has positive rank, so this route through a quotient of rank 0 is replaced rather than followed. Siksek observed, for a generalized Fermat equation, that only the points at which a certain function takes rational values are needed [44, §6, Remark (ii)].

Besides the results of [15] recalled in Section 2 and Theorem 6.7, Corollary 6.8, and Proposition 8.2, the proof uses level lowering for Hilbert modular forms [29, 33, 41, 47] (Lemma 7.2), the modularity of elliptic curves over real quadratic fields [25] and Zhang's theorem [50] (for the ranks), the library of transitive groups of degree 12 and tame specialization [30] (to identify the quotient of $X_0(\mathfrak{p})$ by the involution over $t \mapsto 1 - t$), and the computations of items A1 and A13–A18. A second proof, independent of $J^-$ and of the results of this

paper, is sketched in Remark 7.12. Mihăilescu [40] and Zhou [51] claim, in preprints, general results that would include Theorem 7.1; we do not use them.

7.1. **Darmon's family and the curve $X_0(\mathfrak{p})$.** Let $f(x)=x^5-5x^3+5x$ and, for $t\neq 0,1,\infty$, let $C(t)\colon y^2=f(x)+2-4t$, a curve of genus 2 over $\mathbb{Q}(t)$ (the discriminant of $f+2-4t$ is $2^8 5^5 t^2(t-1)^2$), and $J(t)$ its Jacobian, with real multiplication by $\mathcal{O}_K$ defined over $K$ given by the correspondence of Section 2 with $c$ replaced by 1 [15, Theorem 5.4]. This is Darmon's family for $r=5$ [21]. For a solution $(a,b,c)$ and its *Frey parameter* $t=A/c^5$, the substitution $x=cX$ gives $\Phi(cX)=c^5(f(X)+2-4t)$, as $A-B=(2t-1)c^5$; so $C^-$ is the quadratic twist of $C(t)$ by $c$, and $J^-$ is the twist of $J(t)$ by the character of $K(\sqrt{c})/K$, compatibly with $\mathcal{O}_K$ [15, Lemma 5.5].

Let $\mathfrak{p}$ be a prime of $K$ above a prime $p$ that splits in $K$, so that $\mathcal{O}_K/\mathfrak{p}=\mathbb{F}_p$. Over $U=\mathbb{P}^1\smallsetminus\{0,1,\infty\}$ the $\mathcal{O}_K$-submodules of $J(t)[\mathfrak{p}]$ of $\mathbb{F}_p$-dimension 1, which we call $\mathfrak{p}$-lines, form a finite étale cover of degree $p+1$, defined over $K$; let $X_0(\mathfrak{p})$ be its smooth projective completion, with $t\colon X_0(\mathfrak{p})\to\mathbb{P}^1$. Let $\iota\colon C(t)\to C(1-t)$, $(x,y)\mapsto(-x,\sqrt{-1}\,y)$. It commutes with the real multiplication: $C(t)$ is the quotient of $D_t\colon W^2=Z(Z^{10}+(2-4t)Z^5+1)$ by $Z\mapsto 1/Z$, with $x=Z+1/Z$, $y=W/Z^3$; the real multiplication is generated by the endomorphism induced by the sum of the automorphism $(Z,W)\mapsto(\zeta Z,\zeta^3 W)$ of $D_t$, $\zeta=\zeta_5$, and its inverse, which acts on $dx/y$ and $x\,dx/y$ by the distinct scalars $\zeta+\zeta^{-1}$ and $\zeta^2+\zeta^{-2}$ (the generic endomorphism algebra is $K$, so this is the real multiplication up to $\mathrm{Gal}(K/\mathbb{Q})$); and $\iota$ acts on the same basis by $\mathrm{diag}(\sqrt{-1},-\sqrt{-1})$. So $\iota$ commutes with $\mathcal{O}_K$ and maps $\mathfrak{p}$-lines to $\mathfrak{p}$-lines. It is defined over $K(\sqrt{-1})$, but $\iota$ and its conjugate differ by $-1$, which fixes every $\mathfrak{p}$-line; so $\iota$ induces an involution $w$ of $X_0(\mathfrak{p})$ over $K$ with $t\circ w=1-t$. The function $v=4t(1-t)$ is $w$-invariant and defines

$$v\colon X_0(\mathfrak{p})/w\to\mathbb{P}^1,\qquad \text{of degree } p+1.$$

**Lemma 7.2.** *Let $(a,b,c)$ be a solution of $x^{11}+y^{11}=z^5$ with $10\mid ab$, and $\mathfrak{p}$ a prime of $K$ above 11. Then $\bar\rho_{J^-,\mathfrak{p}}$ is reducible.*

*Proof.* As in the proof of Proposition 8.1(a), exchanging $a$ and $b$ or changing the signs of $a,b,c$ twists $J^-$ by a quadratic character, which does not change reducibility; so we may assume $2\mid a$ and $b\equiv -1 \pmod 4$. By [15, Theorems 6.6, 7.1(2), 7.9, Lemma 6.3, and Lemma 7.5 and its proof] there is $\chi_0\in K(S_2,2)^*$ such that $\rho_{J^-,\lambda}\otimes\chi_0$ is the $\lambda$-adic representation attached to a Hilbert newform of parallel weight 2 and trivial character of level $N=\mathfrak{q}_2\mathfrak{q}_5^2\mathfrak{q}_{ab}$, where $\mathfrak{q}_{ab}$ is the product of the primes dividing $ab$ and prime to 10, at which $J^-$ has multiplicative reduction; and $\bar\rho=\bar\rho_{J^-,\mathfrak{p}}\otimes\chi_0$ is unramified at the primes dividing $\mathfrak{q}_{ab}$ that do not lie above 11, and finite at the primes above 11. Suppose that $\bar\rho$ is irreducible. Then it is absolutely irreducible: otherwise its image would fix two lines of $\mathbb{F}_{121}^2$ conjugate over $\mathbb{F}_{11}$, and the subgroup of $\mathrm{GL}_2(\mathbb{F}_{11})$ fixing them is cyclic of order 120, with $-1$ as its only element of order 2; but for a complex conjugation $c_\infty$, $\bar\rho(c_\infty)$ has order 2 and determinant $-1$, as $\det\bar\rho$ is the mod-11 cyclotomic character [15, Lemma 6.3].

We lower the level in the steps below by the theorems of Jarvis [33, Theorem 6.2], Fujiwara [29, Theorem A and Corollary A′], Taylor [47, Theorem 1] and Rajaei [41], removing the primes above 11 first, as in [33, §8] (compare the proof of [26, Theorem 7]). The conclusion of these steps, that $\bar\rho$ arises from a newform of level $\mathfrak{q}_2\mathfrak{q}_5^2$, is also that of the first case of [15, §10]. For an ideal $\mathfrak{n}$ of $\mathcal{O}_K$ let $U_0(\mathfrak{n})\supseteq U_1(\mathfrak{n})$ be the groups of the matrices $\left(\begin{smallmatrix}\alpha&\beta\\ \gamma&\delta\end{smallmatrix}\right)\in\mathrm{GL}_2(\widehat{\mathcal{O}}_K)$, $\widehat{\mathcal{O}}_K=\mathcal{O}_K\otimes\widehat{\mathbb{Z}}$, with $\gamma\in\mathfrak{n}\widehat{\mathcal{O}}_K$, resp. with moreover $\delta-1\in\mathfrak{n}\widehat{\mathcal{O}}_K$. A form of level $\mathfrak{n}$ with trivial character is fixed by $U_0(\mathfrak{n})$; and a form with trivial character fixed by $U_1(\mathfrak{n})$

is fixed by $U_0(\mathfrak{n})$, which is generated by $U_1(\mathfrak{n})$ and the scalar matrices in $\mathrm{GL}_2(\widehat{\mathcal{O}}_K)$. The hypotheses of these theorems on $K$ and $p = 11$ hold: $\bar\rho$ is absolutely irreducible; 11 is unramified in $K$, so $e = 1 < 10$; and $[K(\zeta_{11}) : K] = 10 \neq 2$, as $\mathbb{Q}(\zeta_{11})^+$ has degree 5 and $K \cap \mathbb{Q}(\zeta_{11}) = \mathbb{Q}$ (the quadratic subfield of $\mathbb{Q}(\zeta_{11})$ is $\mathbb{Q}(\sqrt{-11})$), so the extra conditions these theorems impose when $[K(\zeta_p) : K] = 2$ are void. Fujiwara's results are in his preprint [29], which is unpublished; [33, Theorem 6.2] depends on it when $[K : \mathbb{Q}]$ is even, and [26] and [15] also use it.

(1) *Primes above* 11. Let $\mathfrak{P} \mid 11$ divide $N$. Then $\mathfrak{P} \mid \mathfrak{q}_{ab}$, as $\mathfrak{P} \nmid 10$, so $\mathfrak{P} \parallel N$; the newform is fixed by $U_0(N)$, which contains $U_0(\mathfrak{P}) \cap U_1(N/\mathfrak{P})$; and $\bar\rho$ is finite at $\mathfrak{P}$. So [33, Theorem 6.2] gives a form of parallel weight 2 fixed by $U_1(N/\mathfrak{P})$ to which $\bar\rho$ is attached. Its character $\psi$ has 11-power order, as its reduction is trivial, $\det\bar\rho$ being the mod-11 cyclotomic character [15, Lemma 6.3]. If the other prime $\mathfrak{P}' \mid 11$ divides $N$, then $\mathfrak{P}' \parallel N/\mathfrak{P}$, so the restriction of $\psi$ to the units of the completion of $\mathcal{O}_K$ at $\mathfrak{P}'$ factors through $(\mathcal{O}_K/\mathfrak{P}')^\times$, of order 10, and is trivial; so the form is fixed by $U_0(\mathfrak{P}') \cap U_1(N/\mathfrak{P}\mathfrak{P}')$, and the same theorem removes $\mathfrak{P}'$. In every case $\bar\rho$ is attached to a form fixed by $U_1(N_1)$, where $N_1$ is the largest divisor of $N$ prime to 11.

(2) *The character.* At $v = \mathfrak{q}_5$ the conditions of [29, Theorem A] hold, as $\bar\rho$ is ramified at $\mathfrak{q}_5$ [15, Theorem 7.1(2)] and $\mathrm{N}(\mathfrak{q}_5) = 5 \not\equiv 1 \pmod{11}$. That theorem gives a form attached to $\bar\rho$, fixed by the same group away from $\mathfrak{q}_5$ (its condition (1)), with conductor at $\mathfrak{q}_5$ the Artin conductor of $\bar\rho$ there (its condition (2)), and with trivial character (its condition (3), as $\det\bar\rho$ is the mod-11 cyclotomic character). So $\bar\rho$ is attached to a newform of parallel weight 2 and trivial character whose level divides $N_1$.

(3) *Primes* $\mathfrak{q} \mid \mathfrak{q}_{ab}$ *with* $\mathfrak{q} \nmid 11$ *and* $\mathrm{N}(\mathfrak{q}) \not\equiv 1 \pmod{11}$. Such a prime divides the level at most once, and $\bar\rho$ is unramified at it. So [29, Corollary A′] removes it, and the character stays trivial, by condition (3) of [29, Theorem A].

(4) *Primes* $\mathfrak{q} \mid \mathfrak{q}_{ab}$ *with* $\mathfrak{q} \nmid 11$ *and* $\mathrm{N}(\mathfrak{q}) \equiv 1 \pmod{11}$, one at a time. Let $M$ be the current level, which is prime to 11, with $\mathfrak{q} \parallel M$; the current form has trivial character. (a) By [47, Theorem 1], in the form of [33, §6] and [29, §6], there are a prime $\mathfrak{q}_0 \nmid 11M$ at which $\bar\rho$ is unramified and $\bar\rho(\mathrm{Frob}_{\mathfrak{q}_0})$ is conjugate to $\bar\rho(c_\infty)$, so that $\mathrm{N}(\mathfrak{q}_0) \equiv -1 \pmod{11}$, and a form attached to $\bar\rho$ that is special at $\mathfrak{q}_0$ and fixed by $U_0(M) \cap U_0(\mathfrak{q}_0) = U_0(M\mathfrak{q}_0)$. The character of this form is unramified at every finite prime, hence trivial, as $K$ has narrow class number 1. (b) The main theorem of [41], as stated in [21, Theorem 3.4], applies at the level $\mathfrak{n}\lambda$ with $\lambda = \mathfrak{q}$ and $\mathfrak{n} = M\mathfrak{q}_0/\mathfrak{q}$: the ideals $\mathfrak{n}$, $\lambda$ and (11) are pairwise coprime, $[K : \mathbb{Q}]$ is even and the form is special at the prime $\mathfrak{q}_0 \nmid 11\mathfrak{q}$, and $\bar\rho$ is unramified at $\mathfrak{q}$. It gives a form of level $M\mathfrak{q}_0/\mathfrak{q}$ to which $\bar\rho$ is attached. (c) As $\bar\rho$ is unramified at $\mathfrak{q}_0$ and $\mathrm{N}(\mathfrak{q}_0) \not\equiv 1 \pmod{11}$, [29, Corollary A′] removes $\mathfrak{q}_0$, with trivial character by condition (3) of [29, Theorem A]. The level is now $M/\mathfrak{q}$.

(5) *The level.* So $\bar\rho \cong \bar\rho_{g,\mathfrak{B}}$ for a newform $g$ of parallel weight 2 and trivial character whose level divides $\mathfrak{q}_2\mathfrak{q}_5^2 = (10)$, and a prime $\mathfrak{B} \mid 11$ of its coefficient field. The exponent of the level of $g$ at $\mathfrak{q}_5$ is at least that of the Serre level of $\bar\rho$ [29, §1], which is 2 [15, Theorem 7.1(2)], so it is 2; and there is no newform of level $\mathfrak{q}_5^2$ [15, §9.2]. So $g$ has level (10), and it is 2.2.5.1-100.1-a or -b (item A1), with rational eigenvalues $a_{(3)}(g) = 5$ and $-5$ at the inert prime (3) (Table 5).

If $3 \mid ab$, then $J^-$ has multiplicative reduction at (3) and level lowering gives $a_{(3)}(g)^2 \equiv (9+1)^2 \pmod{\mathfrak{B}}$, but $25 - 100 = -75$ is prime to 11. If $3 \nmid ab$, then $J^-$ has good reduction at (3) and $a_{(3)}(g) \equiv \chi_0((3))\, a_{(3)}(J^-) \pmod{\mathfrak{B}}$, where $a_{(3)}(J^-)$ is $-4$ or 0 according to the residues of $a^{11}, b^{11}, c$ modulo 3 (item A18); but then $a_{(3)}(g) - \chi_0((3))\, a_{(3)}(J^-) \in \{\pm 1, \pm 5, \pm 9\}$, which is prime to 11. So $\bar\rho$, and hence $\bar\rho_{J^-,\mathfrak{p}}$, is reducible. □

**Lemma 7.3.** *Let $p = 11$, $\mathfrak{p} \mid 11$ and $L = \mathbb{Q}(\zeta_5)$. Let $(a, b, c)$ be either a solution with $10 \mid ab$, and put $K' = K$, or a normalized solution with $2 \nmid ab$ and $ab \equiv -1 \pmod 5$, and put $K' = L$. Then $X_0(\mathfrak{p})$ has a point defined over $K'$, lying over $t = a^{11}/c^5$, and $t \in \mathbb{Q} \smallsetminus \{0, 1, \frac12\}$. Its image $P$ in $X_0(\mathfrak{p})/w$ is defined over the same field and satisfies $v(P) \in \mathbb{Q} \smallsetminus \{0, 1\}$.*

*Proof.* By Lemma 7.2 in the first case and Proposition 8.2(a) in the second, $J^-[\mathfrak{p}]$ has an $\mathcal{O}_K$-submodule of $\mathbb{F}_p$-dimension 1 stable under $G_{K'}$. The isomorphism $J^- \to J(t)$ induced by $x = cX$ is defined over $K(\sqrt{c})$, commutes with $\mathcal{O}_K$, and is changed by an element of $G_K$ at most by the sign $-1$, which preserves every line; so it carries this submodule to a $\mathfrak{p}$-line of $J(t)$ stable under $G_{K'}$, which is a point of $X_0(\mathfrak{p})$ over $t$ defined over $K'$. As $abc \neq 0$, $t \neq 0, 1, \infty$; and $t = \frac12$ would give $a^{11} = b^{11}$, so $a = b = \pm 1$ and $c^5 = \pm 2$, which is impossible. Hence $v(P) = 4t(1-t) \in \mathbb{Q}$, and $v(P) \neq 0, 1$. □

7.2. **The quotient $X_0(\mathfrak{p})/w$ for $\mathfrak{p} \mid 11$.** Let $\mathfrak{p} \mid 11$, so that $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_{11}$, and fix $t_0 \in U(\mathbb{C})$ with $t_0 \neq \frac12$. The cover $v\colon X_0(\mathfrak{p})/w \to \mathbb{P}^1$ has degree 12, the number of lines in the plane $J(t_0)[\mathfrak{p}]$ over $\mathbb{F}_{11}$, and it is unramified outside $v = 0, 1, \infty$: for $v \neq 0, 1, \infty$ the two preimages $t$, $1 - t$ of $v$ are distinct points of $U$, and $w$ maps the fiber of $X_0(\mathfrak{p})$ over $t$ bijectively onto the fiber over $1 - t$. The fiber of $v$ over $v(t_0)$ is the set of $\mathfrak{p}$-lines of $J(t_0)$. As $\iota$ and the monodromy of the family commute with $\mathcal{O}_K$, the monodromy of $v$ acts on this fiber through $\mathrm{PGL}_2(\mathbb{F}_{11})$, acting on the lines of $J(t_0)[\mathfrak{p}] \cong \mathbb{F}_{11}^2$. Let $\sigma_0, \sigma_1, \sigma_\infty$ be local monodromies at $v = 0, 1, \infty$ with $\sigma_0\sigma_1\sigma_\infty = 1$; they generate the monodromy group.

*At $v = 0$.* The map $t \mapsto v$ is unramified at $t = 0$, so $\sigma_0$ is the action on lines of the local monodromy of the family at $t = 0$. As $f(x) + 2 = (x+2)(x^2 - x - 1)^2$, the curve $C(0)$ has two nodes, and this local monodromy is unipotent (Picard–Lefschetz). So $\sigma_0$ is 1 or has order 11 and cycle type $[11, 1]$.

*At $v = 1$.* As $v - 1 = -(2t - 1)^2$, a small loop around $v = 1$ lifts to a half-turn around $t = \frac12$, from a point $t_1$ to $1 - t_1$; so $\sigma_1$ is conjugate to the action on lines of the automorphism $\iota$ of $C(\frac12)$. As $\iota^2 = -1$ and $-1$ is not a square modulo 11, $\iota$ acts on $J(\frac12)[\mathfrak{p}]$ with characteristic polynomial $X^2 + 1$: it has determinant 1 and trace 0, and fixes no line. So $\sigma_1$ has cycle type $[2^6]$, and the monodromy group, generated by $\sigma_0$ and $\sigma_1$, lies in $\mathrm{PSL}_2(\mathbb{F}_{11})$.

*At $v = \infty$.* Likewise a small loop around $v = \infty$ lifts to a path from a point $t_2$ to $1 - t_2$ along half of a large circle around $t = \infty$, and $\sigma_\infty$ is conjugate to the action of $\iota$ composed with parallel transport along this path. As $\iota$ is an isomorphism of families over $t \mapsto 1 - t$, it carries the transport along one half of the circle to the transport along the other half; so $\sigma_\infty^2$ is induced by $\iota^2\gamma = -\gamma$, where $\gamma$ is the local monodromy of the family at $t = \infty$. To compute $\gamma$, write $4t = \lambda^5$, $x = \lambda s$ and $y = \lambda^{5/2} y_0$; then $C(t)$ becomes

$$y_0^2 = s^5 - 1 - 5\lambda^{-2}s^3 + 5\lambda^{-4}s + 2\lambda^{-5},$$

which tends to the smooth curve $y_0^2 = s^5 - 1$ as $t \to \infty$. A loop around $t = \infty$ multiplies $\lambda$ by $\zeta^{\pm 1}$ and $\lambda^{5/2}$ by $-1$, so $\gamma$ is the automorphism $(s, y_0) \mapsto (\zeta^{\mp 1}s, -y_0)$ of the limit curve, of order 10, with $\gamma^5 = -1$. As $dx/y$ and $x\,dx/y$ are multiples of $ds/y_0$ and $s\,ds/y_0$, $\gamma$ acts on them by $-\zeta^{\mp 1}$ and $-\zeta^{\mp 2}$. So on the eigenspace of the real multiplication in $H^1(C(t_2), \mathbb{C})$ that contains $dx/y$ and its complex conjugate, $\gamma$ has determinant 1 and trace $-(\zeta + \zeta^{-1})$,

and on the one that contains $x\,dx/y$ it has determinant 1 and trace $-(\zeta^2+\zeta^{-2})$. Hence the trace $\tau \in \mathcal{O}_K$ of $\gamma$ on the free $\mathcal{O}_K$-module $H_1(C(t_2),\mathbb{Z})$ of rank 2 is

$$\tau = -\omega = 1-\phi \quad \text{if } \omega \text{ acts on } dx/y \text{ by } \zeta+\zeta^{-1}, \qquad \tau = 1+\omega = \phi \quad \text{if it acts by } \zeta^2+\zeta^{-2},$$

where $\phi = (1+\sqrt{5})/2 = \omega+1$; the lifts $\pm\gamma$ of $\sigma_\infty^2$ to $\mathrm{SL}_2(\mathbb{F}_{11})$ have traces $\pm\tau$ mod $\mathfrak{p}$, which gives the four values $\pm\phi$, $\pm(\phi-1)$. Modulo either prime above 11, $\phi$ reduces to 8 or 4, so $\tau \not\equiv \pm 2 \pmod{\mathfrak{p}}$; as $\gamma^5 = -1$, the image of $\gamma$ in $\mathrm{PSL}_2(\mathbb{F}_{11})$ has order exactly 5. As $\mathrm{PSL}_2(\mathbb{F}_{11})$ has no element of order 10, $\sigma_\infty$ has order 5, and $\sigma_\infty = \sigma_\infty^6 = \gamma^3$ in $\mathrm{PSL}_2(\mathbb{F}_{11})$. So $\sigma_\infty$ has cycle type $[5,5,1,1]$, and its lifts to $\mathrm{SL}_2(\mathbb{F}_{11})$ have traces $\pm(\tau^3-3\tau)$ mod $\mathfrak{p}$, where

$$\tau^3-3\tau = \phi \ \text{ if } \tau = 1-\phi, \qquad \tau^3-3\tau = 1-\phi \ \text{ if } \tau = \phi. \tag{7.1}$$

Finally $\sigma_0 \neq 1$, as $\sigma_1\sigma_\infty \neq 1$, so $\sigma_0$ has cycle type $[11,1]$. So $v$ has ramification

$$[11,1] \text{ over } v=0, \qquad [2^6] \text{ over } v=1, \qquad [5,5,1,1] \text{ over } v=\infty, \tag{7.2}$$

and no other ramification. Its monodromy group contains elements of orders 2, 5 and 11, so it is a subgroup of $\mathrm{PSL}_2(\mathbb{F}_{11})$ of index dividing $660/110 = 6$; as $\mathrm{PSL}_2(\mathbb{F}_{11})$ is simple and $660 \nmid n!$ for $n \le 6$, it has no proper subgroup of index at most 6. So the monodromy group is $\mathrm{PSL}_2(\mathbb{F}_{11})$, acting on $\mathbb{P}^1(\mathbb{F}_{11})$; it is transitive, and $X_0(\mathfrak{p})/w$ is a geometrically connected curve of genus 1 by the Riemann–Hurwitz formula, $2\cdot 1-2 = -2\cdot 12+10+6+8$.

We now write down an elliptic curve $E$ over $K$ and a function $v_E\colon E \to \mathbb{P}^1$ of degree 12 with the ramification (7.2) (Proposition 7.4), and show that $(X_0(\mathfrak{p})/w, v) \cong (E, v_E)$ for one of the two primes $\mathfrak{p} \mid 11$ (Proposition 7.7). For this, Lemma 7.5 determines the possible monodromy groups of a cover with this ramification, and Lemma 7.6 gives a count of points modulo a prime that tells them apart. Then Proposition 7.8 determines $E(K)$ and $E(L)$, and Propositions 7.9 and 7.10 the points of these groups at which $v_E$ is rational.

Let $E$ be the elliptic curve

$$E\colon y^2+y = x^3-\phi x^2+(2-\phi)x+\phi$$

over $K$ (LMFDB label 2.2.5.1-1331.2-f1), of conductor $(3\phi-1)^2(3\phi-2)$, of norm 1331, with $E(K)_{\mathrm{tors}} = 0$. Its conjugate $E^\sigma$ has conductor $(3\phi-2)^2(3\phi-1)$, so $E^\sigma \not\cong E$. Let $G = (6-3\phi, 16-11\phi) \in E(K)$, and let $u = U_A(x) + U_B(x)\,y$, where $(x-49+29\phi)\,U_A(x)$ and $(x-49+29\phi)\,U_B(x)$ are the polynomials

$$\begin{aligned}
&(-\tfrac{209}{2000}\phi-\tfrac{517}{8000})x^6+(\tfrac{1137}{8000}\phi+\tfrac{327}{4000})x^5+(\tfrac{217}{1000}\phi+\tfrac{2021}{4000})x^4+(-\tfrac{55853}{8000}\phi+\tfrac{39217}{4000})x^3\\
&\quad+(-\tfrac{5019}{400}\phi+\tfrac{16779}{800})x^2+(-\tfrac{12359}{1600}\phi+\tfrac{4281}{320})x+\tfrac{4281}{2000}\phi-\tfrac{8043}{2000},\\
&(-\tfrac{161}{4000}\phi-\tfrac{199}{8000})x^5+(-\tfrac{741}{8000}\phi-\tfrac{113}{2000})x^4+(\tfrac{111}{250}\phi+\tfrac{2219}{8000})x^3+(\tfrac{12013}{8000}\phi-\tfrac{9717}{4000})x^2\\
&\quad+(\tfrac{6321}{500}\phi-\tfrac{172353}{8000})x+\tfrac{21933}{8000}\phi-\tfrac{30319}{8000}.
\end{aligned}$$

Put $v_E = 1/u\colon E \to \mathbb{P}^1$. The formula for $u$ was found by a search modulo the primes above 31 and 41, followed by a 31-adic lift (item A13). Recall that $L = \mathbb{Q}(\zeta_5)$; we have $L = K(\sqrt{-(2+\phi)})$.

**Proposition 7.4.** *The map $v_E$ has degree 12, is unramified outside $\{0,1,\infty\}$, and has ramification (7.2): over 0 the points $O$ (index 11) and $8G$ (index 1); over 1 six points of index 2, whose $x$-coordinates are the roots of an irreducible sextic over $K$; over $\infty$ two points $Q_1, Q_2$ of index 5, with $x$-coordinates the roots of $x^2+(24\phi-40)x+27-17\phi$, defined over $K(\sqrt{11(2+\phi)})$, and two points $Q_3, Q_4$ of index 1, with $x$-coordinates the roots of $x^2+(52\phi-80)x+3451-2129\phi$, defined over $L$ and exchanged by $\mathrm{Gal}(L/K)$.*

*Proof.* Write $N$ for the norm from $K(x,y)$ to $K(x)$. A computation (item A13) gives $N(u) = c_1 q_1^5 q_2/(x-49+29\phi)$ and $N(u-1) = c_2 S^2/(x-49+29\phi)$ with constants $c_1, c_2 \in K^\times$, the two quadratics $q_1$, $q_2$ above and an irreducible sextic $S$, pairwise coprime and squarefree, with $U_B$ nonzero at their roots, which are not abscissas of points of order 2 (they are prime to $4(x^3 - \phi x^2 + (2-\phi)x + \phi) + 1$). So $u$ has divisor $5(Q_1) + 5(Q_2) + (Q_3) + (Q_4) - 11(O) - (8G)$ and $u - 1$ has six double zeros. Then $10 + 6 + 8 = 24 = 2 \cdot 12 + (2 \cdot 1 - 2)$, so there is no other ramification. The fields of definition follow from the discriminants $4 \cdot 11(2+\phi)\phi^{-8}$ of $q_1$ and $-4 \cdot 5^2(2+\phi)\phi^{-8}$ of $q_2$. □

**Lemma 7.5.** *Let $\sigma_0, \sigma_1, \sigma_\infty$ be permutations of a set $\Omega$ of 12 elements with $\sigma_0\sigma_1\sigma_\infty = 1$ and cycle types $[11,1]$, $[2^6]$, $[5,5,1,1]$, and let $\Gamma$ be the group they generate.*

- *(a) $\Gamma$ is 2-transitive, and either it is 3-transitive or $(\Omega, \Gamma)$ is isomorphic to $\mathbb{P}^1(\mathbb{F}_{11})$ with the action of $\mathrm{PSL}_2(\mathbb{F}_{11})$.*
- *(b) Let $\Omega = \mathbb{P}^1(\mathbb{F}_{11})$. The triples as above in $\mathrm{PSL}_2(\mathbb{F}_{11})$ form exactly two orbits under simultaneous conjugation by $\mathrm{PGL}_2(\mathbb{F}_{11})$: in one the lifts of $\sigma_\infty$ to $\mathrm{SL}_2(\mathbb{F}_{11})$ have trace $\pm 3$, in the other $\pm 4$. Each such triple generates $\mathrm{PSL}_2(\mathbb{F}_{11})$, and the centralizer of $\mathrm{PSL}_2(\mathbb{F}_{11})$ in the symmetric group of $\Omega$ is trivial.*
- *(c) Each of $\sigma_0$, $\sigma_1$, $\sigma_\infty$ permutes the 1320 ordered triples of distinct elements of $\Omega$ in cycles of a single length, 11, 2, 5 respectively, so in 120, 660, 264 cycles. If $\Gamma$ is 3-transitive, it is transitive on these triples; if $\Gamma = \mathrm{PSL}_2(\mathbb{F}_{11})$, it has two orbits of 660 triples, on each of which it acts simply transitively.*

*Proof.* (a) The orbits of $\Gamma$ are unions of orbits of $\sigma_0$, which are its fixed point $a$ and $\Omega \smallsetminus \{a\}$; as $\sigma_1$ fixes no point, $\Gamma$ is transitive. The stabilizer of $a$ contains $\sigma_0$, which is transitive on $\Omega \smallsetminus \{a\}$, so $\Gamma$ is 2-transitive. The three permutations are even, so $\Gamma \subseteq A_{12}$. The transitive subgroups of $A_{12}$ that contain elements of the three cycle types are $\mathrm{PSL}_2(\mathbb{F}_{11})$ acting on $\mathbb{P}^1(\mathbb{F}_{11})$, the Mathieu group $M_{12}$ and $A_{12}$ (item A14); $M_{12}$ is 5-transitive and $A_{12}$ is 10-transitive.

(b) Let $\Pi = \mathrm{PSL}_2(\mathbb{F}_{11})$, of order 660. An element of $\Pi$ of cycle type $[11,1]$ is a nontrivial unipotent element; these form two classes of 60 elements, exchanged by conjugation by $\mathrm{PGL}_2(\mathbb{F}_{11})$. An element of cycle type $[2^6]$ has order 2, so its lifts have trace 0 and eigenvalues $\pm\sqrt{-1} \notin \mathbb{F}_{11}$; these form one class of 55 elements. An element of cycle type $[5,5,1,1]$ has order 5, and its lifts have eigenvalues $\lambda^{\pm 1}$ with $\lambda \in \mathbb{F}_{11}^\times$ of order 5 or 10, so trace $\lambda + \lambda^{-1} \in \{\pm 3, \pm 4\}$; these form two classes of 132 elements, one for each trace up to sign, and conjugation by $\mathrm{PGL}_2(\mathbb{F}_{11})$, which preserves traces up to sign, does not exchange them. Now let $x \in \Pi$ be nontrivial unipotent. After conjugation by $\mathrm{PGL}_2(\mathbb{F}_{11})$, which preserves the class of type $[2^6]$ and the traces up to sign, we may assume that $x$ is the image of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. An element $y$ of order 2 is the image of $\pm\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ with $-a^2 - bc = 1$; then $c \neq 0$, as $-1$ is not a square modulo 11, and the lift $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ of $xy$ has trace $c$. For each $c \in \mathbb{F}_{11}^\times$ there are 11 such matrices ($a$ is arbitrary and $b = -(1+a^2)/c$), so for $e \in \{3,4\}$ exactly 11 elements $y$ of order 2 make the lifts of $xy$, hence of $\sigma_\infty = (xy)^{-1}$, have trace $\pm e$. So for each class $\mathcal{K}_0$ of type $[11,1]$ and each class $\mathcal{K}_\infty$ of type $[5,5,1,1]$ there are exactly $60 \cdot 11 = 660$ triples with $\sigma_0 \in \mathcal{K}_0$ and $\sigma_\infty \in \mathcal{K}_\infty$. Each generates $\Pi$, by the argument used above for the monodromy group of $v$: the group it generates has order divisible by $2 \cdot 5 \cdot 11$, hence index at most 6 in $\Pi$. So $\Pi$ acts freely on these 660 triples by conjugation (its center is trivial), and they form one orbit. Conjugation by $\mathrm{PGL}_2(\mathbb{F}_{11})$ exchanges the two classes of type $[11,1]$ and preserves each class of type $[5,5,1,1]$, so the four orbits under $\Pi$ form two orbits under $\mathrm{PGL}_2(\mathbb{F}_{11})$, distinguished by the trace of $\sigma_\infty$. Finally, a permutation $\pi$ of $\Omega$ commuting with $\Pi$ maps

the fixed points of the stabilizer $\Pi_a$ of a point $a$ to fixed points of $\Pi_a$; as $\Pi$ is 2-transitive, $a$ is the only one, so $\pi(a) = a$ for every $a$.

(c) For $1 \le k < 11$, $\sigma_0^k$ fixes only one element of $\Omega$, hence no ordered triple of distinct elements; so every cycle of $\sigma_0$ on triples has length 11, and there are $1320/11 = 120$ of them. Likewise $\sigma_1$ fixes no element, and $\sigma_\infty^k$, $1 \le k < 5$, fixes exactly two, which gives 660 and 264 cycles. A 3-transitive group is transitive on ordered triples of distinct elements. The group $\mathrm{PGL}_2(\mathbb{F}_{11})$ acts simply transitively on the ordered triples of distinct points of $\mathbb{P}^1(\mathbb{F}_{11})$, and $\mathrm{PSL}_2(\mathbb{F}_{11})$ is a subgroup of index 2, so it acts freely, with two orbits of 660 triples. □

**Lemma 7.6.** *Let $\mathfrak{q}$ be a prime of $K$ with residue field $\mathbb{F}_q$ of characteristic greater than 11, at which $E$ has good reduction, and suppose that the reduction $\bar{v}_E\colon \bar{E} \to \mathbb{P}^1_{\mathbb{F}_q}$ of $v_E$ has degree 12, ramification (7.2) over $0, 1, \infty$ and no other critical point. For $s \in \mathbb{F}_q \smallsetminus \{0,1\}$ let $k(s)$ be the number of points of $\bar{E}(\mathbb{F}_q)$ in the fiber of $\bar{v}_E$ over $s$, and put*

$$S_3 = \sum_{s \in \mathbb{F}_q \smallsetminus \{0,1\}} k(s)\big(k(s)-1\big)\big(k(s)-2\big).$$

*If the geometric monodromy group of $\bar{v}_E$ is 3-transitive, then $S_3 \le q + 1 + 278\sqrt{q}$. If it is $\mathrm{PSL}_2(\mathbb{F}_{11})$, then $S_3 = 0$ or $2(q+1) - 280\sqrt{q} - 1044 \le S_3 \le 2(q+1) + 280\sqrt{q}$.*

*Proof.* The cover $\bar{v}_E$ is tame, as its ramification indices are at most 11, so its local monodromies at $0, 1, \infty$ are permutations of the 12 points of a fiber of cycle types $[11,1]$, $[2^6]$, $[5,5,1,1]$. Let $\bar{C}_3$ be the smooth projective curve over $\mathbb{F}_q$ whose points over $s \in \mathbb{P}^1 \smallsetminus \{0,1,\infty\}$ are the ordered triples of distinct points of $\bar{v}_E^{-1}(s)$. Over $\overline{\mathbb{F}}_q$ its components correspond to the orbits of the geometric monodromy group on ordered triples, and by Lemma 7.5(c) it has 120, 660 and 264 points over 0, 1 and $\infty$, of ramification indices 11, 2 and 5. If the group is 3-transitive, $\bar{C}_3$ is geometrically irreducible of degree 1320 over $\mathbb{P}^1$, and the Riemann–Hurwitz formula gives its genus $g$: $2g-2 = -2\cdot 1320 + (1320-120) + (1320-660) + (1320-264) = 276$, so $g = 139$. If the group is $\mathrm{PSL}_2(\mathbb{F}_{11})$, $\bar{C}_3$ has two geometric components, each of degree 660 with 60, 330 and 132 points over 0, 1 and $\infty$ (Lemma 7.5(c)), so each has genus 70: $2\cdot 70 - 2 = -2\cdot 660 + 600 + 330 + 528$. An ordered triple of distinct points of $\bar{E}(\mathbb{F}_q)$ in the fiber over $s \in \mathbb{F}_q \smallsetminus \{0,1\}$ is a point of $\bar{C}_3(\mathbb{F}_q)$, and conversely; so $S_3$ is the number of points of $\bar{C}_3(\mathbb{F}_q)$ not over 0, 1, $\infty$, while $\bar{C}_3$ has at most $120 + 660 + 264 = 1044$ points over 0, 1, $\infty$. By Weil's bound, a geometrically irreducible smooth projective curve of genus $g$ over $\mathbb{F}_q$ has between $q + 1 - 2g\sqrt{q}$ and $q + 1 + 2g\sqrt{q}$ points. In the first case this gives $S_3 \le \#\bar{C}_3(\mathbb{F}_q) \le q + 1 + 278\sqrt{q}$. In the second case Frobenius either exchanges the two components, and then $\bar{C}_3(\mathbb{F}_q) = \emptyset$, as a point over $\mathbb{F}_q$ would lie on both, or fixes both, and then $2(q + 1 - 140\sqrt{q}) - 1044 \le S_3 \le 2(q + 1 + 140\sqrt{q})$. □

**Proposition 7.7.** *For one of the two primes $\mathfrak{p}$ of $K$ above 11 there is an isomorphism $X_0(\mathfrak{p})/w \cong E$ over $K$ that carries $v$ to $v_E$, and then $X_0(\mathfrak{p}^\sigma)/w \cong E^\sigma$, carrying $v$ to $v_E^\sigma$. (Which of the two primes this is depends on how $\mathcal{O}_K$ is identified with the real multiplication; the proof of Theorem 7.1 uses only that there is such a prime.)*

*Proof. The monodromy group of $v_E$.* By Proposition 7.4, $v_E$ is a cover of $\mathbb{P}^1$ of degree 12, unramified outside $\{0,1,\infty\}$, with ramification (7.2), and $E$ is geometrically connected. So its local monodromies form a triple as in Lemma 7.5, and its geometric monodromy group $\Gamma_E$ is either 3-transitive or $\mathrm{PSL}_2(\mathbb{F}_{11})$ acting on $\mathbb{P}^1(\mathbb{F}_{11})$ (Lemma 7.5(a)). We exclude the first case by reduction modulo a prime. Let $q = 500009$, the least prime above $5\cdot 10^5$; as $q \equiv -1 \pmod 5$, it splits in $K$. Let $\mathfrak{q} = (q, \phi - 151941)$, a prime of $K$ of norm $q$. For $q > 313446$,

as here, the lower bound $2(q+1)-280\sqrt{q}-1044$ for a nonzero $S_3$ in the case $\mathrm{PSL}_2(\mathbb{F}_{11})$ of Lemma 7.6 exceeds the bound $q+1+278\sqrt{q}$ of the 3-transitive case, so that a nonzero value of $S_3$ cannot lie in both ranges. The curve $E$ has good reduction at $\mathfrak{q}$, the coefficients of $u$ are $\mathfrak{q}$-integral (Section 7.3), and the identities in the proof of Proposition 7.4 reduce modulo $\mathfrak{q}$ to identities of the same shape with nonzero constants, with $\bar{q}_1\bar{q}_2\bar{S}$ squarefree and prime to $x-\bar{x}(8G)$, to the $y$-coefficient of $\bar{u}$ and to $4(x^3-\phi x^2+(2-\phi)x+\phi)+1$; moreover $d\bar{u}=h_u\,dx/(2y+1)$ with $N(h_u)$ a nonzero constant times $\bar{q}_1^4\bar{S}/(x-\bar{x}(8G))^2$ (item A14). So the reduction $\bar{v}_E$ has degree 12, ramification (7.2) over $0,1,\infty$ and no other critical point, and Lemma 7.6 applies. As $707<\sqrt{q}<708$, if the geometric monodromy group $\bar{\Gamma}_E$ of $\bar{v}_E$ were 3-transitive, then $S_3\le q+1+278\sqrt{q}<q+1+278\cdot 708=696{,}834$. The count gives $S_3=1{,}021{,}680$ (item A14), so $\bar{\Gamma}_E$ is not 3-transitive. (It lies in the window of Lemma 7.6 for $\mathrm{PSL}_2(\mathbb{F}_{11})$ with both components defined over $\mathbb{F}_q$, from $2(q+1)-280\sqrt{q}-1044>800984$ to $2(q+1)+280\sqrt{q}<1198012$.) The cover $v_E$ extends to a finite morphism from the smooth model of $E$ over the local ring of $K$ at $\mathfrak{q}$ to $\mathbb{P}^1$, étale outside the three disjoint sections $0,1,\infty$ and tamely ramified along them, as all ramification indices are at most $11<q$. The groups $\Gamma_E$ and $\bar{\Gamma}_E$ are the images of the tame fundamental groups of the geometric generic and special fibers of $\mathbb{P}^1\smallsetminus\{0,1,\infty\}$ acting on a common fiber of the cover, and the action of the first group factors through the specialization map from it to the second [30, Exp. XIII, 2.10]. So $\Gamma_E\subseteq\bar{\Gamma}_E$; equality holds, as this map is surjective, by the proof of [30, Exp. XIII, Corollaire 2.12]. So $\Gamma_E$ is not 3-transitive, and $\Gamma_E=\mathrm{PSL}_2(\mathbb{F}_{11})$.

*The two moduli covers.* For each prime $\mathfrak{p}\mid 11$, the cover $v\colon X_0(\mathfrak{p})/w\to\mathbb{P}^1$ has monodromy group $\mathrm{PSL}_2(\mathbb{F}_{11})$, acting on the lines of $J(t_0)[\mathfrak{p}]$, and the lifts of its $\sigma_\infty$ have trace $\pm(\tau^3-3\tau)$ mod $\mathfrak{p}$, by (7.1); here $\tau$ is the same element of $\mathcal{O}_K$ for both primes. Under the reductions $\phi\mapsto 8$ and $\phi\mapsto 4$ modulo the two primes above 11, $\pm\phi$ becomes $\pm3$ and $\pm4$, and $\pm(1-\phi)$ becomes $\pm4$ and $\pm3$. So, whatever the normalization of $\mathcal{O}_K$, the triples of the two covers $X_0(\mathfrak{p})/w$ lie in the two different orbits of Lemma 7.5(b), one for each prime.

*Identification.* By the Riemann existence theorem, a connected cover of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ of degree 12 unramified outside $\{0,1,\infty\}$ is determined up to isomorphism by its triple of local monodromies, up to simultaneous conjugation in $S_{12}$. After conjugation, the triple of $v_E$ lies in $\mathrm{PSL}_2(\mathbb{F}_{11})$, and by Lemma 7.5(b) it is conjugate by $\mathrm{PGL}_2(\mathbb{F}_{11})$ to the triple of $X_0(\mathfrak{p})/w$ for the prime $\mathfrak{p}\mid 11$ with the same trace of $\sigma_\infty$. So $(E,v_E)$ and $(X_0(\mathfrak{p})/w,v)$ are isomorphic over $\overline{\mathbb{Q}}$. Both are defined over $K$, and they have no nontrivial automorphism, as the centralizer of $\mathrm{PSL}_2(\mathbb{F}_{11})$ in $S_{12}$ is trivial (Lemma 7.5(b)); so the isomorphism is unique, hence invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and defined over $K$. Finally $X_0(\mathfrak{p})^\sigma=X_0(\mathfrak{p}^\sigma)$, as the real multiplication is defined over $K$, so applying $\sigma$ gives an isomorphism $X_0(\mathfrak{p}^\sigma)/w\cong E^\sigma$ carrying $v$ to $v_E^\sigma$. (As $E^\sigma\not\cong E$, the two moduli covers are not isomorphic.) □

**Proposition 7.8.** *Let $\chi$ be the character of $L/K$ and $E^\chi$ the quadratic twist of $E$ by $\chi$. Then* $\operatorname{rank}E(K)=\operatorname{rank}E^\chi(K)=1$, $E(K)=\mathbb{Z}G$, *and*

$$E(L)=\mathbb{Z}G\oplus\mathbb{Z}H_5,\qquad H_5=(\zeta,\zeta+\zeta^2+2\zeta^3),\quad \zeta=\zeta_5,\ \zeta+\zeta^{-1}=\phi-1,$$

*with $Q_3=5H_5-G$ and $Q_4=-6G-5H_5$.*

*Proof.* The root numbers of $E$ and $E^\chi$ are $-1$, and $L'(E,1)\approx 1.57427$, $L'(E^\chi,1)\approx 4.45887$, computed numerically (item A15); so both have analytic rank 1. Both are modular [25, Theorem 1], and both have conductor exponent 1 at the prime $(3\phi-2)$ above 11 (the conductor of $E^\chi$ is $\mathfrak{q}_5^2(3\phi-1)^2(3\phi-2)$). So Zhang's theorem [50, Theorem A], which applies to a modular elliptic curve over a totally real field when the field has odd degree over $\mathbb{Q}$

or the conductor has exponent 1 at some finite place, gives $\operatorname{rank} E(K) = \operatorname{rank} E^\chi(K) = 1$; points of infinite order are $G$ on $E$ and $G_\chi = (4\phi+2, -11\phi-6)$ on the minimal model $y^2+y = x^3+x^2+(2-5\phi)x-21-40\phi$ of $E^\chi$.

We show that $G$ and $G_\chi$ generate. For $x \in K$ let $h(x)$ be its absolute logarithmic height, and for a point $P$ put $\hat h(P) = \lim_{n\to\infty} h(x(2^nP))/4^n$, so that $\hat h - h\circ x$ is bounded; this is twice the canonical height $\frac12 \lim_{n\to\infty} h(x(2^nP))/4^n$ used by some authors. On a Weierstrass model with integral coefficients, $x(2P) = F(x)/D_2(x)$ with $F = x^4 - b_4x^2 - 2b_6x - b_8$ and $D_2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = (2y + a_1x + a_3)^2$, and the resultant of $F$ and $D_2$ is $\Delta^2$. For a place $v$ of $K$ put $\Psi_v(x) = \log\max(|F(x)|_v, |D_2(x)|_v) - 4\log\max(1, |x|_v)$. The product formula and a telescoping sum give, for $P$ of infinite order (as in [18]),

$$\hat h(P) - h(x(P)) = \frac{1}{[K:\mathbb{Q}]}\sum_v n_v \sum_{n\ge0} 4^{-n-1}\Psi_v(x(2^nP)),$$

with $n_v$ the local degree. At a finite place $v \nmid \Delta$, $\Psi_v = 0$: for $|x|_v \le 1$ an identity $UF + VD_2 = \Delta^2$ with $U, V$ integral polynomials gives $\max(|F(x)|_v, |D_2(x)|_v) = 1$, and for $|x|_v > 1$, $|F(x)|_v = |x|_v^4 > |D_2(x)|_v$. At a finite place $v \mid \Delta$, $\Psi_v(x(R)) = 0$ if $R$ has nonsingular reduction: after a translation of $x$ and $y$ that moves the singular point of the reduction to $(0,0)$, which changes $F$ by a multiple of $D_2$, one has $F \equiv x^4$ and $D_2 \equiv x^2(4x+b_2)$ modulo $v$, so $F$ and $D_2$ vanish together modulo $v$ only at the $x$-coordinate of the singular point, and the only point of the reduction with this $x$-coordinate is the singular point. As the points with nonsingular reduction form a subgroup, for $P$ with nonsingular reduction at every finite place only the two real places $v_1, v_2$ contribute, and there $\Psi_v \ge m_v = \inf \Psi_v$, the infimum over the real $x$ with $D_2(x) \ge 0$, that is, over the $x$-coordinates of $E(K_v)$, with $x = \infty$ (where $\Psi_v = 0$) included. Hence, as $\sum_{n\ge0} 4^{-n-1} = \frac13$,

$$h(x(P)) \le \hat h(P) + C_\infty, \qquad C_\infty = -\tfrac16(m_{v_1} + m_{v_2}),$$

for such $P$. Each $m_v$ is attained at one of the real roots of $D_2$, $F - D_2$, $F + D_2$, $F'$, $D_2'$, $xF' - 4F$ and $xD_2' - 4D_2$, or at $x = \pm1, \infty$. It was computed from this list and, separately, by an interval branch-and-bound search on the compactified real line, which gives rigorous bounds for it (item A15). For $E$, the two infima are $-0.370364\ldots$ and $-0.154969\ldots$, so $C_\infty \in [0.0875556, 0.0875557]$; for $E^\chi$ they are 0 and $-0.342264\ldots$, so $C_\infty \in [0.0570440, 0.0570441]$; we use $C_\infty = 0.0876$ and $0.0571$. In the same way, $\Psi_v \le 0$ at every finite place, and the suprema of $\Psi_{v_1}$ and $\Psi_{v_2}$ give $\hat h(R) - h(x(R)) < 1.05$ for $R \in E(K)$ and $< 1.83$ for $R \in E^\chi(K)$, $R \ne O$; with the values of $h(x(2^{10}G))/4^{10}$ and $h(x(2^9G_\chi))/4^9$, computed from the exact coordinates, this gives $\hat h(G) < 0.027572$ and $\hat h(G_\chi) < 0.281058$. If $G = kP_0$ with $k \ge 5$ prime, then $6P_0$ has nonsingular reduction everywhere (the component groups $E(K_v)/E^0(K_v)$ of the minimal models are $\mathbb{Z}/2$ at $(1-3\phi)$ (type III) and $\mathbb{Z}/3$ at $(3\phi-2)$ (split $I_3$) for both curves, and trivial at $(\phi+2)$ for $E^\chi$ (type $I_0^*$, Tamagawa number 1); 6 kills all of them) and $h(x(6P_0)) \le B = 36\hat h(G)/25 + C_\infty < 0.128$; likewise for $G_\chi$, with $B < 0.462$. Writing $x = r/s^2$ with $r, s \in \mathcal{O}_K$ coprime gives $\mathrm{N}(s)^2 \le H_K(x) \le e^{2B} < 16$, where $H_K(x) = e^{2h(x)}$. Every nonunit of $\mathcal{O}_K$ has norm of absolute value at least 4, so $s$ is a unit, $x \in \mathcal{O}_K$ and $\max(1,|x_1|)\max(1,|x_2|) \le e^{2B}$, where $x_1, x_2$ are the images of $x$ under the two real embeddings. This leaves $x \in \{0, \pm1\}$ for $E$, where $\mathrm{N}(D_2(x)) = -11, 101, 61$, and $x \in \{0, \pm1, \pm\phi, \pm\phi^{-1}\}$ for $E^\chi$, where $\mathrm{N}(D_2(x)) = -5431, -15851, 1421, -1375, -9559, 8341, -24875$. None of these norms is a square in $\mathbb{Q}$, so $D_2(x)$, which is $(2y+a_1x+a_3)^2$ at a point $(x,y)$ of a model $y^2+a_1xy+a_3y = x^3+\cdots$, is never a square in $K$, and no candidate is the $x$-coordinate of a point. By reduction, $G \notin 2E(K)$,

$3E(K)$ (modulo primes above 19 and 29) and $G_\chi \notin 2E^\chi(K)$, $3E^\chi(K)$ (above 19 and 41). Both torsion subgroups are trivial. At a prime of good reduction with residue characteristic $p \geq 3$, unramified in $K$, torsion injects into the reduction. For $E$: $\#E(\mathbb{F}_9) = 11$ at the inert prime 3, and $\#E(\mathbb{F}_{19}) = 26$ at $(19, \phi - 15)$. For $E^\chi$: $\#E^\chi(\mathbb{F}_9) = 9$ and $\#E^\chi(\mathbb{F}_{49}) = 56$ at the inert primes 3 and 7. In each case the gcd is 1. As both ranks are 1, $E(K) = \mathbb{Z}P_1$ and $G = \pm nP_1$. A prime $k \mid n$ would put $G$ in $kE(K)$, which is excluded above for $k = 2, 3$ and for $k \geq 5$. So $E(K) = \mathbb{Z}G$, and likewise $E^\chi(K) = \mathbb{Z}G_\chi$ (item A15). For $P \in E(L)$ let $\bar{P}$ be its conjugate over $K$, and $E(L)^- = \{P : \bar{P} = -P\}$. Then $2P = (P + \bar{P}) + (P - \bar{P})$ lies in $E(K) \oplus E(L)^- = \mathbb{Z}G \oplus \mathbb{Z}G_d$, where $G_d \in E(L)^-$ corresponds to $G_\chi$ under $E(L)^- \cong E^\chi(K)$. A computation in $E(L)$ gives $2H_5 = -(G + G_d)$, and $G$, $G_d \notin 2E(L)$ (reduction at a prime above 41). $E(L)[2] = 0$: if $2T = 0$, then $T + \bar{T} \in E(K)[2] = 0$, so $\bar{T} = -T = T$ and $T \in E(K)[2] = 0$. Since $2E(L) \subseteq \mathbb{Z}G + \mathbb{Z}G_d$ and $\mathbb{Z}G + \mathbb{Z}G_d$ is torsion-free, $E(L)$ is torsion-free, and $P \mapsto 2P$ embeds $E(L)/(\mathbb{Z}G + \mathbb{Z}G_d)$ into $(\mathbb{Z}G + \mathbb{Z}G_d)/2(\mathbb{Z}G + \mathbb{Z}G_d)$. The image is $\{0, G + G_d\}$: $G + G_d = -2H_5$, while $G$ and $G_d$ are not in $2E(L)$. Hence $E(L) = \mathbb{Z}G + \mathbb{Z}G_d + \mathbb{Z}H_5 = \mathbb{Z}G + \mathbb{Z}H_5$. The relations for $Q_3$, $Q_4$ are checked by computation in $E(L)$. □

7.3. **Points over rational values of the parameter.** For a prime $\mathfrak{Q}$ of $K$ or $L$ not dividing $2 \cdot 5 \cdot 11$, the coefficients of $(x - 49 + 29\phi)u$ have denominators dividing $2^6 5^3$, and the leading coefficient of $u$ at $O$ has norm $-2^{-12}5^{-5}$. If moreover the zeros and poles of $u$ remain distinct modulo $\mathfrak{Q}$, then $u$ extends to a morphism from the smooth model of $E$ at $\mathfrak{Q}$, so that the reduction of $v_E(P)$ is $\bar{v}_E(\bar{P})$ (item A16). If $v_E(P) \in \mathbb{P}^1(\mathbb{Q})$ and $q$ is the prime below $\mathfrak{Q}$, then these reductions at all primes above $q$ coincide and lie in $\mathbb{P}^1(\mathbb{F}_q)$.

**Proposition 7.9.** *The points $P \in E(K)$ with $v_E(P) \in \mathbb{P}^1(\mathbb{Q})$ are $O$ and $8G$.*

*Proof.* By Proposition 7.8, $P = nG$ with $n \in \mathbb{Z}$. Let $M = 2^6 3^4 5^2 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 293318625600$, a product of small prime powers, so that the order $N_q$ defined below divides $M$ for many primes $q$. The primes $q$ with $7 \leq q \leq 3000$ and $q \neq 11$ for which the order $N_q$ of $G$ modulo the primes above $q$ divides $M$ are the 35 primes 7, 13, 19, 29, 41, 47, 59, 101, 103, 131, 149, 179, 269, 271, 281, 311, 401, 409, 419, 421, 491, 499, 541, 569, 929, 1019, 1069, 1103, 1459, 1609, 1619, 2371, 2729, 2731, 2801; at each of them $E$ has good reduction and the zeros and poles of $u$ stay distinct. The condition $N_q \mid M$ keeps the combined modulus a divisor of $M$. The classes of $n$ modulo $N_q$ that satisfy the condition above, combined by the Chinese remainder theorem, leave only $n \equiv 0$ or $8 \pmod{M}$ (item A16). The prime 29 splits in $K$; let $\iota_1, \iota_2 \colon K \to \mathbb{Q}_{29}$ be the embeddings with $\iota_1(\phi) \equiv 6$ and $\iota_2(\phi) \equiv 24 \pmod{29}$. As $N_{29} = 24$, $n = 24m$ or $n = 8 + 24m$ with $m \in \mathbb{Z}$, and $T = 24G$ lies in the kernel of reduction at both primes above 29. The functions $F_0(m) = \iota_1 v_E(mT) - \iota_2 v_E(mT)$ and $F_8(m) = \iota_1 v_E(8G + mT) - \iota_2 v_E(8G + mT)$ are power series $\sum_k a_k m^k$, $\sum_k a'_k m^k$ converging on $\mathbb{Z}_{29}$, and the formal logarithms and the expansions of $v_E$ at $O$ (a zero of order 11 with a 29-adic unit as leading coefficient) and at $8G$ (a simple zero, with unit derivative) give $a_0 = \cdots = a_{10} = 0$, $a_{11} \equiv 171 \cdot 29^{11} \pmod{29^{13}}$, so that $v_{29}(a_{11}) = 11$, $v_{29}(a_k) \geq 12$ for $k \geq 12$, and $a'_0 = 0$, $a'_1 \equiv 453 \cdot 29 \pmod{29^3}$, so that $v_{29}(a'_1) = 1$, $v_{29}(a'_k) \geq 2$ for $k \geq 2$ (item A16). If $v_E(P) \in \mathbb{Q}$, then $F_0(m) = 0$, resp. $F_8(m) = 0$, and by Strassmann's theorem $m = 0$. □

**Proposition 7.10.** *The points $P \in E(L)$ with $v_E(P) \in \mathbb{P}^1(\mathbb{Q})$ are $O$, $8G$, $Q_3$ and $Q_4$.*

*Proof.* By Proposition 7.8, $P = n_1 G + n_2 H_5$. The condition stated at the start of Section 7.3 (the reductions of $v_E(P)$ coincide and lie in $\mathbb{P}^1(\mathbb{F}_q)$), applied at the primes of $L$ above

$q = 41, 421, 881, 101, 311$, leaves eight classes of $(n_1, n_2)$ modulo $1636128 = 2^5 \cdot 3^2 \cdot 13 \cdot 19 \cdot 23$, the least common multiple of the orders of $G$ and $H_5$ modulo the primes above these five primes, each of which splits completely in $L$. They are all congruent modulo 144 to the coordinates $(0,0)$, $(8,0)$, $(-1,5)$, $(-6,-5)$ of $O$, $8G$, $Q_3$, $Q_4$ (item A17). The order of $G$ and of $H_5$ modulo every prime above 41 divides 144; as $u$ extends to the smooth model at the primes above 41, the local expansions below have 41-integral coefficients. Let $P_s$ be one of the four points and $P(m) = P_s + 144(m_1 G + m_2 H_5)$, $m \in \mathbb{Z}_{41}^2$. Let $g$ be a local parameter of $v_E$ at $P_s$ with a simple zero there: the 11th root of $v_E$ at $O$ (as $\mu_{11}(\mathbb{Q}_{41}) = 1$), $v_E$ at $8G$, and $u$ at $Q_3$, $Q_4$. Number the four embeddings $\iota_j \colon L \to \mathbb{Q}_{41}$ so that $\iota_j(\zeta) \equiv 10, 16, 18, 37 \pmod{41}$ for $j = 1, 2, 3, 4$. Then $\iota_j g(P(m))$ is $\alpha_j \ell_j(m)$ plus terms of degree at least 2 in $\ell_j(m) = m_1 \lambda_{1j} + m_2 \lambda_{2j}$, where $\lambda_{1j}$ and $\lambda_{2j}$, of valuation 1, are the formal logarithms of $\iota_j(144G)$ and $\iota_j(144H_5)$, and the unit $\alpha_j$ is the value at $P_s$ of $\iota_j(dg/\omega_E)$, $\omega_E = dx/(2y+1)$. The condition $v_E(P(m)) \in \mathbb{Q}$ gives $\iota_1 g(P(m)) = \iota_j g(P(m))$ for $j = 2, 3, 4$; those for $j = 2, 3$ give $F(m) = Bm + R(m) = 0$, where the rows of $B$ are $(\alpha_j \lambda_{1j} - \alpha_1 \lambda_{11},\ \alpha_j \lambda_{2j} - \alpha_1 \lambda_{21})$ for $j = 2, 3$, and $v_{41}(R(m)) \geq 2 + 2v_{41}(m)$. Modulo $41^3$,

$$B \equiv 41 \begin{pmatrix} -459 & -177 \\ -459 & 130 \end{pmatrix}, \quad 41 \begin{pmatrix} 22 & 459 \\ 22 & -138 \end{pmatrix}, \quad 41 \begin{pmatrix} 574 & 626 \\ 810 & -173 \end{pmatrix}, \quad 41 \begin{pmatrix} 817 & 784 \\ 581 & 221 \end{pmatrix}$$

for $P_s = O$, $8G$, $Q_3$, $Q_4$, respectively. So the entries of $B$ have valuation at least 1, and $\det B \equiv 4 \cdot 41^2$, $-14 \cdot 41^2$, $-13 \cdot 41^2$, $-41^2 \pmod{41^3}$ has valuation 2 (item A17). Then $m = -B^{-1} R(m)$ gives $v_{41}(m) \geq 1 + 2v_{41}(m)$, so $m = 0$ and $P = P_s$. □

### 7.4. **Proof of Theorem 7.1.**

*Proof.* Let $(a, b, c)$ be a solution in coprime integers with $abc \neq 0$. By Corollary 6.8, $10 \mid ab$, or $2 \nmid ab$ and $ab \equiv -1 \pmod 5$; in the second case we may assume the solution normalized. Let $\mathfrak{p}$ be the prime of Proposition 7.7, so that $X_0(\mathfrak{p})/w \cong E$ with $v$ carried to $v_E$. By Lemma 7.3, there is $P \in E(K)$, resp. $P \in E(L)$, with $v_E(P) \in \mathbb{Q} \smallsetminus \{0, 1\}$. But by Propositions 7.4, 7.9 and 7.10, the points of $E(L)$ at which $v_E$ is rational are $O$ and $8G$, where $v_E = 0$, and $Q_3$ and $Q_4$, where $v_E = \infty$. □

*Remark* 7.11. For $p = 11$ the class $2 \nmid ab$ is also excluded by [9, Theorem 1.5], as then $2 \mid a + b$, and so is the part of the class $10 \mid ab$ with $11 \mid c$, as then $11 \mid a + b$. So Theorem 7.1 follows already from [15, Theorem 1.1], [9, Theorem 1.5] and the argument of this section with Proposition 7.9 alone, and the class that these two theorems leave is $10 \mid ab$, $11 \nmid c$. Proposition 7.10 shows that the method of this section removes the obstruction of the forms with complex multiplication as well.

*Remark* 7.12. We sketch a second proof of Theorem 7.1, which uses neither $J^-$ nor the results of this paper. Nothing else in the paper depends on this remark, and its computations are in [34]. If $11 \mid c$, then $11 \mid a + b$, which [9, Theorem 1.5] excludes. If $11 \nmid c$, the descent of Dahmen and Siksek [20, §4.3], with 11 in place of 7 (it uses that $\mathbb{Z}[\zeta_{11}]$ has class number 1 [37]), and a sieve with fifth power residue symbols at 331 and 661, the two smallest primes $q \equiv 1 \pmod{55}$ (they split completely in $\mathbb{Q}(\zeta_{11})$, and $5 \mid q - 1$), give $a + \zeta_{11} b = \beta_1^5$ and a point $(X, Y) = (\gamma / z_1^2, (a-b)/(a+b))$, where $a + b = z_1^5$ and $\gamma \in \mathcal{O}_k$ is the norm of $\beta_1$, on the curve $(2 - \vartheta) Y^2 = 4X^5 - (2 + \vartheta)$ of genus 2 over $k = \mathbb{Q}(\vartheta)$, $\vartheta = \zeta_{11} + \zeta_{11}^{-1}$, with $Y \in \mathbb{Q} \smallsetminus \{\pm 1\}$. As 2 is inert in $k$, the condition $Y \in \mathbb{Q}_2$ confines such a point to the residue disks at 2 of $\infty$ and $(1, \pm 1)$, and in each disk to at most two nonzero classes in $\mathcal{V}(k_2)/2\mathcal{V}(k_2)$, $\mathcal{V}$ the Jacobian. The field $k(((2 + \vartheta)/4)^{1/5})$, of degree 25, has class number 1, unconditionally, by the criterion of Belabas, Diaz y Diaz and Friedman [3, Theorem 5.1] and a check that the

prime ideals of norm below $4 \cdot 10^6$ are principal. With this, the 2-Selmer group of $\mathcal{V}$ over $k$ has dimension at most 4, injects into $\mathcal{V}(k_2)/2\mathcal{V}(k_2)$ and misses these classes; so Stoll's form of Chabauty's method [45, Theorem 2.1] shows that the only such points are $(1, \pm 1)$, where $ab = 0$.

## 8. What remains

By Corollary 6.8, for $p \geq 11$ a solution has $10 \mid ab$, or $2 \nmid ab$ and $ab \equiv -1 \pmod 5$, and in the second case, for the normalized solution, $\bar{\rho}_{J^-,\mathfrak{p}}$ is isomorphic to $\bar{\rho}_{\mathcal{J}_4,\mathfrak{p}}$ or $\bar{\rho}_{\mathcal{J}_{16},\mathfrak{p}}$ (Theorem 6.7). For $p = 11$ neither case occurs, by Theorem 7.1. Its proof replaces the quotient of rank 0 that Mazur's method needs by a quotient of $X_0(\mathfrak{p})$ of rank 1 together with the rationality of the Frey parameter $t = a^p/c^5$ (Section 7.1), and the same argument would need the analogous computation at each larger exponent. Chen and Koutsianas deduce from the Borel case of Darmon's Conjecture 4.1 [21] that there is no solution with $10 \mid ab$ for large $p$ [15, Corollary 1.3 and the remark after it]. Here the *Borel case* is the assertion that, for $p$ large, the image of the mod-$p$ representation is not contained in a Borel subgroup, that is, the representation is irreducible. For solutions with $r \mid ab$, $r = 5$ or 7, Darmon [21, Theorem 3.13] states that for $p$ large the representation attached to his Frey variety $J_r^-(a, b, c)$ for $x^p + y^p = z^r$ (for $r = 5$, the Jacobian $J^-$ of $C^-$) is reducible and that a quotient of $J_r^-(a, b, c)$ over $\mathbb{Q}$ then has a rational point of order $p$, by the argument of [21, Proposition 3.11]. His proof first shows that $2 \mid ab$ [21, Corollary 3.12], so for $r = 5$ it concerns the case $10 \mid ab$, and a contradiction would follow if these abelian varieties, when semistable, could not have a rational point of order $p$ [21, §4]. His argument uses the semistability of $J_r^-(a, b, c)$, which holds only up to a quadratic twist [15, Remarks 7.16 and 7.22]. We carry it out for $r = 5$ with the conductors of [15, Theorem 7.1] and for every $p \geq 11$. As in [15, proofs of Theorems 8.6 and 8.7] (compare [6, proof of Theorem 2] for abelian varieties of $\mathrm{GL}_2$-type), the conductor and the determinant force one diagonal character to be unramified above $p$ and of order at most 2. Those proofs then use a fixed prime at which the Frey variety has potentially good reduction. When $10 \mid ab$, $J^-$ has potentially multiplicative reduction at $\mathfrak{q}_2$ and $\mathfrak{q}_5$ [15, Proposition 7.12, Lemma 7.20], and any other fixed prime may divide $ab$, where $J^-$ then has multiplicative reduction [15, Lemma 7.5 and its proof]. Instead, as in Darmon's argument and as for Frey elliptic curves over totally real fields [27, Theorem 2], [28, Lemma 6.4], we obtain a point of order $p$, here $K$-rational, on a quadratic twist of the Frey Jacobian or on its quotient by a subgroup of order $p$.

Throughout this section $\phi = \omega + 1 = (1 + \sqrt{5})/2$; $\infty_1, \infty_2$ are the real places of $K$; $\chi_p$ is the mod-$p$ cyclotomic character; and $\chi_{\mathbb{Q}(\zeta_5)/K}$ is the quadratic character of $\mathbb{Q}(\zeta_5)/K$. An abelian surface over $K$ *with real multiplication by* $\mathcal{O}_K$ *defined over* $K$ is one with an embedding of $\mathcal{O}_K$ into its ring of endomorphisms defined over $K$.

**Proposition 8.1.** *Let $p \geq 11$ be prime, $(a, b, c)$ a solution with $10 \mid ab$, and $\mathfrak{p} \mid p$.*

*(a) If $\bar{\rho}_{J^-,\mathfrak{p}}$ is reducible, then there are a character $\eta\colon G_K \to \{\pm 1\}$ (possibly trivial), unramified outside $\mathfrak{q}_2, \mathfrak{q}_5, \infty_1, \infty_2$, and an abelian surface $\mathcal{S}$ over $K$ with real multiplication by $\mathcal{O}_K$ defined over $K$, equal either to the quadratic twist $J^- \otimes \eta$ or to its quotient by a $G_K$-stable $\mathcal{O}_K$-submodule of $(J^- \otimes \eta)[\mathfrak{p}]$ of $\mathbb{F}_\mathfrak{p}$-dimension 1, such that $\mathcal{S}(K)$ contains a point of order $p$.*

*(b) Suppose that there is a constant $B_0$ such that, for every prime $\ell > B_0$, no abelian surface over $K$ with real multiplication by $\mathcal{O}_K$ defined over $K$ has a $K$-rational point of order $\ell$. Then, by the results of [15] cited in the proof below, for every*

*prime $p > \max(B_0, 10)$ the equation $x^p + y^p = z^5$ has no solution $(a, b, c)$ in coprime integers with $abc \neq 0$ and $10 \mid ab$.*

*Proof.* (a) Exchanging $a$ and $b$, and replacing $(a, b, c)$ by $(-a, -b, -c)$, each replace $\Phi(x)$ by $-\Phi(-x)$, that is, $J^-$ by its quadratic twist by $-1$; the map $x \mapsto -x$ commutes with the real multiplication, whose defining relation $x'^2 - \omega x x' + x^2 + c^2(\omega^2 - 4) = 0$ is unchanged by $(x, x') \mapsto (-x, -x')$. This twist is unramified outside $\mathfrak{q}_2, \infty_1, \infty_2$, so it preserves reducibility and can be absorbed into $\eta$ below. As $10 \mid ab$ and $\gcd(a, b) = 1$, we may therefore assume $2 \mid a$ and $b \equiv -1 \pmod 4$. Here $\bar\rho_{J^-,\mathfrak{p}}$ is the action of $G_K$ on $J^-[\mathfrak{p}]$, as in [15, §6]; whether it is reducible does not depend on the lattice. By [15, Theorem 7.1(2)] (with $5 \mid ab$) there is $\chi_0 \in K(S_2, 2)^*$ such that $\bar\rho' = \bar\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ has Serre level $\mathfrak{q}_2^s\mathfrak{q}_5^2$ with $s \leq 1$, and $\bar\rho'$ is finite at every prime of $K$ above $p$ ([15, §7.3], from [21, Proposition 1.15], $\chi_0$ being unramified above $p$). By [15, Lemma 6.3], $\det \bar\rho' = \chi_p$. As $\bar\rho_{J^-,\mathfrak{p}}$ is reducible, so is $\bar\rho'$:

$$\bar\rho' \cong \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix}, \qquad \theta, \theta' \colon G_K \to \mathbb{F}_\mathfrak{p}^\times, \quad \theta\theta' = \chi_p.$$

*Conductors away from $p$.* As $\chi_p$ is unramified at every finite place $v \nmid p$, $\theta$ and $\theta'$ have the same conductor exponent $e_v$ at such $v$. For a representation $V$ with a stable line $W$, $\dim V^{I_v} \leq \dim W^{I_v} + \dim(V/W)^{I_v}$, and the Swan conductor is additive (wild inertia at $v \nmid p$ is pro-$\ell$ with $\ell \neq p$). So the conductor exponent of $\bar\rho'$ at $v$ is at least $2e_v$. Hence $e_v = 0$ for $v \nmid 10p$, $e_{\mathfrak{q}_2} = 0$ (as $s \leq 1$) and $e_{\mathfrak{q}_5} \leq 1$.

*At $p$.* The prime $p$ is unramified in $K$ and $\bar\rho'$ is finite at every $\mathfrak{p}' \mid p$, so by Raynaud [42, Corollaire 3.4.4], as in [15, (8.7)], the restriction of $\theta \oplus \theta'$ to the inertia group at $\mathfrak{p}'$ is, up to order, $1 \oplus \chi_p$ or the sum of the two fundamental characters of level 2; the second is possible only when $p$ is inert in $K$. Suppose that each of $\theta$ and $\theta'$ is ramified at some prime above $p$. If $p$ splits in $K$, then one of them is ramified at exactly one of the two primes above $p$, where its restriction to inertia is $\chi_p$; if $p$ is inert, the restriction of one of them to inertia is a fundamental character of level 2. So one of them, $\theta_1$, has the following property. In the convention of [15, (8.1)], write the restriction of $\theta_1^{-1}$ to the inertia group at $\mathfrak{p}' \mid p$ as $\theta_1^{-1}|_I = \prod_\tau (\tau \circ \chi_\mathrm{f})^{-n_{\mathfrak{p}'}(\tau)}$, with $\chi_\mathrm{f}$ a fundamental character. Then the exponents $n_{\mathfrak{p}'}(\tau)$ vanish except for one pair $(\mathfrak{p}_0, \tau_0)$, for which $n_{\mathfrak{p}_0}(\tau_0) = 1$. The conductor of $\theta_1$ away from $p$ divides $\mathfrak{q}_5$. So [15, Corollary 8.5] applies with $u = \phi^{12}$, a totally positive unit with $u \equiv 1 \pmod{\mathfrak{q}_2\mathfrak{q}_5}$ ([15, proof of Theorem 8.7]), and gives $\tau_0(u) \equiv 1 \pmod{\mathfrak{p}_0}$. So $p$ divides $\mathrm{N}_{K/\mathbb{Q}}(\phi^{12} - 1) = (160 + 72\sqrt{5})(160 - 72\sqrt{5}) = -320 = -2^6 \cdot 5$, which is impossible for $p \geq 11$. So one of $\theta$, $\theta'$, call it $\theta_0$, is unramified at every prime above $p$.

*The character $\theta_0$.* It is unramified at every finite place except possibly $\mathfrak{q}_5$, where its conductor exponent is at most 1, so it factors through the ray class group of $K$ of modulus $\mathfrak{q}_5\infty_1\infty_2$. This group has order 2 (item A18): $(\mathcal{O}_K/\mathfrak{q}_5)^\times \times \{\pm 1\}^2$ has order 16, and the image of the units $\langle -1, \phi \rangle$ has order 8 ($\phi \equiv 3 \pmod{\mathfrak{q}_5}$ has order 4 in $\mathbb{F}_5^\times$, with signs $(+, -)$, and $-1 \equiv 4$, with signs $(-, -)$). Its nontrivial character is $\chi_{\mathbb{Q}(\zeta_5)/K}$, as $\mathbb{Q}(\zeta_5)/K$ is ramified exactly at $\mathfrak{q}_5$ and the two real places. So $\theta_0 \in \{1, \chi_{\mathbb{Q}(\zeta_5)/K}\}$ and $\theta_0^2 = 1$.

*The twist.* Put $\eta = \chi_0\theta_0$, unramified outside $\mathfrak{q}_2, \mathfrak{q}_5, \infty_1, \infty_2$, and $J' = J^- \otimes \eta$, the quadratic twist. It has real multiplication by $\mathcal{O}_K$ defined over $K$, and $\bar\rho_{J',\mathfrak{p}} = \bar\rho_{J^-,\mathfrak{p}} \otimes \eta = \bar\rho' \otimes \theta_0$. Its diagonal characters $\theta\theta_0$ and $\theta'\theta_0$ are 1 and $\chi_p\theta_0^2 = \chi_p$ in some order. If $\theta\theta_0 = 1$, then $J'[\mathfrak{p}]$ contains a $G_K$-stable $\mathbb{F}_\mathfrak{p}$-line with trivial action, whose nonzero elements are $K$-rational points of order $p$; take $\mathcal{S} = J'$. If $\theta'\theta_0 = 1$, let $\mathcal{C}$ be the stable line, an $\mathcal{O}_K$-submodule of $J'[\mathfrak{p}]$ of $\mathbb{F}_\mathfrak{p}$-dimension 1, and $\mathcal{S} = J'/\mathcal{C}$, an abelian surface over $K$ with real multiplication

by $\mathcal{O}_K$ defined over $K$. The image of $J'[\mathfrak{p}]$ in $\mathcal{S}$ is $J'[\mathfrak{p}]/\mathcal{C}$, nonzero, killed by $\mathfrak{p}$ and with trivial action of $G_K$. Its nonzero elements are $K$-rational points of $\mathcal{S}$ of order $p$.

(b) Let $p > \max(B_0, 10)$ and let $(a, b, c)$ be a solution with $10 \mid ab$. We use the proof of [15, Theorem 1.2] in [15, §10], whose first case shows that if $\bar\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ were irreducible it would arise, by level lowering keeping $\mathfrak{q}_2$ in the level, from one of the two newforms of level $\mathfrak{q}_2\mathfrak{q}_5^2$. These are eliminated as in case (II) of [15, Theorem 1.1], that is, by the comparison of [15, §9.3] at the primes above 3, 7 and 11, for every $\chi_0 \in K(S_2, 2)^*$ and every $p \notin \{2, 3, 5, 7\}$. This comparison tests whether $p$ divides the integer $T(g, \mathfrak{q})$ defined in the caption of Table 5. Table 5 gives the outcome of this comparison (item A18). At a prime $\mathfrak{q}$ above $p$ the condition $p \mid T(g, \mathfrak{q})$ holds for every $g$, as $\mathrm{N}(\mathfrak{q})$ divides $T(g, \mathfrak{q})$, so the comparison there excludes nothing; for $p = 11$ the prime (3) alone excludes both forms, as in the proof of Lemma 7.2. So $\bar\rho_{J^-,\mathfrak{p}}$ is reducible. By (a), some abelian surface over $K$ with real multiplication by $\mathcal{O}_K$ defined over $K$ has a $K$-rational point of order $p > B_0$, against the hypothesis. □

TABLE 5. The two newforms of level $\mathfrak{q}_2\mathfrak{q}_5^2 = (10)$, their Hecke eigenvalues at the primes above 3, 7, 11 (LMFDB), and the primes dividing the greatest common divisor over these four primes $\mathfrak{q}$ of the integer $T(g, \mathfrak{q})$ of [15, §9.3]. This integer is the product of $\mathrm{N}(\mathfrak{q})$, of $a_\mathfrak{q}(g)^2 - (\mathrm{N}(\mathfrak{q})+1)^2$ and, over the residues modulo $\mathfrak{q}$ of a solution with $\mathfrak{q} \nmid ab$, of the norms of $\prod_{\tau \in \mathrm{Gal}(K/\mathbb{Q})}(a_\mathfrak{q}(g) - \tau(a_\mathfrak{q}(J^- \otimes \chi_0)))$, so that an isomorphism $\bar\rho_{J^-,\mathfrak{p}} \otimes \chi_0 \cong \bar\rho_{g,\mathfrak{B}}$ forces $p \mid T(g, \mathfrak{q})$. The set is the same for each of the eight characters $\chi_0 \in K(S_2, 2)^*$.

| form | $a_{(3)}$ | $a_{(7)}$ | $a$ at both primes above 11 | primes dividing $\gcd_\mathfrak{q} T(g, \mathfrak{q})$ |
|---|---|---|---|---|
| 2.2.5.1-100.1-a | 5 | 10 | $-3$ | 3, 5 |
| 2.2.5.1-100.1-b | $-5$ | $-10$ | $-3$ | 3, 5 |

The range $p \geq 11$ in Proposition 8.1(b) comes from [15, §10], which assumes $p \geq 11$ (see the paragraph after (CK4)), although [15, Theorem 1.2] is stated for $p$ sufficiently large. For elliptic curves the corresponding torsion bound is Mazur's over $\mathbb{Q}$ [38] and Merel's over any number field [39]. We know of no uniform bound on rational points of order $p$ for abelian surfaces over $K$ with real multiplication, nor of a case of Darmon's Conjecture 4.1 for them. Darmon raises this torsion question for the varieties $J_r^{\pm}(a, b, c)$ in [21, §4].

**Proposition 8.2.** *Let $p \equiv 1 \pmod 5$ be a prime, $p \geq 11$, $L = \mathbb{Q}(\zeta_5)$ and $\mathfrak{p} \mid p$.*

*(a) If $(a, b, c)$ is a normalized solution with $2 \nmid ab$ and $5 \nmid ab$, then the restriction of $\bar\rho_{J^-,\mathfrak{p}}$ to $G_L$ is a sum of two characters; so $J^-$ has an $L$-rational subgroup that is an $\mathcal{O}_K$-submodule of $J^-[\mathfrak{p}]$ of $\mathbb{F}_\mathfrak{p}$-dimension 1.*

*(b) If $(a, b, c)$ is a solution with $10 \mid ab$, then, by the results of [15] cited in the proof of Proposition 8.1(b), $\bar\rho_{J^-,\mathfrak{p}}$ is reducible over $K$, so $J^-$ has a $K$-rational, hence $L$-rational, subgroup that is an $\mathcal{O}_K$-submodule of $J^-[\mathfrak{p}]$ of $\mathbb{F}_\mathfrak{p}$-dimension 1.*

*Proof.* (a) By Theorem 6.7, $\bar\rho_{J^-,\mathfrak{p}} \cong \bar\rho_{\mathcal{J}_D,\mathfrak{p}}$ for $D = 4$ or 16, compatibly with $K$. As $p \equiv 1 \pmod 5$, $p$ splits completely in $L$, so $\mathfrak{p}$, of norm $p$, splits in $L/K$ into two primes $\mathfrak{P} \neq \bar{\mathfrak{P}}$. Over $L$, $\mathcal{J}_D$ has complex multiplication by $\mathcal{O}_L = \mathbb{Z}[\zeta]$, generated by $[\zeta]$, so $\bar\rho_{\mathcal{J}_D,\mathfrak{p}}|_{G_L}$ is the sum of the two characters by which $G_L$ acts on the $\mathfrak{P}$- and $\bar{\mathfrak{P}}$-torsion of $\mathcal{J}_D$, each a $G_L$-stable line, as $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathbb{F}_\mathfrak{p} = \mathbb{F}_\mathfrak{P} \times \mathbb{F}_{\bar{\mathfrak{P}}}$. The same holds for $\bar\rho_{J^-,\mathfrak{p}}|_{G_L}$, and the preimage of either line is an $L$-rational subgroup of $J^-[\mathfrak{p}]$ that is an $\mathcal{O}_K$-submodule of $\mathbb{F}_\mathfrak{p}$-dimension 1.

(b) This is shown in the proof of Proposition 8.1(b), and a $G_K$-stable line is $G_L$-stable. □

*Remark* 8.3. By Proposition 8.2, for $p \equiv 1 \pmod 5$ both cases left by Corollary 6.8 are instances of the Borel case, over $L$, of [21, Conjecture 4.1], for those Frey Jacobians $J^-$ with $\mathrm{End}_L(J^-) \otimes \mathbb{Q} = \mathrm{End}_{\overline{\mathbb{Q}}}(J^-) \otimes \mathbb{Q} \cong K$, which is the hypothesis of that conjecture with base field $L$ and coefficient field $K$. By [15, Theorem 5.4], $K \subseteq \mathrm{End}_K(J^-) \otimes \mathbb{Q}$, so this hypothesis asks only that $J^-$ have no further endomorphisms over $\overline{\mathbb{Q}}$.

## Appendix A. Computations

The table below lists, in the order of the paper, the computations on which the proofs depend, and two computations (items A6 and A7) that check arguments proved in the text. They are exact computations with polynomials over $\mathbb{Z}$, in number fields, in $p$-adic fields (to a precision that decides the residues and valuations read) and in finite fields, except the numerical $L$-values and the interval arithmetic of item A15. They were carried out in PARI/GP 2.17.3 [49], in Python 3.12 (with SymPy 1.14, python-flint 0.8.0, NumPy and mpmath) and in SageMath 10.9 (with its GAP and SciPy 1.18). Hecke eigenvalues of newforms are taken from the LMFDB [48], as of 1 October 2026. In the table, LMFDB labels of Hilbert newforms and elliptic curves over $K$ omit the prefix 2.2.5.1-. The running time of every program is given in [34].

| item | what it establishes | used in | software |
|---|---|---|---|
| A1 | The newforms over $K$ of parallel weight 2 and level of norm dividing 2000; the LMFDB lists all of them (the dimensions of the newform spaces, with old-form multiplicities, add up to $\dim S_2 = 49$ at norm 2000 and to 9 at norm 400). The trace comparison of [15, §9.3] at the primes above $3, 7, 11$, with squared traces (so for every $\chi_0$), at the levels $\mathfrak{q}_2^s\mathfrak{q}_5^\varepsilon$, $s \in \{1,2\}$, $\varepsilon \in \{2,3\}$: it removes every form of level $\mathfrak{q}_2\mathfrak{q}_5^\varepsilon$ for $p \notin \{2,3,5,7\}$ (at a prime $\mathfrak{q}$ above $p$ the comparison excludes nothing, as the integer it tests has the factor $\mathrm{N}(\mathfrak{q})$; for $p = 11$ the primes above 3 and 7 suffice) and leaves 400.1-b, 2000.1-b, -d, -e and, for $p = 19$, 2000.1-h, at the levels $\mathfrak{q}_2^2\mathfrak{q}_5^\varepsilon$; and at level $\mathfrak{q}_5^3$ the form 125.1-a, which only Remark 5.4 uses. The four forms $g_D$ of Table 2 agree with $\mathcal{J}_D$ at the primes above the 40 primes $q \equiv 1 \pmod 5$ below 1000 | Table 2, Remark 5.4, Lemma 7.2 | PARI/GP (`hyperellcharpoly`) with LMFDB eigenvalues |
| A2 | For each sign of $\left(\frac{ab}{5}\right)$, 32 classes $(A \bmod 25, c \bmod 5)$ have $\varepsilon = 3$ and 8 have $\varepsilon = 2$ | Remark 3.5 | PARI/GP, Python |
| A3 | $D^4 \equiv 6, 11, 16 \pmod{25}$ and $\kappa(-4), \kappa(-16), \kappa(-64) = 4, 3, 2$; the Frobenius polynomials $(x^2+5)^2$ and $(x^2-5)^2$ of $y^2 = x^5 + x$ and $y^2 = x^5 - x$ over $\mathbb{F}_5$ | Proposition 3.4(e), Proposition 5.2(b) | PARI/GP (`hyperellcharpoly`), Python |

| item | what it establishes | used in | software |
|---|---|---|---|
| A4 | The identity and valuations of the model at $\mathfrak{q}_2$ (odd $\lvert A\rvert \le 31$, thirteen values of $c$); the reduction of the real multiplication; the models of $H_D$ at 2 | Proposition 4.1 | PARI/GP, SymPy |
| A5 | The discriminant exponents $3,2,3,2,3,2,3$ of $K(\sqrt{\Delta})/K$ at $\mathfrak{q}_2$ for $\Delta = 2, \phi, 2\phi, -1, -2, -\phi, -2\phi$, $\phi = (1+\sqrt{5})/2$; class number and narrow class number 1 | Proposition 4.1(c) | PARI/GP (`rnfdisc`, `nfdisc`, `bnfnarrow`) |
| A6 | The $G_{\mathbb{Q}_2}$-modules $\mathcal{B}[p]$ and the multipliers of their intertwiners for $p = 3, 7, 11, 13$, a check of the argument at 2 | Proposition 6.6 | PARI/GP (arithmetic on the Jacobian of $w^2 + w = X^5$ over $\mathbb{F}_{2^n}$) |
| A7 | A check of the finite-field algebra in the proof of Lemma 6.5, which shows that $\alpha$ intertwines the actions. For all $\bar{\delta}, \bar{D}, \kappa(\beta), \kappa(-D) \in \mathbb{F}_5^\times$ with $\kappa(\beta) \equiv \pm\kappa(-D)$, $s_0$ is a square in $\mathbb{F}_5$ if and only if $\left(\frac{\bar{\delta}\bar{D}}{5}\right) = +1$. When it is, $s_0^5 = s_0$, $s_0\bar{\delta} = \pm\bar{D}$, and $\alpha \circ g_{J^-} = g_{\mathcal{J}_D} \circ \alpha$ holds in both coordinates for the reduced descent data of that proof, for all $r(g) \in \mathbb{F}_5^\times$, $k_6(g) \in \mathbb{F}_5$ and both powers of Frobenius on $\mathbb{F}_{25}$. This identity is checked at the 50 points $(X, Y)$ with $X \in \mathbb{F}_{25}$ and $Y$ equal to 1 or to a primitive cube root of unity, with each of the three cube roots of unity in $\mathbb{F}_{25}$ in place of the common factor $\bar{v}_g$ (which enters both sides alike) | Lemma 6.5 | PARI/GP |
| A8 | The traces $a_{\mathfrak{q}}$ of Lemma 4.2 at every residue $(A \bmod q, c \bmod q)$ for $q = 11, 31, 41, 61, 71, 101$, compared with point counts and with Frobenius on $J[2]$ on a sample of 1670 curves (every residue at $q = 11$, every seventh at $31 \le q \le 71$), and the integers $B_q$ of Table 3 | Proposition 4.3(a) | PARI/GP, Python (python-flint) |
| A9 | The eigenvalues of the newform 2000.1-h in Table 4, and the matching of the primes that the LMFDB names by generators with the primes $\mathfrak{q}$ of that table. The Brandt module of item A10, with $T_{\mathfrak{q}}$ computed at the ideal generated by the LMFDB's generator, confirms this matching: it gives the same eigenvalues under exactly one isomorphism of coefficient fields, and under none if the two primes above 11, or above 31, are exchanged. For this newform, every residue and every embedding, the primes $p$ allowed by the traces are $2, 3, 5, 7$ at $q = 11$ and $2, 3, 5, 13$ at $q = 31$ | Proposition 4.3(b), Remark 5.4 | PARI/GP with LMFDB eigenvalues, Python |

| item | what it establishes | used in | software |
|---|---|---|---|
| A10 | The Hilbert cusp forms of parallel weight 2 and levels $\mathfrak{q}_2^2\mathfrak{q}_5^3$, $\mathfrak{q}_2^2\mathfrak{q}_5^2$, from the Brandt module of the icosian ring (maximal; class number 1): each eigensystem, old ones included, equals an LMFDB form at the primes above $3, 7, 11, 19, 29, 31, 41$; the comparison of item A1 with these eigenvalues, for every eigensystem; the three new ones with complex multiplication at $\mathfrak{q}_2^2\mathfrak{q}_5^3$ equal those of $\mathcal{J}_4, \mathcal{J}_{16}, \mathcal{J}_{64}$ and the one at $\mathfrak{q}_2^2\mathfrak{q}_5^2$ that of $\mathcal{J}_1$, each under exactly one isomorphism of coefficient fields (determined from the LMFDB eigenvalues at the primes above $q = 11, 31, 41, 61, 71, 101$, the primes $q \equiv 1 \pmod 5$ up to 101) | Table 2, Proposition 4.3(b), Remark 5.4 | PARI/GP, Python |
| A11 | Steps of the proofs of Propositions 6.3 and 6.4 and Lemma 6.5, computed at examples: the roots $r_k$, the integrality of $X_k$ with $\bar{X}_k = k\bar{X}_1$, $\bar{X}_1 = \pm\bar{\delta}$, the reduction of the real multiplication to translations, and the action of inertia, at 24 points $(A, B, c, \delta)$ (22 distinct triples $(A, B, c)$). These points have $\beta$ a power of 4, so that $\beta$ has a fifth root in $\mathbb{Q}(2^{1/5})$ and the computation is exact in $\mathbb{Q}(\zeta_5, 2^{1/5})$ (as $\kappa(2) = 2$, $2^{1/5} \in L_1$). The trace $-2\left(\frac{he}{5}\right)(2\omega + 1)$ of Frobenius on $Y^2 = h(X^5 - X)$ with $\omega$ acting by $T_e + T_e^{-1}$ is also computed, for all $h, e$ | Proposition 6.3, Proposition 6.4, Lemma 6.5 | PARI/GP, Python |
| A12 | The least $k$ with $C^-(-2^k, 2^k, 0) \cong H_D$, $11 \le p < 100$; at $p = 11$, $q = 331$, the residues whose traces equal those of $\mathcal{J}_{16}$ are the three trivial ones | Proposition 6.9 | PARI/GP, Python |
| A13 | The map $v_E$ of Proposition 7.4, found by an exhaustive search modulo the primes above 31 and 41 and a 31-adic Newton lift, then checked exactly over $K$: the factorizations of $N(u)$, $N(u-1)$ and $N(du/\omega_E)$, $\omega_E = dx/(2y+1)$, the divisor of $u$, its critical points, and the fields of definition of $Q_1, \dots, Q_4$ | Proposition 7.4 | PARI/GP, SageMath |
| A14 | The transitive groups of degree 12 in $A_{12}$ with elements of cycle types $[11, 1]$, $[2^6]$, $[5, 5, 1, 1]$, from the library of transitive groups; a check of Lemma 7.5(b), (c) by enumeration in $\mathrm{PSL}_2(\mathbb{F}_{11})$; at the prime of $K$ above $q = 500009$ with $\phi \mapsto 151941$, the reductions of the identities of item A13, with nonzero constants, the coprimality conditions and the norm of $d\bar{u}$; and the sum $S_3 = 1{,}021{,}680$ of Lemma 7.6, against the bound $q + 1 + 278 \cdot 708 = 696{,}834$ for a 3-transitive group | Lemma 7.5, Proposition 7.7 | GAP, PARI/GP, Python, SageMath |

| item | what it establishes | used in | software |
|---|---|---|---|
| A15 | The root numbers $-1$ of $E$ and $E^\chi$, and $L'(E,1) = 1.57427\ldots$, $L'(E^\chi,1) = 4.45887\ldots$ (functional equations checked to $2^{-137}$ and $2^{-141}$); torsion and local data; the infima of $\Psi_{v_1}, \Psi_{v_2}$, upper bounds for their suprema, and the constants $C_\infty$, the values of $h(x(2^nG))/4^n$ and $h(x(2^nG_\chi))/4^n$ for $n \le 10$, resp. $n \le 9$, the search for points of small height and the reductions showing $E(K) = \mathbb{Z}G$, $E^\chi(K) = \mathbb{Z}G_\chi$; the relations $2H_5 = -(G + G_d)$, $Q_3 = 5H_5 - G$, $Q_4 = -6G - 5H_5$ and $G, G_d \notin 2E(L)$ | Proposition 7.8 | PARI/GP, Python, SageMath |
| A16 | The denominators and leading coefficient of $u$ and the good reduction of $v_E$ at the primes used; the sieve for $E(K)$, leaving $n \equiv 0, 8 \pmod M$; the 29-adic orders, formal logarithms and leading coefficients, $a_{11}$ modulo $29^{13}$ and $a'_1$ modulo $29^3$, and the exact values of $F_0(m)$, $F_8(m)$ for $m = 1, 2, 3$ | Proposition 7.9 | PARI/GP, Python |
| A17 | The sieve for $E(L)$ at the primes above $41, 421, 881, 101, 311$; at 41, the formal logarithms of $144G$, $144H_5$, the derivatives of the local parameters, the matrices $B$ modulo $41^3$ and the $2 \times 2$ minors of the linear parts | Proposition 7.10 | PARI/GP, Python |
| A18 | The ray class group of $K$ of modulus $\mathfrak{q}_5\infty_1\infty_2$ has order 2, with class field $\mathbb{Q}(\zeta_5)$; $\phi^{12} \equiv 1 \pmod{\mathfrak{q}_2\mathfrak{q}_5}$ and $\mathrm{N}(\phi^{12} - 1) = -320$; the elimination of the two newforms of level $\mathfrak{q}_2\mathfrak{q}_5^2$ for $p \ge 11$ (Table 5), with their LMFDB eigenvalues compared with `ellap` on the elliptic curves 100.1-a, -b; the traces $a_{(3)}(J^-) \in \{-4, 0\}$ | Lemma 7.2, Proposition 8.1 | PARI/GP (`bnrinit`, `bnrclassfield`), Python |

*Second computations.* Every item was also computed by a second, separately written program, with the same results, except item A10 and the count of dimensions in item A1, computed once, and the class number and narrow class number 1 of $K$ in item A5, which are classical; for item A13 the second program repeats the exact check, not the search, and for the sieve of item A16 it uses other primes and leaves the same two classes of $n$. The data package [34] says which program repeats which computation. For the generation of $E(K)$ and $E^\chi(K)$ (item A15) the second program is in Python, with the real infima bounded by interval branch and bound, and a third check is saturation in SageMath.

Items A1 (the comparison, and the identification of the $g_D$ with the $\mathcal{J}_D$), A5, A6, A7, A11, A15 (the root numbers, the $L'$-values and the torsion), A16, A17 (the 29-adic and 41-adic data) and A18 (the comparison of Table 5) were also done in SageMath, with the same results, by programs written from the text that use no PARI, whose only input in common with the first computations is the LMFDB eigenvalues [34].

**Data availability.** The programs, their outputs and the commands that run them are in [34].

## Declarations

**Research methodology.** The author designed and operated the multi-agent research system used in this work, built on Anthropic Claude Opus 5.5. The system carried out literature analysis, mathematical development and computation, with checks assigned to agents separate from those developing the arguments.

**Funding.** This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

**Declaration of competing interests.** The author declares no competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

**Declaration of generative AI and AI-assisted technologies in the manuscript preparation process.** Anthropic Claude Opus 5.5 was used to draft and revise the manuscript. The author reviewed the material and takes full responsibility for the article.

## References

1. Martin Azon, *Effective Darmon's program for the generalised Fermat equation*, 2025, Preprint, arXiv:2504.01967v2.
2. Martin Azon, Mar Curcó-Iranzo, Maleeha Khawaja, Céline Maistret, and Diana Mocanu, *Conductor exponents for families of hyperelliptic curves*, 2026, Preprint, arXiv:2410.21134v2; to appear in J. Théor. Nombres Bordeaux.
3. Karim Belabas, Francisco Diaz y Diaz, and Eduardo Friedman, *Small generators of the ideal class group*, Math. Comp. **77** (2008), no. 262, 1185–1197.
4. Alex J. Best, Sander R. Dahmen, and Nuno Freitas, *On the generalized Fermat equation* $x^{13} + y^{13} = z^n$, 2025, Preprint, arXiv:2510.12092v1.
5. 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** (2023), no. 2, 715–741.
6. 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** (2017), no. 10, 4111–4117.
7. ———, *A multi-Frey approach to Fermat equations of signature* $(r, r, p)$, Trans. Amer. Math. Soc. **371** (2019), no. 12, 8651–8677.
8. ———, *On Darmon's program for the generalized Fermat equation, I*, J. Reine Angew. Math. **822** (2025), 107–146.
9. ———, *On Darmon's program for the generalized Fermat equation, I*, 2025, Full version, arXiv:2205.15861v5; a shorter version appeared in J. Reine Angew. Math. 822 (2025).
10. Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21, Springer-Verlag, Berlin, 1990.
11. Nils Bruin, *On powers as sums of two cubes*, Algorithmic Number Theory (Leiden, 2000) (Wieb Bosma, ed.), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 169–184.
12. ———, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49.
13. Pedro-José Cazorla García and Lucas Villagra Torcomian, *On the conductor of a family of Frey hyperelliptic curves*, 2026, Preprint, arXiv:2503.21568v2; to appear in Res. Number Theory.
14. Imin Chen and Angelos Koutsianas, *Darmon's Program: A survey*, 2025, Preprint, arXiv:2507.15149v1.
15. ———, *A modular approach to Fermat equations of signature* $(p, p, 5)$ *using Frey hyperelliptic curves*, 2025, Preprint, arXiv:2210.02316v2; to appear in Algebra Number Theory.
16. Imin Chen and Deniz Suozer, *Reduction of Weil–Deligne representations*, 2026, Preprint, arXiv:2609.36467v1.
17. Imin Chen and Lucas Villagra Torcomian, *A note on conductors of Frey representations at 2*, 2025, Preprint, arXiv:2509.23540v1.

18. J. E. Cremona, M. Prickett, and Samir Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number Theory **116** (2006), no. 1, 42–68.
19. Sander R. Dahmen, *Classical and modular methods applied to Diophantine equations*, Ph.D. thesis, Universiteit Utrecht, 2008.
20. Sander R. Dahmen and Samir Siksek, *Perfect powers expressible as sums of two fifth or seventh powers*, Acta Arith. **164** (2014), no. 1, 65–100.
21. Henri Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's last theorem*, Duke Math. J. **102** (2000), no. 3, 413–449.
22. Abraham de Moivre, *Aequationum quarundam potestatis tertiae, quintae, septimae, nonae, & superiorum, ad infinitum usque pergendo, in terminis finitis, ad instar regularum pro cubicis quae vocantur Cardani, resolutio analytica*, Philos. Trans. Roy. Soc. London **25** (1707), no. 309, 2368–2371.
23. E. Victor Flynn and Joseph L. Wetherell, *Finding rational points on bielliptic genus 2 curves*, Manuscripta Math. **100** (1999), no. 4, 519–533.
24. Nuno Freitas, *On the Fermat-type equation* $x^3 + y^3 = z^p$, Comment. Math. Helv. **91** (2016), no. 2, 295–304.
25. Nuno Freitas, Bao V. Le Hung, and Samir Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math. **201** (2015), no. 1, 159–206.
26. Nuno Freitas and Samir Siksek, *The asymptotic Fermat's last theorem for five-sixths of real quadratic fields*, Compos. Math. **151** (2015), no. 8, 1395–1415.
27. ———, *Criteria for irreducibility of mod p representations of Frey curves*, J. Théor. Nombres Bordeaux **27** (2015), no. 1, 67–76.
28. ———, *Fermat's last theorem over some small real quadratic fields*, Algebra Number Theory **9** (2015), no. 4, 875–895.
29. Kazuhiro Fujiwara, *Level optimization in the totally real case*, 2006, Preprint, arXiv:math/0602586v1.
30. Alexander Grothendieck, *Revêtements étales et groupe fondamental (SGA 1)*, Lecture Notes in Math., vol. 224, Springer-Verlag, Berlin, 1971.
31. Emmanuel Halberstadt and Alain Kraus, *Courbes de Fermat: résultats et problèmes*, J. Reine Angew. Math. **548** (2002), 167–234.
32. Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York–Heidelberg, 1977.
33. Frazer Jarvis, *Correspondences on Shimura curves and Mazur's principle at p*, Pacific J. Math. **213** (2004), no. 2, 267–280.
34. Manvir Jaswal, *Programs and data for "The generalized Fermat equation* $x^p + y^p = z^5$ *and inertia at* $\sqrt{5}$*"*, 2026, Zenodo, doi:10.5281/zenodo.23149240.
35. ———, *Real multiplication and the generalized Fermat equation* $x^5 + y^3 = z^p$, 2026, Preprint, Zenodo, doi:10.5281/zenodo.23149238.
36. Alain Kraus, *Sur l'équation* $a^3 + b^3 = c^p$, Experiment. Math. **7** (1998), no. 1, 1–13.
37. J. Myron Masley and Hugh L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286/287** (1976), 248–256.
38. Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.
39. Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1–3, 437–449.
40. Preda Mihăilescu, *The strong Fermat–Catalan equation*, 2025, Preprint, arXiv:2509.18275v1.
41. Ali Rajaei, *On the levels of mod ℓ Hilbert modular forms*, J. Reine Angew. Math. **537** (2001), 33–65.
42. Michel Raynaud, *Schémas en groupes de type* $(p, \dots, p)$, Bull. Soc. Math. France **102** (1974), 241–280.
43. Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), no. 3, 492–517.
44. Samir Siksek, *Explicit Chabauty over number fields*, Algebra Number Theory **7** (2013), no. 4, 765–793.
45. Michael Stoll, *Chabauty without the Mordell–Weil group*, Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory (Gebhard Böckle, Wolfram Decker, and Gunter Malle, eds.), Springer, Cham, 2017, pp. 623–663; numbering as in arXiv:1506.04286v2.
46. Walter Tautz, Jaap Top, and Alain Verberkmoes, *Explicit hyperelliptic curves with real multiplication and permutation polynomials*, Canad. J. Math. **43** (1991), no. 5, 1055–1064.
47. Richard Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. **98** (1989), no. 2, 265–280.

48. The LMFDB Collaboration, *The L-functions and modular forms database*, 2026, https://www.lmfdb.org.
49. The PARI Group, *PARI/GP version 2.17.3*, 2025, Univ. Bordeaux, https://pari.math.u-bordeaux.fr.
50. Shou-Wu Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27–147.
51. Zhong-Peng Zhou, *The inter-universal Teichmüller theory and new Diophantine results over rational numbers. II*, 2025, Preprint, arXiv:2510.05448v1.

Toronto, Canada
*Email address*: manvirjaswal@icloud.com