REAL MULTIPLICATION AND THE GENERALIZED FERMAT EQUATION $x^5 + y^3 = z^p$

MANVIR JASWAL

ABSTRACT. Let (X, Y, Z) be a primitive solution of $x^5+y^3 = z^p$ with $p \geq 7$ prime. Pacetti and Villagra Torcomian attach to it a genus-2 Frey curve whose Jacobian J_t, $t = -X^5/Y^3$, has real multiplication by the integers of $\mathbb{Q}(\sqrt{5})$. In a preprint they show that, if p lies outside an explicit finite set and $\mathfrak{p}$ is a prime above p, the mod-$\mathfrak{p}$ representation of J_t is reducible, or congruent to a Hilbert newform with complex multiplication, or congruent to the Jacobian at $t = -1/8$ or $t = 9/8$, the parameters of $1^5+2^3 = 3^2$ and $(-3)^5+6^3 = (-3)^3$. Comparing the fields cut out by inertia at $\sqrt{5}$, we show that this last congruence forces $5 \nmid XYZ$ and restricts t to eight classes modulo 25, and, by comparing traces of Frobenius at an auxiliary prime, to four classes when $p \geq 17$. A congruence multiplies the Weil pairings by a scalar, and by comparing this scalar at 3 and at $\sqrt{5}$ we show that the congruence cannot occur when $3 \mid Y$ and $p \equiv 19, 29, 31, 41 \pmod{60}$. Assuming statements of the preprint, we deduce that, for every prime p outside that explicit finite set, there are no solutions in several families of classes, among them those with $3 \nmid XYZ$.

CONTENTS

1. Introduction 1
2. The Frey curve and the two special parameters 6
3. The local picture at $\sqrt{5}$ 19
4. The orientation at $\sqrt{5}$ 28
5. A symplectic argument at 3 and $\sqrt{5}$ 37
6. Consequences of the results of Pacetti and Villagra Torcomian 46
Appendix A. Computations 62
Declarations 65
References 65

1. INTRODUCTION

For integers $a, b, c \geq 2$, the generalized Fermat equation of signature (a, b, c) is $x^a+y^b = z^c$, and a solution (x, y, z) is primitive if x, y, z are pairwise coprime. When $1/a+1/b+1/c < 1$, Darmon and Granville [12] proved that there are only finitely many primitive solutions, and when moreover $a, b, c \geq 3$, Beal's conjecture predicts that there are none with $xyz \neq 0$. The survey [1] describes what is known. For families of signatures in which one exponent is a varying prime p, the modular method, in the form proposed by Darmon [11], attaches to a solution an abelian variety over a totally real field, its Frey variety, whose residual Galois

2020 *Mathematics Subject Classification.* Primary 11D41; Secondary 11F80, 11G10, 11G30, 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. 65.

representation is, after modularity and level lowering, that of a Hilbert newform of small level. The solution is excluded if no such newform can occur. Recent work carries this out for several signatures with Frey hyperelliptic curves [3, 8, 33].

This paper concerns the signature $(5, 3, p)$:

$$x^5 + y^3 = z^p, \tag{1.1}$$

p a prime. A primitive solution of (1.1) is a triple (X, Y, Z) of pairwise coprime nonzero integers with $X^5 + Y^3 = Z^p$. Pacetti and Villagra Torcomian [33] attach to it the genus-2 curve

$$C_t\colon v^2 = 5u^6 - 12u^5 + 10tu^3 + t^2, \qquad t = -X^5/Y^3,$$

whose Jacobian J_t has real multiplication by the ring of integers $\mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{5})$, by a correspondence of Kumar and Mukamel [26, Theorem 14] (Proposition 2.2). For a prime $\mathfrak{p}$ of K above p, the module $J_t[\mathfrak{p}]$ is a two-dimensional representation $\bar{\rho}_{t,\mathfrak{p}}$ of $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. We write σ for the nontrivial automorphism of K and $\mathfrak{p}' = \sigma(\mathfrak{p})$ for the conjugate of $\mathfrak{p}$. Theorem A of [33] says that for p outside the set $\mathcal{P} = \{2, 3, 5, 7, 11, 13, 19, 29, 31, 41, 61, 71, 79, 89, 101, 109\}$, either $\bar{\rho}_{t,\mathfrak{p}}$ is reducible, or it is congruent to the representation of a Hilbert newform over K with complex multiplication, or it is congruent to $J_s[\mathfrak{p}]$ or $J_s[\mathfrak{p}']$ for one of the two parameters

$$s = -\tfrac{1}{8} \quad \text{and} \quad s = \tfrac{9}{8},$$

which come from the identities $1^5 + 2^3 = 3^2$ and $(-3)^5 + 6^3 = (-3)^3$ (Section 2.4). We call these the *special parameters*, and say that $\bar{\rho}_{t,\mathfrak{p}}$ is congruent to J_s if $J_t[\mathfrak{p}] \cong J_s[\mathfrak{p}]$ or $J_t[\mathfrak{p}] \cong J_s[\mathfrak{p}']$ as G_K-modules. An isomorphism $J_t[\mathfrak{p}] \cong J_s[\mathfrak{p}]$ that respects the real multiplication is a congruence in the *direct orientation*, and an isomorphism $J_t[\mathfrak{p}] \cong J_s[\mathfrak{p}']$ that conjugates it by σ is one in the *conjugate orientation* (Definition 4.5). The newforms attached to $J_{-1/8}$ and $J_{9/8}$ have level $3^3(\sqrt{5})^3$, one of the levels the method must treat [33, §1.2], so they cannot be removed by comparing levels. Pacetti and Villagra Torcomian remove the congruence with J_s when $3 \nmid Y$ by the local type at 3 [33, Theorem 7.18]. Their Theorem C asserts that, under a conjecture on large images of Galois representations [33, Conjecture 1] (stated as (LI) in Section 2.5), there is no primitive solution with $3 \nmid Y$ for $p \notin \mathcal{P}$ larger than an unspecified constant. The proof of Theorem C also needs a further large-image hypothesis, for the J_t that are isogenous over $\overline{\mathbb{Q}}$ to the square of an elliptic curve without complex multiplication (Remark 6.16). For solutions with $3 \mid Y$, the congruence with J_s is the main obstruction left by their method. As a corollary of Theorem A they state that for every prime $p \notin \{2, 7, 11, 13, 19, 29, 31, 41, 61\}$ there is no primitive solution in which Z is odd and divisible by 3 or by 5 [33, Theorem B] (Theorem 2.17). For $p = 7$, [24, Theorem 1.3] shows that (1.1) has no primitive solution, assuming the results of Dahmen and Siksek [10] and of Putz [34], by which a primitive solution determines one of seven explicit septic number fields; [24] excludes each of these seven fields. Chocian [9] also proves this, from the same results of Dahmen and Siksek and of Putz, excluding six of the fields through a plane quartic of genus 3 and the seventh with results of [33], level lowering over K and a Hecke comparison at 29.

The preprint [33] has not appeared in a refereed journal, and its proofs rely in turn on a preprint of Golfieri Madriaga and Pacetti [18] and on a preprint of Golfieri Madriaga, Pacetti and Rodriguez Villegas [19] (Section 2.5). Theorems 1, 2 and 3 below use no statement of [33]. The results that do are in Section 6 and in the accompanying Supplement, and each names the statements of [33] it assumes by the labels of Section 2.5, which Table 1 below summarizes.

This paper studies the congruence with J_s, and with forms with complex multiplication, through the local representation at the prime $\sqrt{5}$ of K, and records the consequences. The comparison of inertia fields at $\sqrt{5}$ on which Theorem 1 rests also applies to the equation $x^p + y^p = z^5$, for which Chen and Koutsianas [8] carry out Darmon's program with a Frey hyperelliptic curve over K, and which is treated in [23].

1.1. **Ceccon's results.** For $p > 109$ and solutions with $3 \mid Y$ and $5 \nmid Y$, Ceccon [6, Proposition 2.1] shows, using results of [33], that X and Z are odd, Y is even, $5 \nmid Z$, and $\bar\rho_{t,\mathfrak{p}}$ is absolutely irreducible of level $3^3(\sqrt{5})^3$ and congruent to $J_{-1/8}$ or $J_{9/8}$. He deduces lower bounds for the prime divisors of Z and for $|Z|$ [6, Theorem 1.1 and Corollary 1.2], and states that, for solutions with $3 \mid Y$ and $p > 109$, $\bar\rho_{t,\mathfrak{p}}$ is irreducible when the conductor exponents at 3 and $\sqrt{5}$ are both 2 [6, Lemma 4.3]. He also shows that solutions with $3 \mid Y$ have $X \not\equiv \pm 4 \pmod 9$, for p large under [33, Conjecture 1] ([5, Theorem 1.1]), and for $p > 109$ from [33, Theorem 7.8] in his working notes [7]. For solutions with $3 \mid Y$, these notes also state, without proof, four facts proved here: a congruence with J_s forces $t \bmod 25 \in \mathcal{A}$ (Theorem 1(a)); on each such class the local representation of J_t at $\sqrt{5}$ agrees, up to conjugating the coefficients by σ, with that of exactly one of $J_{-1/8}$ and $J_{9/8}$, and the two have opposite orientations of the real multiplication (Theorem 3.7, and by Proposition 4.15(a) the local representations of $J_{-1/8}$ and $J_{9/8}$ at $\sqrt{5}$ differ by this conjugation and an unramified quadratic twist); these orientations tell the two special parameters apart (Section 4); and for one class of solutions and $p \equiv 19, 29, 31, 41 \pmod{60}$ the factors by which a congruence multiplies the Weil pairings at 3 and at $\sqrt{5}$ do not match (Theorem 3(a)). Theorem 6.17 assumes $5 \nmid Z$, which [6, Proposition 2.1] proves for $p > 109$ and solutions with $3 \mid Y$ and $5 \nmid Y$; to the conclusions of that proposition it adds $5 \nmid X$ and $t \bmod 25 \in \mathcal{A}$, and it also holds for the primes $p \notin \mathcal{P}$ below 109. Proposition 6.4 shows that $\bar\rho_{t,\mathfrak{p}}$ is irreducible, the conclusion of [6, Lemma 4.3], for every solution with $3 \mid Y$, every $p \geq 7$ and all conductor exponents, assuming only the statement (T2.1) of Section 2.5 (see Table 1).

1.2. **Results.** Write $\mathcal{A} = \{3, 8, 9, 13, 14, 19, 23, 24\}$, $\mathcal{B} = \{7, 12, 17, 22\}$ and $\mathcal{T} = \{2, 4, 18\}$. If $5 \nmid XYZ$, the residue of t modulo 25 lies in one of these three sets, which are distinguished by the field generated over the maximal unramified extension of $\mathbb{Q}_5$ by the Weierstrass points of C_t (Definition 3.1 and Proposition 3.5). Both special parameters lie in $\mathcal{A}$, as $-1/8 \equiv 3$ and $9/8 \equiv 23 \pmod{25}$. The proofs of Theorems 1, 2 and 3 rest on local computations at 3 and $\sqrt{5}$, with the criteria of Liu [28] and of Dokchitser, Dokchitser, Maistret and Morgan [13] and the results of Serre and Tate [40], and on computations at auxiliary primes.

Theorem 1. *Let $p \geq 7$ be prime, $\mathfrak{p}$ a prime of K above p, (X, Y, Z) a primitive solution of (1.1) and $t = -X^5/Y^3$.*

- *(a) If $\bar\rho_{t,\mathfrak{p}}$ is congruent to J_s for a special parameter s, then $5 \nmid XYZ$ and $t \bmod 25 \in \mathcal{A}$; in particular $X \equiv Y^3$ or $X \equiv 2Y^3 \pmod 5$.*
- *(b) If $5 \nmid XYZ$ and $t \bmod 25 \in \mathcal{A}$, then $\bar\rho_{t,\mathfrak{p}}$ is not congruent to the residual representation of any Hilbert newform over K with complex multiplication whose level is divisible only by 3 and $\sqrt{5}$.*
- *(c) For $5 \nmid XYZ$ and $t \bmod 25 \in \mathcal{A}$, the local representation of J_t at $\sqrt{5}$ agrees, up to conjugating the coefficients by σ, with that of exactly one J_s, which depends only on $t \bmod 25$: it is $J_{-1/8}$ for $t \equiv 3, 8, 9, 24$ and $J_{9/8}$ for $t \equiv 13, 14, 19, 23 \pmod{25}$.*

Theorem 2. *Let $p \geq 17$ be prime, $\mathfrak{p}$ a prime of K above p, and (X, Y, Z) a primitive solution of (1.1).*

(a) *If* $5 \nmid XYZ$ *and* $t \equiv 9, 14, 19, 24 \pmod{25}$*, then* $\bar{\rho}_{t,\mathfrak{p}}$ *is congruent to neither* $J_{-1/8}$ *nor* $J_{9/8}$*. Consequently a congruence of* $\bar{\rho}_{t,\mathfrak{p}}$ *with some* J_s *requires* $5 \nmid XYZ$ *and* $t \equiv 3, 8, 13, 23 \pmod{25}$*, and is with* $J_s[\mathfrak{p}]$*.*

(b) *For* $c \in \{3, 9\}$*, the semisimplification of* $\bar{\rho}_{t,\mathfrak{p}}$ *is not isomorphic to that of the mod-*$\mathfrak{p}$ *representation of* $G^{\sigma}_{J_{0,c}}$*, the conjugate by* σ *of the newform* $G_{J_{0,c}}$ *of* $J_{0,c} = \mathrm{Jac}(V^2 = U^6 + 12cU)$ *(Definition 4.4), which has complex multiplication by* $\mathbb{Q}(\zeta_5)$*.*

Theorem 3. *Let* (X, Y, Z) *be a primitive solution of* (1.1) *with* $3 \mid Y$*,* $\mathfrak{p}$ *a prime of* K *above* p*, and* s *a special parameter.*

(a) *If* $p \equiv 19, 29, 31, 41 \pmod{60}$*, then* $\bar{\rho}_{t,\mathfrak{p}}$ *is not congruent to* J_s*.*

(b) *If* $p \geq 7$*,* $p \equiv \pm 2 \pmod 5$*, and either* $(3/p) = -1$ *and* $X \equiv \pm 1 \pmod 9$*, or* $(3/p) = 1$ *and* $X \equiv \pm 2 \pmod 9$*, then there is no* G_K*-isomorphism* $J_t[p] \to J_s[p]$ *that is* $\mathcal{O}_K/p$*-linear or semilinear for the Frobenius of* $\mathcal{O}_K/p$*.*

For p inert in K, so that $\mathfrak{p} = p\mathcal{O}_K$ and σ induces the Frobenius of $\mathcal{O}_K/p$, every congruence of $\bar{\rho}_{t,\mathfrak{p}}$ with J_s yields an isomorphism of one of the two kinds in (b) (§4.2), so (b) says that $\bar{\rho}_{t,\mathfrak{p}}$ is not congruent to J_s.

Under the statements of [33] labeled in Section 2.5, the elimination in the proof of [33, Theorem A], combined with Theorems 1, 2 and 3, gives the following. Section 6 states each part with its hypotheses, Table 1 lists the statements of [33] each part assumes, and Table 7 lists, class by class, what is excluded and by which result.

Theorem 4. *Assume the statements of* [33] *that Table 1 lists for each part. Let* $p \notin \mathcal{P}$ *be prime,* $\mathfrak{p}$ *a prime of* K *above* p*, and* (X, Y, Z) *a primitive solution.*

(a) *If* $5 \nmid XYZ$*, then* $t \equiv 2, 3, 4, 8, 13, 18$ *or* $23 \pmod{25}$*; if* $5 \mid X$*, then* $Y \not\equiv \pm 6, \pm 8, \pm 9, \pm 12 \pmod{25}$ *(Theorem 6.25).*

(b) $3 \mid XYZ$ *(Theorem 6.20).*

(c) *If* $3 \mid Y$ *and* $5 \nmid YZ$*, then* $5 \nmid X$*,* $X \not\equiv \pm 4 \pmod 9$*,* $2 \mid Y$*,* $t \bmod 25 \in \mathcal{A}$ *and* $\bar{\rho}_{t,\mathfrak{p}}$ *is congruent to some* J_s *(Theorem 6.17).*

(d) *If* $p \equiv 19, 29, 31, 41 \pmod{60}$ *(so that* $p \geq 139$*, the smaller such primes lying in* $\mathcal{P}$*), then either* $30 \mid Z$ *and* $\bar{\rho}_{t,\mathfrak{p}}$ *is reducible, or* $6 \mid X$ *and* $\bar{\rho}_{t,\mathfrak{p}}$ *is congruent to a form with complex multiplication by* $\mathbb{Q}(\zeta_5)$*, or* $5 \mid Y$ *and it is congruent to a form with complex multiplication by* $\mathbb{Q}(\sqrt{5}, \sqrt{-3})$*; each class contains a trivial solution, one with* $XYZ = 0$ *(Theorem 6.21). For these* p *the Supplement reduces the three classes to rational points on modular curves over* K *(Theorem S1.12).*

(e) *If* $3 \mid Z$ *or* $5 \mid Z$*, then* $30 \mid Z$ *and* $\bar{\rho}_{t,\mathfrak{p}}$ *is reducible, with semisimplification* $\theta_{15} \oplus \theta_{15}\bar{\chi}_p$*, where* θ_{15} *is the character of* $\mathbb{Q}(\zeta_{15})^+/K$ *and* $\bar{\chi}_p$ *the mod-*p *cyclotomic character; this holds for every prime* $p \geq 7$ *outside* $\{7, 11, 13, 19, 29, 31, 41, 61\}$ *(Theorem 6.23).*

In (a), the classes $t \equiv 9, 14, 19, 24$ are removed by Theorem 2(a), the classes $t \equiv 7, 12, 17, 22$ by Theorem 2(b) and the local types at $\sqrt{5}$ and 3 (by Lemma 6.12, the type at 3 leaves only the two forms of Theorem 2(b) and the newform of $J_{0,1}$, the Jacobian of the trivial solution $X = 0$), and the classes with $5 \mid X$, those with $Y^4 \equiv 11$ or $21 \pmod{25}$, by a comparison with the Jacobians $J_{0,c}$ at $\sqrt{5}$ (Proposition 3.10); Theorem C of Pacetti and Villagra Torcomian already asserts this for the last two kinds under (LI), for p large; its proof also needs a further large-image hypothesis (Remark 6.16). Parts (b), (c) and (e) use that $\bar{\rho}_{t,\mathfrak{p}}$ is irreducible unless $30 \mid Z$ (Proposition 6.4), in place of [33, Corollary 7.7], and

TABLE 1. The statements of [33] assumed in each part of Theorem 4, with the labels of Section 2.5; for (P7.4), the entry gives the part of [33, Proposition 7.4] used, at $\ell = 3$.

Label	Statement of [33]	(a)	(b)	(c)	(d)	(e)
(LL)	level lowering: an irreducible $\bar\rho_{t,\mathfrak{p}}$ arises from a Hilbert newform of parallel weight 2 and trivial character whose level is the conductor of $\bar\rho_{t,\mathfrak{p}}$	•	•	•	•	•
(Ex_0)	$\varepsilon_3 \in \{2,3\}$, and $\varepsilon_3 = 2$ if $3 \mid Z$	•			•	•
(EL)	the newforms left by the elimination in the proof of [33, Theorem A]	•	•	•	•	•
(T2.1)	multiplicative reduction at the primes dividing Z but not 15; $\bar\rho_{t,\mathfrak{p}}$ unramified outside $15p$ and finite above p	•	•	•	•	•
(P7.4)	(a) potentially multiplicative reduction at 3 if $v_3(t-1) > 3$	(a)			(a)	(a)

part (e) contains [33, Theorem B] for $p \geq 7$ and adds to it $15 \mid Z$ and the reducibility of $\bar\rho_{t,\mathfrak{p}}$ (Remark 6.24).

1.3. **The ideas of the proofs.** *Theorem 1.* When $5 \nmid YZ$, the six roots of the sextic split 5-adically into one root and a cluster of five, and the field the cluster generates over the maximal unramified extension of $\mathbb{Q}_5(5^{1/4})$ takes one of exactly three values, according to t mod 25 (to Y mod 25 when $5 \mid X$): that extension itself, or one of two cyclic extensions of degree 5 of it. The special parameters give one of the latter, and the trivial solution $X = 0$, with $t = 0$, whose Jacobian has complex multiplication by $\mathbb{Q}(\zeta_5)$, gives the other. A congruence modulo a prime $p \geq 7$ forces the fields cut out by inertia at $\sqrt{5}$ on the two Jacobians to agree. This comparison of inertia fields is the method of Billerey, Chen, Dieulefait and Freitas [2, §3], used at the prime 3 in [33, Theorem 7.18]. For (c), $J_{-1/8}$ and $J_{9/8}$ have the same local representations at 2, at 3 and at the real places, while at $\sqrt{5}$ they differ, up to conjugating the coefficients by σ, by the unramified quadratic twist (Theorem 3.7 and Proposition 4.15).

Theorem 2. Here the real multiplication enters. Each J_t carries the action ι of $\mathcal{O}_K$ and its conjugate $\iota \circ \sigma$. We fix ι once for the whole family, by its eigenvalues on the differentials du/v and $u\,du/v$ (Definition 4.2). Then a congruence of $J_t[\mathfrak{p}]$ with J_s either respects ι, giving an isomorphism $J_t[\mathfrak{p}] \cong J_s[\mathfrak{p}]$, or conjugates it by σ, giving an isomorphism $J_t[\mathfrak{p}] \cong J_s[\mathfrak{p}']$, and the local computation at $\sqrt{5}$ decides which: for $t \equiv 9, 14, 19, 24 \pmod{25}$ only $J_s[\mathfrak{p}']$ is possible (Proposition 4.15). Such an isomorphism would make the traces of Frobenius of J_t and J_s at a prime $\mathfrak{q}$ of K above an auxiliary prime q conjugate modulo $\mathfrak{p}$, and a computation over $\mathbb{F}_q$ with the Weil bound shows that they are not. The auxiliary prime must split in K, satisfy $16q < p^2$, and have $a_{\mathfrak{q}}(J_s)$ irrational, so that it differs from its conjugate. The prime $q = 19$ serves for $p \geq 23$ and $q = 11$ for $p = 17, 19$, while at $q = 29$ both $a_{\mathfrak{q}}(J_s)$ are rational and the argument fails (Remark 4.18). Part (b) is proved in the same way at 11.

Theorem 3. An isomorphism $\phi\colon J_t[\mathfrak{p}] \to J_s[\mathfrak{p}]$ or $J_s[\mathfrak{p}']$ multiplies the Weil pairings by a scalar, its *multiplier* c: $\langle \phi x, \phi y\rangle = c\langle x, y\rangle$. This scalar can be read off locally at any place of potentially good reduction. At 3 it is 3 up to squares, and at $\sqrt{5}$ it is 1, so the isomorphism cannot exist when 3 is not a square in the residue field of $\mathfrak{p}$, which happens exactly for $p \equiv 19, 29, 31, 41 \pmod{60}$. This is the symplectic argument of Halberstadt and Kraus [22],

used by Freitas [15] for $x^3+y^3=z^p$, carried to abelian surfaces with real multiplication. For p inert in K every element of $\mathbb{F}_p^\times$ is a square in $\mathcal{O}_K/p$, and part (b) uses instead the square class over $\mathbb{Q}$ of the multiplier of an isomorphism that is linear or semilinear, with the local root number at 3 of an elliptic curve (Section 5.5).

Theorem 4. By (LL), (Ex) and (EL), for $p \notin \mathcal{P}$ an irreducible $\bar\rho_{t,\mathfrak{p}}$ is congruent to J_s or to one of finitely many newforms with complex multiplication. For $5 \nmid XYZ$, Theorem 1 says which, according to the class of t modulo 25, and Theorem 2 and the local types at $\sqrt{5}$ and 3 of the newforms of the Jacobians $J_{0,c}$ then remove the classes listed after Theorem 4. For $3 \nmid XYZ$, the field cut out by inertia at 3 separates J_t from the Jacobian of the trivial solution $Y=0$. For $p \equiv 19, 29, 31, 41 \pmod{60}$, Theorem 3(a), with Lemma 6.18(d) when $3 \nmid Y$, removes the congruence with J_s, and what remains are three classes of solutions, each containing a trivial solution, so we do not expect local arguments to exclude them (Theorem 6.21).

1.4. **Outline.** Section 2 recalls the Frey curve, the real multiplication and the special parameters, and states the results of [33] that are used, with their labels. Section 3 proves Theorem 1, Section 4 proves Theorem 2, and Section 5 proves Theorem 3. Section 6 proves the results that use [33]. The Supplement is a separate document accompanying this paper, with its own numbering (prefix S); it contains, for $p \equiv 19, 29, 31, 41 \pmod{60}$, further results that use [33], among them the reduction of the equation to rational points on modular curves, and the computations on which these rest. The proofs of Theorems 1, 2, 3 and 4 do not depend on it. Appendix A lists the computations on which the proofs depend. The programs and their outputs are in [25].

1.5. **Notation.**

K, $\mathcal{O}_K$, σ	$\mathbb{Q}(\sqrt{5})$, its ring of integers, its nontrivial automorphism
F, F^{ur}, I_F	$K_{\sqrt{5}} = \mathbb{Q}_5(\sqrt{5})$, its maximal unramified extension, its inertia group
(X,Y,Z), t	a primitive solution of $X^5+Y^3=Z^p$, and $t=-X^5/Y^3$
C_t, J_t	the Frey curve $v^2=5u^6-12u^5+10tu^3+t^2$ and its Jacobian (Section 2.2)
$\mathfrak{p}$, $\mathfrak{p}'$	a prime of K above p, and $\sigma(\mathfrak{p})$
$\rho_{t,\lambda}$, $\bar\rho_{t,\mathfrak{p}}$	the λ-adic representation of J_t, and $J_t[\mathfrak{p}]$
s, J_s	a special parameter $-1/8$ or $9/8$, and the Jacobian of C_s (Section 2.4)
ε_3, ε_5	the conductor exponents of $\rho_{t,\lambda}$ at (3) and $(\sqrt{5})$ (in §§2.5 and 6 also of $\bar\rho_{t,\mathfrak{p}}$)
$\mathcal{A}$, $\mathcal{B}$, $\mathcal{T}$	sets of residues of t modulo 25 (Definition 3.1)
$\mathcal{P}$	$\{2,3,5,7,11,13,19,29,31,41,61,71,79,89,101,109\}$
(LL), (Ex), ...	statements of [33] used in Section 6 (Section 2.5)

2. The Frey curve and the two special parameters

This section introduces the Frey curve C_t, its real multiplication by $\mathcal{O}_K$, the trivial solutions and the two special parameters, and states the results of [33] that are used, with the labels by which Section 6 and the Supplement refer to them. It ends with local facts at $\sqrt{5}$, 2 and 3, and a ray class group of K, used in the later sections.

2.1. **The equation.** Let $p \geq 7$ be prime. A primitive solution of

$$X^5+Y^3=Z^p \tag{2.1}$$

is a triple (X,Y,Z) of pairwise coprime nonzero integers satisfying (2.1). As 5, 3, p are odd, $(X,Y,Z) \mapsto (-X,-Y,-Z)$ permutes the primitive solutions, so we impose no sign conditions. Exactly one of X,Y,Z is even. Pacetti and Villagra Torcomian [33] write the

equation as $a^5 + b^p + c^3 = 0$; the dictionary is $(a, b, c) = (X, -Z, Y)$, and every statement of [33] quoted below is translated into X, Y, Z. We put $t = -X^5/Y^3$, so that $t - 1 = -Z^p/Y^3$ and $t \notin \{0, 1\}$.

2.2. **The Frey curve.** Let $K = \mathbb{Q}(\sqrt{5})$, $\mathcal{O}_K = \mathbb{Z}[\varphi]$ with $\varphi = (1 + \sqrt{5})/2$, and σ the nontrivial automorphism of K. For $t \neq 0, 1$ in a field of characteristic 0, and for X, Y in such a field, let

$$C_t\colon v^2 = f_t(u) \coloneqq 5u^6 - 12u^5 + 10tu^3 + t^2, \qquad \operatorname{disc}(f_t) = 2^{12}3^6 5^5\, t^8 (t-1)^2,$$

$$C_{X,Y}\colon V^2 = \mathcal{F}_{X,Y}(U) \coloneqq U^6 + 10XU^3 + 12YU + 5X^2, \quad \operatorname{disc}(\mathcal{F}_{X,Y}) = 2^{12}3^6 5^5 (X^5 + Y^3)^2,$$

and $J_t = \operatorname{Jac}(C_t)$; C_t is the curve of [33, (32), §7.1]. The polynomial identities, Igusa invariants and conductors quoted in this section were computed with PARI/GP [44] (`genus2igusa`, `genus2red`) and by symbolic computation; the programs are in [25]. We write $\mathcal{I}_2, \mathcal{I}_4, \mathcal{I}_6, \mathcal{I}_8, \mathcal{I}_{10}$ for the Igusa invariants of a curve $v^2 = f(u)$ with f of degree 6, normalized as in `genus2igusa` (which calls them $J_2, \dots, J_{10}$), so that $\mathcal{I}_{10} = 2^{-12} \operatorname{disc}(4f)$; they are 4^{2i} times the invariants J_{2i} of f in the normalization of [28], a factor that leaves unchanged the quotients of weight 0 used below.

Lemma 2.1. *If $XY \neq 0$ and $t = -X^5/Y^3$, then $(u, v) = (-X^2/(YU),\ -X^5 V/(Y^3 U^3))$ is an isomorphism $C_{X,Y} \to C_t$ over $\mathbb{Q}(X, Y)$. For $\nu \neq 0$, $(U, V) \mapsto (\nu U, \nu^3 V)$ is an isomorphism $C_{X,Y} \to C_{\nu^3 X, \nu^5 Y}$.*

Proof. One has $f_t(u) = X^{10} \mathcal{F}_{X,Y}(U)/(Y^6 U^6)$ and $\nu^6 \mathcal{F}_{X,Y}(U) = \mathcal{F}_{\nu^3 X, \nu^5 Y}(\nu U)$. □

Proposition 2.2. *Let J be J_t with $t \in \mathbb{Q} \setminus \{0, 1\}$, or $J_0 \coloneqq \operatorname{Jac}(C_{0,1})$, or $J_\infty \coloneqq \operatorname{Jac}(C_{1,0})$. There is a ring homomorphism $\iota\colon \mathcal{O}_K \to \operatorname{End}_K(J)$ such that:*

- *(a) $\iota(\varphi)^2 = \iota(\varphi) + 1$, and $\iota(\mathcal{O}_K)$ is fixed by the Rosati involution;*
- *(b) there is $\delta \in \{\pm 1\}$, the same for all these J, such that $\iota(\sqrt{5})$ acts by $\delta\sqrt{5}$ on du/v and by $-\delta\sqrt{5}$ on $u\,du/v$ (on C_t), and by $\delta\sqrt{5}$ on $U\,dU/V$ and by $-\delta\sqrt{5}$ on dU/V (on $C_{0,1}$ and $C_{1,0}$);*
- *(c) ${}^c\iota(\alpha) = \iota(\sigma(\alpha))$ for $c \in G_\mathbb{Q} \setminus G_K$ and $\alpha \in \mathcal{O}_K$.*

Proof. Kumar and Mukamel [26, Theorem 14] give, for the family $C(P, Q)\colon y^2 = z^6 + 2Pz^5 + 10Qz^3 + 10Q^2 z - 5(P-1)Q^2$, an explicit correspondence with coefficients in $K(P, Q)$ whose endomorphism T of the Jacobian over $K(P, Q)$ is Rosati-invariant and satisfies $T^2 - T - 1 = 0$; dz/y and $z\,dz/y$ are eigenforms of T, with eigenvalues independent of (P, Q) [26, §6 and the proof of Proposition 17]. The substitution $z = -6/(5u)$, $Q = (-6/5)^3/t$, $y = vz^3/t$ turns C_t into

$$C(0, Q)\colon y^2 = z^6 + 10Qz^3 + 10Q^2 z + 5Q^2, \qquad \operatorname{disc} = 200000\, Q^{10}(125Q + 216)^2,$$

and carries dz/y, $z\,dz/y$ to $\mathbb{Q}(t)^\times$-multiples of $u\,du/v$, du/v. As the line $P = 0$ is not in the discriminant locus, the Jacobian is an abelian scheme over the local ring of the (P, Q)-plane over K at the generic point of $\{P = 0\}$, a discrete valuation ring, and T extends over it [4, §1.2, Definition 1 and Proposition 8], [29, Ch. II, Proposition 6.4 and Corollary 6.6]; the extension still satisfies $T^2 - T - 1 = 0$, is self-adjoint, and has dz/y, $z\,dz/y$ as eigenforms. The same argument at the local rings of the t-line over K where C_t is smooth ($t \neq 0, 1, \infty$) gives $T \in \operatorname{End}_K(J_t)$; put $\iota(\varphi) = T$. For J_0, the family $C_{X,1}$ is isomorphic to C_{-X^5} over $K(X)$ by Lemma 2.1, which carries du/v, $u\,du/v$ to $-X^{-3}\,U\,dU/V$, $X^{-1}\,dU/V$; so T is defined on its generic fiber and extends over the local ring $A = K[X]_{(X)}$, where $C_{X,1}$ is smooth

[4, §1.2, Proposition 8], [29, Ch. II, Corollary 6.6]. As dU/V, $U\,dU/V$ form an A-basis of the differentials of the family, the extension multiplies $U\,dU/V$ by the eigenvalue of T on du/v, and dU/V by its eigenvalue on $u\,du/v$, on the generic fiber and hence at $X = 0$. For J_∞ use $C_{1,Y}$ at $Y = 0$ ($t = -1/Y^3$, $du/v = -Y^2\,U\,dU/V$, $u\,du/v = Y\,dU/V$). For (c), ${}^cT$ and $1 - T$ both act on the $\mathbb{Q}$-rational forms of (b) by the conjugates of the eigenvalues of T, so they are equal, an endomorphism being determined by its action on differentials in characteristic 0. □

For a prime ℓ, $T_\ell(J)$ is torsion-free over the product of discrete valuation rings $\mathcal{O}_K \otimes \mathbb{Z}_\ell$, hence free of rank 2. For a prime $\lambda \mid \ell$ of K let $V_\lambda(J) = T_\ell(J) \otimes_{\mathcal{O}_K \otimes \mathbb{Z}_\ell} K_\lambda$ and $\rho_{t,\lambda}\colon G_K \to \mathrm{GL}_2(K_\lambda)$ the action of G_K on $V_\lambda(J_t)$ (similarly $\rho_{0,\lambda}$, $\rho_{\infty,\lambda}$). By (a) the Weil pairing on $T_\ell(J)$ is the trace of a $K \otimes \mathbb{Q}_\ell$-bilinear alternating pairing, so $\det \rho_{t,\lambda}$ is the cyclotomic character. For a prime $\mathfrak{p}$ of K above p, with $\mathfrak{p}' = \sigma(\mathfrak{p})$, let

$$\bar{\rho}_{t,\mathfrak{p}} = J_t[\mathfrak{p}] = \{P \in J_t[p] : \iota(\alpha)P = 0 \text{ for all } \alpha \in \mathfrak{p}\},$$

of dimension 2 over $\mathcal{O}_K/\mathfrak{p}$. We write ε_3, ε_5 for the conductor exponents of $\rho_{t,\lambda}$ ($\lambda \nmid 15$) at (3) and $(\sqrt{5})$, which do not depend on λ. Where J_t has potentially good reduction this follows from the argument in the proof of Lemma 2.7; otherwise the reduction is potentially totally toric, and, as in that proof, on an inertia group I at that prime, $\rho_{t,\lambda}|_I \cong \psi \otimes \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ with ψ independent of λ and $* \neq 0$; the exponent is then 2 or 1 according as ψ is ramified or not. In Sections 2.5 and 6 and in the Supplement, ε_3 and ε_5 also denote the conductor exponents of $\bar{\rho}_{t,\mathfrak{p}}$ at these primes, which for $p \geq 7$ are those of $\rho_{t,\lambda}$ where J_t has potentially good reduction.

Lemma 2.3. *Let J be as in Proposition 2.2, and λ a prime of K above a prime $\ell \neq 3, 5$ that splits in K. If J has conductor exponents b_3, b_5 over $\mathbb{Q}$ at 3, 5, then the representation of G_K on $V_\lambda(J)$ has conductor exponents $b_3/2$ at (3) and $b_5 - 2$ at $(\sqrt{5})$.*

Proof. As ℓ splits in K, $K_\lambda = \mathbb{Q}_\ell$. By Proposition 2.2(c), $G_\mathbb{Q} \smallsetminus G_K$ exchanges the summands of $V_\ell(J) = V_\lambda(J) \oplus V_{\sigma(\lambda)}(J)$, so $V_\ell(J) \cong \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} V_\lambda(J)$, and the conductor exponent at a prime q is $\sum_{v|q} f_v n_v + 2v_q(d_K)$, where n_v is the exponent of $V_\lambda(J)$ at v. For Artin representations this is [38, Ch. VI, §3, Proposition 6(b)]; it holds for ℓ-adic representations as well, since for a representation W of G_K, by Mackey's formula, $(\mathrm{Ind}_{G_K}^{G_\mathbb{Q}} W)|_{I_q}$ is, for each $v \mid q$, a sum of f_v conjugates of $\mathrm{Ind}_{I_v}^{I_q} W$, where Serre's formula applies to the Weil–Deligne representation (whose image of inertia is finite), and $\dim(\mathrm{Ind}_{I_v}^{I_q} U)^{I_q} = \dim U^{I_v}$ (Frobenius reciprocity) takes care of the monodromy term. Here (3) is inert and $(\sqrt{5})$ ramified with $v_5(d_K) = 1$. □

Lemma 2.4. *Let J be J_t with $t \in \mathbb{Q} \smallsetminus \{0, 1\}$, J_0, J_∞, or $J_{0,c} = \mathrm{Jac}(V^2 = U^6 + 12cU)$ with $c \in \mathbb{Q}^\times$, with its real multiplication ι (Proposition 2.2; for $J_{0,c}$ as in §4.1), and let $\rho_{J,\lambda}$ be the action of G_K on $V_\lambda(J)$. Let v be a finite place of K, of residue characteristic r and residue field $\mathbb{F}_q$, at which J has potentially good reduction; for J_0, J_∞ and $J_{0,c}$, which have complex multiplication over $\mathbb{Q}(\zeta_5)$, $K(\sqrt{-3})$ and $\mathbb{Q}(\zeta_5)$ respectively, this holds at every v, by* [40, Theorem 6(a)] *over that field (Lemma 2.5; for $J_{0,c}$ the complex multiplication is through $(U, V) \mapsto (\zeta_5 U, \zeta_5^3 V)$). Let w be an element of the Weil group W_{K_v} that acts on $\overline{\mathbb{F}}_r$ by $x \mapsto x^{q^n}$, $n \in \mathbb{Z}$. Then there is $a(w) \in K$, lying in $\mathcal{O}_K$ if $n \geq 0$, such that for every prime $\ell \neq r$ the characteristic polynomial of w on the free $K \otimes \mathbb{Q}_\ell$-module $V_\ell(J)$, as a $K \otimes \mathbb{Q}_\ell$-linear map, is $x^2 - a(w)x + q^n$. In particular, for every prime $\lambda \nmid r$ of K, $\mathrm{tr}\,\rho_{J,\lambda}(w)$ is the image of $a(w)$ in K_λ and $\det \rho_{J,\lambda}(w) = q^n$: for w in the inertia group I_v the trace lies in $\mathcal{O}_K$, and at a place v of good reduction a Frobenius element Frob_v (the case $n = 1$) has characteristic*

polynomial $x^2 - a_v x + q$ with $a_v \in \mathcal{O}_K$, in both cases independently of $\lambda \nmid r$. If moreover $\rho_{J,\lambda}|_{I_v}$ is absolutely irreducible, every representation of W_{K_v} on a 2-dimensional K_λ-vector space with the trace function of $\rho_{J,\lambda}|_{W_{K_v}}$ is isomorphic to $\rho_{J,\lambda}|_{W_{K_v}}$.

Proof. Let L/K_v be a finite Galois extension over which J has good reduction, $\mathcal{N}$ the Néron model of J_L, an abelian scheme over $\mathcal{O}_L$, and $\bar{B}$ its special fiber base-changed to $\overline{\mathbb{F}}_r$. By the Néron mapping property [4, §1.2, Definition 1 and Proposition 8], [29, Ch. II, Proposition 6.4 and Corollary 6.6], $\mathrm{Gal}(L/K_v)$ acts on $\mathcal{N}$ by automorphisms of schemes compatible with its action on $\mathcal{O}_L$, and each $\iota(\alpha)$, $\alpha \in \mathcal{O}_K$, extends to an endomorphism of $\mathcal{N}$ commuting with this action (by uniqueness, as $\iota(\alpha)$ is defined over K). For $\ell \neq r$, reduction identifies $V_\ell(J)$ with $V_\ell(\bar{B})$ compatibly with ι (the reduction over L being good, the part of $T_\ell(J)$ identified in [21, Exp. IX, (4.2.6)] is all of it), and the action of G_{K_v} on $V_\ell(J)$ with the action deduced by transport of structure from its action on $\mathcal{N}$ and on $\overline{\mathbb{F}}_r$ [21, Exp. IX, 4.2, (4.2.6)].

Let $n \geq 0$. By [21, Exp. IX, Lemme 4.3.2, (4.3.3)–(4.3.5)], the automorphism of $\bar{B}(\overline{\mathbb{F}}_r)$ induced by w is the map on points of an $\overline{\mathbb{F}}_r$-endomorphism F_w of the abelian variety $\bar{B}$, the composite of the q^n-th power map of the underlying scheme with the automorphism of $\bar{B}$ defined by w; F_w commutes with $\iota(\mathcal{O}_K)$, as both factors do. For $\alpha \in \mathcal{O}_K$, $\iota(\alpha)F_w$ is an endomorphism of $\bar{B}$, so its characteristic polynomial on $V_\ell(\bar{B})$ has integer coefficients independent of ℓ [30, §19, Theorem 4]. Let $a_\ell \in K \otimes \mathbb{Q}_\ell$ be the trace of w on the free $K \otimes \mathbb{Q}_\ell$-module $V_\ell(J)$. Then $\mathrm{Tr}_{K\otimes\mathbb{Q}_\ell/\mathbb{Q}_\ell}(\alpha a_\ell)$ is the trace of $\iota(\alpha)F_w$ on $V_\ell(\bar{B})$, an integer independent of ℓ, for every $\alpha \in \mathcal{O}_K$. As the trace form of K is nondegenerate, $a_\ell =: a(w)$ lies in K and does not depend on ℓ. Its image in each K_λ is a sum of two eigenvalues of F_w, which are roots of a monic polynomial with integer coefficients, so $a(w) \in \mathcal{O}_K$. The determinant is the cyclotomic character, which is q^n at w (Section 2.2; for $J_{0,c}$, ι is Rosati-invariant as the specialization of the Rosati-invariant ι of the family of §4.1). If $n < 0$, apply this to w^{-1}: a 2×2 matrix M satisfies $\mathrm{tr}\, M = \det M \cdot \mathrm{tr}\, M^{-1}$, so $a(w) = q^n a(w^{-1}) \in K$. The statements for $\rho_{J,\lambda}$ follow, as $V_\lambda(J) = V_\ell(J) \otimes_{K\otimes\mathbb{Q}_\ell} K_\lambda$.

For the last assertion, let $\rho = \rho_{J,\lambda}|_{W_{K_v}}$, ρ' a representation with the same trace, and $\mathfrak{a}$ the kernel of ρ on the group algebra $E = K_\lambda[W_{K_v}]$. For $x \in \mathfrak{a}$ and $k \geq 1$, $\mathrm{tr}\, \rho'(x^k) = \mathrm{tr}\, \rho(x^k) = 0$, so $\rho'(x)$ is nilpotent (K_λ has characteristic 0), and the ideal $\rho'(\mathfrak{a})$ lies in the radical of $\rho'(E)$. Hence the semisimplification of ρ' is a module over $E/\mathfrak{a}$, which is $\mathrm{End}(K_\lambda^2)$ by Burnside's theorem as ρ is absolutely irreducible; so it is isomorphic to ρ, which is irreducible, and $\rho' \cong \rho$. □

2.3. **The trivial solutions.** The trivial solutions ($XYZ = 0$, $\gcd(X, Y, Z) = 1$) are $(0, \pm 1, \pm 1)$ with $t = 0$, $(\pm 1, 0, \pm 1)$ with $t = \infty$, and $(\pm 1, \mp 1, 0)$ with $t = 1$. The first two give $C_{0,\pm 1} \cong C_{0,1}$ and $C_{\pm 1,0} \cong C_{1,0}$ (Lemma 2.1, $\nu = -1$).

Lemma 2.5. *(a) $J_0 = \mathrm{Jac}(V^2 = U^6 + 12U)$ has complex multiplication by $\mathbb{Q}(\zeta_5) \supset K$, defined over $\mathbb{Q}(\zeta_5)$; for $\lambda \nmid 15$, $\rho_{0,\lambda} \otimes \overline{K}_\lambda$ is induced from a character of $G_{\mathbb{Q}(\zeta_5)}$, and $\rho_{0,\lambda}$ has conductor $3^2(\sqrt{5})^3$.*

(b) $J_\infty = \mathrm{Jac}(V^2 = U^6 + 10U^3 + 5)$ has complex multiplication by $K(\sqrt{-3})$, defined over $K(\sqrt{-3})$, with CM type induced from $\mathbb{Q}(\sqrt{-15})$; so J_∞ is not absolutely simple: $J_{\infty,\overline{\mathbb{Q}}}$ is isogenous to E^2 for an elliptic curve E with complex multiplication by $\mathbb{Q}(\sqrt{-15})$, and $\mathrm{End}^0(J_{\infty,\overline{\mathbb{Q}}}) \cong M_2(\mathbb{Q}(\sqrt{-15}))$. For $\lambda \nmid 15$, $\rho_{\infty,\lambda} \otimes \overline{K}_\lambda$ is induced from a character of $G_{K(\sqrt{-3})}$, and $\rho_{\infty,\lambda}$ has conductor $3^3(\sqrt{5})^2$.

(c) The fiber at $t = 1$ is $v^2 = (u^2 - u - 1)^2(5u^2 - 2u + 1)$, a rational curve with nodes at $u = \varphi$ and $u = \sigma(\varphi)$, whose branches are defined over $K(\sqrt{3\sqrt{5}\varphi}) = \mathbb{Q}(\zeta_{15})^+$.

Proof. (a) The automorphism $\alpha(U, V) = (\zeta_5 U, \zeta_5^3 V)$ multiplies dU/V, $U\,dU/V$ by ζ_5^{-2}, ζ_5^{-1}, so its eigenvalues on $H^1(J_0)$ are the primitive fifth roots of unity and $\mathbb{Q}[\alpha] \cong \mathbb{Q}(\zeta_5)$. By Proposition 2.2(b), α and $\iota(\varphi)$ are diagonal in the same basis of differentials, so their commutator acts by 0 on differentials and is 0, an endomorphism being determined by its action on differentials in characteristic 0. As $H^1(J_0(\mathbb{C}), \mathbb{Q})$ is free of rank one over $\mathbb{Q}[\alpha] \cong \mathbb{Q}(\zeta_5)$, the commutant of $\mathbb{Q}[\alpha]$ in $\mathrm{End}_{\mathbb{Q}} H^1(J_0(\mathbb{C}), \mathbb{Q})$ is $\mathbb{Q}[\alpha]$; so $\iota(\varphi) \in \mathbb{Q}[\alpha]$, and $\iota(K)$ is the real subfield of $\mathbb{Q}[\alpha]$. The CM type $\{\zeta_5 \mapsto \zeta_5^{-2}, \zeta_5 \mapsto \zeta_5^{-1}\}$ is primitive, as $\mathbb{Q}(\zeta_5)$ has no imaginary quadratic subfield, so J_0 is absolutely simple and $\mathrm{End}^0(J_{0,\overline{\mathbb{Q}}}) = \mathbb{Q}(\zeta_5)$ [41, §8.2], [29, Ch. I, Propositions 3.12 and 3.13]. Hence $V_\lambda(J_0)$ is free of rank one over $\mathbb{Q}(\zeta_5) \otimes_K K_\lambda$, $G_{\mathbb{Q}(\zeta_5)}$ acts on it through a character, and $\rho_{0,\lambda} \otimes \overline{K}_\lambda$ is induced. (b) The automorphism $\alpha(U, V) = (\zeta_3 U, V)$ multiplies dU/V, $U\,dU/V$ by ζ_3, ζ_3^2, so $\alpha^2 + \alpha + 1 = 0$, and α commutes with $\iota(\varphi)$ as in (a); so $\mathbb{Q}[\iota(\varphi), \alpha]$ is a nonzero quotient of the field $K \otimes \mathbb{Q}(\zeta_3) = K(\sqrt{-3})$, hence isomorphic to it, and $V_\lambda(J_\infty)$ is free of rank one over $K(\sqrt{-3}) \otimes_K K_\lambda$, as $H^1(J_\infty(\mathbb{C}), \mathbb{Q})$ is free of rank one over $K(\sqrt{-3})$. By Proposition 2.2(b), $\iota(\sqrt{5})$ has different eigenvalues on dU/V and $U\,dU/V$, and so has $\sqrt{-3} = 2\alpha + 1$; so the two embeddings of the CM type agree on $\sqrt{-15} = \sqrt{5}\sqrt{-3}$, the type is induced from $\mathbb{Q}(\sqrt{-15})$, and $J_{\infty,\overline{\mathbb{Q}}}$ is isogenous to the square of an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-15})$ [41, §8.2], [29, Ch. I, proof of Proposition 3.13]. For the conductors, a computation (item C1; the computations are numbered as items in Table 8 of Appendix A) gives conductors $3^4 \cdot 5^5$ for $C_{0,1}$ and $3^6 \cdot 5^4$ for $C_{1,0}$, so both have good reduction at 2 and $(b_3, b_5) = (4, 5)$, $(6, 4)$; apply Lemma 2.3 for λ above a prime split in K, and for the other λ the argument in the proof of Lemma 2.7, as J_0 and J_∞, having complex multiplication, have potentially good reduction at 3 and $\sqrt{5}$. This agrees with [33, Lemmas 4.4 and 4.5]. (c) The node at $u = u_0 \in \{\varphi, \sigma(\varphi)\}$ has branches $v = \pm(u - u_0)(u_0 - \sigma(u_0))\sqrt{5u_0^2 - 2u_0 + 1}$, and $(\varphi - \sigma(\varphi))^2(5\varphi^2 - 2\varphi + 1) = 15(\varphi + 2) = 5 \cdot 3\sqrt{5}\varphi$. Of the three quadratic subextensions of $\mathbb{Q}(\zeta_{15})/K$, namely $K(\sqrt{-3})$, $\mathbb{Q}(\zeta_5) = K(\sqrt{-\sqrt{5}\varphi})$ and $K(\sqrt{3\sqrt{5}\varphi})$, only the last is totally real. □

2.4. **The special parameters.** The integer solutions $1^5 + 2^3 = 3^2$ and $(-3)^5 + 6^3 = (-3)^3$ of $X^5 + Y^3 = Z^n$ $(n = 2, 3)$ have $t = -1/8$ and $t = 9/8$. In the form of [33, Example 5.2, Table 7.3] they are $(-1)^5 + 3^2 + (-2)^3 = 0$ and $3^2 \cdot 1^5 + (-1) + (-2)^3 = 0$, which Pacetti and Villagra Torcomian call ghost solutions of their equation (2) [33, §5]. We call $-1/8$ and $9/8$ the *special parameters*, and write s for either. By Lemma 2.1,

$$C_{-1/8} \cong C_{1,2} \colon V^2 = U^6 + 10U^3 + 24U + 5, \qquad C_{9/8} \cong C_{-3,6} \colon V^2 = U^6 - 30U^3 + 72U + 45.$$

Definition 2.6. Let $\mathfrak{p}$ be a prime of K above $p \geq 7$ and s a special parameter. We say that $\bar{\rho}_{t,\mathfrak{p}}$ *is congruent to* J_s if $J_t[\mathfrak{p}] \cong J_s[\mathfrak{p}]$ or $J_t[\mathfrak{p}] \cong J_s[\mathfrak{p}']$ as $\mathbb{F}_p[G_K]$-modules.

Lemma 2.7. *For $\lambda \nmid 15$, $\rho_{s,\lambda}$ has conductor $3^3(\sqrt{5})^3$. At (3) and $(\sqrt{5})$, J_s has potentially good reduction and the image of inertia is finite of order divisible by no prime other than $2, 3, 5$. For every prime $\mathfrak{p}$ above $p \geq 7$, $\bar{\rho}_{s,\mathfrak{p}}$ has conductor exponent 3 at (3) and at $(\sqrt{5})$, and is irreducible on an inertia group at (3).*

Proof. By computation (item C1), $C_{1,2}$ and $C_{-3,6}$ have conductor $3^6 \cdot 5^5$ over $\mathbb{Q}$ (so J_s has good reduction at 2), so $\varepsilon_3 = \varepsilon_5 = 3$ for λ above a prime split in K (Lemma 2.3), as in

[33, Lemmas 5.6, 5.7, Table 7.3]. Let $v \in \{(3), (\sqrt{5})\}$. If J_s did not have potentially good reduction at v, the semistable reduction of J_s over a finite extension would have a nonzero toric part, whose character group is a torsion-free $\mathcal{O}_K$-module, hence of rank $2 = \dim J_s$; then inertia at v would act through $\psi \otimes \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ with $\psi^2 = \det = 1$ and ψ independent of λ [21, Exp. IX, 2.3–2.4, 3.5, 3.6, 4.1–4.2], tamely as the residue characteristic of v is odd, so with conductor exponent at most 2. So the reduction is potentially good, and inertia at v acts on $V_\ell(J_s)$ through a finite group Φ, the same for all $\ell \neq 3, 5$, whose elements have characteristic polynomials in $\mathbb{Z}[x]$ of degree 4, independent of ℓ [40, §2]; an element of prime order r has $r - 1 \leq 4$. The conductor exponent at v of $V_\ell(J_s)$, as a $\mathbb{Q}_\ell$-representation of G_{K_v}, is determined by the character of Φ and the ramification filtration, so it does not depend on ℓ. For ℓ split in K it is the sum of the exponents of $\rho_{s,\lambda}$ and $\rho_{s,\sigma(\lambda)}$, that is 6 (Lemma 2.3 applies to both); for ℓ inert, $V_\ell(J_s) = V_\lambda(J_s)$ has dimension 2 over K_λ, so $\rho_{s,\lambda}$ has exponent $6/2 = 3$. Hence $\varepsilon_3 = \varepsilon_5 = 3$ for every $\lambda \nmid 15$. As $p \nmid |\Phi|$, reduction preserves the invariants and the Swan conductor, so $\bar{\rho}_{s,\mathfrak{p}}$ has the same exponents. If it were reducible on inertia at (3), it would be $\chi \oplus \chi^{-1}$ there (it is semisimple as $p \nmid |\Phi|$, and the determinant is unramified), of even exponent $2a(\chi)$. □

So $J_s[\mathfrak{p}]$ is irreducible. By [33, Theorem 2.4(1)], J_s is modular: $\rho_{s,\lambda} \cong \rho_{g_s,\lambda}$ for a Hilbert newform g_s over K of parallel weight 2 and level $3^3(\sqrt{5})^3$. The forms $g_{-1/8}$ and $g_{9/8}$ are the two newforms of that level that survive the elimination of [33] (Remark 2.14; [33, §1.2]).

2.5. **Results of Pacetti and Villagra Torcomian.** The Jacobian of C_t realizes over K, up to a Tate twist, the hypergeometric motive $\mathcal{H}^+(t)$ [33, §§2.2, 7.1], so their representation $\rho^+_{\mathfrak{p}}$ is $\rho_{t,\mathfrak{p}}$, that is, $\rho_{t,\lambda}$ for $\lambda = \mathfrak{p}$. We use the version arXiv:2512.17845v1 of [33]. Its proofs in turn cite [18] (behind their Theorems 2.1 and 2.4, which are used for their Theorem 7.8) and the preprint [19] (behind their Proposition 3.2, hence their Lemma 7.3, and behind the trace formulas used in their elimination). Throughout, (X, Y, Z) is a primitive solution, $t = -X^5/Y^3$, and $\mathfrak{p} \mid p$.

Theorem 2.8 ([33, Theorem 2.1(2)–(4)]). *J_t has multiplicative reduction at every prime of K dividing Z and not 15. The representation $\bar{\rho}_{t,\mathfrak{p}}$ is unramified outside $15p$ and finite at the primes above p.*

Theorem 2.9 ([33, Lemma 7.3]). *Let $t \in \mathbb{Q} \smallsetminus \{0, 1\}$, $A_t\colon y^2 + 3xy + ty = x^3$, and χ_5 the mod-5 cyclotomic character, which on G_K is the character of $\mathbb{Q}(\zeta_5)/K$. Then $J_t[(\sqrt{5})]$ and $(A_t[5] \otimes \chi_5)|_{G_K}$ have isomorphic semisimplifications.*

This is the second congruence of [33, Lemma 7.3], where $A_t = E_3^+(t)$ ([33, Proposition 3.1, (19)]). Written with $A_t[5]$, it carries the twist by χ_5, which is needed: for $t = 3$ the traces of Frobenius at a prime above 29 differ without it.

Theorem 2.10 ([33, Proposition 7.4, Remark 7.5]). *Let $\ell \in \{3, 5\}$ and $t \in \mathbb{Q} \smallsetminus \{0, 1\}$.*

(a) If $v_\ell(t - 1) > 3$, then J_t has potentially multiplicative reduction at ℓ.

(b) If $v_\ell(t-1) = 0$, and moreover $v_3(17t+108) \leq 3$ in case $\ell = 3$, then J_t has potentially good reduction at ℓ.

If $t = -X^5/Y^3$ for a primitive solution, then $v_3(17t+108) \leq 3$; so if $\ell \mid Z$, J_t has potentially multiplicative reduction at ℓ, and if $\ell \nmid YZ$, it has potentially good reduction at ℓ.

The last sentence uses [33, Remark 7.5], and $v_\ell(t - 1) = p\, v_\ell(Z) > 3$ if $\ell \mid Z$, $v_\ell(t - 1) = 0$ if $\ell \nmid YZ$. At $\ell = 5$ we reprove both cases for primitive solutions (Lemmas 2.18 and 2.19).

Theorem 2.11 ([33, Corollary 7.7]). *Let ℓ be a prime, $C(2) = 13$, $C(3) = 41363281$, $C(5) = 335809$. If $\ell \nmid Z$ and $p > C(\ell)$, then $\bar{\rho}_{t,\mathfrak{p}}$ is absolutely irreducible for every $\mathfrak{p} \mid p$.*

This statement enters the proof of [33, Theorem B] (Theorem 2.17); in its place we use Proposition 6.4. Its printed derivation of $C(2) = 13$ takes the traces of Frobenius at (2) on J_t to be -1 and -8, but 8 exceeds the Weil bound 4; the traces are -1 and 0 (Lemma 2.22(a)). For $\ell \in \{2, 3, 5\}$ its conclusion holds for every $p \geq 7$, given three of the statements labeled below (Remark 6.5).

Theorem 2.12 ([33, Theorem 7.8]). *If $\bar{\rho}_{t,\mathfrak{p}}$ is irreducible, then $\bar{\rho}_{t,\mathfrak{p}} \cong \bar{\rho}_{g,\mathfrak{P}}$ for a Hilbert newform g over K of parallel weight 2, trivial character and level the conductor of $\bar{\rho}_{t,\mathfrak{p}}$, supported on 3 and $\sqrt{5}$, and a prime $\mathfrak{P} \mid p$ of its coefficient field. Moreover $\varepsilon_3 = 2$ if $3 \mid XZ$; if $3 \mid Y$ and $X \equiv \pm 4 \pmod 9$, equivalently $X^5 \equiv \pm 2Y_0^3 \pmod 9$ with $Y_0 = 3^{-v_3(Y)}Y$; and if $3 \nmid XYZ$ and $X^5 \equiv 4Y^3 \pmod 9$; otherwise $\varepsilon_3 = 3$.*

The first sentence of Theorem 2.12 is the level-lowering statement of [33, Theorem 7.8], with the level given as the conductor of $\bar{\rho}_{t,\mathfrak{p}}$, as in its proof, and the last sentence is its part (i). Part (ii) concerns ε_5, which we determine instead by Lemma 3.11, from Lemmas 2.19 and 2.20 and Proposition 3.5(e); the remark below corrects two of its cases.

Remark (part (ii) of [33, Theorem 7.8]). In our notation, with $X_0 = 5^{-v_5(X)}X$, part (ii) of [33, Theorem 7.8] states that $\varepsilon_5 = 2$ if $5 \mid YZ$, if $5 \mid X$ and $Y^3/X_0^5 \equiv 6, 12, 28 \pmod{25}$, and if $5 \nmid XYZ$ and $Y^3/X \equiv 6, 8, 17, 19 \pmod{25}$, and that $\varepsilon_5 = 3$ otherwise. By Lemma 3.11, the correct statement exchanges the two lists of residues and reads Y^3/X^5 for Y^3/X and 18 for 28. The second and third cases as printed are wrong in both directions, as four classes modulo 25 show; in each, the true value is that of Lemma 3.11. On the class of $(X, Y) = (1, 2)$, which contains the special parameter $t = -1/8$, $Y^3/X \equiv Y^3/X^5 \equiv 8$, so the printed statement gives $\varepsilon_5 = 2$, whereas $\varepsilon_5 = 3$; indeed $J_{-1/8}$ has conductor $3^6 \cdot 5^5$ over $\mathbb{Q}$ (Lemma 2.7), and [33, Table 7.3] gives $3^3(\sqrt{5})^3$ for $t_0 = -1/8$. On the class of $(1, 8)$, $Y^3/X \equiv Y^3/X^5 \equiv 12$, so it gives $\varepsilon_5 = 3$, whereas $\varepsilon_5 = 2$. If $5 \mid X$ and $(X_0, Y) \equiv (1, 8) \pmod{25}$, then $Y^3/X_0^5 \equiv 12$, so it gives $\varepsilon_5 = 2$, whereas $\varepsilon_5 = 3$; and if $(X_0, Y) \equiv (2, 11) \pmod{25}$, then $Y^3/X_0^5 \equiv 8$, so it gives $\varepsilon_5 = 3$, whereas $\varepsilon_5 = 2$.

Theorem 2.13 ([33, Theorem A]). *Let $p \notin \mathcal{P}$, where*

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 19, 29, 31, 41, 61, 71, 79, 89, 101, 109\}.$$

Then one of the following holds:

(1) $\bar{\rho}_{t,\mathfrak{p}}$ is reducible;
(2) $\bar{\rho}_{t,\mathfrak{p}} \cong \bar{\rho}_{g,\mathfrak{P}}$ for a Hilbert newform g over K with complex multiplication;
(3) $\bar{\rho}_{t,\mathfrak{p}}$ is congruent to J_s for a special parameter s.

The elimination in [33] does not distinguish a newform from its Galois conjugate [33, Remark 7.9], so alternative (3), which [33] states as a congruence between $\bar{\rho}_{t,\mathfrak{p}}$ and the mod-$\mathfrak{p}$ representation of C_s, is to be read with $J_s[\mathfrak{p}]$ or $J_s[\mathfrak{p}']$, as in Definition 2.6; this is how it is stated in Theorem 2.13. The CM fields in (2) are $K(\sqrt{-3})$ and $\mathbb{Q}(\zeta_5)$ (Remark 2.14); Remark 2.15 compares this with the text of [33].

Remark 2.14. The proof of [33, Theorem A] applies Theorem 2.12 and eliminates newforms at the levels $3^i(\sqrt{5})^j$, $i, j \in \{2, 3\}$, using the primes $\ell \nmid 30$ below a prime of K of norm at most 400; by the last sentence of Theorem 2.12, Lemma 2.20 and Proposition 3.5(e), the conductor of $\bar{\rho}_{t,\mathfrak{p}}$ is one of these levels. The survivors are: at $3^2(\sqrt{5})^2$, three forms with

complex multiplication, one with rational Hecke eigenvalues and complex multiplication by $K(\sqrt{-3})$ and two with coefficient field $\mathbb{Q}(\sqrt{5})$ and complex multiplication by $\mathbb{Q}(\zeta_5)$, for $p \notin \{2,3,5,11,19,29\}$; at $3^2(\sqrt{5})^3$, seven forms with complex multiplication by $\mathbb{Q}(\zeta_5)$, among them that of J_0, for $p \notin \{2,3,5,7,11,13,19,29,31\}$; at $3^3(\sqrt{5})^2$, seven forms with complex multiplication by $K(\sqrt{-3})$, among them that of J_∞, for $p \notin \{2,3,5,7,11,19,29,31,41,61\}$; at $3^3(\sqrt{5})^3$, $g_{-1/8}$ and $g_{9/8}$, for $p \notin \mathcal{P}$. In the case $\ell \mid Y$, the test of [33, §7.4] keeps the form with rational Hecke eigenvalues at every auxiliary prime ℓ, for every p, contrary to [33, Remark 7.11] (see the remark below). At level $3^3(\sqrt{5})^2$ the list printed in [33] omits 31, which their computation gives: in their output [32] the newforms numbered 88, 93, 94 and 99 of this level are discarded only for $p \notin \{2,3,31,41,61\}$. Thus if $p \notin \mathcal{P}$ and $\bar\rho_{t,\mathfrak{p}}$ is irreducible, then either it is isomorphic to $\bar\rho_{g,\mathfrak{P}}$ for one of these newforms with complex multiplication, of level $3^2(\sqrt{5})^2$, $3^2(\sqrt{5})^3$ or $3^3(\sqrt{5})^2$, or it is congruent to J_s, and then $\varepsilon_3 = \varepsilon_5 = 3$.

Remark ([33, Remark 7.11]). In the elimination of [33, §7.4] a solution is treated at each auxiliary prime ℓ in one of three cases: $\ell \nmid XYZ$, $\ell \mid XY$ and $\ell \mid Z$. [33, Remark 7.11] states that a newform whose coefficient field is not K is eliminated in the first case by some auxiliary prime, and that the argument applies to all three cases. The second statement fails for the form with rational Hecke eigenvalues at level $3^2(\sqrt{5})^2$ in Remark 2.14 (LMFDB label 2.2.5.1-2025.1-e [43]), which we call Θ: at every prime $\lambda \nmid 15$ of $\mathbb{Q}(\zeta_{15})$ its trace of Frob_λ is $N(\lambda)$ times the value at $e = 1/5$ of [33, (39)], their formula for the case $\ell \mid Y$ with $t = \ell^{v_\ell(t)}e$, so their test keeps it at every auxiliary prime, for every p. Indeed, $\psi(N_{\mathbb{Q}(\zeta_{15})/K(\sqrt{-3})}\lambda) = -\chi_\lambda(5)^5 J(\chi_\lambda^2, \chi_\lambda^8)$ for one of the two Hecke characters ψ of $K(\sqrt{-3})$ whose theta series is Θ, with χ_λ as in [33, (14)] and J the Jacobi sum: both sides are Hecke characters of $\mathbb{Q}(\zeta_{15})$ with the same infinity type (the Jacobi sum by [46]; $\lambda \mapsto \chi_\lambda(5)^5$ is the Artin symbol of $\mathbb{Q}(\zeta_{15}, \sqrt[3]{5})/\mathbb{Q}(\zeta_{15})$), and their ratio has order dividing 6 and conductor dividing $\mathfrak{p}_3^4\mathfrak{p}_5$, where $\mathfrak{p}_3$, $\mathfrak{p}_5$ are the primes above 3, 5. As $\mathbb{Q}(\zeta_{15})$ has class number 1, the ratio is trivial once it is trivial at primes whose classes, with those of the units, generate $(\mathcal{O}_{\mathbb{Q}(\zeta_{15})}/\mathfrak{p}_3^4\mathfrak{p}_5)^\times$ modulo sixth powers; this is checked in item C22 of the Supplement. The elimination lists (EL) do not rest on [33, Remark 7.11]: the computation [32] tests every newform of the four levels, whatever its coefficient field, and Θ is among the survivors recorded in Remark 2.14.

Remark 2.15. In the proof of [33, Theorem A], the seven forms that survive at level $3^2(\sqrt{5})^3$ are said to have complex multiplication by $\mathbb{Q}(\sqrt{-3})$ and to include the form of the trivial solution with $Y = 0$, and the seven at level $3^3(\sqrt{5})^2$ to have complex multiplication by $\mathbb{Q}(\zeta_{15})$ and to include the form of $X = 0$. The two levels are interchanged there: J_0 (from $X = 0$) and J_∞ (from $Y = 0$) have conductors $3^4 \cdot 5^5$ and $3^6 \cdot 5^4$ over $\mathbb{Q}$ (`genus2red`; also [33, Lemmas 4.4, 4.5]), that is, levels $3^2(\sqrt{5})^3$ and $3^3(\sqrt{5})^2$ (Lemma 2.3), and complex multiplication by $\mathbb{Q}(\zeta_5)$ and by $K(\sqrt{-3}) = \mathbb{Q}(\sqrt{5}, \sqrt{-3})$ respectively (Lemma 2.5). For example, at the two primes of K above 11, which are inert in $K(\sqrt{-3})$, the form of J_0 has eigenvalues $2 \pm 2\sqrt{5}$, so it does not have complex multiplication by $K(\sqrt{-3})$. Neither [33, Theorem A] nor Theorem 6.21 is affected.

Theorem 2.16 ([33, Theorem 7.18]). *If $3 \nmid Y$ and $p > 3$, then $\bar\rho_{t,\mathfrak{p}}$ is not congruent to J_s for either special parameter s.*

Their proof compares the fields cut out by inertia at 3, which are the same for $J_s[\mathfrak{p}]$ and $J_s[\mathfrak{p}']$, so it excludes both cases of Definition 2.6.

Theorem 2.17 ([33, Theorem B]). *Let $p \geq 7$ be a prime not in $\{7, 11, 13, 19, 29, 31, 41, 61\}$. Then $X^5 + Y^3 = Z^p$ has no primitive solution with Z odd and divisible by 3 or by 5.*

Pacetti and Villagra Torcomian state this for every prime $p \notin \{2, 7, 11, 13, 19, 29, 31, 41, 61\}$, the cases $p = 3$ and $p = 5$ being earlier results that they cite. Their proof uses Theorem 2.11 with $\ell = 2$ for the irreducibility of $\bar{\rho}_{t,\mathfrak{p}}$; Theorem 2.10, by which J_t has potentially multiplicative reduction at 3 or at $\sqrt{5}$; a level lowering that keeps this special local type, which is not part of Theorem 2.12 and for which no reference is given; and the elimination lists of Remark 2.14 at the three levels with an exponent 2, whose exceptional sets have union $\{2, 3, 5, 7, 11, 13, 19, 29, 31, 41, 61\}$. Theorem 6.23 proves a stronger statement for the same primes from inputs used elsewhere in this paper, without Theorem 2.11 and without that level lowering.

Labels. Each result of Section 6 and of the Supplement that uses [33] lists which of the following statements it assumes.

- (LL) *Level lowering*: the first sentence of Theorem 2.12.
- (Ex) *The exponent at* 3: the last sentence of Theorem 2.12 (part (i) of [33, Theorem 7.8]), which gives the conductor exponent ε_3 of an irreducible $\bar{\rho}_{t,\mathfrak{p}}$.
- (Ex_0) For every primitive solution, the conductor exponent ε_3 of $\rho_{t,\lambda}$ at (3) lies in $\{2, 3\}$, and $\varepsilon_3 = 2$ if $3 \mid Z$.
- (Ex_9) For every primitive solution with $3 \nmid XZ$, the conductor exponent of $\rho_{t,\lambda}$ at (3) is 2 if $3 \mid Y$ and $X \equiv \pm 4 \pmod 9$, or if $3 \nmid Y$ and $X^5 \equiv 4Y^3 \pmod 9$, and 3 otherwise. It is proved in Lemma 6.2(e).
- (EL) *The elimination lists* in the proof of [33, Theorem A], as recorded in Remark 2.14.
- (T7.18) Theorem 2.16. For $p \geq 7$ it is proved in Lemma 6.18(d), given (P7.4)(a) at $\ell = 3$ when $3 \mid Z$.
- (T2.1) Theorem 2.8.
- (P7.4) Theorem 2.10; we write (P7.4)(a) for its part (a), and (P7.4)(a) at $\ell = 3$ for that part with $\ell = 3$.
- (LI) *The large-image conjecture* [33, Conjecture 1] (compare [11, Conjecture 4.1]): for a totally real field K' and a number field L there is a constant $C(L, K')$ such that for every abelian variety A over L of GL_2-type with $\mathrm{End}_L(A) \otimes \mathbb{Q} = \mathrm{End}_{\overline{L}}(A) \otimes \mathbb{Q} \cong K'$ and every prime $\mathfrak{p}$ of K' above a rational prime $p > C(L, K')$, the image of the mod-$\mathfrak{p}$ representation of A contains $\mathrm{SL}_2(\mathcal{O}_{K'}/\mathfrak{p})$.

Theorem 2.12 is stated for irreducible $\bar{\rho}_{t,\mathfrak{p}}$, but its proof takes ε_3 from [33, Corollary 3.6, Remark 3.7, Lemma 7.3], which concern $\rho_{t,\lambda}$ and do not assume $\bar{\rho}_{t,\mathfrak{p}}$ irreducible. (Ex_0) and (Ex_9) are the values of part (i) of [33, Theorem 7.8] read in this way, as statements about $\rho_{t,\lambda}$ (in characteristic 0); where J_t has potentially good reduction at (3), $\bar{\rho}_{t,\mathfrak{p}}$ has the same exponent for $p \geq 7$ (§6.1). When $3 \mid X$, $\varepsilon_3 = 2$ is proved without input from [33] (Lemma 6.2(a)).

Of these statements, (Ex_9) and (T7.18) are proved in this paper as stated in their labels (Lemma 6.2(e), Lemma 6.18(d)), and no result below assumes them; (Ex_0) is proved for the solutions with $3 \nmid Z$ (Lemma 6.2(a),(e)), so that what is used of (Ex) and (Ex_0) is the value $\varepsilon_3 = 2$ when $3 \mid Z$. (P7.4) is proved at $\ell = 5$ for primitive solutions (Lemmas 2.18 and 2.19); at $\ell = 3$ we use only part (a). We checked (EL) against the output [32] of the computation of [33], which is how the prime 31 missing from the printed list at level $3^3(\sqrt{5})^2$ was found (Remark 2.14), and we take from [33] that the two forms surviving at level $3^3(\sqrt{5})^3$ are those

of $J_{-1/8}$ and $J_{9/8}$. We take (LL), (T2.1), (P7.4)(a) at $\ell = 3$ and the value $\varepsilon_3 = 2$ when $3 \mid Z$ from [33], without checking their proofs; the first two rest on [18] and on the modularity and level-lowering theorems cited there.

2.6. **Local facts at $\sqrt{5}$.** Let $F = K_{\sqrt{5}} = \mathbb{Q}_5(\sqrt{5})$, F^{ur} its maximal unramified extension, I_F its inertia group, and v the valuation on $\overline{\mathbb{Q}}_5$ with $v(5) = 1$.

Lemma 2.18. *Let $X, Y \in \mathbb{Z}_5$ with $5 \nmid Y(X^5 + Y^3)$, and $t = -X^5/Y^3$.*

(a) $\mathcal{F}_{X,Y}$ has one root $r_0 \in \mathbb{Q}_5$, with $v(r_0) = 1 + 2v(X)$, and five roots $r_1, \dots, r_5$ that are units congruent to $-2Y$ modulo the maximal ideal, with $v(r_i - r_j) = 1/4$ for $1 \le i < j \le 5$.

(b) $C_{X,Y}$, and so C_t, has potentially good reduction over $\mathbb{Q}_5$.

(c) If $X \neq 0$, the roots of f_t are $x_i = -X^2/(Yr_i)$: $x_0 \in \mathbb{Q}_5$ with $v(x_0) = -1$, and $x_1, \dots, x_5$ with $v(x_i) = 2v(X)$ and $v(x_i - x_j) = 2v(X) + 1/4$. In particular, if $t \in \mathbb{Z}_5$ and $5 \nmid t(1-t)$, then f_t has one root of valuation -1, in $\mathbb{Q}_5$, and five unit roots pairwise at distance exactly $5^{-1/4}$.

Proof. (a) The coefficients of $U^6, U^3, U, 1$ in $\mathcal{F}_{X,Y}$ have valuations 0, ≥ 1, 0, $1 + 2v(X)$, so the Newton polygon gives one root r_0 of valuation $1 + 2v(X)$, in $\mathbb{Q}_5$ as the only root of that valuation, and five unit roots. Modulo 5, $\mathcal{F}_{X,Y} \equiv U(U^5 + 2Y) = U(U + 2Y)^5$, so the unit roots are $\equiv -2Y$ and $v(r_0 - r_i) = 0$; hence $\sum_{1 \le i < j \le 5} v(r_i - r_j) = v(\operatorname{disc} \mathcal{F}_{X,Y})/2 = 5/2$.

(b) By computation (item C1), the Igusa invariants of C_t are

$$\mathcal{I}_2 = -1200t^2, \quad \mathcal{I}_4 = -480000t^4, \quad \mathcal{I}_6 = 43520000t^6 + 276480000t^5,$$
$$\mathcal{I}_8 = -70656000000t^8 - 82944000000t^7, \quad \mathcal{I}_{10} = 2388787200000\, t^8(t-1)^2,$$

so that

$$\frac{\mathcal{I}_2^5}{\mathcal{I}_{10}} = -\frac{5^5 t^2}{3(t-1)^2}, \qquad \frac{\mathcal{I}_4^5}{\mathcal{I}_{10}^2} = -\frac{5^{10} t^4}{3^7 (t-1)^4},$$
$$\frac{\mathcal{I}_6^5}{\mathcal{I}_{10}^3} = \frac{5^5 t(17t+108)^5}{3^{18}(t-1)^6}, \qquad \frac{\mathcal{I}_8^5}{\mathcal{I}_{10}^4} = -\frac{5^{10} t^3 (23t+27)^5}{3^{19}(t-1)^8};$$

they also appear in [33, proof of Proposition 7.4]. Here $t \in \mathbb{Z}_5$ and $t - 1 = -(X^5 + Y^3)/Y^3$ is a unit, so these quotients are 5-integral, and C_t has potentially good reduction by Liu's criterion [28, Théorème 1]. If $X = 0$, a direct computation gives $\mathcal{I}_2 = \mathcal{I}_4 = \mathcal{I}_6 = \mathcal{I}_8 = 0$ and $\mathcal{I}_{10} = 2388787200000\, Y^6$ for $C_{0,Y}$, so the quotients vanish and the same criterion applies to $C_{0,Y}$.

We complete the proof of (a). By [13, Theorem 1.9(3)], (b) means that no cluster of roots has size 2, 3 or 4. The unit roots form a cluster, and for $1 \le i < j \le 5$ the smallest disc containing r_i, r_j cuts out a cluster inside it of size at least 2, so of size 5; hence all $v(r_i - r_j)$ are equal, to $(5/2)/10 = 1/4$.

(c) Use $x_i - x_j = X^2(r_i - r_j)/(Yr_ir_j)$. For $t \in \mathbb{Z}_5$ with $5 \nmid t(1-t)$ take $X = 1$ and $Y \in \mathbb{Z}_5^\times$ with $Y^3 = -1/t$ (cubing is bijective on $\mathbb{Z}_5^\times$). □

For a primitive solution, $5 \nmid YZ$ is exactly $5 \nmid Y(X^5 + Y^3)$. The lemma also applies to both special parameters, since $-1/8 \equiv 3$ and $9/8 \equiv 23 \pmod{25}$.

Lemma 2.19. *Let $X, Y \in \mathbb{Z}_5$ with $5 \nmid XY$, $X^5 + Y^3 \neq 0$ and $m := v_5(X^5 + Y^3) \ge 3$, and let $t = -X^5/Y^3$. (Every primitive solution with $5 \mid Z$ and $p \ge 3$ qualifies: $m = p\, v_5(Z)$.)*

(a) *The roots of $\mathcal{F}_{X,Y}$ in $\overline{\mathbb{Q}}_5$ are: one root $r_0 \in \mathbb{Q}_5$ with $v(r_0) = 1$; one unit root $r_c \in \mathbb{Q}_5$; and four unit roots forming two pairs $\mathfrak{t}_1$, $\mathfrak{t}_2$, exchanged by $\mathrm{Gal}(F/\mathbb{Q}_5)$, with $v(r - r') = (2m-3)/4$ for the two roots of a pair and $v(r - r') = 1/2$ for any two distinct unit roots not in the same pair. The proper clusters, in the sense of* [13]*, are $\mathcal{R}$ (all six roots), $\mathfrak{s}$ (the five unit roots, depth $1/2$) and the twins $\mathfrak{t}_1$, $\mathfrak{t}_2$.*

(b) *J_t has potentially totally toric reduction at $\sqrt{5}$.*

(c) *Let ξ be the quadratic character of I_F cut out by $F^{\mathrm{ur}}(5^{1/4})$ (it is nontrivial). For every prime λ of K not above 5, $\rho_{t,\lambda}|_{I_F}$ is tame with semisimplification $\xi \oplus \xi$ and no nonzero invariants; so $\varepsilon_5(\rho_{t,\lambda}) = 2$, and J_t has conductor exponent 4 at 5 over $\mathbb{Q}$.*

(d) *For every prime $\mathfrak{p}$ of K above an odd prime $p \neq 5$, $\bar{\rho}_{t,\mathfrak{p}}$ has conductor exponent 2 at $\sqrt{5}$.*

In (c) *and* (d)*, $t \in \mathbb{Q}$ (for instance $X, Y \in \mathbb{Z}$); for $t \in \mathbb{Q}_5$ the same holds for the local representations of J_t over F with its $\mathcal{O}_K$-action, and with $\mathbb{Q}_5$ in place of $\mathbb{Q}$.*

Proof. Normalization. Cubing is a bijection of $\mathbb{Z}_5^\times$ (as $\mathbb{Z}_5^\times \cong \mu_4 \times (1 + 5\mathbb{Z}_5)$ and 3 is prime to $4 \cdot 5$), so there is $\lambda_0 \in \mathbb{Z}_5^\times$ with $\lambda_0^3 X = -1$. By Lemma 2.1, $(U, V) \mapsto (\lambda_0 U, \lambda_0^3 V)$ is an isomorphism $C_{X,Y} \to C_{-1,Y'}$ over $\mathbb{Q}_5$, $Y' = \lambda_0^5 Y$; it multiplies all root differences by the unit λ_0, so it preserves the cluster picture, and $-1 + Y'^3 = \lambda_0^{15}(X^5 + Y^3)$ has valuation m. Write $Y' = \omega(1 + \eta)$ with $\omega \in \mu_4$ and $\eta \in 5\mathbb{Z}_5$; as $Y'^3 \equiv 1 \pmod 5$, $\omega^3 = 1$, so $\omega = 1$, and $v(\eta) = m$, as $(1+\eta)^3 - 1 = 3\eta + 3\eta^2 + \eta^3$. Put $G(U) = \mathcal{F}_{-1,1+\eta}(U)$. Then

$$G_0 \coloneqq \mathcal{F}_{-1,1} = (U^2 - U - 1)^2(U^2 + 2U + 5), \qquad G = G_0 + 12\eta U,$$

and $v(\operatorname{disc} G) = 5 + 2m$ (Section 2.2).

Roots near φ. The roots of $U^2 - U - 1$ are φ and $\sigma(\varphi)$, both in F, and $\varphi - \sigma(\varphi) = \sqrt{5}$. Expanding at φ, $G(\varphi + h) = \sum_{k=0}^{6} c_k h^k$ with

$$c_0 = 12\eta\varphi, \quad c_1 = 12\eta, \quad c_2 = 15\sqrt{5}\,\varphi, \quad c_3 = 10(4\varphi + 1), \quad c_4 = 15\varphi^2, \quad c_5 = 6\varphi, \quad c_6 = 1,$$

of valuations $m, m, 3/2, 1, 1, 0, 0$ (φ and $4\varphi + 1 = 3 + 2\sqrt{5}$ are units). The lower convex hull of the points $(k, v(c_k))$ is $(0, m)$–$(2, 3/2)$–$(5, 0)$–$(6, 0)$: the first segment has slope $-(2m-3)/4 < -1/2$ because $m \geq 3$, and $(1, m)$, $(3, 1)$, $(4, 1)$ lie on or above the hull. Hence G has exactly two roots r with $v(r - \varphi) = (2m-3)/4$, forming a pair $\mathfrak{t}_1$, three with $v(r - \varphi) = 1/2$ and one with $v(r - \varphi) = 0$. Applying the generator of $\mathrm{Gal}(F/\mathbb{Q}_5)$ (G has coefficients in $\mathbb{Q}_5$), exactly two roots, forming $\mathfrak{t}_2$, satisfy $v(r - \sigma(\varphi)) = (2m-3)/4$, and three satisfy $v(r - \sigma(\varphi)) = 1/2$.

The other two roots. The coefficients of $U^6, U^3, U, 1$ in G have valuations $0, 1, 0, 1$, so G has one root r_0 of valuation 1, in $\mathbb{Q}_5$ as the only root of that valuation, and five unit roots; $v(r_0 - \varphi) = 0$. As $v(\varphi - \sigma(\varphi)) = 1/2 < (2m-3)/4$, $\mathfrak{t}_1 \cap \mathfrak{t}_2 = \emptyset$, and the unit roots outside $\mathfrak{t}_1 \cup \mathfrak{t}_2$ consist of one root r_c. From the polygon at φ, $v(r_c - \varphi) = 1/2$ and $v(r - \varphi) = 1/2$ for $r \in \mathfrak{t}_2$. Hence for $r \in \mathfrak{t}_1$ and $r' \in \mathfrak{t}_2$, $v(r - r') = v((r - \varphi) - (r' - \varphi)) = 1/2$; likewise $v(r - r_c) = 1/2$ for $r \in \mathfrak{t}_1 \cup \mathfrak{t}_2$ (using $\sigma(\varphi)$ for $\mathfrak{t}_2$). The root r_c is the only unit root r with $v(r - r') \leq 1/2$ for every other root r'; $G_{\mathbb{Q}_5}$ preserves this property, so $r_c \in \mathbb{Q}_5$.

Depth of the twins. Let δ_i be $v(r - r')$ for the two roots of $\mathfrak{t}_i$; $\delta_1 = \delta_2$, as $\mathrm{Gal}(F/\mathbb{Q}_5)$ exchanges $\mathfrak{t}_1$ and $\mathfrak{t}_2$. The sum of the $v(r - r')$ over the unordered pairs of distinct roots is $v(\operatorname{disc} G)/2 = (5 + 2m)/2$; the five pairs containing r_0 contribute 0, and the eight pairs of unit roots not inside a twin contribute 4, so $\delta_1 = (2m-3)/4$. So the clusters are $\mathcal{R}$, $\mathfrak{s} = \mathcal{R} \smallsetminus \{r_0\}$ (depth $1/2$), $\mathfrak{t}_1$, $\mathfrak{t}_2$ (depth $(2m-3)/4$) and the singletons. This proves (a).

(b) By [13, Theorem 1.9(7)] (which is Theorem 10.3(7) there), the potential toric rank of J_t is the number of even non-übereven clusters other than $\mathcal{R}$, less 1 if $\mathcal{R}$ is übereven. Here these clusters are $\mathfrak{t}_1$, $\mathfrak{t}_2$ (even, with odd children), and $\mathcal{R}$ is not übereven (its children $\mathfrak{s}$ and $\{r_0\}$ are odd). So the potential toric rank is $2 = \dim J_t$.

(c) Work over F, with $v_F(\sqrt{5}) = 1$, so that the depths are $d_{\mathcal{R}} = 0$, $d_{\mathfrak{s}} = 1$ and $d_{\mathfrak{t}_i} = (2m-3)/2$. Each $\mathfrak{t}_i$ is stable under G_F (its center φ, resp. $\sigma(\varphi)$, lies in F), and so is $\mathcal{R}$. The principal clusters [13, Definition 1.5] are those of size at least 3 other than $\mathcal{R}$, which is excluded as it is even with two children (no cluster has a child of size $2g = 4$); so the only one is $\mathfrak{s}$, whose component $y^2 = c_{\mathfrak{s}}(x - \mathrm{red}_{\mathfrak{s}}(r_c))$ has genus 0. By [13, Theorem 1.20] (which is Theorem 10.1 there), as G_F-representations

$$H^1_{\text{ét}}(C_{X,Y} \otimes \overline{F}, \mathbb{Q}_\ell) \cong H^1_t \otimes \mathrm{Sp}_2, \qquad H^1_t = \epsilon_{\mathfrak{t}_1} \oplus \epsilon_{\mathfrak{t}_2},$$

the abelian part being 0. By [13, Remark 1.14] (see Remark 8.4 there), the restriction of $\epsilon_{\mathfrak{t}_i}$ to the stabilizer of $\mathfrak{t}_i$, which contains I_F, is unramified if and only if $|I_F/I_{\mathfrak{t}_i}|\,(v_F(c_f) + \sum_{r \notin \mathfrak{t}_i} d_{r \wedge \mathfrak{t}_i})$ is even, where $\mathfrak{t}_i^* = \mathfrak{t}_i$ (its parent $\mathfrak{s}$ is not übereven) and $I_{\mathfrak{t}_i} = I_F$; here $c_f = 1$, and the sum is $d_{\mathcal{R}} + 3d_{\mathfrak{s}} = 3$ (r_0 gives $\mathcal{R}$, the other three roots give $\mathfrak{s}$), which is odd. So $\epsilon_{\mathfrak{t}_i}|_{I_F}$ is the nontrivial quadratic character ξ of I_F. (Directly: with h_1, h_2 the roots $r - \varphi$, $r \in \mathfrak{t}_1$, $\theta^2_{\mathfrak{t}_1} = \prod_{r \notin \mathfrak{t}_1}(\varphi - r)$ is the constant term of $G(\varphi + h)/((h - h_1)(h - h_2))$, which is $c_2(1 + \mathfrak{m}) = 15\sqrt{5}\,\varphi(1 + \mathfrak{m})$ by the polygon above; $3\varphi \equiv 4 \pmod{\sqrt{5}}$ is a square, so $15\sqrt{5}\,\varphi \equiv \sqrt{5}$ modulo squares of $F^\times$, and $\epsilon_{\mathfrak{t}_1}|_{I_F}$ is the character of $F^{\mathrm{ur}}(5^{1/4}) = F^{\mathrm{ur}}(\sqrt{\sqrt{5}})$, of order 2 as $v_F(\sqrt{5}) = 1$ is odd.) Hence $H^1_{\text{ét}}|_{I_F}$ has semisimplification $\xi^{\oplus 4}$ and no nonzero I_F-invariants. Since $V_\ell(J_t)$ is the dual of $H^1_{\text{ét}}$ twisted by $\mathbb{Q}_\ell(1)$, on which inertia acts trivially, the same holds for $V_\ell(J_t)$, and so for each of its summands $V_\lambda(J_t)$, $\lambda \mid \ell$. The extension $F(\mathcal{R})/F$ is tame ($r_0, r_c \in \mathbb{Q}_5$, and each $\mathfrak{t}_i$ generates an extension of F of degree at most 2), so J_t is tame over F [13, Theorem 1.9(4)], that is, semistable over a tamely ramified extension L/F; the pro-5 group $P_F \subset I_L$ then acts unipotently, hence through a finite group, hence trivially, and the Swan conductor is 0. Therefore $\varepsilon_5(\rho_{t,\lambda}) = 2$, and over $\mathbb{Q}$ the exponent is $\varepsilon_5 + 2 = 4$ (Lemma 2.3).

(d) Choose $\tau \in I_F$ with $\xi(\tau) = -1$. By (c), $\rho_{t,\mathfrak{p}}(\tau)$ has characteristic polynomial $(x+1)^2$, so its reduction $\bar{\rho}_{t,\mathfrak{p}}(\tau)$ has characteristic polynomial $(x+1)^2$, and as p is odd, 1 is not an eigenvalue: $\bar{\rho}_{t,\mathfrak{p}}$ has no nonzero I_F-invariants. Wild inertia acts trivially on $\rho_{t,\mathfrak{p}}$, hence on $\bar{\rho}_{t,\mathfrak{p}}$. So the residual exponent is 2. □

Lemma 2.20. *Let (X, Y, Z) be a primitive solution, $\mathfrak{p}$ a prime above $p \geq 7$, and suppose $5 \mid YZ$. Then the conductor exponent of $\bar{\rho}_{t,\mathfrak{p}}$ at $(\sqrt{5})$ is 2.*

Proof. If $5 \mid Y$, then $5 \nmid X$, and $U = 5^{1/6}W$, $V = 5^{1/2}V'$ give

$$V'^2 = W^6 + 2\sqrt{5}\,XW^3 + 12 \cdot 5^{-5/6}YW + X^2 \equiv W^6 + X^2$$

modulo the maximal ideal, a smooth curve of genus 2. So $C_{X,Y}$ has good reduction over $F^{\mathrm{ur}}(5^{1/6})$, of degree 3 over F^{ur}. A generator of $\mathrm{Gal}(F^{\mathrm{ur}}(5^{1/6})/F^{\mathrm{ur}})$ acts on the special fiber by $W \mapsto \zeta_3^{\mp 1} W$, with quotient $V'^2 = S^2 + X^2$ ($S = W^3$) of genus 0. By the criterion of Néron–Ogg–Shafarevich and the description of the inertia action in its proof [40, §§1–2], I_F acts on $V_\ell(J_t)$ through this group of order 3, as it acts on V_ℓ of the Jacobian of the special fiber. If a finite group acts on a curve, the invariants in V_ℓ of its Jacobian are V_ℓ of the Jacobian of the quotient curve; here the quotient has genus 0, so $V_\ell(J_t)^{I_F} = 0$. Equivalently, by the Lefschetz fixed-point formula, the generator fixes the 4 points over $W = 0$ and $W = \infty$, so its trace on H^1 is $2 - 4 = -2$, which for an element of order 3 on a 4-dimensional

space forces the eigenvalues $\zeta_3, \zeta_3, \zeta_3^2, \zeta_3^2$. So $\rho_{t,\lambda}$, and $\bar{\rho}_{t,\mathfrak{p}}$ as $p \neq 3$, are tame at $(\sqrt{5})$ with conductor exponent 2.

If $5 \mid Z$, then $5 \nmid XY$ and $v_5(X^5 + Y^3) = p\, v_5(Z) \geq 7$, so Lemma 2.19(d) applies: the exponent is 2. □

Corollary 2.21. *Let (X, Y, Z) be a primitive solution and $\mathfrak{p}$ a prime above $p \geq 7$. If $\bar{\rho}_{t,\mathfrak{p}}$ is congruent to J_s, then $5 \nmid YZ$. Given the statement on ε_3 in Theorem 2.12, moreover $3 \nmid XZ$; if $3 \mid Y$ then $X \not\equiv \pm 4 \pmod 9$; and if $3 \nmid Y$ then $X^5 \not\equiv 4Y^3 \pmod 9$.*

Proof. By Lemma 2.7, $\bar{\rho}_{t,\mathfrak{p}}$ is irreducible with conductor exponents 3 at (3) and $(\sqrt{5})$. By Lemma 2.20 the exponent at $(\sqrt{5})$ is 2 if $5 \mid YZ$, so $5 \nmid YZ$. By the statement on ε_3 in Theorem 2.12, $\varepsilon_3 = 3$ excludes the three cases in which $\varepsilon_3 = 2$, which gives the other conclusions. □

2.7. **The primes 2 and 3, and a ray class group.** The three lemmas below are used in Section 3 and again in Section 6. Here $\rho = \rho_{t,\mathfrak{p}}$ and $\bar{\rho} = \bar{\rho}_{t,\mathfrak{p}}$ for a primitive solution and a prime $\mathfrak{p}$ of K above $p \geq 7$, $k_\mathfrak{p}$ is the residue field of $\mathfrak{p}$, $\bar{\chi}_p$ is the mod-p cyclotomic character, and $G_v \supset I_v$ are the decomposition and inertia groups at $v = (2), (3)$, whose completions are $\mathbb{Q}_4$ and $\mathbb{Q}_9$, the unramified quadratic extensions of $\mathbb{Q}_2$ and $\mathbb{Q}_3$. We write θ_M for the character of a quadratic extension M/K, and $\theta_{-3} = \theta_{K(\sqrt{-3})}$, $\theta_\zeta = \theta_{\mathbb{Q}(\zeta_5)}$, $\theta_{15} = \theta_{-3}\theta_\zeta = \theta_{\mathbb{Q}(\zeta_{15})^+}$; recall $\mathbb{Q}(\zeta_5) = K(\sqrt{-\sqrt{5}\varphi})$ and $\mathbb{Q}(\zeta_{15})^+ = K(\sqrt{3\sqrt{5}\varphi})$.

Lemma 2.22 (the prime 2)**.** *(a) If $2 \nmid Z$, then J_t has good reduction at (2), and $a_2 := \operatorname{tr}\rho(\mathrm{Frob}_{(2)}) \in \mathcal{O}_K$ is -1 if $2 \mid Y$ and 0 if $2 \mid X$; in particular it does not depend on $\mathfrak{p}$.*

(b) Assume (T2.1)*. If $2 \mid Z$, then $\bar{\rho}$ is unramified at (2), $\bar{\rho}|^{\mathrm{ss}}_{G_2} = \psi_2 \oplus \psi_2\bar{\chi}_p$ with ψ_2 unramified of order at most 2, and $\operatorname{tr}\bar{\rho}(\mathrm{Frob}_{(2)}) = \pm 5$ in $k_\mathfrak{p}$.*

Proof. (a) With $V = 2w + U^3 + X$ the model becomes $w^2 + (U^3 + X)w = 2XU^3 + 3YU + X^2$, with smooth special fiber $w^2 + (U^3 + 1)w = 1$ if $2 \mid Y$ and $w^2 + U^3 w = U$ if $2 \mid X$. Their Frobenius polynomials over $\mathbb{F}_4$ are $(x^2 + x + 4)^2$ and $(x^2 + 4)^2$ (PARI/GP). The Frobenius polynomial of J_t over $\mathbb{F}_4$ is the product of $x^2 - a_2 x + 4$ and its σ-conjugate, and $x^2 + x + 4$, $x^2 + 4$ are irreducible over K. (b) By Theorem 2.8, J_t has multiplicative reduction at (2); the Tate uniformization gives the rest, and the trace is $\pm(1 + N(2))$. □

Lemma 2.23. *(a) K has narrow class number 1, and $\mathrm{Cl}_K(3\sqrt{5}\,\infty_1\infty_2) \cong \mathbb{Z}/4 \times \mathbb{Z}/2$.*

(b) φ generates $(\mathcal{O}_K/3)^\times \cong \mathbb{F}_9^\times$ and $(\mathcal{O}_K/\sqrt{5})^\times \cong \mathbb{F}_5^\times$ (where $\varphi \equiv 3$); $\varphi^8 = 21\varphi + 13$ is totally positive, $\varphi^8 \equiv 1 \pmod{3\sqrt{5}}$, and $N_{K/\mathbb{Q}}(\varphi^8 - 1) = -45$.

(c) The quadratic characters of $\mathrm{Cl}_K(3\sqrt{5}\,\infty_1\infty_2)$ are θ_{-3}, θ_ζ and θ_{15}, ramified at the finite primes $\{3\}$, $\{\sqrt{5}\}$ and $\{3, \sqrt{5}\}$; θ_{-3} and θ_ζ are nontrivial at both real places and θ_{15} is trivial at both.

(d) (3) and (2) are inert in $\mathbb{Q}(\zeta_5)/K$; $(\sqrt{5})$ is inert and (2) splits in $K(\sqrt{-3})/K$.

Proof. (a) is a computation (item C3). (b) is direct. For (c), the three fields are distinct, quadratic over K and unramified outside $3\sqrt{5}\infty_1\infty_2$; for (d), 2 and 3 have order 4 modulo 5, -3 is not a square modulo 5, and $\mathbb{Q}_2(\sqrt{5}) = \mathbb{Q}_2(\sqrt{-3})$. □

Lemma 2.24. *Let τ_3 be a generator of tame inertia in I_3. For $X, Y \in \mathbb{Z}_3$ with $3 \mid X$, $3 \nmid Y$, $X^5 + Y^3 \neq 0$, the representation $\rho_{X,Y,\lambda}|_{I_3}$ ($\lambda \nmid 3$) of $\mathrm{Jac}(C_{X,Y})$, with the real multiplication of Proposition 2.2, is isomorphic to $\rho_{J_0,\lambda}|_{I_3}$; its image has order 5, and $\operatorname{tr}\rho_{J_0,\lambda}(\tau_3) = T \in \{(-1 \pm \sqrt{5})/2\}$.*

Proof. Every unit of $\mathbb{Z}_3$ is a fifth power in $\mathbb{Z}_9$, so $L = \mathbb{Q}_3^{\mathrm{ur}}(\pi)$, $\pi^5 = -12Y$, does not depend on Y, and $\tau_3(\pi)/\pi \in \mu_5$ does not either. With $U = \pi z$, $V = \pi^3 w$, $C_{X,Y}$ becomes $w^2 = z^6 + 10X\pi^{-3}z^3 - z + 5X^2\pi^{-6}$, with coefficients of valuation $\geq 2/5$ and $\geq 4/5$: good reduction over L with special fiber $\widetilde{C}\colon w^2 = z^6 - z$, on which τ_3 acts by $(z, w) \mapsto (\zeta z, \zeta^3 w)$, ζ the reduction of $\tau_3(\pi)/\pi$, of order 5 with genus-0 quotient. $\operatorname{Jac}\widetilde{C}$ is supersingular (its Weil polynomial over $\mathbb{F}_9$ is $(x^2+9)^2$), and the centralizer of $\mathbb{Q}(\zeta_5) = \mathbb{Q}([\zeta])$ in its endomorphism algebra $M_2(B_{3,\infty})$ is $\mathbb{Q}(\zeta_5)$. The reduction of $\iota(\sqrt{5})$ commutes with the inertia action, so it is $\pm(1 + 2([\zeta] + [\zeta]^{-1}))$; the sign is determined by its eigenvalue on the regular differential $z\,dz/w = \pi \cdot U\,dU/V$, which has nonzero reduction and is an eigenform with the eigenvalue of the family. So the I_3-module V_λ, with its action of $\mathcal{O}_K$, is the same for all such (X, Y), including $(0, 1)$. □

3. The local picture at $\sqrt{5}$

For $p \geq 7$, inertia at $\sqrt{5}$ on $J_t[\mathfrak{p}]$ is controlled by the field of the roots of f_t (Lemma 3.4), which takes three values according to the class of t modulo 25 (Proposition 3.5). This confines the congruences with J_s to eight classes (Theorem 3.6) and attaches one special parameter to each (Theorem 3.7).

3.1. **Notation and the classes modulo 25.** We keep the notation of Section 2.6. Let W_F be the Weil group of F, μ its unramified quadratic character, $\mathbb{Q}_5^{\mathrm{ur}}$ the maximal unramified extension of $\mathbb{Q}_5$, ω the Teichmüller lift and res the reduction to $\overline{\mathbb{F}}_5$. Fix π with $\pi^4 = 5$ and $\zeta_8 \in \mathbb{Q}_5^{\mathrm{ur}}$ with $\zeta_8^4 = -1$, and put $L_0 = \mathbb{Q}_5^{\mathrm{ur}}(\pi)$. Then $F^{\mathrm{ur}} \subset L_0$, and $\mathbb{Q}_5(\zeta_5) = \mathbb{Q}_5(\zeta_8\pi) \subset L_0$ as $(1-\zeta_5)^4 = -5u$ with $u \equiv 1/(-4!) \equiv 1$. As the tame extensions of $\mathbb{Q}_5^{\mathrm{ur}}$ are the $\mathbb{Q}_5^{\mathrm{ur}}(5^{1/e})$, $L_0 = \mathbb{Q}_5^{\mathrm{ur}}(\zeta_5)$ is the only quadratic extension of F^{ur}.

For $X, Y \in \mathbb{Z}_5$ with $5 \nmid Y(X^5 + Y^3)$ let $r_0 \in \mathbb{Q}_5$ and the *cluster* $r_1, \dots, r_5$ be the roots of $\mathcal{F}_{X,Y}$ as in Lemma 2.18(a) (units $\equiv -2Y \equiv 3Y$, pairwise at distance $5^{-1/4}$), and $N_{X,Y} = \mathbb{Q}_5^{\mathrm{ur}}(r_0, \dots, r_5)$. If $X \neq 0$ and $t = -X^5/Y^3$, the bijection $r \mapsto -X^2/(Yr)$ onto the roots of f_t (Lemma 2.1) preserves the fields $\mathbb{Q}_5(r)$, and $N_{X,Y} =: N_t$ is the field of the Weierstrass points of C_t over $\mathbb{Q}_5^{\mathrm{ur}}$. For $t \in \mathbb{Z}_5$ with $5 \nmid t(1-t)$ we take $(X, Y) = (1, Y)$, $Y^3 = -1/t$.

Definition 3.1. For $t \in \mathbb{Z}_5$ with $5 \nmid t(1-t)$ we write $t \in \mathcal{T}$, $\mathcal{A}$ or $\mathcal{B}$ according as t mod 25 lies in

$$\mathcal{T} = \{2, 4, 18\}, \qquad \mathcal{A} = \{3, 8, 9, 13, 14, 19, 23, 24\}, \qquad \mathcal{B} = \{7, 12, 17, 22\}.$$

So $t \equiv 2 \pmod 5$ on $\mathcal{B}$ and $t \equiv 3, 4$ on $\mathcal{A}$. If $X, Y \in \mathbb{Z}_5^\times$ then $t \equiv -XY \pmod 5$. The parameters $-1/8 \equiv 3$ and $9/8 \equiv 23 \pmod{25}$ lie in $\mathcal{A}$. If $X \in 5\mathbb{Z}_5 \smallsetminus \{0\}$ and $Y \in \mathbb{Z}_5^\times$, we write $t \in \mathcal{T}$ if $-12Y$ is a fifth power in $\mathbb{Z}_5$, that is, if $Y \equiv 2, 11, 14, 23 \pmod{25}$ (the fifth powers of units are the units $\equiv \pm 1, \pm 7 \pmod{25}$), and $t \in \mathcal{B}$ otherwise; equivalently, with $X = 5^k X_1$, $5 \nmid X_1$, $s' = -X_1^5/Y^3$, $t \in \mathcal{T}$ exactly when $s' \equiv 3, 4, 21, 22 \pmod{25}$. For a primitive solution with $5 \nmid YZ$, t lies in exactly one of $\mathcal{T}$, $\mathcal{A}$, $\mathcal{B}$, as $1 - t = Z^p/Y^3$.

Lemma 3.2. *Let $t, t' \in \mathbb{Z}_5$ with $5 \nmid t(1-t)$ and $t \equiv t' \pmod{25}$. Then $Y \equiv Y' \pmod{25}$ for $Y^3 = -1/t$, $Y'^3 = -1/t'$. Let r_i, r_i' be the roots of $\mathcal{F}_{1,Y}$, $\mathcal{F}_{1,Y'}$.*

(a) $v(r_0 - r_0') \geq 3$ and, after renumbering, $v(r_i - r_i') \geq 1$ for $1 \leq i \leq 5$. Then $\mathbb{Q}_5(r_i') = \mathbb{Q}_5(r_i)$, and $g(r_i') = r_j'$ whenever $g \in G_{\mathbb{Q}_5}$ and $g(r_i) = r_j$. In particular $N_{t'} = N_t$.

(b) For every prime $\ell \neq 5$, $V_\ell(J_t)|_{W_F} \cong V_\ell(J_{t'})|_{W_F}$.

Proof. (a) $\mathcal{F}_{1,Y'}(U)-\mathcal{F}_{1,Y}(U) = 12(Y'-Y)U$, so for a cluster root r of $\mathcal{F}_{1,Y}$, $\sum_{j\geq 1} v(r-r'_j) = v(\mathcal{F}_{1,Y'}(r)) \geq 2$. As the r'_j are pairwise at distance $5^{-1/4}$, exactly one, r', has $v(r-r') > 1/4$, and then $v(r-r') \geq 2-1 = 1$; distinct r get distinct partners, and the matching, defined by distances, commutes with $G_{\mathbb{Q}_5}$. Krasner's lemma in both directions gives $\mathbb{Q}_5(r') = \mathbb{Q}_5(r)$. Similarly $v(r_0 - r'_0) = v(\mathcal{F}_{1,Y'}(r_0)) \geq 3$.

(b) With $c = \mathcal{F}'_{1,Y}(r_0) \in \mathbb{Z}_5^\times$, $\gamma \in \mathbb{Q}_5^{\mathrm{ur}}$, $\gamma^2 = c$, $e_i = 1/(r_i - r_0)$, $\varpi^2 = \pi$, the substitutions $w = 1/(U-r_0)$, $y = Vw^3$, $w = e_1 + \pi z$, $y = \varpi^5\gamma y'$ give the smooth model $y'^2 = \prod_{i=1}^5 (z - z_i)$, $z_i = (e_i - e_1)/\pi$, over $L' = N_t(\varpi)$ (the model of Proposition 5.12). As w, y are defined over $\mathbb{Q}_5$, $g \in W_F$ acts on its special fiber $\widetilde{C}$ by

$$(\bar{z}, \bar{y}') \mapsto (\bar{u}_g\, \bar{g}(\bar{z}) + \bar{b}_g,\ \bar{v}_g\, \bar{g}(\bar{y}')), \qquad \bar{u}_g = \operatorname{res} \tfrac{g(\pi)}{\pi},\ \bar{b}_g = \operatorname{res} \tfrac{g(e_1)-e_1}{\pi},\ \bar{v}_g = \operatorname{res} \tfrac{g(\varpi^5\gamma)}{\varpi^5\gamma},$$

$\bar{g}$ being the automorphism of $\overline{\mathbb{F}}_5$ induced by g. The representation $V_\ell(J_t)|_{W_F}$ is the one induced on $V_\ell(\mathrm{Jac}\,\widetilde{C})$ [40, §2, Theorem 2 and its proof]: an element $g \in W_F$ maps the model over $\mathcal{O}_{L'}$ to its g-conjugate, which gives the semilinear automorphism of the special fiber and, by functoriality of the Néron model, the action on V_ℓ. The same construction for t', with the roots numbered as in (a), gives the same field L', the same special fiber and the same action of W_F on it. Indeed, $\bar{u}_g$ does not depend on the curve, and by (a), $\bar{z}'_i = \bar{z}_i$ and $\bar{b}'_g = \bar{b}_g$. As $c'/c \in 1 + 5\mathbb{Z}_5$, we may take $\gamma' = \gamma\sqrt{c'/c}$ with $\sqrt{c'/c} \in \mathbb{Q}_5$, which gives $\bar{v}'_g = \bar{v}_g$. □

3.2. **Cyclic quintic extensions of L_0.** For a finite Galois extension N'/N_0 of fields between $\mathbb{Q}_5^{\mathrm{ur}}$ and $\overline{\mathbb{Q}}_5$, with uniformizer Π, and $h \in \mathrm{Gal}(N'/N_0)$, put $i(h) = v_{N'}(h\Pi - \Pi)$, so that $h \in G_i$ iff $i(h) \geq i+1$ [38, Ch. IV, §1]. If $i(h) \geq 2$,

$$v_{N'}(hx - x) = v_{N'}(x) + i(h) - 1 \qquad \text{for } x \in N'^\times,\ 5 \nmid v_{N'}(x), \tag{3.1}$$

since $\mathcal{O}_{N'} = \mathcal{O}_{N_0}[\Pi]$ gives $v_{N'}(hu - u) \geq i(h)$ for units u, and $h(\Pi^k u)/\Pi^k u = (1+\theta)^k hu/u \equiv 1 + k\theta \pmod{\Pi^{i(h)}}$, where $h\Pi = (1+\theta)\Pi$ and $v_{N'}(\theta) = i(h) - 1$.

Lemma 3.3. *Let $U_j = 1 + \pi^j \mathcal{O}_{L_0}$.*

- *(a) $U_5 \subset L_0^{\times 5}$ and $U_4 \cap L_0^{\times 5} = U_5$, so $\alpha \mapsto 1 + 5\alpha$ induces an $\mathbb{F}_5$-isomorphism $\overline{\mathbb{F}}_5 \to U_4 L_0^{\times 5}/L_0^{\times 5}$. For an $\mathbb{F}_5$-line $\mathcal{L} \subset \overline{\mathbb{F}}_5$ let $N(\mathcal{L}) = L_0((1+5\alpha)^{1/5})$ with $\mathrm{res}(\alpha)$ spanning $\mathcal{L}$.*
- *(b) The $N(\mathcal{L})$ are cyclic of degree 5 over L_0 with lower break 1, and every such extension is $N(\mathcal{L})$ for exactly one $\mathcal{L}$.*
- *(c) Let ϕ be an automorphism of $N(\mathcal{L})$ with $\phi(L_0) = L_0$, restricting to the Frobenius on $\mathbb{Q}_5^{\mathrm{ur}}$ and commuting with $\mathrm{Gal}(N(\mathcal{L})/L_0)$. If $\phi(\zeta_5) = \zeta_5^c$, then $z^5 = cz$ for $z \in \mathcal{L}$.*

Put $N_{\mathcal{B}} = N(\mathbb{F}_5)$ and $N_{\mathcal{A}} = N(\mathcal{L}_{\mathcal{A}})$, $\mathcal{L}_{\mathcal{A}} = \{z : z^5 = -z\}$. Then $N_{\mathcal{A}} \neq N_{\mathcal{B}}$ and $[N_{\mathcal{A}} N_{\mathcal{B}} : L_0] = 25$.

Proof. (a) As $\pi^4 = 5$, $(1+\pi z)^5 \equiv 1 + \pi^5(z + z^5) \pmod{\pi^6}$ and $(1+\pi^j z)^5 \equiv 1 + \pi^{j+4} z \pmod{\pi^{j+5}}$ for $j \geq 2$. As $z \mapsto z + z^5$ is onto $\overline{\mathbb{F}}_5$, successive approximation gives $U_5 \subset L_0^{\times 5}$, and $U_1^5 \subset U_5$. If $y^5 \in U_4$, then $y = \omega(y) y_1$ with $y_1 \in U_1$ and $\omega(y)^5 = 1$, so $y^5 \in U_5$. Finally $(1+5\alpha)(1+5\beta) \equiv 1 + 5(\alpha+\beta) \pmod{\pi^8}$.

(b) Let $N = L_0(y)$, $y^5 = x$, be cyclic of degree 5 (totally ramified, as $\overline{\mathbb{F}}_5$ is algebraically closed), $h(y) = \zeta y$. As prime-to-5 roots of unity are fifth powers in $\mathbb{Q}_5^{\mathrm{ur}}$, we may take $x = \pi^a u$, $0 \leq a \leq 4$, $u \in U_1$. Since $v_N(\zeta - 1) = 5$, (3.1) applied to y if $a \neq 0$, and to $y - 1$ if $a = 0$ and $v(u-1) = j/4$, $1 \leq j \leq 4$ (then $v(y-1) = j/20$), gives the break 5, resp. $5 - j$;

if $u \in U_5$ then $N = L_0$. So the break is 1 exactly when $x = 1 + 5\alpha$ with α a unit, and N determines the line $\mathbb{F}_5 \operatorname{res}(\alpha)$ by (a).

(c) With $N(\mathcal{L}) = L_0(y)$, $y^5 = x = 1 + 5\alpha$: $\phi(y) = y^k\beta$, $\beta \in L_0$, and $\zeta^k\phi(y) = h(\phi y) = \phi(hy) = \zeta^c\phi(y)$, so $\phi(x) \equiv x^c$ modulo fifth powers; and $\operatorname{res}\phi(\alpha) = \operatorname{res}(\alpha)^5$, $x^c \equiv 1 + 5c\alpha \pmod{25}$. □

3.3. **A separation lemma.**

Lemma 3.4. *Let J be one of the Jacobians of Proposition 2.2, with potentially good reduction at $\sqrt{5}$, R the set of roots of its sextic, and ρ_λ the representation of G_K on $V_\lambda(J)$, $\lambda \nmid 5$.*

- *(a) $\rho_\lambda(I_F)$ is a finite subgroup of $\mathrm{SL}_2(K_\lambda)$ of order divisible only by primes ≤ 5, and the traces $\chi_J(h)$, $h \in I_F$, lie in K and do not depend on λ. Let L_J be the fixed field of $\ker \rho_\lambda|_{I_F}$. The group $H_J = \{h : \chi_J(h) = \pm 2\}$ is the kernel of I_F on $J[2]$ and on R; so $F^{\mathrm{ur}}(R) \subseteq L_J$, with $[L_J : F^{\mathrm{ur}}(R)] \le 2$.*
- *(b) Let J', R' be another such pair, $p \ge 7$, $\mathfrak{p} \mid p$, $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}'\}$. If $J[\mathfrak{p}] \cong J'[\mathfrak{q}]$ as $\mathbb{F}_p[I_F]$-modules, then $L_J = L_{J'}$ and $F^{\mathrm{ur}}(R) = F^{\mathrm{ur}}(R')$. An $\mathcal{O}_K$-linear I_F-isomorphism $J[\mathfrak{p}] \to J'[\mathfrak{p}]$ forces $\chi_J = \chi_{J'}$, and a σ-semilinear one $J[\mathfrak{p}] \to J'[\mathfrak{p}']$ forces $\chi_J = \sigma \circ \chi_{J'}$.*
- *(c) If $p \ge 7$, $\rho' \colon G_F \to \mathrm{GL}_2(E)$, $E/\mathbb{Q}_p$ finite, has $\rho'(I_F)$ finite of order prime to p, and $J[\mathfrak{p}]$ and $\bar{\rho}'$ become isomorphic on I_F over a common finite field, then L_J is the fixed field of $\ker \rho'|_{I_F}$.*

Proof. (a) Finiteness and the primes are as in the proof of Lemma 2.7; $\det \rho_\lambda$ is cyclotomic (Section 2.2), trivial on I_F; the characteristic polynomials of $\rho_\lambda(h)$ lie in $K[x]$ and do not depend on λ (Lemma 2.4). A finite-order element of SL_2 with trace ± 2 is ± 1. For $\lambda = (2)$, inert and unramified over $\mathbb{Q}_2$: if h is trivial on $J[2] = T_\lambda/2T_\lambda$, then $g = \rho_\lambda(h) \in 1 + 2M_2(\mathcal{O}_{K_\lambda})$ has g^2 in the torsion-free group $1+4M_2$, so $g^2 = 1$ and $g = \pm 1$. $J[2]$ is generated by differences of Weierstrass points, on which $S_6 \cong \mathrm{Sp}_4(\mathbb{F}_2)$ acts faithfully. So H_J is also the kernel on R, and $\rho_\lambda(H_J) \subseteq \{\pm 1\}$.

(b) The eigenvalues of elements of a group of order prime to p reduce injectively, so representations over p-adic fields with isomorphic reductions are isomorphic. For p split this gives $\rho_{\mathfrak{p}}|_{I_F} \cong \rho'_{\mathfrak{q}}|_{I_F}$ over $\mathbb{Q}_p$; for p inert, $V_p(J)|_{I_F} \cong V_p(J')|_{I_F}$. So the kernels agree, and so do the sets of elements acting by ± 1, which are H_J, $H_{J'}$. An $\mathcal{O}_K$-linear isomorphism lifts over $K_{\mathfrak{p}}$ to $\rho_{\mathfrak{p}}|_{I_F} \cong \rho'_{\mathfrak{p}}|_{I_F}$; a σ-semilinear one is a linear isomorphism onto the reduction of $\sigma_{\mathfrak{p}} \circ \rho'_{\mathfrak{p}'}$, of trace $\sigma \circ \chi_{J'}$, with $\sigma_{\mathfrak{p}} \colon K_{\mathfrak{p}'} \to K_{\mathfrak{p}}$ induced by σ.

(c) This follows by the same lifting, over a common finite extension of $K_{\mathfrak{p}}$ and E. □

3.4. **The fields.**

Proposition 3.5. *Let $X, Y \in \mathbb{Z}_5$, $Y \ne 0$, $5 \nmid Y(X^5 + Y^3)$, $t = -X^5/Y^3$, $N = N_{X,Y}$.*

- *(a) If $5 \nmid X$, the cluster has one root in $\mathbb{Q}_5$ and four generating a totally ramified quartic extension exactly when $t \in \mathcal{T}$, and then $N = L_0$; otherwise $\mathbb{Q}_5(r_1)$ is totally ramified of degree 5.*
- *(b) If $5 \nmid X$ and $t \in \mathcal{A} \cup \mathcal{B}$, $E^{\mathrm{gal}} = \mathbb{Q}_5(r_1, \dots, r_5)$ is totally ramified of degree 20, with group $\mathbb{F}_{20}$ acting on the cluster as the affine group of $\mathbb{F}_5$, and the fixed field of its subgroup of order 5 is*

$$M_t = \mathbb{Q}_5\big((-5(1-t)^2)^{1/4}\big) = \mathbb{Q}_5(\zeta_5) \quad \text{if } t \in \mathcal{B}, \qquad M_t = \mathbb{Q}_5(5^{1/4}) \quad \text{if } t \in \mathcal{A}.$$

(c) *If* $5 \mid X$, *then* $N = L_0$ *for* $t \in \mathcal{T}$, *and* $N = L_0((-12Y)^{1/5})$, *with* $\mathrm{Gal}(N/\mathbb{Q}_5^{\mathrm{ur}}) \cong \mathbb{F}_{20}$, *for* $t \in \mathcal{B}$; *in both cases the cluster roots generate the same fields over* $\mathbb{Q}_5$ *as the roots of* $U^5 + 12Y$, *whose splitting field has quartic subfield* $\mathbb{Q}_5(\zeta_5)$, *as for* $\mathcal{B}$ *in (b).*

(d) *If* $t \in \mathcal{A} \cup \mathcal{B}$, *then* $F^{\mathrm{ur}}(r_0, \dots, r_5) = N = L_0(r_1)$ *is cyclic of degree* 5 *over* L_0 *with lower break* 1, *and* $N = N_{\mathcal{A}}$ *for* $t \in \mathcal{A}$, $N = N_{\mathcal{B}}$ *for* $t \in \mathcal{B}$. *So if* X', Y' *satisfy the same hypotheses as* X, Y *and* $t' = -X'^5/Y'^3$, *then for* $t \in \mathcal{A}$, $t' \in \mathcal{B}$ *and cluster roots* r, r' *of* $\mathcal{F}_{X,Y}$, $\mathcal{F}_{X',Y'}$, $25 \mid e(\mathbb{Q}_5(r, r')/\mathbb{Q}_5)$; *if* t, t' *both lie in* $\mathcal{A}$ *or both in* $\mathcal{B}$, *no such pair has* $25 \mid e$.

(e) *Suppose* $t \in \mathbb{Q}$ *and* $\lambda \nmid 5$. *If* $t \in \mathcal{T}$, $|\rho_{t,\lambda}(I_F)|$ *divides* 4 *and* $\varepsilon_5 = 2$. *In all cases* $V_\lambda(J_t)^{I_F} = 0$, *so* $\varepsilon_5 = 2$ *exactly when* $\rho_{t,\lambda}(I_F)$ *has order prime to* 5. *If* $t \in \mathcal{A} \cup \mathcal{B}$, *then* $[L_{J_t} : N] = 2$, $\rho_{t,\lambda}(I_F)$ *is binary dihedral of order* 20, *its subgroup of order* 5 *has lower break* 2, *and* $\varepsilon_5 = 3$. *The field* L_{J_t} *depends only on* N.

(f) *Let* X', Y', t' *be as in* (d). *If* t, t' *both lie in* $\mathcal{A}$, *or both in* $\mathcal{B}$ *with* $5 \nmid XX'$, *then the fields* E^{gal} *of (b) for* t *and for* t' *are equal.*

Proof. Let $\mathcal{F} = \mathcal{F}_{X,Y}$, $c \in \mathbb{Z}_5$ with $c \equiv 3Y$, and $\mathcal{F}(c + w) = \sum a_k w^k$. The valuations of $a_6, \dots, a_0$ are 0, 0 ($a_5 = 6c$), 1 ($a_4 = 15c^2$), ≥ 1, 1 ($a_2 = 15c(c^3 + 2X)$, $c^3 + 2X \equiv 2(X + Y^3)$), ≥ 1, ≥ 1. If $v(a_0) = 1$, the Newton polygon gives $v(r_i - c) = 1/5$ for the cluster, which is then wild of degree 5. If $v(a_0) \geq 2$, then $v(a_1) = 1$, since otherwise three cluster roots would be within $5^{-1/3}$ of each other (Lemma 2.18(a)). So one cluster root r_* lies in $\mathbb{Q}_5$, the others satisfy $v(r_i - r_*) = 1/4$ and have degree at most 4, hence generate tame totally ramified quartic extensions, and $N = L_0$.

(a) $\mathcal{F}(c)$ mod 25 does not depend on c; take $c = 3Y$: $\mathcal{F}(3Y) = 729Y^6 + 270XY^3 + 36Y^2 + 5X^2$. If $5 \nmid X$, with $Y^4 = 1 + 5e$ and $m = XY \equiv -t$,

$$\mathcal{F}(3Y) \equiv 5Y^2(3 + 4e + 4m + m^2) \pmod{25},$$

so $v(\mathcal{F}(3Y)) \geq 2$ iff $e \equiv (t-1)(t-3) \pmod 5$. As $X^5 \equiv \omega(X)$ and $Y \equiv \omega(Y)(1 - 5e)$ modulo 25, $t \equiv \omega(t)(1 - 10e)$; with $\omega(2) \equiv 7$, $\omega(3) \equiv 18$, $\omega(4) \equiv 24$ the condition reads $t \equiv 7 \cdot 11 \equiv 2$, $t \equiv 18$, $t \equiv 24 \cdot 21 \equiv 4 \pmod{25}$: this is $\mathcal{T}$.

(b) Differences of cluster roots have valuation $1/4$, so 20 divides the ramification index of E^{gal}. Its group is a solvable transitive subgroup of S_5 of order divisible by 20, so $\mathbb{F}_{20}$, and E^{gal} is totally ramified. Its cyclic quartic subfield is $M_t = \mathbb{Q}_5((5u)^{1/4})$ for a unit u, and since the residue field is $\mathbb{F}_5$, $u \equiv \mathrm{res}(x^4/5)$ for every $x \in E^{\mathrm{gal}}$ with $v(x) = 1/4$. For $x = \delta = r_j - r_i$, the expansion of $\mathcal{F}(r_i + \delta)/\delta = 0$ has all terms of valuation $\geq 5/4$ except $\mathcal{F}'(r_i)$ and $6r_i\delta^4$, so $6r_i\delta^4 \equiv -\mathcal{F}'(r_i)$; and $U\mathcal{F}'(U) = 6\mathcal{F}(U) - 30(XU^3 + 2YU + X^2)$. With $r_i \equiv 3Y$, $Y^6 \equiv Y^2$:

$$u \equiv \frac{Xr_i^3 + 2Yr_i + X^2}{r_i^2} \equiv \frac{(X + Y^3)^2}{4Y^2} \equiv -(1 + XY)^2 \equiv -(1 - t)^2 \pmod 5,$$

which is -1 for $t \equiv 2$ (and $\mathbb{Q}_5((-5)^{1/4}) = \mathbb{Q}_5(\zeta_5)$) and 1 for $t \equiv 3, 4$.

(c) For a root β of $U^5 + 12Y$, $v(\mathcal{F}(\beta)) = v(10X\beta^3 + 5X^2) \geq 2$, and the argument of Lemma 3.2(a), with the roots $\beta\zeta_5^k$ in place of the cluster of $\mathcal{F}_{1,Y'}$, matches them with the cluster, preserving fields. Write $-12Y = \omega(-12Y)(1 + 5g)$; it is a fifth power iff $5 \mid g$, i.e. $t \in \mathcal{T}$, and then $N = \mathbb{Q}_5^{\mathrm{ur}}(\zeta_5) = L_0$. Otherwise $N = L_0(\beta)$ has degree 5 over L_0 (Lemma 3.3(a)), and $\mathrm{Gal}(L_0/\mathbb{Q}_5^{\mathrm{ur}})$ acts faithfully on $\mathrm{Gal}(N/L_0) \cong \mu_5$.

(d) In case (b), $N = \mathbb{Q}_5^{\mathrm{ur}}E^{\mathrm{gal}} \supseteq \mathbb{Q}_5^{\mathrm{ur}}M_t = L_0$ and $N = L_0(r_1)$; (3.1) with $v_N(r_1 - c) = 4$, $v_N(hr_1 - r_1) = 5$, for h a generator of $\mathrm{Gal}(N/L_0)$, gives the break 1, so $N = N(\mathcal{L})$. In $\mathrm{Gal}(N/M_t) = \mathrm{Gal}(\mathbb{Q}_5^{\mathrm{ur}}/\mathbb{Q}_5) \times \mathrm{Gal}(E^{\mathrm{gal}}/M_t)$ the Frobenius ϕ of the first factor commutes with $\mathrm{Gal}(N/L_0)$. It fixes ζ_5 if $M_t = \mathbb{Q}_5(\zeta_5)$; if $M_t = \mathbb{Q}_5(5^{1/4})$ it fixes π and sends $\zeta_8\pi = (-5)^{1/4}$

to $-\zeta_8\pi$, so $\phi(\zeta_5) = \zeta_5^{-1}$. Lemma 3.3(c) gives $\mathcal{L} = \mathbb{F}_5$ on $\mathcal{B}$ and $\mathcal{L} = \mathcal{L}_\mathcal{A}$ on $\mathcal{A}$. In case (c), $N = L_0((1+5g)^{1/5}) = N_\mathcal{B}$ with $5 \nmid g$. For the pairs, $L_0(r) = N_t$ and $L_0(r') = N_{t'}$. If $t \in \mathcal{A}$ and $t' \in \mathcal{B}$, then $[L_0(r,r') : L_0] = 25$ and $[L_0(r,r') : \mathbb{Q}_5^{\mathrm{ur}}(r,r')] \mid 4$, so $25 \mid [\mathbb{Q}_5^{\mathrm{ur}}(r,r') : \mathbb{Q}_5^{\mathrm{ur}}] = e(\mathbb{Q}_5(r,r')/\mathbb{Q}_5)$. If t, t' both lie in $\mathcal{A}$ or both in $\mathcal{B}$, then $\mathbb{Q}_5^{\mathrm{ur}}(r,r') \subseteq N_t$, which has degree 20 over $\mathbb{Q}_5^{\mathrm{ur}}$.

(e) By Lemma 2.18 and Lemma 3.4(a), $\Phi = \rho_{t,\lambda}(I_F) \cong \mathrm{Gal}(L_{J_t}/F^{\mathrm{ur}})$ with $[L_{J_t} : N] \le 2$. First, $V_\lambda(J_t)^{I_F} = 0$. By Proposition 5.12, whose proof uses only Lemma 2.18(a) and so applies to all $X, Y \in \mathbb{Z}_5$ with $5 \nmid Y(X^5 + Y^3)$, each $\tau \in I_F$ acts on the special fiber $\widetilde{C}$ by $z \mapsto \theta_5(\tau)^{-2} z + b(\tau)$, and on dz/y' by $\theta_5(\tau)^3$, with θ_5, $\widetilde{C}$, z and y' as in §5.3. If $\theta_5(\tau_0)$ has order 4, the image g of τ_0 acts on dz/y' by an element of order 4, so $g^2 \ne 1$, while g^2 fixes z. So g^2 is the hyperelliptic involution, which acts by -1 on $V_\ell(\mathrm{Jac}\,\widetilde{C})$, and $V_\ell(J_t)^{\tau_0} = 0$ [40, §2]. Hence ε_5 is 2 plus the Swan conductor, and equals 2 exactly when Φ has order prime to 5. If $t \in \mathcal{T}$, $[N : F^{\mathrm{ur}}] = 2$, so $|\Phi| \mid 4$, the Swan conductor is 0 and $\varepsilon_5 = 2$. If $t \in \mathcal{A} \cup \mathcal{B}$, $\Phi/(\Phi \cap \{\pm 1\}) \cong \mathrm{Gal}(N/F^{\mathrm{ur}}) \cong D_5$, the index-2 subgroup of $\mathbb{F}_{20}$; a lift g of an involution has $g^2 = -1$, -1 being the only involution of SL_2, so $|\Phi| = 20$, Φ has a unique involution and is binary dihedral. For $h \in \Phi$ of order 5, in $L = L_{J_t}$ ($e(L/\mathbb{Q}_5^{\mathrm{ur}}) = 40$) $v_L(r_1 - c) = 8$ and $v_L(hr_1 - r_1) = 10$, so $i(h) = 3$ and $G_0 = \Phi$, $G_1 = G_2 = \langle h \rangle$, $G_3 = 1$. As $V^{G_1} = 0$, the conductor exponent is $2 + 2 \cdot \frac{5}{20} \cdot 2 = 3$ [38, Ch. VI, §2].

For the last assertion, if $t \in \mathcal{T}$, the image g of τ_0 has order 4, so $|\Phi| = 4$ and L_{J_t} is $F^{\mathrm{ur}}(5^{1/8})$, the only tamely ramified extension of F^{ur} of degree 4. Let $t \in \mathcal{A} \cup \mathcal{B}$. If $N_{t'} = N$, let ψ, ψ' be the projections of $\Gamma = \mathrm{Gal}(\overline{\mathbb{Q}}_5/F^{\mathrm{ur}})$ to $\mathrm{Gal}(L_{J_t}/F^{\mathrm{ur}})$, $\mathrm{Gal}(L_{J_{t'}}/F^{\mathrm{ur}})$. Automorphisms of D_5 lift to $\langle a, b \mid a^{10} = 1, b^2 = a^5, bab^{-1} = a^{-1} \rangle$ ($a \mapsto a^k$, $b \mapsto a^m b$), so there is an isomorphism β between these groups compatible with restriction to N. Then $g \mapsto \psi(g)(\beta\psi'(g))^{-1}$ is a homomorphism $\Gamma \to \{\pm 1\}$, trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}_5/L_0)$ as $L_0 \subset N$ is the only quadratic extension of F^{ur}. Since $\ker\psi, \ker\psi' \subset \mathrm{Gal}(\overline{\mathbb{Q}}_5/N)$, they are equal.

(f) Let E, E' be the two fields, $N = N_t = N_{t'}$ (by (d)), $\Gamma = \mathrm{Gal}(N/\mathbb{Q}_5)$ and $I = \mathrm{Gal}(N/\mathbb{Q}_5^{\mathrm{ur}}) \cong \mathbb{F}_{20}$ (by (b)). As E is Galois and totally ramified over $\mathbb{Q}_5$ and $\mathbb{Q}_5^{\mathrm{ur}} E = N$, $H = \mathrm{Gal}(N/E)$ is normal in Γ, $H \cap I = 1$, and restriction maps H isomorphically onto $\mathrm{Gal}(\mathbb{Q}_5^{\mathrm{ur}}/\mathbb{Q}_5)$. Being normal with trivial intersection, H and I commute. Let $\phi \in H$ and $\phi' \in H' = \mathrm{Gal}(N/E')$ restrict to the Frobenius of $\mathbb{Q}_5^{\mathrm{ur}}$. Then $\phi'\phi^{-1} \in I$ commutes with I, so it lies in the center of $\mathbb{F}_{20}$, which is trivial. Hence $\phi = \phi'$, so $H = H'$, each being the closed subgroup generated by ϕ, resp. ϕ'; and $E = E'$. □

3.5. **The classes allowed by a congruence.**

Theorem 3.6. *Let $p \ge 7$ be prime, (X, Y, Z) a primitive solution of $X^5 + Y^3 = Z^p$, $t = -X^5/Y^3$, and $\mathfrak{p}$ a prime of K above p.*

- *(a) If $\bar\rho_{t,\mathfrak{p}}$ is congruent to J_s for some $s \in \{-1/8, 9/8\}$, then $5 \nmid XYZ$ and $t \in \mathcal{A}$, that is, $t \equiv 3, 8, 9, 13, 14, 19, 23, 24 \pmod{25}$; in particular $X \equiv Y^3$ or $X \equiv 2Y^3 \pmod 5$.*
- *(b) If $5 \nmid XYZ$ and $t \in \mathcal{A}$ (where $\varepsilon_5 = 3$ by Proposition 3.5(e)), then $\bar\rho_{t,\mathfrak{p}}$ is not congruent to the residual representation of any Hilbert newform over K with complex multiplication whose level is divisible only by 3 and $\sqrt{5}$.*

Proof. (a) By Corollary 2.21, $5 \nmid YZ$, so J_t, like J_s, has potentially good reduction at $\sqrt{5}$ (Lemma 2.18), and $N_t = N_s = N_\mathcal{A}$ by Lemma 3.4(b) and Proposition 3.5(d). If $5 \mid X$ or $t \in \mathcal{T} \cup \mathcal{B}$, N_t is L_0 or $N_\mathcal{B}$ by Proposition 3.5(a),(c),(d). So $t \in \mathcal{A}$, and $X \equiv -tY^3 \equiv 2Y^3$ or Y^3.

(b) Let $\mathcal{G}$ have complex multiplication by M, so $\rho_{\mathcal{G},\mathfrak{P}} = \mathrm{Ind}_{G_M}^{G_K} \psi_{\mathfrak{P}}$ for a character $\psi_{\mathfrak{P}}$ of G_M. An induced representation is ramified where M/K is, so, comparing primes $\mathfrak{P}$ of two different residue characteristics, M/K is unramified outside $3\sqrt{5}$. The quadratic character of M/K is tame at 3 and $\sqrt{5}$ and odd at both real places, so it factors through $\mathrm{Cl}_K(3\sqrt{5}\,\infty_1\infty_2)$. By Lemma 2.23(c), $M = K(\sqrt{-3})$ or $\mathbb{Q}(\zeta_5)$. With w the prime of M above $\sqrt{5}$, $\rho_{\mathcal{G}}|_{G_F} \cong \mathrm{Ind}_{G_{M_w}}^{G_F} \psi_w$, and ψ_w on inertia factors through some $\mathcal{O}_w^\times/(1+\mathfrak{m}_w^n)$, of order $(q-1)q^{n-1}$, $q \in \{5, 25\}$; so $\rho_{\mathcal{G}}(I_F)$ is finite of order prime to p. If $\bar{\rho}_{t,\mathfrak{p}}$ is congruent to $\rho_{\mathcal{G}}$, Lemma 3.4(c) gives $L_{J_t} = L_{\mathcal{G}}$, which contains $N_t = N_{\mathcal{A}}$ with $\mathrm{Gal}(N_t/F^{\mathrm{ur}}) \cong D_5$ (Proposition 3.5(d),(e)).

If $M = K(\sqrt{-3})$, $\sqrt{5}$ is inert in M (Lemma 2.23(d)), so $\rho_{\mathcal{G}}|_{I_F} = \psi_w \oplus \psi_w^c$ has abelian image, and N_t would be abelian over F^{ur}.

If $M = \mathbb{Q}(\zeta_5)$, $M_w = \mathbb{Q}_5(\zeta_5)$ has inertia group $\mathrm{Gal}(\overline{\mathbb{Q}}_5/L_0)$, of index 2 in I_F, acting through $\psi_w \oplus \psi_w^c$ with image of order divisible by 5 (as $|\rho_{\mathcal{G}}(I_F)| = 20$); ψ_w and its conjugate ψ_w^c have the same image there, so ψ_w cuts out over L_0 a cyclic extension, abelian over M_w, of degree divisible by 5, contained in $L_{\mathcal{G}}L_0$. Let W_0 be its subextension of degree 5 over L_0. As $L_0 \subseteq N_t \subseteq L_{J_t} = L_{\mathcal{G}}$, W_0 lies in L_{J_t}, and $\mathrm{Gal}(L_{J_t}/L_0)$, the preimage of $\mathrm{Gal}(N_t/L_0)$ in the binary dihedral group $\mathrm{Gal}(L_{J_t}/F^{\mathrm{ur}})$ (Proposition 3.5(e)), is cyclic of order 10. So N_t is the only subextension of L_{J_t}/L_0 of degree 5, and $W_0 = N_t$. A Frobenius lift $\phi \in \mathrm{Gal}(N_t/M_w)$ commutes with $\mathrm{Gal}(N_t/L_0)$ and fixes ζ_5, so $N_t = N_{\mathcal{B}}$ by Lemma 3.3(c), a contradiction. □

3.6. **One special parameter for each class.** For $\lambda \nmid 5$ let $\rho_{t,\lambda}^{\sigma} = \sigma_\lambda \circ \rho_{t,\sigma(\lambda)}$, with $\sigma_\lambda \colon K_{\sigma(\lambda)} \to K_\lambda$ induced by σ. Its traces are the σ-conjugates of those of $\rho_{t,\lambda}$. Let $\mathcal{A}_{\mathbb{Q}}$ be the set of $t \in \mathbb{Q}$ with $v_5(t) = 0$ and $t \bmod 25 \in \mathcal{A}$. It contains $-1/8$, $9/8$ and the parameters of the primitive solutions with $5 \nmid XYZ$, $t \in \mathcal{A}$. The orientations are those of Definition 4.5, for the real multiplication of Proposition 2.2 normalized as in Definition 4.2; §4.1 uses nothing from this section.

Theorem 3.7. *(a) For every prime $\lambda \nmid 30$ of K, $\rho_{-1/8,\lambda}$ and $\rho_{9/8,\lambda}$ are isomorphic on the decomposition groups at (2), at (3) and at the two real places.*

(b) For $t, t' \in \mathcal{A}_{\mathbb{Q}}$ there is a unique pair $(o, e) = (o(t,t'), e(t,t')) \in \{0,1\}^2$ with

$$\rho_{t,\lambda}|_{W_F} \cong (\rho_{t',\lambda}^{\sigma^o} \otimes \mu^e)|_{W_F} \qquad \text{for every prime } \lambda \nmid 5 \text{ of } K.$$

For every prime $\ell \neq 5$, $V_\ell(J_t)|_{W_F} \cong V_\ell(J_{t'})|_{W_F} \otimes \mu^{e(t,t')}$, and $e(t,t')$ depends only on $t \bmod 25$ and $t' \bmod 25$.

(c) $e(9/8, -1/8) = 1$. Hence for each $t \in \mathcal{A}_{\mathbb{Q}}$ exactly one $s = s(t) \in \{-1/8, 9/8\}$ has $e(t,s) = 0$, and $s(t)$ depends only on $t \bmod 25$.

(d) Let $p \geq 7$, let (X,Y,Z) be a primitive solution with $5 \nmid XYZ$ and $t \in \mathcal{A}$, let $s \in \{-1/8, 9/8\}$ and $\mathfrak{p} \mid p$. A congruence of $J_t[\mathfrak{p}]$ with J_s in the direct orientation forces $(o(t,s), e(t,s)) = (0,0)$, and one in the conjugate orientation forces $(o(t,s), e(t,s)) = (1,0)$.

A congruence with $J_{s(t)}$ is in the direct orientation if $o(t, s(t)) = 0$ and in the conjugate one if $o(t, s(t)) = 1$; $o(t, s(t))$ depends only on $t \bmod 25$ by Proposition 4.15(b); Propositions 4.11 and 4.15 determine $s(t)$ and $o(t, s(t))$.

Proof. The traces of $\rho_{t,\lambda}$ on W_F lie in K and do not depend on $\lambda \nmid 5$ (Lemma 2.4). As $\rho_{t,\lambda}|_{I_F}$ is absolutely irreducible for $t \in \mathcal{A}_{\mathbb{Q}}$ (Proposition 3.5(e)), they determine $\rho_{t,\lambda}|_{W_F}$ up to isomorphism, and so do those of $\rho_{t,\lambda}^{\sigma}$ and of their twists by μ; so the relations below hold for one λ iff for all.

(b) By Proposition 3.5(d),(e), $L_{J_t} = L_{J_{t'}} =: L$, and $\rho_{t,\lambda}|_{I_F}$, $\rho_{t',\lambda}|_{I_F}$ are faithful 2-dimensional representations of the binary dihedral group $\mathrm{Gal}(L/F^{\mathrm{ur}})$. It has exactly two such, induced from $a \mapsto \zeta_{10}$ and $a \mapsto \zeta_{10}^3$ for a generator a of its cyclic subgroup of order 10, with traces $(-1 \pm \sqrt{5})/2$ on elements of order 5, exchanged by σ; so $\rho_{t,\lambda}|_{I_F} \cong \rho_{t',\lambda}^{\sigma^o}|_{I_F}$ for exactly one o. Then W_F acts on the line $\mathrm{Hom}_{I_F}(\rho_{t',\lambda}^{\sigma^o}, \rho_{t,\lambda})$ by an unramified χ with $\chi^2 = 1$ (both determinants are cyclotomic), so $\chi = \mu^e$; e is unique, as Frobenius acts by -1 on $\mathrm{Hom}_{I_F}(\rho, \rho \otimes \mu)$. Summing over the embeddings of K gives the relation for V_ℓ; by Krull–Schmidt it determines e (as $\rho_{t',\lambda} \otimes \mu$ is isomorphic neither to $\rho_{t',\lambda}$ nor, on I_F, to $\rho_{t',\lambda}^{\sigma}$), and $V_\ell(J_t)|_{W_F}$ depends only on t mod 25 (Lemma 3.2(b)).

(a) At (2): as $2 \mid Y$ for both models of Section 2.4, both curves reduce to $w^2+(U^3+1)w = 1$ over $\mathbb{F}_2$, with Frobenius polynomial $(x^2 + x + 4)^2$ over $\mathbb{F}_4$, and $x^2 + x + 4$ is irreducible over K (Lemma 2.22); so $\mathrm{Frob}_{(2)}$ has characteristic polynomial $x^2 + x + 4$, with distinct roots, for both. At a real place complex conjugation has eigenvalues ± 1 for both. At (3): $\rho_{s,\lambda}(I_3)$ is finite and irreducible (Lemma 2.7), with normal Sylow 3-subgroup and cyclic quotient, so it is binary dihedral of order $4 \cdot 3^k$ (it is Dic_3, Lemma 5.9 and Proposition 5.10) and its order is prime to 5. By Lemma 5.17, $J_s[\sqrt{5}] \cong A_s[5] \otimes \chi_0$ as $\mathbb{F}_5[G_{\mathbb{Q}}]$-modules with the same χ_0 for both special parameters, and $A_{-1/8}$, $A_{9/8}$ are linked by a cyclic isogeny of degree 9 over $\mathbb{Q}$ (Remark 3.8(iii)); so $J_{-1/8}[\sqrt{5}] \cong J_{9/8}[\sqrt{5}]$ as $\mathbb{F}_5[G_{\mathbb{Q}}]$-modules, and they are irreducible on I_3. Lifting on I_3, $\rho_{9/8,\sqrt{5}} \cong \rho_{-1/8,\sqrt{5}} \otimes \chi$ at (3) with χ unramified, $\chi^2 = 1$; modulo $\sqrt{5}$, Frobenius acts on $\mathrm{Hom}_{I_3}(\bar\rho, \bar\rho \otimes \bar\chi)$ by $\bar\chi$ and fixes a nonzero vector, so $\chi = 1$. As the traces of $\rho_{s,\lambda}$ on W_{K_3} lie in K and do not depend on $\lambda \nmid 3$ (Lemma 2.4), and $\rho_{s,\lambda}|_{I_3}$ is absolutely irreducible (its image is the nonabelian group Dic_3), this holds on W_{K_3}, and so, by continuity, on its closure G_{K_3}, for all $\lambda \nmid 30$.

(c) By Lemma 4.10, which uses only (b), and Lemma 4.9(d), $(-1)^{e(9/8,-1/8)} = (m(9/8)\, m(-1/8)/5) = (2/5) = -1$. Composing the relations of (b), $e(t, 9/8) \equiv e(t, -1/8)+1 \pmod 2$, which defines $s(t)$, depending only on t mod 25 by (b).

(d) A direct, resp. conjugate, congruence is an isomorphism between the reductions of $\rho_{t,\mathfrak{p}}$ and $\rho' = \rho_{s,\mathfrak{p}}$, resp. $\rho' = \rho_{s,\mathfrak{p}}^{\sigma}$ (proof of Lemma 3.4(b)). As the inertia image has order 20, prime to p, $\rho_{t,\mathfrak{p}}|_{I_F} \cong \rho'|_{I_F}$, and since $\rho_{s,\mathfrak{p}}|_{I_F} \not\cong \rho_{s,\mathfrak{p}}^{\sigma}|_{I_F}$, $o = 0$, resp. $o = 1$. Then $\bar\rho' \cong \bar\rho' \otimes \bar\mu^e$, with $\bar\rho'$ absolutely irreducible on I_F; Frobenius acts on $\mathrm{Hom}_{I_F}(\bar\rho', \bar\rho' \otimes \bar\mu^e)$ by $(-1)^e \neq 1$ unless $e = 0$. □

Remark 3.8. Computations for Theorem 3.7 (PARI/GP). (i) $C_{1,2} \cong C_{-1/8}$ and $C_{-3,6} \cong C_{9/8}$ have conductor $3^6 5^5$ (`genus2red`). (ii) Numerically, without a rigorous error bound, `lfunrootres` gives, and `lfuncheckfeq` confirms with this conductor, the global root numbers $w(J_{-1/8}/\mathbb{Q}) = -1$ and $w(J_{9/8}/\mathbb{Q}) = +1$ (item C5; reading these values as root numbers uses the modularity of J_s, Section 2.4, [33, Theorem 2.4(1)]). Their ratio -1 agrees with Theorem 3.7(c): by inductivity in degree 0 [42, §3], good reduction outside 15, Theorem 3.7(a) at (3) and, at the real places, the Hodge types, the same for both (Proposition 2.2(b)), the ratio is that of the root numbers of $\rho_{9/8,\lambda}|_{W_F}$ and $\rho_{-1/8,\lambda}|_{W_F}$, which is $(-1)^{e(9/8,-1/8)}$ by Theorem 3.7(b), as conjugating the coefficients by σ, which amounts to conjugating $\rho_{t,\lambda}|_{W_F}$ by an element of $W_{\mathbb{Q}_5} \smallsetminus W_F$ (Proposition 2.2(c)), leaves the root number unchanged, and the unramified quadratic twist multiplies it by $(-1)^3$, 3 being the conductor exponent [42, §3.4]. (iii) $A_{-1/8}$, $A_{9/8}$ have conductor 27, minimal models $y^2 + y = x^3 - 30x + 63$, $y^2 + y = x^3 - 7$, and a cyclic isogeny of degree 9 over $\mathbb{Q}$ between them (`ellisomat`); this is used in the proof of Theorem 3.7(a). No part of Theorem 3.7 uses a statement of [33].

3.7. **The classes with 5 | X.** For $c \in \{1,3,9,27,81\}$ let $J_{0,c} = \mathrm{Jac}(C_{0,c})$, $C_{0,c}\colon V^2 = U^6 + 12cU$; so $J_{0,1} = J_0$, and $c^4 \equiv 1, 6, 11, 16, 21 \pmod{25}$ respectively. The real multiplication of Proposition 2.2 extends to $J_{0,c}$ by the argument given there for J_0 (with the family $C_{X,c}$), with the same eigenvalue on $U\,dU/V$, and we normalize it as in Definition 4.2. By Proposition 3.5(c), $J_{0,27}$ is tame at $\sqrt{5}$ ($-12 \cdot 27 \equiv 1 \pmod{25}$) and the others are wild, with $N_{0,c} = N_{\mathcal{B}}$. For a Jacobian J with real multiplication as in Proposition 2.2, potentially good reduction at $\sqrt{5}$ and wild inertia there, we say J has *type* (o,e) *relative to* J_0 if $\rho_{J,\lambda}|_{W_F} \cong (\rho_{0,\lambda}^{\sigma^o} \otimes \mu^e)|_{W_F}$. When $N_J = N_{\mathcal{B}}$ such a pair exists, is unique and does not depend on $\lambda \nmid 5$, by the proof of Theorem 3.7(b) with $N_{\mathcal{B}}$ in place of $N_{\mathcal{A}}$. This is the notion of Theorem 3.7(b), now relative to J_0, and agrees with Definition 4.6.

Lemma 3.9. *Relative to J_0, $J_{0,1}$ and $J_{0,3}$ have type $(0,0)$, and $J_{0,9}$ and $J_{0,81}$ have type $(1,1)$. The four representations $(\rho_{0,\lambda}^{\sigma^o} \otimes \mu^e)|_{W_F}$, $(o,e) \in \{0,1\}^2$, are the only representations of W_F with cyclotomic determinant whose restriction to I_F has the trace function χ_{J_0} or $\sigma \circ \chi_{J_0}$ (Lemma 3.4(a)), and their reductions modulo a prime $\mathfrak{p}$ above $p \geq 7$ are pairwise nonisomorphic.*

Proof. Let $E = \mathbb{Q}_5(\zeta)$, $\zeta = \zeta_5$, τ the generator of $\mathrm{Gal}(E/F)$, $\pi_E = 1 - \zeta$, $\mathcal{U}^1 = 1 + \pi_E\mathcal{O}_E$, and ψ_0 the character $1 + a\pi_E \mapsto \zeta^a$ of $\mathcal{U}^1/\mathcal{U}^2 \cong \mathbb{F}_5$. The automorphism $[\zeta](U,V) = (\zeta U, \zeta^3 V)$ of $C_{0,c}$ commutes with the real multiplication (both are diagonal on dU/V, $U\,dU/V$; Lemma 2.5), so for $\ell \equiv 1 \pmod 5$, $\rho_{0,c,\lambda}|_{W_F} = \mathrm{Ind}_{W_E}^{W_F}\theta_c$ for a character θ_c of $E^\times$ (local class field theory), with $\theta_c|_{\mu_4}$ the Legendre symbol as the determinant is cyclotomic. The prime λ does not matter (Theorem 3.7, proof). The isomorphism $(U,V) \mapsto (c^{1/5}U, c^{3/5}V)$ from $C_{0,1}$ to $C_{0,c}$ commutes with $[\zeta]$ and multiplies $U\,dU/V$ by a scalar, so it respects the real multiplication and $\theta_c = \theta_1 \cdot (c,\cdot)_E^{\varepsilon}$, with $(\cdot,\cdot)_E$ the Hilbert symbol of degree 5 and a fixed $\varepsilon = \pm 1$; $(c,\cdot)_E$ is trivial on $\mathbb{Q}_5^\times$ (its restriction to $\mathbb{Q}_5^\times$ is fixed by the automorphism of E of cyclotomic character 2 and raised to the power 2 by that automorphism).

Wild parts. Write $\theta_1|_{\mathcal{U}^1} = \psi_0^n$, $n \not\equiv 0$ (J_0 is wild) and $(3,\cdot)_E^{\varepsilon}|_{\mathcal{U}^1} = \psi_0^j$. As $J_{0,27}$ is tame, $n + 3j \equiv 0$, so $\theta_{3^k}|_{\mathcal{U}^1} = \psi_0^{n(1+3k)}$, that is $\psi_0^n, \psi_0^{-n}, \psi_0^{2n}, 1, \psi_0^{-2n}$ for $c = 1,3,9,27,81$. Since $\theta^\tau|_{\mathcal{U}^1} = (\theta|_{\mathcal{U}^1})^{-1}$ and $\rho_{0,\lambda}^{\sigma} = \mathrm{Ind}(\tilde{\sigma}\theta_1)$ with $\tilde{\sigma}(\zeta) = \zeta^2$ has wild part $\psi_0^{\pm 2n}$, $o = 0$ for $c = 1,3$ and $o = 1$ for $c = 9, 81$.

Unramified parts. Let $\theta' \in \{\theta_1, \theta_1^\tau\}$ ($o = 0$) or $\{\tilde{\sigma}\theta_1, (\tilde{\sigma}\theta_1)^\tau\}$ ($o = 1$) with $\theta'|_{\mathcal{U}^1} = \theta_c|_{\mathcal{U}^1}$. Then θ_c/θ' is trivial on μ_4, $\mathcal{U}^1$ and $F^\times$, so it is 1 or $\mu \circ N_{E/F}$, according to the sign $\theta_c(\pi_E)/\theta'(\pi_E)$, as $\mu \circ N_{E/F}(\pi_E) = -1$. If $o = 0$, both $\theta_c(\pi_E)$ and $\theta_1^\tau(\pi_E) = \theta_1(-\zeta^{-1})\theta_1(\pi_E)$ lie in $\mu_5\theta_1(\pi_E)$, so $e = 0$. If $o = 1$, the ratio lies in $\mu_5\,\theta_1(\pi_E)/\tilde{\sigma}(\theta_1(\pi_E))$. Let ψ_1 be the Hecke character of $\mathbb{Q}(\zeta_5)$ attached to J_0; its infinity type is a CM type $\Phi = \{a,b\}$, that is, the pair of embeddings $\zeta \mapsto \zeta^a$, $\zeta \mapsto \zeta^b$ with $a, b \in (\mathbb{Z}/5)^\times$ and $b \neq \pm a$. We evaluate ψ_1 on the principal idele of $\pi_E = 1 - \zeta$. The element π_E is a unit at every finite place except $P_5 = (\pi_E)$, and ψ_1 is unramified outside P_3P_5, since the conductor of J_0 is $3^2(\sqrt{5})^3$ (Lemma 2.5). At $P_3 = 3\mathcal{O}$ the restriction of ψ_1 to units has order 5, since the image of inertia at 3 of J_0 has order 5 (Lemma 2.24 with $(X,Y) = (0,1)$). So $\theta_1(\pi_E) \in \mu_5\Phi(\pi_E)^{\pm 1}$, and $\theta_1(\pi_E)/\tilde{\sigma}(\theta_1(\pi_E)) \in \mu_5\big(\Phi(\pi_E)/\tilde{\sigma}\Phi(\pi_E)\big)^{\pm 1}$, where

$$\frac{\Phi(\pi_E)}{\tilde{\sigma}\Phi(\pi_E)} = \frac{(1-\zeta^a)(1-\zeta^b)}{(1-\zeta^{2a})(1-\zeta^{2b})} = \frac{1}{(1+\zeta^a)(1+\zeta^b)} \in -\mu_5$$

for each CM type, as $(1+\zeta)(1+\zeta^2) = -\zeta^4$, $(1+\zeta)(1+\zeta^3) = -\zeta^2$, $(1+\zeta^2)(1+\zeta^4) = -\zeta^3$, $(1+\zeta^3)(1+\zeta^4) = -\zeta$. Hence the ratio is -1 and $e = 1$.

A representation whose restriction to I_F has the trace function χ_{J_0} or $\sigma\circ\chi_{J_0}$ is $\operatorname{Ind}\theta$ with $\theta|_{\mathcal{U}^1}$ one of $\psi_0^{\pm n},\psi_0^{\pm 2n}$ and $\theta(\pi_E)$ fixed up to sign by the determinant, which gives the four types. Modulo $\mathfrak{p}$, the wild parts $\psi_0^{\pm n}$ and $\psi_0^{\pm 2n}$ stay distinct (on an element of order 5 of inertia the traces are T and $\sigma(T)$, with $T-\sigma(T)=\pm\sqrt{5}$ a unit at $\mathfrak{p}$), and $\bar\mu\circ N_{E/F}(\pi_E)=-1\neq 1$. □

Proposition 3.10. *Let $X,Y\in\mathbb{Z}_5$ with $5\mid X$ and $5\nmid Y$, and let $c\in\{1,3,9,27,81\}$ with $c^4\equiv Y^4 \pmod{25}$.*

(a) For every prime $\ell\neq 5$, $V_\ell(J_{X,Y})|_{W_F}\cong V_\ell(J_{0,c})|_{W_F}$, where $J_{X,Y}=\operatorname{Jac}(C_{X,Y})$.

(b) Hence, by Lemma 3.9: if $Y^4\equiv 16 \pmod{25}$ (that is, $t\in\mathcal{T}$), inertia at $\sqrt{5}$ acts through a group of order dividing 4; if $Y^4\equiv 1,6$, $V_\ell(J_{X,Y})|_{W_F}\cong V_\ell(J_0)|_{W_F}$; if $Y^4\equiv 11,21$, $V_\ell(J_{X,Y})|_{W_F}\cong V_\ell(J_0)|_{W_F}\otimes\mu$, and the representations in these two cases are not isomorphic.

(c) Suppose moreover $X,Y\in\mathbb{Q}$, $X\neq 0$. Then $\rho_{X,Y,\lambda}|_{W_F}\cong\rho_{0,c,\lambda}|_{W_F}$ for every $\lambda\nmid 5$, for the real multiplication of Proposition 2.2; so for $Y^4\not\equiv 16$ the type of $J_{X,Y}$ relative to J_0 is $(0,0)$ if $Y^4\equiv 1,6$ and $(1,1)$ if $Y^4\equiv 11,21 \pmod{25}$.

Proof. (a) Let $\lambda_E=1-\zeta_5$, u_0 a root of $U^5=-12Y$, s with $s^2=\lambda_E^5u_0$, $L=\mathbb{Q}_5(u_0,\zeta_5,s)$, $\mathcal{F}_{X,Y}(u_0+\delta)=\sum h_i\delta^i$ and $k=v(X)\geq 1$ (or $X=0$). Then $h_0=10Xu_0^3+5X^2$, $h_1=30Xu_0^2-60Y$, $h_2=30Xu_0+15u_0^4$, $h_3=20u_0^3+10X$, $h_4=15u_0^2$, $h_5=6u_0$, $h_6=1$, of valuations $\geq 1+k$, $1,1,1,1,0,0$. So $g_X(z)=\mathcal{F}_{X,Y}(u_0+\lambda_Ez)/(\lambda_E^5u_0)$ has integral coefficients, of valuations $\geq k-\frac14,0,\frac14,\frac12,\frac34,0,\frac14$, and reduces to z^5-z: the z-coefficient is $-12Y(5/\lambda_E^4)/u_0\equiv 12Y/u_0=-u_0^4\equiv -1$, as $5/\lambda_E^4\equiv -1 \pmod{\lambda_E}$, and the z^5-coefficient is 6. Hence $y^2=g_X(z)$, with $U=u_0+\lambda_Ez$, $V=sy$, is a smooth model of $C_{X,Y}$ over $\mathcal{O}_L$ with special fiber $y^2=z^5-z$, and, as U, V are defined over $\mathbb{Q}_5$, $g\in W_F$ acts on it by $\bar z\mapsto \operatorname{res}(g\lambda_E/\lambda_E)\,\bar g(\bar z)+\operatorname{res}((gu_0-u_0)/\lambda_E)$, $\bar y\mapsto\operatorname{res}(gs/s)\,\bar g(\bar y)$, independently of X. By [40, §2, Theorem 2 and its proof], $V_\ell(J_{X,Y})|_{W_F}\cong V_\ell(J_{0,Y})|_{W_F}$. Finally $c^4\equiv Y^4 \pmod{25}$ means $Y/c\in\mu_4(1+25\mathbb{Z}_5)=\mathbb{Z}_5^{\times 5}$, and $(U,V)\mapsto(\kappa U,\kappa^3V)$ with $\kappa^5=Y/c$, $\kappa\in\mathbb{Q}_5$, is an isomorphism $C_{0,c}\to C_{0,Y}$ over $\mathbb{Q}_5$.

(b) follows from (a) and Lemma 3.9, as $J_{0,27}$ is tame and $V_\ell(J_0)|_{W_F}\not\cong V_\ell(J_0)|_{W_F}\otimes\mu$ (as in the proof of Theorem 3.7(b)).

(c) Put $X=5T$. The coefficients of g_X are polynomials in T, so the model of (a) is a smooth curve over the normal ring $\mathcal{O}_L\langle T\rangle$ whose special fiber is the constant curve $y^2=z^5-z$ over $\overline{\mathbb{F}}_5[T]$, with the W_F-action of (a). The real multiplication, defined over $K(X)$ on the generic fiber (Proposition 2.2), extends to its Jacobian [14, Proposition I.2.7], and its reduction, an endomorphism of a constant abelian scheme over a connected base, is constant [31, Ch. 6, §1], as in Lemma 4.13. So the W_F-representations V_λ formed with the real multiplication ι of the family (Proposition 2.2) agree at X and at $X=0$: $\rho_{X,Y,\lambda}|_{W_F}\cong\rho_{0,Y,\lambda}|_{W_F}$. The isomorphism $C_{0,c}\to C_{0,Y}$ of (a) multiplies dU/V and $U\,dU/V$ by scalars, so it respects ι, and Lemma 3.9 gives the types. □

3.8. **The conductor exponent at $\sqrt{5}$.** The following lemma gives ε_5 for every primitive solution; it corrects part (ii) of [33, Theorem 7.8] (see the remark after Theorem 2.12).

Lemma 3.11. *Let $p\geq 7$ be prime, (X,Y,Z) a primitive solution of $X^5+Y^3=Z^p$, $t=-X^5/Y^3$, $X_0=5^{-v_5(X)}X$, λ a prime of K not above 5, and $\mathfrak{p}$ a prime of K above p. Then $\rho_{t,\lambda}$ and $\bar\rho_{t,\mathfrak{p}}$ have the same conductor exponent ε_5 at $(\sqrt{5})$. It is 2 if $5\mid YZ$; if $5\nmid YZ$, it is 2 for $t\in\mathcal{T}$ and 3 for $t\in\mathcal{A}\cup\mathcal{B}$. Equivalently, $\varepsilon_5=2$ if $5\mid YZ$, if $5\mid X$*

and $Y^3/X_0^5 \equiv 6, 8, 17, 19 \pmod{25}$*, and if* $5 \nmid XYZ$ *and* $Y^3/X^5 \equiv 6, 12, 18 \pmod{25}$*; and* $\varepsilon_5 = 3$ *otherwise.*

Proof. If $5 \mid Y$, both exponents are 2 by the proof of Lemma 2.20; if $5 \mid Z$, by Lemma 2.19(c),(d). Let $5 \nmid YZ$, that is, $5 \nmid Y(X^5 + Y^3)$; then t lies in $\mathcal{T}$, $\mathcal{A}$ or $\mathcal{B}$ (Definition 3.1). By Proposition 3.5(e), $\rho_{t,\lambda}$ has exponent 2 if $t \in \mathcal{T}$ and 3 if $t \in \mathcal{A} \cup \mathcal{B}$, and $\rho_{t,\lambda}(I_F)$ is finite, of order dividing 4, respectively equal to 20. As $p \geq 7$ does not divide this order, reduction modulo $\mathfrak{p}$ is injective on $\rho_{t,\mathfrak{p}}(I_F)$ and preserves the invariants and the Swan conductor, so $\bar{\rho}_{t,\mathfrak{p}}$ has the same exponent. Finally we write $t \in \mathcal{T}$ in residues (Definition 3.1). If $5 \nmid X$, then $t \in \mathcal{T}$ means $t \equiv 2, 4, 18 \pmod{25}$, that is, $Y^3/X^5 = -1/t \equiv 12, 6, 18 \pmod{25}$. If $5 \mid X$, it means $Y \equiv 2, 11, 14, 23 \pmod{25}$, that is, $Y^3 \equiv 8, 6, 19, 17 \pmod{25}$, cubing being a bijection of the group $(\mathbb{Z}/25\mathbb{Z})^\times$ of order 20; as $X_0^5 \equiv \pm 1, \pm 7 \pmod{25}$ and $\{6, 8, 17, 19\} = 8 \cdot \{\pm 1, \pm 7\}$, this is $Y^3/X_0^5 \equiv 6, 8, 17, 19 \pmod{25}$. □

4. The orientation at $\sqrt{5}$

A congruence of $J_t[\mathfrak{p}]$ with J_s can respect the real multiplication or conjugate it by σ. We fix the real multiplication once for the family, determine for each class of $\mathcal{A}$ which special parameter it meets at $\sqrt{5}$ and in which orientation, and exclude the conjugate orientation for $p \geq 17$ by comparing traces of Frobenius at the auxiliary prime 19 (or 11).

Theorem 4.1. *Let* $p \geq 17$ *be prime and let* (X, Y, Z) *be a primitive solution of* $X^5 + Y^3 = Z^p$*, with* $t = -X^5/Y^3$*.*

(i) If $5 \nmid XYZ$ *and* $t \equiv 9, 14, 19, 24 \pmod{25}$*, then for every prime* $\mathfrak{p}$ *of* K *above* p*,* $J_t[\mathfrak{p}]$ *is congruent to neither* $J_{-1/8}$ *nor* $J_{9/8}$*, in either orientation.*

(ii) Consequently, if $J_t[\mathfrak{p}]$ *is congruent to* J_s *for some* $s \in \{-1/8, 9/8\}$ *and some* $\mathfrak{p} \mid p$*, then* $5 \nmid XYZ$*,* $t \equiv 3, 8, 13, 23 \pmod{25}$*, the congruence is in the direct orientation, and* $s = -1/8$ *if* $t \equiv 3, 8 \pmod{25}$*,* $s = 9/8$ *if* $t \equiv 13, 23 \pmod{25}$*.*

As $t \equiv -X/Y^3 \pmod 5$, the classes of (i) are those of $\mathcal{A}$ with $X \equiv Y^3$, and those of (ii) those with $X \equiv 2Y^3 \pmod 5$. We write $\mathcal{A}^d = \{3, 8, 13, 23\}$ and $\mathcal{A}^c = \{9, 14, 19, 24\}$. The computations of this section were done with PARI/GP [44], Python and Sage [45], and are described in Appendix A.

4.1. Normalization and orientations.

Definition 4.2. By Proposition 2.2(b), du/v and $u\,du/v$ are eigenforms of $\iota(\sqrt{5})$ with eigenvalues $\pm\sqrt{5}$, in an order that is the same for the whole family. Replacing ι by $\iota \circ \sigma$ if necessary, we fix it so that $\iota(\sqrt{5})^*(du/v) = \sqrt{5}\,du/v$ and $\iota(\sqrt{5})^*(u\,du/v) = -\sqrt{5}\,u\,du/v$ for every $t \in \overline{K} \smallsetminus \{0, 1\}$. Throughout the paper, the real multiplication of J_t is this one.

Each J_t carries both ι and $\iota \circ \sigma$, so the real multiplications of two members of the family can be compared only after a choice made for all t at once, as here. The normalization extends to the members $C_{0,c}\colon V^2 = U^6 + 12cU$ ($c \in \mathbb{Q}^\times$) of the family $C_{X,Y}$ of Lemma 2.1. The Jacobians of $C_{X,Y}$ form an abelian scheme over the normal scheme $S = \operatorname{Spec} \mathcal{O}_K[1/30][X, Y, Y^{-1}, (X^5 + Y^3)^{-1}]$, to which ι extends [14, Proposition I.2.7]. Under the isomorphism of Lemma 2.1, $du/v = -(Y^2/X^3)\,U\,dU/V$ and $u\,du/v = (Y/X)\,dU/V$; so on every fiber, in particular on $J_{0,c} = \operatorname{Jac} C_{0,c}$, $\iota(\sqrt{5})$ acts by $\sqrt{5}$ on $U\,dU/V$ and by $-\sqrt{5}$ on dU/V. The isomorphism $(U, V) \mapsto (-U, V)$ from $C_{X,Y}$ to $C_{-X,-Y}$ fixes $U\,dU/V$, so it respects ι.

Lemma 4.3. *Let J be J_t, $t \in \mathbb{Q} \smallsetminus \{0,1\}$, or $J_{0,c}$, $c \in \mathbb{Q}^\times$, and let $q \nmid 30$ be a prime split in K, $q = \mathfrak{q}\mathfrak{q}'$, at which J has good reduction. The traces $a_\mathfrak{q}(J), a_{\mathfrak{q}'}(J) \in \mathcal{O}_K$ of $\mathrm{Frob}_\mathfrak{q}$, $\mathrm{Frob}_{\mathfrak{q}'}$ on $\rho_{J,\lambda}$ satisfy $a_{\mathfrak{q}'}(J) = \sigma(a_\mathfrak{q}(J))$, $|a_\mathfrak{q}(J)| \le 2\sqrt{q}$ in both real embeddings, and the reduction of J at q has Frobenius polynomial $L_q(J) = (T^2 - a_\mathfrak{q} T + q)(T^2 - \sigma(a_\mathfrak{q})T + q)$.*

Proof. The traces lie in $\mathcal{O}_K$ and do not depend on $\lambda \nmid q$ (Lemma 2.4, at the place $\mathfrak{q}$ of good reduction). $\mathrm{Frob}_{\mathfrak{q}'}$ is conjugate to $\gamma\,\mathrm{Frob}_\mathfrak{q}\,\gamma^{-1}$ with $\gamma \in G_\mathbb{Q} \smallsetminus G_K$, and γ acts σ-semilinearly for $\mathcal{O}_K$ by Proposition 2.2(c); for $J_{0,c}$ the same argument applies, as the eigenforms $U\,dU/V$ and dU/V are $\mathbb{Q}$-rational. So $a_{\mathfrak{q}'} = \sigma(a_\mathfrak{q})$. For ℓ split in K, $V_\ell(J)$ is the sum of the two λ-adic modules, which gives L_q, and the bound is Weil's. □

Definition 4.4. For J as in Lemma 4.3, $a_\mathfrak{q}(J)$ is always taken for the real multiplication of Definition 4.2. We write G_J for the system of eigenvalues $\mathfrak{q} \mapsto a_\mathfrak{q}(J)$, and G_J^σ for $\mathfrak{q} \mapsto \sigma(a_\mathfrak{q}(J))$, at the primes $\mathfrak{q} \nmid 15$ of good reduction of J, and use the same names for the Hilbert newforms over K with these eigenvalues. The λ-adic representations of G_J and G_J^σ are $\rho_{J,\lambda}$ and $\rho_{J,\lambda}^\sigma$.

Definition 4.5. Let $t, s \in \mathbb{Q} \smallsetminus \{0,1\}$, $\mathfrak{p} \mid p$ and $\mathfrak{p}' = \sigma(\mathfrak{p})$. A *congruence of $J_t[\mathfrak{p}]$ with J_s in the direct orientation* is an isomorphism of G_K-modules $\phi\colon J_t[\mathfrak{p}] \to J_s[\mathfrak{p}]$ with $\phi \circ \iota(\alpha) = \iota(\alpha) \circ \phi$ for $\alpha \in \mathcal{O}_K$; one *in the conjugate orientation* is an isomorphism of G_K-modules $\phi\colon J_t[\mathfrak{p}] \to J_s[\mathfrak{p}']$ with $\phi \circ \iota(\alpha) = \iota(\sigma(\alpha)) \circ \phi$.

For split p the condition on $\mathcal{O}_K$ is automatic ($\sigma(\alpha) \bmod \mathfrak{p}'$ and $\alpha \bmod \mathfrak{p}$ are the same element of $\mathbb{F}_p$), so the two orientations are $J_t[\mathfrak{p}] \cong J_s[\mathfrak{p}]$ and $J_t[\mathfrak{p}] \cong J_s[\mathfrak{p}']$. For inert p they are the $\mathcal{O}_K/p$-linear and the σ-semilinear G_K-isomorphisms $J_t[p] \to J_s[p]$.

4.2. **The local representations at $\sqrt{5}$.** We use F, W_F, I_F, μ, $\rho_{t,\lambda}^\sigma$ and the set $\mathcal{A}_\mathbb{Q}$ of rational t with $v_5(t) = 0$ and $t \bmod 25 \in \mathcal{A}$ as in Sections 3.1 and 3.6. Below, $t, t' \in \mathcal{A}_\mathbb{Q}$, and from Theorem 3.7(b),(d) we use:

- (O1) there is a unique $(o,e) = (o(t,t'), e(t,t')) \in \{0,1\}^2$ with $\rho_{t,\lambda}|_{W_F} \cong (\rho_{t',\lambda}^{\sigma^o} \otimes \mu^e)|_{W_F}$ for every $\lambda \nmid 5$, and then $V_\ell(J_t)|_{W_F} \cong V_\ell(J_{t'})|_{W_F} \otimes \mu^e$ for every $\ell \ne 5$;
- (O2) if $p \ge 7$, (X,Y,Z) is a primitive solution with $5 \nmid XYZ$ and $t \in \mathcal{A}$, and $s \in \{-1/8, 9/8\}$, then a congruence of $J_t[\mathfrak{p}]$ with J_s in the direct (resp. conjugate) orientation forces $(o(t,s), e(t,s)) = (0,0)$ (resp. $(1,0)$).

Definition 4.6. Let J be $J_{t'}$ or $J_{0,c}$, $\lambda \nmid 5$, and ρ a 2-dimensional representation of W_F over K_λ. If there is a unique $(o,e) \in \{0,1\}^2$ with $\rho \cong (\rho_{J,\lambda}^{\sigma^o} \otimes \mu^e)|_{W_F}$, we call (o,e) the *type of ρ at $\sqrt{5}$ relative to J*. By (O1), the type of $\rho_{t,\lambda}|_{W_F}$ relative to $J_{t'}$ is $(o(t,t'), e(t,t'))$.

For inert $p \ge 7$, $\bar\rho_{t,p}$ is absolutely irreducible on I_F (its image there has order 20, prime to p, and is the binary dihedral group of Proposition 3.5(e), acting faithfully), so by Schur's lemma every $\mathbb{F}_p[G_K]$-isomorphism $J_t[p] \cong J_s[p]$ yields one that is $\mathcal{O}_K/p$-linear or σ-semilinear: the two orientations account for every congruence.

The roots and the good model. Let $t_0 \in \mathcal{A}_\mathbb{Q}$ and v the valuation with $v(5) = 1$. By Lemma 2.18(c), f_{t_0} has one root $u_0 \in \mathbb{Q}_5$ with $v(u_0) = -1$ and five unit roots $u_1, \dots, u_5$ with $v(u_i - u_j) = 1/4$. By Proposition 3.5(b) and Section 3.1, their splitting field E_{t_0} is totally ramified of degree 20 over $\mathbb{Q}_5$, with group $\mathbb{F}_{20}$ acting faithfully on them, and contains a root ϱ of $x^4 - 5$. As $\mu_4 \subset \mathbb{Z}_5$, we may take $\varrho^2 = \sqrt{5}$. Let res be the reduction to the residue field $\mathbb{F}_5$.

Lemma 4.7. *(a) $\pi_{t_0}(u_i) = \mathrm{res}((u_i - u_1)/\varrho)$, formed with the* base root u_1*, is a bijection onto $\mathbb{F}_5$, through which $\mathrm{Gal}(E_{t_0}/\mathbb{Q}_5)$ acts by all affine maps of $\mathbb{F}_5$; the elements fixing ϱ act by translations.*

(b) If $t_1 \in \mathcal{A}_{\mathbb{Q}}$ and $t_1 \equiv t_0 \pmod{25}$, each u_i has a unique root u_i' of f_{t_1} with $v(u_i - u_i') \geq 1$; $\mathbb{Q}_5(u_i') = \mathbb{Q}_5(u_i)$, $E_{t_1} = E_{t_0}$, and $\pi_{t_1}(u_i') = \pi_{t_0}(u_i)$ with base root u_1'.

Proof. (a) The $(u_i - u_j)/\varrho$, $i \neq j$, are units, so the residues are distinct; for $\gamma \in \mathrm{Gal}(E_{t_0}/\mathbb{Q}_5)$, $\gamma(\varrho)/\varrho \in \mu_4 \subset \mathbb{Z}_5$ and $\pi_{t_0}(\gamma u_i) = \mathrm{res}(\gamma(\varrho)/\varrho)\,\pi_{t_0}(u_i) + \pi_{t_0}(\gamma u_1)$; the action is faithful, and $\mathbb{F}_{20}$ has the order of the affine group. (b) is Lemma 3.2(a), transported to f_t by $u = -1/(Yr)$ (Section 3.1); the positions do not change as $(u_i' - u_i)/\varrho$ lies in the maximal ideal. □

Let $\varpi^2 = \varrho$, $P = \mathbb{Q}_5(\varpi) \supset F$ and $E_{t_0}' = E_{t_0}(\varpi)$, totally ramified of degree 40 with residue field $\mathbb{F}_5$. As $E_{t_0} \cap P = \mathbb{Q}_5(\varrho)$, $\mathrm{Gal}(E_{t_0}'/P) = \mathrm{Gal}(E_{t_0}/\mathbb{Q}_5(\varrho))$, cyclic of order 5. The substitution $u = u_1 + \varrho z$, $v = \varpi^5 v'$ turns C_{t_0} into

$$v'^2 = d_0\Big(1 + \frac{\varrho z}{u_1 - u_0}\Big)\prod_{i=1}^{5}(z - z_i), \qquad d_0 = 5(u_1 - u_0), \quad z_i = \frac{u_i - u_1}{\varrho}.$$

Dividing $f_{t_0}(u_0) = 0$ by u_0^5 gives $5u_0 \equiv 12 \pmod{5^3}$, so $d_0 \equiv 3 \pmod 5$; $v(\varrho/(u_1 - u_0)) = 5/4$, and the z_i reduce to the elements of $\mathbb{F}_5$. So C_{t_0} has good reduction over E_{t_0}' with special fiber $\widetilde{C}\colon v'^2 = 3(z^5 - z)$, the same for every t_0. Let $g \in I_P \subset I_F$ map to a nontrivial element of $\mathrm{Gal}(E_{t_0}'/P)$. It fixes ϱ and ϖ, so it acts on $\widetilde{C}$ [40, §2] by $z \mapsto z + b_g(t_0)$ with $b_g(t_0) = \pi_{t_0}(gu_1) \in \mathbb{F}_5^{\times}$. In particular $\rho_{t_0,\lambda}(g)$ has order 5. Let $\phi_0 \in W_{E_{t_0}'}$ be a Frobenius element, so $\mu(\phi_0 g) = -1$.

Lemma 4.8. $\mathrm{tr}\,(\phi_0 g \mid V_\ell(J_{t_0})) = 5\,(b_g(t_0)/5)$ *for every prime $\ell \neq 5$.*

Proof. $\phi_0 g$ acts on $\widetilde{C}$ as $\Phi \circ T$, with Φ the Frobenius of $\widetilde{C}/\mathbb{F}_5$ and T the translation by $b = b_g(t_0)$, defined over $\mathbb{F}_5$; so $\mathrm{tr} = 6 - \#\mathrm{Fix}(\Phi \circ T)$. A fixed point is the point at infinity or has $z^5 - z = -b$ (five values of z) and $v' \in \mathbb{F}_5$ with $v'^2 = -3b$ $(1 + (-3b/5)$ values). So $\mathrm{tr} = -5(-3b/5) = 5(b/5)$, as $(-3/5) = -1$. □

4.3. **The special parameter of each class.** Let $t_0 \in \mathcal{A}_{\mathbb{Q}}$ and let $y_1, \ldots, y_5$ be the unit roots of $f_{-1/8}$.

Lemma 4.9. *(a) $E_{t_0} = E_{-1/8} =: E$.*

(b) There is a unique bijection $\nu\colon \{u_i\} \to \{y_i\}$ commuting with $\mathrm{Gal}(E/\mathbb{Q}_5)$, and $\mathbb{Q}_5(\nu(u_i)) = \mathbb{Q}_5(u_i)$.

(c) With base root $\nu(u_1)$ for $-1/8$, $\pi_{-1/8}(\nu(u_i)) = m(t_0)\,\pi_{t_0}(u_i)$ for some $m(t_0) \in \mathbb{F}_5^{\times}$, and $b_g(-1/8) = m(t_0)\,b_g(t_0)$.

(d) $m(t_0)$ depends only on $t_0 \bmod 25$, and

$t_0 \bmod 25$	3	8	9	13	14	19	23	24
$m(t_0)$	1	4	4	3	2	3	2	1
$(m(t_0)/5)$	+1	+1	+1	−1	−1	−1	−1	+1

In particular $m(-1/8) = 1$ and $m(9/8) = 2$.

Proof. (a) Via $u_i = -1/(Yr_i)$ (Section 3.1), E_{t_0} and $E_{-1/8}$ are the fields E^{gal} of Proposition 3.5(b) for t_0 and $-1/8$. Both parameters lie in $\mathcal{A}$, so the two fields are equal by Proposition 3.5(f). (b) Each subgroup of order 4 of $\mathbb{F}_{20}$ fixes exactly one root of each set. Let $\nu(u_i)$ be the root with the same stabilizer as u_i. (c) $\psi = \pi_{-1/8} \circ \nu \circ \pi_{t_0}^{-1}$ normalizes

the affine group of $\mathbb{F}_5$ in the symmetric group, which is its own normalizer, so ψ is affine with $\psi(0) = 0$: $\psi(z) = m(t_0)z$; and $b_g(-1/8) = \pi_{-1/8}(g\nu(u_1)) = \psi(b_g(t_0))$. (d) Constancy follows from Lemma 4.7(b). For the values, let $\bar{u} \in \{2, 3\}$, $\bar{u} \equiv 3t_0^2 \pmod 5$, be the common residue of the u_i. The field $L = \mathbb{Q}_5(u_1)$ is totally ramified of degree 5 with uniformizer $u_1 - \bar{u}$ (its valuation is positive, lies in $\frac{1}{5}\mathbb{Z}$ and is at most $v(u_1 - u_2) = 1/4$), and $\nu(u_1) \in L$ is a unit, so $\nu(u_1) = R(u_1)$ with $R(X) = \sum_{k=0}^{4} \beta_k (X - \bar{u})^k$, $\beta_k \in \mathbb{Z}_5$. As ν commutes with $\mathrm{Gal}(E/\mathbb{Q}_5)$, $\nu(u_i) = R(u_i)$ for every i. For $i \neq 1$, the residue of $(R(u_i) - R(u_1))/(u_i - u_1)$ is $\pi_{-1/8}(\nu(u_i))/\pi_{t_0}(u_i) = m(t_0)$, and in this quotient the terms with $k \geq 2$ have positive valuation. So $m(t_0) \equiv \beta_1 \pmod 5$. This gives the values in (d) without machine computation. Write $t_0 = 3 + 5n$ if $t_0 \equiv 3 \pmod 5$, so that $\bar{u} = 2$, and $t_0 = 4 + 5n$ if $t_0 \equiv 4 \pmod 5$, so that $\bar{u} = 3$; here $n \in \mathbb{Z}_{(5)}$. The elements $\Pi_1 = u_1 - \bar{u}$ and $\Pi_2 = \nu(u_1) - 2$ of L have norms $-f_{t_0}(\bar{u})/(5(\bar{u} - u_0))$ and $-f_{-1/8}(2)/(5(2 - y_0))$ to $\mathbb{Q}_5$, where y_0 is the root of $f_{-1/8}$ of valuation -1; here $5(\bar{u} - u_0) \equiv 5(2 - y_0) \equiv 3 \pmod 5$, as $5u_0 \equiv 5y_0 \equiv 12 \pmod{5^3}$, and $f_{t_0}(\bar{u}) \equiv 5(2 + n)$, resp. $15n \pmod{25}$, which has valuation 1 on $\mathcal{A}$, as has $f_{-1/8}(2) \equiv 10 \pmod{25}$. So Π_1 and Π_2 are uniformizers of L; as $\Pi_2 - (\beta_0 - 2) \in \Pi_1 \mathcal{O}_L$, $\beta_0 \equiv 2 \pmod 5$ and $\beta_1 \equiv \Pi_2/\Pi_1$ modulo the maximal ideal; and, as a unit of L has the residue of its norm, $m(t_0) \equiv 2/(2 + n)$, resp. $2/(3n)$, modulo 5. This is $1, 4, 3, 2$ for $t_0 \equiv 3, 8, 13, 23$ and $4, 2, 3, 1$ for $t_0 \equiv 9, 14, 19, 24 \pmod{25}$. The coefficient β_1 can also be determined modulo 5 by exact computation. Let $\tilde{u}_1$ be a root of a monic $\tilde{Q} \in \mathbb{Z}[X]$ approximating the factor of f_{t_0} with unit roots, such that $\tilde{Q}(X + \bar{u})$ is Eisenstein, and let $\tilde{y} = \sum_{k=0}^{4} \tilde{\beta}_k (\tilde{u}_1 - \bar{u})^k$, $\tilde{\beta}_k \in \mathbb{Z}_{(5)}$, be an approximate root of $f_{-1/8}$ in $\mathbb{Q}(\tilde{u}_1)$, found digit by digit and refined by Newton's method. We use Hensel's lemma in the form: if $\mathcal{K}$ is complete for a discrete valuation v, $F \in \mathcal{O}_\mathcal{K}[X]$, $a \in \mathcal{O}_\mathcal{K}$ and $v(F(a)) > 2v(F'(a))$, then F has a root $\alpha \in \mathcal{O}_\mathcal{K}$ with $v(\alpha - a) \geq v(F(a)) - 2v(F'(a))$ [27, Ch. II, §2, Prop. 2]. Exact evaluation of f_{t_0}, $f_{-1/8}$ and their derivatives at $\tilde{u}_1$ and $\tilde{y}$ shows that the field $\mathbb{Q}_5(\tilde{u}_1)$ contains a root u_1 of f_{t_0} with $v(u_1 - \tilde{u}_1) \geq 28$, so that $\mathbb{Q}_5(\tilde{u}_1) = \mathbb{Q}_5(u_1)$ (both have degree 5), and a unit root y of $f_{-1/8}$ with $v(y - \tilde{y}) \geq 91/5$. So y is fixed by the stabilizer of u_1, that is, $y = \nu(u_1)$; and as both errors exceed $1/5$, $\beta_1 \equiv \tilde{\beta}_1 \pmod 5$. By the constancy just proved, this computation at one parameter in each class confirms the values in (d). Table 3 gives the matching at these parameters and at the two special parameters. The coefficients of $\tilde{Q}$ and the $\tilde{\beta}_k$ were computed to precision 5^{30}. Item C8 describes a second computation, in Sage, with E built from Table 2. □

Lemma 4.10. *For $t, t' \in \mathcal{A}_\mathbb{Q}$, $(-1)^{e(t,t')} = \left(m(t)m(t')/5\right)$.*

Proof. Both curves have good reduction over $E' = E(\varpi)$ with special fiber $\widetilde{C}$, and Lemma 4.8 with (O1) gives $5(b_g(t)/5) = (-1)^{e(t,t')} 5(b_g(t')/5)$; and $b_g(t)b_g(t') = b_g(-1/8)^2/(m(t)m(t'))$ by Lemma 4.9(c). □

For $(t, t') = (9/8, -1/8)$ this gives $e = 1$, which is the proof of Theorem 3.7(c). The numerical root numbers of Remark 3.8(ii) give the same value, a check on the sign in Lemma 4.8.

Proposition 4.11. *Let $t \in \mathcal{A}_\mathbb{Q}$. Then $e(t, -1/8) = 0$ if $t \equiv 3, 8, 9, 24 \pmod{25}$, and $e(t, 9/8) = 0$ if $t \equiv 13, 14, 19, 23 \pmod{25}$. Write $s(t) = -1/8$ in the first case and $s(t) = 9/8$ in the second. Consequently, if $p \geq 7$ and (X, Y, Z) is a primitive solution with $5 \nmid XYZ$ and $t \in \mathcal{A}$, then $J_t[\mathfrak{p}]$ can be congruent, in either orientation, only to $J_{s(t)}$.*

k	$a_k \bmod 5^{40}$	$v_5(a_k)$
16	1429174291387070611951769205	1
12	707204409652567460511389431 5	1
8	708187024539720733484410410	1
4	316947448625574589415800 1495	1
0	444291164238501412853498 6370	1

TABLE 2. The Eisenstein polynomial $x^{20}+\sum_k a_k x^k$ defining $E = \mathbb{Q}_5(y_1, 5^{1/4})$, y_1 a unit root of $f_{-1/8}$: the characteristic polynomial of the uniformizer $5^{1/4}/(y_1 - 2)$, with coefficients reduced to integers in $[0, 5^{40})$. The other coefficients are 0 modulo 5^{40}. The Sage computation of item C8 uses them modulo 5^8 and 5^{20}. A root π of this polynomial has four conjugates π' with $v(\pi - \pi') = 1/10$ and fifteen with $v(\pi - \pi') = 1/20$; so every polynomial of degree 20 with 5-integral coefficients congruent to it modulo 5^3 has a root $\tilde{\pi}$ with $v(\pi - \tilde{\pi}) \geq 3/20$, and by Krasner's lemma it defines E.

		$\pi_{-1/8}(\nu(u_i))$								
$t_0 \bmod 25$	t_0	$\pi_{t_0}(u_i) = 0$	1	2	3	4	$b_g(t_0)$	$b_g(-1/8)$	$m(t_0)$	$(m(t_0)/5)$
3	$-1/8$	0	1	2	3	4	4	4	1	$+1$
23	9/8	0	2	4	1	3	2	4	2	-1
3	28	0	1	2	3	4	4	4	1	$+1$
8	33	0	4	3	2	1	1	4	4	$+1$
9	34	0	4	3	2	1	1	4	4	$+1$
13	38	0	3	1	4	2	3	4	3	-1
14	39	0	2	4	1	3	2	4	2	-1
19	44	0	3	1	4	2	3	4	3	-1
23	48	0	2	4	1	3	2	4	2	-1
24	49	0	1	2	3	4	4	4	1	$+1$

TABLE 3. The matching ν of the unit roots of f_{t_0} with those of $f_{-1/8}$ in E. The roots u_i are listed in the order of their positions $\pi_{t_0}(u_i) = 0, 1, 2, 3, 4$ (the base root is u_1 for t_0 and $\nu(u_1)$ for $-1/8$); ϱ is one fixed root of $x^4 - 5$ in E and g one fixed element of order 5 of $\mathrm{Gal}(E/\mathbb{Q}_5(\varrho))$, the same in every row. In every row $\pi_{-1/8}(\nu(u_i)) = m(t_0)\,\pi_{t_0}(u_i)$ and $b_g(-1/8) = m(t_0)\,b_g(t_0)$.

Proof. By Lemmas 4.10 and 4.9(d), $(-1)^{e(t,-1/8)} = (m(t)/5)$ and $(-1)^{e(t,9/8)} = (2m(t)/5) = -(m(t)/5)$. The last statement follows from (O2). □

4.4. **The orientation of each class.** Let $t_0 \in \mathcal{A}_{\mathbb{Q}}$. Put $w = 1/(u - u_0)$, $\hat{v} = vw^3$: then $\hat{v}^2 = h(w) = w^6 f_{t_0}(u_0 + 1/w)$ has degree 5, with roots $w_i = 1/(u_i - u_0)$, $v(w_i) = 1$, $v(w_i - w_j) = 9/4$. With $\Lambda = 25\varrho$, the substitution $w = w_1 + \Lambda\xi$, $\hat{v} = 5^{29/8}v''$ gives a model $v''^2 = \upsilon \prod_{i=1}^5 (\xi - \xi_i)$ over $\mathcal{O}_{E'_{t_0}}$, υ a unit. As $\xi_i = -z_i(w_i/5)(w_1/5)$ and $w_i/5 \equiv 1/d_0 \equiv 1/3$, ξ_i reduces to $-z_i/9 \equiv \pi_{t_0}(u_i)$; so the special fiber is $v''^2 = \bar{\upsilon}(\xi^5 - \xi)$, $\bar{\upsilon} \in \mathbb{F}_5^\times$, on which g acts by $\xi \mapsto \xi + b_g(t_0)$. As the model is smooth of odd degree and the residue characteristic is prime to 6, the classes $\xi^j\, d\xi/v''$ $(0 \leq j \leq 3)$ are a basis of the de Rham cohomology of the

t_0 mod 25	t_0	res($N_{02}/625$)	res($N_{13}/625$)	min v, other entries	$\eta(t_0)$
3	$-1/8$	4	2	1/4	$+1$
23	9/8	4	2	1/4	$+1$
3	28	4	2	1/4	$+1$
8	33	4	2	1/4	$+1$
9	34	1	3	1/4	-1
13	38	4	2	1/4	$+1$
14	39	1	3	1/4	-1
19	44	1	3	1/4	-1
23	48	4	2	1/4	$+1$
24	49	1	3	1/4	-1

TABLE 4. The reduction of $\iota(\sqrt{5})$ in the basis $\xi^j\, d\xi/v''$: the residues of the entries $(0,2)$ and $(1,3)$, $N_{02}/625$ and $N_{13}/625$, and the least valuation among the other fourteen entries of the matrix $(\sqrt{5}\Lambda^{j-k}N_{jk})$, four of which, $(2,0),(2,1),(3,0),(3,1)$, are 0. Then $\eta(t_0) = \mathrm{res}(N_{02}/625)/4$.

smooth proper model (they are integral, with cup-product determinant $2^8 \cdot 3^{-2}\upsilon^{-4}$, a unit). The real multiplication preserves this lattice.

Lemma 4.12. *(a)* $\operatorname{tr}\rho_{t_0,\lambda}(g) = (\theta_g(t_0)\sqrt{5} - 1)/2$ *with* $\theta_g(t_0) = \pm 1$ *independent of* $\lambda \nmid 5$.

(b) On the de Rham cohomology of the special fiber, in the basis $\xi^j\, d\xi/v''$*, the reduction of* $\iota(\sqrt{5})$ *is* $\eta(t_0)D$*, where* D *sends* $\xi^2\, d\xi/v'' \mapsto 4\, d\xi/v''$*,* $\xi^3\, d\xi/v'' \mapsto 2\xi\, d\xi/v''$ *and kills* $d\xi/v''$*,* $\xi\, d\xi/v''$*, and* $\eta(t_0) = \theta_g(t_0)\,(b_g(t_0)/5)$ *does not depend on* g*.*

(c) For $t, t' \in \mathcal{A}_{\mathbb{Q}}$*,* $(-1)^{o(t,t')} = \theta_g(t)\theta_g(t') = \eta(t)\eta(t')\,(-1)^{e(t,t')}$*.*

Proof. (a) $\rho_{t_0,\lambda}(g)$ has order 5 and determinant 1, so its trace is $\zeta + \zeta^{-1} \in \{(-1 \pm \sqrt{5})/2\}$, in K and independent of λ (Lemma 2.4). (b) Let $\tilde{\gamma}$ be the automorphism of the special fiber induced by g. As $\rho(g) + \rho(g)^{-1}$ is the scalar $\zeta + \zeta^{-1}$ on each $\rho_{t_0,\lambda}$, $1 + 2(\tilde{\gamma} + \tilde{\gamma}^{-1}) = \theta_g(t_0)\tilde{\iota}(\sqrt{5})$ on V_ℓ of the special fiber, hence in its endomorphism ring. With $\tilde{\gamma}^*\xi = \xi + b$, $(1 + 2(\tilde{\gamma}^* + \tilde{\gamma}^{*-1}))\xi^j = \xi^j + 2((\xi+b)^j + (\xi-b)^j)$ is 5, 5ξ, $5\xi^2 + 4b^2$, $5\xi^3 + 12b^2\xi$ for $j = 0, \dots, 3$, that is $b^2 D$ modulo 5, and $b^2 \equiv (b/5)$. Replacing g by g^k multiplies b by k and θ_g by $(k/5)$. (c) By (O1), $\theta_g(t) = (-1)^{o(t,t')}\theta_g(t')$, as μ is trivial on I_F; and $(b_g(t)b_g(t')/5) = (-1)^{e(t,t')}$ by the proof of Lemma 4.10. □

Lemma 4.13. $\eta(t_0)$ *depends only on* t_0 mod 25*.*

Proof. Write $t_0 = c + 25T$. Over the Tate algebra $\mathcal{O}_{E'}\langle T\rangle$, $E' = E'_c$, Hensel's lemma gives $5u_0$ (the root $\equiv 12$ of $W - 12 + 250t_0W^{-2} + 5^5 t_0^2 W^{-5}$) and the ξ_i as analytic functions with constant reductions. For the ξ_i: with w_1 kept at its value for $T = 0$, the cluster polynomial, $h(w_1 + \Lambda\xi)$ made monic, is a polynomial over $\mathcal{O}_{E'}\langle T\rangle$ whose coefficients differ from their values at $T = 0$ by elements of Gauss norm at most $5^{-3/4} < 1$, so that it reduces, as at $T = 0$, to $\xi^5 - \xi$, which has simple roots; the ξ_i are the differences of its roots with the root that vanishes at $T = 0$. So the Jacobians form an abelian scheme over the normal scheme $\operatorname{Spec}\mathcal{O}_{E'}\langle T\rangle$ with constant special fiber over $\mathbb{A}^1_{\mathbb{F}_5}$. The real multiplication extends [14, Proposition I.2.7], its reduction is constant by rigidity [31, Ch. 6, §1], and g acts by the constant translation $b_g(c)$. □

Lemma 4.14. *$\eta(-1/8)=\eta(9/8)=1$, and for $t_0\in\mathcal{A}_{\mathbb{Q}}$, $\eta(t_0)=1$ if $t_0\equiv 3 \pmod 5$ and $\eta(t_0)=-1$ if $t_0\equiv 4 \pmod 5$.*

Proof. By Lemma 4.13 one parameter per class suffices. With $\nabla=\nabla_{d/dt}$, in the de Rham cohomology of C_t minus its points at infinity (basis $u^i\,du/v$, $0\le i\le 4$),

$$15t^2(t-1)\,\nabla(du/v)=\left(5u^4-9u^3+3tu+t(9-10t)\right)du/v,$$
$$30t(t-1)\,\nabla(u\,du/v)=\left(5u^3-6u^2+2(3-5t)u+t\right)du/v.$$

The four classes $du/v,\nabla(du/v),u\,du/v,\nabla(u\,du/v)$ are independent, and ι commutes with ∇, so by Definition 4.2 the $\pm\sqrt{5}$-eigenspaces of $\iota(\sqrt{5})$ on $H^1_{\mathrm{dR}}(C_t/K(t))$ are $W_+=\langle du/v,\nabla(du/v)\rangle$ and $W_-=\langle u\,du/v,\nabla(u\,du/v)\rangle$. At t_0, we move these classes to the basis $w^j\,dw/\hat{v}$, where $u=u_0+1/w$ and $du/v=-w\,dw/\hat{v}$, removing the poles at $w=0$ with $d(w^{-k}\hat{v})$. In this basis $\iota(\sqrt{5})=\sqrt{5}M$, where $M=\pm 1$ on $W_\pm$. Expanding $w^i=(w_1+\Lambda\xi)^i$, we find that the matrix of $\iota(\sqrt{5})$ in the basis $\xi^j\,d\xi/v''$ has entries $\sqrt{5}\Lambda^{j-k}N_{jk}$, where $N=BMB^{-1}$ and $B_{ji}=\binom{i}{j}w_1^{i-j}$. As $\varrho^2=\sqrt{5}$, $\eta(t_0)$ is the residue of the $(0,2)$ entry $N_{02}/625$, divided by 4.

The entries $(2,0)$, $(2,1)$, $(3,0)$, $(3,1)$ of N vanish: $du/v=-w\,dw/\hat{v}$ and $u\,du/v=-(1+u_0w)\,dw/\hat{v}$ span $\langle dw/\hat{v},w\,dw/\hat{v}\rangle$ and are eigenvectors of M, so M preserves this span, and so do B and B^{-1}, which are upper triangular.

We computed N in PARI/GP at the two special parameters and at twelve parameters in each class; the computation at the two special parameters and at one parameter in each class, those of Table 4, proves the lemma. The roots enter only through approximations: a rational number $\tilde{u}_0$, and a root $\tilde{u}_1$ of a monic quintic $\tilde{Q}\in\mathbb{Z}[X]$, both obtained by truncating PARI/GP's 5-adic root and factorization of f_{t_0} at precision 5^{80}; all further arithmetic is exact, in $\mathbb{Q}$ and in the number field $\mathbb{Q}(\tilde{u}_1)$. With $\bar{u}$ as in the proof of Lemma 4.9, $\tilde{Q}(X+\bar{u})$ is Eisenstein, so $L=\mathbb{Q}_5(\tilde{u}_1)$ is a field, totally ramified of degree 5, on which v is computed from norms. Exact evaluation gives $v(f_{t_0}(\tilde{u}_1))\ge 80$ and $v(f'_{t_0}(\tilde{u}_1))=1$, and, for $G(U)=5^5f_{t_0}(U/5)$, which is monic in $\mathbb{Z}_{(5)}[U]$, $v(G(5\tilde{u}_0))\ge 80$ and $v(G'(5\tilde{u}_0))=0$. By Hensel's lemma, in the form recalled in the proof of Lemma 4.9, L contains a root u_1 of f_{t_0} with $v(u_1-\tilde{u}_1)\ge 78$, hence $L=\mathbb{Q}_5(u_1)$, and $v(u_0-\tilde{u}_0)\ge 79$. Besides ring operations (with the exact coefficients of the formulas above), the computation of N divides by 5 and 10 (removing the poles), by u_1-u_0 (of valuation -1) and by the determinant of the matrix of coordinates of the four classes in the basis $w^j\,dw/\hat{v}$ (of valuation -10 at every parameter). If $v(a-\tilde{a})\ge\varepsilon_a$ and $v(b-\tilde{b})\ge\varepsilon_b$, then $v(ab-\tilde{a}\tilde{b})\ge\min(v(\tilde{a})+\varepsilon_b,\,v(\tilde{b})+\varepsilon_a,\,\varepsilon_a+\varepsilon_b)$, and if moreover $\varepsilon_a>v(\tilde{a})$, then $v(a)=v(\tilde{a})$ and $v(a^{-1}-\tilde{a}^{-1})\ge\varepsilon_a-2v(\tilde{a})$. Carrying these bounds through every step shows that, at every parameter, each entry of the computed matrix $(\sqrt{5}\Lambda^{j-k}N_{jk})$ differs from the true entry by an element of valuation at least $303/4$. At every parameter the computed valuations are at most $49/20$ and the entries $(0,2)$, $(1,3)$ are units, so these valuations and residues are those of the true matrix. At $t_0=-1/8$ the valuations of the entries are

$$\begin{pmatrix} 1/2 & 1/4 & 0 & 3/4 \\ 7/4 & 1/2 & 49/20 & 0 \\ \infty & \infty & 1/2 & 1/4 \\ \infty & \infty & 7/4 & 1/2 \end{pmatrix}$$

(∞: the entry is 0), with residues 4 and 2 at $(0,2)$ and $(1,3)$, so $\eta(-1/8)=1$. At every parameter all entries are integral, valuation 0 occurs exactly at $(0,2)$ and $(1,3)$ with residues in the ratio $2:1$, and the $(0,2)$ residue is 4 for $9/8$ and $t_0\equiv 3 \pmod 5$, and 1 for $t_0\equiv 4$

(mod 5). Table 4 gives these data for the two special parameters and one parameter in each class. With the error bounds, the computation at all 98 parameters takes about 12 seconds. □

Proposition 4.15. *(a)* $o(9/8,-1/8) = e(9/8,-1/8) = 1$*:* $\rho_{9/8,\lambda}|_{W_F} \cong (\rho^{\sigma}_{-1/8,\lambda} \otimes \mu)|_{W_F}$.

(b) For $t \in \mathcal{A}_{\mathbb{Q}}$, $e(t,s(t)) = 0$, *and* $o(t,s(t)) = 0$ *if* $t \bmod 25 \in \mathcal{A}^d$ *(for* $t = -X^5/Y^3$*:* $X \equiv 2Y^3 \pmod 5$*),* $o(t,s(t)) = 1$ *if* $t \bmod 25 \in \mathcal{A}^c$ *(for* $t = -X^5/Y^3$*:* $X \equiv Y^3 \pmod 5$*).*

(c) Let $p \geq 7$ *and let* (X,Y,Z) *be a primitive solution with* $5 \nmid XYZ$ *and* $t \in \mathcal{A}$*. A congruence of* $J_t[\mathfrak{p}]$ *with some* J_s *is with* $s = s(t)$*, in the direct orientation if* $t \bmod 25 \in \mathcal{A}^d$ *and in the conjugate orientation if* $t \bmod 25 \in \mathcal{A}^c$*.*

Proof. (a) $e = 1$ by Lemmas 4.10 and 4.9(d), and then $(-1)^o = \eta(9/8)\eta(-1/8)(-1)^e = -1$ by Lemma 4.12(c), Lemma 4.14. (b) $e(t,s(t)) = 0$ by Proposition 4.11, so $(-1)^{o(t,s(t))} = \eta(t)\eta(s(t)) = \eta(t)$. (c) follows from (b), Proposition 4.11 and (O2). □

Part (c) rests on Proposition 4.11: with the other special parameter the orientation would be the other one, by (a).

4.5. **An auxiliary prime.**

Proposition 4.16. *Let* $p \geq 17$ *be prime,* (X,Y,Z) *a primitive solution of* $X^5 + Y^3 = Z^p$*,* $t = -X^5/Y^3$ *and* $s \in \{-1/8, 9/8\}$*. Then for no prime* $\mathfrak{p}$ *of* K *above* p *is* $J_t[\mathfrak{p}]$ *congruent to* J_s *in the conjugate orientation.*

No condition on XYZ modulo 2, 3 or 5 is needed.

Lemma 4.17. *Let* $q \in \{11, 19\}$*,* $q = \mathfrak{q}\mathfrak{q}'$ *in* K*, let* $p \neq q$ *be a prime with* $16q < p^2$*,* $\mathfrak{p} \mid p$*, and* $A \in \mathcal{O}_K$ *with* $|A| \leq 2\sqrt{q}$ *in both real embeddings. Let* (X,Y,Z) *be a primitive solution of* $X^5 + Y^3 = Z^p$*,* $t = -X^5/Y^3$*, and suppose that* $\bar{\rho}^{\mathrm{ss}}_{t,\mathfrak{p}}$ *is unramified at* $\mathfrak{q}$ *and* $\mathfrak{q}'$*, with traces of* $\mathrm{Frob}_{\mathfrak{q}}$ *and* $\mathrm{Frob}_{\mathfrak{q}'}$ *congruent to* A *and* $\sigma(A)$ *modulo* $\mathfrak{p}$*.*

(a) If $q \nmid Z$*, then* J_t *has good reduction at* q *and* $a_{\mathfrak{q}}(J_t) = A$*, so* $L_q(J_t) = (T^2 - AT + q)(T^2 - \sigma(A)T + q)$*. The reduction is the Jacobian of* C_τ*,* $\tau = t \bmod q \notin \{0,1\}$*, if* $q \nmid XY$*; of* $V^2 = U^6 + 12\bar{Y}U$ *if* $q \mid X$*; of* $V^2 = U^6 + 10\bar{X}U^3 + 5\bar{X}^2$ *if* $q \mid Y$*.*

(b) If $q \mid Z$*, then* p^2 *divides* $\mathrm{N}(A - \epsilon(q+1))$ *for some* $\epsilon \in \{\pm 1\}$*.*

Proof. If $b \in \mathcal{O}_K$ with $b \equiv A$ and $\sigma(b) \equiv \sigma(A) \pmod{\mathfrak{p}}$, then $b - A \in \mathfrak{p} \cap \sigma(\mathfrak{p}) = p\mathcal{O}_K$. (a) By Lemma 2.1, J_t is the Jacobian of $V^2 = U^6 + 10XU^3 + 12YU + 5X^2$, of discriminant $2^{12}3^65^5Z^{2p}$, so it has good reduction at q, with the reductions listed ($1 - t = Z^p/Y^3$). By Lemma 4.3, $b = a_{\mathfrak{q}}(J_t)$ has traces b, $\sigma(b)$ at $\mathrm{Frob}_{\mathfrak{q}}$, $\mathrm{Frob}_{\mathfrak{q}'}$, so $\delta = a_{\mathfrak{q}}(J_t) - A \in p\mathcal{O}_K$, with $|\delta| \leq 4\sqrt{q}$ in both embeddings; so $|\mathrm{N}(\delta)| \leq 16q < p^2$ and $\delta = 0$. (b) Here $n = v_q(1-t) = p\, v_q(Z)$, and $f_t = f_1 + (t-1)(10u^3 + 2) + (t-1)^2$ with $f_1 = (5u^2 - 2u + 1)(u^2 - u - 1)^2$. Modulo q the roots of $u^2 - u - 1$ are distinct and not roots of $5u^2 - 2u + 1$ (discriminants 5, -16, resultant 45), and $10u^3 + 2$ is a unit at them (norm -16); so C_t reduces to a rational curve with two nodes of thickness n, and J_t has toric reduction. By [21, Exp. IX, §§2–3], on the decomposition group at $\mathfrak{q}$, $\rho_{t,\lambda}$ is an extension of α by α times the cyclotomic character, with α unramified, given by the action of Frobenius on the character group, a rank-one $\mathcal{O}_K$-module. So $\alpha(\mathrm{Frob}) = \epsilon \in \{\pm 1\}$, the same at $\mathfrak{q}$ and $\mathfrak{q}'$, and every lift of $\mathrm{Frob}_{\mathfrak{q}}$ or $\mathrm{Frob}_{\mathfrak{q}'}$ has trace $\epsilon(q+1)$ on $J_t[\mathfrak{p}]$. So $p\mathcal{O}_K$ divides $A - \epsilon(q+1)$, which is nonzero by the bound on A, and $p^2 \mid \mathrm{N}(A - \epsilon(q+1))$. □

For a curve of genus 2 over $\mathbb{F}_q$ write its Frobenius polynomial as $T^4+c_1T^3+c_2T^2+qc_1T+q^2$. The proofs use the following pairs (c_1, c_2), computed by point counts over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ in Python (item C10).

- $C_\tau\colon v^2 = 5u^6 - 12u^5 + 10\tau u^3 + \tau^2$, $\tau \neq 0, 1$:

$\tau \in \mathbb{F}_{11}$	2	3	4	5	6
(c_1, c_2)	$(4, 21)$	$(-1, 21)$	$(0, 17)$	$(3, 23)$	$(10, 47)$
$\tau \in \mathbb{F}_{11}$	7	8	9	10	
(c_1, c_2)	$(2, 3)$	$(5, 17)$	$(-4, 26)$	$(1, 11)$	

$\tau \in \mathbb{F}_{19}$	2	3	4	5	6	7
(c_1, c_2)	$(9, 47)$	$(3, 39)$	$(2, 19)$	$(7, 39)$	$(-10, 63)$	$(-4, 37)$
$\tau \in \mathbb{F}_{19}$	8	9	10	11	12	13
(c_1, c_2)	$(4, 22)$	$(-6, 27)$	$(11, 67)$	$(9, 57)$	$(-1, 37)$	$(6, 42)$
$\tau \in \mathbb{F}_{19}$	14	15	16	17	18	
(c_1, c_2)	$(-5, 13)$	$(7, 49)$	$(2, 19)$	$(-2, 34)$	$(4, 37)$	

  Here $-1/8 \equiv 4$, $9/8 \equiv 8 \pmod{11}$ and $-1/8 \equiv 7$, $9/8 \equiv 13 \pmod{19}$.
- $V^2 = U^6 + 12\bar{Y}U$, $\bar{Y} \in \mathbb{F}_q^\times$: $(-4, 6)$, $(-9, 41)$, $(1, -9)$, $(1, 21)$ ($\bar{Y} = 2, 9$ only), $(11, 51)$ ($\bar{Y} = 3, 8$ only) for $q = 11$; $(0, 38)$ for $q = 19$.
- $V^2 = U^6 + 10\bar{X}U^3 + 5\bar{X}^2$, $\bar{X} \in \mathbb{F}_q^\times$: $(0, 22)$ for $q = 11$; $(-4, -3)$, $(8, 54)$ for $q = 19$.
- $J_{0,3}$ and $J_{0,9}$ at $q = 11$: $(11, 51)$ and $(1, 21)$.

If $L_q(J_s) = (T^2-aT+q)(T^2-\sigma(a)T+q)$, $a = a_{\mathfrak{q}}(J_s)$, then $a+\sigma(a) = -c_1$ and $a\sigma(a) = c_2-2q$, so at $q = 11$ we have $a = \pm\sqrt{5}$ for $s = -1/8$ and $a = (-5 \pm 3\sqrt{5})/2$ for $s = 9/8$, and at $q = 19$ we have $a = 2 \pm \sqrt{5}$ for $s = -1/8$ and $a = -3 \pm \sqrt{5}$ for $s = 9/8$. In these four cases $(a - \sigma(a))^2 = c_1^2 - 4(c_2 - 2q)$ is 20, 45, 20 and 20, respectively.

Proof of Proposition 4.16. Suppose there is a congruence $J_t[\mathfrak{p}] \to J_s[\mathfrak{p}']$ in the conjugate orientation. Let $q = 19$ if $p \geq 23$ and $q = 11$ if $p \in \{17, 19\}$; then $q \neq p$ and $16q < p^2$. C_s has good reduction at q (s, $1 - s$ are $\{2, 3\}$-units); put $A = \sigma(a_{\mathfrak{q}}(J_s))$. For split p, as $x \bmod \mathfrak{p}' = \sigma(x) \bmod \mathfrak{p}$ in $\mathbb{F}_p$, the traces of $\mathrm{Frob}_{\mathfrak{q}}$, $\mathrm{Frob}_{\mathfrak{q}'}$ on $J_t[\mathfrak{p}]$ are $\sigma(a_{\mathfrak{q}}(J_s)) = A$ and $\sigma(a_{\mathfrak{q}'}(J_s)) = a_{\mathfrak{q}}(J_s) = \sigma(A)$ modulo $\mathfrak{p}$ (Lemma 4.3); for inert p the isomorphism is σ-semilinear and gives the same. So Lemma 4.17 applies.

If $q \nmid Z$, the reduction of J_t has Frobenius polynomial $L_q(J_s)$. By the lists, it is not one of the curves with $q \mid XY$, and it is C_τ only for $\tau = \bar{s} = s \bmod q$. Then J_t and J_s have the same reduction at $\mathfrak{q}$ with the same $\mathcal{O}_K$-action, since ι extends to the Jacobian over the normal scheme $\mathrm{Spec}\,\mathcal{O}_K[1/30][t, 1/(t(t-1))]$ [14, Proposition I.2.7]; so $\sigma(a) = A = a_{\mathfrak{q}}(J_t) = a$ for $a = a_{\mathfrak{q}}(J_s)$, contradicting $(a - \sigma(a))^2 \neq 0$.

If $q \mid Z$, p^2 divides $\mathrm{N}(A - \epsilon(q+1)) = (q+1)^2 + \epsilon(q+1)c_1 + c_2 - 2q$. For $\epsilon = 1, -1$ these are $139, 139$ ($s = -1/8$) and $199, 79$ ($s = 9/8$) at $q = 11$, and $319 = 11 \cdot 29$, 479 and $524 = 2^2 \cdot 131$, $284 = 2^2 \cdot 71$ at $q = 19$: none is divisible by 17^2, 19^2, or the square of a prime ≥ 23. □

Remark 4.18. In the direct orientation the same steps give only $a_{\mathfrak{q}}(J_t) = a_{\mathfrak{q}}(J_s)$, which every $t \equiv s \pmod{q}$ satisfies: for $t \bmod 25 \in \mathcal{A}^d$, J_s itself passes every such test. At $q = 29$, the next split prime, both J_s have $L_{29} = (T^2 + 5T + 29)^2$, so $a_{\mathfrak{q}}(J_s) = -5$ is rational and the argument fails there.

4.6. **Proof of Theorem 4.1.** (i) Here $t \in \mathcal{A}_{\mathbb{Q}}$ with $t \bmod 25 \in \mathcal{A}^c$. By Proposition 4.11, $J_t[\mathfrak{p}]$ is congruent to no J_s with $s \neq s(t)$. By Proposition 4.15(c), a congruence with $J_{s(t)}$ would be in the conjugate orientation, which Proposition 4.16 excludes for $p \geq 17$. (ii) By Theorem 3.6, a congruence forces $5 \nmid XYZ$ and $t \in \mathcal{A}$. By (i), $t \bmod 25 \in \mathcal{A}^d$, and by Proposition 4.15(c) and Proposition 4.11 the congruence is with $J_{s(t)}$, in the direct orientation. □

4.7. **The conjugated forms of $J_{0,3}$ and $J_{0,9}$.**

Theorem 4.19. *Let $p \geq 17$ be prime, $\mathfrak{p}$ a prime of K above p, and (X, Y, Z) any primitive solution of $X^5 + Y^3 = Z^p$, $t = -X^5/Y^3$. For $c \in \{3, 9\}$ let $J_{0,c} = \mathrm{Jac}(V^2 = U^6 + 12cU)$ and $G = G^{\sigma}_{J_{0,c}}$ (Definition 4.4), whose eigenvalue at each $\mathfrak{q} \nmid 15$ is $\sigma(a_{\mathfrak{q}}(J_{0,c}))$. Then $\bar{\rho}^{\mathrm{ss}}_{t,\mathfrak{p}} \ncong \bar{\rho}^{\mathrm{ss}}_{G,\mathfrak{p}}$.*

For $q = 11 = \mathfrak{q}\mathfrak{q}'$ with $\mathfrak{q} = (11, \sqrt{5} - 4)$, the Frobenius polynomials at 11 of $J_{0,3}$ and $J_{0,9}$ are $(T^2 - aT + 11)(T^2 - \sigma(a)T + 11)$ with

$$a = a_{\mathfrak{q}}(J_{0,3}) = (-11 + \sqrt{5})/2, \qquad a = a_{\mathfrak{q}}(J_{0,9}) = (-1 + \sqrt{5})/2,$$

so $(a - \sigma(a))^2 = 5 \neq 0$. For $A = \sigma(a)$ and $\epsilon = 1, -1$, the proof also uses the norms $\mathrm{N}(A - 12\epsilon) = 305 = 5 \cdot 61$, 41 ($c = 3$) and $155 = 5 \cdot 31$, 131 ($c = 9$). Which of the two conjugates is $a_{\mathfrak{q}}(J_{0,c})$ is determined by the Cartier–Manin matrix: on the reduction, $\iota(a)$ is Frobenius plus Verschiebung, so the Cartier operator acts on $U\,dU/V$ by $a \bmod \mathfrak{q}$. Only $a \neq \sigma(a)$ is used.

Proof. Suppose $\bar{\rho}^{\mathrm{ss}}_{t,\mathfrak{p}} \cong \bar{\rho}^{\mathrm{ss}}_{G,\mathfrak{p}}$. As $J_{0,c}$ has good reduction at 11 ($\mathrm{disc}(U^6 + 12cU) = \mathrm{disc}\,\mathcal{F}_{0,c} = 2^{12}3^6 5^5 c^6$, §2.2), $\rho_{G,\mathfrak{p}} = \rho^{\sigma}_{J_{0,c},\mathfrak{p}}$ is unramified at $\mathfrak{q}, \mathfrak{q}'$, with traces $\sigma(a) = A$ at $\mathrm{Frob}_{\mathfrak{q}}$ and $\sigma(a_{\mathfrak{q}'}(J_{0,c})) = a = \sigma(A)$ at $\mathrm{Frob}_{\mathfrak{q}'}$ (Lemma 4.3). So Lemma 4.17 applies with $q = 11$, as $16 \cdot 11 < 17^2$.

If $11 \nmid Z$, the reduction of J_t at 11 has Frobenius polynomial $L_{11}(J_{0,c})$, and $a_{\mathfrak{q}}(J_t) = \sigma(a)$. By the lists, the only reductions with this polynomial are $V^2 = U^6 + 12\bar{Y}U$ with $\bar{Y} \equiv \pm c$, so $11 \mid X$ and $Y \equiv \pm c \pmod{11}$. These are fibers of the abelian scheme over S of Section 4.1 at the closed points $(X, Y) = (0, \pm c)$ above $\mathfrak{q}$; the fiber at $(0, c)$ is the reduction of $J_{0,c}$, and the one at $(0, -c)$ is isomorphic to it by $(U, V) \mapsto (-U, V)$, compatibly with ι. So $a_{\mathfrak{q}}(J_t) = a_{\mathfrak{q}}(J_{0,c}) = a \neq \sigma(a)$, a contradiction.

If $11 \mid Z$, p^2 divides one of 305, 41 ($c = 3$) or 155, 131 ($c = 9$), which are squarefree; impossible. □

Remark 4.20. For $G_{J_{0,c}}$ itself the argument fails, as it must: the fibers with $11 \mid X$, $Y \equiv \pm c \pmod{11}$ carry exactly its eigenvalue.

5. A symplectic argument at 3 and $\sqrt{5}$

A congruence with J_s multiplies the Weil pairing by a scalar. On inertia at 3 it is realized on special fibers by a Frobenius isogeny of degree 3 on each factor of a product $E \times E$ of elliptic curves, and at $\sqrt{5}$ by an isomorphism of curves. So, up to squares, the scalar is 3 at 3 and 1 at $\sqrt{5}$. Comparing the square classes of this scalar at two places is the symplectic argument of Halberstadt and Kraus for elliptic curves [22], with the local criteria of [16]. Freitas [15, §2] used it at the places 2 and 3 to remove the elliptic curve 72a1 from the equation $x^3 + y^3 = z^p$ for $p \equiv 2 \pmod 3$. Theorem 5.1 extends this argument to abelian surfaces with real multiplication. For elliptic curves the multiplier class 3 at the prime 3 appears in [17, Lemma 4.4 and its proof].

Theorem 5.1. *Let $p \equiv 19, 29, 31, 41 \pmod{60}$ be prime (that is, p splits in K and $(3/p) = -1$), $\mathfrak{p}$ a prime of K above p, (X, Y, Z) a primitive solution of $X^5 + Y^3 = Z^p$ with $3 \mid Y$, $t = -X^5/Y^3$, and $s \in \{-1/8, 9/8\}$. Then $J_t[\mathfrak{p}]$ is isomorphic as a G_K-module neither to $J_s[\mathfrak{p}]$ nor to $J_s[\mathfrak{p}']$.*

Corollary 5.2. *Let p, $\mathfrak{p}$ and s be as in Theorem 5.1. Given* (P7.4)(a) *at $\ell = 3$, which is used only when $3 \mid Z$, the conclusion of Theorem 5.1 holds for every primitive solution of $X^5 + Y^3 = Z^p$, whether or not $3 \mid Y$. Consequently, if $p \geq 139$, then given Theorem 2.13 and* (P7.4)(a) *at $\ell = 3$, every primitive solution satisfies alternative (1) or (2) of Theorem 2.13.*

Proof. If $3 \mid Y$ this is Theorem 5.1, and if $3 \nmid Y$ it is Lemma 6.18(d). Alternative (3) of Theorem 2.13 is a congruence with J_s (Definition 2.6). The primes of $\mathcal{P}$ in these classes are $19, \ldots, 101$, and the next prime in these classes is 139. □

Theorem 5.3. *Let $p \geq 7$ be a prime with $p \equiv \pm 2 \pmod 5$, (X, Y, Z) a primitive solution of $X^5 + Y^3 = Z^p$ with $3 \mid Y$, $t = -X^5/Y^3$, and $s \in \{-1/8, 9/8\}$. Suppose that $(3/p) = -1$ and $X \equiv \pm 1 \pmod 9$, or that $(3/p) = 1$ and $X \equiv \pm 2 \pmod 9$. Then there is no G_K-equivariant isomorphism $J_t[p] \to J_s[p]$ that is $\mathcal{O}_K/p$-linear, and none that is semilinear for the Frobenius of $\mathcal{O}_K/p$.*

5.1. **Weil pairings and multipliers.** A linear isomorphism η between $\mathbb{F}_p$-planes with nondegenerate alternating forms multiplies the form by a unique $c \in \mathbb{F}_p^\times$, the *multiplier* of η. Replacing η by $a\eta$ multiplies c by a^2. Weil pairings are written $e(x, y) = \zeta_p^{\langle x, y \rangle}$, with e_A for the pairing of A, and $a^\dagger$ is the Rosati adjoint. By Proposition 2.2, $\mathcal{O}_K$ acts on J_t and J_s over K by Rosati-invariant endomorphisms. The polarization and the endomorphisms extend to Néron models, so the same holds on special fibers.

Lemma 5.4. *Let p be a prime that splits in K, and A a principally polarized abelian surface over a field of characteristic $\neq p$ with an action of $\mathcal{O}_K$ by Rosati-invariant endomorphisms. Then $A[p] = A[\mathfrak{p}] \oplus A[\mathfrak{p}']$, an orthogonal sum of planes on which the Weil pairing is nondegenerate. If $\psi \colon A \to B$ is an isogeny of degree prime to p between two such surfaces with $\psi a = a\psi$ (respectively $\psi a = \sigma(a)\psi$) for $a \in \mathcal{O}_K$ and $\psi^\dagger \psi = m \in \mathbb{Z}$, then ψ restricts to an isomorphism $A[\mathfrak{p}] \to B[\mathfrak{p}]$ (respectively $B[\mathfrak{p}']$) of multiplier m mod p.*

Proof. For $a \in \mathfrak{p}' \smallsetminus \mathfrak{p}$, $x = ax' \in A[\mathfrak{p}]$ and $y \in A[\mathfrak{p}']$, $e(x, y) = e(x', ay) = 1$; so the summands are orthogonal, hence nondegenerate. The characteristic polynomial of $\sqrt{5}$ on $T_p(A)$ is rational, so the eigenvalues $\pm\sqrt{5} \in \mathbb{Z}_p$ have equal multiplicity and $\dim A[\mathfrak{p}] = 2$. Finally $e_B(\psi x, \psi y) = e_A(x, \psi^\dagger \psi y)$. □

Let $k/\mathbb{Q}_\ell$ be finite, $\ell \neq p$, and A/k a principally polarized abelian surface with an action of $\mathcal{O}_K$ by Rosati-invariant endomorphisms and with potentially good reduction. By Serre and Tate [40, §2], I_k acts on the special fiber $\tilde{A}$ through $\phi_A \colon I_k \to \Phi_A \subset \mathrm{Aut}(\tilde{A})$, preserving the polarization and $\mathcal{O}_K$, and $T_p(A) \cong T_p(\tilde{A})$ compatibly with I_k, $\mathcal{O}_K$ and Weil pairings. The group Φ_A is finite of order divisible only by primes ≤ 5: its elements have characteristic polynomials in $\mathbb{Z}[x]$ of degree 4 [40, §2, Theorem 2(ii)], so an element of prime order r has $r - 1 \leq 4$. If $A = \mathrm{Jac}(C)$ and C has potentially good reduction, Φ_A acts on the special fiber $\tilde{C}$.

Lemma 5.5. *Let A, B be as above, $p \geq 7$ (split or inert in K), $\mathfrak{q}_A, \mathfrak{q}_B$ primes of K above p, $V_\mathfrak{q} = T_p \otimes_{\mathcal{O}_K \otimes \mathbb{Z}_p} K_\mathfrak{q}$, and $\eta \colon A[\mathfrak{q}_A] \to B[\mathfrak{q}_B]$ an isomorphism commuting with I_k, either $\mathcal{O}_K$-linear or σ-semilinear. Then $\ker \phi_A = \ker \phi_B$, so $\Phi_A \cong \Phi_B$; and for $\tau \in I_k$ the traces of $\phi_A(\tau)$ on $V_{\mathfrak{q}_A}(\tilde{A})$ and of $\phi_B(\tau)$ on $V_{\mathfrak{q}_B}(\tilde{B})$ are equal, respectively σ-conjugate.*

Proof. If $n \in \Phi_A$ is trivial on $V_{\mathfrak{q}_A}(\tilde{A})$, the identity component A' of $\ker(n-1)$ is $\mathcal{O}_K$-stable with $V_p(A') \supseteq V_{\mathfrak{q}_A}(\tilde{A})$. If p is inert in K, then $\mathfrak{q}_A = p\mathcal{O}_K$ and $V_{\mathfrak{q}_A}(\tilde{A}) = V_p(\tilde{A})$. If p splits, $V_{\mathfrak{q}_A}(\tilde{A})$, of dimension 2, lies in one eigenspace of $\sqrt{5}$ on $V_p(A')$, and the other eigenspace has the same dimension, as the characteristic polynomial of $\sqrt{5}$ on $V_p(A')$ is rational. In either case $V_p(A') = V_p(\tilde{A})$, so $A' = \tilde{A}$ and $n = 1$. As $p \nmid |\Phi_A|$ and the kernel of reduction on $\mathrm{GL}(T_p)$ is pro-p, Φ_A acts faithfully on $A[\mathfrak{q}_A]$, so $\ker \phi_A$ is the kernel of I_k on $A[\mathfrak{q}_A]$; likewise for B. The eigenvalues of $\phi_A(\tau)$ on $V_{\mathfrak{q}_A}$ are roots of unity of order prime to p, determined by their reductions, which are the eigenvalues on $A[\mathfrak{q}_A]$; η matches these with those of $\phi_B(\tau)$ on $B[\mathfrak{q}_B]$, after applying σ if η is semilinear. □

Lemma 5.6. *Let E_1, E_2 be elliptic curves over an algebraically closed field, $B = E_1 \times E_2$ with the product polarization, and $T \in \mathrm{End}(B)$ with $T^\dagger = T$ and $T^2 + T - 1 = 0$. After ordering the factors and identifying E_2 with $E_1 =: E$ by an isomorphism, $T = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, and every polarized automorphism of B commuting with T is* $\mathrm{diag}(h, h)$, *$h \in \mathrm{Aut}(E)$.*

Proof. Write $T = \left(\begin{smallmatrix} a & b' \\ b & d \end{smallmatrix}\right)$; as $T^\dagger = \left(\begin{smallmatrix} \hat{a} & \hat{b} \\ \hat{b'} & \hat{d} \end{smallmatrix}\right)$, $a = \hat{a} \in \mathbb{Z}$, $d \in \mathbb{Z}$, $b' = \hat{b}$. Then $T^2 + T - 1 = 0$ gives $\deg b = 1 - a - a^2$ and $\hat{b}(a + d + 1) = 0$; $b = 0$ is impossible, so $a + d = -1$, $a \in \{0, -1\}$ and $\deg b = 1$. Exchanging the factors if needed and identifying them by b gives the matrix. A polarized automorphism g has $g^\dagger g = 1$, so $\deg g_{11} + \deg g_{21} = 1 = \deg g_{12} + \deg g_{22}$ and g is monomial. An antidiagonal g does not commute with T, and $\mathrm{diag}(h_1, h_2)$ does only if $h_1 = h_2$. □

5.2. **The prime 3.** We use the model $C_{X,Y} \colon V^2 = \mathcal{F}_{X,Y}(U) = U^6 + 10XU^3 + 12YU + 5X^2$ of Section 2.2 and Lemma 2.1. Let I_3 be the inertia group of $\mathbb{Q}_9 = K_{(3)}$, $\varpi_3 = 3^{1/4}$, $\theta_3(\tau) = \tau(\varpi_3)/\varpi_3 \bmod \mathfrak{m} \in \mu_4(\overline{\mathbb{F}}_3)$, and $\alpha_\pm \in \mathbb{F}_9$ the roots of $w^2 + w - 1$. Inertia acts on special fibers as in [13, Theorem 8.8]. We let it act on differentials by pullback (the other convention inverts every character below, for all curves at once).

Lemma 5.7. *Let $X, Y \in \mathbb{Z}$, $3 \nmid X$, $3 \mid Y$. The roots of $\mathcal{F}_{X,Y}$ are units and form two sets $\mathfrak{s}_\pm$ of three, $r \in \mathfrak{s}_\pm$ if and only if $\bar{r}^3 = \bar{X}\alpha_\pm$; $v(r - r') = 0$ for $r \in \mathfrak{s}_+$, $r' \in \mathfrak{s}_-$, and $v(r - r') = 1/2$ for distinct r, r' in one set. Frobenius exchanges $\mathfrak{s}_+$ and $\mathfrak{s}_-$, and I_3 preserves each.*

Proof. Modulo 3, $\mathcal{F}_{X,Y} \equiv X^2((U^3/X)^2 + U^3/X - 1)$. As cubing is injective on $\overline{\mathbb{F}}_3$, each root reduces to the unique cube root of $\bar{X}\alpha_+$ or to that of $\bar{X}\alpha_-$, three roots to each, and these are nonzero as $3 \nmid X$. This gives the units and the two sets. Roots in different sets have distinct reductions, so their differences are units. As α_+ and α_- are conjugate in $\mathbb{F}_9$ over $\mathbb{F}_3$, Frobenius exchanges $\bar{X}\alpha_+$ and $\bar{X}\alpha_-$, hence the two sets, and inertia, acting trivially on the residue field, preserves each. Let $R(d) = \mathrm{Res}_U(\mathcal{F}_{X,Y}(U), \mathcal{F}_{X,Y}(U+d))/d^6 = \prod_{i \neq j}(d + r_i - r_j)$, monic of degree 30 with coefficients $R_k \in \mathbb{Z}[X, Y]$, and $R_0 = \pm 2^{12}3^6 5^5 (X^5 + Y^3)^2$ of valuation 6. With $Y = 3Y_1$, PARI/GP [25, 44] gives: $R_k(X, 3Y_1) = 0$ for $k = 1, 2, 3, 5, 7, 9, 11$; the coefficients of $R_k(X, 3Y_1) \in \mathbb{Z}[X, Y_1]$ have 3-adic valuation at least $6, 5, 6, 7$ for $k = 4, 6, 8, 10$; and $R_{12}(X, 3Y_1) \equiv X^6 \pmod 3$. So the Newton polygon of R has vertices $(0, 6)$, $(12, 0)$, $(30, 0)$: twelve differences have valuation $1/2$, eighteen valuation 0, and the latter are the cross differences. □

Proposition 5.8. *In the situation of Lemma 5.7, $J = \mathrm{Jac}(C_{X,Y})$ has potentially good reduction at 3, $\tilde{J} = E_+ \times E_-$ with the product polarization, where $E_\pm$ are the stable components attached to $\mathfrak{s}_\pm$, and I_3 preserves each $E_\pm$ and acts on $H^0(E_\pm, \Omega^1)$ by θ_3.*

Proof. The clusters other than the set of roots are odd, so J has potentially good reduction [13, Theorem 1.9(6)], and the principal clusters $\mathfrak{s}_\pm$ give the two components of genus one [13, Theorems 8.6, 8.8]. For $\mathfrak{s}_+$ choose $z_1 \in \mathfrak{s}_+$, λ with $v(\lambda) = 1/2$, $c = \prod_{r\in\mathfrak{s}_-}(z_1 - r)$ (a unit) and $\kappa_0^2 = \lambda^3 c$. Then $U = z_1 + \lambda z$, $V = \kappa_0 y$ give

$$y^2 = \prod_{r\in\mathfrak{s}_+}\Big(z - \frac{r - z_1}{\lambda}\Big)\prod_{r\in\mathfrak{s}_-}\Big(1 + \frac{\lambda z}{z_1 - r}\Big),$$

whose reduction is E_+, and $dU/V = \kappa^{-1}dz/y$ with $\kappa^2 = \lambda c$. An element $\tau \in I_3$ acts on E_+ by $z \mapsto \overline{\lambda/\tau(\lambda)}\,z + \overline{(z_1 - \tau(z_1))/\tau(\lambda)}$, $y \mapsto \overline{\kappa_0/\tau(\kappa_0)}\,y$, so on dz/y by $\overline{\tau(\kappa)/\kappa}$. Units contribute 1 (inertia is trivial on the residue field), so for $v(\kappa) = m/12$ this is $\theta_3(\tau)^{-m}$, as the image of $\tau(3^{1/12})/3^{1/12}$ in μ_4 has cube $\theta_3(\tau)$; here $m = 3$; likewise for $\mathfrak{s}_-$. □

Lemma 5.9. *For $(X, Y) = (1, 2)$ and $(-3, 6)$ ($t = -1/8$, $9/8$) the roots of $\mathcal{F}_{X,Y}$ form two sets of three, exchanged by Frobenius and preserved by I_3; the differences have valuation 0 across and $5/6$ within for $(1, 2)$, and $1/3$ across and $1/2$ within for $(-3, 6)$, whose roots have valuation $1/3$. So J_s has potentially good reduction at 3, $\tilde{J}_s = E_+ \times E_-$, I_3 acts on $H^0(E_\pm, \Omega^1)$ by θ_3^3, and 12 divides $|\Phi_{J_s}|$.*

Proof. For $(1, 2)$, $\mathcal{F} \equiv U^6 + U^3 - 1 \pmod 3$; for $(-3, 6)$, $\mathcal{F} = U^6 - 30U^3 + 72U + 45$ has Newton polygon of slope $-1/3$, and $U = 3^{1/3}w$ gives $\mathcal{F}/9 \equiv (w^3)^2 - w^3 - 1 \pmod{\mathfrak{m}}$. The depths, that is, the valuations within the sets, come from the Newton polygon of the polynomial R of the proof of Lemma 5.7. Here $R_0 = \pm 2^{12}3^6 5^5(X^5 + Y^3)^2$ with $X^5 + Y^3 = 3^2$, resp. -3^3, and PARI/GP gives $R_k = 0$ for odd k and for $k = 2, 26, 28$, and the following valuations $v(R_k)$ (item C12):

k	0	4	6	8	10	12	14	16	18	20	22	24	30
$(1, 2)$	10	7	7	4	4	0	3	3	1	3	3	1	0
$(-3, 6)$	12	11	11	10	8	6	7	7	5	5	5	3	0

So the Newton polygon of R has vertices $(0, 10)$, $(12, 0)$, $(30, 0)$ for $(1, 2)$, and $(0, 12)$, $(12, 6)$, $(30, 0)$ for $(-3, 6)$: twelve differences have valuation $5/6$, resp. $1/2$, and eighteen valuation 0, resp. $1/3$. The eighteen are the differences across: for $(1, 2)$ they are units by the reduction modulo 3, and for $(-3, 6)$ they have valuation exactly $1/3$, as roots in different sets have w-coordinates with different residues. As in Proposition 5.8, $v(\kappa) = (d + 3e)/2$, where d is the depth and e the valuation across, is $5/12$, resp. $3/4$, giving $\theta_3^{-5} = \theta_3^{-9} = \theta_3^3$. Over an extension of $\mathbb{Q}_9^{\mathrm{ur}}$ of ramification index prime to 3 the semistability criterion [13, Definition 1.8, Theorem 1.9(1)] fails (depth $5/6$, respectively roots of valuation $1/3$), so $3 \mid |\Phi_{J_s}|$. □

Let $E_0 \colon y^2 = x^3 - x$ over $\overline{\mathbb{F}}_3$. Its automorphisms $[u, r] \colon (x, y) \mapsto (u^2x + r, u^3y)$, $u^4 = 1$, $r \in \mathbb{F}_3$, form the dicyclic group Dic_3 of order 12, with $[u, r]^*(dx/y) = \chi_\omega([u, r])dx/y$, $\chi_\omega([u, r]) = u^{-1}$. Elliptic curves with $j \neq 0$ have only the automorphisms ± 1. The Frobenius isogeny F_0 of E_0 has degree 3 and $F_0[u, r] = [u^3, r]F_0$. Writing $\mathrm{Dic}_3 = \langle a, b \mid a^3 = b^4 = 1,\ bab^{-1} = a^{-1}\rangle$, its automorphisms are $a \mapsto a^{\pm 1}$, $b \mapsto a^j b^{\pm 1}$. The inner ones ($b \mapsto a^j b$) preserve χ_ω and the others invert it. So $[u, r] \mapsto [u^3, r]$ is outer.

Proposition 5.10. *Let $p \geq 7$ split in K, $X, Y \in \mathbb{Z}$ with $3 \nmid X$, $3 \mid Y$, $J = \mathrm{Jac}(C_{X,Y})$, $s \in \{-1/8, 9/8\}$ and $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}'\}$. Every isomorphism of I_3-modules $J[\mathfrak{p}] \to J_s[\mathfrak{q}]$ has multiplier in $3(\mathbb{F}_p^\times)^2$.*

Proof. Suppose one exists. Apply Lemma 5.6 to $T = \varphi - 1$ on $\tilde{J}$ and $\tilde{J}_s$ (Proposition 5.8 and Lemma 5.9): $\tilde{J} = E_t^2$, $\tilde{J}_s = E_s^2$, $T = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, and inertia acts by $\mathrm{diag}(\phi_t, \phi_t)$, $\mathrm{diag}(\phi_s, \phi_s)$

with $\chi_\omega \circ \phi_t = \theta_3$ and $\chi_\omega \circ \phi_s = \theta_3^3$. As these have order 4, E_t and E_s have $j = 0$. We identify both with E_0. By Lemma 5.9 ϕ_s is onto Dic_3, and by Lemma 5.5 so is ϕ_t, with the same kernel. So $\phi_s = \beta \circ \phi_t$ with $\beta \in \mathrm{Aut}(\mathrm{Dic}_3)$ inverting χ_ω, hence outer: $\beta(g) = hg^{(3)}h^{-1}$ for some $h \in \mathrm{Aut}(E_0)$, where $F_0 g = g^{(3)} F_0$. Then $\psi_0 = hF_0$ satisfies $\psi_0 \phi_t(\tau) = \phi_s(\tau)\psi_0$.

The isogeny $\psi = \mathrm{diag}(\psi_0, \psi_0)$ intertwines inertia, commutes with $\mathcal{O}_K = \mathbb{Z}[T]$, has degree 9 and $\psi^\dagger \psi = \deg \psi_0 = 3$. By Lemma 5.4 and Serre–Tate it gives an I_3-isomorphism $J[\mathfrak{p}] \to J_s[\mathfrak{p}]$ of multiplier 3. For $\mathfrak{q} = \mathfrak{p}'$ use $M\psi$ with $M = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$: $M^\dagger M = 1$, M commutes with the diagonal inertia action, and $MTM^{-1} = -1 - T = \sigma(T)$. Finally I_3 acts on $J_s[\mathfrak{q}]$ through the reduction of the faithful irreducible 2-dimensional representation $V_p(E_0)$ of Dic_3, absolutely irreducible as $p \nmid 12$. By Schur's lemma every I_3-isomorphism is a scalar multiple of the one constructed. □

5.3. **The prime $\sqrt{5}$.** Let $F = K_{\sqrt{5}}$, I_F its inertia group, $\varpi_5^4 = \sqrt{5}$, and $\theta_5(\tau) = \tau(\varpi_5)/\varpi_5 \bmod \mathfrak{m} \in \mu_4(\overline{\mathbb{F}}_5)$, of order 4. Let $\tilde{C}_0 \colon y^2 = x^5 - x$ over $\overline{\mathbb{F}}_5$, with hyperelliptic involution ν, and $G = \mathrm{Aut}(\tilde{C}_0)$.

Lemma 5.11. *Let $X, Y \in \mathbb{Z}$ with $5 \nmid Y(X^5 + Y^3)$, for instance $(X, Y) = (1, 2)$ or $(-3, 6)$. Then Lemma 2.18(a),(b) gives a root $r_0 \in \mathbb{Z}_5$ of $\mathcal{F}_{X,Y}$ and five roots $r_1, \dots, r_5$ with $v(r_i - r_0) = 0$ (as $v(r_0) \geq 1$ and $r_1, \dots, r_5$ are units) and $v(r_i - r_j) = 1/4$ $(1 \leq i < j)$, and shows that $C_{X,Y}$ has potentially good reduction at 5.*

Proposition 5.12. *In the situation of Lemma 5.11, $C_{X,Y}$ acquires good reduction with special fiber $\tilde{C} \colon y'^2 = \prod_{i=1}^5 (z - \bar{z}_i)$. Each $\tau \in I_F$ acts on $\tilde{C}$ by $z \mapsto \alpha(\tau) z + b(\tau)$ with $\alpha(\tau) \in \mu_4$, and on dz/y' by $\theta_5(\tau)^3$. An element of order 5 of the image of I_F is a translation $z \mapsto z + b$, $b \neq 0$, and $\langle dz/y' \rangle$ is the unique line of $H^0(\tilde{C}, \Omega^1)$ it stabilizes. It acts trivially on that line.*

Proof. With $w = 1/(U - r_0)$, $y = Vw^3$: $y^2 = -D \prod_{i=1}^5 (w - e_i)$, $e_i = 1/(r_i - r_0)$, $D = -\mathcal{F}'_{X,Y}(r_0)$ a unit, $v(e_i - e_j) = 1/4$. With $\lambda = \varpi_5^2$, $w = e_1 + \lambda z$ and $y = \mu y'$, $\mu^2 = -D\lambda^5$: $y'^2 = \prod (z - z_i)$, $z_i = (e_i - e_1)/\lambda$ distinct modulo $\mathfrak{m}$, and $dw/y = \kappa^{-1} dz/y'$ with $\kappa = \sqrt{-D}\, \varpi_5^3$. As $r_0 \in \mathbb{Z}_5$, w is fixed by I_F, and as in Proposition 5.8 τ acts by $z \mapsto \overline{\lambda/\tau(\lambda)}\, z + \overline{(e_1 - \tau(e_1))/\tau(\lambda)}$, with $\lambda/\tau(\lambda) \in \mu_4$, and on dz/y' by $\overline{\tau(\kappa)/\kappa} = \theta_5(\tau)^3$. An affine map of order 5 with linear part in μ_4 is a translation. It fixes y' (odd order) and acts on the basis dz/y', $z\, dz/y'$ by a nontrivial unipotent matrix. □

Lemma 5.13.

(i) A curve $\tilde{C}$ of genus 2 over $\overline{\mathbb{F}}_5$ with an automorphism γ of order 5 is isomorphic to $\tilde{C}_0$, and $\tilde{C}/\langle \gamma \rangle$ has genus 0.

(ii) G consists of the maps $(x, y) \mapsto ((ax + b)/(cx + d), ey/(cx + d)^3)$ with $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_5)$, $e^2 = \det M$; $|G| = 240$ and $G/\langle \nu \rangle \cong \mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$.

(iii) Let $P \subset G$ have order 5, let $F_{20} \subset S_5$ be the normalizer of the image of P, and let Φ be the preimage in G of the dihedral subgroup D_5 of F_{20}. Then Φ is isomorphic to the dicyclic group $\mathrm{Dic}_5 = \langle g_1, g_2 \mid g_1^{10} = 1,\ g_2^2 = g_1^5 = \nu,\ g_2 g_1 g_2^{-1} = g_1^{-1} \rangle$, and every subgroup of G isomorphic to Dic_5 is conjugate to Φ.

Proof. (i) For the Artin–Schreier cover $\tilde{C} \to \tilde{C}/\langle \gamma \rangle$, Riemann–Hurwitz reads $2 = 5(2g' - 2) + 4 \sum (m_i + 1)$, $m_i \geq 1$; so $g' = 0$, one branch point, $m = 2$, and $\tilde{C} \colon Y^5 - Y = \alpha X^2 + \beta X + \gamma_0$, which becomes $Y^5 - Y = \alpha X'^2$. (ii) $(ax+b)^5(cx+d) - (ax+b)(cx+d)^5 = (ad-bc)(x^5 - x)$ over $\mathbb{F}_5$, and (M, e), $(\lambda M, \lambda^3 e)$ give the same map, so these are 240 automorphisms. Conversely

an automorphism induces a Möbius map preserving $\mathbb{P}^1(\mathbb{F}_5)$, hence in $\mathrm{PGL}_2(\mathbb{F}_5)$. (iii) Take $\gamma = (x+1, y)$; then $F_{20} = \{x \mapsto mx + b\}$, and D_5 is the part with $m = \pm 1$. The lifts $(\mathrm{diag}(-1,1), \pm 2)$ of $x \mapsto -x$ square to $(1,-1) = \nu$, all reflections of D_5 are conjugate, and $g_1 = \gamma\nu$ with such a lift g_2 gives the presentation. A subgroup $H \cong \mathrm{Dic}_5$ contains ν, since otherwise it maps isomorphically onto a subgroup of order 20 of S_5, a conjugate of F_{20}, which has trivial center. So H is the preimage of a subgroup of order 10, a conjugate of D_5 by Sylow. □

Proposition 5.14. *Let $p \geq 7$ split in K, $X, Y \in \mathbb{Z}$ with $5 \nmid Y(X^5 + Y^3)$, $J = \mathrm{Jac}(C_{X,Y})$, $s \in \{-1/8, 9/8\}$ and $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}'\}$. Every isomorphism of I_F-modules $J[\mathfrak{p}] \to J_s[\mathfrak{q}]$ has multiplier in $(\mathbb{F}_p^\times)^2$.*

Proof. Suppose one exists, and let $\phi_t \colon I_F \to \Phi_t \subset \mathrm{Aut}(\tilde{C}_t)$, $\phi_s \colon I_F \to \Phi_s \subset \mathrm{Aut}(\tilde{C}_s)$ be the actions on the special fibers of Proposition 5.12.

The groups. As $V_{\mathfrak{q}}(J_s)$ has conductor exponent 3 at $\sqrt{5}$ (Lemma 2.7), wild inertia acts through a nontrivial normal 5-subgroup $P = \langle\gamma\rangle$ of Φ_s, with Φ_s/P cyclic; $\tilde{C}_s \cong \tilde{C}_0$ by Lemma 5.13(i), and $|P| = 5$. By Proposition 5.12, Φ_s preserves $\langle dz/y' \rangle$; let χ_1 be its character there, so $\chi_1 \circ \phi_s = \theta_5^3$ and $\chi_1(\gamma) = 1$. As $\tilde{C}_s/P \cong \mathbb{P}^1$, $1 + \gamma + \cdots + \gamma^4 = 0$, so $\mathbb{Q}(\gamma) \cong \mathbb{Q}(\zeta_5)$ in $\mathrm{End}^0(\tilde{J}_s)$, containing $\delta = 1 + 2(\gamma + \gamma^{-1})$, $\delta^2 = 5$. The algebra generated by γ and $\sqrt{5} \in \mathcal{O}_K$ is a quotient of $\mathbb{Q}(\zeta_5)[w]/(w^2 - 5) \cong \mathbb{Q}(\zeta_5)^2$, not all of it (that would split $\tilde{J}_s$ into two factors with $\mathbb{Q}(\zeta_5)$-action). So $\sqrt{5} = \pm\delta$: $\gamma + \gamma^{-1}$ is the image of some $c \in \{(-1 \pm \sqrt{5})/2\}$, and $\gamma^2 + \gamma^{-2}$ that of $c^2 - 2 = \sigma(c) \neq c$. An element of Φ_s commutes with $\mathcal{O}_K$, so it conjugates γ to $\gamma^{\pm 1}$. Hence Φ_s lies in the preimage of D_5, of order 20, and equals it because χ_1 has order 4 and kills P. So $\Phi_s \cong \mathrm{Dic}_5$, and by Lemma 5.5 $\Phi_t \cong \Phi_s$; thus $\tilde{C}_t \cong \tilde{C}_0$, and all of the above holds for Φ_t, with $\chi_1 \circ \phi_t = \theta_5^3$.

The intertwiner. For $\ell \equiv 1 \pmod 5$, Φ_s acts on the two eigenspaces of $\mathcal{O}_K$ in $V_\ell(\tilde{J}_s)$ by nonisomorphic irreducible representations (γ has eigenvalues $\zeta_5^{\pm 1}$, respectively $\zeta_5^{\pm 2}$, and a lift of a reflection exchanges its eigenlines), so the commutant of Φ_s in $\mathrm{End}^0(\tilde{J}_s)$ is K; likewise for Φ_t. By Lemma 5.13(iii) there is an isomorphism $\alpha \colon \tilde{C}_t \to \tilde{C}_s$ with $\alpha\Phi_t\alpha^{-1} = \Phi_s$. It carries commutant to commutant, so it is $\mathcal{O}_K$-linear or σ-semilinear. A lift $h \in G$ of an element of order 4 of F_{20} normalizes Φ_s and conjugates γ to $\gamma^{\pm 2}$, hence c to $\sigma(c)$; replacing α by $h\alpha$ if needed, α is $\mathcal{O}_K$-linear if $\mathfrak{q} = \mathfrak{p}$ and σ-semilinear if $\mathfrak{q} = \mathfrak{p}'$. Write $\phi_s = \beta \circ \phi_t'$ with $\phi_t' = \alpha\phi_t\alpha^{-1}$ and $\beta \in \mathrm{Aut}(\Phi_s)$. By Lemma 5.5, applied to the given isomorphism, whose linearity is that of α, β preserves the trace of $\rho = V_{\mathfrak{q}}(\tilde{J}_s)$; as $\mathrm{tr}\,\rho(\gamma^{\pm 2}) \neq \mathrm{tr}\,\rho(\gamma)$, $\beta(\gamma) = \gamma^{\pm 1}$. Take generators g_1, g_2 of $\Phi_s \cong \mathrm{Dic}_5$ as in Lemma 5.13(iii), with $g_1 = \gamma\nu$, where γ generates the wild-inertia subgroup P and ν is the hyperelliptic involution, and g_2 any element of Φ_s over a reflection of D_5. Then $\beta(g_1) = g_1^{\pm 1}$. Also β preserves χ_1, as α carries the line fixed by $\alpha^{-1}P\alpha$ to the line fixed by P. After composing with conjugation by g_2, $\beta(g_1) = g_1$ and $\beta(g_2) = g_1^j g_2$; such a β is conjugation by $g_1^{j/2}$ if j is even; since $\chi_1(g_1) = \chi_1(\nu) = -1$, $\chi_1(g_1^j g_2) = (-1)^j \chi_1(g_2)$ forces j even, so $\beta = \mathrm{Ad}(u)$ with $u \in \Phi_s$. Then $\psi = u\alpha$ intertwines ϕ_t and ϕ_s, has the linearity of α and, as an isomorphism of curves, $\psi^\dagger\psi = 1$; it gives an I_F-isomorphism of multiplier 1 (Lemma 5.4), and Schur's lemma ($\rho \bmod \mathfrak{q}$ is absolutely irreducible, $p \nmid 20$) gives the claim. □

5.4. **Proof of Theorem 5.1.** Here $p \geq 19$ splits in K, $3 \nmid X$, and $J_t \cong \mathrm{Jac}(C_{X,Y})$ compatibly with $\mathcal{O}_K$ (Lemma 2.1 and Proposition 2.2). Let $\eta \colon J_t[\mathfrak{p}] \to J_s[\mathfrak{q}]$, $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}'\}$, be a G_K-isomorphism. Its multiplier c is also that of its restrictions to inertia groups.

If $5 \mid YZ$, there is no such η by Corollary 2.21. If $5 \nmid YZ$, that is $5 \nmid Y(X^5 + Y^3)$, then $c \in 3(\mathbb{F}_p^\times)^2$ by Proposition 5.10 and $c \in (\mathbb{F}_p^\times)^2$ by Proposition 5.14; so 3 is a square modulo p, which is false for $p \equiv \pm 5 \pmod{12}$. □

Remark 5.15. For p split with $(3/p) = 1$, the two multipliers, 3 at 3 and 1 at $\sqrt{5}$, are both squares in $\mathbb{F}_p^\times$, so the argument gives nothing. For p inert, the proof of Theorem 5.3 gives, for the multiplier of a $G_\mathbb{Q}$-equivariant isomorphism, the class $[3 \cdot 5^{e_3}]$ at 3, with $e_3 = 0$ if $X \equiv \pm 1$ and $e_3 = 1$ if $X \equiv \pm 2 \pmod 9$, and the class $[1]$ at $\sqrt{5}$; as $(5/p) = -1$, these classes agree in the remaining cases, $(3/p) = 1$ with $X \equiv \pm 1$ and $(3/p) = -1$ with $X \equiv \pm 2 \pmod 9$, where the argument gives nothing. For $X \equiv \pm 4 \pmod 9$, Lemma 5.19 does not apply; but then $\varepsilon_3 = 2$ (Lemma 6.2(e)), while $J_s[\mathfrak{p}]$ has exponent 3 at (3) (Lemma 2.7), so there is no congruence with J_s for any $p \geq 7$.

5.5. **Primes inert in K.** Let $A_t \colon y^2 + 3xy + ty = x^3$ (Theorem 2.9), with $c_4 = 81 - 72t$, $\Delta = -27t^3(t-1)$, $j = 27(8t-9)^3/(t^3(t-1))$. Over $\mathcal{U} = \mathbb{P}^1_\mathbb{Q} \smallsetminus \{0, 1, \infty\}$, C_t is smooth with Jacobian $\mathcal{J}$, A_t is an elliptic curve, and the real multiplication of Proposition 2.2 is defined over $K(t)$, satisfies ${}^\varsigma\iota(\alpha) = \iota(\sigma(\alpha))$ for $\varsigma \notin G_{K(t)}$, and specializes to each J_{t_0}. For $J = \mathcal{J}$ or $J = J_{t_0}$ let $J[\sqrt{5}] = \ker \iota(\sqrt{5})$, a $G_\mathbb{Q}$-stable $\mathbb{F}_5$-plane. With $\lambda = \sqrt{5}$ and $\mathcal{O}_\lambda = \mathbb{Z}_5[\lambda]$, $J[\sqrt{5}] = \lambda T_5/5T_5 \cong T_5/\lambda T_5$ by multiplication by λ, compatibly with $\mathcal{O}_\lambda$-linear maps (over $G_\mathbb{Q}$ the two planes differ by the quadratic character of $K/\mathbb{Q}$). Let χ_{ur} be the restriction of this character to $G_{\mathbb{Q}_3}$, the unramified quadratic character of $G_{\mathbb{Q}_3}$.

Lemma 5.16. *Let $T_0, T_1 \in \mathrm{GL}_2(\mathbb{F})$ be transvections over a field $\mathbb{F}$ with $\mathrm{tr}(T_0T_1) \neq 2$. Then the pair is determined up to simultaneous conjugation by $\mathrm{tr}(T_0T_1)$, and fixes no line over $\overline{\mathbb{F}}$.*

Proof. A common fixed line would make T_0T_1 unitriangular. In a basis of the two fixed lines, $T_0 = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$, $T_1 = \left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right)$ with $ab \neq 0$ and $\mathrm{tr}(T_0T_1) = 2 + ab$; conjugating by $\mathrm{diag}(1, a)$ gives $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ ab & 1 \end{smallmatrix}\right)$. □

Lemma 5.17. *There is a character $\chi_0 \colon G_\mathbb{Q} \to \mathbb{F}_5^\times$ such that $J_{t_0}[\sqrt{5}] \cong A_{t_0}[5] \otimes \chi_0$ as $\mathbb{F}_5[G_\mathbb{Q}]$-modules for every $t_0 \in \mathbb{Q} \smallsetminus \{0, 1\}$.*

Proof. As $\pi_1(\mathcal{U})$ conjugates $\iota(\sqrt{5})$ to $\pm\iota(\sqrt{5})$, $\mathcal{V} = \mathcal{J}[\sqrt{5}]$ and $\mathcal{W} = \mathcal{A}[5]$ are lisse sheaves of $\mathbb{F}_5$-planes on $\mathcal{U}$, with fibers $J_{t_0}[\sqrt{5}]$, $A_{t_0}[5]$ at $t_0 \in \mathcal{U}(\mathbb{Q})$, on which $G_\mathbb{Q}$ acts through a section $G_\mathbb{Q} \to \pi_1(\mathcal{U}, \bar{t}_0)$. The geometric group $\Pi = \pi_1(\mathcal{U}_{\overline{\mathbb{Q}}})$ is topologically generated by γ_0, γ_1, generators of inertia at 0 and 1, with $\gamma_\infty = (\gamma_0\gamma_1)^{-1}$ generating inertia at ∞ [20, Exp. XIII]. For $\rho = \rho_\mathcal{V}, \rho_\mathcal{W}$ we show: $\rho(\gamma_0)$, $\rho(\gamma_1)$ are transvections and $\rho(\gamma_\infty)$ has characteristic polynomial $x^2 + x + 1$ (properties independent of the choice of generators).

For $\mathcal{W}$: A has types I_3, I_1 at $t = 0, 1$, so, by Tate's uniformization, inertia acts by $\left(\begin{smallmatrix} 1 & 3 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$; at ∞, $y^2 + 3sxy + s^2y = x^3$ ($s = 1/t$) has $\Delta' = -27s^8(1-s)$, $c_4' = -9s^3(8 - 9s)$, so inertia acts through a subgroup of order 3 of $\mathrm{SL}_2(\mathbb{Z}_5)$.

For $\mathcal{V}$, write $C_t \colon y^2 = f_t(x)$. At $t = 0$: with $\tau^5 = t$, $x = \tau^2 u$, $y = \tau^5 v$, C_t becomes $v^2 = 1 - 12u^5 + 10\tau u^3 + 5\tau^2 u^6$, with good reduction $v^2 = 1 - 12u^5$, and $\mathrm{Gal}(\overline{\mathbb{Q}}((\tau))/\overline{\mathbb{Q}}((t))) = \mu_5$ acts on the special fiber by $(u, v) \mapsto (\zeta^{-2}u, v)$, of order 5 and nontrivial on H^1 by the Lefschetz fixed-point formula. So $\rho(\gamma_0) \in \mathrm{GL}_2(\mathcal{O}_\lambda)$ has order 5, and so has its reduction, since for $B \in \lambda^k M_2(\mathcal{O}_\lambda) \smallsetminus \lambda^{k+1} M_2(\mathcal{O}_\lambda)$, $k \geq 1$, $(1 + B)^5 - 1 \equiv 5B \not\equiv 0 \pmod{\lambda^{k+3}}$; as $(x-1)^5 = x^5 - 1$, $\rho_\mathcal{V}(\gamma_0)$ is a transvection. At $t = \infty$: with $\varrho^3 = 1/t$, $x = u/\varrho$, $y = tw$, C_t becomes $w^2 = 5u^6 + 10u^3 + 1 - 12\varrho u^5$, with good reduction, and μ_3 acts on the special fiber by $(u, w) \mapsto (\zeta_3 u, w)$, with eigenvalues ζ_3, ζ_3^2 on $H^0(\Omega^1)$; so the K_λ-linear $\rho(\gamma_\infty)$ has order 3, no eigenvalue 1, and distinct eigenvalues as $\zeta_3 \notin K_\lambda$: characteristic polynomial

x^2+x+1. At $t=1$: $f_1=(x^2-x-1)^2(5x^2-2x+1)$, and near $(\varphi,0)$ the model is $y^2-H^2(x-\varphi)^2=(t-1)\cdot(\text{unit})$, and conjugately near $(\sigma(\varphi),0)$. Here $H^2=f_1/(x-\varphi)^2$ is a unit, as its value at φ is $15(\varphi+2)\neq 0$, and the right side is $(t-1)$ times a unit, as $\underline{f_t}-f_1=(t-1)(10x^3+t+1)$ and $10\varphi^3+2\neq 0$. The model, a double cover of $\mathbb{P}^1$ over $\overline{\mathbb{Q}}[[t-1]]$, is projective and regular. Its special fiber is a rational curve with two nodes of thickness 1, so inertia acts by $1+N$, where $N\colon T_5/T_5^I\to T_5^I$ is the monodromy pairing, the length pairing $\pm\mathrm{diag}(1,1)$ on H_1 of the dual graph [21, Exp. IX, 9.2, 12.3–12.4 and Théorème 12.5], an isomorphism. Both sides are $\mathcal{O}_\lambda$-modules of rank 1, so $N=\left(\begin{smallmatrix}0&n\\0&0\end{smallmatrix}\right)$ with $n\in\mathcal{O}_\lambda^\times$, and $\rho_{\mathcal{V}}(\gamma_1)$ is a transvection.

Now $\operatorname{tr}\rho(\gamma_0\gamma_1)=\operatorname{tr}\rho(\gamma_\infty)^{-1}=-1\neq 2$ for both, so by Lemma 5.16 $\rho_{\mathcal{V}}\cong\rho_{\mathcal{W}}$ as representations of Π, absolutely irreducible. So $\mathrm{Hom}_\Pi(\mathcal{W},\mathcal{V})$ is a line, on which $\pi_1(\mathcal{U})$ acts through $G_{\mathbb{Q}}$ by a character χ_0. Thus $\mathcal{V}\cong\mathcal{W}\otimes\chi_0$ on $\mathcal{U}$, and we specialize. □

Lemma 5.18. *Let $t_0,t_1\in\mathbb{Q}\smallsetminus\{0,1\}$ with $v_3(j(A_{t_i}))\geq 0$, suppose $I_3=I_{\mathbb{Q}_3}$ acts on $T_5(A_{t_1})$ through* Dic_3*, and $A_{t_0}[5]\cong A_{t_1}[5]\otimes\chi_{\mathrm{ur}}^e$ over $G_{\mathbb{Q}_3}$, $e\in\{0,1\}$. Then (a) $V_5(A_{t_0})|_{I_3}\cong V_5(A_{t_1})|_{I_3}$; (b) $V_5(A_{t_0})\cong V_5(A_{t_1})\otimes\chi_{\mathrm{ur}}^\epsilon$ as $G_{\mathbb{Q}_3}$-representations for a unique $\epsilon\in\{0,1\}$, and $\epsilon=e$.*

Proof. (a) I_3 acts on $T_5(A_{t_i})$ through finite groups of order dividing 24, which inject into $\mathrm{GL}_2(\mathbb{F}_5)$, so the two kernels agree. For g in the common quotient, the eigenvalues of g on $V_5(A_{t_i})$ are roots of unity of order prime to 5, determined by their reductions, the eigenvalues on $A_{t_i}[5]$. (b) $V_5(A_{t_1})|_{I_3}$ is the faithful irreducible representation of Dic_3, so $\mathrm{Hom}_{I_3}(V_5(A_{t_1}),V_5(A_{t_0}))$ is a line on which $G_{\mathbb{Q}_3}$ acts by an unramified χ, $\chi^2=1$ by determinants: $\chi=\chi_{\mathrm{ur}}^\epsilon$. As an I_3-isomorphism $V_5(A_{t_1})\to V_5(A_{t_1})\otimes\chi_{\mathrm{ur}}$ would be a scalar anticommuting with Frobenius, ϵ is unique. The same argument modulo 5 ($5\nmid 12$) with Brauer–Nesbitt gives $A_{t_0}[5]\cong A_{t_1}[5]\otimes\chi_{\mathrm{ur}}^\epsilon$ and $\epsilon=e$. □

Lemma 5.19. *Let X,Y be coprime with $3\mid Y$, $X\not\equiv\pm4\pmod 9$, and $t=-X^5/Y^3$. Then A_t has conductor exponent 3 at 3, and its local root number is $W_3(A_t)=-1$ if $X\equiv\pm1\pmod 9$ and $+1$ if $X\equiv\pm2\pmod 9$. Both $A_{-1/8}$ and $A_{9/8}$ have conductor 27 and $W_3=-1$, and I_3 acts on $T_5(A_s)$ through* Dic_3*.*

Proof. With $Y=3^kY_0$ and $u=-X^5/Y_0^3$, $(x,y)\mapsto(3^{-2k}x,3^{-3k}y)$ turns A_t into $y^2+a_1xy+uy=x^3$, $a_1=3^{k+1}$, with $c_4=a_1(a_1^3-24u)$, $c_6=-216u^2+36a_1^3u-a_1^6$, $\Delta=u^3(a_1^3-27u)$: $v(c_4)\geq 3$, $v(c_6)=v(\Delta)=3$, the model is minimal, and $c_6'=c_6/27\equiv u^2\pmod 9$. Modulo 3 the singular point is $(-1,u)$. Moving it to the origin gives $a_6'\equiv-(2u^2+1)\pmod 9$, divisible by 9 exactly when $u\equiv\pm2\pmod 9$. As $X^6\equiv Y_0^6\equiv 1$, $u^2\equiv X^{-2}\pmod 9$, so $u\equiv\pm2$ if and only if $X\equiv\pm4$, excluded. So Tate's algorithm gives type II and Ogg's formula conductor exponent 3. In Rizzo's Table II [36] (indices $v(c_4,c_6,\Delta)$ reduced by the largest multiple of $(4,6,12)$, and $c_{4,2}=c_4/9$), the row $(\geq 2,3,3)$ applies, its condition $c_6'^2+2\not\equiv 3c_{4,2}\pmod 9$ holding as $c_6'^2\equiv 1,4$; it gives $W_3=+1$ if and only if $c_6'\equiv 4,7,8\pmod 9$. Here $c_6'\equiv u^2\equiv X^{-2}\in\{1,7\}$, and $u^2\equiv 7$ exactly when $X\equiv\pm2\pmod 9$. The curves $A_{-1/8}$, $A_{9/8}$ have minimal models $[0,0,1,-30,63]$, $[0,0,1,0,-7]$, in the isogeny class $27a$ (global root number $+1$, $W_\infty=-1$), so $W_3=-1$. Their 2-division field $\mathbb{Q}(\sqrt[3]{2},\zeta_3)$ has ramification index 6 at 3, so the inertia image, inside the automorphism group Dic_3 of the reduction, maps onto $\mathrm{Dic}_3/\{\pm1\}\cong S_3$. It is Dic_3, as the subgroup of order 6 is cyclic. □

Proof of Theorem 5.3. Let $k=\mathcal{O}_K/p=\mathbb{F}_{p^2}$ and $\psi_0\colon J_t[p]\to J_s[p]$ a G_K-isomorphism, k-linear or σ-semilinear. As in the proof of Theorem 5.1, $5\nmid YZ$ (Corollary 2.21); also $3\nmid XZ$. As the Rosati involution is trivial on $\mathcal{O}_K$, the Weil pairing on $J[p]$ is $\zeta_p^{\mathrm{Tr}_{k/\mathbb{F}_p}\mathcal{E}}$ for a unique

k-bilinear alternating $\mathcal{E}$, and $\mathcal{E}(\varsigma x, \varsigma y) = \omega(\varsigma)\sigma_\varsigma(\mathcal{E}(x,y))$ for $\varsigma \in G_{\mathbb{Q}}$, with ω cyclotomic and σ_ς the Frobenius of k if $\varsigma \notin G_K$ and the identity otherwise (Proposition 2.2(c)).

Descent. $J_s[p]$ is absolutely irreducible over G_K (inertia at 3 acts through Dic_3), so ψ_0 is unique up to $k^\times$, and $\varsigma\psi_0\varsigma^{-1} = \xi\psi_0$ for $\varsigma \notin G_K$, with $\xi^{p+1} = 1$; by Hilbert 90 $\xi = b^{1-p}$ with $b \in k^\times$, and $\psi = b\psi_0$ is $G_{\mathbb{Q}}$-equivariant, unique up to $\mathbb{F}_p^\times$. If $\mathcal{E}_s(\psi x, \psi y) = c\,\mathcal{E}_t(x,y)$ (or $c\,\sigma(\mathcal{E}_t(x,y))$), applying ς gives $c \in \mathbb{F}_p^\times$, with a well-defined class $[c]$ modulo squares.

At $\sqrt{5}$: $[c] = [1]$. The proof of Proposition 5.14 applies to ψ_0 (with Lemma 5.5 for inert p) and gives an isomorphism of curves $\psi_5 \colon \tilde{C}_t \to \tilde{C}_s$ intertwining I_F, with the same linearity as ψ_0. For $w \in I_{\mathbb{Q}_5} \smallsetminus I_F$, which acts σ-semilinearly, with actions w_t, w_s on $\tilde{C}_t$, $\tilde{C}_s$, $z = \psi_5 w_t \psi_5^{-1} w_s^{-1}$ centralizes Φ_s, whose centralizer in G is $\{1, \nu\}$ (its image in S_5 centralizes D_5). By the proof of Proposition 5.12, w acts on the line fixed by P by $\overline{w(\kappa)/\kappa}$ with $v(\kappa) = 3/8$, the same scalar for t and s, while ν acts by -1; so $z = 1$ and ψ_5 intertwines $I_{\mathbb{Q}_5}$. On $J[p]$, $\psi = a\bar{\psi}_5$ with $a \in k^\times$ (Schur over I_F), and commuting with w gives $a^p = a$; so $[c] = [a^2] = [1]$.

At 3: $[c] = [3 \cdot 5^{e_3}]$. The proof of Proposition 5.10 gives an isogeny $\psi_3 \colon \tilde{J}_t \to \tilde{J}_s$ of the special fibers at 3, namely $\psi_3 = \mathrm{diag}(hF_0, hF_0)$, with $\psi_3^\dagger \psi_3 = 3$, that commutes with T (so it is $\mathcal{O}_K$-linear) and with the actions of I_3; the σ-semilinear isogeny $M\psi_3$ has the same properties. In that proof $\phi_t(I_3) = \phi_s(I_3) = \mathrm{Dic}_3$, acting diagonally on E_0^2. Let $\mathrm{Fr} \in G_{\mathbb{Q}_3}$ be a Frobenius element. The Serre–Tate identifications are equivariant for all of $G_{\mathbb{Q}_3}$, which acts on the special fibers by semilinear automorphisms [40, §2]; write Fr_t, Fr_s for the actions of Fr on $\tilde{J}_t$, $\tilde{J}_s$. They preserve the polarizations, and as $\mathrm{Fr} \notin G_{K_3}$ (3 is inert in K) they are σ-semilinear for $\mathcal{O}_K$ (Proposition 2.2(c)). As Fr normalizes I_3, the isogeny $\psi_3' = \mathrm{Fr}_s^{-1}\psi_3\mathrm{Fr}_t$ again commutes with T and with the actions of I_3, and $\psi_3'^\dagger\psi_3' = \mathrm{Fr}_t^{-1}\psi_3^\dagger\psi_3\mathrm{Fr}_t = 3$. So $\kappa_3 = \psi_3^{-1}\psi_3' \in \mathrm{End}^0(\tilde{J}_t)$ commutes with T and with $\mathrm{diag}(\mathrm{Dic}_3)$. The elements of Dic_3 span $\mathrm{End}^0(E_0)$, a quaternion algebra with center $\mathbb{Q}$, so the commutant of $\mathrm{diag}(\mathrm{Dic}_3)$ in $\mathrm{End}^0(E_0^2) = M_2(\mathrm{End}^0(E_0))$ is $M_2(\mathbb{Q})$, and the commutant of $T = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ in $M_2(\mathbb{Q})$ is $\mathbb{Q}[T] \cong K$. Hence $\kappa_3 \in K$; as K is fixed by the Rosati involution, $3 = \psi_3'^\dagger\psi_3' = \kappa_3\,\psi_3^\dagger\psi_3\,\kappa_3 = 3\kappa_3^2$, so $\kappa_3 = \pm 1$. Put $\kappa_3 = (-1)^{e_3}$.

On $J[p]$, Schur's lemma (I_3 acts on $J_s[p]$ through Dic_3, absolutely irreducibly) gives $\psi = a\bar{\psi}_3$ with $a \in k^\times$ if ψ_0 is k-linear. As ψ is $G_{\mathbb{Q}}$-equivariant, $\mathrm{Fr}_s^{-1}\psi\mathrm{Fr}_t = \psi$; and as Fr acts σ-semilinearly, $\mathrm{Fr}_s^{-1} \circ a = a^p \circ \mathrm{Fr}_s^{-1}$ on $J_s[p]$. So $a\bar{\psi}_3 = a^p\kappa_3\bar{\psi}_3$, that is $a^{p-1} = \kappa_3$: $a \in \mathbb{F}_p^\times$ if $e_3 = 0$, and $a \in \sqrt{5}\,\mathbb{F}_p^\times$ if $e_3 = 1$. As ψ_3 is $\mathcal{O}_K$-linear with $\psi_3^\dagger\psi_3 = 3$, the identity $e(\psi_3 x, \psi_3 y) = e(x, \psi_3^\dagger\psi_3 y)$ of Weil pairings gives $\mathcal{E}_s(\bar{\psi}_3 x, \bar{\psi}_3 y) = 3\mathcal{E}_t(x,y)$, so $[c] = [3a^2] = [3 \cdot 5^{e_3}]$. If ψ_0 is σ-semilinear, then $\psi = aM\bar{\psi}_3$, and the same argument with $M\psi_3$ in place of ψ_3 gives $\mathrm{Fr}_s^{-1}M\psi_3\mathrm{Fr}_t = \kappa_M M\psi_3$ with $\kappa_M = \pm 1$, $a^{p-1} = \kappa_M$ and $[c] = [3a^2]$. Here $\kappa_M = \kappa_3$: as $M\sqrt{5} = -\sqrt{5}M$, M preserves $\tilde{J}_s[\sqrt{5}]$, on which I_3 acts absolutely irreducibly ($5 \nmid 12$) and commutes with M, so M acts there by a scalar $m \in \mathbb{F}_5^\times$; on $\tilde{J}_t[\sqrt{5}]$ this gives $\kappa_M m\psi_3 = \mathrm{Fr}_s^{-1}m\psi_3\mathrm{Fr}_t = m\kappa_3\psi_3$, so $\kappa_M \equiv \kappa_3 \pmod{\sqrt{5}}$, and $\kappa_M = \kappa_3$.

The sign e_3. As $\deg\psi_3 = 9$ and $\psi_3 w_t = \chi_{\mathrm{ur}}(w)^{e_3} w_s \psi_3$ for $w \in G_{\mathbb{Q}_3}$, $J_t[\sqrt{5}] \cong J_s[\sqrt{5}] \otimes \chi_{\mathrm{ur}}^{e_3}$ over $G_{\mathbb{Q}_3}$, so $A_t[5] \cong A_s[5] \otimes \chi_{\mathrm{ur}}^{e_3}$ by Lemma 5.17, and $V_5(A_t) \cong V_5(A_s) \otimes \chi_{\mathrm{ur}}^{e_3}$ by Lemmas 5.19 and 5.18 ($v_3(j(A_t)) = 3 - v_3(t) > 0$). Tate's formula for the twist by an unramified quadratic character χ, $\varepsilon(V \otimes \chi) = \chi(\pi)^{a(V)}\varepsilon(V)$ [42, §3.4], with $a(V) = 3$ and root numbers computed from V_5, gives $W_3(A_t) = (-1)^{e_3} W_3(A_s) = (-1)^{e_3+1}$. By Lemma 5.19, $e_3 = 0$ if $X \equiv \pm 1$ and $e_3 = 1$ if $X \equiv \pm 2 \pmod 9$. Finally $[1] = [3 \cdot 5^{e_3}]$ means $(3/p)(5/p)^{e_3} = 1$, with $(5/p) = -1$, contradicting both hypotheses. □

6. Consequences of the results of Pacetti and Villagra Torcomian

Each result below that assumes statements of [33] names the labels of Section 2.5 that it uses. The results of §§6.1–6.3 hold for every $p \geq 7$: they say when $\bar{\rho}_{t,\mathfrak{p}}$ can be reducible, and which forms with complex multiplication it can be congruent to.

6.1. **Notation and local lemmas.** Throughout, (X, Y, Z) is a primitive solution, $p \geq 7$, $\mathfrak{p} \mid p$ with residue field $k_{\mathfrak{p}}$, $\rho = \rho_{t,\mathfrak{p}}$, $\bar{\rho} = \bar{\rho}_{t,\mathfrak{p}}$, $C_{X,Y}\colon V^2 = \mathcal{F}_{X,Y}(U)$ is the model of Lemma 2.1, and $\chi_p = \det \rho$ is the p-adic cyclotomic character, with reduction $\bar{\chi}_p$. $G_v \supset I_v$ are decomposition and inertia groups at $v = (2), (3)$ (completions $\mathbb{Q}_4, \mathbb{Q}_9$), and $G_F \supset I_F$ at $(\sqrt{5})$. For $w \in \{3, F\}$, μ_w is the unramified quadratic character of G_w and η_w the quadratic character of I_w. Artin maps send uniformizers to arithmetic Frobenius elements. Where J_t has potentially good reduction at (3) or $(\sqrt{5})$, the image of inertia is finite with prime divisors at most 5 (its elements have characteristic polynomials in $\mathbb{Z}[x]$ of degree 4 [40, §2, Theorem 2(ii)], so an element of prime order r has $r - 1 \leq 4$), so $\bar{\rho}$ has the same conductor exponent ε_3, resp. ε_5, as ρ.

Inputs from [33]. When $3 \mid X$, $\varepsilon_3 = 2$ is part of Lemma 6.2(a), which needs no input from [33]; when $3 \mid Z$, Lemma 6.2(b) uses (P7.4)(a) at $\ell = 3$ and (Ex_0); when $3 \nmid XZ$, $\varepsilon_3 \in \{2, 3\}$ is part of (Ex_0), and is proved in Lemma 6.2(e) without input from [33]. At $\sqrt{5}$ we use no input from [33]: $\varepsilon_5 = 2$ if $5 \mid YZ$ (Lemmas 2.20 and 2.19), and $\varepsilon_5 \in \{2, 3\}$ if $5 \nmid YZ$ (Proposition 3.5(e)).

Odd representations. Complex conjugation has eigenvalues $1, -1$, and a non-split Cartan element with an eigenvalue in $k_{\mathfrak{p}}$ is scalar. So $\bar{\rho}$, like any odd two-dimensional representation over a finite field, is irreducible if and only if it is absolutely irreducible.

Newforms. For a Hilbert newform g over K and $\mathfrak{P} \mid p$ we write $\rho_{g,\mathfrak{P}}$ for its $\mathfrak{P}$-adic representation and $a_{\mathfrak{l}}(g)$ for its eigenvalue at $\mathfrak{l}$, and $\bar{\rho} \cong \bar{\rho}_{g,\mathfrak{P}}$ for an isomorphism over $\overline{\mathbb{F}}_p$; θ_M is the character of a quadratic M/K, and g has complex multiplication by a totally imaginary M if $\rho_{g,\mathfrak{P}} \cong \rho_{g,\mathfrak{P}} \otimes \theta_M$ (then $a_{\mathfrak{l}}(g) = 0$ for $\mathfrak{l}$ inert in M). The characters θ_{-3}, θ_ζ and θ_{15} are those of §2.7.

Lemma 6.1. *Let $v \in \{(3), (\sqrt{5})\}$. If J_t has potentially good reduction at v and ε_v is odd, then $\bar{\rho}|_{I_v}$ is absolutely irreducible.*

Proof. $\bar{\rho}|_{I_v}$ is semisimple with exponent ε_v. If it were $\chi \oplus \chi'$ over $\overline{\mathbb{F}}_p$, then $\chi\chi' = \bar{\chi}_p|_{I_v} = 1$ and the exponent would be $2a(\chi)$, which is even. □

Lemma 6.2 (the prime 3)**.** *(a) If $3 \mid X$, then J_t has potentially good reduction at 3, $\rho(I_3)$ is cyclic of order 5, $\varepsilon_3 = 2$, $\bar{\rho}|_{G_3}$ is absolutely irreducible, $\bar{\rho}|_{G_3} \cong \bar{\rho}|_{G_3} \otimes \mu_3$, and $\bar{\rho}|_{I_3} \ncong \bar{\rho}|_{I_3} \otimes \eta_3$.*

(b) Assume (P7.4)(a) *at $\ell = 3$ and* (Ex_0)*. If $3 \mid Z$, then $\rho|_{G_3} \cong \psi_3 \otimes \left(\begin{smallmatrix} \chi_p & * \\ 0 & 1 \end{smallmatrix}\right)$ with ψ_3 a ramified quadratic character, and $\bar{\rho}|_{I_3}^{\mathrm{ss}} = \eta_3 \oplus \eta_3$.*

(c) If $3 \nmid XZ$, then J_t has potentially good reduction at 3, and if moreover $\varepsilon_3 = 3$, then $\bar{\rho}|_{I_3}$ is absolutely irreducible.

(d) Let $3 \nmid XZ$. The roots of $\mathcal{F}_{X,Y}$ form two sets s_1, s_2 of three; roots in different sets differ by a unit, roots in the same set by an element of valuation exactly $1/2$. Inertia acts on the invariant differential of each component of the stable reduction by a character of order 4. If moreover $\varepsilon_3 = 2$, then $\rho|_{G_3} \otimes \overline{K}_{\mathfrak{p}} \cong \chi_1 \oplus \chi_2$ with $\chi_1|_{I_3}$ of order 4, $\chi_2|_{I_3} = \chi_1^{-1}|_{I_3}$, and $\chi_i(\mathrm{Art}(-3)) \in 3\mu_{12}$.

(e) Let $3 \nmid XZ$. If $3 \mid Y$ and $X \equiv \pm 4 \pmod 9$, or if $3 \nmid Y$ and $X^5 \equiv 4Y^3 \pmod 9$, then $\rho(I_3)$ is cyclic of order 4 and $\varepsilon_3 = 2$; otherwise $\rho(I_3)$ is the dicyclic group of order 12

and $\varepsilon_3 = 3$. In particular (Ex$_9$) *holds, and, with (a),* (Ex$_0$) *holds for every primitive solution with $3 \nmid Z$.*

Proof. (a) Let $\pi^5 = 3$ and $X = 3X_1$. With $U = \pi W$ and $V = \pi^3 V'$, the curve $C_{X,Y}$ becomes

$$V'^2 = G(W) \coloneqq W^6 + 10X_1\pi^2 W^3 + 4YW + 5X_1^2\pi^4,$$

where $G \in \mathbb{Z}_3[\pi][W]$ is monic and $\operatorname{disc} G = 3^{-6} \operatorname{disc} \mathcal{F}_{X,Y} = 2^{12}5^5(X^5 + Y^3)^2$ is a unit, as $3 \nmid Y$. So $C_{X,Y}$ has good reduction over $\mathbb{Q}_3(\pi)$, with special fiber $V'^2 = W^6 + \bar{Y}W$, and I_3 acts on $V_\lambda(J_t)$, $\lambda \nmid 3$, through $\mathrm{Gal}(\mathbb{Q}_3^{\mathrm{ur}}(\pi)/\mathbb{Q}_3^{\mathrm{ur}})$, cyclic of order 5, by automorphisms of the special fiber [40, §2]. A generator, $\pi \mapsto \zeta_5\pi$, acts by $(W, V') \mapsto (\bar{\zeta}_5^{-1}W, \bar{\zeta}_5^{-3}V')$, with quotient $T^2 = s(s + \bar{Y})$, where $s = W^5$ and $T = V'W^2$, of genus 0. So I_3 acts tamely, through a cyclic group $\langle\tau\rangle$ of order 5, without nonzero invariants: $\rho(\tau)$ has eigenvalues $\zeta^{\pm 1}$ with ζ a primitive fifth root of unity, and $\varepsilon_3 = 2$; as $p \neq 5$, the same holds for $\bar{\rho}$. Frobenius conjugates τ to $\tau^9 = \tau^{-1}$, so it swaps the eigenlines of τ (distinct modulo $\mathfrak{p}$ as $p \neq 5$): $\bar{\rho}|_{G_3}$ is absolutely irreducible and induced from $G_{\mathbb{Q}_{81}} = \ker \mu_3$, which fixes them. Finally $\{\chi\eta_3, \chi^{-1}\eta_3\} = \{\chi, \chi^{-1}\}$ for the eigencharacter χ of order 5 would force $\chi^2 = \eta_3$.

(b) $v_3(t - 1) = p\, v_3(Z) > 3$, so by (P7.4)(a) the reduction is potentially multiplicative, of toric rank 2 ($\mathcal{O}_K$ acts on the character group); this gives the shape, $\psi_3^2 = 1$ by the determinant, and ψ_3 is ramified as $\varepsilon_3 = 2$ by (Ex$_0$).

(d) Modulo 3, $\mathcal{F}_{X,Y} \equiv U^6 + XU^3 - X^2 = (U - X\alpha_2)^3(U - X\alpha_1)^3$ over $\mathbb{F}_9$, where $\alpha_1, \alpha_2 = \alpha_1^3 \in \mathbb{F}_9 \smallsetminus \mathbb{F}_3$ are the roots of $x^2 + x - 1$; this gives s_1, s_2 and the unit differences between them. Let $D(z) = \mathrm{Res}_U(\mathcal{F}_{X,Y}(U), \mathcal{F}_{X,Y}(U + z))/z^6$, monic of degree 30 with the differences $r_i - r_j$ ($i \neq j$) as roots. The computation of item C12 gives its coefficients D_k for $k \leq 12$: $D_k = 0$ for odd k and $k = 2$, and

$$\begin{aligned} D_0 &= -2^{12}3^6 5^5(X^5 + Y^3)^2, & D_4 &= -2^4 3^5 5^7 X^2 Y(71X^5 - 64Y^3), \\ D_6 &= 3^5 5^6 X^3(163X^5 - 512Y^3), & D_8 &= -2^8 3^4 5^6 \cdot 19\, X^4 Y^2, \\ D_{10} &= 2^4 3^4 5^4 Y(639X^5 + 64Y^3), & D_{12} &= 2^2 5^3 X(496883X^5 - 266112Y^3). \end{aligned}$$

As $v_3(D_0) = 6$, $D_{12} \equiv X^6 \equiv 1 \pmod 3$ and D_4, D_6, D_8, D_{10} have contents of valuation $5, 5, 4, 4$, the Newton polygon of D is the segment $(0, 6)$–$(12, 0)$ followed by a horizontal one: twelve differences have valuation $1/2$ and eighteen are units, and the units are the eighteen ordered pairs from different sets (agreeing with Lemma 5.7 when $3 \mid Y$).

So s_1, s_2 are odd clusters of depth $1/2$, J_t has potentially good reduction, and the stable reduction has a genus-1 component E_i for each s_i ($\mathcal{R} = s_1 \cup s_2$, the cluster of all six roots, even with two children, is not principal), with J_t reducing to $E_1 \times E_2$ [13, Theorems 1.9(6), 1.11]. For $z_1 \in s_1$, $U = z_1 + \sqrt{3}\, w$ and the unit $C_2 = \prod_{r \in s_2}(z_1 - r)$, $V^2 = (\sqrt{3})^3 C_2 \prod_{r \in s_1}(w - (r - z_1)/\sqrt{3})(1 + O(\mathfrak{m}))$ with distinct rescaled roots, and, for $y_1 = V/(\sqrt{3}\,\kappa)$ with $\kappa^2 = \sqrt{3}\, C_2$, $dw/y_1 = \kappa\, dU/V$. As dU/V is defined over $\mathbb{Q}_9$, $\gamma \in I_3$ acts on dw/y_1 by $\chi_\omega(\gamma) = \gamma(\kappa)/\kappa \bmod \mathfrak{m}$, and $\chi_\omega^2 \equiv \gamma(\sqrt{3})/\sqrt{3} = \eta_3$; so χ_ω has order 4.

Let $\varepsilon_3 = 2$. Then I_3 acts tamely through a cyclic group $\langle\tau\rangle$, embedded in $\mathrm{Aut}(E_1) \times \mathrm{Aut}(E_2)$ (as G_3 fixes each cluster, whose residue is in $\mathbb{F}_9$), a group in which elements of order prime to 3 have order dividing 4; so $|\langle\tau\rangle| = 4$, and each E_i, defined over $\mathbb{F}_9$, has an automorphism of order 4, so $j(E_i) = 0$ and E_i is supersingular. As $4 \mid 9 - 1$, Frobenius commutes with τ and fixes its eigenlines (eigenvalues $\pm i$): this gives $\chi_1 \oplus \chi_2$. Over $L = \mathbb{Q}_9(3^{1/4})$, totally ramified with residue field $\mathbb{F}_9$, J_t has good reduction, and $\mathrm{Art}(N_{L/\mathbb{Q}_9} 3^{1/4}) = \mathrm{Art}(-3)$ acts as the Frobenius of $E_1 \times E_2$ over $\mathbb{F}_9$, whose eigenvalues lie in $\{\pm 3, \pm 3i, 3\zeta_6^{\pm 1}, 3\zeta_3^{\pm 1}\} \subset 3\mu_{12}$.

(c) The first assertion is in (d), the second is Lemma 6.1.

(e) Let $\Phi = \rho(I_3)$, finite as J_t has potentially good reduction at 3, and L_t the fixed field of $\ker \rho|_{I_3}$, so that $\mathrm{Gal}(L_t/\mathbb{Q}_3^{\mathrm{ur}}) \cong \Phi$. By (d) and its proof, the reduction over L_t is $E_1 \times E_2$ with the product polarization, and I_3 acts on the invariant differential of E_1 by a character of order 4. As in the proof of Proposition 5.10, Lemma 5.6 identifies E_2 with $E_1 =: E$ so that I_3 acts through polarized automorphisms $\mathrm{diag}(h,h)$, $h \in \mathrm{Aut}(E)$ [40, §2]; as some h acts on $H^0(E,\Omega^1)$ by an element of order 4, $j(E) = 0$, so $E \cong E_0$ and $\mathrm{Aut}(E) = \mathrm{Dic}_3$ (§5.2). So Φ embeds in Dic_3 and maps onto μ_4 under χ_ω, whose kernel is the subgroup of order 3: Φ is cyclic of order 4, or $\Phi \cong \mathrm{Dic}_3$. In the first case I_3 acts tamely and a generator of Φ has eigenvalues $\pm i$, so $\varepsilon_3 = 2$.

By the proof of Lemma 3.4(a), which applies at 3, L_t contains the roots of $\mathcal{F}_{X,Y}$ and has degree at most 2 over the field they generate over $\mathbb{Q}_3^{\mathrm{ur}}$. Let $c \in \mathbb{Z}_9$ reduce to the common residue of the roots in s_1, and $\mathcal{F}_{X,Y}(c+z) = \sum_k a_k z^k$. Then $a_6 = 1$; $a_3 = 10(2c^3 + X)$ is a unit, as $\bar{c}^3/\bar{X}$ is a root of w^2+w-1, so not in $\mathbb{F}_3$; $3 \mid a_k$ for $k = 1,2,4,5$; and $3 \mid a_0 = \mathcal{F}_{X,Y}(c)$, whose class modulo 9 does not depend on the choice of c, as $3 \mid a_1 = \mathcal{F}'_{X,Y}(c)$. If $v(a_0) = 1$, the Newton polygon gives $v(r-c) = 1/3$ for $r \in s_1$, so 3 divides the ramification index of $\mathbb{Q}_3^{\mathrm{ur}}(s_1)$, hence $|\Phi|$, and $\Phi \cong \mathrm{Dic}_3$. If $v(a_0) \geq 2$, the valuations $v(r-c)$, $r \in s_1$, add up to $v(a_0) \geq 2$ (the roots in s_2 contribute 0), and at most one of them exceeds $1/2$, the roots of s_1 being pairwise at distance $3^{-1/2}$; so one root $r_* \in s_1$ has $v(r_* - c) \geq 1$, lies in $\mathbb{Q}_9$ as the only root in that disc, and the other two roots of s_1, a $G_{\mathbb{Q}_9}$-stable pair, generate an extension of $\mathbb{Q}_9$ of degree at most 2. Then $\mathbb{Q}_3^{\mathrm{ur}}(s_1)$, and its Frobenius conjugate $\mathbb{Q}_3^{\mathrm{ur}}(s_2)$, are tamely ramified, so $3 \nmid [L_t : \mathbb{Q}_3^{\mathrm{ur}}]$ and Φ is cyclic of order 4.

Let $\Phi \cong \mathrm{Dic}_3$, so that $v(a_0) = 1$, $e(L_t/\mathbb{Q}_3^{\mathrm{ur}}) = 12$, and the wild inertia group is the subgroup $\langle h \rangle$ of order 3. As h does not act by ± 1, it moves some root (proof of Lemma 3.4(a)); replacing s_1 and c by their Frobenius conjugates if necessary, h permutes s_1 cyclically. For $r \in s_1$, $v_{L_t}(r-c) = 12 \cdot \frac{1}{3} = 4$ is prime to 3 and $v_{L_t}(hr - r) = 12 \cdot \frac{1}{2} = 6$, so (3.1), whose proof applies at 3, gives $i(h) = 3$: $G_0 = \Phi$, $G_1 = G_2 = \langle h \rangle$ and $G_3 = 1$. As h fixes no nonzero vector, $\varepsilon_3 = 2 + \frac{3}{12} \cdot 2 + \frac{3}{12} \cdot 2 = 3$ [38, Ch. VI, §2].

It remains to compute $v(a_0)$. Let $w \in \mathbb{Z}_9$ be a root of $w^2 + w - 1$, and $\epsilon = \pm 1$ and $k \in \mathbb{Z}$ with $X \equiv \epsilon(1 + 3k) \pmod 9$. Then $c = -\epsilon(1+w)$ has $c^3 = -\epsilon(3 + 2w)$, as $w^2 = 1 - w$, so $\bar{c}^6 + \bar{X}\bar{c}^3 - \bar{X}^2 = \bar{w}^2 + \bar{w} - 1 = 0$, and we may take for s_1 the set of roots congruent to c. Again from $w^2 = 1 - w$, and from $\epsilon X \equiv 1 + 3k$, $X^2 \equiv 1 + 6k \pmod 9$,

$$\mathcal{F}_{X,Y}(c) = (3+2w)^2 - 10\epsilon X(3+2w) - 12\epsilon Y(1+w) + 5X^2 \equiv 3(1+w)(2+k-\epsilon Y) \pmod 9,$$

and $1 + w$ is a unit. So $v(a_0) \geq 2$ if and only if $k \equiv 1 + \epsilon Y \pmod 3$. If $3 \mid Y$, this means $X \equiv \pm 4 \pmod 9$. If $3 \nmid Y$, then $Y \equiv \epsilon \pmod 3$, as $3 \nmid X^5 + Y^3$, and it means $k \equiv 2$, that is, $X \equiv 7\epsilon \pmod 9$, that is, $X^5 \equiv X^{-1} \equiv 4\epsilon \equiv 4Y^3 \pmod 9$. □

Lemma 6.3 (the prime $\sqrt{5}$)**.** *(a) If $5 \mid Y$, then J_t has potentially good reduction at $\sqrt{5}$, $\rho(I_F)$ is cyclic of order 3, $\bar{\rho}|_{G_F}$ is absolutely irreducible, $\bar{\rho}|_{G_F} \cong \bar{\rho}|_{G_F} \otimes \mu_F$, and $\bar{\rho}|_{I_F} \ncong \bar{\rho}|_{I_F} \otimes \eta_F$.*

(b) If $5 \mid Z$, then $\rho|_{G_F} \cong \psi_F \otimes \left(\begin{smallmatrix} \chi_p & * \\ 0 & 1 \end{smallmatrix}\right)$ with ψ_F a ramified quadratic character, and $\bar{\rho}|_{I_F}^{\mathrm{ss}} = \eta_F \oplus \eta_F$.

(c) If $5 \nmid YZ$, then J_t has potentially good reduction at $\sqrt{5}$, and if moreover $\varepsilon_5 = 3$, then $\bar{\rho}|_{I_F}$ is absolutely irreducible.

(d) If $5 \nmid YZ$ and $\varepsilon_5 = 2$, then $\rho|_{G_F} \otimes \overline{K}_{\mathfrak{p}} \cong \chi_1 \oplus \chi_2$ with $\chi_1|_{I_F}$ of order 4 and $\chi_2|_{I_F} = \chi_1^{-1}|_{I_F}$.

Proof. (a) By the proof of Lemma 2.20, $C_{X,Y}$ has good reduction over $\mathbb{Q}_5(5^{1/6})$, and I_F acts on $V_\lambda(J_t)$, $\lambda \nmid 5$, through $\mathrm{Gal}(F^{\mathrm{ur}}(5^{1/6})/F^{\mathrm{ur}})$, cyclic of order 3, without nonzero invariants. So $\rho(I_F)$ is cyclic of order 3, generated by τ with eigenvalues $\zeta^{\pm 1}$, ζ a primitive cube root of unity, and Frobenius acts by $\tau \mapsto \tau^5 = \tau^{-1}$; the rest is as in Lemma 6.2(a).

(b) As in the proof of Lemma 6.2(b), with Lemma 2.19(b),(c): the reduction is potentially totally toric, and ψ_F is ramified.

(c) Lemma 2.18(b) and Lemma 6.1.

(d) I_F acts tamely ($\varepsilon_5 = 2$) through a cyclic group of order n, with $4 \mid n$ by Proposition 5.12; the eigenvalues $\zeta^{\pm 1}$ of a generator have degree at most 4, so $n \in \{4, 8, 12\}$, and $\{\zeta^5, \zeta^{-5}\} = \{\zeta, \zeta^{-1}\}$ (Frobenius) gives $n = 4$. As $4 \mid 5 - 1$, Frobenius fixes the two eigenlines. □

6.2. **Irreducibility.**

Proposition 6.4. *Let $p \geq 7$ be prime, split or inert in K, and $\mathfrak{p} \mid p$. Assume* (T2.1), (P7.4)(a) *at $\ell = 3$ and* (Ex_0). *If $\bar\rho$ is reducible, then $30 \mid Z$ and $\bar\rho^{\mathrm{ss}} \cong \theta_{15} \oplus \theta_{15}\bar\chi_p$. In particular $\bar\rho$ is absolutely irreducible whenever $30 \nmid Z$.*

Proof. Step 1. Let $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$. As $\bar\rho$ is odd, it is reducible already over $k_\mathfrak{p}$: write $\bar\rho^{\mathrm{ss}} = \psi_1 \oplus \psi_2$, $\psi_1\psi_2 = \bar\chi_p$, with $k_\mathfrak{p}^\times$-valued characters unramified at the finite places not dividing $15p$ (Theorem 2.8). They are tame at 3: on I_3 we have $\psi_2 = \psi_1^{-1}$, so the conductor exponent of $\bar\rho^{\mathrm{ss}}$ at 3, which is at most $\varepsilon_3 \leq 3$, equals $2a(\psi_1)$, and $a(\psi_1) \leq 1$; likewise at $\sqrt{5}$, as $\varepsilon_5 \leq 3$. Let $f \in \{1, 2\}$ be the degree of the primes above p, so that $k_\mathfrak{p} = \mathbb{F}_{p^f}$. The restriction of ψ_1 to an inertia group $I_\mathfrak{l}$ at a prime $\mathfrak{l} \mid p$ is a power ω_f^a of the fundamental character of level f, as ψ_1 is a character of $G_{K_\mathfrak{l}}$; as $J_t[p]$ is finite flat at the primes above p (Theorem 2.8), which are unramified over p, and $e = 1 < p - 1$, Raynaud's theorem [35, Théorème 3.4.3 and Corollaire 3.4.4] (see [39, §2.8]) shows that the base-p digits of a are 0 or 1. So $\psi_1|_{I_\mathfrak{l}}$ is 1 or $\bar\chi_p$ if p splits, and 1, ω_2, ω_2^p or $\omega_2^{p+1} = \bar\chi_p$ if p is inert. Let $u = \varphi^8$, a totally positive unit with $u \equiv 1 \pmod{3\sqrt{5}}$ and $N(u - 1) = -45$ (Lemma 2.23(b)). The idele class character of ψ_1 is trivial on u at the real places, at 3 and $\sqrt{5}$ (where it is tame) and at the finite places not dividing $15p$ (where it is unramified), so the product of its components at the primes above p is trivial on u. If p splits and ψ_1 is $\bar\chi_p$ on inertia at one prime above p and trivial at the other, this gives $u \equiv 1$ modulo a prime above p, so $p \mid N(u - 1)$. If p is inert and $\psi_1|_{I_\mathfrak{p}}$ is ω_2 or ω_2^p, it gives $\bar u = 1$ in $k_\mathfrak{p} = \mathbb{F}_{p^2}$, as $x \mapsto x^p$ is bijective on $k_\mathfrak{p}$, so $p^2 \mid N(u - 1)$. Both are impossible. After renumbering, $\bar\rho^{\mathrm{ss}} = \psi \oplus \psi^{-1}\bar\chi_p$ with ψ unramified above p and tame at 3, $\sqrt{5}$: a character of $\mathrm{Cl}_K(3\sqrt{5}\,\infty_1\infty_2)$, of order dividing 4.

Step 2. As $\bar\rho$ is reducible, Lemmas 6.2 and 6.3 give $3 \nmid X$, $5 \nmid Y$, and: $\psi|_{I_3}$ has order 2 if $3 \mid Z$, and order 4 if $3 \nmid XZ$ (then $\varepsilon_3 = 2$); likewise at $\sqrt{5}$.

Step 3. The idele class character of ψ is trivial on φ, its components away from 3, $\sqrt{5}$, ∞_2 are trivial on φ, and the one at ∞_2 is ± 1; as φ generates both $(\mathcal{O}_K/3)^\times$ and $(\mathcal{O}_K/\sqrt{5})^\times$, the orders of $\psi|_{I_3}$ and $\psi|_{I_F}$ are both 4 or both at most 2: either $15 \mid Z$, or $3 \nmid XZ$, $5 \nmid YZ$ and $\varepsilon_3 = \varepsilon_5 = 2$.

Step 4. If Z is odd, Lemma 2.22(a) gives $a_2 \in \{0, -1\}$ and $a_2 \equiv \psi(\mathrm{Frob}_{(2)}) + 4\psi(\mathrm{Frob}_{(2)})^{-1} \in \{\pm 5, \pm 3i\}$ modulo $\mathfrak{p}$, forcing $p \in \{2, 3, 5\}$. So Z is even.

Step 5. Suppose we are in the second case of Step 3. Then $\psi|_{I_3}$ and $\psi|_{I_F}$ have order 4, so $\psi^2|_{I_3} = \eta_3$ and $\psi^2|_{I_F} = \eta_F$, and $\psi^2 = \theta_{15}$ (Lemma 2.23(c)). As (2) is inert in $\mathbb{Q}(\zeta_5)/K$ and splits in $K(\sqrt{-3})/K$ (Lemma 2.23(d)), $\theta_{15}((2)) = -1$, so $x = \psi(\mathrm{Frob}_{(2)})$ satisfies $x^2 = -1$. As Z is even, Lemma 2.22(b) gives $\pm 5 = x + 4x^{-1} = -3x$ in $k_\mathfrak{p}$; squaring, $p \mid 25 + 9 = 34$, so $p = 17$. But Lemma 6.2(d) gives $\psi(\mathrm{Art}(-3)) \equiv 3\zeta$ for a fourth root of unity $\psi(\mathrm{Art}(-3))$

and some $\zeta \in \mu_{12}$, so $p \mid 3^{12}-1 = 2^4 \cdot 5 \cdot 7 \cdot 13 \cdot 73$, which 17 does not divide. So $15 \mid Z$, and by Step 4, $30 \mid Z$.

Step 6. Now $\psi|_{I_3} = \eta_3$ and $\psi|_{I_F} = \eta_F$, so ψ^2 is unramified, hence trivial, and ψ is the quadratic character ramified exactly at 3 and $\sqrt{5}$: $\psi = \theta_{15}$ (Lemma 2.23(c)). □

Remark 6.5. Lemmas 6.1–6.3, 2.22 and 2.23 hold, under their stated assumptions, for every $p \geq 7$ and every $\mathfrak{p} \mid p$. For each $\ell \in \{2,3,5\}$ in [33, Corollary 7.7], the last sentence of Proposition 6.4 gives its conclusion (Theorem 2.11) for every $p \geq 7$, given (T2.1), (P7.4)(a) at $\ell = 3$ and (Ex_0).

6.3. **Congruences with forms with complex multiplication.**

Proposition 6.6. *Let $p \geq 7$ and $\mathfrak{p} \mid p$. Assume* (T2.1), (P7.4)(a) *at $\ell = 3$ and* (Ex_0). *Suppose $\bar{\rho}$ is irreducible and $\bar{\rho} \cong \bar{\rho}_{g,\mathfrak{P}}$ for a Hilbert newform g over K of parallel weight 2, trivial character and level divisible only by* (3) *and* $(\sqrt{5})$, *with complex multiplication by a totally imaginary quadratic extension M/K. Then M is $\mathbb{Q}(\zeta_5)$ or $K(\sqrt{-3})$, and:*

(a) if $M = \mathbb{Q}(\zeta_5)$, then $2 \mid X$, $3 \mid X$ and $5 \nmid YZ$;

(b) if $M = K(\sqrt{-3})$, then $5 \mid Y$ and $3 \nmid XZ$; if moreover the level of g is $3^i(\sqrt{5})^j$ with $i,j \in \{2,3\}$ and $p \notin \{7,19\}$, then $2 \nmid Z$.

Proof. $\bar{\rho} \cong \bar{\rho} \otimes \theta_M$, and θ_M has conductor dividing $3\sqrt{5}\infty_1\infty_2$ and is nontrivial at both real places, so $\theta_M \in \{\theta_{-3}, \theta_\zeta\}$ (Lemma 2.23(c)).

(a) $\theta_\zeta|_{G_3} = \mu_3$. If $3 \mid Z$, comparing semisimplifications (Lemma 6.2(b)) forces $\bar{\chi}_p|_{G_3} = \mu_3$, i.e. $9 \equiv -1 \pmod{p}$, so $p \mid 10$, which is impossible. If $3 \nmid XZ$ and $\varepsilon_3 = 3$, an irreducible μ_3-invariant $\bar{\rho}|_{G_3}$ is induced from $G_{\mathbb{Q}_{81}} \supset I_3$, so reducible on I_3, against Lemma 6.2(c). If $\varepsilon_3 = 2$, then $\bar{\chi}_2 = \bar{\chi}_1\mu_3$ would give $\bar{\chi}_1^2 = 1$ on I_3, against Lemma 6.2(d). So $3 \mid X$. At $\sqrt{5}$, $\theta_\zeta|_{I_F} = \eta_F$: $\eta_F \oplus \eta_F \not\cong 1 \oplus 1$ excludes $5 \mid Z$, and Lemma 6.3(a) excludes $5 \mid Y$. At 2, $a_{(2)}(g) = 0$ ((2) is inert in M), while Lemma 2.22 gives -1 if $2 \mid Y$ and ± 5 if $2 \mid Z$; so $2 \mid X$.

(b) $\theta_{-3}|_{G_F} = \mu_F$. If $5 \mid Z$, this forces $5 \equiv -1 \pmod{p}$, so $p \mid 6$, which is impossible; and $5 \nmid YZ$ is excluded as at 3 in (a) by Lemma 6.3(c),(d); so $5 \mid Y$. As $\theta_{-3}|_{I_3} = \eta_3$, Lemma 6.2(a) excludes $3 \mid X$ and $\eta_3 \oplus \eta_3 \not\cong 1 \oplus 1$ excludes $3 \mid Z$. If $2 \mid Z$, then $a_{(2)}(g) \equiv \pm 5$ modulo a prime above $\mathfrak{p}$ (Lemma 2.22(b)). By the computation below, whose output (item C14) includes the list of values of $a_{(2)}$ that occur, every newform as in (b) at level $3^i(\sqrt{5})^j$, $i,j \in \{2,3\}$, has $a_{(2)} \in \{\pm 1, \pm 2, \pm 4, (\pm 1 \pm 3\sqrt{5})/2\}$ and $N_{K/\mathbb{Q}}(a_{(2)} \mp 5) \in \{1,9,16,19,36,49,81\}$, so p would divide a nonzero integer with prime factors in $\{2,3,7,19\}$.

The computation. $M = K(\sqrt{-3})$ has class number 1. Such a g is the theta series of an algebraic Hecke character ψ of M with infinity type a CM type Φ and level $3^{1+a_3}(\sqrt{5})^{2a_5}$, where $\mathfrak{Q}_3^{a_3}\mathfrak{Q}_5^{a_5}$ is its conductor ($\mathfrak{Q}_3, \mathfrak{Q}_5$ above 3, $\sqrt{5}$); so $j = 2$ and $\psi((\alpha)) = \Phi(\alpha)/\chi(\alpha)$ for a character χ of $(\mathcal{O}_M/\mathfrak{Q}_3^2\mathfrak{Q}_5)^\times$ with $\chi = \Phi$ on units. Running through all such χ and keeping those with $\psi(\mathfrak{l}\mathcal{O}_M) = \theta_{-3}(\mathfrak{l})N\mathfrak{l}$ for $\mathfrak{l}$ above $7 \leq \ell \leq 300$ (a conclusive test of trivial character, as these primes generate $\mathrm{Cl}_K(3\sqrt{5}\infty_1\infty_2)$) gives 18 characters per CM type, 15 of them at the levels with $j = 2$, which give 3 newforms at level $3^2(\sqrt{5})^2$ and 27 at $3^3(\sqrt{5})^2$, with the stated $a_{(2)}$ (item C14). □

6.4. **Setting and inputs.** Throughout, p is prime, split or inert in K, $\mathfrak{p} \mid p$ is any prime of K, (X,Y,Z) is a primitive solution, $t = -X^5/Y^3$ and $\bar{\rho} = \bar{\rho}_{t,\mathfrak{p}}$. As $\mathcal{P}$ contains every prime below 17, $p \notin \mathcal{P}$ implies $p \geq 17$. We write $3^{\varepsilon_3}(\sqrt{5})^{\varepsilon_5}$ for the conductor of $\bar{\rho}$ away from p; where J_t has potentially good reduction it is also that of $\rho_{t,\lambda}$ (§6.1). For $5 \nmid XYZ$, t lies in $\mathcal{A}$, $\mathcal{B}$ or $\mathcal{T}$ (Definition 3.1). At $\sqrt{5}$, $\varepsilon_5 \in \{2,3\}$ (§6.1). Propositions 6.4 and 6.6

are proved under (T2.1), (P7.4)(a) at $\ell = 3$ and (Ex_0); both hold for every $p \geq 7$, split or inert. Their proofs use (P7.4)(a) at $\ell = 3$ and (Ex_0) only when $3 \mid Z$, and otherwise only $\varepsilon_3 \in \{2, 3\}$; so for solutions with $3 \nmid XZ$, where $\varepsilon_3 \in \{2, 3\}$ is Lemma 6.2(e), they use no statement of [33] other than (T2.1). In Lemma 6.7, (Ex) is used only for $\varepsilon_3 \in \{2, 3\}$, which also follows, when $3 \nmid XZ$, from Lemma 6.2(e), and in general from (Ex_0) with (P7.4)(a) at $\ell = 3$ (Lemma 6.2(b) when $3 \mid Z$; potentially good reduction and §6.1 otherwise). In Lemma 6.8, where $\varepsilon_3 = 3$, (Ex) is used only for the value of ε_3: (P7.4)(a) at $\ell = 3$ and (Ex_0) give $3 \nmid XZ$ (Lemma 6.2(a),(b)), and when $3 \nmid XZ$ the two conditions modulo 9 follow from Lemma 6.2(e). So below, Lemmas 6.7 and 6.8 are applied either with (Ex) or with these inputs in its place.

Lemma 6.7. *Assume* (LL), (Ex) *and* (EL). *Let $p \notin \mathcal{P}$ and suppose that $\bar{\rho}$ is irreducible. Then $\varepsilon_3, \varepsilon_5 \in \{2, 3\}$, and one of the following holds.*

- *(S) $\bar{\rho}$ is congruent to J_s for a special parameter s, and $\varepsilon_3 = \varepsilon_5 = 3$.*
- *(CM) $\bar{\rho} \cong \bar{\rho}_{g,\mathfrak{P}}$ for a Hilbert newform g over K of parallel weight 2, trivial character and level $3^{\varepsilon_3}(\sqrt{5})^{\varepsilon_5} \neq 3^3(\sqrt{5})^3$, with complex multiplication by a totally imaginary quadratic extension M of K.*

If moreover (T2.1), (P7.4)(a) *at $\ell = 3$ and* (Ex_0) *hold, then in case* (CM) *either $M = \mathbb{Q}(\zeta_5)$ and $2 \mid X$, $3 \mid X$, $5 \nmid YZ$; or $M = K(\sqrt{-3})$ and $5 \mid Y$, $3 \nmid XZ$, $2 \nmid Z$.*

Proof. By (LL), (Ex) and (EL) (Remark 2.14), $\bar{\rho} \cong \bar{\rho}_{g,\mathfrak{P}}$ for a newform g, and either g is one of $g_{-1/8}$, $g_{9/8}$, of level $3^3(\sqrt{5})^3$, and $\bar{\rho}$ is congruent to J_s, or g is one of the newforms with complex multiplication at the three other levels. The last sentence is Proposition 6.6, whose condition $p \notin \{7, 19\}$ holds. □

Lemma 6.8. *Let $p \geq 7$ and suppose $\bar{\rho}$ is congruent to J_s for a special parameter s. Then $\bar{\rho}$ is irreducible with conductor $3^3(\sqrt{5})^3$, $5 \nmid XYZ$ and $t \bmod 25 \in \mathcal{A}$. Given* (Ex), *moreover $3 \nmid XZ$, $X \not\equiv \pm 4 \pmod 9$ if $3 \mid Y$, and $X^5 \not\equiv 4Y^3 \pmod 9$ if $3 \nmid Y$. Given* (T2.1) *(through Lemma 2.22(b)), $2 \mid Y$. Given* (Ex), *or* (P7.4)(a) *at $\ell = 3$, also $3 \mid Y$.*

Proof. By Theorem 3.6(a), $5 \nmid XYZ$ and $t \bmod 25 \in \mathcal{A}$. Irreducibility and the conductor are Lemma 2.7, the assertions given (Ex) are Corollary 2.21, and $3 \mid Y$ is Lemma 6.18(d), which uses (P7.4)(a) at $\ell = 3$ only when $3 \mid Z$, a case that (Ex) excludes. For $2 \mid Y$: the proof of Lemma 2.22(a) applies to $(X, Y) = (1, 2)$, $(-3, 6)$, so $a_{(2)}(J_s) = -1$. If $2 \mid X$, then Z is odd and $\operatorname{tr} \bar{\rho}(\mathrm{Frob}_{(2)}) = 0$ by Lemma 2.22(a); if $2 \mid Z$, then $\bar{\rho}$ is unramified at (2) and $\operatorname{tr} \bar{\rho}(\mathrm{Frob}_{(2)}) = \pm 5$ by Lemma 2.22(b). A congruence with J_s, in either orientation, gives $\operatorname{tr} \bar{\rho}(\mathrm{Frob}_{(2)}) = -1$ in $\overline{\mathbb{F}}_p$, so p would divide 1, 4 or 6. Hence $2 \mid Y$. □

6.5. **The classes modulo 25.**

Theorem 6.9. *Assume* (LL), (Ex) *and* (EL); *for* (ii) *also* (T2.1) *and* (P7.4)(a) *at $\ell = 3$; and for the part $2 \mid Y$ of $6 \mid Y$ in* (i) *also* (T2.1). *Let $p \notin \mathcal{P}$ be prime, split or inert in K, let $\mathfrak{p} \mid p$, and let (X, Y, Z) be a primitive solution of $X^5 + Y^3 = Z^p$ with $5 \nmid XYZ$ and $t \bmod 25 \notin \mathcal{T}$, that is, $t \equiv 3, 7, 8, 9, 12, 13, 14, 17, 19, 22, 23, 24 \pmod{25}$.*

- *(i) If $t \bmod 25 \in \mathcal{A} = \{3, 8, 9, 13, 14, 19, 23, 24\}$, then $\varepsilon_3 = 3$, $6 \mid Y$, $X \not\equiv \pm 4 \pmod 9$, and $\bar{\rho}_{t,\mathfrak{p}}$ is congruent to J_s for a special parameter s.*
- *(ii) If $t \bmod 25 \in \mathcal{B} = \{7, 12, 17, 22\}$, then $\varepsilon_3 = 2$, $6 \mid X$, and $\bar{\rho}_{t,\mathfrak{p}} \cong \bar{\rho}_{g,\mathfrak{P}}$ for a Hilbert newform g over K of parallel weight 2, trivial character and level $3^2(\sqrt{5})^3$ with complex multiplication by $\mathbb{Q}(\zeta_5)$.*

In particular, for these p there is no primitive solution with $5 \nmid XYZ$ and $t \bmod 25 \in \mathcal{A}$ unless $6 \mid Y$ and $X \not\equiv \pm 4 \pmod 9$, and none with $5 \nmid XYZ$ and $t \bmod 25 \in \mathcal{B}$ unless $6 \mid X$.

Here ε_3 is also the exponent of $\rho_{t,\lambda}$ (Lemma 6.2(a),(c)). In (i), the conclusions $\varepsilon_3 = 3$ and the congruence use only (LL), (Ex) and (EL); (Ex) puts the level among those of the elimination lists.

Proof. As $5 \nmid YZ$, J_t has potentially good reduction at $(\sqrt{5})$ (Lemma 2.18(b)), and $\varepsilon_5 = 3$ (Proposition 3.5(e)). So $\bar\rho|_{I_F}$, hence $\bar\rho$, is irreducible (Lemma 6.1), and Lemma 6.7 applies.

(i) Let $t \bmod 25 \in \mathcal{A}$. Case (CM) is excluded by Theorem 3.6(b). So we are in case (S). By Lemma 6.8, $3 \mid Y$ (by Lemma 6.18(d)), $X \not\equiv \pm 4 \pmod 9$ and $2 \mid Y$.

(ii) Let $t \bmod 25 \in \mathcal{B}$. Case (S) is excluded by Theorem 3.6(a), because $t \bmod 25 \notin \mathcal{A}$. So we are in case (CM), with level $3^2(\sqrt{5})^3$, and as $5 \nmid Y$, Lemma 6.7 gives $M = \mathbb{Q}(\zeta_5)$, $2 \mid X$ and $3 \mid X$. Its last sentence is used here only with (T2.1) and (P7.4)(a) at $\ell = 3$: (Ex_0) enters it only through the value of ε_3 (in $\{2, 3\}$, and 2 if $3 \mid Z$), which (Ex) gives. When $3 \mid Z$, the value 2 for $\bar\rho$ forces the character ψ_3 of Lemma 6.2(b) to be ramified, since for unramified ψ_3 the line $\psi_3\chi_p$ would be fixed by I_3 modulo $\mathfrak{p}$ and the exponent of $\bar\rho$ at most 1. □

Theorem 6.10. *Assume* (LL), (Ex) (*for* $\varepsilon_3 \in \{2, 3\}$) *and* (EL). *Then for every prime $p \notin \mathcal{P}$ the equation $X^5 + Y^3 = Z^p$ has no primitive solution with $5 \nmid XYZ$ and $t = -X^5/Y^3 \equiv 9, 14, 19, 24 \pmod{25}$.*

Proof. Let (X, Y, Z) be such a solution and $\mathfrak{p} \mid p$. As $\mathcal{A}^c \subset \mathcal{A}$, the proof of Theorem 6.9(i), with only these inputs, gives $J_t[\mathfrak{p}] \cong J_s[\mathfrak{p}]$ or $J_s[\mathfrak{p}']$ as $\mathbb{F}_p[G_K]$-modules. For p split these are the two orientations (Definition 4.5). For p inert, tensoring with $\mathbb{F}_{p^2} = \mathcal{O}_K/p$ gives $\bar\rho \oplus \bar\rho^\sigma \cong \bar\rho_{s,\mathfrak{p}} \oplus \bar\rho^\sigma_{s,\mathfrak{p}}$, and as both $\bar\rho$ and $\bar\rho_{s,\mathfrak{p}}$ are irreducible (Lemma 6.8), $\bar\rho \cong \bar\rho_{s,\mathfrak{p}}$ or $\bar\rho^\sigma_{s,\mathfrak{p}}$: a linear or σ-semilinear isomorphism, that is, the direct or the conjugate orientation (as also shown in §4.2, after Definition 4.6). As $p \geq 17$, Theorem 4.1(i) excludes both. □

6.6. **The classes $\mathcal{B}$ and the classes with $5 \mid X$.** For $c \in \mathbb{Q}^\times$ let $J_{0,c} = \mathrm{Jac}(C_{0,c})$, $C_{0,c}\colon V^2 = U^6 + 12cU$ (so $J_{0,1} = J_0$), and $J^{(-3)}_{0,c} = \mathrm{Jac}(-3V^2 = U^6 + 12cU)$. The family $C_{X,c}$ is smooth at $X = 0$, so, as in the proof of Proposition 2.2, the real multiplication of the family extends to $J_{0,c}$ with the same eigenvalue on $U\,dU/V$. For these Jacobians and for J_t, $a_\mathfrak{q}(J)$, G_J, G_J^σ and the type (o, e) relative to J_0 at $\sqrt{5}$ are as in Definitions 4.4 and 4.6. Each $J_{0,c}$ has complex multiplication by $\mathbb{Q}(\zeta_5)$ through $(U, V) \mapsto (\zeta_5 U, \zeta_5^3 V)$ (Lemma 2.5(a)).

Lemma 6.11. *The Hilbert newforms over K of parallel weight 2, trivial character and level dividing $3^2(\sqrt{5})^3$ with complex multiplication by $\mathbb{Q}(\zeta_5)$ are the 20 forms G_J, G_J^σ, for J one of the ten Jacobians $J_{0,c}$, $J^{(-3)}_{0,c}$, $c \in \{1, 3, 9, 27, 81\}$. Those of level $3^2(\sqrt{5})^3$ come from $J_{0,1}, J_{0,3}, J_{0,9}, J^{(-3)}_{0,1}, J^{(-3)}_{0,3}, J^{(-3)}_{0,9}, J^{(-3)}_{0,81}$; $J_{0,27}$, $J^{(-3)}_{0,27}$ give level $3^2(\sqrt{5})^2$ and $J_{0,81}$ level $(\sqrt{5})^3$.*

Proof. Such a form is the theta series of an algebraic Hecke character ψ of $M = \mathbb{Q}(\zeta_5)$ (class number 1: Minkowski's bound is 1.70) with infinity type a CM type, $\psi(\mathfrak{a}\mathcal{O}_M) = \theta_\zeta(\mathfrak{a})N\mathfrak{a}$ for ideals $\mathfrak{a}$ of K, and level $(\sqrt{5})\,N_{M/K}(\mathrm{cond}\,\psi)$; so $\mathrm{cond}\,\psi \mid P_3P_5^2$, where $P_3 = 3\mathcal{O}_M$ and $P_5 = (1 - \zeta_5)$; and ψ, $\psi \circ c_M$, with c_M the complex conjugation of M, give the same form. Counting characters of $(\mathcal{O}_M/P_3P_5^2)^\times$ with the prescribed values on ζ_5 and on $(\mathcal{O}_K/3\sqrt{5})^\times$ gives 10 for each of the four CM types. The ten Jacobians have conductor over $\mathbb{Q}$ dividing $3^4 \cdot 5^5$, so by Lemma 2.3 their Hecke characters and those characters' $\mathrm{Gal}(M/\mathbb{Q})$-conjugates lie among the 40 (PARI's `genus2red`: $3^4 \cdot 5^5$ for $J_{0,1}, J_{0,3}, J_{0,9}$, their twists and $J^{(-3)}_{0,81}$; $3^4 \cdot 5^4$ for $J_{0,27}$, $J^{(-3)}_{0,27}$; 5^5 for $J_{0,81}$; confirmed by the functional equation, `lfuncheckfeq`). That lemma

applies here, as its proof uses only Proposition 2.2(c), which holds for $J_{0,c}$ by the argument of Proposition 2.2 and passes to $J_{0,c}^{(-3)}$ because the twisting cocycle ± 1 commutes with ι. Comparing degree-4 Euler factors over $\mathbb{Q}$ at every prime $7 \le \ell \le 400$, each Jacobian matches exactly four characters, one $\mathrm{Gal}(M/\mathbb{Q})$-orbit, and each character exactly one Jacobian; this identifies all 40 characters, and the levels are read off. (PARI/GP; item C15.) □

Lemma 6.12. *Let τ_3 and T be as in Lemma 2.24.*

(a) $\operatorname{tr}\rho_{J_{0,c},\lambda}(\tau_3)$ is $\sigma(T)$ for $c = 3, 9$, T for $c = 27$ and 2 for $c = 81$; for $J_{0,c}^{(-3)}$ it is the negative of that for $J_{0,c}$.

(b) Let $p \ge 7$, (X, Y, Z) a primitive solution with $3 \mid X$, and $\bar\rho_{t,\mathfrak{p}} \cong \bar\rho_{G,\mathfrak{p}}$ for a newform G of level $3^2(\sqrt{5})^3$ with complex multiplication by $\mathbb{Q}(\zeta_5)$. Then $G \in \{G_{J_0}, G^\sigma_{J_{0,3}}, G^\sigma_{J_{0,9}}\}$.

Proof. (a) For $c = 3^k$ take $\pi_k = \pi_0\, 3^{k/5}$, $\pi_0^5 = -12$: then $\tau_3(\pi_k)/\pi_k = (\tau_3(\pi_0)/\pi_0)^{1+k}$, so τ_3 acts on the special fiber $\widetilde{C}\colon w^2 = z^6 - z$ of the proof of Lemma 2.24 by the $(1+k)$-th power of its action for J_0, with traces $\sigma(T)$, $\sigma(T)$, T, 2 for $k = 1, \dots, 4$; the quadratic character of $\mathbb{Q}_9(\sqrt{-3})$ is -1 on τ_3. (b) The images of I_3 (orders 5, 10, 2) are prime to p, so $\operatorname{tr}\rho_G(\tau_3) \equiv T$ modulo a prime above p. The differences of T and $\sigma(T)$, $-T$, $-\sigma(T)$, -2 have norms $-5, -4, 1, 1$, so $\operatorname{tr}\rho_G(\tau_3) = T$. As $\operatorname{tr}\rho_{G^\sigma}(\tau_3) = \sigma(\operatorname{tr}\rho_G(\tau_3))$, Lemma 6.11, Lemma 2.24 and (a) leave the three forms stated. □

TABLE 5. The data of the proof of Lemma 6.13, in its notation, at one parameter $t = 2 + 5s$ in each class of $\mathcal{B}$. Here $m \equiv 2/s \pmod 5$ is the scalar of the matching ν of the unit roots u_i of f_t with the roots of $U^5 + 12$; the Vandermonde ratio $S = \prod_{i<j}(\nu(u_i) - \nu(u_j))/(u_i - u_j)$ is a unit of $\mathbb{Z}_5$ with residue $m^{10} = (m/5)$; and, as both special fibers are $v'^2 = 3(z^5 - z)$, the Lefschetz count gives $(-1)^e = (m/5)$. The residues of $N_{02}/625$, $N_{13}/625$ are those of the entries $(0,2)$, $(1,3)$ of the matrix of $\iota(\sqrt{5})$ on the de Rham lattice of C_t, divided by the unit $\sqrt{5}\lambda_E^{-2}$, $\lambda_E = 1 - \zeta_5$; for J_0, in the odd model $V_1^2 = 12w^5 + 1$ (where $\Lambda_0 = \lambda_E$ and no factor 625 occurs), the corresponding residues are 3 and 4. Then $\eta(t)\eta(J_0) = -3\operatorname{res}(N_{02}/625)$, and $(-1)^o = \eta(t)\eta(J_0)(-1)^e$.

$t \bmod 25$	t	m	$\operatorname{res} S$	$(-1)^e$	$\operatorname{res}(N_{02}/625)$	$\operatorname{res}(N_{13}/625)$	$\eta(t)\eta(J_0)$	(o,e)
7	32	2	4	-1	2	1	-1	$(0,1)$
12	37	1	1	$+1$	2	1	-1	$(1,0)$
17	42	4	1	$+1$	2	1	-1	$(1,0)$
22	47	3	4	-1	2	1	-1	$(0,1)$

Lemma 6.13. *Let $t \in \mathbb{Z}_5$ with $t \bmod 25 \in \mathcal{B}$. Then $\rho_{t,\lambda}|_{W_F}$ has type $(0,1)$ relative to J_0 if $t \equiv 7, 22 \pmod{25}$ and type $(1,0)$ if $t \equiv 12, 17 \pmod{25}$. In particular it never has the type $(0,0)$ of J_0.*

Proof. We compare C_t with $C_{0,1}\colon V^2 = U^6 + 12U = U(U^5 + 12)$ by the method of §§4.2–4.4, with $\lambda_E = 1 - \zeta_5$ in place of ϱ, and state the analogue of each of Lemmas 4.7, 4.8, 4.9, 4.10, 4.12, 4.13 and 4.14 that we use. Write $t = 2 + 5s$ with $s \in \mathbb{Z}_5$, so that $t \bmod 25 \in \mathcal{B}$ means $5 \nmid s$. We use v and res as in §4.2.

The roots and the field. By Lemma 2.18(c), f_t has one root $u_0 \in \mathbb{Q}_5$ with $v(u_0) = -1$ and five unit roots $u_1, \dots, u_5$ with $v(u_i - u_j) = 1/4$, congruent to $3t^2 \equiv 2$; as in §4.2, $5u_0 \equiv 12 \pmod{5^3}$. Let $U_1, \dots, U_5$ be the roots of $U^5 + 12$, congruent to $U_i^5 = -12 \equiv 3$, and $E_{\mathcal{B}} = \mathbb{Q}_5(\zeta_5, U_1)$ their splitting field. By Proposition 3.5(b),(d) (with $X = 1$, $Y^3 = -1/t$ and $u_i = -1/(Yr_i)$), $\mathbb{Q}_5(u_1, \dots, u_5)$ is Galois and totally ramified of degree 20 over $\mathbb{Q}_5$, and its compositum with $\mathbb{Q}_5^{\mathrm{ur}}$ is $N_{\mathcal{B}}$, so that the type is defined (§3.7). By Proposition 3.5(c),(d) with $(X, Y) = (0, 1)$ ($-12 \equiv 13 \pmod{25}$ is not a fifth power in $\mathbb{Z}_5$), $\mathbb{Q}_5^{\mathrm{ur}} E_{\mathcal{B}} = L_0(U_1) = N_{\mathcal{B}}$, of degree 20 over $\mathbb{Q}_5^{\mathrm{ur}}$, so $E_{\mathcal{B}}$, Galois of degree at most 20 over $\mathbb{Q}_5$, is totally ramified of degree 20. The proof of Proposition 3.5(f) uses only these properties of the two fields, so $\mathbb{Q}_5(u_1, \dots, u_5) = E_{\mathcal{B}}$, and $\mathrm{Gal}(E_{\mathcal{B}}/\mathbb{Q}_5) \cong \mathbb{F}_{20}$ acts faithfully on $\{u_i\}$ and on $\{U_i\}$. The residue field of $E_{\mathcal{B}}$ is $\mathbb{F}_5$, $v(\lambda_E) = 1/4$, $5/\lambda_E^4 \equiv -1 \pmod{\lambda_E}$ (§3.1), and $\gamma(\lambda_E)/\lambda_E \equiv a \pmod{\lambda_E}$ if $\gamma(\zeta_5) = \zeta_5^a$.

Positions and the matching (Lemma 4.7(a), Lemma 4.9(b),(c)). Their proofs apply with λ_E in place of ϱ, as $\gamma(\lambda_E)/\lambda_E$ is a unit with residue in $\mathbb{F}_5^\times$. So there is a unique bijection $\nu\colon \{u_i\} \to \{U_i\}$ commuting with $\mathrm{Gal}(E_{\mathcal{B}}/\mathbb{Q}_5)$, and $\mathbb{Q}_5(\nu(u_i)) = \mathbb{Q}_5(u_i)$; the positions $\pi_t(u_i) = \mathrm{res}((u_i - u_1)/\lambda_E)$ and $\pi_0(U_i) = \mathrm{res}((U_i - \nu(u_1))/\lambda_E)$ are bijections onto $\mathbb{F}_5$, on which the elements of $\mathrm{Gal}(E_{\mathcal{B}}/\mathbb{Q}_5(\zeta_5))$ act by translations; and $\pi_0(\nu(u_i)) = m\,\pi_t(u_i)$ for some $m = m(t) \in \mathbb{F}_5^\times$.

The scalar m. We show that $m \equiv 2/s \pmod 5$; so $m = 2, 1, 4, 3$ for $t \equiv 7, 12, 17, 22 \pmod{25}$, and $(m/5) = (2/5)(s/5) = -(s/5)$. The field $L = \mathbb{Q}_5(u_1)$ is totally ramified of degree 5 and contains $\Pi_1 = u_1 - 2$ and $\Pi_2 = \nu(u_1) - 3$. As $f_t(u) = 5(u - u_0)\prod_{i=1}^5 (u - u_i)$, their norms are

$$N_{L/\mathbb{Q}_5}(\Pi_1) = \prod_{i=1}^5 (u_i - 2) = -\frac{f_t(2)}{5(2 - u_0)}, \qquad N_{L/\mathbb{Q}_5}(\Pi_2) = \prod_{i=1}^5 (U_i - 3) = -(3^5 + 12) = -255,$$

where $f_t(2) = t^2 + 80t - 64 \equiv 20s \pmod{25}$ and $5(2 - u_0) \equiv 3 \pmod 5$. So $v(\Pi_1) = v(\Pi_2) = 1/5$, both are uniformizers of L, and $\nu(u_1) = \sum_{k=0}^4 \beta_k \Pi_1^k$ with $\beta_k \in \mathbb{Z}_5$ and $\beta_0 \equiv 3 \pmod 5$. As in the proof of Lemma 4.9(d), $m \equiv \beta_1 \pmod 5$, and $\beta_1 \equiv \Pi_2/\Pi_1$ modulo the maximal ideal. A unit of L and its conjugates have the same residue in $\mathbb{F}_5$, so the residue of its norm is its fifth power, that is, its own residue. Hence

$$m \equiv \frac{N_{L/\mathbb{Q}_5}(\Pi_2)}{N_{L/\mathbb{Q}_5}(\Pi_1)} = \frac{51 \cdot 5(2 - u_0)}{f_t(2)/5} \equiv \frac{3}{4s} \equiv \frac{2}{s} \pmod 5.$$

The Vandermonde ratio $S = \prod_{i<j} (\nu(u_i) - \nu(u_j))/(u_i - u_j)$ lies in $\mathbb{Q}_5$, as ν commutes with $\mathrm{Gal}(E_{\mathcal{B}}/\mathbb{Q}_5)$, and each of its ten factors is a unit with residue $(\pi_0(\nu(u_i)) - \pi_0(\nu(u_j)))/(\pi_t(u_i) - \pi_t(u_j)) = m$; so $\mathrm{res}\, S = m^{10} = m^2 = (m/5)$.

The good models and e (Lemmas 4.8 and 4.10). Let $\varpi_E^2 = \lambda_E$, $P_E = \mathbb{Q}_5(\varpi_E)$, which contains $\mathbb{Q}_5(\zeta_5) \supset F$, and $E'_{\mathcal{B}} = E_{\mathcal{B}}(\varpi_E)$, totally ramified of degree 40 with residue field $\mathbb{F}_5$. As $E_{\mathcal{B}} \cap P_E = \mathbb{Q}_5(\zeta_5)$, $\mathrm{Gal}(E'_{\mathcal{B}}/P_E) \cong \mathrm{Gal}(E_{\mathcal{B}}/\mathbb{Q}_5(\zeta_5))$ is cyclic of order 5. The substitution $u = u_1 + \lambda_E z$, $v = \varpi_E^5 v'$ turns C_t into

$$v'^2 = d_0\Big(1 + \frac{\lambda_E z}{u_1 - u_0}\Big)\prod_{i=1}^5 (z - z_i), \qquad d_0 = 5(u_1 - u_0) \equiv 3, \quad z_i = \frac{u_i - u_1}{\lambda_E},$$

and $U = \nu(u_1) + \lambda_E z$, $V = \varpi_E^5 V'$ turn $C_{0,1}$ into $V'^2 = \nu(u_1)(1 + \lambda_E z/\nu(u_1))\prod_{i=1}^5 (z - (U_i - \nu(u_1))/\lambda_E)$, with $\nu(u_1) \equiv 3$. So both curves have good reduction over $E'_{\mathcal{B}}$ with the same special fiber $\widetilde{C}\colon v'^2 = 3(z^5 - z)$. Let $g \in I_{P_E} \subset I_F$ map to a nontrivial element of $\mathrm{Gal}(E'_{\mathcal{B}}/P_E)$. It fixes λ_E and ϖ_E, so it acts on the special fiber of C_t by $z \mapsto z + b_g(t)$,

$b_g(t) = \pi_t(gu_1)$, and on that of $C_{0,1}$ by $z \mapsto z + b_g(J_0)$, $b_g(J_0) = \pi_0(g\nu(u_1)) = m\, b_g(t)$. Let $\phi_0 \in W_{E'_{\mathcal{B}}}$ be a Frobenius element, so that $\mu(\phi_0 g) = -1$. The proof of Lemma 4.8 uses only $\widetilde{C}$ and the translation, so $\operatorname{tr}(\phi_0 g \mid V_\ell(J)) = 5\,(b/5)$ for $(J,b) = (J_t, b_g(t))$ and for $(J,b) = (J_0, b_g(J_0))$, for every prime $\ell \neq 5$. As in the proof of Theorem 3.7(b), the type (o,e) gives $V_\ell(J_t)|_{W_F} \cong V_\ell(J_0)|_{W_F} \otimes \mu^e$, and the traces at $\phi_0 g$ give

$$(-1)^e = \Big(\frac{b_g(t)\, b_g(J_0)}{5}\Big) = \Big(\frac{m}{5}\Big) = -\Big(\frac{s}{5}\Big)\,:$$

$e = 1$ for $t \equiv 7, 22$ and $e = 0$ for $t \equiv 12, 17 \pmod{25}$.

The de Rham lattices and o (Lemma 4.12). For C_t we use the model of §4.4: $w = 1/(u - u_0)$, $\hat{v} = vw^3$, $\hat{v}^2 = h(w)$ of degree 5 with roots $w_i = 1/(u_i - u_0)$, and, with $\Lambda = 25\lambda_E$, the substitution $w = w_1 + \Lambda\xi$, $\hat{v} = 5^3\varpi_E^5 v''$, which gives $v''^2 = \upsilon \prod_{i=1}^5 (\xi - \xi_i)$ over $\mathcal{O}_{E'_{\mathcal{B}}}$ with υ a unit and $\xi_i = -z_i(w_i/5)(w_1/5) \equiv -z_i/9 \equiv \pi_t(u_i)$, as $w_i/5 \equiv 1/d_0 \equiv 1/3$. For $C_{0,1}$ we use the odd model $V_1^2 = 12w^5 + 1$ ($w = 1/U$, $V_1 = Vw^3$), with roots $w_i^0 = 1/U_i$ and base root $w_1^0 = 1/\nu(u_1)$, and, with $\Lambda_0 = \lambda_E$, the substitution $w = w_1^0 + \lambda_E\xi$, $V_1 = \varpi_E^5 v''$, which gives $v''^2 = 12 \prod_{i=1}^5 (\xi - \xi_i^0)$ with $\xi_i^0 = -(U_i - \nu(u_1))/(\lambda_E U_i \nu(u_1)) \equiv \pi_0(U_i)$, as $U_i\nu(u_1) \equiv 9$. In both cases g acts on the special fiber by $\xi \mapsto \xi + b_g$, with $b_g = b_g(t)$, resp. $b_g(J_0)$, and, as in §4.4, the classes $\xi^j\, d\xi/v''$ $(0 \le j \le 3)$ are a basis of the de Rham cohomology of the smooth proper model, preserved by the real multiplication. The proof of Lemma 4.12 applies to $J = J_t$ and to $J = J_0$: $\operatorname{tr}\rho_{J,\lambda}(g) = (\theta_g(J)\sqrt{5} - 1)/2$ with $\theta_g(J) = \pm 1$; the reduction of $\iota(\sqrt{5})$ in the basis $\xi^j\, d\xi/v''$ is $\eta(J)D$, with D as in Lemma 4.12(b) and $\eta(J) = \theta_g(J)\,(b_g/5)$ (formed now with λ_E; only the product below enters); and $\theta_g(J_t) = (-1)^o \theta_g(J_0)$, as μ is trivial on I_F. Hence, with $\eta(t) = \eta(J_t)$,

$$(-1)^o = \eta(t)\,\eta(J_0)\Big(\frac{b_g(t)\, b_g(J_0)}{5}\Big) = \eta(t)\,\eta(J_0)\,(-1)^e.$$

The normalization of η for J_0. The automorphism $\alpha(U,V) = (\zeta_5 U, \zeta_5^3 V)$ acts on the odd model by $(w, V_1) \mapsto (\zeta_5^{-1} w, V_1)$, so $\alpha^*(w^j\, dw/V_1) = \zeta_5^{-j-1} w^j\, dw/V_1$. By Lemma 2.5(a), $\iota(\sqrt{5})$ lies in the real subfield of $\mathbb{Q}[\alpha] \cong \mathbb{Q}(\zeta_5)$, so $\iota(\sqrt{5}) = \pm(1 + 2(\alpha + \alpha^{-1}))$, which acts on $w^j\, dw/V_1$ by $\pm(1 + 2(\zeta_5^{j+1} + \zeta_5^{-j-1}))$: one value for $j = 0, 3$ and the opposite value for $j = 1, 2$. As $dw/V_1 = -U\, dU/V$, on which $\iota(\sqrt{5})$ acts by $\sqrt{5}$ (§4.1), the matrix of $\iota(\sqrt{5})$ in the basis $w^j\, dw/V_1$ is $\sqrt{5}M_0$ with $M_0 = \operatorname{diag}(1, -1, -1, 1)$. Expanding $w^i = (w_1^0 + \lambda_E\xi)^i$ as in the proof of Lemma 4.14, its matrix in the basis $\xi^j\, d\xi/v''$ has entries $\sqrt{5}\lambda_E^{j-k}(N_0)_{jk}$, where, with $(B_0)_{ji} = \binom{i}{j}(w_1^0)^{i-j}$,

$$N_0 = B_0 M_0 B_0^{-1} = \begin{pmatrix} 1 & -2w_1^0 & 2(w_1^0)^2 & 0 \\ 0 & -1 & 0 & 6(w_1^0)^2 \\ 0 & 0 & -1 & 6w_1^0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

As $w_1^0 \equiv 1/3 \equiv 2$, the entries $(0,2)$ and $(1,3)$ are $\sqrt{5}\lambda_E^{-2}$ times units with residues 3 and 4, and the other entries have positive valuation. So $4\eta(J_0) = 3\operatorname{res}(\sqrt{5}\lambda_E^{-2})$.

The computation for J_t (Lemma 4.14). The proof of Lemma 4.14 uses only the Gauss–Manin formulas for the family and the model above. So the matrix of $\iota(\sqrt{5})$ in the basis $\xi^j\, d\xi/v''$ has entries $\sqrt{5}\Lambda^{j-k}N_{jk}$, with $N = BMB^{-1}$ as there; as $\Lambda^2 = 625\lambda_E^2$, its $(0,2)$ entry is $\sqrt{5}\lambda_E^{-2} \cdot N_{02}/625$, and $4\eta(t) = \operatorname{res}(\sqrt{5}\lambda_E^{-2})\operatorname{res}(N_{02}/625)$. As $5\lambda_E^{-4} \equiv -1$ and $16 \equiv 1 \pmod 5$,

$$\eta(t)\,\eta(J_0) = 3\operatorname{res}(5\lambda_E^{-4})\operatorname{res}(N_{02}/625)/16 = -3\operatorname{res}(N_{02}/625).$$

We computed N at the parameters of Table 5 exactly as in the proof of Lemma 4.14, with approximations $\tilde{u}_0$ and $\tilde{Q}$ at precision 5^{80}, $\tilde{Q}(X+2)$ Eisenstein, and exact arithmetic in $\mathbb{Q}$ and $\mathbb{Q}(\tilde{u}_1)$. At each of them $v(f_t(\tilde{u}_1)) \geq 80$, $v(f_t'(\tilde{u}_1)) = 1$, $v(G(5\tilde{u}_0)) \geq 80$ and $v(G'(5\tilde{u}_0)) = 0$, so $v(u_1 - \tilde{u}_1) \geq 78$ and $v(u_0 - \tilde{u}_0) \geq 79$; the determinant of the matrix of coordinates of the four classes has valuation -10; and the propagation of the errors shows that each entry of the computed matrix $(\sqrt{5}\Lambda^{j-k}N_{jk})$ differs from the true entry by an element of valuation at least $303/4$. The valuations of the computed entries are those displayed in the proof of Lemma 4.14 at $-1/8$, except that the entry $(1,2)$ has valuation $9/4$, and $N_{02}/625$, $N_{13}/625$ are units with residues 2 and 1, in the ratio $2:1$ of D. So $\eta(t)\eta(J_0) = -6 \equiv -1$, and $(-1)^o = -(-1)^e$: $o = 0$ for $t \equiv 7, 22$ and $o = 1$ for $t \equiv 12, 17 \pmod{25}$.

Constancy (Lemma 4.13). By the formula for m, e depends only on t mod 25. The proof of Lemma 4.13 applies to the classes in $\mathcal{B}$, with $E'_{\mathcal{B}}$ and λ_E in place of E'_c and ϱ, as it uses only the valuations of u_0, w_1, Λ and of the coefficients of f_t, which are the same; so $\eta(t)$, and hence o, depends only on t mod 25. This proves the lemma. □

Theorem 6.14. *Assume* (LL), (EL), (T2.1), (P7.4)(a) *at* $\ell = 3$ *and* (Ex_0). *Then for every prime* $p \notin \mathcal{P}$ *the equation* $X^5 + Y^3 = Z^p$ *has no primitive solution with* $5 \nmid XYZ$ *and* $t = -X^5/Y^3 \equiv 7, 12, 17, 22 \pmod{25}$.

Proof. Let (X, Y, Z) be such a solution and $\mathfrak{p} \mid p$. By Theorem 6.9(ii) (whose proof applies with these inputs, §6.4), $3 \mid X$ and $\bar{\rho} \cong \bar{\rho}_{G,\mathfrak{P}}$ for a newform G of level $3^2(\sqrt{5})^3$ with complex multiplication by $\mathbb{Q}(\zeta_5)$; by Lemma 6.11 its coefficient field is K, and replacing G by G^σ if $\mathfrak{P} \neq \mathfrak{p}$ (for p inert, if the identification of residue fields is the conjugate one) we may take $\mathfrak{P} = \mathfrak{p}$. By Lemma 6.12(b), $G \in \{G_{J_0}, G^\sigma_{J_{0,3}}, G^\sigma_{J_{0,9}}\}$, and $p \geq 17$, so Theorem 4.19 excludes the last two. If $G = G_{J_0}$, the reductions of $\rho_{t,\mathfrak{p}}|_{W_F}$ and $\rho_{J_0,\mathfrak{p}}|_{W_F}$ agree; but the first has type $(0,1)$ or $(1,0)$ (Lemma 6.13), the second $(0,0)$, and the four types remain distinct modulo $\mathfrak{p}$ for $p \neq 2, 5$ (Lemma 3.9). □

Theorem 6.15. *Assume* (LL), (EL), (T2.1), (P7.4)(a) *at* $\ell = 3$ *and* (Ex_0). *Then for every prime* $p \notin \mathcal{P}$ *the equation* $X^5 + Y^3 = Z^p$ *has no primitive solution with* $5 \mid X$ *and* $Y \equiv \pm 6, \pm 8, \pm 9, \pm 12 \pmod{25}$.

Proof. Here $Y^4 \equiv 11$ or $21 \pmod{25}$, and by Proposition 3.10(a),(c) $\rho_{t,\lambda}|_{W_F} \cong \rho_{J_{0,c},\lambda}|_{W_F}$ with $c = 9$ or 81: its conductor exponent at $\sqrt{5}$ is 3 (Lemma 6.11) and its type relative to J_0 is $(1,1)$ (Lemma 3.9). As $5 \nmid YZ$, J_t has potentially good reduction at $\sqrt{5}$, so $\bar{\rho}|_{I_F}$ is irreducible (Lemma 6.1). In Lemma 6.7, case (S) is excluded by Theorem 3.6(a) since $5 \mid X$; so $\bar{\rho} \cong \bar{\rho}_{g,\mathfrak{P}}$ with g of level $3^{\varepsilon_3}(\sqrt{5})^3 \neq 3^3(\sqrt{5})^3$ with complex multiplication, by $\mathbb{Q}(\zeta_5)$ since $5 \nmid Y$, and $2 \mid X$, $3 \mid X$ (Proposition 6.6; the field of complex multiplication is determined there from local data, Remark 2.15). So $\varepsilon_3 = 2$, and as in the proof of Theorem 6.14, $g \in \{G_{J_0}, G^\sigma_{J_{0,3}}, G^\sigma_{J_{0,9}}\}$ (Lemma 6.12), the last two are excluded by Theorem 4.19, and G_{J_0} has type $(0,0) \neq (1,1)$ modulo $\mathfrak{p}$. □

For $5 \mid X$ and $Y \equiv \pm 1, \pm 3, \pm 4, \pm 7 \pmod{25}$ the same argument gives $6 \mid X$ and $\bar{\rho}_{t,\mathfrak{p}} \cong \bar{\rho}_{G_{J_0},\mathfrak{p}}$, in the orientation of J_0, and stops there: by Proposition 3.10(c) these classes have the type of J_0 itself at $\sqrt{5}$.

Remark 6.16. A solution in the classes of Theorems 6.14 and 6.15 would have $6 \mid X$ (by Theorem 6.9(ii) and the proof of Theorem 6.15), hence $3 \nmid Y$. Pacetti and Villagra Torcomian [33, Theorem C] state that there is no primitive solution with $3 \nmid Y$ for $p \notin \mathcal{P}$ larger than an unspecified constant, under (LI). Their proof also needs a further large-image hypothesis,

for the J_t that are isogenous over $\overline{\mathbb{Q}}$ to the square of an elliptic curve without complex multiplication; for $p \equiv \pm 1 \pmod 5$ it is the following.

(LI′) There is a constant C' such that for every prime $p > C'$ with $p \equiv \pm 1 \pmod 5$, every primitive solution (X, Y, Z) of $X^5 + Y^3 = Z^p$ for which J_t is isogenous over $\overline{\mathbb{Q}}$ to the square of an elliptic curve without complex multiplication, and every prime $\mathfrak{p}$ of K above p, the image of $\bar\rho_{t,\mathfrak{p}}$ contains $\mathrm{SL}_2(\mathbb{F}_p)$.

Indeed, (LI) concerns abelian varieties A with $\mathrm{End}_L(A)\otimes\mathbb{Q} = \mathrm{End}_{\overline{L}}(A)\otimes\mathbb{Q} \cong K'$, while such a J_t has $\mathrm{End}_{\overline{\mathbb{Q}}}(J_t)\otimes\mathbb{Q} \cong M_2(\mathbb{Q})$, so (LI) does not apply to it. The proof of [33, Theorem C] treats these J_t in one sentence, as a case in which [33, Conjecture 1] is proven; but Serre's open image theorem [37] gives a bound for each such J_t separately, not one bound for all solutions. Here the classes of Theorems 6.14 and 6.15 are excluded without (LI) or (LI′), for every $p \notin \mathcal{P}$, given the statements of [33] that these theorems assume.

6.7. The solutions with $3 \mid Y$ and with $3 \nmid XYZ$.

Theorem 6.17. *Assume* (LL), (EL) *and* (T2.1). *Let $p \notin \mathcal{P}$ be prime, $\mathfrak{p} \mid p$, and let (X, Y, Z) be a primitive solution of $X^5 + Y^3 = Z^p$ with $3 \mid Y$ and $5 \nmid YZ$. Then*

$$5 \nmid X, \qquad X \not\equiv \pm 4 \pmod 9, \qquad 2 \mid Y, \qquad t \bmod 25 \in \mathcal{A},$$

and $\bar\rho_{t,\mathfrak{p}}$ is congruent to J_s for a special parameter s. In particular there is no primitive solution with $3 \mid Y$, $5 \nmid YZ$, and either $5 \mid X$ or $t \bmod 25 \in \mathcal{B} \cup \mathcal{T}$.

Proof. Here $3 \nmid XZ$, J_t has potentially good reduction at (3) and $(\sqrt{5})$ (Lemma 6.2(c), Lemma 6.3(c)), and $\varepsilon_3, \varepsilon_5 \in \{2, 3\}$ (Lemma 6.2(e), Proposition 3.5(e)).

If $\bar\rho$ is irreducible, the conclusion holds. Case (CM) of Lemma 6.7 needs $3 \mid X$ or $5 \mid Y$ (Proposition 6.6, which, as $3 \nmid XZ$, needs only (T2.1) here; §6.4). In case (S), Lemma 6.8 gives $5 \nmid XYZ$ (so $5 \nmid X$), $t \bmod 25 \in \mathcal{A}$ and $2 \mid Y$; and, as $\varepsilon_3 = 3$ and $3 \mid Y$, $X \not\equiv \pm 4 \pmod 9$ (Lemma 6.2(e)).

$\bar\rho$ is irreducible. By Proposition 6.4, which here also needs only (T2.1), a reducible $\bar\rho$ would give $30 \mid Z$, which is false as $3 \nmid Z$. □

For a Jacobian A as in Proposition 2.2 with potentially good reduction at 3 and $\lambda \nmid 3$, let $L_A \subset \overline{\mathbb{Q}}_3$ be the fixed field of $\ker \rho_{A,\lambda}|_{I_3}$, Galois over $\mathbb{Q}_3^{\mathrm{ur}}$ with group $\rho_{A,\lambda}(I_3)$. For $g \in I_3$, $\rho_{A,\lambda}(g)$ has characteristic polynomial $x^2 - a(g)x + 1$ with $a(g) \in \mathcal{O}_K$ independent of $\lambda \nmid 3$ (Lemma 2.4). As g has finite image, $\rho_{A,\lambda}(g) = 1$ for one $\lambda \nmid 3$ if and only if $a(g) = 2$, that is, if and only if g acts trivially on $V_\ell(A)$ for every $\ell \neq 3$. So L_A does not depend on λ, A has good reduction over L_A [40, Theorem 1], and L_A is Galois over $\mathbb{Q}_3$ if A is defined over $\mathbb{Q}$.

Lemma 6.18. *(a) Let A be J_t, where $t = -X^5/Y^3$ for coprime integers X, Y with $3 \nmid XY(X^5 + Y^3)$, or $A = J_\infty$. Then L_A contains the roots of f_t, respectively of $F_{1,0} = U^6 + 10U^3 + 5$, and $9 \nmid [L_A : \mathbb{Q}_3^{\mathrm{ur}}]$.*

(b) If moreover $X^5 \not\equiv 4Y^3 \pmod 9$, then $L_{J_t} \neq L_{J_\infty}$.

(c) Let (X, Y, Z) be a primitive solution with $3 \nmid XYZ$ and $X^5 \not\equiv 4Y^3 \pmod 9$, let $p \geq 7$, and let $\mathfrak{p}, \mathfrak{p}^*$ be primes of K above p. Then the restrictions of $\bar\rho_{t,\mathfrak{p}}$ and $\bar\rho_{\infty,\mathfrak{p}^*}$ to I_3 have different kernels; in particular they are not isomorphic, even after extension of scalars.

(d) Let (X, Y, Z) be a primitive solution with $3 \nmid Y$, let $p \geq 7$, $\mathfrak{p} \mid p$, and s a special parameter. If $3 \nmid Z$, or if $3 \mid Z$ and (P7.4)(a) *at $\ell = 3$ holds, then $\bar\rho_{t,\mathfrak{p}}$ is not congruent to J_s. So* (T7.18) *holds for $p \geq 7$, given* (P7.4)(a) *at $\ell = 3$ when $3 \mid Z$.*

Proof. (a) The pairs (X,Y) in (a) and $(X,Y)=(1,0)$ satisfy $3\nmid X$ and $3\nmid X^5+Y^3$, so by Lemma 6.2(d) and its proof the roots of $\mathcal{F}_{X,Y}$ form two clusters s_1,s_2 of three roots at mutual distance $3^{-1/2}$, A has potentially good reduction, and the stable reduction has one genus-1 component E_i for each cluster; in the chart $U=z_1+\sqrt{3}\,w$ of that proof ($z_1\in s_1$) the three roots $r\in s_1$ give the three points $w=(r-z_1)/\sqrt{3}$, $V=0$, whose reductions on E_1 are distinct, and likewise for s_2. So the six Weierstrass points specialize to six distinct points of the stable fiber. As A has good reduction over L_A, the curve is semistable over L_A [13, Theorem 1.9(1)], with stable model defined over the ring of integers of L_A. An element of $\mathrm{Gal}(\overline{\mathbb{Q}}_3/L_A)$ acts trivially on this model and on its special fiber, so, specialization being Galois-equivariant, it fixes each Weierstrass point. Hence L_A contains the roots of $\mathcal{F}_{X,Y}$, and so those of f_t, which are $-X^2/(Yr)$ for the roots r of $\mathcal{F}_{X,Y}$ (Lemma 2.1).

The finite group $\rho_{A,\lambda}(I_3)$ lies in $\mathrm{SL}_2(\overline{K}_\lambda)$ (det is cyclotomic), so its Sylow 3-subgroups are cyclic (an abelian subgroup of exponent 3 is simultaneously diagonalizable with determinant 1), and an element of order 9 would have trace $\zeta_9+\zeta_9^{-1}\notin K$. So $9\nmid|\rho_{A,\lambda}(I_3)|=[L_A:\mathbb{Q}_3^{\mathrm{ur}}]$.

(b) Here $t,1-t\in\mathbb{Z}_3^\times$, and $t\equiv 5\pmod 9$ exactly when $X^5\equiv 4Y^3\pmod 9$; so $t\equiv t_0\pmod 9$ with $t_0\in\{2,8\}$. We use the following computation, made with PARI/GP 2.17.3 [44] (`polcompositum`, `idealprimedec`): for $t_0=2$ and $t_0=8$, f_{t_0} is irreducible over $\mathbb{Q}$, the field $\mathbb{Q}(r_0)$ generated by a root has a single prime above 3, with $(e,f)=(3,2)$, and every prime above 3 of every compositum of $\mathbb{Q}(r_0)$ with the field of a root of $F_{1,0}$ has ramification index 9. Hence for every root r_0 of f_{t_0} and every root r_∞ of $F_{1,0}$ in $\overline{\mathbb{Q}}_3$, $[\mathbb{Q}_3^{\mathrm{ur}}(r_0,r_\infty):\mathbb{Q}_3^{\mathrm{ur}}]=e(\mathbb{Q}_3(r_0,r_\infty)/\mathbb{Q}_3)=9$ (item C18).

We pass from t_0 to t by Krasner's lemma. Modulo 3, $f_t\equiv f_{t_0}\equiv 2u^6+2u^3+1=2(u^2+u+2)^3$, and u^2+u+2 is irreducible over $\mathbb{F}_3$; so the roots of f_t and of f_{t_0} are units falling into the same two residue classes, three in each. The roots of f_{t_0} in one residue class are pairwise at distance exactly $3^{-1/2}$. Indeed, they are the $-X_0^2/(Y_0r)$, r a root of $\mathcal{F}_{X_0,Y_0}$ (Lemma 2.1), for $Y_0=1$ and $X_0\in\mathbb{Z}_3$ with $X_0^5=-t_0$ (the fifth-power map is bijective on $\mathbb{Z}_3^\times$); here $3\nmid X_0(X_0^5+Y_0^3)=X_0(1-t_0)$, so the proof of Lemma 6.2(d), which uses only $3\nmid X(X^5+Y^3)$, shows that the roots of $\mathcal{F}_{X_0,Y_0}$ in one residue class are pairwise at distance exactly $3^{-1/2}$; and so are those of f_{t_0}, as X_0, Y_0 and the roots r are units. Let r be a root of f_t. Then

$$f_{t_0}(r)=f_{t_0}(r)-f_t(r)=(t_0-t)(10r^3+t+t_0)$$

has valuation at least 2. Writing $f_{t_0}(r)=5\prod_j(r-r'_j)$ over the roots r'_j of f_{t_0}, the three r'_j in the other residue class contribute 0, so some r'_j has $v(r-r'_j)\geq 2/3>1/2$. Every conjugate of r'_j over $\mathbb{Q}_3$ other than r'_j is at distance at least $3^{-1/2}$ from it, so Krasner's lemma gives $\mathbb{Q}_3(r'_j)\subseteq\mathbb{Q}_3(r)$.

Now suppose $L_{J_t}=L_{J_\infty}=L$. By (a), L contains r and every root r_∞ of $F_{1,0}$, hence $\mathbb{Q}_3^{\mathrm{ur}}(r'_j,r_\infty)$, of degree 9 over $\mathbb{Q}_3^{\mathrm{ur}}$. Then $9\mid[L:\mathbb{Q}_3^{\mathrm{ur}}]$, contradicting (a).

(c) The images of I_3 have order prime to p (§6.1), so reduction modulo $\mathfrak{p}$, $\mathfrak{p}^*$ is injective on them and the kernels are $\mathrm{Gal}(\overline{\mathbb{Q}}_3/L_{J_t})\neq\mathrm{Gal}(\overline{\mathbb{Q}}_3/L_{J_\infty})$.

(d) Suppose $J_t[\mathfrak{p}]\cong J_s[\mathfrak{q}]$ as $\mathbb{F}_p[G_K]$-modules, with $\mathfrak{q}\in\{\mathfrak{p},\mathfrak{p}'\}$. By Lemma 2.7, J_s has potentially good reduction at 3, and by Lemma 5.9, 12 divides $|\Phi_{J_s}|$; as $\Phi_{J_s}\cong\rho_{s,\mathfrak{q}}(I_3)$ (§5.1 and the paragraph before the lemma) acts faithfully on $J_s[\mathfrak{q}]$ (its order is prime to p), an element of I_3 mapping to an element of order 3 of Φ_{J_s} has eigenvalues of order 3 on $J_s[\mathfrak{q}]$. If $3\mid Z$, then by (P7.4)(a) at $\ell=3$ the reduction of J_t at 3 is potentially multiplicative, of toric rank 2, so that $\rho_{t,\mathfrak{p}}|_{I_3}\cong\psi_3\otimes\left(\begin{smallmatrix}1&*\\0&1\end{smallmatrix}\right)$ with $\psi_3^2=1$ (proof of Lemma 6.2(b)), and every element of I_3 has only the eigenvalues ±1 on $J_t[\mathfrak{p}]$, a contradiction. So $3\nmid Z$, and J_t has potentially good reduction at 3 (Lemma 6.2(a),(c)). As in the proof of (c), the kernels of I_3 on $J_t[\mathfrak{p}]$ and

on $J_s[\mathfrak{q}]$, which agree, are those of $\rho_{t,\lambda}|_{I_3}$ and $\rho_{s,\lambda}|_{I_3}$; so $L_{J_t} = L_{J_s} =: L$ and $\Phi_{J_t} \cong \Phi_{J_s}$. If $3 \mid X$, Φ_{J_t} is cyclic of order 5 (Lemma 6.2(a)), a contradiction. So $3 \nmid XYZ$, and as $|\Phi_{J_t}| \neq 4$, Lemma 6.2(e) gives $X^5 \not\equiv 4Y^3 \pmod 9$, that is, $t \equiv t_0 \pmod 9$ with $t_0 \in \{2, 8\}$. By (a) and the proof of (b), L contains a root r_0' of f_{t_0}. As $L = L_{J_s}$, it also contains the roots of the sextic $U^6 + 10U^3 + 24U + 5$ of $C_{1,2}$, respectively $U^6 - 30U^3 + 72U + 45$ of $C_{-3,6}$: an element of $\mathrm{Gal}(\overline{\mathbb{Q}}_3/L)$ acts trivially on $V_\ell(J_s)$ for $\ell \neq 3$, hence on $J_s[2]$, so it fixes the Weierstrass points (proof of Lemma 3.4(a)). By the computation of item C18, $[\mathbb{Q}_3^{\mathrm{ur}}(r_0', r_s) : \mathbb{Q}_3^{\mathrm{ur}}] = 9$ for every root r_s of either sextic. So $9 \mid [L : \mathbb{Q}_3^{\mathrm{ur}}]$, against (a). □

By Lemma 2.5(b), $\rho_{\infty,\lambda}$ is induced from an algebraic Hecke character of $K(\sqrt{-3})$. Its theta series is a Hilbert newform g_∞ over K of parallel weight 2, trivial character and level $3^3(\sqrt{5})^2$, with $\rho_{g_\infty,\lambda} \cong \rho_{\infty,\lambda}$. Let g_∞^σ be its conjugate under $\mathrm{Gal}(K/\mathbb{Q})$, with $a_{\mathfrak{l}}(g_\infty^\sigma) = a_{\sigma(\mathfrak{l})}(g_\infty)$.

Lemma 6.19. *Let g be a Hilbert newform over K of parallel weight 2, trivial character and level $3^i(\sqrt{5})^j$ with $i, j \in \{2, 3\}$, with complex multiplication by $K(\sqrt{-3})$. Then $a_{(2)}(g) = -1$ if and only if $g \in \{g_\infty, g_\infty^\sigma\}$; these two have level $3^3(\sqrt{5})^2$.*

Proof. The newforms in question are the theta series of the 60 algebraic Hecke characters of $K(\sqrt{-3})$ found in the proof of Proposition 6.6 (30 newforms, each from two characters ψ, $\psi \circ c$). A computation with PARI/GP (item C19) gives: exactly four of the characters have $a_{(2)} = -1$, all four give level $3^3(\sqrt{5})^2$, and they are exactly the characters whose Euler factors agree with those of J_∞ over $\mathbb{Q}$ at every prime $7 \leq \ell \leq 200$. These primes generate the relevant ray class group, so the four characters are those of g_∞ and g_∞^σ. □

Theorem 6.20. *Assume* (LL); (EL)*, including its statement that the surviving newforms at the levels $3^2(\sqrt{5})^2$, $3^2(\sqrt{5})^3$ and $3^3(\sqrt{5})^2$ have complex multiplication; and* (T2.1)*. Let $p \notin \mathcal{P}$ be prime, split or inert in K. Then the equation $X^5 + Y^3 = Z^p$ has no primitive solution with $3 \nmid XYZ$.*

Proof. Let (X, Y, Z) be such a solution and $\mathfrak{p} \mid p$.

$\bar\rho$ is irreducible. By Proposition 6.4, which needs only (T2.1) here, as $3 \nmid XZ$ (§6.4), a reducible $\bar\rho$ would give $30 \mid Z$, which is false as $3 \nmid Z$.

Reduction to complex multiplication by $K(\sqrt{-3})$. A congruence with J_s is excluded by Lemma 6.18(d), as $3 \nmid YZ$; so we are in case (CM) of Lemma 6.7, and since $3 \nmid X$, $M = K(\sqrt{-3})$, $5 \mid Y$ and Z is odd (Proposition 6.6, which here also needs only (T2.1)). By the computation in the proof of Proposition 6.6, the level of g is $3^{\varepsilon_3}(\sqrt{5})^2$ and $a_{(2)}(g) \in \{\pm 1, \pm 2, \pm 4, (\pm 1 \pm 3\sqrt{5})/2\} \subset \mathcal{O}_K$.

The trace at (2). As Z is odd, J_t has good reduction at (2) and $a_{(2)}(J_t)$ is 0 if $2 \mid X$ and -1 if $2 \mid Y$ (Lemma 2.22(a)); so $p \mid N_{K/\mathbb{Q}}(a_{(2)}(g) - a_{(2)}(J_t))$. If $2 \mid X$, this is $N_{K/\mathbb{Q}}(a_{(2)}(g)) \in \{1, 4, 16, -11\}$. So $2 \mid Y$, and p divides $N_{K/\mathbb{Q}}(a_{(2)}(g) + 1) \in \{0, 1, 4, 9, 25, -9, -11\}$; as $p \notin \mathcal{P}$ (so $p \notin \{2, 3, 5, 11\}$), $a_{(2)}(g) = -1$. By Lemma 6.19, $g \in \{g_\infty, g_\infty^\sigma\}$, of level $3^3(\sqrt{5})^2$. So $\varepsilon_3 = 3$, and by Lemma 6.2(e), $X^5 \not\equiv 4Y^3 \pmod 9$.

The prime 3. If $g = g_\infty$, then $\bar\rho \cong \bar\rho_{g_\infty,\mathfrak{P}} = \bar\rho^{\mathrm{ss}}_{\infty,\mathfrak{p}^*}$ for a prime $\mathfrak{p}^*$ of K above p, after extension of scalars. If $g = g_\infty^\sigma$, then $\rho_{g_\infty^\sigma,\mathfrak{P}}(h) = \rho_{g_\infty,\mathfrak{P}}(chc^{-1})$ with $c \in G_{\mathbb{Q}} \smallsetminus G_K$ in a decomposition group at 3 (3 is inert in K); as L_{J_∞} is Galois over $\mathbb{Q}_3$, the kernel on I_3 is unchanged. In both cases $\bar\rho|_{I_3}$, which is semisimple, has the same kernel as $\bar\rho_{\infty,\mathfrak{p}^*}|_{I_3}$, contradicting Lemma 6.18(c). □

6.8. The primes $p \equiv 19, 29, 31, 41 \pmod{60}$.

Theorem 6.21. *Assume* (LL), (Ex_0), (EL), (T2.1), *and* (P7.4)(a) *at* $\ell = 3$. *Let* $p \equiv 19, 29, 31, 41 \pmod{60}$ *with* $p \geq 139$, *let* $\mathfrak{p} \mid p$, *and let* (X, Y, Z) *be a primitive solution of* $X^5 + Y^3 = Z^p$. *Then exactly one of the following holds.*

- *(E)* $30 \mid Z$, *and* $\bar{\rho}$ *is reducible with* $\bar{\rho}^{\mathrm{ss}} \cong \theta_{15} \oplus \theta_{15}\bar{\chi}_p$ (θ_{15} *the character of* $\mathbb{Q}(\zeta_{15})^+/K$).
- *(Z)* $6 \mid X$, $\gcd(Z, 30) = 1$ *and* $5 \nmid Y$, *and* $\bar{\rho} \cong \bar{\rho}_{g,\mathfrak{P}}$ *for a Hilbert newform* g *over* K *of parallel weight* 2 *and trivial character with complex multiplication by* $\mathbb{Q}(\zeta_5)$.
- *(T)* $5 \mid Y$, $3 \nmid X$ *and* $\gcd(Z, 30) = 1$, *and* $\bar{\rho} \cong \bar{\rho}_{g,\mathfrak{P}}$ *for such a newform* g *with complex multiplication by* $K(\sqrt{-3}) = \mathbb{Q}(\sqrt{5}, \sqrt{-3})$.

Proof. These p split in K, $p \notin \mathcal{P}$. If $\bar{\rho}$ is reducible, (E) holds by Proposition 6.4. Otherwise [33, Theorem 7.8] gives g with $\bar{\rho} \cong \bar{\rho}_{g,\mathfrak{P}}$ at level $3^{\varepsilon_3}(\sqrt{5})^{\varepsilon_5}$, $\varepsilon_i \in \{2, 3\}$ (Theorem 2.8, (Ex_0), Lemma 6.2(b); at $\sqrt{5}$, Lemma 2.20 if $5 \mid Y$, Lemma 2.19 and Lemma 6.3(b) if $5 \mid Z$, and Proposition 3.5(e) if $5 \nmid YZ$), and by the elimination lists g has complex multiplication or $\bar{\rho}$ is congruent to some J_s; the latter is excluded by Lemma 6.18(d) if $3 \nmid Y$ and by Theorem 5.1 if $3 \mid Y$. Now Proposition 6.6 gives (Z) or (T) (in (T), $2 \nmid Z$ as $p \notin \{7, 19\}$), and $\gcd(Z, 30) = 1$ follows by coprimality. The classes are disjoint: $30 \mid Z$ only in (E), $5 \nmid Y$ in (Z), $5 \mid Y$ in (T). □

Corollary 6.22. *Under the assumptions of Theorem 6.21, every primitive solution has* $\gcd(Z, 30) \in \{1, 30\}$, *and if* $\gcd(Z, 30) = 1$, *then* $6 \mid X$ *or* $5 \mid Y$. *Of the* 48 *possibilities for which of* X, Y, Z *is divisible by* 2, *by* 3 *and by* 5, *only the seven in Table 6 can occur.*

TABLE 6. The divisibility patterns allowed by Theorem 6.21; "–" means that none of X, Y, Z is divisible by the prime.

class	(E)	(Z)	(Z)	(T)	(T)	(T)	(T)
2 divides	Z	X	X	Y	X	Y	X
3 divides	Z	X	X	Y	Y	–	–
5 divides	Z	X	–	Y	Y	Y	Y

Proof. Read off from Theorem 6.21. □

Each class contains a trivial solution: $Z = 0$ ($t = 1$) for (E), $X = 0$ (J_0, with complex multiplication by $\mathbb{Q}(\zeta_5)$) for (Z), and $Y = 0$ (J_∞, with complex multiplication by $K(\sqrt{-3})$) for (T). So we do not expect local comparisons, or auxiliary primes in the style of Mazur, to exclude any class (Supplement, Remark S1.1).

Under the assumptions of Theorem 6.21, so for $p \equiv 19, 29, 31, 41 \pmod{60}$ with $p \geq 139$, the Supplement reduces the three classes to rational points on modular curves over K that classify Borel and normalizer-of-Cartan level structures on $J_t[\mathfrak{p}]$ (Theorem S1.12). It shows that in the classes in which $\mathfrak{p}$ is inert in the field of complex multiplication, J_t has good reduction at p with Frobenius polynomial $(T^2 + p)^2$ (Propositions S1.14 and S1.15), and it proves that no primitive solution has $\varepsilon_3 = \varepsilon_5 = 3$ (Theorem S1.3).

6.9. **The solutions with $3 \mid Z$ or $5 \mid Z$.** The description of the class (E) in Theorem 6.21 holds for every p outside a small set, with fewer inputs.

Theorem 6.23. *Assume* (LL) *and* (Ex_0); (EL) *at the levels* $3^2(\sqrt{5})^2$, $3^2(\sqrt{5})^3$ *and* $3^3(\sqrt{5})^2$, *including its statement that the surviving newforms at these levels have complex multiplication;*

(T2.1); *and* (P7.4)(a) *at* $\ell = 3$. *Let* $p \geq 7$ *be a prime not in* $\{7, 11, 13, 19, 29, 31, 41, 61\}$, *split or inert in* K, *let* $\mathfrak{p} \mid p$, *and let* (X, Y, Z) *be a primitive solution of* $X^5 + Y^3 = Z^p$ *with* $3 \mid Z$ *or* $5 \mid Z$. *Then* $30 \mid Z$, *and* $\bar{\rho}$ *is reducible with* $\bar{\rho}^{\mathrm{ss}} \cong \theta_{15} \oplus \theta_{15}\bar{\chi}_p$. *In particular no primitive solution has* Z *odd and divisible by* 3 *or by* 5.

Proof. Suppose that $\bar{\rho}$ is irreducible. By [33, Theorem 7.8], $\bar{\rho} \cong \bar{\rho}_{G,\mathfrak{P}}$ for a newform G of level $3^{\varepsilon_3}(\sqrt{5})^{\varepsilon_5}$, where $\varepsilon_3, \varepsilon_5 \in \{2, 3\}$ (as in the proof of Theorem 6.21), with $\varepsilon_3 = 2$ if $3 \mid Z$ and $\varepsilon_5 = 2$ if $5 \mid Z$. So the level is one of the three named, at which the elimination discards every newform other than the surviving ones, which have complex multiplication, for p outside $\{2, 3, 5, 11, 19, 29\}$, $\{2, 3, 5, 7, 11, 13, 19, 29, 31\}$ and $\{2, 3, 5, 7, 11, 19, 29, 31, 41, 61\}$ respectively (Remark 2.14); p lies outside all three. So G has complex multiplication, and by Proposition 6.6 either $3 \mid X$ and $5 \nmid YZ$, or $5 \mid Y$ and $3 \nmid XZ$. As X, Y, Z are pairwise coprime, both contradict $3 \mid Z$ and both contradict $5 \mid Z$. So $\bar{\rho}$ is reducible, and Proposition 6.4 gives the rest. □

Remark 6.24. The last sentence of Theorem 6.23 is [33, Theorem B] (Theorem 2.17) for $p \geq 7$, with the same excluded primes, which come from the elimination lists (EL). Theorem 6.23 adds that these solutions have $30 \mid Z$ and a reducible $\bar{\rho}$ with the semisimplification above, so that for these primes every primitive solution has $\gcd(Z, 30) \in \{1, 2, 30\}$; and its proof uses Propositions 6.4 and 6.6 in place of [33, Corollary 7.7] and of a level lowering that preserves the special local type. For $p \equiv 19, 29, 31, 41 \pmod{60}$ with $p \geq 139$ it is the class (E) of Theorem 6.21.

6.10. **Summary, class by class.**

Theorem 6.25. *Assume* (LL), (EL), (T2.1), (P7.4)(a) *at* $\ell = 3$ *and* (Ex_0). *Let* $p \notin \mathcal{P}$ *be prime and* (X, Y, Z) *a primitive solution of* $X^5 + Y^3 = Z^p$, $t = -X^5/Y^3$.

(a) If $5 \nmid XYZ$, *then* $t \equiv 2, 3, 4, 8, 13, 18$ *or* $23 \pmod{25}$.

(b) If $5 \mid X$, *then* $Y \not\equiv \pm 6, \pm 8, \pm 9, \pm 12 \pmod{25}$.

(c) If, besides $p \notin \mathcal{P}$, $p \equiv 19, 29, 31, 41 \pmod{60}$, *then* $5 \nmid XYZ$ *forces* $t \equiv 2, 4, 18 \pmod{25}$, *and every primitive solution satisfies one of:* $30 \mid Z$ *and* $\bar{\rho}_{t,\mathfrak{p}}$ *is reducible;* $5 \mid Y$; $6 \mid X$ *and either* $5 \nmid XYZ$ *with* $t \equiv 2, 4, 18 \pmod{25}$, *or* $5 \mid X$ *with* $Y \equiv \pm 1, \pm 2, \pm 3, \pm 4, \pm 7, \pm 11 \pmod{25}$.

(d) If $3 \mid Z$ *or* $5 \mid Z$, *then* $30 \mid Z$ *and* $\bar{\rho}_{t,\mathfrak{p}}$ *is reducible; in particular* $3 \mid Z$ *if and only if* $5 \mid Z$.

Proof. If $5 \nmid Y$ and $5 \mid t$, then $5 \mid X$ and $5^5 \mid t$; if $t \equiv 1 \pmod 5$, then $5 \mid Z$ and $5^p \mid t - 1$. So for $5 \nmid XYZ$ the residue of t is one of the 15 classes of $\mathcal{A} \cup \mathcal{B} \cup \mathcal{T}$, and (a) follows from Theorems 6.14 and 6.10, (b) is Theorem 6.15. (d) is Theorem 6.23, whose excluded primes all lie in $\mathcal{P}$. For (c), $p \geq 139$; for $t \bmod 25 \in \mathcal{A}^d = \{3, 8, 13, 23\}$, Theorem 6.9(i) gives $3 \mid Y$, $5 \nmid Y$ and a congruence with some J_s, which Theorem 5.1 excludes. By Theorem 6.21, every solution is in (E): $30 \mid Z$ and $\bar{\rho}$ reducible; (T): $5 \mid Y$; or (Z): $6 \mid X$, $5 \nmid YZ$, and then $5 \nmid XYZ$ with $t \equiv 2, 4, 18$, or $5 \mid X$ with Y outside the classes of (b). □

Table 7 lists every class modulo 25, with the result that removes it or the fact that it remains; every result it cites holds under the hypotheses of Theorem 6.25 (for (Ex), see §6.4).

TABLE 7. The classes modulo 25 for $p \notin \mathcal{P}$, given the results of [33] named in Theorem 6.25.

Class	Further condition	Status	Result
$t \equiv 5, 6, 10, 11, 15, 16, 20, 21$		does not occur	Theorem 6.25
$5 \nmid XYZ$, $t \equiv 7, 12, 17, 22$		no solution	Theorem 6.14
$5 \nmid XYZ$, $t \equiv 9, 14, 19, 24$		no solution	Theorem 6.10
$5 \nmid XYZ$, $t \equiv 3, 8, 13, 23$	$p \equiv 19, 29, 31, 41$ (60)	no solution	Theorems 5.1 and 6.9
	$p \equiv \pm 2$ (5), $(3/p) = -1$, $X \equiv \pm 1$ (9), or $(3/p) = 1$, $X \equiv \pm 2$ (9)	no solution	Theorems 5.3 and 6.9
	other p	remains: $6 \mid Y$, $X \not\equiv \pm 4$ (9), congruence with $J_{s(t)}$, direct orientation	Theorems 4.1 and 6.9
$5 \nmid XYZ$, $t \equiv 2, 4, 18$	$3 \mid Y$	no solution	Theorem 6.17
	$3 \nmid XYZ$	no solution	Theorem 6.20
	$3 \mid Z$	no solution	Theorem 6.23
	$3 \mid X$	remains; only with $6 \mid X$ if $p \equiv 19, 29, 31, 41$ (60)	Theorem 6.21
$5 \mid X$, $Y \equiv \pm 6, \pm 8, \pm 9, \pm 12$		no solution	Theorem 6.15
$5 \mid X$, $Y \equiv \pm 1, \pm 3, \pm 4, \pm 7$		remains: $6 \mid X$, $\bar{\rho}_{t,\mathfrak{p}} \cong \bar{\rho}_{G_{J_0},\mathfrak{p}}$	Theorem 6.15 and the paragraph after it
$5 \mid X$, $Y \equiv \pm 2, \pm 11$	$3 \mid Y$, or $3 \nmid XYZ$, or $3 \mid Z$	no solution	Theorems 6.17, 6.20 and 6.23
	$3 \mid X$	remains; only with $6 \mid X$ if $p \equiv 19, 29, 31, 41$ (60)	Theorem 6.21
$5 \mid Z$ ($t \equiv 1$)		only with $30 \mid Z$ and $\bar{\rho}_{t,\mathfrak{p}}$ reducible, $\bar{\rho}^{\mathrm{ss}}_{t,\mathfrak{p}} \cong \theta_{15} \oplus \theta_{15}\bar{\chi}_p$	Theorem 6.23
$5 \mid Y$ ($v_5(t) < 0$)	$3 \nmid XYZ$, or $3 \mid Z$	no solution	Theorems 6.20 and 6.23
	$3 \mid X$ or $3 \mid Y$	remains; only with $3 \mid Y$, in class (T) of Theorem 6.21, if $p \equiv 19, 29, 31, 41$ (60)	Theorem 6.21

APPENDIX A. COMPUTATIONS

The computations are made with polynomials over $\mathbb{Z}$, in number fields, in finite fields and in p-adic fields to a fixed precision sufficient to determine the residues and valuations used. Every item except item C16 was computed a second time by a separately written program, and for most items one of the two computations does not use PARI, in whole or in part; the programs and these second computations are described item by item in [25]. Only the evaluations of L-functions in item C5, and three checks in the second computations of items, are numerical: the checks of conductors by `lfuncheckfeq` in items C1 and C15, of the Igusa invariants from complex roots in item C1, and of the global root numbers of $A_{-1/8}$, $A_{9/8}$ in item C13. The computations were made with PARI/GP 2.17.3 [44], Python 3.12 (with cypari2 for access to PARI, SymPy 1.14, mpmath 1.4.1, NumPy 2.5.2, SciPy 1.18 and python-flint 0.8.0), SageMath 10.9 [45], and, for one computation of the Supplement, the C programming language. Table 8 lists the computations in the order of first use, with the approximate total running time of all the programs of each item on a single processor core.

TABLE 8. Computations used in the proofs.

Item	Establishes	Used in	Software	Time
C1	$\operatorname{disc} f_t$, $\operatorname{disc} \mathcal{F}_{X,Y}$, the identity $f_t(-X^2/(YU)) = X^{10}\mathcal{F}_{X,Y}(U)/(Y^6U^6)$, the substitution carrying C_t to $C(0,Q)$ and its discriminant; the Igusa invariants of C_t and the quotients $\mathcal{I}_{2i}^5/\mathcal{I}_{10}^i$; the conductor exponents $(b_3,b_5) = (4,5)$, $(6,4)$, $(6,5)$, $(6,5)$ of $C_{0,1}$, $C_{1,0}$, $C_{1,2}$, $C_{-3,6}$	§§2.2–2.6; Remarks 2.15 and 3.8	PARI/GP, SymPy, mpmath, NumPy, SageMath	5 min
C2	Frobenius polynomials $x^4 + x^2 + 4$ and $x^4 + 4$ over $\mathbb{F}_2$ of $w^2 + (U^3+1)w = 1$ and $w^2 + U^3 w = U$, hence $(x^2+x+4)^2$ and $(x^2+4)^2$ over $\mathbb{F}_4$	Lemma 2.22(a)	PARI/GP, Python	1 s
C3	K has narrow class number 1 and $\mathrm{Cl}_K(3\sqrt{5}\,\infty_1\infty_2) \cong \mathbb{Z}/4 \times \mathbb{Z}/2$ (`bnrinit`)	Lemma 2.23(a)	PARI/GP, SageMath	5 s
C4	Frobenius polynomials of $w^2 = z^6 - z$: $x^4 + 9$ over $\mathbb{F}_3$, $(x^2+9)^2$ over $\mathbb{F}_9$, $(x+9)^4$ over $\mathbb{F}_{81}$; its Jacobian is supersingular	Lemma 2.24	PARI/GP, SageMath	6 s
C5	Numerical, without a rigorous error bound: for $C_{1,2}$ and $C_{-3,6}$ with conductor $3^6 5^5$ the functional equation holds to about 140 and 145 bits, and the root numbers are $w = -1$ and $w = +1$ (`lfungenus2`, `lfuncheckfeq`, `lfunrootres`)	Remark 3.8(ii), as a numerical check	PARI/GP, mpmath, NumPy, SciPy	5 min
C6	$A_{-1/8}$, $A_{9/8}$ have minimal models $y^2 + y = x^3 - 30x + 63$, $y^2 + y = x^3 - 7$ and conductor 27, and are joined by a cyclic isogeny of degree 9 (`ellminimalmodel`, `ellisomat`)	Theorem 3.7(a), Remark 3.8(iii)	PARI/GP, SageMath	7 s
C7	The Hecke characters of the $J_{0,c}$ and their twists by -3, from twisted point counts: their orders on $(\mathcal{O}_M/P_3)^\times$ (5 for J_0), the types at P_5 ($(0,0)$ for $J_{0,3}$, $(1,1)$ for $J_{0,9}$ and $J_{0,81}$, $J_{0,27}$ tame); the twist e of curves with $5 \mid X$	confirms Lemma 2.24, Lemma 3.9, Proposition 3.10(c)	PARI/GP	2 min
C8	The scalars $m(t_0) = 1,4,4,3,2,3,2,1$ for $t_0 \equiv 3,8,9,13,14,19,23,24 \pmod{25}$, exactly (Hensel's lemma; errors of valuation $\geq 91/5$) and in Sage; the equality of fields in Lemma 4.9(a)	Lemma 4.9(a),(d)	PARI/GP, SageMath, Python	3 min
C9	The Gauss–Manin derivatives in the proof of Lemma 4.14; the matrix of $\iota(\sqrt{5})$, up to errors of valuation $\geq 303/4$, giving $\eta = 1$ at $-1/8$, $9/8$ and for $t_0 \equiv 3$, and $\eta = -1$ for $t_0 \equiv 4 \pmod 5$; the cup-product determinant in §4.4	Lemma 4.14, hence Proposition 4.15	PARI/GP, SymPy, python-flint	45 s
C10	The pairs (c_1,c_2) of §4.5 for every C_τ and every fiber with $q \mid XY$, $q = 11, 19$; the fibers sharing the polynomial of a special parameter; the norms of the case $q \mid Z$	Proposition 4.16; Theorem 4.19 ($q = 11$)	Python, PARI/GP	5 s
C11	At $\mathfrak{q} = (11, \sqrt{5} - 4)$: $a_{\mathfrak{q}}(J_{0,3}) = (-11 + \sqrt{5})/2$ and $a_{\mathfrak{q}}(J_{0,9}) = (-1 + \sqrt{5})/2$, each told apart from its conjugate by the Cartier–Manin matrix; no fiber has trace $\sigma(a)$ at $\mathfrak{q}$; only the fibers with $11 \mid X$, $Y = \pm c$ have the polynomial of $J_{0,c}$; the norms 305, 41, 155, 131	Theorem 4.19	PARI/GP, Python	5 min

TABLE 8. Computations used in the proofs (continued).

Item	Establishes	Used in	Software	Time
C12	The coefficients D_k, $k \le 12$, of $D(z) = \mathrm{Res}_U(\mathcal{F}_{X,Y}(U), \mathcal{F}_{X,Y}(U+z))/z^6$ and their 3-adic valuations; for $Y = 3Y_1$, the vanishing and valuations of R_k in Lemma 5.7; the valuations of the coefficients R_k, and of the root differences, for $(X,Y) = (1,2)$, $(-3,6)$	Lemmas 5.7 and 5.9; Lemma 6.2(d)	PARI/GP, SymPy, SageMath	8 s
C13	The data in the proof of Lemma 5.17 (the models at $t = 0, \infty$ and their reductions, f_1, c_4 and Δ of A_t); for $A_{-1/8}$, $A_{9/8}$: minimal models, conductor 27, $W_3 = -1$, global root number $+1$, and the 2-division field $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, with ramification index 6 at 3	Lemmas 5.17 and 5.19	PARI/GP, SageMath	16 s
C14	Newforms with complex multiplication by $M = K(\sqrt{-3})$: the characters $\psi((\alpha)) = \Phi(\alpha)/\chi(\alpha)$, χ a character of $(\mathcal{O}_M/\mathfrak{Q}_3^2\mathfrak{Q}_5)^\times$, with trivial character on the primes above $7 \le \ell \le 300$: 18 for each CM type (15 per type at the levels $3^2(\sqrt{5})^2$ and $3^3(\sqrt{5})^2$), giving 3 newforms at level $3^2(\sqrt{5})^2$ and 27 at $3^3(\sqrt{5})^2$; their $a_{(2)}$ and the norms $\{1, 9, 16, 19, 36, 49, 81\}$	Proposition 6.6(b), Lemma 6.19 and Theorem 6.20	PARI/GP, SageMath	20 s
C15	The algebraic Hecke characters of $M = \mathbb{Q}(\zeta_5)$ (class number 1, `bnfcertify`) of conductor dividing $P_3P_5^2$ with trivial-character theta series: 40, at levels $(\sqrt{5})^3$ (4), $3^2(\sqrt{5})^2$ (8), $3^2(\sqrt{5})^3$ (28), matched with the ten $J_{0,c}$, $J_{0,c}^{(-3)}$ by Euler factors at $7 \le \ell \le 400$; the conductors of these Jacobians (`genus2red`)	Lemma 6.11	PARI/GP, Python	14 s
C16	The traces of a generator of tame inertia at 3 on $J_{0,c}$, $c = 3, 9, 27, 81$: $\sigma(T)$, $\sigma(T)$, T, 2, and their negatives for the twists by -3; images of inertia of orders $5, 5, 5, 1$ and $10, 10, 10, 2$	confirms Lemma 6.12(a)	PARI/GP	7 s
C17	The types of the classes $\mathcal{B}$: the matrix of $\iota(\sqrt{5})$ on the de Rham lattice of C_t, up to errors of valuation $\ge 303/4$, at twelve parameters in each class (residues 2, 1 of $N_{02}/625$, $N_{13}/625$), and the scalars $m = 2, 1, 4, 3$ for $t \equiv 7, 12, 17, 22 \pmod{25}$ (Hensel's lemma), at twenty-one; the data of J_0 in the odd model; and, by further programs, the types $(0,1)$ for $t \equiv 7, 22$ and $(1,0)$ for $t \equiv 12, 17$ at eight representatives of each class	Lemma 6.13	PARI/GP, SageMath	2 min
C18	For $t_0 = 2, 8$: f_{t_0} is irreducible, $\mathbb{Q}(r_0)$ has one prime above 3, with $(e,f) = (3,2)$, and every prime above 3 of every compositum of $\mathbb{Q}(r_0)$ with the field of a root of $F_{1,0}$, of $U^6 + 10U^3 + 24U + 5$ or of $U^6 - 30U^3 + 72U + 45$ has ramification index 9 (`polcompositum`, `idealprimedec`)	Lemma 6.18(b),(d)	PARI/GP, Python, SageMath	24 s
C19	Of the 60 characters of item C14 at the levels $3^2(\sqrt{5})^2$ and $3^3(\sqrt{5})^2$, exactly four have $a_{(2)} = -1$, all at level $3^3(\sqrt{5})^2$, and they are those whose Euler factors agree with those of J_∞ over $\mathbb{Q}$ at every prime $7 \le \ell \le 200$	Lemma 6.19	PARI/GP, SageMath	14 s

Data availability. The programs, their outputs and the commands that run them are in [25].

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. Michael A. Bennett, Preda Mihăilescu, and Samir Siksek, *The generalized Fermat equation*, Open Problems in Mathematics (John Forbes Nash, Jr. and Michael Th. Rassias, eds.), Springer, Cham, 2016, pp. 173–205.
2. Nicolas Billerey, Imin Chen, Luis Dieulefait, and Nuno Freitas, *A multi-Frey approach to Fermat equations of signature* (r, r, p), Trans. Amer. Math. Soc. **371** (2019), no. 12, 8651–8677.
3. ———, *On Darmon's program for the generalized Fermat equation, I*, J. Reine Angew. Math. **822** (2025), 107–146.
4. Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21, Springer-Verlag, Berlin, 1990.
5. Massimo Ceccon, *The case* $3 \mid c$ *in the generalized Fermat equation* $x^5 + y^p = z^3$, preprint, Zenodo, 2 April 2026, doi:10.5281/zenodo.19388263.
6. ———, *Finite auxiliary-prime support on the* $3 \mid c$ *branch of the generalized Fermat equation of signature* $(5, p, 3)$, preprint, version 1.0, Zenodo, 15 August 2026, doi:10.5281/zenodo.21974186.
7. ———, *Working notes, dated 8–11 August 2026*, unpublished; deposited on 17 August 2026 with the files of [6] in the Zenodo record doi:10.5281/zenodo.21974186.
8. Imin Chen and Angelos Koutsianas, *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.
9. Peter Chocian, *The primitive generalized Fermat equation* $x^3 + y^5 = z^7$*: a computer-assisted proof*, 2026, preprint, arXiv:2609.26996v1.
10. Sander R. Dahmen and Samir Siksek, *On the generalized Fermat equation* $x^5 + y^3 = z^7$, working paper, July 2024, few.vu.nl/~sdn249/GFE357.pdf.
11. Henri Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's last theorem*, Duke Math. J. **102** (2000), no. 3, 413–449.
12. Henri Darmon and Andrew Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), no. 6, 513–543.
13. Tim Dokchitser, Vladimir Dokchitser, Céline Maistret, and Adam Morgan, *Arithmetic of hyperelliptic curves over local fields*, Math. Ann. **385** (2023), no. 3–4, 1213–1322.
14. Gerd Faltings and Ching-Li Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 22, Springer-Verlag, Berlin, 1990.
15. Nuno Freitas, *On the Fermat-type equation* $x^3 + y^3 = z^p$, Comment. Math. Helv. **91** (2016), no. 2, 295–304.
16. Nuno Freitas and Alain Kraus, *On the symplectic type of isomorphisms of the p-torsion of elliptic curves*, Mem. Amer. Math. Soc. **277** (2022), no. 1361, v+105.

17. Nuno Freitas, Bartosz Naskręcki, and Michael Stoll, *The generalized Fermat equation with exponents 2, 3, n*, Compos. Math. **156** (2020), no. 1, 77–113.
18. Franco Golfieri Madriaga and Ariel Pacetti, *Hypergeometric motives and the generalized Fermat equation*, 2025, with an appendix by A. Pacetti and F. Rodriguez Villegas; preprint, arXiv:2412.08804v2.
19. Franco Golfieri Madriaga, Ariel Pacetti, and Fernando Rodriguez Villegas, *On rank 2 hypergeometric motives*, 2026, with an appendix by E. Lorenzo García and A. Pacetti; preprint, arXiv:2603.17978v1.
20. Alexander Grothendieck, *Revêtements étales et groupe fondamental (SGA 1)*, Lecture Notes in Math., vol. 224, Springer-Verlag, Berlin-New York, 1971.
21. ———, *Groupes de monodromie en géométrie algébrique. I (SGA 7 I)*, Lecture Notes in Math., vol. 288, Springer-Verlag, Berlin-New York, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969, avec la collaboration de M. Raynaud et D. S. Rim; Exposé IX: *Modèles de Néron et monodromie*, pp. 313–523.
22. Emmanuel Halberstadt and Alain Kraus, *Courbes de Fermat: résultats et problèmes*, J. Reine Angew. Math. **548** (2002), 167–234.
23. Manvir Jaswal, *The generalized Fermat equation $x^{11} + y^{11} = z^5$*, 2026, preprint, Zenodo, doi:10.5281/zenodo.23149242.
24. ———, *The generalized Fermat equation $X^5 + Y^3 = Z^7$*, 2026, preprint, Zenodo, doi:10.5281/zenodo.22949749.
25. ———, *Programs and data for "Real multiplication and the generalized Fermat equation $x^5 + y^3 = z^p$"*, 2026, Zenodo, doi:10.5281/zenodo.23149236.
26. Abhinav Kumar and Ronen E. Mukamel, *Real multiplication through explicit correspondences*, LMS J. Comput. Math. **19, suppl. A** (2016), 29–42.
27. Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.
28. Qing Liu, *Courbes stables de genre 2 et leur schéma de modules*, Math. Ann. **295** (1993), no. 2, 201–222.
29. James S. Milne, *Complex multiplication*, 2020, course notes, version 0.10, https://www.jmilne.org/math/CourseNotes/cm.html.
30. David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970.
31. David Mumford, John Fogarty, and Frances Kirwan, *Geometric invariant theory*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete (2), vol. 34, Springer-Verlag, Berlin, 1994.
32. Ariel Pacetti and Lucas Villagra Torcomian, *GFE-5p3: code for the article "On the generalized Fermat equation of signature $(5, p, 3)$"*, 2025, GitHub repository, https://github.com/lucasvillagra/GFE-5p3, commit `e88f914` (22 December 2025), file `Outputs/TheoremA.txt`.
33. ———, *On the generalized Fermat equation of signature $(5, p, 3)$*, 2025, preprint, arXiv:2512.17845v1.
34. Piet Hein Casper Putz, *Enumeration of local and global étale algebras applied to generalized Fermat equations*, Ph.D. thesis, Vrije Universiteit Amsterdam, 2024, doi:10.5463/thesis.832.
35. Michel Raynaud, *Schémas en groupes de type $(p, \dots, p)$*, Bull. Soc. Math. France **102** (1974), 241–280.
36. Ottavio G. Rizzo, *Average root numbers for a nonconstant family of elliptic curves*, Compos. Math. **136** (2003), no. 1, 1–23.
37. Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
38. ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, translated from the French by Marvin Jay Greenberg.
39. ———, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230, doi:10.1215/S0012-7094-87-05413-5.
40. Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), no. 3, 492–517.
41. Goro Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series, vol. 46, Princeton University Press, Princeton, NJ, 1998.
42. John Tate, *Number theoretic background*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., vol. XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 3–26.
43. The LMFDB Collaboration, *The L-functions and modular forms database*, 2026, https://www.lmfdb.org.

44. The PARI Group, *PARI/GP version 2.17.3*, 2025, Univ. Bordeaux, https://pari.math.u-bordeaux.fr/.
45. The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 10.9)*, https://www.sagemath.org.
46. André Weil, *Jacobi sums as "Grössencharaktere"*, Trans. Amer. Math. Soc. **73** (1952), no. 3, 487–495.

Toronto, Canada
Email address: manvirjaswal@icloud.com