THE GENERALIZED FERMAT EQUATION $x^p + y^p = z^5$ AND RELATIVE CLASS NUMBERS

MANVIR JASWAL

ABSTRACT. We prove that the equation $x^p + y^p = z^5$ has no solution in nonzero coprime integers for every prime $p \geq 13$ such that $p \not\equiv 1 \pmod 5$ and $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$, using results of Chen and Koutsianas (to appear in Algebra & Number Theory) on Darmon's Frey surfaces. These conditions hold at 41 primes $13 \leq p < 1000$ and at 2432 primes $13 \leq p < 10^5$. For every prime $p \geq 7$ with $p \not\equiv 1 \pmod 5$ and $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$ we prove, without these results, that no solution (a, b, c) has $10p \mid ab$. Such solutions are close, at each of 2, 5 and p, to one of the trivial solutions $(1, 0, 1)$, $(0, 1, 1)$, which survive every local test. To exclude such solutions we attach to a solution a curve of genus $2(p-1)$ whose Jacobian has multiplication by $\mathbb{Z}[\zeta_5, \zeta_p + \zeta_p^{-1}]$. It belongs to a family of quotients, by an involution, of cyclic covers in a hypergeometric family of the kind used in Darmon's program. The member of this family at the trivial solution is $Y^5 = R^p - 1$, which has complex multiplication, and we compare the 5-adic Tate modules of the two curves one power of $1 - \zeta_5$ at a time. The obstructions to extending this comparison lie in Selmer groups that vanish when $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$, as in Kummer's theorem for regular primes; the local condition at 5 comes from Breuil–Kisin modules over a tamely ramified extension. The generalized Riemann hypothesis is not used.

CONTENTS

1. Introduction 2
2. Frey objects and the case split 8
3. Case (B) with $p \nmid ab$ 12
4. Case (C) 18
5. The quotient curve and the CM point 23
6. The CM point at 5: graded pieces and Selmer groups 34
7. The criterion 44
8. The local conditions at 5 46
9. Proof of the main theorems 63
10. Where the theorem applies 65
11. Remarks and an open question 66
Appendix A. Case (C): the place 2, the primes above 11 and inertia at $\sqrt{5}$ 67
Appendix B. Computations 73
Declarations 75
References 75

Date: October 28, 2026.

2020 *Mathematics Subject Classification.* Primary 11D41; Secondary 11F80, 11R18, 11R29, 11R34, 14L05.

Key words and phrases. Generalized Fermat equation, Frey hyperelliptic curves, real multiplication, Selmer groups, relative class numbers, Breuil–Kisin modules, cyclotomic descent, modular method.

1. Introduction

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

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

and call a triple (a, b, c) of coprime integers with $abc \neq 0$ and $a^p + b^p = c^5$ a *solution*. The triples with $abc = 0$, such as $(1, 0, 1)$ and $(1, -1, 0)$, are the *trivial solutions*, which are not solutions in our sense. For each prime $p \geq 3$ the equation has only finitely many solutions [23, Theorem 2]. For fixed p the equation has been solved for $p = 3$ [11], $p = 5$ (a case of Fermat's Last Theorem) and $p = 7$ [20, Theorem 2], and proofs for $p = 11$ [41, Theorem 7.1] and $p = 13$ [4] have been announced in preprints. The proof for $p = 11$ in the author's earlier paper [41] uses results of [14]. For even exponents, $x^{2n} + y^{2n} = z^5$ has no solution in coprime nonzero integers for every $n \geq 2$ [2]. For the generalized Fermat equation in general, see the surveys [3] and [64], and for Darmon's program [13].

For the whole family, Darmon [21] proposed a program: attach to a solution Frey abelian varieties over $\mathbb{Q}(\zeta_5)^+ = \mathbb{Q}(\sqrt{5})$ with real multiplication, and carry out the modular method with them. Chen and Koutsianas [14] carried out this program with Darmon's two Frey surfaces $J^{\pm}$ over $K = \mathbb{Q}(\sqrt{5})$, using mainly J^-. They proved that for every $n \geq 3$ there is no solution of $x^n + y^n = z^5$ with $2 \nmid ab$ and $5 \mid ab$, nor with $2 \mid ab$ and $5 \nmid ab$ [14, Theorem 1.1], and that, assuming Darmon's conjecture on the image of the residual representations, there is none for p sufficiently large [14, Corollary 1.3]. They describe two obstructions that remain: the irreducibility of the residual representation when $10 \mid ab$, and the Hilbert newforms with complex multiplication that the trivial solutions produce when $2 \nmid ab$, $5 \nmid ab$. Billerey, Chen, Dieulefait and Freitas treat $x^p + y^p = z^r$ with $r \mid ab$, $2 \nmid ab$ and p large when $r \geq 5$ is a regular prime [5]; for $r = 5$ this lies inside the case $2 \nmid ab$, $5 \mid ab$ of the theorem of Chen and Koutsianas. Azon carries out Darmon's program for $Ax^p + By^p = Cz^r$ with coefficients; for example, for $p > 71$ the equation $7x^p + y^p = 3z^5$ has no non-trivial primitive solution with $10 \mid ab$ [1, Theorem 1.1]. Mihăilescu studied $x^p + y^p = z^q$ in $\mathbb{Q}(\zeta_{pq})$ [57]. At $q = 5$ his Theorem 4 states that if $p \geq 7$, $p \not\equiv 1 \pmod 5$ and 5 does not divide the relative class number $h^-(\mathbb{Q}(\zeta_{5p}))$, then every solution has $p \nmid c$, $25 \mid ab$ and $\min(|a|, |b|)$ above an explicit bound, unless $p^4 \equiv 1$ or $(2^{p-1}p^p)^4 \equiv 1 \pmod{25}$; the theorem lists a third exception, $2^4 \equiv 1 \pmod{25}$, which never holds. These solutions are the case his method leaves open [57, §10.2], [3, §2.3]. In earlier work [41, Theorems A and B] we showed, using results of [14], that for every prime $p \geq 11$ no solution has $ab \equiv \pm 2 \pmod 5$, and that every solution has $10 \mid ab$, or $2 \nmid ab$ and $ab \equiv -1 \pmod 5$; the solutions with $2 \nmid ab$ and $5 \nmid ab$ are treated in Section 4, starting from these congruences.

This paper proves a criterion of Kummer's type for the solutions that these methods leave open. For a CM field F let $h^-(F)$ be its relative class number. Let $p \geq 7$ be a prime with $p \not\equiv 1 \pmod 5$ and $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$ (Remark 11.3 lists the steps that use $p \not\equiv 1 \pmod 5$). In a solution with $10p \mid ab$, each of 2, 5 and p divides a or b, so at each of these primes the solution is close to one of the trivial solutions $(1, 0, 1)$, $(0, 1, 1)$. We exclude the solutions with $10p \mid ab$ by an argument that uses no result of [14], and in which, as in Kummer's theorem for regular primes, the equation becomes a condition on a class number (Theorem 1.2). With results of [14] for the other solutions, the equation then has no solution for these primes when $p \geq 13$ (Theorem 1.1). In the case that Mihăilescu's method leaves open, Theorem 1.2 excludes the solutions with $2p \mid ab$, and Theorem 1.1 excludes all of them for $p \geq 13$, with no condition modulo 25. Darmon used the regularity of r in a similar way for $x^p + y^p = z^r$: if r is a regular prime, then for p larger than a constant depending only on r, and for every

solution with $r \mid ab$ (a first case solution), the mod-$\mathfrak{p}$ representation of his Frey variety $J_r^+(a,b,c)$, for a prime $\mathfrak{p} \mid p$ of $\mathbb{Q}(\zeta_r)^+$, is reducible. The argument excludes the $\mathfrak{r}$-Eisenstein $\mathbb{Q}$-forms of level 1 or $\mathfrak{r}$, where $\mathfrak{r}$ is the prime of $\mathbb{Q}(\zeta_r)^+$ above r, since they would yield an unramified cyclic extension of $\mathbb{Q}(\zeta_r)$ of degree r, which does not exist when r is regular [21, Definitions 3.6 and 3.17, Propositions 3.19 and 3.20, Lemma 3.21 and Theorem 3.22].

Zhou, by inter-universal Teichmüller theory [77, Theorem A], and Mihăilescu, by cyclotomic methods [58, Theorem 1], have announced in preprints results that would cover (1.1) for every p (Mihăilescu's for every $p \geq 7$). The results of this paper depend neither on them nor on [4].

1.1. **Results.** For a solution, either exactly one of $2, 5$ divides abc, or neither does, or $10 \mid abc$. In Section 2.3 we say that a solution is in *case (C)* if $2 \nmid abc$ and $5 \nmid abc$, and, when $10 \mid abc$, in *case (A)* or *case (B)* according as the representation of G_K on $J^-[\mathfrak{p}]$ is irreducible for some prime $\mathfrak{p} \mid p$ of K or for none; a solution is in *class (d)* if $10p$ divides one of a, b (the other solutions with $10p \mid abc$, in which 2, 5 and p do not all divide the same variable, form the classes (a)–(c) of Section 2.3). Table 1 below shows where each kind of solution is treated.

TABLE 1. Where the solutions are treated, for $p \geq 13$ with $p \not\equiv 1 \pmod 5$, with (a,b,c) a solution. Rows 1–4 use the results of [14] listed in Table 2; row 5 uses no result of [14].

solutions	conclusion	reference
exactly one of $2, 5$ divides abc	none	[14, Theorem 1.1]
$2 \nmid abc$, $5 \nmid abc$ (case (C))	none if $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$	Theorem 4.1
$10 \mid abc$, $p \nmid abc$, $p \equiv \pm 2 \pmod 5$	none	Theorem 3.8
$10 \mid abc$, $p \nmid abc$, $p \equiv -1 \pmod 5$	none	Propositions 2.3, 3.9 and 3.10
$10p \mid abc$	none if $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$	Theorem 9.2

The proof of Theorem 1.1 uses the results of [14] listed in Table 2 as (CK1)–(CK4); Lemma 2.1 extracts the precise ranges needed from [14, §§9.3, 10]. What Theorem 1.1 takes from the author's earlier paper [41] is proved here (Proposition 2.4, Appendix A). The paper [14] is to appear in Algebra & Number Theory, and we use its arXiv version 2. Level lowering for Hilbert modular forms over K rests here, as in [14] and [33], partly on Fujiwara's unpublished preprint [34]. Apart from the existence of crystalline characters with prescribed weights, a standard fact for which we cite Conrad's preprint [19], no other unrefereed result is used in this paper. The generalized Riemann hypothesis is not used.

Theorem 1.1. *Let $p \geq 13$ be a prime with $p \not\equiv 1 \pmod 5$ and $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$. Then the equation $x^p + y^p = z^5$ has no solution.*

For $p \equiv \pm 2 \pmod 5$ the proof uses only (CK1), the results of [14] on J^+ and those for case (C) listed in (CK4) (Theorem 9.3). The bound $p \geq 13$ comes only from case (C), where Proposition 4.4 needs $p \geq 11$, and $11 \equiv 1 \pmod 5$; at $p = 7$ the solutions of case (C) with $5 \nmid c$ remain, and the equation $x^7 + y^7 = z^5$ was solved by Dahmen and Siksek [20] (Remark 9.4). The class-number condition in Theorem 1.1 is decided by generalized Bernoulli numbers, as Kummer's is: $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$ if and only if no $B_{1,\chi}$, for χ an odd Dirichlet character of conductor p or $5p$, lies in a fixed prime above 5 of $\mathbb{Q}(\mu_{4(p-1)})$ (Appendix B, (C1)). The hypotheses hold at 41 primes $13 \leq p < 1000$, the four smallest being 13, 19, 23,

29 (for $p = 13$ see [4, Theorem 1.1]), and at 2432 primes $13 \le p < 10^5$ (Section 10). We do not know whether infinitely many primes satisfy these hypotheses. The corresponding question for regular primes is open (Jensen proved that infinitely many primes are irregular; see [75, Theorem 5.17]).

The solutions with $10p \mid ab$ are excluded by the argument of Sections 5 to 9, which uses no result of [14].

Theorem 1.2. *Let $p \ge 7$ be a prime with $p \not\equiv 1 \pmod 5$ and $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$. Then no solution (a, b, c) has $10p \mid ab$.*

Theorem 1.1 is Theorem 9.3, and Theorem 1.2 is Theorem 9.2.

1.2. **The idea.** Table 1 shows the shape of the proof of Theorem 1.1. Every row but the last is treated by the modular method with Darmon's two Frey surfaces and classical cyclotomic arithmetic. The trivial solution $(1, 0, 1)$ has $b = 0$, so it satisfies the condition $10p \mid ab$ of the last row, and that row needs another argument, the main point of this paper. In outline: to a solution with $10p \mid b$ we attach a curve of genus $2(p-1)$ whose Jacobian has multiplication by the ring of integers of $M' = \mathbb{Q}(\zeta_5, \zeta_p + \zeta_p^{-1})$, a subfield of index 2 of $M = \mathbb{Q}(\zeta_{5p})$, and which at 2, 5 and p is a deformation of a curve with complex multiplication coming from the trivial solution. We compare the 5-adic Tate modules of the two Jacobians one power of $\varpi = 1 - \zeta_5$ at a time. Each obstruction to improving the comparison is a class in one of two Selmer groups over K, with coefficients induced from characters of $L = \mathbb{Q}(\sqrt{5}, \zeta_p)$ and of $L^+ = \mathbb{Q}(\sqrt{5}, \zeta_p + \zeta_p^{-1})$: $\mathrm{Sel}(W)$, of the classes unramified away from 5 that at 5 come from a Bloch–Kato subgroup, and $\mathrm{Sel}(\Theta)$, of the classes unramified everywhere. By class field theory and reflection they vanish when the minus parts of the 5-class groups of M' and L do, that is, when $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$, as $h^-(\mathbb{Q}(\zeta_{5p})) = h^-(L)h^-(M')$ up to a power of 2 (Corollary 6.14). The comparison can then be improved at every power of ϖ, and the two Tate modules are isomorphic as G_K-modules; but at a prime above a prime dividing $(a^p + b^p)/(a + b)$, Frobenius has an eigenvalue in $\mathbb{Q}(\zeta_5)$ on the first Jacobian and none on the second (Proposition 5.11). The hard step is the local condition at 5, where the ramification is too large for finite flat models to be unique. We describe the steps in turn.

A quotient of a hypergeometric cover, and a comparison with the trivial solution. The hypergeometric family of cyclic covers $y^{5p} = x^{3p+5}(1-x)^{2p}(1-tx)^{3p-5}$ (hypergeometric in the sense of Cohen and Wolfart [18, §3.3]) has local monodromies of orders p, p and, projectively, 5 at $t = 0, 1, \infty$, and its monodromy is that of the triangle group of signature $(p, p, 5)$. We call the fiber at $t = a^p/c^5$ of a family with these local monodromies, or a quadratic twist of it, a *Frey object* for (1.1), after Darmon's Frey representations [21, Definition 1.1], whose local monodromies at 0, 1, ∞ have, projectively, the orders p, q, r for $x^p + y^q = z^r$. The exponents are also chosen so that the involution $x \mapsto (tx - 1)/(t(x - 1))$ of the line lifts to the cover. The lift is defined only over $\mathbb{Q}(t)$ with a p-th root of $t(1 - t)$ adjoined, and after a twist by the Kummer character of $(t(1 - t))^{(p+1)/2p}$ one of its conjugates under μ_p is defined over $\mathbb{Q}(t)$ (Section 5.2). In the parameter u with $t = 1/(1 + u^p)$, the quotient by the lift is the curve

$$D_u \colon Y^5 = (1 + u^p)^4 \prod_{j \in \mathbb{Z}/p} (R - \zeta_p^j + u\zeta_p^{-j})$$

of genus $2(p-1)$, whose Jacobian has multiplication by the ring of integers of M' (Section 5). At $u = 0$ it is $Y^5 = R^p - 1$, with complex multiplication by $\mathbb{Q}(\zeta_{5p})$: the CM point, coming from the trivial solution. At a solution with $10p \mid b$ we take $u = b/a$, which is divisible by 2, 5 and p, and write D_{sol} for $D_{b/a}$, which is the cyclic quintic cover of the line branched at the

points $a\zeta_p^j - b\zeta_p^{-j}$ (Proposition 5.1(d)). At each of 2, 5 and p the curve D_{sol} is a deformation of the CM point, and the 5-adic Tate modules T' of $\operatorname{Jac} D_{\mathrm{sol}}$ and T_0 of $\operatorname{Jac} D_0$ agree modulo ϖ by a canonical isomorphism, the residual identification ι_{can}: the points of order ϖ are the classes of the divisors of degree 0 supported on the branch points (Lemma 5.2).

An induction on the power of ϖ. We try to make T' and T_0 isomorphic one power of ϖ at a time. An isometry $T' \to T_0$ (for the skew-Hermitian forms whose traces are the Weil pairings) inducing ι_{can} has *depth* D if it is Galois-equivariant modulo ϖ^D but not modulo ϖ^{D+1}. Its failure modulo ϖ^{D+1}, the *leading digit*, is a cohomology class of G_K with values in a graded piece of the adjoint of T_0. This piece depends only on the parity of D, as multiplication by $\sqrt{5}$, a unit times ϖ^2, identifies the pieces in depths D and $D+2$: for odd D the module $W = \operatorname{Ind}_{G_L}^{G_K} \mu_5$, and for even D the module $\Theta = \operatorname{Ind}_{G_{L^+}}^{G_K} \mathbb{F}_5(\chi_{L/L^+})$ induced from the quadratic character of L/L^+ (Proposition 6.4). The class is unramified away from 5 and p, as $\operatorname{Jac} D_{\mathrm{sol}}$ has good reduction there, also at 2 and at the primes dividing c (Proposition 5.6 and Lemma 5.7). At p it is unramified because there the 5-adic Tate modules of the two Jacobians are isomorphic, compatibly with the Weil pairings (Proposition 5.5). Only the existence of this local isomorphism is used, not its reduction modulo ϖ, which need not be ι_{can}. So the argument also runs when 2, 5 and p divide different variables: when $p \mid a$, the symmetry $(R, Y) \mapsto (-R, -Y)$ between the quotient curves attached to (a, b) and to (b, a) provides the isomorphism at p (Section 9.1). At 5 the class lies in the Bloch–Kato subgroup, because the comparison is induced by finite flat models (Section 8). So it lies in a Selmer group, and if the Selmer groups vanish the induction never stops (Theorem 7.2). The Selmer groups are computed in Section 6. The one of Θ is dual to the minus part of the 5-class group of L. When that vanishes, the one of W consists of the classes $x \in L^\times/L^{\times 5}$ that are fixed by complex conjugation, have $v_w(x) \equiv 0 \pmod 5$ at every prime $w \nmid 5$ of L and are fifth powers at every prime above 5; by reflection, it has the dimension of the minus part of the 5-class group of M'. When the order $f = \operatorname{ord}_p 5$ of 5 modulo p is odd, complex conjugation moves the primes above 5, and the computation then needs an argument on valuations through the Kummer tower obtained by adjoining the 5-power roots of a uniformizer (Section 6.8). This is the step in which, as for Kummer's regular primes, the equation becomes a class-number condition.

The end of the induction. If the induction never stops, $T' \cong T_0$ as Galois modules. A prime ℓ dividing $(a^p + b^p)/(a + b)$, which exists because $b \neq 0$, then gives a contradiction. Such an ℓ divides c, and at a prime $\lambda \mid \ell$ of $\mathbb{Q}(\zeta_{5p})$ the cover of which D_{sol} is a quotient has a semistable model whose special fiber contains p curves $Y^5 = \bar{z}W^6(1-W)^2$ of genus 2, one for each root $\bar{z}$ of $\bar{z}^p = \bar{a}^{p(3p-5)}$ in the residue field, with complex multiplication by $\mathbb{Q}(\zeta_5)$ (Proposition 5.6; at a solution the cover is $y^{5p} = x^{3p+5}(1-x)^{2p}(c^5 - a^p x)^{3p-5}$, whose right side is $\equiv a^{p(3p-5)}(x^6(1-x)^2)^p$ modulo ℓ, as $\ell \mid c$). So the Frobenius at λ on $\operatorname{Jac} D_{\mathrm{sol}}$ has an eigenvalue in $\mathbb{Q}(\zeta_5)$, while by Stickelberger's theorem no Frobenius eigenvalue of D_0, a Jacobi sum, lies in $\mathbb{Q}(\zeta_5)$ (Proposition 5.11). The trivial solution has $b = 0$ and survives every local test. Only this global step, which uses $b \neq 0$, separates a solution from it.

The local condition at 5. The CM point has good reduction over the tame extension $\tilde{F} = \mathbb{Q}_{5^f}(\nu)$, $\nu = (-5)^{1/4p}$, whose ramification index $4p$ is far beyond the range in which finite flat models are unique ($e < 4$, [65, Théorème 3.3.3]). Over $\tilde{F}$ all the curves D_u with $v_5(u) > 5/(2p)$ have smooth models with one and the same special fiber (Section 8.1). At every solution with $10p \mid ab$, labeled so that $5 \mid b$, $u = b/a$ has $v_5(u) \geq 2$, by a Stickelberger argument (Lemma 8.2), and this is enough to place D_u and D_0 in one family over the power-series ring $\mathcal{O}_{\tilde{F}}[[z]]$, z a new variable, at the parameters $z = \nu^{5p+1}$ and $z = 0$. The

exponent $5p+1$ is the least integer above Fontaine's ramification bound $5e/4 = 5p$ for group schemes killed by 5, with $e = 4p$ [29, Théorème A], and this is what the specialization lemma needs (Lemma 8.4 and Remark 8.6). Lau's classification of finite flat group schemes over $\mathcal{O}_{\tilde{F}}[[z]]$ and a rigidity lemma for Breuil–Kisin modules then identify their 5-torsion group schemes (Proposition 8.5). A rigidity statement for the residual Breuil–Kisin module of the CM point (Lemma 8.10) propagates this identification to every depth, and Kisin's theory turns the leading digit into a crystalline class (Theorem 8.12). The leading digit has a *diagonal part*, its component in $\mathcal{O}_M$, which acts on T_0 through the complex multiplication, and an off-diagonal part, the complementary component; at even depths only the diagonal part occurs. For f even, Kisin's theory shows that, at even depths from 4 on, the class of the diagonal part vanishes at 5 (Theorem 8.12(ii)); at depth 2, for either parity of f, the identification of the 5-torsion group schemes already makes it vanish (Lemma 7.1). When f is odd, the primes of M' above 5 split in M, and the argument at even depths from 4 on shows that the class is unramified at 5, which is all that $\mathrm{Sel}(\Theta)$ asks (Theorem 8.15).

The other solutions. In case (C) a Stickelberger argument in $\mathbb{Q}(\zeta_p)$, of the kind Mihăilescu used for Catalan's equation [56], shows $a \equiv b \pmod{25}$ when $5 \nmid c$, which contradicts the conductor exponent 3 of J^- at $\sqrt{5}$ (Theorem A.9, after [41]), as it would make that exponent 2 (Proposition 4.4); this branch needs no class number. The branch $5 \mid c$ is excluded by Mihăilescu's descent in $\mathbb{Q}(\zeta_{5p})$, which needs $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$ (Section 4). For $10 \mid ab$, $p \nmid ab$ and inert p, Darmon's second Frey surface J^+ is modular and its residual representation reducible. Its trace of Frobenius at p is then $\pm 1 \pm p$, being $\equiv \pm 1 \pmod{p}$, even and at most $2p$ in absolute value (Lemma 3.7), while its $\sqrt{5}$-torsion forces the trace to be divisible by 5 (Theorem 3.8). At split p, case (A) is excluded by (CK2) and (CK3) (Proposition 2.3). In case (B) the reducible representation of J^- constrains the traces of Frobenius at the primes above p, and the 2-torsion of Darmon's family $C(t)$ of genus-2 curves (of whose Jacobians J^- is a quadratic twist) and a comparison at 11, the least prime that splits completely in $\mathbb{Q}(\zeta_5)$, exclude the values it allows; a finite computation treats $p = 19$ and 79, the primes of the form $20k^2 - 1$ below 144: the traces that remain, $2k\sqrt{5}$ with $k \in \mathbb{Z}$, force $p = 20k^2 - 1$, and the comparison at 11, where the traces are $\equiv \pm(11+1)$ modulo $\mathfrak{p}$, needs $p > (11+1)^2 = 144$ (Section 3.3).

1.3. **Relation to earlier work.** The Frey surfaces $J^\pm$, the reducibility of the residual representation of J^+ when $5 \mid ab$ and the passage from a reducible residual representation to a rational point of order p (Proposition 2.4) are Darmon's [21]; the conductors and the elimination step are Chen and Koutsianas's [14]. The Jacobians of the cyclic covers behind D_u contain, up to isogeny, hypergeometric abelian varieties in the sense of Cohen and Wolfart [18, §3.3], of the kind Darmon used to construct Frey representations attached to triangle groups [21, §1]; for signature (p, p, r) Golfieri Madriaga and Pacetti realize them as hypergeometric motives [37, Definition 1.1], and the appendix by Pacetti and Rodriguez Villegas matches these motives with Darmon's curves, up to a quadratic twist [37, Corollaries A.5 and A.11]. Quotients of such covers by an involution that inverts part of the action of the roots of unity appear in work of Tautz, Top and Verberkmoes [71, §2] and of Darmon [21, pp. 422–423], and Golfieri Madriaga, Pacetti and Rodriguez Villegas construct them for a class of Euler's curves [38, §9], the curves $y^N = x^A(1-x)^B(1-zx)^C z^D$ of [38, Definition 8.2]. On the coordinate x our involution is the involution [38, (75)]. The curve D_{sol} is the cyclic quintic cover of the line branched at the points $a\zeta_p^j - b\zeta_p^{-j}$, the branch points of Kraus's hyperelliptic Frey curve [47, §V], [6, §3]. What we add is the model D_u and the comparison of its 5-adic Tate module with that of the CM point, one power of

$1-\zeta_5$ at a time. The cyclotomic descent in the branch $5 \mid c$ is Mihăilescu's [57]: a solution gives an equation $X^5 + Y^5 = \varepsilon(\zeta_5 - \zeta_5^{-1})^N(\zeta_p - \zeta_p^{-1})^M Z^5$ in the integers of L^+, with ε a unit and integers N, M (Theorem 4.5), and writing the factors $\zeta_5^i X + \zeta_5^{-i} Y$ of $X^5 + Y^5$, normalized, as units times fifth powers gives another such equation with fewer prime factors of Z. Our proof follows his and completes it at three points (Section 4.2): the case in which X or Y is a unit, the units in these factors, and, in the passage from a solution to the first such equation, the field in which the factors are written as units times fifth powers. At 5 we use Kisin's theory of Breuil–Kisin modules [43, 44], Lau's classification over complete regular local rings [50, 51], and a rigidity lemma that is a special case of [12, Lemma 3.1.10]. We know of no reference for the specialization lemma (Lemma 8.4) in the form we use, an isomorphism of models natural in a family over $\mathcal{O}_{\tilde{F}}[[z]]$. For the 5-torsion of abelian schemes its conclusion on points also follows from Fontaine's lifting lemma [29, Proposition 1.7]. The Selmer-group computations use the Greenberg–Wiles formula [22, Theorem 2.19] and the dimension formula of Bloch and Kato [8]. They describe the Selmer groups of the graded pieces, which are induced from characters of L and of L^+, by class groups and units of L and M', through Kummer theory and the argument behind Leopoldt's reflection theorem [53], [75, §10.2].

Two other ways around a trivial solution are closest to ours. The symplectic method decides, by local information at a prime $\ell \neq p$, whether an isomorphism $E[p] \cong E'[p]$ of elliptic curves over $\mathbb{Q}$ can be chosen to preserve the Weil pairing [32]. Darmon and Merel show that for $x^n + y^n = 2z^n$ and $x^n + y^n = z^2$ the mod-p representation of the Frey curve is that of the curve of a trivial solution, with image the normalizer of a Cartan subgroup, and exclude the non-split case through rational points on modular curves and the winding quotient [24, Proposition 4.1 and Theorem 8.1]. Both work with residual representations modulo p; we compare instead the 5-adic Tate modules of D_{sol} and of the CM point D_0, one power of $1-\zeta_5$ at a time, and every obstruction lies in a Selmer group.

1.4. **Plan.** We prove Theorems 1.1 and 1.2. Section 2 fixes the Frey objects, lists the results of [14] we use, and divides the solutions into cases. Section 3 treats case (B) with $p \nmid ab$ and Section 4 treats case (C). Sections 5, 6, 7 and 8 treat class (d), with no input from Sections 2, 3 and 4 beyond the case split of Section 2.3 and Lemma 4.3, and Section 5 opens with an outline of that argument. Section 9 assembles the proofs and Section 10 gives the counts. Section 11 discusses the limits of the method. Appendix A treats case (C) at 2, at the primes above 11 and at $\sqrt{5}$, and Appendix B lists the computations; the programs and their outputs are in [42].

1.5. **Notation.**

K, $\mathcal{O}_K$, σ, ϕ	$\mathbb{Q}(\sqrt{5})$, its integers, its nontrivial automorphism, $(1+\sqrt{5})/2$ (in Sections 6 and 8 ϕ is also the Frobenius of Breuil–Kisin modules)
$\mathfrak{q}_2$, $\mathfrak{q}_5$, $\mathfrak{p}$, $D_{\mathfrak{q}_5}$	the primes of K above 2, 5, and a prime above p; a decomposition group at $\mathfrak{q}_5$
f, g	the order of 5 in $(\mathbb{Z}/p)^\times$, and $(p-1)/f$
M, M', L, L^+	$\mathbb{Q}(\zeta_{5p})$, $\mathbb{Q}(\zeta_5, \zeta_p + \zeta_p^{-1})$, $\mathbb{Q}(\sqrt{5}, \zeta_p)$, $\mathbb{Q}(\sqrt{5}, \zeta_p + \zeta_p^{-1})$ (Section 4.2 also has the fields L_{pq}, L_p, L^{++})
c, σ_m, ϖ	complex conjugation, the generator of $\mathrm{Gal}(M/M')$ ($m \equiv 1 \pmod 5$, $m \equiv -1 \pmod p$), $1-\zeta_5$

J^-, J, η, J^+	Darmon's Frey Jacobian (as in [14]), its twist $J^- \otimes \eta$ (Proposition 2.4), Darmon's J^+
C', D_u, D_0, D_{sol}	the twisted cyclic cover, its quotient, the CM point, the quotient at a solution
T', T_0, ι_{can}	5-adic Tate modules of $\operatorname{Jac} D_{\mathrm{sol}}$, $\operatorname{Jac} D_0$, and the residual identification between them modulo ϖ
$\mathcal{O}$, λ', $\mathfrak{a}$, h', h_0	$\mathcal{O}_{M',\lambda'}$ for a prime λ' of M' above 5, its inverse different, and the skew-Hermitian forms on T', T_0 whose traces are the Weil pairings (Section 5.9)
$\mathrm{ad}^{\mathrm{pol}}$, $\mathcal{T}$, W, Θ	the polarized adjoint (the trace-zero $\mathcal{O}_{M'}$-linear endomorphisms of T_0 that are skew for its skew-Hermitian form), its off-diagonal module ($\mathcal{T}\sigma_m$ is its component in $\mathcal{O}_M\sigma_m$), the graded pieces
ψ, Ψ, $\Psi^\flat$	the CM character of D_0, $\psi/(\sigma_m \circ \psi)$, and its extension to G_L
$\mathrm{Sel}(W)$, $\mathrm{Sel}(\Theta)$, $\mathcal{L}_5$, G	the Selmer groups of Definition 6.5 (the classes unramified away from 5 that lie in $\mathcal{L}_5$ at 5, resp. the classes unramified everywhere), the local condition at 5 of $\mathrm{Sel}(W)$ (the image of the Bloch–Kato subgroup $H^1_f(K_5, \mathcal{T})$, $K_5 = K_{\mathfrak{q}_5}$), and the group of the $x \in L^\times/L^{\times 5}$ with $v_w(x) \equiv 0 \pmod 5$ at every prime $w \nmid 5$ of L (Section 6.4)
Art	for a local field F, reciprocity $F^\times \to G_F^{\mathrm{ab}}$, normalized so that a uniformizer maps to arithmetic Frobenius in the unramified quotient; the local pairing is $(x, h) = h(\mathrm{Art}(x))$
depth, leading digit	of an isometry $\varphi\colon T' \to T_0$ with difference cocycle $X(g) = \varphi\rho'(g)\varphi^{-1}\rho_0(g)^{-1} - 1$, ρ' and ρ_0 the actions of G_K: the largest D with $X \equiv 0 \pmod{\varpi^D}$, and, if φ is normalized ($\det(1+X) = 1$) and $D \geq 1$, the class of X in $\mathrm{gr}^D \mathrm{ad}^{\mathrm{pol}}$ (Section 7.1)
$\tilde{F}$, ν	$\mathbb{Q}_{5^f}((-5)^{1/4p})$, its uniformizer $(-5)^{1/4p}$
$[P]$	1 if the statement P holds, and 0 otherwise

2. Frey objects and the case split

This section fixes Darmon's Frey Jacobian J^- in the normalization of Chen and Koutsianas [14, Lemma 5.5], lists the results of [14] that the proof uses, and divides the solutions into the cases and classes that Sections 3, 4, 5, 6, 7, 8 and 9 treat. Its two propositions are taken from [14] and, with a complete proof, from the author's earlier paper [41].

2.1. **Solutions and the Frey Jacobian.** Let p be an odd prime. A *solution* is a triple (a, b, c) of coprime integers with $a^p + b^p = c^5$ and $abc \neq 0$. A prime dividing two of a, b, c divides the third, so a, b, c are pairwise coprime. The maps $(a, b, c) \mapsto (b, a, c)$ and $(a, b, c) \mapsto (-a, -b, -c)$ permute the solutions.

Let $K = \mathbb{Q}(\sqrt{5})$, with ring of integers $\mathcal{O}_K$, nontrivial automorphism σ and fundamental unit $\phi = (1 + \sqrt{5})/2$. The prime 2 is inert in K and 5 ramifies. We write $\mathfrak{q}_2 = (2)$ and $\mathfrak{q}_5 = (\sqrt{5})$, and $\mathfrak{p}$ for a prime of K above p. The prime p splits in K if $p \equiv \pm 1 \pmod 5$ and is inert if $p \equiv \pm 2 \pmod 5$. Following [14, Lemma 5.5], the *Frey curve* of a solution is

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

a curve of genus 2 over $\mathbb{Q}$, and $J^- = \operatorname{Jac} C^-$. By [14, Theorem 5.4] and [71, Theorem 1 and §3.1], $\mathcal{O}_K$ acts on J^- by endomorphisms defined over K, the element $\zeta_5 + \zeta_5^{-1}$ acting by the correspondence of Tautz, Top and Verberkmoes. For a prime $\mathfrak{p} \mid p$ of K we write $\bar\rho_{J^-,\mathfrak{p}}$ for the representation of G_K on $J^-[\mathfrak{p}]$, a 2-dimensional vector space over $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$; whether it is irreducible does not change under the symmetries of the solutions, which twist J^- by -1. Frobenius elements are arithmetic. For a prime ℓ, χ_ℓ is the ℓ-adic cyclotomic character, and χ_p also denotes its reduction modulo p, the mod-p cyclotomic character.

2.2. **The inputs from [14].** We cite [14], which is to appear in Algebra & Number Theory, by the statement numbers of its version arXiv:2210.02316v2. We use no result of the author's earlier paper [41] without proof: Proposition 2.4 and Appendix A prove what we take from it. Let $K(S_2, 2) \subseteq K^\times/K^{\times 2}$ be the group of classes Δ with $v_\mathfrak{q}(\Delta)$ even at every prime $\mathfrak{q} \neq \mathfrak{q}_2$, and $K(S_2,2)^*$ the group of quadratic characters of G_K that they define, which is $\langle -1, \phi, 2\rangle$, of order 8. Table 2 lists what we take from [14]. In (CK2), where $\bar\rho_{J^-,\mathfrak{p}}$ is twisted by a character $\chi_0 \in K(S_2,2)^*$, [14, Theorem 7.1(2)] assumes $2 \mid a$ and $b \equiv -1 \pmod 4$, which the symmetries of the solutions allow: they change χ_0 by the character of -1.

Of the results of [14], only [14, Theorem 1.2 and Corollary 1.3] are stated for p sufficiently large; for the first the bound is explicit in its proof. The proof of [14, Theorem 1.2], in [14, §10] (pp. 29–30), begins "As before, we may assume that $n = p \geq 11$ is a prime"; it contains (CK3) and the last part of (CK4), which we restate with their exceptions.

Lemma 2.1 ([14, §§9.3, 10])**.** *Let $p \geq 11$ be prime and $\mathfrak{p} \mid p$ a prime of K.*

(a) Let (a,b,c) be a solution with $10 \mid ab$, $2 \mid a$ and $b \equiv -1 \pmod 4$, and χ_0 as in (CK2). If $\bar\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ is irreducible, it is isomorphic to $\bar\rho_{g,\mathfrak{B}}$ for one of the two newforms g of parallel weight 2 and level (10) and a prime $\mathfrak{B} \mid p$ of the coefficient field of g. For $p \notin \{2,3,5,7\}$ no such isomorphism holds, for any $\chi_0 \in K(S_2,2)^*$ and any $\mathfrak{p} \mid p$.

(b) Let (a,b,c) be a solution with $2 \nmid ab$, $5 \nmid ab$, $2 \mid c$ and $a \equiv -1 \pmod 4$, and let $p \neq 19$. Let $\varepsilon \in \{2,3\}$ be the conductor exponent at $\mathfrak{q}_5$ of the $\mathfrak{l}$-adic representation $\rho_{J^-,\mathfrak{l}}$ of G_K on $T_\ell(J^-) \otimes_{\mathcal{O}_K \otimes \mathbb{Z}_\ell} \mathcal{O}_{K,\mathfrak{l}}$, for any prime $\mathfrak{l} \nmid 5$ of K [14, Proposition 7.24]. Then $\bar\rho_{J^-,\mathfrak{p}} \otimes \chi_0 \cong \bar\rho_{g,\mathfrak{B}}$ for some $\chi_0 \in K(S_2,2)^*$, a prime $\mathfrak{B} \mid p$ of the coefficient field of g, and a newform g of parallel weight 2, trivial character and level $\mathfrak{q}_2^2\mathfrak{q}_5^\varepsilon$ which is attached to J_1 if $\varepsilon = 2$ and to one of J_4, J_{16}, J_{64} if $\varepsilon = 3$. Here J_D is the Jacobian of $y^2 = x^5 + D$; J_1 is also the quadratic twist by $K(\sqrt{2})/K$ of the Jacobian of $y^2 = x^5 + 32$, which is C^- with $a^p = -8$, $b^p = 8$ and $c = 0$.

Proof. In both cases J^- is modular and its $\mathfrak{p}$-adic representation $\rho_{J^-,\mathfrak{p}}$ has determinant χ_p [14, Theorem 6.6, Lemma 6.3], and for the χ_0 of [14, Theorem 7.1(2)] the Serre level of $\bar\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ is $\mathfrak{q}_2^s\mathfrak{q}_5^\varepsilon$, with $s \leq 1$ and $\varepsilon = 2$ in (a) and $s \leq 2$ in (b), the exponent at $\mathfrak{q}_5$ being that of $\rho_{J^-,\mathfrak{l}} \otimes \chi_0$ [14, §7.3]; in (b) the representation is irreducible [14, Theorem 8.7]. Level lowering [14, §9.2], made prime by prime and keeping $\mathfrak{q}_2$ in the level (the remark after [14, (9.8)]), gives g of level $\mathfrak{q}_2\mathfrak{q}_5^\varepsilon$ or $\mathfrak{q}_2^2\mathfrak{q}_5^\varepsilon$. The comparison of traces at the primes above 3, 7 and 11 tests whether p divides the norm, from the coefficient field of g to $\mathbb{Q}$, of the number $T(g,\mathfrak{q})$ of [14, §9.3], a product of $N\mathfrak{q}$, of $a_\mathfrak{q}(g)^2 - (N\mathfrak{q}+1)^2$ and of norms to $\mathbb{Q}$ of differences between $a_\mathfrak{q}(g)$ and the Galois conjugates of traces of Frobenius [14, (9.4), (9.9), (9.10)]; no factor involves $\mathfrak{p}$, so the test does not depend on $\mathfrak{p}$. It is made "for all choices of χ_0" and removes every newform of level $\mathfrak{q}_2\mathfrak{q}_5^\varepsilon$ for $p \notin \{2,3,5,7\}$ [14, §9.3] (p. 29). This gives (a), which is the first case of [14, §10]. In the second case of [14, §10] it removes every newform of level $\mathfrak{q}_2^2\mathfrak{q}_5^\varepsilon$ except four for $p \notin \{2,3,5,19\}$: one of level $\mathfrak{q}_2^2\mathfrak{q}_5^2$, attached to J_1 (2.2.5.1-400.1-b in [72]), and three of level $\mathfrak{q}_2^2\mathfrak{q}_5^3$, attached to J_4, J_{16}, J_{64} (2.2.5.1-2000.1-e, -d, -b), the Jacobians

of the curves C^- with $c = 0$ and $a^p = -b^p = -1, -4, -16$. ([14, §10] writes these four as $J^-(-8, 8, 0) \otimes \chi_2$, with χ_2 there the character of $K(\sqrt{2})/K$, $J^-(-1, 1, 0)$, $J^-(-4, 4, 0)$ and $J^-(-16, 16, 0)$, with a^p, b^p in the place of a, b.) As the level of g has $\mathfrak{q}_5$-exponent ε, this gives (b). The only conditions on p used are $p \geq 11$ and the exceptions listed, which come from the comparisons of traces. □

TABLE 2. The results of [14] that the proofs use. Here (a, b, c) is a solution, $\mathfrak{p} \mid p$ a prime of K, $\chi_0 \in K(S_2, 2)^*$, and the last column gives the primes p at which the result is used.

	result	used in	p
(CK1)	[14, Theorem 1.1]: for $n \geq 3$, the equation $x^n + y^n = z^5$ has no solution with $2 \nmid ab$ and $5 \mid ab$, nor with $2 \mid ab$ and $5 \nmid ab$.	Table 1, Lemma 2.2 and Theorem 9.3	all
(CK2)	[14, Theorem 6.6, Lemma 6.3, Theorem 7.1(2), §7.3]: J^- is modular, and if $10 \mid ab$ and $p \geq 11$, then for some χ_0 the representation $\bar{\rho}' = \bar{\rho}_{J^-,\mathfrak{p}} \otimes \chi_0$ has Serre level $\mathfrak{q}_2^s\mathfrak{q}_5^2$ with $s \leq 1$, is finite at every prime of K above p, and has determinant χ_p.	Propositions 2.3, 2.4, 3.9 and 3.10	≥ 11
(CK3)	[14, §10, first case, with §9.3]: if $10 \mid ab$, $p \geq 11$ and $\bar{\rho}'$ is irreducible, then level lowering for Hilbert modular forms [14, §9.2] gives $\bar{\rho}' \cong \bar{\rho}_{g,\mathfrak{B}}$ for one of the two newforms g of parallel weight 2 and level $\mathfrak{q}_2\mathfrak{q}_5^2 = (10)$ and a prime $\mathfrak{B} \mid p$ of the coefficient field of g, and the comparison of traces of [14, §9.3] at the primes above 3, 7 and 11, made there for every $\chi_0 \in K(S_2, 2)^*$ and, through the norm [14, (9.4)], for every $\mathfrak{p} \mid p$, excludes both for every $p \notin \{2, 3, 5, 7\}$.	Proposition 2.3	≥ 11
(CK4)	[14, Theorem 5.4, Lemma 5.5(2), Lemma 6.3, Theorem 6.4, the proof of Proposition 6.5, Lemmas 7.5 and 7.6 and their proofs, (7.1), (7.2), (7.5), (7.8), and §9.2], used in Section 3; [14, Corollary 8.5, with the proof of Proposition 8.4], used in Proposition 2.4 (the unit and ray class group calculations are also in the proofs of [14, Theorems 8.6 and 8.7]); and, for case (C), the results of [14] that Appendix A uses: [14, Propositions 7.23 and 7.24, and the model in the proof of Proposition 7.23] (the reduction of J^- at $\mathfrak{q}_5$ when $5 \nmid ab$), and, when $2 \nmid ab$ and $5 \nmid ab$, [14, Lemma 6.3, Lemma 7.5 and its proof, Theorems 6.6, 7.1(2), 7.9 and 8.7, §7.3] (determinant, multiplicative, hence purely toric, reduction at the primes dividing ab away from 10, modularity, conductor, Serre level and irreducibility) and the case $2 \nmid ab$, $5 \nmid ab$ of the proof of [14, Theorem 1.2] in [14, §§9.3, 10] (level lowering, as cited in [14, §9.2], and the comparison of traces).	Proposition 2.4, Section 3; Lemma 4.2 and Proposition 4.4, Appendix A	≥ 7; ≥ 13

The other results of [14] that we use hold for every $p \geq 11$; among them, Theorem 5.4, Lemma 5.5, Lemma 6.3, Theorems 6.4 and 6.6, Lemmas 7.5 and 7.6 and Propositions 7.23 and 7.24 assume of p only that it is odd (the standing assumption of [14, §§5 and 6]),

Theorems 7.1, 7.9 and 8.7 assume $p > 5$, Corollary 8.5 assumes that p is unramified in K, and the spaces of Hilbert cusp forms shown to be zero in [14, §9.2] do not depend on p. At $p = 19$, in case (C), the comparison of traces leaves one further newform, 2.2.5.1-2000.1-h in [72], without complex multiplication, which Proposition A.2(c) and Proposition A.4(b) exclude. The proof of Theorem 1.1 uses the results of [14] in Table 2; Theorem 1.2 uses no result of [14].

2.3. **The case split.** Let (a, b, c) be a solution. Either exactly one of $2, 5$ divides ab, or neither divides ab, or $10 \mid ab$. We say that the solution is in

- *case (A)* if $10 \mid ab$ and $\bar\rho_{J^-,\mathfrak{p}}$ is irreducible for some prime $\mathfrak{p} \mid p$ of K;
- *case (B)* if $10 \mid ab$ and $\bar\rho_{J^-,\mathfrak{p}}$ is reducible for every prime $\mathfrak{p} \mid p$ of K;
- *case (C)* if $2 \nmid ab$ and $5 \nmid ab$.

Let $p \neq 5$. If $10p \mid ab$, each of 2, 5 and p divides exactly one of a and b, and we say that the solution is in

- *class (a)* if p and 2 divide one of a, b and 5 divides the other;
- *class (b)* if p and 5 divide one of a, b and 2 divides the other;
- *class (c)* if p divides one of a, b and 10 divides the other;
- *class (d)* if $10p$ divides one of a, b.

These classes are defined without J^-, for every solution with $10p \mid ab$, whether it lies in case (A) or in case (B). A solution in class (d) is labeled so that $10p \mid b$, using the symmetry $(a, b, c) \mapsto (b, a, c)$. Theorem 9.2 excludes class (d) without using J^-.

Lemma 2.2. *Let $p \neq 5$. Every solution lies in exactly one of the following sets: the solutions for which exactly one of $2, 5$ divides ab (the solutions excluded by (CK1)); those with $2 \nmid ab$ and $5 \nmid ab$ (case (C)); those with $10 \mid ab$ and $p \nmid ab$; and those with $10p \mid ab$. A solution with $10 \mid ab$ lies in exactly one of case (A), case (B) with $p \nmid ab$, and the classes (a)–(d) of case (B).*

Proof. The number of primes among $2, 5$ dividing ab (1, 0 or 2) and, when it is 2, whether $p \mid ab$ separate the four sets; cases (A) and (B) are complementary; and in case (B) with $p \mid ab$ the primes among $2, 5$ that divide the same one of a, b as p form $\{2\}$, $\{5\}$, $\varnothing$ or $\{2, 5\}$, the classes (a)–(d). □

Proposition 2.3 (Chen–Koutsianas)**.** *Let $p \geq 11$ be prime. No solution lies in case (A): if $10 \mid ab$, then $\bar\rho_{J^-,\mathfrak{p}}$ is reducible for every prime $\mathfrak{p} \mid p$ of K.*

Proof. We use (CK2) and (CK3). If $\bar\rho_{J^-,\mathfrak{p}}$ were irreducible, so would be $\bar\rho' = \bar\rho_{J^-,\mathfrak{p}} \otimes \chi_0$, against (CK3). Both Lemma 2.1(a) and (CK3) cover every $\mathfrak{p} \mid p$ and every $\chi_0 \in K(S_2, 2)^*$. □

In case (B) the reducibility takes a rigid form, which the arguments of Section 3 start from. It is Darmon's passage from a reducible residual representation to a rational point of order p [21, Proposition 3.11 and Theorem 3.13], carried out with the conductors of [14] in [41, Proposition 8.1(a)].

Proposition 2.4. *Let $p \geq 11$ be prime, (a, b, c) a solution in case (B), and $\mathfrak{p} \mid p$ a prime of K. There is a character $\eta\colon G_K \to \{\pm 1\}$, possibly trivial, unramified outside $\mathfrak{q}_2$, $\mathfrak{q}_5$ and the real places ∞_1, ∞_2 of K, such that the twist $J = J^- \otimes \eta$ satisfies*

$$J[\mathfrak{p}] \cong \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix}, \qquad \{\theta, \theta'\} = \{1, \chi_p\}.$$

If $\theta = 1$, the nonzero points of the stable line are K-rational points of J of order p; if $\theta' = 1$, the quotient $J/J[\mathfrak{p}]^\theta$ by the stable line, an abelian surface over K with real multiplication by $\mathcal{O}_K$ defined over K, has the K-rational points of order p given by the image of $J[\mathfrak{p}]$.

Proof. This is [41, Proposition 8.1(a)] with the diagonal characters from its proof; we give the proof. One of the two diagonal characters of $\bar\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ is unramified at every prime above p, by [14, Corollary 8.5] with the unit ϕ^4, and so factors through a ray class group of K of order 2; twisting by it and by χ_0 gives J. The symmetries of the solutions twist J^- by -1, a character unramified outside $\mathfrak{q}_2\infty_1\infty_2$, so we may assume $2 \mid a$ and $b \equiv -1 \pmod 4$. With $\bar\rho' = \bar\rho_{J^-,\mathfrak{p}} \otimes \chi_0$ as in (CK2), write $\bar\rho' \cong \left(\begin{smallmatrix} \theta_1 & * \\ 0 & \theta_2 \end{smallmatrix}\right)$ with $\theta_1\theta_2 = \chi_p$. The two characters have the same conductor exponent e_v at every finite place $v \nmid p$, and the conductor exponent of $\bar\rho'$ at v is at least that of $\theta_1 \oplus \theta_2$, which is $2e_v$; so the Serre level forces e_v to vanish away from $\mathfrak{q}_5$ and to be at most 1 at $\mathfrak{q}_5$. At a prime $\mathfrak{p}' \mid p$ of K (unramified over p, as $p \neq 5$), $\bar\rho'$ is finite, so by Raynaud's theorem [65, Corollaire 3.4.4] on finite flat group schemes of type $(p, \dots, p)$, as in [14, (8.7)], the restriction of $\theta_1 \oplus \theta_2$ to the inertia group at $\mathfrak{p}'$ is, up to order, $1 \oplus \chi_p$ or the sum of the two fundamental characters of level 2, the second only when p is inert in K. Suppose that each of θ_1, θ_2 is ramified at some prime above p. Then one of them, ϑ, restricts to inertia as χ_p at one prime $\mathfrak{p}_0 \mid p$ and trivially at the other if p splits in K, and as a fundamental character of level 2 at $\mathfrak{p}_0 = p\mathcal{O}_K$ if p is inert. In the convention of [14, (8.1) and Proposition 8.4(2)], the exponents $n_{\mathfrak{p}'}(\tau)$ (τ running over the embeddings of $\mathcal{O}_K/\mathfrak{p}'$ into $\bar{\mathbb{F}}_p$) of ϑ^{-1} vanish except for one pair $(\mathfrak{p}_0, \tau_1)$, for which $n_{\mathfrak{p}_0}(\tau_1) = 1$, and the conductor of ϑ^{-1} away from p divides $\mathfrak{q}_5$. The proof of [14, Proposition 8.4] uses its hypothesis (1) only through the triviality of the character, composed with the reciprocity map, on $\mathcal{O}_{K_v}^\times$ for the finite places $v \nmid 5p$ and on the units $\equiv 1 \pmod{\mathfrak{q}_5}$ of $K_{\mathfrak{q}_5}$, that is, only the conductor away from p. So [14, Corollary 8.5] applies to ϑ^{-1} with the totally positive unit $u = \phi^4 = (7 + 3\sqrt{5})/2$, for which $u - 1 = \sqrt{5}\,\phi^2 \in \mathfrak{q}_5$ (no congruence at $\mathfrak{q}_2$ is needed, unlike in [14, proof of Theorem 8.7], as the conductor of ϑ^{-1} away from p divides $\mathfrak{q}_5$), and gives $\tau_1(u) \equiv 1 \pmod{\mathfrak{p}_0}$. So p divides $\mathrm{N}_{K/\mathbb{Q}}(\phi^4 - 1) = -5$, which is impossible for $p \geq 11$. Hence one of the two characters, θ_0, is unramified at every prime above p. It then factors through the ray class group of K of modulus $\mathfrak{q}_5\infty_1\infty_2$, which has order 2 [14, proof of Theorem 8.6]: as K has class number 1, this group is the quotient of $(\mathcal{O}_K/\mathfrak{q}_5)^\times \times \{\pm 1\}^2$, of order 16, by the image of the units $\langle -1, \phi\rangle$, of order 8 ($\phi \equiv 3 \pmod{\mathfrak{q}_5}$ has order 4 in $\mathbb{F}_5^\times$, with signs $(+,-)$, and $-1 \equiv 4$, with signs $(-,-)$). As $\mathbb{Q}(\zeta_5)/K$ is ramified only at $\mathfrak{q}_5$, tamely, and at ∞_1, ∞_2, its character ψ_1 is the nontrivial character of this group, so $\theta_0 \in \{1, \psi_1\}$. Put $\eta = \chi_0\theta_0$, unramified outside $\mathfrak{q}_2$, $\mathfrak{q}_5$, ∞_1, ∞_2 as χ_0 and θ_0 are; then $\bar\rho_{J,\mathfrak{p}} = \bar\rho' \otimes \theta_0$ has diagonal characters 1 and $\chi_p\theta_0^2 = \chi_p$. If $\theta = 1$, G_K fixes the stable line, so its nonzero points, killed by $p \in \mathfrak{p}$, are K-rational points of order p. If $\theta' = 1$, G_K fixes the image of $J[\mathfrak{p}]$ in the quotient of J by the stable line, and the nonzero points of this image have order p in the same way; the stable line is an $\mathcal{O}_K$-submodule, as $\mathcal{O}_K$ acts on $J[\mathfrak{p}]$ through $\mathbb{F}_\mathfrak{p}$, so $\mathcal{O}_K$ acts on the quotient, faithfully since each nonzero element of $\mathcal{O}_K$ is an isogeny of J. □

For a case-(B) solution, $J = J^- \otimes \eta$ always denotes the twist of Proposition 2.4.

3. Case (B) with $p \nmid ab$

This section excludes the solutions of case (B) with $p \nmid ab$, at the primes the main theorems need. Besides J^- it uses Darmon's second Frey surface J^+. At inert p these solutions are excluded by J^+ alone: its residual representation is reducible, which leaves only the values $\pm 1 \pm p$ for the trace of Frobenius at p, while its $\sqrt{5}$-torsion forces that trace to be divisible

by 5 (Section 3.2). At split p they are excluded by J^-, through the traces of Frobenius at p and at the auxiliary prime 11 (Section 3.3). The solutions of case (B) with $p \mid ab$ have $10p \mid ab$, so Theorem 1.2 excludes them when $p \geq 7$, $p \not\equiv 1 \pmod 5$ and $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$.

3.1. **Darmon's second Frey surface.** For a solution (a, b, c) let

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

which is isomorphic over $\mathbb{Q}$ to $C^+(t) \colon y^2 = (x + 2)(D_5(x) + 2 - 4t)$, $D_5(x) = x^5 - 5x^3 + 5x$, $t = a^p/c^5$ [14, Lemma 5.5(2)], and let J^+ be its Jacobian. We write $J^+(t)$ for the Jacobian of $C^+(t)$ over $\mathbb{Q}(t)$, and $J^+(t_0)$ for that of $C^+(t_0)$ when $t_0 \in \mathbb{Q} \setminus \{0, 1\}$. As for J^-, $\mathcal{O}_K$ acts on J^+ by endomorphisms defined over K, and for $\tau \in G_\mathbb{Q} \setminus G_K$ one has $\tau \circ [\alpha] \circ \tau^{-1} = [\sigma(\alpha)]$ [71, Theorem 1 and the Remark on p. 1058], [21, pp. 420 and 443], [14, Theorem 5.4 and proof of Proposition 6.5]. For every prime $\mathfrak{l} \mid \ell$ of K, $\rho_\mathfrak{l}^+$ is the action of G_K on $T_\ell(J^+) \otimes_{\mathcal{O}_K \otimes \mathbb{Z}_\ell} \mathcal{O}_{K,\mathfrak{l}}$, with $\det \rho_\mathfrak{l}^+ = \chi_\ell$ [14, Lemma 6.3], and at a prime $\mathfrak{q} \nmid \ell$ of good reduction the $\mathcal{O}_K$-trace $a_\mathfrak{q} \in \mathcal{O}_K$ of Frobenius does not depend on $\mathfrak{l}$ and satisfies the Weil bound at both real places. For a prime $\mathfrak{p} \mid p$ of K we write $\bar\rho_\mathfrak{p}^+$ for the representation of G_K on $J^+[\mathfrak{p}]$. The model above has discriminant $2^{20}5^5(a^2b)^{2p}$ [14, (7.2)]. Let ψ_1 be the quadratic character of $\mathbb{Q}(\zeta_5)/K$; it is the restriction of the mod-5 cyclotomic character, and $\psi_1(\mathrm{Frob}_\mathfrak{q}) \equiv N\mathfrak{q} \pmod 5$ for $\mathfrak{q} \nmid 5$.

Lemma 3.1. *Let p be an odd prime, $p \neq 5$, and (a, b, c) a solution with $5 \mid ab$.*

(a) At a prime $\mathfrak{q} \nmid 10$ of K, J^+ has good reduction if $\mathfrak{q} \nmid ab$, and purely toric reduction with every thickness a multiple of $p\, v_\mathfrak{q}(ab)$ if $\mathfrak{q} \mid ab$. Hence $J^+[p]$ is unramified at every $\mathfrak{q} \nmid 10p$, and finite at every prime above p (for the primes dividing ab by [21, Proposition 1.15(2)], the monodromy pairing being $\equiv 0 \pmod p$).

(b) At $\mathfrak{q}_5$, for every $\mathfrak{l}$, including $\mathfrak{l} = \mathfrak{q}_5$, $\rho_\mathfrak{l}^+|_{D_{\mathfrak{q}_5}} \cong \nu_5 \otimes \left(\begin{smallmatrix} \chi_\ell & * \\ 0 & 1 \end{smallmatrix}\right)$ with $\nu_5 = 1$ if $5 \mid a$ and $\nu_5 = \psi_1|_{D_{\mathfrak{q}_5}}$ if $5 \mid b$; the conductor exponent of $\rho_\mathfrak{l}^+$ ($\mathfrak{l} \nmid 5$) at $\mathfrak{q}_5$ is 1 if $5 \mid a$ and 2 if $5 \mid b$.

Proof. (a) For $\mathfrak{q} \nmid 10ab$ the model is smooth. For $\mathfrak{q} \mid ab$, $\mathfrak{q} \nmid 10$, the special fiber is $y^2 = (x + 2\tilde c)^2(x^2 - \tilde c x - \tilde c^2)^2$ if $\mathfrak{q} \mid a$ and $y^2 = (x + 2\tilde c)(x - 2\tilde c)(x^2 + \tilde c x - \tilde c^2)^2$ if $\mathfrak{q} \mid b$, as $c^5 D_5(x/c) \pm 2c^5 = (x \pm 2c)(x^2 \mp cx - c^2)^2$, and the reduction is semistable [14, Lemma 7.5], purely toric as the components are rational. The thicknesses of the nodes are $2m, m, m$ with $m = v_\mathfrak{q}(t) = p\, v_\mathfrak{q}(a)$, resp. m, m with $m = v_\mathfrak{q}(1 - t) = p\, v_\mathfrak{q}(b)$, by the computation of Lemma 3.2 below, all units there being $\mathfrak{q}$-units. Grothendieck's description of the monodromy [39, Exp. IX, §§9–12] then gives the claims. (b) Let $\nu_0 = 1$ if $5 \mid a$, and ν_0 the character of $K_{\mathfrak{q}_5}(5^{1/4})/K_{\mathfrak{q}_5}$ if $5 \mid b$. By [14, Lemma 7.6 and its proof], $J^+ \otimes \nu_0$ has purely toric reduction over $K_{\mathfrak{q}_5}$; by the Mumford–Raynaud uniformization [28, Chapters II–III], $(J^+ \otimes \nu_0)(\bar K_{\mathfrak{q}_5})$ is the quotient of the $\bar K_{\mathfrak{q}_5}$-points of a torus by a lattice Λ, $\mathcal{O}_K$-equivariantly, with Frobenius acting on Λ and on the character group X of the torus through a character μ with values ± 1. So for every ℓ, including $\ell = 5$, $T_\ell(J^+ \otimes \nu_0)$ is an extension of $\Lambda \otimes \mathbb{Z}_\ell$ by $X^\vee \otimes \mathbb{Z}_\ell(1)$, where $X^\vee$ is the dual of X, and $\nu_5 = \nu_0\mu$. If $5 \mid a$, the components and nodes of the special fiber $y^2 = x^2(x - 2\tilde c)^2(x + 2\tilde c)^2$ are $\mathbb{F}_5$-rational and $\mu = 1$. If $5 \mid b$, the nodes $x = \pm 2\tilde c$ of the special fiber $y^2 = -\tilde c x(x - 2\tilde c)^2(x + 2\tilde c)^2$ of [14, (7.8)] are non-split, as the squares $3\tilde c^4$ and $2\tilde c^4$ of their tangent slopes are not squares modulo 5. So μ is the unramified quadratic character, and $\nu_5 = \psi_1|_{D_{\mathfrak{q}_5}}$, as $K(\zeta_5) = K(\sqrt{-\sqrt{5}\phi})$ and $-\phi \equiv 2 \pmod{\sqrt{5}}$ is not a square. For $\ell \neq 5$ the inertia group acts trivially on $X^\vee \otimes \mathbb{Q}_\ell(1)$, as μ and χ_ℓ are unramified; and as the reduction of $J^+ \otimes \nu_0$ is purely toric, the inertia invariants of $V_\ell(J^+ \otimes \nu_0)$ have dimension $2 = \operatorname{rank} X$ [67, §1, Lemmas 1 and 2], so they are $X^\vee \otimes \mathbb{Q}_\ell(1)$. Hence, for $\mathfrak{l} \nmid 5$, as $X \otimes \mathbb{Q}$ is a K-line, the inertia invariants of $V_\mathfrak{l}(J^+ \otimes \nu_0)$ form a line and inertia acts on $V_\mathfrak{l}(J^+ \otimes \nu_0)$

through a nontrivial unipotent; so the inertia invariants of $\rho_{\mathfrak{l}}^{+}$ have dimension 1 if $\nu_5 = 1$ and 0 if ν_5 is ramified. As ν_5 is tamely ramified, so is $\rho_{\mathfrak{l}}^{+}$ at $\mathfrak{q}_5$, and the conductor exponent is 1 if $5 \mid a$ and 2 if $5 \mid b$. This agrees with [14, Theorem 7.7, Remark 7.8], stated for $2 \nmid ab$, whose proof uses that hypothesis only for the reduction at $\mathfrak{q}_2$, in its first sentence. □

Lemma 3.2 (the prime 2)**.** *Let p be odd and (a,b,c) a solution with $2 \mid ab$. Then J^{+} has purely toric reduction over $K_{\mathfrak{q}_2}$. If $2 \mid a$, the torus is split and the monodromy pairing is $m \left(\begin{smallmatrix} 3 & -1 \\ -1 & 2 \end{smallmatrix}\right)$ with $m = p\, v_2(a)$; if $2 \mid b$, the torus splits over the unramified quadratic extension, and the pairing is $m \cdot 1$ with $m = p\, v_2(b)$. Hence $J^{+}[p]$ is unramified at $\mathfrak{q}_2$.*

Proof. Put $P(x) = x^2 - x - 1$; then $D_5(x) = (x+2)P(x)^2 - 2 = (x-2)P(-x)^2 + 2$. Over $W(\mathbb{F}_4)$, $y \mapsto 2y + (x+2)P(x)$ and $y \mapsto 2y + xP(-x)$ give the models $y^2 + (x+2)P(x)y + t(x+2) = 0$ and $y^2 + xP(-x)y + P(-x)^2 + (x+2)(t-1) = 0$ [21, proof of Theorem 1.10]. If $2 \mid a$, $v_2(t) = m$, and the first model reduces to $y(y + x(x^2 + x + 1)) = 0$: two smooth rational curves over $\mathbb{F}_2$ meeting transversally at $x = 0$ and at the two roots of $x^2 + x + 1$ in $\mathbb{F}_4$, with smooth points at infinity. The node over $x = -2$ has thickness $v(t^2) = 2m$ (locally $(y + t/P)(y + (x+2)P - t/P) = -t^2/P^2$ with $P = P(x)$ and $P(-2) = 5$ a unit) and the nodes over the roots of P, units at 2, have thickness m. So the pairing on H_1 of the dual graph (two vertices, three edges, all over $\mathbb{F}_4$) is as stated. If $2 \mid b$, $v_2(t-1) = m$, and the second model reduces to $y^2 + xh_2 y + h_2^2 = 0$, $h_2 = x^2 + x + 1$: a rational curve with two nodes over the roots of h_2, whose branches are conjugate over $\mathbb{F}_4$ (as $z^2 + x_0 z + 1$ has no root in $\mathbb{F}_4$ for the roots x_0 of h_2), each of thickness m (locally $(y - z_1 P(-x))(y - z_2 P(-x)) = -(t-1)(x+2)$, with z_1, z_2 the roots of $z^2 + xz + 1$); Frobenius acts by -1 on H_1. In both cases the reduction is purely toric, the torus splits over an unramified extension, and the pairing is $\equiv 0 \pmod{p}$, so inertia acts trivially on $J^{+}[p]$ [39, Exp. IX, §§9–12]. □

Purely toric reduction at $\mathfrak{q}_2$ when $2 \mid a$ is in the proof of [21, Proposition 1.15]. Toric reduction at $\mathfrak{q}_2$, and conductor exponent 1 there for the $\mathfrak{l}$-adic representations, are also in [1, Proposition 4.23, Theorem 5.12], and semistable models at $\mathfrak{q}_2$ are in [15, §§3.1.2–3.1.3].

Lemma 3.3 (the $\sqrt{5}$-torsion)**.** *For every $t_0 \in \mathbb{Q} \smallsetminus \{0,1\}$, the semisimplification of $J^{+}(t_0)[\sqrt{5}]$ as an $\mathbb{F}_5[G_K]$-module is $1 \oplus \psi_1$. Hence at a prime $\mathfrak{q} \nmid 5$ of good reduction $a_{\mathfrak{q}} \equiv 1 + N\mathfrak{q} \pmod{\sqrt{5}}$, and at an inert prime p of good reduction the $\mathcal{O}_K$-trace of the $\mathbb{F}_{p^2}$-Frobenius is divisible by 5 if it is a rational integer.*

Proof. This is [21, Theorem 2.6(2) and the parenthesis in its proof] (see also [25, Proposition 2.3]): $J^{+}(t)[\sqrt{5}]$ over $K(t)$ contains a $K(t)$-rational point of order 5, which specializes to every t_0 since $C^{+}(t)$ is smooth over $\mathbb{P}^1_K \smallsetminus \{0, 1, \infty\}$; the quotient is ψ_1 since the Weil pairing gives $\det \rho_{\mathfrak{q}_5}^{+} = \chi_5$ (for J^{+} of a solution this is [14, Lemma 6.3]). □

Lemma 3.4 (modularity)**.** *Let $p \neq 5$ be an odd prime and (a,b,c) a solution with $5 \mid ab$. Then J^{+} is modular: there is a Hilbert newform over K of parallel weight 2 and trivial character whose $\mathfrak{l}$-adic representations are the $\rho_{\mathfrak{l}}^{+}$.*

Proof. This is [21, Theorem 2.9(1)] and [14, Theorem 6.4] (the ordinarity at $\mathfrak{q}_5$ needed in [69, Theorem A] is Lemma 3.1(b)); the newform has parallel weight 2 and trivial character as $\det \rho_{\mathfrak{l}}^{+} = \chi_\ell$ [14, Lemma 6.3]. □

Lemma 3.5. *The spaces of Hilbert cusp forms over K of parallel weight 2, trivial character and level 1, $\mathfrak{q}_5$, $\mathfrak{q}_5^2$ are zero.*

This is [21, Table 2] (from [21, Theorem 3.9]) and [14, §9.2]; see also (C2) in Appendix B.

3.2. **Solutions with $p \nmid ab$ at inert primes.** Let $p \equiv \pm 2 \pmod 5$ be a prime, $p \geq 7$, so $\mathfrak{p} = p\mathcal{O}_K$ with $\mathbb{F}_\mathfrak{p} = \mathbb{F}_{p^2}$ and $\psi_1(\mathrm{Frob}_\mathfrak{p}) = -1$. Let θ_{p^n-1} denote a fundamental character of level n of the inertia group $I_\mathfrak{p}$, and $\omega = \chi_p|_{I_\mathfrak{p}}$.

Proposition 3.6. *Let (a,b,c) be a solution with $10 \mid ab$ and $p \nmid ab$. Then $\bar\rho^+_\mathfrak{p}$ is reducible.*

Proof. We follow the argument for [21, Theorem 3.10(1)], with the levels at $\mathfrak{q}_5$ and $\mathfrak{q}_2$ of Lemma 3.1(b) and Lemma 3.2. *Inertia at $\mathfrak{p}$.* J^+ has good reduction at $\mathfrak{p}$ and $e(\mathfrak{p}/p) = 1 < p-1$. By Raynaud's description of finite flat vector space schemes of rank one [65, Corollaire 3.4.4], the two characters of $(\bar\rho^+_\mathfrak{p}|_{I_\mathfrak{p}})^{\mathrm{ss}}$ are $\{1,\omega\}$ or $\{\theta_{p^2-1}, \theta^p_{p^2-1}\}$ if there is an $\mathbb{F}_{p^2}$-rational stable line over $G_{K_\mathfrak{p}}$, and otherwise $\theta^{1+p}_{p^4-1} \oplus \theta^{p^2+p^3}_{p^4-1}$ or $\theta^{1+p^3}_{p^4-1} \oplus \theta^{p+p^2}_{p^4-1}$. In each case the ratio of the two characters has order $p-1$, $p+1$ or $(p^2+1)/2$, never 2. *Irreducibility on $G_{K(\zeta_p)}$.* Suppose $\bar\rho^+_\mathfrak{p}$ irreducible. Then it is absolutely irreducible (complex conjugation has distinct eigenvalues with rational eigenlines). If its restriction to $G_{K(\zeta_p)}$ were reducible, it would be induced from the quadratic subextension $K(\sqrt{p^*})$, so its inertia characters at $\mathfrak{p}$ would differ by the quadratic character $\omega^{(p-1)/2}$, which the previous step excludes. *Level lowering.* By Lemma 3.4, $\bar\rho^+_\mathfrak{p} \cong \bar\rho_{f_0}$ with f_0 of level $N = \mathfrak{q}_5^e\mathfrak{q}_2 \prod_{\mathfrak{q}\mid ab, \mathfrak{q}\nmid 10} \mathfrak{q}$, where $e \in \{1,2\}$ is the conductor exponent of Lemma 3.1(b). By Lemma 3.1(a) and Lemma 3.2, $\bar\rho^+_\mathfrak{p}$ is unramified at $\mathfrak{q}_2$ and at every $\mathfrak{q} \mid ab$, $\mathfrak{q} \nmid 10$, which divide N exactly once, and it is finite at $\mathfrak{p}$. Level lowering for Hilbert modular forms [34], [40], [63], by the argument of the proof of [33, Theorem 7] (with f_0 Steinberg at $\mathfrak{q}_5$ after the twist by ψ_1 when $5 \mid b$, as $\psi_1 \otimes \psi_1 \otimes \mathrm{St} = \mathrm{St}$) gives $\bar\rho^+_\mathfrak{p} \cong \bar\rho_g$ for a newform g of parallel weight 2 and level dividing $\mathfrak{q}_5^2$. The character of g factors through the ray class group of K of modulus $\mathfrak{q}_5^2\infty_1\infty_2$, a quotient of $(\mathcal{O}_K/\mathfrak{q}_5^2)^\times \times \{\pm 1\}^2$, so its order divides 80, which is prime to p. Its reduction modulo p is trivial, as $\det \bar\rho_g = \chi_p$, so the character is trivial, and Lemma 3.5 excludes g. □

Lemma 3.7. *Let (a,b,c) be as in Proposition 3.6. Then $(\bar\rho^+_\mathfrak{p})^{\mathrm{ss}} = \theta^+ \oplus (\theta^+)^{-1}\chi_p$ with $\theta^+ \in \{1, \psi_1\}$, and $p \nmid c$; the reduction J_0 of J^+ at $\mathfrak{p}$ is ordinary, and the $\mathcal{O}_K$-trace A of its $\mathbb{F}_{p^2}$-Frobenius Π is a rational integer with $A \in \{s_\mathfrak{p} + p, s_\mathfrak{p} - p\}$, $s_\mathfrak{p} = \theta^+(\mathrm{Frob}_\mathfrak{p})$.*

Proof. One of the two characters of $(\bar\rho^+_\mathfrak{p})^{\mathrm{ss}}$ is unramified at $\mathfrak{p}$, and class field theory makes it 1 or ψ_1. The reduction is then ordinary, which rules out $p \mid c$, and the unit root of Frobenius, the 2-torsion of J_0 and the Weil bound give $A = s_\mathfrak{p} \pm p$.

The characters. Write $(\bar\rho^+_\mathfrak{p})^{\mathrm{ss}} = \lambda_1 \oplus \lambda_2$, $\lambda_1\lambda_2 = \chi_p$. They are unramified away from $\mathfrak{q}_5$, $\mathfrak{p}$ and the infinite places (Lemma 3.1(a) and Lemma 3.2), and $\lambda_i|_{I_{\mathfrak{q}_5}} \in \{1, \psi_1|_{I_{\mathfrak{q}_5}}\}$ by Lemma 3.1(b). At $\mathfrak{p}$ their inertia characters are $\{1,\omega\}$ or $\{\theta_{p^2-1}, \theta^p_{p^2-1}\}$, and the second is impossible. Indeed, $\lambda_1 \circ \mathrm{rec}_K$ is trivial on the principal idèle of the totally positive unit $\phi^4 \equiv 1 \pmod{\mathfrak{q}_5}$, and the components of this idèle contribute nothing except at $\mathfrak{p}$: at the real places because ϕ^4 is totally positive, at $\mathfrak{q}_5$ because λ_1 is tamely ramified there and $\phi^4 \equiv 1 \pmod{\mathfrak{q}_5}$, and at the other finite places because λ_1 is unramified there and ϕ^4 is a unit. So the component at $\mathfrak{p}$ is trivial too, which would give $(\phi \bmod \mathfrak{p})^{\pm 4} = 1$ in $\mathbb{F}_{p^2}$, while $N(\phi^4 - 1) = -5$. So one of the two characters, θ^+, is unramified at $\mathfrak{p}$. It factors through the ray class group of K of modulus $\mathfrak{q}_5\infty_1\infty_2$, which has order 2 and whose nontrivial character is ψ_1 (proof of Proposition 2.4): $\theta^+ \in \{1, \psi_1\}$.

Ordinarity. As $p \nmid ab$, J^+ has good reduction at $\mathfrak{p}$ (Lemma 3.1(a)). Over $\mathcal{O}_{K_\mathfrak{p}}$, unramified over $\mathbb{Z}_p$, the closure of the stable line in the $\mathfrak{p}$-torsion of the Néron model and the quotient are finite flat, and the one with trivial inertia character, on which G_K acts through θ^+, is étale [65, Théorème 3.3.3]. So $J_0[p] = J_0[\mathfrak{p}]$ has an étale part of order p^2 (Raynaud's theorem

applies as $e(\mathfrak{p}/p) = 1 < p-1$), on whose points Frobenius acts by $s_\mathfrak{p}$; so $J_0[p](\bar{\mathbb{F}}_p)$ has order at least p^2 (an étale quotient of $J_0[p]$ is a quotient of $J_0[p]^{\mathrm{et}}$), hence exactly $p^2 = p^{\dim J_0}$, that is, J_0 is ordinary.

The prime p does not divide c. If $p \mid c$, then C^+ reduces to $y^2 = x(x^5 - 4a^p)$, whose Jacobian has complex multiplication by $\mathbb{Z}[\zeta_5]$. After $x \mapsto 1/x$ this curve is $y^2 = 1 - 4a^p x^5$, of p-rank 0 for $p \not\equiv 1 \pmod 5$ by the Cartier–Manin computation in the proof of Proposition 3.9, against ordinarity.

The trace. J_0 is defined over $\mathbb{F}_p$, and its $\mathbb{F}_p$-Frobenius π satisfies $\pi[\alpha] = [\sigma\alpha]\pi$, so $\Pi = \pi^2$ commutes with $\mathcal{O}_K$ and its characteristic polynomial $X^2 - AX + p^2$ is fixed by σ: $A \in \mathbb{Z}$ (compare [6, Lemma 3.14]), and $|A| \le 2p$. On the étale part of $T_p(J_0)$, free of rank one over $\mathcal{O}_K \otimes \mathbb{Z}_p = \mathbb{Z}_{p^2}$, Π acts by the unit root, which is $\equiv A \pmod p$; so $A \equiv s_\mathfrak{p} \pmod p$. It remains to show that A is even. The six Weierstrass points of $C^+(t_0)$, $t_0 = a^p/c^5$, modulo p are -2 and the roots of $D_5(x) + 2 - 4t_0$, which are the numbers $\zeta_5^k w + \zeta_5^{-k} w^{-1}$, $k \in \mathbb{Z}/5$, for a root w of $w^5 + w^{-5} = 4t_0 - 2$. The p-th power map sends w to a root $\zeta_5^n w^{\pm 1}$ of the same equation, so the p^2-th power map sends w to $\zeta_5^j w$ for some $j \in \mathbb{Z}/5$, and ζ_5 to $\zeta_5^{p^2} = \zeta_5^{-1}$. So Π fixes -2 and permutes the others by $k \mapsto j - k$, and its characteristic polynomial on $J_0[2]$ over $\mathbb{F}_2$ is $(X+1)^4$, as this permutation is an involution and the differences of Weierstrass points generate $J_0[2]$, so that $(\Pi + 1)^2 = \Pi^2 + 1 = 0$ there, while over $\mathbb{F}_4 = \mathcal{O}_K/2$ it is $X^2 + \bar{A}X + 1$; if $\bar{A} = 1$ this would give $(X^2 + X + 1)^2$. So A is even, and $A - s_\mathfrak{p}$ is odd, divisible by p, of absolute value at most $2p + 1$: $A = s_\mathfrak{p} \pm p$. □

Theorem 3.8. *Let $p \ge 7$ be a prime with $p \equiv \pm 2 \pmod 5$. There is no solution with $10 \mid ab$ and $p \nmid ab$.*

Proof. We use the results on J^+ in (CK4). By Proposition 3.6 and Lemma 3.7, $A = s_\mathfrak{p} \pm p \equiv \pm 1 \pm 2 \pmod 5$, which is never 0. By Lemma 3.3 applied to $t_0 = a^p/c^5$ at $\mathfrak{p}$, a prime of good reduction (Lemma 3.1(a)) at which A is a rational integer (Lemma 3.7), $A \equiv 0 \pmod 5$. □

The theorem uses nothing about J^-; it excludes in particular the solutions of case (B) with $p \nmid ab$ at these primes. The mechanism is Darmon's: the reducibility of $\bar{\rho}^+_\mathfrak{p}$ when $5 \mid ab$ [21, Theorem 3.10(1)] and the $\sqrt{5}$-torsion [21, Theorem 2.6(2)], here compared through the trace of Frobenius at the exponent prime p itself. For $x^p + y^p = z^{11}$, Darmon used, in place of the point of order 5 of Lemma 3.3, a rational point of order 11, against a Frobenius trace at the prime 2 [21, Theorem 3.14], and Chen and Koutsianas compare the trace at $\mathfrak{q}_2$ with a reducible $\bar{\rho}^+_\mathfrak{p}$ [14, Theorem 8.6]. Kraus's argument for Frey curves [46, proof of Théorème 2], [48, Lemme 6.4] uses the facts about the trace of Frobenius at the exponent prime that Lemma 3.7 uses: its residue modulo p, its parity, which comes from the 2-torsion, and the Weil bound; in his argument these facts already leave no possible value of the trace.

3.3. **Solutions with $p \nmid ab$ at split primes.** For $\delta \in K^\times$ let χ_δ be the quadratic character of $K(\sqrt{\delta})/K$ (χ_p remains the cyclotomic character), so that $K(S_2, 2)^* = \{\chi_\delta : \delta \in \langle -1, \phi, 2\rangle\}$. In the proof of Proposition 2.4, $\eta = \chi_0\theta_0$ after the symmetries of the solutions have been used to assume $2 \mid a$ and $b \equiv -1 \pmod 4$. They twist J^- by χ_{-1} (the sign change $(a, b, c) \mapsto (-a, -b, -c)$, for instance, fixes $t = a^p/c^5$ and replaces c by $-c$ in the twist by c below), so for the solution itself η is $\chi_0\theta_0$ or $\chi_{-1}\chi_0\theta_0$. As $\chi_{-1}\chi_0 \in K(S_2, 2)^*$, we write $\eta = \chi_{\delta_0}\theta_0$ with $\delta_0 \in \langle -1, \phi, 2\rangle$ and $\theta_0 \in \{1, \psi_1\}$, so that $N_{K/\mathbb{Q}}(\delta_0) \in \{\pm 1, \pm 4\}$ modulo squares. With $t = a^p/c^5$ and $C(t)\colon y^2 = D_5(x) + 2 - 4t$, the curve C^- is the quadratic twist of $C(t)$ by c over $\mathbb{Q}$, so $J^- = \operatorname{Jac} C(t) \otimes \chi_c$. For $\tau \in G_\mathbb{Q} \smallsetminus G_K$, τ maps $J^-[\mathfrak{p}]$ onto $J^-[\sigma\mathfrak{p}]$, so $\bar{\rho}_{J^-,\sigma\mathfrak{p}} \cong \bar{\rho}^\tau_{J^-,\mathfrak{p}}\colon g \mapsto \bar{\rho}_{J^-,\mathfrak{p}}(\tau^{-1}g\tau)$ [21, p. 443], [14, proof of Proposition 6.5].

Proposition 3.9. *Let $p \geq 11$ be a prime with $p \not\equiv 1 \pmod 5$ and (a,b,c) a case-(B) solution. Then $p \nmid c$.*

The argument is Serre's supersingular-reduction argument [66, Proposition 12] (a reducible representation with an unramified character cannot come from reduction of p-rank 0), applied to the reduction modulo p, a twist of the curve $y^2 = x^5 - 4$ of the trivial solution $(1,-1,0)$, whose Jacobian has complex multiplication by $\mathbb{Z}[\zeta_5]$ [21, Proposition 3.7(2)], [14, Remark 5.7]. Compare [46, proof of Théorème 2] and [48, Lemme 6.4].

Proof. We use (CK2) and (CK4). Suppose $p \mid c$; then $p \nmid ab$, C^- has good reduction at p (its discriminant is $2^{16}5^5(ab)^{2p}$ [14, (7.1)]), and it reduces to $y^2 = x^5 - 4a^p$. The characters of $\bar\rho_{J^-,\mathfrak{p}}$ are η and $\eta\chi_p$, with η unramified at p. Over $\mathcal{O}_{K_\mathfrak{p}}$, unramified over $\mathbb{Z}_p$, the closure of the stable line and the quotient are finite flat, and the one with unramified generic fiber is étale [65, Théorème 3.3.3]; so the reduction has p-rank at least 1. But the Cartier–Manin matrix of $y^2 = x^5 - 4a^p$ in characteristic p, whose entries are the coefficients of x^{pi-j} $(i,j \in \{1,2\})$ in $(x^5 - 4a^p)^{(p-1)/2}$, has at most one nonzero entry, off the diagonal, when $p \not\equiv 1 \pmod 5$, so the p-rank is 0. □

Proposition 3.10. *Let $p \geq 17$ be a prime split in K. No case-(B) solution has $p \nmid abc$.*

Proof. We use (CK2) and (CK4). Let $\mathfrak{p}\mathfrak{p}' = p\mathcal{O}_K$, with embeddings $\iota_1, \iota_2 = \iota_1 \circ \sigma$ of K into $\mathbb{Q}_p$, and let (a,b,c) be a case-(B) solution with $p \nmid abc$.

Step 1. As t and $1-t$ are p-adic units, $C(t)$ has good reduction at $\mathfrak{p}$ and $\mathfrak{p}'$, with reduction $C(t_0)$, $t_0 = a/(a+b) \bmod p$. Let $J_0 = \operatorname{Jac} C(t_0)$ over $\mathbb{F}_p$, with $\mathcal{O}_K$ acting through ι_1, and let its Frobenius endomorphism π satisfy $\pi^2 - \alpha\pi + p = 0$, with $\alpha \in \mathcal{O}_K$ and $|\alpha| \leq 2\sqrt{p}$ at both real places of K. The representation $\bar\rho_{\operatorname{Jac} C(t),\mathfrak{p}} = \bar\rho_{J^-,\mathfrak{p}} \otimes \chi_c$ has semisimplification $\mu \oplus \mu\chi_p$ with $\mu = \eta\chi_c$ quadratic and unramified at p. As in Lemma 3.7, $J_0[\mathfrak{p}^\infty]$ is ordinary and its étale quotient has character $\mu|_{D_\mathfrak{p}}$, so $\iota_1(\alpha) \equiv \varepsilon_1 = \mu(\mathrm{Frob}_\mathfrak{p}) \pmod p$; at $\mathfrak{p}'$, through τ (compare [6, Lemma 3.14]), $\iota_2(\alpha) \equiv \varepsilon_2 = \mu(\mathrm{Frob}_{\mathfrak{p}'}) \pmod p$. *Step 2.* If $\varepsilon_1 = \varepsilon_2 = \varepsilon$, then $\alpha - \varepsilon \in p\mathcal{O}_K$ with $|N(\alpha - \varepsilon)| \leq (2\sqrt{p}+1)^2 < p^2$, so $\alpha = \pm 1$. If $\varepsilon_1 = -\varepsilon_2$, then $\operatorname{Tr}\alpha \equiv 0 \pmod p$ and $|\operatorname{Tr}\alpha| \leq 4\sqrt{p} < p$, so $\alpha = k\sqrt{5}$ with $k \in \mathbb{Z}$, $5k^2 \equiv 1 \pmod p$ and $5k^2 \leq 4p$. *Step 3.* For every $t_0 \in \mathbb{F}_p \smallsetminus \{0,1\}$, $\alpha \not\equiv 1 \pmod{2\mathcal{O}_K}$: the roots of $D_5(x) = 4t_0 - 2$ are the numbers $\zeta_5^i w + \zeta_5^{-i} w^{-1}$, $i \in \mathbb{Z}/5$, for a root w of $w^5 + w^{-5} = 4t_0 - 2$, and Frobenius permutes them through the dihedral group, $i \mapsto \pm i + j$ for some j (as in the proof of Lemma 3.7); on $J_0[2]$ its $\mathbb{F}_2$-characteristic polynomial is therefore $(X+1)^4$ or $X^4+X^3+X^2+X+1$, while for $\bar\alpha = 1$ it would be $(X^2+X+1)^2$. So $\alpha \neq \pm 1$, and in the second alternative k is even ($\sqrt{5} \equiv 1 \pmod 2$), $k = 2k'$, and $20k'^2 - 1$ is odd, positive, $< 4p$ and divisible by p: it is p or $3p$. *Step 4.* $\chi_c(\mathrm{Frob}_\mathfrak{p}) = \chi_c(\mathrm{Frob}_{\mathfrak{p}'})$, $\theta_0(\mathrm{Frob}_\mathfrak{p}) = \theta_0(\mathrm{Frob}_{\mathfrak{p}'})$, and $\chi_{\delta_0}(\mathrm{Frob}_\mathfrak{p})\chi_{\delta_0}(\mathrm{Frob}_{\mathfrak{p}'}) = (\frac{N(\delta_0)}{p})$; so $\varepsilon_1 = -\varepsilon_2$ forces $N(\delta_0) < 0$ and $p \equiv 3 \pmod 4$, whence $20k'^2 - 1 = p$.

Step 5: $N(\delta_0) > 0$ if $p > 144$. The prime 11 splits, $11 = \mathfrak{q}\mathfrak{q}'$. If $11 \nmid ab$, J^- has good reduction at $\mathfrak{q}, \mathfrak{q}'$, and the traces of $\bar\rho_{J^-,\mathfrak{p}}$ and $\bar\rho_{J^-,\mathfrak{p}'}$ at $\mathrm{Frob}_\mathfrak{q}$ give $a_\mathfrak{q} \equiv 12\eta(\mathfrak{q}) \pmod \mathfrak{p}$ and $a_\mathfrak{q} \equiv 12\eta(\mathfrak{q}') \pmod{\mathfrak{p}'}$; if $\eta(\mathfrak{q}) = \eta(\mathfrak{q}')$, then $0 < |N(a_\mathfrak{q} \mp 12)| \leq (12 + 2\sqrt{11})^2 < p^2$ is divisible by p^2, and otherwise $a_\mathfrak{q} = m\sqrt{5}$ with $5m^2 \equiv 144 \pmod p$ and $5m^2 \leq 44$, so, as $p > 144$, $5m^2 = 144$; both are impossible. So $11 \mid ab$, say $11 \mid a$. The special fiber of C^- at $\mathfrak{q}$ is $y^2 = (x + 2\tilde c)(x^2 - \tilde c x - \tilde c^2)^2$ [14, (7.5)], with two $\mathbb{F}_{11}$-rational nodes at $x = \tilde c r$, $r \in \{\phi, \phi'\}$, whose branch slopes satisfy $\mathrm{slope}^2 = 5\tilde c^3(r+2)$, which is $c\sqrt{5}\phi$ times a square in both cases. So $J^- \otimes \chi_c\chi_{\sqrt{5}\phi}$ has split multiplicative reduction at $\mathfrak{q}$ and $\mathfrak{q}'$, and comparing $\{11\eta(\mathfrak{q}), \eta(\mathfrak{q})\}$ with $\{11\chi_c\chi_{\sqrt{5}\phi}(\mathfrak{q}), \chi_c\chi_{\sqrt{5}\phi}(\mathfrak{q})\}$ modulo p ($11^2 \not\equiv 1$) gives $\eta(\mathfrak{q}) = \chi_c(\mathfrak{q})\chi_{\sqrt{5}\phi}(\mathfrak{q})$, and likewise at $\mathfrak{q}'$. As $\chi_c(\mathfrak{q}) = \chi_c(\mathfrak{q}')$ and $\chi_{\sqrt{5}\phi}(\mathfrak{q}) = \chi_{\sqrt{5}\phi}(\mathfrak{q}')$, $\eta(\mathfrak{q}) = \eta(\mathfrak{q}')$; as 11 splits completely in

$\mathbb{Q}(\zeta_5)$, $\psi_1(\mathfrak{q}) = \psi_1(\mathfrak{q}')$; so $(\frac{N(\delta_0)}{11}) = 1$, and $N(\delta_0) > 0$ as $(\frac{-1}{11}) = -1$. This contradicts Step 4 for $p > 144$. Among the split primes $p < 144$, only 19 and 79 have the form $20k'^2 - 1$. At these no $t_0 \in \mathbb{F}_p \smallsetminus \{0, 1\}$ has Frobenius polynomial $X^4 + (p-1)X^2 + p^2$, that is, $\alpha = \pm 2k'\sqrt{5}$: the 94 polynomials are listed in Appendix B, (C3). □

The proposition is the analogue, with a Frobenius argument at p (compare [46, proof of Théorème 2]), of the classical theorems on the first case of Fermat's Last Theorem. The dihedral 2-torsion of the family excludes $\alpha = \pm 1$, the only Frobenius trace the reducible representation allows when $\varepsilon_1 = \varepsilon_2$. When $\varepsilon_1 = -\varepsilon_2$, Steps 4 and 5 (the comparison at 11) and, for $p = 19$ and 79, the computation (C3) exclude $\alpha = k\sqrt{5}$.

4. Case (C)

In case (C), for a solution ordered so that $a \equiv -1 \pmod 4$, the Frey surface J^- is congruent, at every $p \geq 13$, to the Jacobian of $y^2 = x^5 + 4$, $y^2 = x^5 + 16$ or $y^2 = x^5 + 64$, curves attached to trivial solutions $(\alpha, -\alpha, 0)$ [14, Theorem 1.2], Theorem A.9. So the modular method alone cannot exclude case (C). We use instead the arithmetic of $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_{5p})$, together with two facts that Appendix A proves from the results of [14] for case (C) listed in (CK4): a case-(C) solution has $ab \equiv \pm 1 \pmod 5$, and J^- has wild conductor at $\sqrt{5}$. The section proves:

Theorem 4.1. *Let $p \geq 13$ be a prime with $p \not\equiv 1 \pmod 5$ and $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$. No solution lies in case (C).*

Proof. We use the case-(C) results in (CK4). By Proposition 4.4 every case-(C) solution has $5 \mid c$, and Theorem 4.6(b) excludes solutions with $5 \mid c$. □

The second step uses $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$; the first uses no class number at all when $p \not\equiv 1 \pmod 5$.

4.1. **The branch $5 \nmid c$.** For a case-(C) solution let ε be the conductor exponent at $\mathfrak{q}_5$ of the $\mathfrak{l}$-adic representation $\rho_{J^-,\mathfrak{l}}$ of J^-, for a prime $\mathfrak{l} \nmid 5$ of K. By [14, Propositions 7.23 and 7.24], $\varepsilon = 3$ if $v_5(d) = 1$ and $\varepsilon = 2$ if $v_5(d) \geq 2$, where $d = \Phi(x_0)$, $x_0 = -a^p - 2c$ and $\Phi(x) = x^5 - 5c^2x^3 + 5c^4x - 2(a^p - b^p)$.

Lemma 4.2. *Let $p \geq 13$ be prime and (a, b, c) a case-(C) solution. Then $ab \equiv \pm 1 \pmod 5$ and $\varepsilon = 3$.*

Proof. We use the case-(C) results in (CK4). As $2 \mid c$, $a \equiv -b \pmod 4$, so one of the two orders of a, b has $a \equiv -1 \pmod 4$. Exchanging a and b keeps ab, and replaces C^- by its twist by -1, a square in $K_{\mathfrak{q}_5}$, which keeps ε. So the lemma is part of Theorem A.9. □

Step 4 of the proof of the next proposition, and Lemma 8.2, use the following consequence of Stickelberger's theorem; the argument is Mihăilescu's for Catalan's equation [56], [7, Theorem 3.2 and §3.1].

Lemma 4.3. *Let $p \neq 5$ be an odd prime, $F = \mathbb{Q}(\zeta_p)$, c complex conjugation, σ_k the automorphism $\zeta_p \mapsto \zeta_p^k$ of F, and $\theta_{\mathrm{Stick}} = \frac{1}{p}\sum_{k=1}^{p-1} k\,\sigma_k^{-1}$ the Stickelberger element. Let $\alpha \in \mathcal{O}_F$ be prime to 5 with $(\alpha) = \mathfrak{A}^5$ for an ideal $\mathfrak{A}$, and suppose that $\alpha/\bar{\alpha} \equiv \pm(1 + 5y) \pmod{25}$ with $y \in \mathcal{O}_F \otimes \mathbb{Z}_5$. Then $p\theta_{\mathrm{Stick}}y \equiv 0 \pmod 5$, where $p\theta_{\mathrm{Stick}}y = \sum_k k\,\sigma_k^{-1}(y)$.*

Proof. As $p\theta_{\mathrm{Stick}}$ lies in $\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})] \cap \theta_{\mathrm{Stick}}\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$, $\mathfrak{A}^{p\theta_{\mathrm{Stick}}} = (\gamma)$ is principal [75, Theorem 6.10], so $\alpha^{p\theta_{\mathrm{Stick}}} = u\gamma^5$ with u a unit. As c commutes with $\mathrm{Gal}(F/\mathbb{Q})$, $(\alpha/\bar\alpha)^{p\theta_{\mathrm{Stick}}} = (u/\bar u)(\gamma/\bar\gamma)^5$; the unit $u/\bar u$ has absolute value 1 at every complex place, so it is a root of unity $\pm\zeta_p^k$, a fifth power. Hence $(\alpha/\bar\alpha)^{p\theta_{\mathrm{Stick}}}$ is a fifth power in F. On the other hand $(\alpha/\bar\alpha)^{p\theta_{\mathrm{Stick}}} \equiv \pm(1 + 5p\theta_{\mathrm{Stick}}y) \pmod{25}$, as $\prod_k (1+5y_k)^{n_k} \equiv 1 + 5\sum_k n_k y_k$. Since 5 is unramified in F, $(1+5\mathcal{O}_w)^5 = 1 + 25\mathcal{O}_w$ at every $w \mid 5$, and $\pm(1+5z)$ is a fifth power in F_w only if $z \in 5\mathcal{O}_w$. So $p\theta_{\mathrm{Stick}}y \equiv 0 \pmod 5$. □

Proposition 4.4. *Let $p \geq 11$ be a prime with $p \not\equiv 1 \pmod 5$, so that $p \geq 13$. Every case-(C) solution has $5 \mid c$.*

Proof. We use the case-(C) results in (CK4). Let (a, b, c) be a case-(C) solution with $5 \nmid c$; write $\zeta = \zeta_p$ and $F = \mathbb{Q}(\zeta)$.

Step 1: $a \equiv b \pmod 5$. By Lemma 4.2, $b \equiv \pm a^{-1}$, and $a^{-1} \equiv \pm a$ as $a^2 \equiv \pm 1 \pmod 5$; so $b \equiv \pm a$. If $b \equiv -a$, then $5 \mid a + b \mid c^5$; so $b \equiv a \pmod 5$.

Step 2: a fifth power. If $p \mid c$ let $\alpha = (a + \zeta b)/(1 - \zeta)$, and if $p \nmid c$ let $\alpha = \zeta^{-r}(a + \zeta b)$, $r = (p+1)/2$. As $\Phi_p(a,b) = (a^p + b^p)/(a+b) = \prod_{j=1}^{p-1}(a + \zeta^j b)$, $\gcd(a + b, \Phi_p(a,b)) \mid p$ and $v_p(\Phi_p(a,b)) = 1$ if $p \mid c$, the conjugates of α are pairwise coprime integers prime to $5p$ whose product is a fifth power, so $(\alpha) = \mathfrak{A}^5$. Moreover $\alpha + \bar\alpha = a - b$ if $p \mid c$ (from $1/(1-\zeta) + 1/(1-\zeta^{-1}) = 1$), and $\alpha = \zeta^{-r}a + \zeta^r b$ if $p \nmid c$.

Step 3: the expansion at 5. Write $b = a(1 + 5s)$, $s \in \mathbb{Z}_5$, and $t = (\zeta - 1)/(\zeta + 1)$, a 5-adic unit. Then $(a+\zeta b)/(a+\zeta^{-1}b) \equiv \zeta(1+5st) \pmod{25}$, so $\alpha/\bar\alpha \equiv \pm(1+5st) \pmod{25\mathcal{O}_F \otimes \mathbb{Z}_5}$, with the sign $+$ if $p \nmid c$ (as $\zeta^{-2r} = \zeta^{-1}$) and $-$ if $p \mid c$ (as $(1-\zeta^{-1})/(1-\zeta) = -\zeta^{-1}$).

Step 4: Stickelberger. By Step 3 and Lemma 4.3, applied to the element α of Step 2 with $y = st$, $s \cdot (p\theta_{\mathrm{Stick}}t) \equiv 0$ in $\mathcal{O}_F/5\mathcal{O}_F$. Now $t = \varrho\zeta$ with $\varrho = \sum_{j=1}^{p-1}(-1)^{j+1}\sigma_j$, as $(1+\zeta)\sum_j (-1)^{j+1}\zeta^j = \zeta - 1$, and $x \mapsto x\zeta$ is an isomorphism $\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})] \to \mathbb{Z}[\zeta]$; so $p\theta_{\mathrm{Stick}}t = (p\theta_{\mathrm{Stick}}\varrho)\zeta$. The coefficient of σ_1 in $p\theta_{\mathrm{Stick}}\varrho$ is $\sum_k k(-1)^{k+1} = -(p-1)/2$, prime to 5 as $p \not\equiv 1 \pmod 5$, so $p\theta_{\mathrm{Stick}}\varrho \notin 5\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$ and $s \equiv 0 \pmod 5$: $a \equiv b \pmod{25}$.

Step 5: the conductor at $\sqrt{5}$. By Step 4, $a^p \equiv b^p \pmod{25}$, so $c^5 = a^p + b^p \equiv 2a^p \pmod{25}$ and $c \equiv c^5 \equiv 2a^p \pmod 5$. Hence $x_0 = -a^p - 2c \equiv -5a^p \equiv 0 \pmod 5$, and each term of $d = x_0^5 - 5c^2x_0^3 + 5c^4x_0 - 2(a^p - b^p)$ is divisible by 25. So $v_5(d) \geq 2$ and $\varepsilon = 2$, against Lemma 4.2. □

The congruence $a \equiv b \pmod{25}$ of Step 4 is the case $q = 5$, $f = -1$ of the congruence $x + fy \equiv 0 \pmod{q^2}$, $f \in \{-1, 0, 1\}$, which Mihăilescu states for $x^p + y^p = z^q$ when $\max\{p, p(p-20)/16\} > q$ and $q \nmid h^-(\mathbb{Q}(\zeta_p))$ [57, Theorem 2]. The proof above replaces the class-number hypothesis by Lemma 4.3.

4.2. **The branch $5 \mid c$.** Mihăilescu treats the equation $x^p + y^p = z^q$ with $q \mid z$ by a descent in $\mathbb{Q}(\zeta_{pq})$ adapted from Kummer's descent for the second case of Fermat's Last Theorem [57, Theorems 6–8], and states part (b) of Theorem 4.6 below for $p > 3$ (the statement of Theorem 7 there prints $f = -1$; its proof treats $q \mid x + y$, that is, $f = 1$ in the convention of its (5)). His descent theorem [57, Theorem 6, p. 29], for an equation of the shape of Theorem 4.5 below, assumes that X and Y are not units, which its two applications in the proof of his Theorem 4 [57, Theorems 7 and 8, pp. 35–38] do not verify. The proof of his Theorem 6 writes each factor $\zeta_q^i X + \zeta_q^{-i} Y$ of $X^q + Y^q$, normalized, as a unit times a q-th power, and shows by [57, Lemma 7, p. 13] that these units are q-th powers; that lemma asks of a unit that its quotient by a rational integer be a q-th power in every completion above q, but the proof establishes this property only for their quotient by $-Y$, which in

general is not a rational integer [57, proof of Theorem 6, after Lemma 18, p. 32]. In the two applications the factors are written as units times q-th powers in $\mathbb{Q}(\zeta_q, \zeta_p + \zeta_p^{-1})$ by [57, Lemma 5], but that field need not contain them, as they are in general not fixed by the automorphism $\zeta_p \mapsto \zeta_p^{-1}$, $\zeta_q \mapsto \zeta_q$ [57, proof of Theorem 7, after (72), p. 36, and proof of Theorem 8, p. 37]. The proof below follows his method, treats these three points (Steps 3 and 4 of Theorem 4.5, Steps 2 and 3 of Theorem 4.6), and uses no other result of [57] than those recalled in (F1)–(F4).

Let $q \geq 5$ and $p \neq q$ be odd primes, $\zeta = \zeta_p$, $\xi = \zeta_q$, $L_{pq} = \mathbb{Q}(\zeta, \xi)$, $F = \mathbb{Q}(\zeta)$ and $F^+ = \mathbb{Q}(\zeta + \zeta^{-1})$. Let j_p, j_q be the partial complex conjugations ($j_p \colon \zeta \mapsto \zeta^{-1}$, ξ fixed, and conversely), $\mathsf{c} = j_p j_q$ complex conjugation, and L_p, L^{++} the fixed fields of j_p and of $\langle j_p, j_q \rangle$. At $q = 5$, $L_{5p} = M$, $L_p = M'$ and $L^{++} = L^+$ in the notation of Section 1.5. Put $\pi_q = \xi - \xi^{-1}$ and $\pi_p = \zeta - \zeta^{-1}$. For a prime $\mathfrak{Q}$ of L_{pq} above q, $v_{\mathfrak{Q}}(\pi_q) = 1$ and $v_{\mathfrak{Q}}(q) = q - 1$, as q is unramified in F. An element prime to q is *q-primary* if it is a q-th power in every completion above q, in the sense of [57, §5.1] (not Eisenstein's sense of "primary"). For an ideal $\mathfrak{a}$ of $\mathcal{O}_{L_{pq}}$ let $\omega(\mathfrak{a})$ be the number of distinct prime ideals dividing it. We use the following facts.

(F1) If $q \nmid h^-(L_{pq})$ then $q \nmid h(L_{pq})$, and q-primary units of L_{pq} are q-th powers [57, Proposition 3]. This is a case of the reflection theorem. Indeed, write the q-Sylow subgroup of the class group as $A = A^+ \oplus A^-$ under c; the q-part of $h^-(L_{pq})$ is $|A^-|$, so $A^- = 0$. If $A^+ \neq 0$, Kummer theory ($\mu_q \subset L_{pq}$) writes an unramified cyclic extension of degree q, on whose Galois group c acts trivially, as $L_{pq}(\beta^{1/q})$ with $\mathsf{c}\beta \equiv \beta^{-1}$ modulo q-th powers. Then $(\beta) = \mathfrak{b}^q$ with $[\mathfrak{b}] \in A^- = 0$, so $\beta = u\gamma^q$ with u a unit and $u\,\mathsf{c}(u)$ a q-th power. As $u/\mathsf{c}(u)$ is a root of unity (L_{pq} is CM), so is u^2, and hence u, modulo q-th powers. Then $u \equiv \xi^b$, and $q \mid b$ because $L_{pq}(\xi^{1/q}) = L_{pq}(\zeta_{q^2})$ is ramified at q. So β is a q-th power, a contradiction. Consequently q divides the class number of no subfield k with $[L_{pq} : k]$ prime to q (extension of ideals followed by the norm is the $[L_{pq} : k]$-th power), and every q-primary unit u of L_{pq} is a q-th power ($L_{pq}(u^{1/q})/L_{pq}$ is unramified, hence trivial).

(F2) If $k \subseteq L_{pq}$ has class number prime to q, and $\varphi, \psi \in \mathcal{O}_k$ generate coprime ideals of $\mathcal{O}_{L_{pq}}$ with $\varphi\psi = C^q$, $C \in \mathcal{O}_k$, then $\varphi = \upsilon\mu^q$ with $\upsilon \in \mathcal{O}_k^\times$, $\mu \in \mathcal{O}_k$. (The ideals $\varphi\mathcal{O}_k$ and $\psi\mathcal{O}_k$ are coprime, as a common prime would lie under a common prime of $\mathcal{O}_{L_{pq}}$, and their product is $(C\mathcal{O}_k)^q$; so $\varphi\mathcal{O}_k = \mathfrak{a}^q$, and $\mathfrak{a} = \mu\mathcal{O}_k$ as $q \nmid h(k)$.)

(F3) Let $\mathfrak{Q}$ be a prime of L_{pq} above q. A root of unity $\delta \in L_{pq}$ with $\delta \equiv 1 \pmod{\mathfrak{Q}^2}$ is 1 ($v_{\mathfrak{Q}}(1 - \delta) = 0$ unless $\delta = 1$ or δ has order q, and $v_{\mathfrak{Q}}(1 - \xi^b) = 1$ for $q \nmid b$). If $\beta \equiv 1 \pmod{\mathfrak{Q}^{q+1}}$ for every $\mathfrak{Q} \mid q$, then β is q-primary (the logarithm is an isomorphism $1 + \mathfrak{Q}^k \to \mathfrak{Q}^k$ for $k \geq 2$, and $\mathfrak{Q}^{q+1} = q\mathfrak{Q}^2$). If $w \in F$ is a unit at a prime $\mathfrak{q} \mid q$ of F and $w^q \equiv 1 \pmod{\mathfrak{q}^k}$, $k \geq 2$, then $w \equiv 1 \pmod{\mathfrak{q}^{k-1}}$.

(F4) $(1-\zeta)\mathcal{O}_{L_{pq}}$ is the product of the primes above p, each of ramification index $p-1$; if $-1 \in \langle p \bmod q \rangle$, c fixes each of them (the decomposition group in $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong (\mathbb{Z}/q)^\times$ of every prime of $\mathbb{Q}(\xi)$ above p is $\langle p \bmod q \rangle$, which then contains -1, the restriction of c to $\mathbb{Q}(\xi)$; so c fixes each prime of $\mathbb{Q}(\xi)$ above p, and each of these is totally ramified in L_{pq}, so has one prime above it, which c therefore fixes).

(F5) $\prod_{i=0}^{q-1}(\xi^i a + \xi^{-i} b) = a^q + b^q$ and $\prod_{i=1}^{q-1}(\xi^i - \xi^{-i}) = q$; with $N_i = -(\xi^i - \xi^{-i})^2$ and $i \not\equiv \pm k \pmod q$, $\upsilon_{ik} = \pi_q^2(1/N_i - 1/N_k)$ and π_q^{q-1}/q are units of $\mathbb{Q}(\xi)^+$.

(F6) If $X \in L_{pq}^\times$ and $X^q \in L^{++}$, then $\xi^k X \in L^{++}$ for some k.

(F7) If $[L_{pq} : k]$ is prime to q and $u \in k^\times$ is a q-th power in L_{pq}, then $u = v^q$ with $v \in k$, and v is a unit if u is: if $u = \beta^q$ and $qm + [L_{pq} : k]n = 1$, take $v = u^m \,\mathrm{N}_{L_{pq}/k}(\beta)^n$. This applies to F, F^+, L_p and L^{++}, of index $q-1$, $2(q-1)$, 2 and 4.

(F2), the first part of (F3) and the last clause of (F4) are versions of [57, Lemmas 5, 6 and 16], respectively, and we include their proofs.

Theorem 4.5 (descent)**.** *Let $q \geq 5$ and $p \neq q$ be odd primes with $q \nmid h^-(L_{pq})$. There are no $X, Y, Z \in \mathcal{O}_{L^{++}}$, $\varepsilon \in \mathcal{O}_{L^{++}}^\times$, integer exponents $N > 2q$, $M \geq 0$ with*

$$X^q + Y^q = \varepsilon \pi_q^N \pi_p^M Z^q, \qquad XYZ \neq 0, \quad (X, Y) = (1), \quad (XYZ, pq) = (1),$$

and $-1 \in \langle p \bmod q \rangle$ in case $M > 0$.

This is the conclusion $q \mid h^-(L_{pq})$ of [57, Theorem 6], read contrapositively, with five changes to its hypotheses: X and Y may be units; $p = 3$ is allowed; $-1 \in \langle p \bmod q \rangle$ is assumed only when $M > 0$; N is proved even in Step 1 rather than assumed even, and $M \neq 1$ is not assumed (Step 1 shows that M is even); and X and Y are assumed coprime. The proof follows his.

Proof. Suppose there is a solution, and choose one, for all admissible ε, N, M, with $\omega(Z)$ least.

Step 1: parities and valuations. Applying j_q, which fixes X, Y, Z, ε, π_p and changes the sign of π_q, gives $(-1)^N = 1$; applying j_p gives $(-1)^M = 1$. So $N \geq 2q+2$. Put $\varphi_i' = \xi^i X + \xi^{-i} Y$, so that $X^q + Y^q = \prod_{i=0}^{q-1} \varphi_i'$ by (F5). At a prime $\mathfrak{Q} \mid q$, $(X+Y)^q \equiv X^q + Y^q \equiv 0$, and $X + Y$ lies in the fixed field of j_q, over which $\mathfrak{Q}$ is ramified, so $v_\mathfrak{Q}(X+Y) \geq 2$. As $\varphi_i' = \xi^{-i}((\xi^{2i} - 1)X + (X+Y))$, this gives $v_\mathfrak{Q}(\varphi_i') = 1$ for $i \neq 0$ and $v_\mathfrak{Q}(X+Y) = N - (q-1)$. At a prime $\mathfrak{P} \mid p$ with $M > 0$, $(-X/Y)^q \equiv 1$, so $-X \equiv \xi^a Y \pmod{\mathfrak{P}}$ for some a. Applying c, which fixes X, Y and $\mathfrak{P}$ (F4), gives $-X \equiv \xi^{-a} Y$; as $\xi^a - \xi^{-a}$ divides q for $q \nmid a$, we get $a \equiv 0$. So $\mathfrak{P} \mid X + Y$, $\varphi_i' \equiv (\xi^i - \xi^{-i})X \not\equiv 0 \pmod{\mathfrak{P}}$ for $i \neq 0$, and $v_\mathfrak{P}(X+Y) = M$.

Step 2: the factors. Put $\varphi_i = \varphi_i'/(\xi^i - \xi^{-i})$ for $1 \leq i \leq q-1$ and $\varphi_0 = q(X+Y)/(\varepsilon \pi_q^N \pi_p^M)$. By Step 1 and (F5): (a) every φ_i is integral and prime to pq; (b) $\prod_{i=0}^{q-1} \varphi_i = Z^q$; (c) the φ_i are pairwise coprime, since a common prime of φ_i and φ_k divides $\xi^{-k}\varphi_i' - \xi^{-i}\varphi_k' = (\xi^{i-k} - \xi^{k-i})X$ and $\xi^k \varphi_i' - \xi^i \varphi_k' = (\xi^{k-i} - \xi^{i-k})Y$, hence X and Y; (d) $\varphi_0 \in L^{++}$, $\varphi_i \in L_p$ and $j_q(\varphi_i) = \mathsf{c}(\varphi_i) = \varphi_{q-i}$ for $i \geq 1$; (e) $\varphi_i = -Y + \xi^i(X+Y)/(\xi^i - \xi^{-i}) \equiv -Y \pmod{\mathfrak{Q}^{N-q}}$ for $i \geq 1$ and every $\mathfrak{Q} \mid q$.

Step 3: no φ_i with $i \geq 1$ is a unit. If φ_i were a unit, $\delta = \varphi_i/\mathsf{c}(\varphi_i)$ would be a unit all of whose conjugates have absolute value 1, as L_{pq} is an abelian CM field, hence a root of unity. By (e) for φ_i and for $\mathsf{c}(\varphi_i)$ (c permutes the primes above q and fixes Y), $\delta \equiv 1 \pmod{\mathfrak{Q}^{N-q}}$ with $N - q \geq 2$, so $\delta = 1$ by (F3), that is, $\varphi_i = \varphi_{q-i}$. But $\varphi_i - \varphi_{q-i} = (\xi^i + \xi^{-i})(X+Y)/(\xi^i - \xi^{-i}) \neq 0$, as $X + Y \neq 0$ (otherwise $Z = 0$).

Step 4: q-th powers with one common unit. By (F1), q divides neither $h(L_p)$ nor $h(L^{++})$. So (F2), applied in L_p to φ_i ($i \geq 1$) and in L^{++} to φ_0, gives $\varphi_i = \upsilon_i \mu_i^q$ with υ_i a unit and μ_i an integer of the same field. As $N - q \geq q + 2$, (e) and (F3) show that $\varphi_i/(-Y)$ is q-primary for $i \geq 1$, and by (b) so is $\varphi_0/(-Y) = (Z/(-Y))^q \prod_{i \geq 1}(-Y/\varphi_i)$. Hence each υ_i/υ_0 is a q-primary unit, a q-th power in L_{pq} by (F1), and the q-th power of a unit of L_p by (F7). Changing the μ_i accordingly, $\varphi_i = \upsilon_0 \mu_i^q$ for all i, with $\mu_0 \in L^{++}$ and $\mu_i \in L_p$; and for $1 \leq i \leq (q-1)/2$ we may take $\mu_{q-i} = j_q(\mu_i)$, by (d).

Step 5: the derived equation. With $S = X + Y$, $\varphi_i \varphi_{q-i} = S^2/N_i - XY$, so $\varphi_1\varphi_{q-1} - \varphi_2\varphi_{q-2} = (1/N_1 - 1/N_2)S^2$. Inserting $\varphi_k\varphi_{q-k} = \upsilon_0^2(\mu_k\mu_{q-k})^q$ and $S = \varepsilon \pi_q^N \pi_p^M \upsilon_0 \mu_0^q / q$ and

dividing by υ_0^2 gives

$$X_1^q + Y_1^q = \varepsilon_1 \pi_q^{2(N-q)} \pi_p^{2M} Z_1^q,$$
$$X_1 = \mu_1 \mu_{q-1}, \quad Y_1 = -\mu_2 \mu_{q-2}, \quad Z_1 = \mu_0^2, \quad \varepsilon_1 = \upsilon_{12} \varepsilon^2 (\pi_q^{q-1}/q)^2,$$

with ε_1 a unit of L^{++} by (F5). The elements $X_1 = \mu_1 j_q(\mu_1)$ and $Y_1 = -\mu_2 j_q(\mu_2)$ lie in L_p and are fixed by j_q, so they lie in $\mathcal{O}_{L^{++}}$. As $(\mu_k)^q = (\varphi_k)$ and the φ_k are pairwise coprime and prime to pq, $(X_1, Y_1) = (1)$ and $(X_1 Y_1 Z_1, pq) = (1)$; also $2(N-q) > 2q$, and $2M > 0$ only if $M > 0$. So (X_1, Y_1, Z_1) is again a solution.

Step 6: descent. By (b) and (c), every prime dividing Z divides exactly one φ_k, so $\omega(Z) = \sum_k \omega(\varphi_k) \geq \omega(\varphi_0) + q - 1$ by Step 3, while $\omega(Z_1) = \omega(\varphi_0)$. So $\omega(Z_1) < \omega(Z)$, against the choice of the solution. □

Theorem 4.6. *Let $p \neq 5$ be an odd prime with $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$.*

(a) There are no coprime integers x, y, z with $x^p + y^p = z^5$, $5 \mid z$ and $p \nmid z$.

(b) If moreover $p \not\equiv 1 \pmod 5$, there are no coprime integers x, y, z with $x^p + y^p = z^5$, $z \neq 0$ and $5 \mid z$.

Proof. Take $q = 5$ in the notation above, and let (x, y, z) be a triple as in (a) or (b); then $z \neq 0$. We turn (x, y, z) into a solution of the equation of Theorem 4.5, which that theorem excludes: Step 1 writes α as a unit times a fifth power, and Steps 2 and 3 treat $p \nmid z$ and, for $p \not\equiv 1 \pmod 5$, $p \mid z$.

Step 1: preliminaries. As $5 \mid z$ and x, y, z are coprime, $5 \nmid xy$; as $t \mapsto t^p$ is bijective on $(\mathbb{Z}/5)^\times$, $x^p \equiv (-y)^p$ gives $5 \mid x + y$, and $x + y \neq 0$ as $z \neq 0$. Put $n = v_5(z) \geq 1$. As $\Phi_p(x, y) = (x^p + y^p)/(x + y) \equiv p y^{p-1} \pmod{x+y}$, $\gcd(x + y, \Phi_p(x, y))$ divides p and $5 \nmid \Phi_p(x, y)$, so $v_5(x + y) = 5n$. If $p \nmid z$, then $x + y = 5^{5n} C^5$; if $p \mid z$ and $m = v_p(z)$, then $v_p(\Phi_p(x, y)) = 1$ and $x + y = p^{5m-1} 5^{5n} C^5$; in both cases $C \in \mathbb{Z}$ is prime to $5p$. Let $e = 0$ if $p \nmid z$ and $e = 1$ if $p \mid z$, and $\alpha = (x + \zeta y)/(1 - \zeta)^e \in \mathcal{O}_F$. Its norm $\Phi_p(x, y)/p^e$ is a fifth power prime to $5p$, and its conjugates are pairwise coprime, since a common prime of two of them divides $(\zeta^i - \zeta^j)y$ and $(\zeta^{-i} - \zeta^{-j})x$, hence p. So (α) is the fifth power of an ideal. By (F1), $5 \nmid h(F)$, so $\alpha = \zeta^c \varepsilon^+ \rho_0^5$ with $\rho_0 \in \mathcal{O}_F$ and ε^+ a unit of F^+, since every unit of the prime-conductor field $F = \mathbb{Q}(\zeta_p)$ is a power of ζ_p times a real unit (for a unit ε of F, $\varepsilon/\bar{\varepsilon}$ is a root of unity, as it has absolute value 1 at every complex place, and it is $\equiv 1 \pmod{1-\zeta}$, so it is ζ^{2k} for some k, and $\zeta^{-k}\varepsilon$ is real). Put $r = (p+1)/2$, so that $\zeta^r + \zeta^{-r} = \zeta^{-r}(1 + \zeta)$ is a unit of F^+ and $\zeta^r - \zeta^{-r} = \zeta^{-r}(\zeta - 1)$.

Step 2: the case $p \nmid z$. Choose d with $5d \equiv c - r \pmod p$ and put $\rho_1 = \zeta^d \rho_0$, so that $\zeta^{-r}\alpha = \varepsilon^+ \rho_1^5$. As $\zeta^{-r}\alpha + \zeta^r \bar{\alpha} = (x + y)(\zeta^r + \zeta^{-r})$,

$$\rho_1^5 + \bar{\rho}_1^5 = (x + y)\varepsilon_0 = 5^{5n} C^5 \varepsilon_0, \qquad \varepsilon_0 = (\zeta^r + \zeta^{-r})/\varepsilon^+,$$

a unit of F^+. Let $S = \rho_1 + \bar{\rho}_1$. By (F3) for $w = -\rho_1/\bar{\rho}_1$, $v_{\mathfrak{Q}}(S) \geq 4(5n - 1) \geq 2$ at every prime $\mathfrak{Q}$ of L_{5p} above 5. In $\rho_1^5 + \bar{\rho}_1^5 = \prod_{i=0}^4 (\xi^i \rho_1 + \xi^{-i} \bar{\rho}_1)$ (F5), the factor $\xi^i \rho_1 + \xi^{-i} \bar{\rho}_1 = (\xi^i - \xi^{-i})\rho_1 + \xi^{-i} S$ has $v_{\mathfrak{Q}} = 1$ for $i \neq 0$, so $v_{\mathfrak{Q}}(S) = 4(5n - 1)$. At the primes above p, $S \equiv 2\rho_1 \pmod{1-\zeta}$ is a unit. Put $\varphi_i = (\xi^i \rho_1 + \xi^{-i} \bar{\rho}_1)/(\xi^i - \xi^{-i})$ for $1 \leq i \leq 4$ and $\varphi_0 = S/(5^{5n-1}\varepsilon_0) \in F^+$. As in Step 2 of the proof of Theorem 4.5, these are integral, prime to $5p$ and pairwise coprime (a common prime divides ρ_1 and $\bar{\rho}_1$, which are coprime), their product is C^5, and $\varphi_i \equiv \rho_1 \pmod{\mathfrak{Q}^{4(5n-1)-1}}$ for $i \geq 1$. Here $\mathsf{c}(\varphi_i) = -\varphi_i$ for $i \geq 1$, and these factors need not lie in L_p; so we apply (F2) to them in L_{5p}, and to φ_0 in F^+. Then (F3) and (F1), as in Step 4 of that proof, give $\varphi_i = \upsilon_0 \mu_i^5$ $(0 \leq i \leq 4)$ with υ_0 a unit of F^+, $\mu_0 \in \mathcal{O}_{F^+}$ and $\mu_i \in \mathcal{O}_{L_{5p}}$. Now $\varphi_i \varphi_{5-i} = S^2/N_i - \rho_1 \bar{\rho}_1$, so $\varphi_1 \varphi_4 - \varphi_2 \varphi_3 = (1/N_1 - 1/N_2) S^2$.

Put $X_1 = \mu_1\mu_4$, $Y_1 = -\mu_2\mu_3$ and $Z_1 = \mu_0^2$; as $X_1^5, Y_1^5 \in L^{++}$, (F6) lets us multiply μ_4 and μ_3 by powers of ξ so that $X_1, Y_1 \in \mathcal{O}_{L^{++}}$. Dividing by υ_0^2 and inserting $S = 5^{5n-1}\varepsilon_0\upsilon_0\mu_0^5$ gives

$$X_1^5 + Y_1^5 = \varepsilon_1\pi_q^N Z_1^5, \qquad N = 2(4(5n-1)-1) \geq 30, \qquad \varepsilon_1 = \upsilon_{12}(5/\pi_q^4)^{2(5n-1)}\varepsilon_0^2,$$

a solution of the equation of Theorem 4.5 with $M = 0$ (its other hypotheses hold as in Step 5 of that proof). This contradicts Theorem 4.5.

Step 3: the case $p \mid z$, for $p \not\equiv 1 \pmod 5$. Then $\langle p \bmod 5\rangle$ is a nontrivial subgroup of the cyclic group $(\mathbb{Z}/5)^\times$, so it contains -1. As ζ^c is the fifth power of a p-th root of unity, we may absorb it into ρ_0 and write $\alpha = \varepsilon^+\rho^5$. From $\alpha = (x+y)/(1-\zeta) - y$ we get $\alpha - \bar\alpha = -(x+y)(\zeta^r + \zeta^{-r})/(\zeta^r - \zeta^{-r})$, so

$$\rho^5 - \bar\rho^5 = -p^{5m-1}5^{5n}C^5\varepsilon_0/(\zeta^r - \zeta^{-r}), \qquad \varepsilon_0 = (\zeta^r + \zeta^{-r})/\varepsilon^+.$$

With $S = \rho - \bar\rho$, the argument of Step 2 gives $v_{\mathfrak{Q}}(S) = 4(5n-1)$, and $v_{\mathfrak{P}}(S) = (p-1)(5m-1)-1$ at the primes $\mathfrak{P}$ above p (F4). The factors $\varphi_i = (\xi^i\rho - \xi^{-i}\bar\rho)/(\xi^i - \xi^{-i})$, $1 \leq i \leq 4$, now fixed by c, and $\varphi_0 = -S(\zeta^r - \zeta^{-r})/(p^{5m-1}5^{5n-1}\varepsilon_0) \in F^+$ are integral, prime to $5p$, pairwise coprime, with product C^5. As in Step 2, with the real units p/π_p^{p-1} and $(\zeta^r - \zeta^{-r})/\pi_p$ absorbed into the unit, this gives a solution of the equation of Theorem 4.5 with $N = 2(4(5n-1)-1)$ and $M = 2((p-1)(5m-1)-1) > 0$. As $-1 \in \langle p \bmod 5\rangle$, Theorem 4.5 excludes it. □

For $p > 3$, part (b) is what [57, Theorems 7 and 8] state at $q = 5$ (Theorem 7 with $f = 1$, as noted at the start of Section 4.2). As stated, Mihăilescu's Theorem 2 and Propositions 9 and 11 at $q = 5$ [57] (Theorem 2 assumes $5 \nmid h^-(\mathbb{Q}(\zeta_p))$, which follows from $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$ by (F1)) give, together with part (b), Theorem 4.1 except for the primes $p \equiv 19, 22, 23 \pmod{25}$. Indeed, in case (C) with $5 \nmid c$, Theorem 2 gives $a \equiv b \pmod{25}$, as $f = 1$ would give $5 \mid c$ and $f = 0$ would give $25 \mid ab$. Then Proposition 9 ($p \nmid c$) requires $2^4 \equiv 1 \pmod{25}$, which is false, and Proposition 11 ($p \mid c$) requires $(2^{p-1}p^p)^4 \equiv 1 \pmod{25}$, which for $p \not\equiv 1 \pmod 5$ holds exactly when $p \equiv 19, 22, 23 \pmod{25}$. Below 1000 the primes in these classes that satisfy the hypotheses of Theorem 4.1 are $p = 19, 23, 397, 419, 547, 647, 719$. The proofs of these three statements, in [57, §§3–7], do not use his descent [57, Theorems 6–8], to which the three points of Section 4.2 belong.

5. The quotient curve and the CM point

From here to Section 9, $p \geq 7$ is a prime with $p \not\equiv 1 \pmod 5$. Class (d) is treated with a second Frey object, a curve of genus $2(p-1)$ whose Jacobian has multiplication by the ring of integers of $M' = \mathbb{Q}(\zeta_5, \zeta_p + \zeta_p^{-1})$. The trivial solution $(1, 0, 1)$ gives a curve with complex multiplication by $\mathbb{Z}[\zeta_{5p}]$, the *CM point*, and a class-(d) solution gives a curve that is close to it at 2, 5 and p. This section constructs both curves and the comparison between their 5-adic Tate modules modulo $1 - \zeta_5$, and proves the local and global facts about them that the criterion of Section 7 uses.

The argument for class (d). Let (a, b, c) be a class-(d) solution, labeled so that $10p \mid b$, and let T' and T_0 be the 5-adic Tate modules of $\operatorname{Jac} D_{\mathrm{sol}}$ and of the CM point $\operatorname{Jac} D_0$ (Section 5.3). They agree modulo $\varpi = 1 - \zeta_5$ through the residual identification ι_{can} (Section 5.4), which lifts to an isometry $\varphi\colon T' \to T_0$ (Lemma 5.12). Theorem 7.2 improves φ one power of ϖ at a time. At the first power where φ fails to commute with G_K, the failure is a class in H^1 of a graded piece W or Θ of the polarized adjoint of T_0 (Proposition 6.4), and this class lies in a Selmer group: it is unramified away from 5 and p by Lemma 5.7, and at p by Proposition 5.5; at 5 it lies in the local condition of Definition 6.5 by Section 8 (by Lemma 7.1 at the second

power); and the real places impose no condition, as H^1 of a group of order 2 with 5-primary coefficients is 0. When $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$ the Selmer groups vanish (Corollary 6.14), so the induction never stops and gives $T' \cong T_0$ as G_K-modules. Proposition 5.11 excludes this through the Frobenius at a prime dividing $(a^p + b^p)/(a + b)$, and the proof of Theorem 9.2 assembles the steps.

5.1. **Fields.** Fix $\zeta_5, \zeta_p \in \overline{\mathbb{Q}}$ and put $\zeta_{5p} = \zeta_5\zeta_p$. Let $M = \mathbb{Q}(\zeta_{5p})$ and, for $t \in (\mathbb{Z}/5p)^\times$, let $\sigma_t \in \mathrm{Gal}(M/\mathbb{Q})$ be $\zeta_{5p} \mapsto \zeta_{5p}^t$; $\mathsf{c} = \sigma_{-1}$ is complex conjugation. Let m be the class with $m \equiv 1 \pmod 5$ and $m \equiv -1 \pmod p$, and put

$$M' = M^{\sigma_m} = \mathbb{Q}(\zeta_5, \zeta_p + \zeta_p^{-1}), \qquad L = M^{\sigma_m \mathsf{c}} = \mathbb{Q}(\sqrt{5}, \zeta_p), \qquad L^+ = L^{\mathsf{c}} = \mathbb{Q}(\sqrt{5}, \zeta_p + \zeta_p^{-1}).$$

L and M' are CM fields with common maximal real subfield L^+, and both contain K. Let f be the order of 5 in $(\mathbb{Z}/p)^\times$ and $g = (p-1)/f$; then 5 splits into g primes in $\mathbb{Q}(\zeta_p)$, unramified, and $M \otimes \mathbb{Q}_5$ is a product of g fields, each totally ramified of degree 4 over $\mathbb{Q}_{5^f}$. Put $\varpi = 1 - \zeta_5$: it is a uniformizer at every prime of M, M' above 5 (the primes of M above 5 are unramified over M'), and $5 = \varpi^4 \cdot (\text{unit})$. If $p \equiv \pm 2 \pmod 5$, then f is even: 5 is not a square modulo p, as $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1$, so $f \nmid (p-1)/2$.

5.2. **The curves.** For $t \neq 0, 1$ put $T = t(1-t)$ and let C_t' be the smooth projective curve

$$C_t' \colon y^{5p} = T^{5(p+1)/2}\, x^{3p+5}(1-x)^{2p}(1-tx)^{3p-5},$$

with μ_{5p} acting by $y \mapsto \zeta y$. It is the twist, by the Kummer character of $T^{(p+1)/2p}$, of $C_t \colon y^{5p} = x^{3p+5}(1-x)^{2p}(1-tx)^{3p-5}$, a cyclic cover of the line branched at $0, 1, 1/t, \infty$ with exponents $3p+5$, $2p$, $3p-5$, $-8p$. These exponents do two things. First, as $A + B \equiv 5$, $B + C \equiv -5$ and $A + C \equiv p \pmod{5p}$ for $(A, B, C, D) = (3p+5, 2p, 3p-5, -8p)$, the part of H^1 on which μ_{5p} acts through primitive characters has local monodromies of orders p, p and, projectively, 5 at $t = 0, 1, \infty$ (the local exponents are computed in Lemma 5.8), so that $t_0 = a^p/c^5$ gives a Frey object for (1.1). Second, as $mA \equiv C$ and $mB \equiv D \pmod{5p}$, the involution $x \mapsto (tx-1)/(t(x-1))$, which exchanges 0 with $1/t$ and 1 with ∞, lifts to an involution of the cover inducing σ_m on μ_{5p}. On C_t that lift is defined only over $\mathbb{Q}(t, W)$ with $W^p = 1/T$; after the twist by $T^{(p+1)/2p}$ exactly one of its μ_p-conjugates, Σ', is defined over $\mathbb{Q}(t)$. The new parts of the Jacobians of such covers are the hypergeometric abelian varieties of Cohen and Wolfart [18, §3]; Darmon uses them to construct Frey representations attached to triangle groups [21, §1]. The involution Σ' of the twisted cover C_t' (Proposition 5.1(a)) is of the kind constructed in [38, §9], and on x it is the involution [38, (75)] (with $z = t$). Quotients of such covers by an involution that inverts the action of a group of roots of unity appear in [71, Proposition 3] and [21, pp. 422–423]. The curve has genus $4p$. Its *new part* N_t is the abelian subvariety cut out by the idempotent $e = \prod_{q \in \{5,p\}}(1 - q^{-1}\sum_{\zeta \in \mu_q}[\zeta])$ of $\mathbb{Q}[\mu_{5p}]$. The new part N_t has dimension $4(p-1)$, $\mathbb{Q}[\mu_{5p}]e \cong M$, and each primitive character of μ_{5p} occurs in $H^1(N_t)$ with multiplicity 2. Indeed, for a primitive χ none of the four exponents is $\equiv 0 \pmod{5p}$, so the χ-part of $H^1(C_t')$ has dimension $4 - 2 = 2$ (compare [18, §3, p. 100]).

Proposition 5.1 (the quotient curve)**.** *Let $p \geq 7$, $p \not\equiv 1 \pmod 5$.*

(a) C'_t has an involution Σ', defined over $\mathbb{Q}(t)$, with $\Sigma'[\zeta]\Sigma'^{-1} = [\zeta^m]$ for $\zeta \in \mu_{5p}$ (compare [21, p. 422]*).*

(b) The quotient $C'_t/\langle\Sigma'\rangle$ has genus $2(p-1)$, and with $t = 1/(1+u^p)$ it is birational over $\mathbb{Q}(u)$ to

$$D_u\colon Y^5 = (1+u^p)^4 F_u(R), \qquad F_u(R) = \prod_{j\in\mathbb{Z}/p} (R - \zeta_p^j + u\zeta_p^{-j}) = D_p(R,-u) - 1 + u^p,$$

where, for an integer $n \geq 1$, $D_n(R,\alpha)$ is the Dickson polynomial of degree n, $D_n(z+\alpha/z,\alpha) = z^n + \alpha^n/z^n$.

(c) The quotient map $q\colon C'_t \to C'_t/\langle\Sigma'\rangle$ induces an isogeny over $\mathbb{Q}(t)$ from $\mathrm{Jac}(C'_t/\langle\Sigma'\rangle)$ onto the Σ'-invariant part B_t of N_t, and $V_\ell(\mathrm{Jac}(C'_t/\langle\Sigma'\rangle)) \cong V_\ell(N_t)^{\Sigma'=1}$ for every prime ℓ.

(d) At $u = 0$ the curve is $D_0\colon Y^5 = R^p - 1$. At a solution (a,b,c), with $u_0 = b/a$ and $t_0 = a^p/c^5$, the curve D_{u_0} is isomorphic over $\mathbb{Q}$ to

$$D_{\mathrm{sol}}\colon Y^5 = D_p(R,-ab) - a^p + b^p = \prod_{j\in\mathbb{Z}/p} (R - a\zeta_p^j + b\zeta_p^{-j}),$$

and C'_{t_0} is isomorphic over $\mathbb{Q}$, μ_{5p}-equivariantly, to

$$C'\colon Y^{5p} = x^{3p+5}(1-x)^{2p}(c^5 - a^p x)^{3p-5}.$$

Proof. Fix integers r_1, r_2 with $5r_1 - pr_2 = 1$. On C'_t put $v' = y^5/(x^3(1-x)^2(1-tx)^3)$ and $X = x/(1-tx)$; then $v'^p = (T^{(p+1)/2}X)^5$, and $\hat w = v'^{r_1}(T^{(p+1)/2}X)^{-r_2}$ satisfies $\hat w^p = T^{(p+1)/2}X$ and $v' = \hat w^5$. With $Z = (y/\hat w)(1+tX)^2$, as $\hat w^5 = v'$, one has $Z^5 = x^3(1-x)^2(1-tx)^3(1+tX)^{10}$, which the substitutions $x = X/(1+tX)$, $1-x = (1-(1-t)X)/(1+tX)$ and $1-tx = 1/(1+tX)$ turn into $X^3(1-(1-t)X)^2(1+tX)^2$; with $X = T^{-(p+1)/2}\hat w^p$ this gives

$$C'_t \cong \{Z^5 = T^{-3(p+1)/2}\hat w^{3p}(1 - \hat w^p/\beta_1)^2(1 - \hat w^p/\beta_2)^2\},$$

where $\beta_1 = T^{(p+1)/2}/(1-t)$ and $\beta_2 = -T^{(p+1)/2}/t$, so that $\beta_1\beta_2 = -T^p$, with μ_5 acting by $Z \mapsto \zeta_5 Z$ and μ_p by $\hat w \mapsto \zeta_p \hat w$. Let $\kappa = -T$, so $\kappa^p = \beta_1\beta_2$. The map $\Sigma'(\hat w, Z) = (\kappa/\hat w, \kappa^p Z/\hat w^{2p})$ preserves the equation, since $\hat w \mapsto \kappa/\hat w$ exchanges the factors $1 - \hat w^p/\beta_1$ and $1 - \hat w^p/\beta_2$ up to the factors $-\beta_2/\hat w^p$ and $-\beta_1/\hat w^p$. It is an involution defined over $\mathbb{Q}(t)$ that commutes with μ_5 and inverts μ_p, which is (a); on X it induces $X \mapsto -1/(TX)$. The functions $r = \hat w + \kappa/\hat w$ and $Y = Z/\hat w^p$ generate the function field of the quotient $D_t = C'_t/\langle\Sigma'\rangle$. Since $\hat w^p + \kappa^p/\hat w^p = D_p(r,\kappa)$ and $\beta_1 + \beta_2 = (2t-1)T^{(p-1)/2}$, one has $(1 - \hat w^p/\beta_1)(1 - \hat w^p/\beta_2)/\hat w^p = Q_t(r)/(\beta_1\beta_2)$ with $Q_t(r) = D_p(r,-T) - (2t-1)T^{(p-1)/2}$, so $Y^5 = T^{-3(p+1)/2}\big(Q_t(r)/(\beta_1\beta_2)\big)^2 = T^{-3(p+1)/2-2p}Q_t(r)^2$. Replacing Y by $Y^3/Q_t(r)$ gives $Y^5 = T^{-(21p+9)/2}Q_t(r)$, that is, as $-(21p+9)/2 = 9(p-1)/2 - 15p$, $D_t\colon Y^5 = T^{9(p-1)/2}Q_t(r)$ up to fifth powers. The roots of Q_t are distinct for $t \neq 0, 1$ and $\deg Q_t = p$ is prime to 5, so D_t is a μ_5-cover of the line totally ramified over $p+1$ points, of genus $2(p-1)$. With $t = 1/(1+u^p)$ and $\xi = u^{(p-1)/2}/(1+u^p)$ one has $\xi^2 = T/u$ and, by homogeneity of the Dickson polynomial, $Q_t(\xi R) = \xi^p F_u(R)$, which gives (b) after a change of Y by a fifth power. Thus D_u is D_t at $t = 1/(1+u^p)$. The numbers $R_j = \zeta_p^j - u\zeta_p^{-j}$ are the roots of F_u, since $D_p(z - u/z, -u) = z^p - u^p/z^p$.

(c) The group μ_{5p} acts on $H^1(N_t)$ through primitive characters, each with multiplicity 2, and Σ' maps the χ-part to the χ^m-part, $\chi^m \neq \chi$; so Σ' has an invariant subspace of dimension $4(p-1)$ there. On the part of $H^1(C'_t)$ where μ_{5p} acts through characters of order

5, Σ' acts as -1, and no character of order p occurs (the quotient C'_t/μ_5 has genus 0, and by (b) the Σ'-invariants of the new part already have dimension $4(p-1)$, twice the genus of D_t). As q^* identifies $H^1(D_t)$ with $H^1(C'_t)^{\Sigma'}$, (c) follows.

(d) At $u=0$, $F_0 = R^p - 1$. At a solution, $1+u_0^p = c^5/a^p$, and $R = R'/a$ gives $\prod_j(R - \zeta_p^j + u_0\zeta_p^{-j}) = a^{-p}\prod_j(R' - a\zeta_p^j + b\zeta_p^{-j})$; the numbers $R'_j = a\zeta_p^j - b\zeta_p^{-j}$ are the roots of $D_p(R', -ab) - a^p + b^p$, because $R'_j = w - ab/w$ with $w = a\zeta_p^j$. So $Y = c^4a^{-p}Y'$ gives $D_{u_0} \cong D_{\mathrm{sol}}$. Finally, at t_0 one has $1 - t_0 = b^p/c^5$ and $T = (ab)^p/c^{10}$, and the constants $T^{5(p+1)/2}$ and $c^{5(3p-5)}$ of C'_{t_0} and C' differ by the $5p$-th power of $c^8(ab)^{-(p+1)/2}$; so $y \mapsto c^8(ab)^{-(p+1)/2}y$ is the isomorphism. □

We write D_{sol} also for D_{u_0}, and D_t for $C'_t/\langle\Sigma'\rangle$; by (b), D_u is D_t at $t = 1/(1+u^p)$. For any coprime nonzero integers a, c we write $C'\colon Y^{5p} = x^{3p+5}(1-x)^{2p}(c^5 - a^p x)^{3p-5}$; via $Y = c^{(3p-5)/p}y$ it is the twist of C_{t_0}, $t_0 = a^p/c^5$, by the Kummer character of $c^{(3p-5)/p}$, and at a solution it is C'_{t_0} by (d). The roots of $D_p(R, -ab) - a^p + b^p$ satisfy

$$R'_i - R'_j = (\zeta_p^i - \zeta_p^j)(a + b\zeta_p^{-i-j}), \qquad \prod_{k\in\mathbb{Z}/p}(a + b\zeta_p^k) = a^p + b^p = c^5. \tag{5.1}$$

5.3. **Multiplication by $\mathcal{O}_{M'}$.** The automorphism $Z \mapsto \zeta_5 Z$ of C'_t commutes with Σ' and induces on D_u the automorphism $[\zeta_5]\colon Y \mapsto \zeta_5^3 Y$. For $a \in (\mathbb{Z}/p)^\times$ let $\Phi_a = q_* \circ [\zeta_p^a]_* \circ q^* \in \mathrm{End}(\mathrm{Jac}\, D_t)$ (as in [71, §3.1]; the correspondence Z_u below is that of [71, Lemma 7 and p. 1062], with u in place of 1). Then $q^*\Phi_a = ([\zeta_p^a] + [\zeta_p^{-a}])q^*$, so Φ_a is the endomorphism $[\zeta_p^a] + [\zeta_p^{-a}]$ of B_t, and $\zeta_5 \mapsto [\zeta_5]$, $\zeta_p^a + \zeta_p^{-a} \mapsto \Phi_a$ define an action of $\mathcal{O}_{M'} = \mathbb{Z}[\zeta_5] \otimes \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ on $\mathrm{Jac}\, D_u$. In the coordinate R, Φ_1 is the correspondence Z_{u*}, where Z_u is the closure of

$$\{q_u(R,R') = 0,\ Y' = Y\}, \qquad q_u(R,R') = R'^2 - (\zeta_p + \zeta_p^{-1})RR' + R^2 + u(2 - \zeta_p^2 - \zeta_p^{-2}) : \tag{5.2}$$

with $R = z - u/z$, the two roots of $q_u(R,\cdot)$ are $\zeta_p^{\pm1}z - u/(\zeta_p^{\pm1}z)$. The coefficients of q_u lie in $\mathbb{Q}(\zeta_p + \zeta_p^{-1})(u)$, so $\mathcal{O}_{M'}$ acts by endomorphisms defined over $M'(u)$. At $u = 0$ we use the same rule: $[\zeta_5]$ is $Y \mapsto \zeta_5^3 Y$ and $\Phi_a = [\zeta_p^a]_* + [\zeta_p^{-a}]_*$ with $[\zeta_p^a](R, Y) = (\zeta_p^a R, Y)$, the value at $u = 0$ of the same family of correspondences. On $\mathrm{Jac}\, D_0$ the actions of μ_5 and μ_p generate an action of $\mathbb{Z}[\zeta_{5p}] = \mathcal{O}_M$, so $\mathrm{Jac}\, D_0$ has complex multiplication by M, and $\mathcal{O}_{M'} \subset \mathcal{O}_M$ acts as above. An element $g \in G_{\mathbb{Q}}$ acts on these structures semilinearly: $g \circ [\alpha] \circ g^{-1} = [g(\alpha)]$.

For a solution in class (d) put

$$T' = T_5(\mathrm{Jac}\, D_{\mathrm{sol}}), \qquad T_0 = T_5(\mathrm{Jac}\, D_0),$$

with their actions ρ', ρ_0 of G_K. For $u_0 \in \mathbb{Q}$ with $u_0^p \neq -1$ we write likewise $T' = T_5(\mathrm{Jac}\, D_{u_0})$, with ι_{can} (Section 5.4) built from $e_j(u_0) \mapsto e_j(0)$; at a solution, with $u_0 = b/a$, this is the T' above by Proposition 5.1(d). They are modules over $\mathcal{O}_{M'} \otimes \mathbb{Z}_5 = \prod_{\lambda'|5} \mathcal{O}_{M',\lambda'}$, free of rank 2: each component is torsion-free over a discrete valuation ring, and its rank is 2 because V_5 of an abelian variety of dimension $2(p-1)$ with an action of the field M' of degree $2(p-1)$ is free of rank 2 over $M' \otimes \mathbb{Q}_5$ [59, Chapter I, Proposition 10.23]. The group G_K acts $\mathcal{O}_{M'}$-semilinearly. The principal polarizations give perfect alternating Weil pairings, and for the Rosati involution, which is complex conjugation c on $\mathcal{O}_{M'}$, they are the traces of perfect skew-Hermitian forms h', h_0 on T', T_0 with values in the inverse different $\mathfrak{D}^{-1}$ of $\mathcal{O}_{M'} \otimes \mathbb{Z}_5$ (Section 5.9). When we work at one prime λ' of M' above 5, we write $\mathcal{O} = \mathcal{O}_{M',\lambda'}$ and T', T_0 for $T' \otimes_{\mathcal{O}_{M'} \otimes \mathbb{Z}_5} \mathcal{O}$ and $T_0 \otimes \mathcal{O}$.

5.4. **The canonical residual identification.** For u with $u^p \neq -1$ let $P_j(u) = (\zeta_p^j - u\zeta_p^{-j}, 0) \in D_u$, $j \in \mathbb{Z}/p$, let ∞ be the unique point at infinity, and $e_j(u) = [P_j(u) - \infty] \in \mathrm{Jac}(D_u)$.

Let (A, λ) be a principally polarized abelian variety over a field of characteristic 0 with $\mathbb{Z}[\zeta_5] \subset \mathrm{End}\, A$, on which the Rosati involution is complex conjugation c; points are taken over an algebraic closure. Let $e_5 \colon A[5] \times A^\vee[5] \to \mu_5$ be the Weil pairing [59, Chapter I, §13]. The element $\varpi' = 5/\mathsf{c}(\varpi)$ lies in $\mathbb{Z}[\zeta_5]$, and $\varpi' A[5] = A[\mathsf{c}(\varpi)] = A[\varpi]$, because $\mathsf{c}(\varpi)^{-1} T_5 A = 5^{-1}\varpi' T_5 A$ and $\varpi/\mathsf{c}(\varpi) = -\zeta_5$ is a unit; in the same way $\mathsf{c}(\varpi')A[5] = A[\varpi]$. For $P, P' \in A[\varpi]$ put

$$e_\varpi(P, P') = e_5(P, \lambda Q) \qquad \text{for any } Q \in A[5] \text{ with } \varpi' Q = P'. \tag{5.3}$$

This does not depend on Q: if $Q' \in A[5]$ and $\varpi' Q' = 0$, write $P = \mathsf{c}(\varpi')\tilde{P}$ with $\tilde{P} \in A[5]$; then $e_5(P, \lambda Q') = e_5(\tilde{P}, \mathsf{c}(\varpi')^\vee \lambda Q') = e_5(\tilde{P}, \lambda \varpi' Q') = 1$ by [59, Chapter I, Proposition 13.2(a)] (on first components), since $\mathsf{c}(\varpi')^\vee \circ \lambda = \lambda \circ \varpi'$ says that the Rosati involution [59, Chapter I, §14] maps $\mathsf{c}(\varpi')$ to ϖ'.

Lemma 5.2. *Let $u^p \neq -1$.*

(a) The classes $e_j(u)$ lie in $\mathrm{Jac}(D_u)[1-\zeta_5]$, generate it, and satisfy the single relation $\sum_j e_j(u) = 0$; so $\mathrm{Jac}(D_u)[1-\zeta_5]$ has dimension $p-1$ over $\mathbb{F}_5$.

(b) $\Phi_1 e_j(u) = e_{j+1}(u) + e_{j-1}(u)$, $[\zeta_5]e_j(u) = e_j(u)$, and for $u \in \mathbb{Q}$ and $g \in G_\mathbb{Q}$ with $g(\zeta_p) = \zeta_p^a$, $g(e_j(u)) = e_{aj}(u)$.

(c) The pairing $e_\varpi(e_i(u), e_k(u))$ of (5.3), for the principal polarization, does not depend on u.

Hence, for $u \in \mathbb{Q}$, $e_j(u) \mapsto e_j(0)$ is an isomorphism of $\mathcal{O}_{M'}$-semilinear $G_\mathbb{Q}$-modules $\mathrm{Jac}(D_u)[1-\zeta_5] \cong \mathrm{Jac}(D_0)[1-\zeta_5]$, isometric for e_ϖ.

Proof. (a) The points $P_j(u)$ and ∞ are fixed by $[\zeta_5]$, so $e_j(u)$ is killed by $1-\zeta_5$, and $\mathrm{div}(Y) = \sum_j P_j(u) - p\infty$ gives the relation. As $T_5(\mathrm{Jac}\, D_u)$ is free over $\mathbb{Z}_5[\zeta_5]$ of rank $4(p-1)/4 = p-1$, the group $\mathrm{Jac}(D_u)[1-\zeta_5]$ has dimension $p-1$. If $\sum_j n_j e_j(u) = 0$ with $0 \le n_j < 5$, a function h with divisor $\sum_j n_j P_j(u) - (\sum_j n_j)\infty$ is an eigenfunction of $[\zeta_5]$, hence of the form $Y^k r(R)$ with $0 \le k < 5$ and r rational. Comparing orders at the $P_j(u)$ (where Y has a simple zero and $r(R)$ an order divisible by 5) gives $n_j = k$ for all j. So the p classes span a space of dimension $p-1$. (b) On C_t' (coordinates of the proof of Proposition 5.1) the zeros of Z other than $\hat{w} = 0, \infty$ are the points $Q_j = (\xi\zeta_p^j, 0)$ and $\Sigma' Q_j = (-u\xi\zeta_p^{-j}, 0)$, with $\xi = u^{(p-1)/2}/(1+u^p)$ as there (so $\xi^p = \beta_1$ and $\xi^2 = T/u$), and the image of Q_j in D_u is $P_j(u)$. As $[\zeta_p]Q_j = Q_{j+1}$ and $[\zeta_p]\Sigma' Q_j = \Sigma' Q_{j-1}$, and the two points over ∞ are fixed by $[\zeta_p]$ and exchanged by Σ', we get $\Phi_1[P_j(u)] = [P_{j+1}(u)] + [P_{j-1}(u)]$ and $\Phi_1[\infty] = 2[\infty]$; at $u = 0$ this is immediate. The other two statements are clear. (c) Over the u-line $U = \mathbb{A}^1 \smallsetminus \{u^p = -1\}$ over M, which is connected and contains $u = 0$, the group schemes $\mathrm{Jac}[5]$ and $\mathrm{Jac}[\varpi]$ are finite étale, and the second is trivialized by the sections e_j. As the discriminant $\pm p^p(1+u^p)^{p-1}$ of F_u (by (5.1) with $(a,b) = (1,u)$) is a unit on U, Lemma 5.3 makes the family of curves D_u a smooth proper curve over U with the section ∞, so $\mathrm{Jac} \to U$ is an abelian scheme [9, §9.4, Proposition 4], and its principal polarization is defined over U. The Weil pairing e_5 of the principal polarization is defined over U: up to the sign convention, it is the Cartier pairing between the kernels of [5] and of its dual, which for the abelian scheme $\mathrm{Jac} \to U$ is a perfect pairing of finite flat group schemes over U, compatible with base change [61, Theorem 1.1 and Corollary 1.3(ii)]. As

$\varpi'\colon \mathrm{Jac}[5] \to \mathrm{Jac}[\varpi]$ is surjective, (5.3) defines a pairing of group schemes over U, and $e_\varpi(e_i, e_k)\colon U \to \mu_5$ is constant. With (b), the map $e_j(u) \mapsto e_j(0)$ commutes with $G_\mathbb{Q}$, ζ_5 and Φ_1, hence with $\mathcal{O}_{M'} = \mathbb{Z}[\zeta_5, \Phi_1]$. □

Since $\varpi\mathcal{O}_{M'} = \prod_{\lambda'|5} \lambda'$, the lemma identifies the λ'-torsion for every $\lambda' \mid 5$ at once. Multiplication by ϖ^{-1} identifies $T/\varpi T$ with $\mathrm{Jac}[\varpi] \otimes \omega_5$ for $T = T'$, T_0, where ω_5 is the mod-5 cyclotomic character (as $g(\varpi) \equiv \omega_5(g)\varpi \pmod{\varpi^2}$). We call the resulting isomorphism

$$\iota_{\mathrm{can}}\colon T'/\varpi T' \xrightarrow{\sim} T_0/\varpi T_0,$$

the twist by ω_5 of $e_j(u_0) \mapsto e_j(0)$ on both sides, the *residual identification*. It is $\mathcal{O}_{M'}$-linear and G_K-equivariant.

5.5. **Local comparison at p.** At a class-(d) solution, $u_0 = b/a$ is divisible by 2, 5 and p, so D_{u_0} is q-adically close to D_0 for $q \in \{2, 5, p\}$. The two lemmas below are standard: the first gives a smooth proper model of a curve from an affine equation, and the second computes the reduction of an endomorphism given by a correspondence.

Lemma 5.3. *Let A be a ring, $n \geq 1$ an integer prime to 5, $\gamma \in A^\times$, and $f = Y^5 - \gamma X^n - \sum_{(i,j)\in S} a_{ij} X^i Y^j \in A[X, Y]$ with $5i + nj < 5n$ for $(i, j) \in S$. The closure $\mathcal{X}$ of $\{f = 0\}$ in the weighted projective plane $\mathbb{P}_A(5, n, 1)$ (weights $5, n, 1$ for X, Y, Z) is proper over A, and $\mathcal{X} \smallsetminus \{f = 0\}$ is the image of a section ∞ along which $\mathcal{X}$ is smooth of relative dimension 1. So if $\operatorname{Spec} A[X, Y]/(f)$ is smooth over A, then $\mathcal{X}$ is a smooth proper curve over A.*

Proof. Modulo Z the homogenized equation is $Y^5 - \gamma X^n$, and Y^6, X^{n+1} lie in the ideal generated by it, Z and XY; so $\mathcal{X} \subset D_+(Z) \cup D_+(XY)$. The degree-0 monomials on $D_+(XY)$ are generated by $\alpha = Y^5/X^n$, α^{-1} and $\beta = ZX^aY^b$ with $5a + nb = -1$, so $D_+(XY) = \operatorname{Spec} A[\alpha^{\pm 1}, \beta]$, and there the equation reads $\alpha - \gamma - \beta h = 0$, where $h \in A[\alpha^{\pm 1}, \beta]$ collects the terms of S. Its zero set outside $D_+(Z)$ is the section $(\alpha, \beta) = (\gamma, 0)$, along which the derivative in α is 1. □

Lemma 5.4. *Let $\mathcal{O}_F$ be a complete discrete valuation ring with fraction field F and finite residue field k, $\mathcal{X}$ a smooth proper curve over $\mathcal{O}_F$ with geometrically connected fibers and a section ∞, and $\mathcal{J} = \mathrm{Pic}^0_{\mathcal{X}/\mathcal{O}_F}$, an abelian scheme and the Néron model of $A = \mathrm{Jac}\,\mathcal{X}_F$. Every $\alpha \in \mathrm{End}_F(A)$ extends to $\mathcal{J}$; let $\bar\alpha$ be its reduction. If $\gamma_1, \dots, \gamma_d$ are automorphisms of $\bar{\mathcal{X}}$ fixing $\bar\infty$, and every $P \in (\mathcal{X} \smallsetminus \infty)(\mathcal{O}_{F_1})$, F_1/F finite, has $\alpha[P - \infty] = [P_1 + \cdots + P_d - d\infty]$ with integral P_i whose reductions are $\gamma_1(\bar P), \dots, \gamma_d(\bar P)$, then $\bar\alpha = \gamma_{1*} + \cdots + \gamma_{d*}$.*

Proof. The abelian scheme property and the Néron property are [9, §9.4, Proposition 4 and §1.2, Proposition 8]. Reduction sends $[P - \infty]$ to $[\bar P - \bar\infty]$ and commutes with α; every point of $\bar{\mathcal{X}} \smallsetminus \bar\infty$ lifts to an integral point over an unramified extension [9, §2.3, Proposition 5], and the classes $[\bar P - \bar\infty]$ generate $\mathrm{Jac}(\bar{\mathcal{X}})(\bar k)$. □

Proposition 5.5 (local comparison)**.** *Let $p \geq 7$, $p \not\equiv 1 \pmod 5$. For $u \in p\mathbb{Z}_p$ and every prime $\ell \neq p$, $T_\ell(\mathrm{Jac}\, D_u) \cong T_\ell(\mathrm{Jac}\, D_0)$ as $\mathcal{O}_{M'}$-semilinear $\mathbb{Z}_\ell[G_{\mathbb{Q}_p}]$-modules, compatibly with the Weil pairings.*

Proof. Let $\pi = \zeta_p - 1$ and v the valuation with $v(p) = 1$. Write $F_u(R) = (R^p - 1) + \sum_{i=1}^{(p-1)/2} d_i u^i R^{p-2i} + u^p$, where $d_i = p\binom{p-i}{i}/(p-i) \in p\mathbb{Z}$, and put $P_u(V) = \pi^{-p} F_u(1 + \pi V)$. The part $\pi^{-p}((1 + \pi V)^p - 1)$ is monic of degree p, with V-coefficient $p\pi^{1-p} \equiv -1 \pmod \pi$ and other coefficients of positive valuation. The terms $\pi^{-p} d_i u^i (1 + \pi V)^{p-2i}$ have valuation at least $i\,v(u) - 1/(p-1) > 0$, and the constant term $\pi^{-p} u^p$ has valuation $p(v(u) - 1/(p-1)) > 0$.

So P_u is monic and integral and $P_u \equiv V^p - V \pmod{\pi}$ for $u \in p\mathbb{Z}_p$. With ϵ the principal fifth root of the principal unit $1+u^p$ and $Y = \pi^{p/5}\epsilon^4 Y''$, D_u becomes $Y''^5 = P_u(V)$ over $F_\pi = \mathbb{Q}_p(\zeta_p, \pi^{1/5})$, with special fiber the smooth curve $Y''^5 = V^p - V$ of genus $2(p-1)$, the same for every $u \in p\mathbb{Z}_p$; and $g \in G_{\mathbb{Q}_p}$ acts on the model by $V \mapsto (\pi/g(\pi))V$, $Y'' \mapsto (\pi^{1/5}/g(\pi^{1/5}))^p Y''$, formulas that do not involve u. The endomorphisms Φ_a extend to the abelian scheme over $\mathcal{O}_{F_\pi}$, and $[\zeta_5]$, which is defined over the unramified extension $F_\pi(\zeta_5)$ of F_π (as $\zeta_5 \notin F_\pi$), extends over its integers as $Y'' \mapsto \zeta_5^3 Y''$. Their reductions do not depend on u. Indeed, over $\mathcal{O}_{F_\pi}[[w]]$ with $u = \pi w$ the family is smooth and proper with constant special fiber (after $V \mapsto V - w$), the Φ_a extend over the normal base [28, Chapter I, Proposition 2.7], and endomorphisms of a constant abelian scheme over the connected base $\operatorname{Spec}\mathbb{F}_p[[w]]$ are constant [60, Proposition 6.1]. At $w = 0$, Φ_a reduces to $\sigma_*^a + \sigma_*^{-a}$ with $\sigma(V, Y'') = (V+1, Y'')$. Specialization through the abelian scheme then identifies $T_\ell(\operatorname{Jac} D_u)$ with T_ℓ of the special fiber, $G_{\mathbb{Q}_p}$-equivariantly for the reduced descent data, linearly for the reductions of $[\zeta_5]$ and Φ_a, and isometrically, as the Weil pairings are pairings of finite flat group schemes over the base [61, Theorem 1.1 and Corollary 1.3(ii)]. None of these data depends on u, so we compose with the inverse for $u = 0$. □

5.6. **The curve C' at the primes dividing c.** At a class-(d) solution, a and c are prime to $10p$. The curve C' depends only on a and c, and we compute its reduction at the primes dividing c from a semistable model.

Proposition 5.6. *Let a, c be coprime nonzero integers, $\ell \mid c$ a prime with $\ell \nmid 5p$, $\lambda \mid \ell$ a prime of M, $\mathcal{O}_\lambda$ the ring of integers of M_λ (unramified over $\mathbb{Z}_\ell$) and $k = \mathcal{O}_\lambda/\ell$.*

(a) C' has a semistable model over $\mathcal{O}_\lambda$ whose special fiber consists of a curve $\tilde{B}$ of genus $2p$, the smooth model of $y^{5p} = \bar{a}^{2p^2} X^{3p+5}(1-X)^{3p-5}$, and p curves $C_{\bar{z}}$ of genus 2, the smooth models of $Y^5 = \bar{z}W^6(1-W)^2$ for the p roots $\bar{z} \in k$ of $\bar{z}^p = \bar{a}^{p(3p-5)}$, each meeting $\tilde{B}$ in one ordinary double point; the dual graph is a tree. Hence $\operatorname{Jac} C'$ has good reduction at λ, with special fiber $\operatorname{Jac}\tilde{B} \times \prod_{\bar{z}} \operatorname{Jac} C_{\bar{z}}$, μ_{5p}-equivariantly.

(b) For every prime $r \neq \ell$ and every embedding ι of $M \otimes \mathbb{Q}_r$ into $\overline{\mathbb{Q}}_r$, the ι-part of $e \cdot V_r(\operatorname{Jac} C') \otimes \overline{\mathbb{Q}}_r$ has dimension 2 and is the sum of two lines stable under $\operatorname{Frob}_\lambda$, coming from $\tilde{B}$ and from the $C_{\bar{z}}$; on the second, $\operatorname{Frob}_\lambda$ acts by $\iota(\gamma)$ with $\gamma \in \mathbb{Q}(\zeta_5)$. So $P_{\mathrm{new}}(X) = \det(X - \operatorname{Frob}_\lambda \mid e \cdot V_r(\operatorname{Jac} C')) \in \mathbb{Z}[X]$ has a root in $\mathbb{Q}(\zeta_5)$.

Proof. (a) Write C' as $y^{5p} = X^{3p+5}(1-X)^{3p-5}(a^p - c^5X)^{2p}$ via $x = c^5X/a^p$, $Y = c^6 a^{-(p+1)} y$. Let $\alpha = c^5/a^p$ and let $\mathcal{P} \subset \mathbb{P}^1(X) \times \mathbb{P}^1(W)$ over $\mathcal{O}_\lambda$ be the closure of the graph of $W = \alpha X$; its special fiber is two lines $P_B = \{W = 0\}$ and $P_M = \{1/X = 0\}$ meeting at one point, with complete local ring $\mathcal{O}_\lambda[[s, W]]/(sW - \alpha)$, $s = 1/X$. Let $\mathcal{X}$ be the normalization of $\mathcal{P}$ in the function field of C'. Over P_B away from the node, y^{5p} equals $X^{3p+5}(1-X)^{3p-5}$ times a unit, and the exponents $3p \pm 5$ are prime to $5p$; this gives $\tilde{B}$, smooth. Over P_M away from the node, in the coordinate W, $Y^{5p} = W^{3p+5}(c^5 - a^pW)^{3p-5}(1-W)^{2p}$ and $c^5 - a^pW = -a^pW(1 - \alpha/W)$, so $Y^{5p} = (W^6(1-W)^2)^p u_M$ with u_M a unit with residue $\bar{a}^{p(3p-5)}$; with $z = Y^5/(W^6(1-W)^2)$, $z^p = u_M$ is étale and $Y^5 = zW^6(1-W)^2$ gives the p curves $C_{\bar{z}}$, smooth (exponents $6, 2, -8$ prime to 5). At the node, $a^p - c^5X = a^p(1-W)$ and $1 - X = -X(1-s)$, so $h_N = y^5 s^6$ satisfies $h_N^p = a^{2p^2}(1-s)^{3p-5}(1-W)^{2p}$, a unit of $\mathcal{O}_\lambda[[s, W]]/(sW - \alpha)$; as $\mu_p \subset \mathcal{O}_\lambda$, the p roots h_N give p branches of $\mathcal{X}$ above the node. Let $\mathcal{O}' = \mathcal{O}_\lambda[a^{1/5}]$, unramified as $\ell \nmid 5a$. The residue of h_N at the node is $\zeta\bar{a}^{2p}$ with $\zeta \in \mu_p$, a fifth power in the residue field of $\mathcal{O}'$, so by Hensel's lemma h_N has a fifth root $h_N^{1/5}$ on each

branch over $\mathcal{O}'$. Put $\vartheta_1 = (X/y)h_N^{1/5}$ and $\vartheta_1' = (Y/W)h_N^{-1/5}$. As $X = 1/s$, $W = \alpha X$ and $Y = c^6 a^{-(p+1)} y$, they satisfy $\vartheta_1^5 = s$, $\vartheta_1'^5 = a^{p-5}W$ and $\vartheta_1\vartheta_1' = (X/W)(Y/y) = c/a$. So each branch is $\mathcal{O}'[[\vartheta_1, \vartheta_1']]/(\vartheta_1\vartheta_1' - c/a)$, which is normal and of degree 5 over $\mathcal{O}'[[s, W]]/(sW - \alpha)$ (the p branches account for the degree $5p$ of the cover), with $\vartheta_1' = 0$ over P_B and $\vartheta_1 = 0$ over P_M. As $z = a^{p-5}h_N(1-W)^{-2}$, the branch on which $h_N \equiv \zeta\bar{a}^{2p}$ meets $C_{\bar{z}}$ for $\bar{z} = \zeta\bar{a}^{3p-5}$. Above the node there are therefore p ordinary double points of thickness $v_\ell(c)$, one on each $C_{\bar{z}}$, and as semistability descends along the unramified extension, $\mathcal{X}$ is semistable over $\mathcal{O}_\lambda$ itself. The dual graph is therefore a star: one vertex for $\tilde{B}$, one for each of the p curves $C_{\bar{z}}$, and one edge from $\tilde{B}$ to each $C_{\bar{z}}$. It has $p+1$ vertices and p edges, so it is a tree, and the arithmetic genus of the special fiber,

$$g(\tilde{B}) + \sum_{\bar{z}} g(C_{\bar{z}}) + (p - (p+1) + 1) = 2p + p \cdot 2 + 0 = 4p,$$

equals the genus of C'. If $n = v_\ell(c) > 1$, the nodes are A_{n-1} singularities of $\mathcal{X}$; the minimal desingularization $\mathcal{X}' \to \mathcal{X}$ replaces each by a chain of $n-1$ projective lines [54, §10.3.2], so $\mathcal{X}'$ is regular and semistable, and its dual graph is a subdivision of that of $\mathcal{X}$. If $n = 1$, $\mathcal{X}$ is regular, and we put $\mathcal{X}' = \mathcal{X}$. The dual graph of $\mathcal{X}'$ is a subdivided star, a tree, so by [9, §9.5, Theorem 4] ($\mathcal{X}'$ regular, proper and flat, with reduced special fiber) $\mathrm{Pic}^0_{\mathcal{X}'/\mathcal{O}_\lambda}$ is the identity component of the Néron model, and by [9, §9.2, Example 8] its special fiber is the product of the Jacobians of the components (the inserted lines contribute nothing), an abelian variety: good reduction. By [67, §1] the reduction is compatible with the action of μ_{5p} (the automorphisms of $\mathcal{X}$ lift to $\mathcal{X}'$, as the minimal desingularization is unique) and identifies Frob_λ with the product of the Frobenius endomorphisms of the components. (b) For an abelian variety A over a field, a number field $F \subset \mathrm{End}^0(A)$ and a prime r different from the characteristic, $V_r(A)$ is free over $F \otimes \mathbb{Q}_r$ [59, Chapter I, Proposition 10.23], and the characteristic polynomial over $F \otimes \mathbb{Q}_r$ of an endomorphism α commuting with F has coefficients in F: for $f \in F$ and $k \geq 0$ the trace of $f\alpha^k$ on $V_r(A)$ over $\mathbb{Q}_r$ is rational, as $f\alpha^k \in \mathrm{End}^0(A)$, and it equals $\mathrm{Tr}_{F\otimes\mathbb{Q}_r/\mathbb{Q}_r}(fs_k)$, where s_k is the trace of α^k over $F \otimes \mathbb{Q}_r$; so $s_k \in F$ by the nondegeneracy of the trace form of $F/\mathbb{Q}$, and Newton's identities give the coefficients. Counting dimensions of invariants under μ_5 and μ_p ($\tilde{B}/\mu_p$ has genus 2, $\tilde{B}/\mu_5$ genus 0; μ_p permutes the $C_{\bar{z}}$ simply transitively and $C_{\bar{z}}/\mu_5 \cong \mathbb{P}^1$), each primitive ι-part of $e \cdot V_r(\mathrm{Jac}\,\tilde{B})$ and of $e \cdot V_r(\prod \mathrm{Jac}\, C_{\bar{z}})$ has dimension 1. On $\mathrm{Jac}\, C_{\bar{z}}$ the field $\mathbb{Q}(\zeta_5)$ acts through μ_5, and V_r is free of rank one over $\mathbb{Q}(\zeta_5) \otimes \mathbb{Q}_r$; so the Frobenius endomorphism of $C_{\bar{z}}$, which commutes with μ_5 (defined over k), lies in $\mathbb{Q}(\zeta_5)$, and it is the same element γ for every $\bar{z}$ because μ_p, also defined over k, permutes the $C_{\bar{z}}$. Its eigenvalue on the second line is therefore $\iota(\gamma)$. As P_{new} has rational coefficients and vanishes at $\iota(\gamma)$, it vanishes at γ. □

Lemma 5.7 (ramification)**.** *Let (a, b, c) be a solution with $10p \mid abc$. Then T' and T_0 are unramified at every prime $\ell \notin \{5, p\}$.*

Proof. The roots R_j' of $D_p(R, -ab) - a^p + b^p$, a monic polynomial in $\mathbb{Z}[R]$, are distinct modulo every prime of $\mathbb{Z}[\zeta_p]$ not dividing pc, by (5.1). So if $\ell \nmid 5pc$ (this includes $\ell = 2$: c is odd, as $2 \mid ab$), D_{sol} is a μ_5-cover of the line with $p+1$ distinct branch points modulo ℓ, tamely ramified, and has good reduction at ℓ (as in Lemma 5.3). If $\ell \mid c$, then $\ell \nmid 10p$, and by Proposition 5.6(a) inertia at ℓ, which lies in G_{M_λ} as $M_\lambda/\mathbb{Q}_\ell$ is unramified, acts trivially on $V_r(\mathrm{Jac}\, C')$ for $r \neq \ell$; by Proposition 5.1(c),(d), $V_r(\mathrm{Jac}\, D_{\mathrm{sol}})$ is a $G_\mathbb{Q}$-stable subquotient of it. Take $r = 5$. The curve D_0 has good reduction away from $5p$, as the discriminant of $R^p - 1$ is $\pm p^p$. □

5.7. **Determinants.** For a field $F \supseteq M$, $\delta \in F^\times$ and $g \in G_F$ write $\kappa_\delta(g) = g(\delta^{1/p})/\delta^{1/p} \in \mu_p \subset M^\times$ for the Kummer character of δ.

Lemma 5.8 (local exponents and twists)**.** *Let $(A, B, C) = (3p + 5, 2p, 3p - 5)$, let χ be a primitive character of μ_{5p} with $\chi(\zeta_{5p}) = e^{2\pi ik/5p}$, $1 \le k < 5p$, and let $C_t\colon y^{5p} = x^A(1-x)^B(1-tx)^C$.*

(a) Up to duality, the χ-part of $H^1(C_t)$ over $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ is the local system of solutions of $t(1-t)w'' + (\gamma - (\alpha+\beta+1)t)w' - \alpha\beta w = 0$, where $\alpha = kC/5p$, $\beta = 1 - kA/5p$ and $\gamma = 2 - k(A+B)/5p$. Its local exponents are $\{0, 1-\gamma\}$ at 0, $\{0, \gamma-\alpha-\beta\}$ at 1 and $\{\alpha, \beta\}$ at ∞, and the determinants of its local monodromies are $e^{2\pi ik/p}$, $e^{2\pi ik/p}$ and $e^{-4\pi ik/p}$.

(b) Let μ_{5p} act on Jacobians by push-forward, and identify $\mathbb{Q}[\mu_{5p}]e$ with M by $[\zeta] \mapsto \zeta$. Let $F \supseteq M$ be a field, $\Gamma\colon y^{5p} = f(x)$ a curve over F with $[\zeta]\colon y \mapsto \zeta y$ such that $e \cdot V_r(\operatorname{Jac}\Gamma)$ is free of rank 2 over $M \otimes \mathbb{Q}_r$ (as for C_t, by (a)), ρ the action of G_F on $V_r(\operatorname{Jac}\Gamma)$, $\delta \in F^\times$, and $\Gamma^\delta\colon y^{5p} = \delta^5 f(x)$, the twist of Γ by $\delta^{1/p}$. Then $\tau_\delta(x, y) = (x, \delta^{-1/p}y)$ satisfies $\tau_\delta(g(P)) = [\kappa_\delta(g)]\, g(\tau_\delta(P))$ for $g \in G_F$, so $\tau_{\delta *}$ identifies $e \cdot V_r(\operatorname{Jac}\Gamma^\delta)$ with $e \cdot V_r(\operatorname{Jac}\Gamma)$, on which g acts by $\kappa_\delta(g)\rho(g)$, and the determinant over $M \otimes \mathbb{Q}_r$ is multiplied by κ_δ^2.

Proof. (a) By Euler's integral representation, the periods of dx/y^k on C_t satisfy this equation and span its solutions [18, §3, p. 99 and (6)], applied to the exponents (kA, kB, kC). For $k \ne 1$ this is the classical Euler–Pochhammer representation, and the periods span the solutions as none of α, β, $\gamma-\alpha$, $\gamma-\beta$ is an integer. As $[\zeta]^*(dx/y^k) = \zeta^{-k}dx/y^k$, this local system is the χ-part up to duality. The exponents are the roots of the indicial equations $X(X-1+\gamma) = 0$, $X(X+\alpha+\beta-\gamma) = 0$ and $(X-\alpha)(X-\beta) = 0$ at 0, 1 and ∞. The determinant of the monodromy is that of the Wronskian $t^{-\gamma}(1-t)^{\gamma-\alpha-\beta-1}$, so the local determinants are $e^{2\pi i(1-\gamma)}$, $e^{2\pi i(\gamma-\alpha-\beta)}$ and $e^{2\pi i(\alpha+\beta)}$; as $A+B = 5p+5$, $B+C = 5p-5$ and $C-A = -10$, these are $e^{2\pi ik/p}$, $e^{2\pi ik/p}$ and $e^{-4\pi ik/p}$. (b) Applying g to the coefficients of τ_δ gives $g\tau_\delta g^{-1} = [\kappa_\delta(g)]^{-1} \circ \tau_\delta$, which is the first claim. On $e \cdot V_r$, free of rank 2 over $M \otimes \mathbb{Q}_r$, $[\kappa_\delta(g)]$ acts as the scalar $\kappa_\delta(g) \in \mu_p \subset M$, which commutes with $\rho(g)$ for $g \in G_F$. □

Lemma 5.9 (determinants)**.** *(a) For every prime r, the determinant over $M \otimes \mathbb{Q}_r$ of $e \cdot V_r(\operatorname{Jac} C_t')$, a character of $G_{M(t)}$, is the inflation of a character $\det_*$ of G_M.*

(b) For every $u_0 \in \mathbb{Q}$ with $u_0^p \ne -1$, $\det_{M'\otimes\mathbb{Q}_r} V_r(\operatorname{Jac} D_{u_0})$ and $\det_{M'\otimes\mathbb{Q}_r} V_r(\operatorname{Jac} D_0)$ coincide on G_M for every prime r.

Proof. Let χ be a primitive character of μ_{5p}, $\chi(\zeta_{5p}) = e^{2\pi ik/5p}$. By Lemma 5.8(a), the determinant of the χ-part of $H^1(C_t)$ has local monodromy $e^{\pm 2\pi ik/p}$ both at 0 and at 1, one sign for both (that of the duality). As $e^{2\pi ik/p}$ is the image of $\zeta_{5p}^5 \in \mu_p$ under the embedding of M that gives χ, the M-valued determinant of the new part of $H^1(C_t)$ has the same local monodromy $\zeta_{5p}^{\pm 5}$ at 0 and at 1. A local system of rank one on $\mathbb{P}^1_{\bar M} \setminus \{0, 1, \infty\}$ is determined by its local monodromies at 0 and 1, and these are those of a power $\kappa_{t(1-t)}^\varepsilon$ of the Kummer sheaf of $t(1-t)$. The quotient of the determinant by $\kappa_{t(1-t)}^\varepsilon$ is then trivial on the geometric fundamental group, so it factors through G_M. So the M-determinant of the new part of $V_r(\operatorname{Jac} C_t)$ is $\det_* \cdot \kappa_{t(1-t)}^\varepsilon$ for a character $\det_*$ of G_M and some $\varepsilon \in \mathbb{Z}/p$. As C_t' is the twist of C_t by $T^{(p+1)/2p}$, its new part has determinant $\det_* \kappa_{t(1-t)}^{\varepsilon+p+1} = \det_* \kappa_{t(1-t)}^{\varepsilon+1}$ by Lemma 5.8(b).

The value at $u = 0$. By Proposition 5.1(c), $V_r(N_t) \cong V_r(\operatorname{Jac} D_t) \oplus [\zeta_p - \zeta_p^{-1}]V_r(\operatorname{Jac} D_t)$, since $[\zeta_p] - [\zeta_p]^{-1}$ is invertible on $V_r(N_t)$, commutes with $G_{M(t)}$ and anticommutes with Σ';

so $V_r(N_t) \cong V_r(\operatorname{Jac} D_t) \otimes_{M'} M$ as $G_{M(t)}$-modules, and the M-determinant of $V_r(N_t)$ is the M'-determinant of $V_r(\operatorname{Jac} D_t)$. In the variable u, $t(1-t) = u^p(1+u^p)^{-2}$, so $\kappa_{t(1-t)} = \kappa_{1+u^p}^{-2}$, and $\det_{M'} V_r(\operatorname{Jac} D_u) = \det_* \kappa_{1+u^p}^{-2(\varepsilon+1)}$ on $G_{M(u)}$. The family D_u is smooth over the normal connected scheme $U = \operatorname{Spec} M[u, (1+u^p)^{-1}]$, which contains $u = 0$, and both sides are lisse characters on U; specializing at $u = 0$, where $1 + u^p = 1$, gives $\det_* = \det_{M'} V_r(\operatorname{Jac} D_0)$, which is unramified outside $5pr$.

The exponent. For coprime a, c with $a^p \neq c^5$ the curve C' is the twist of C_{t_0}, $t_0 = a^p/c^5$, by $c^{(3p-5)/p}$ (after Proposition 5.1), so its new part has determinant $\det_* \kappa_{t_0(1-t_0)}^{\varepsilon} \kappa_c^{-10}$ (Lemma 5.8(b) with $\delta = c^{3p-5}$), where $t_0(1-t_0) = a^p(c^5 - a^p)c^{-10}$, which gives $\det_* \kappa_{c^5-a^p}^{\varepsilon} \kappa_c^{-10(\varepsilon+1)}$. The number $\varepsilon \in \mathbb{Z}/p$ does not depend on r: it is read off from the local monodromy of the complex local system. So we may take $r \neq 2$. For $(a, c) = (1, 2)$ the determinant is then unramified at the primes above 2 by Proposition 5.6(a) with $\ell = 2$, while $\det_*$ and κ_{31} are unramified there and κ_2 is ramified of order p. Hence $p \mid 10(\varepsilon+1)$, i.e. $\varepsilon = -1$, for every r. This proves (a): the determinant for C'_t is $\det_*$. For (b), $\det_{M'} V_r(\operatorname{Jac} D_u) = \det_*$ on U, and specializing at $u = u_0$ (where $u_0^p \neq -1$) gives $\det_{M'} V_r(\operatorname{Jac} D_{u_0}) = \det_*$. □

5.8. **The non-isomorphism.** The trivial solution $(1, 0, 1)$ has $D_{\mathrm{sol}} = D_0$. What separates a class-(d) solution from it is a prime dividing $\Phi_p(a, b) = (a^p + b^p)/(a + b)$.

Lemma 5.10. *Let (a, b, c) be a solution with $10p \mid ab$. Then $\Phi_p(a, b) = c_1^5$ for an integer $c_1 > 1$ dividing c, and every prime $\ell \mid \Phi_p(a, b)$ divides c, satisfies $\ell \nmid 10pab$ and $\ell \equiv 1 \pmod p$.*

Proof. $\Phi_p(a, b) \equiv a^{p-1} \pmod b$ and $\equiv b^{p-1} \pmod a$, and $\equiv pa^{p-1} \pmod{a+b}$, so $\Phi_p(a, b)$ is prime to ab, hence to p, and to $a + b$ (as $p \nmid a + b$). Also $\Phi_p(a, b) = \prod_{k=1}^{p-1}(a + \zeta_p^k b) > 0$, and $|a + \zeta_p^k b| \geq B\,|\sin(2\pi k/p)|$ with $B = \max(|a|, |b|) \geq 2$ gives $\Phi_p(a, b) \geq p(B/2)^{p-1} > 1$. As $(a + b)\Phi_p(a, b) = c^5$ with coprime factors, $\Phi_p(a, b) = c_1^5$. If $\ell \mid \Phi_p(a, b)$, then $\ell \nmid ab$, so $(-a/b)^p \equiv 1 \pmod \ell$ and $-a/b \not\equiv 1$; so $p \mid \ell - 1$, and $\ell \neq 2, 5$ as c is odd and prime to 5. □

Proposition 5.11. *Let (a, b, c) be a solution with $10p \mid ab$, $\ell \mid \Phi_p(a, b)$ a prime, $\lambda \mid \ell$ a prime of M and $r \neq \ell$ a prime. Then $\operatorname{Jac} D_{\mathrm{sol}}$ and $\operatorname{Jac} D_0$ have good reduction at λ, the polynomial $P_0(X) = \det(X - \mathrm{Frob}_\lambda \mid V_r \operatorname{Jac} D_0) \in \mathbb{Z}[X]$ has no root in $\mathbb{Q}(\zeta_5)$, and $P_{\mathrm{sol}}(X) = \det(X - \mathrm{Frob}_\lambda \mid V_r \operatorname{Jac} D_{\mathrm{sol}}) \in \mathbb{Z}[X]$ has one. Hence T' and T_0 are not isomorphic as $\mathbb{Z}_5[G_M]$-modules, and a fortiori not as $\mathcal{O}_{M'}$-semilinear G_K-modules.*

Proof. By Lemma 5.10, $\ell \mid c$, $\ell \nmid 10p$ and $\ell \equiv 1 \pmod p$; put $q = N\lambda$, so $q \equiv 1 \pmod{5p}$. *The CM side.* Let χ_λ be the character of $(\mathcal{O}_M/\lambda)^\times$ of order $5p$ with $\chi_\lambda(x) \equiv x^{(q-1)/5p} \pmod \lambda$, $\theta_p = \chi_\lambda^5$ and $\theta_5 = \chi_\lambda^p$. Counting points on $Y^5 = R^p - 1$ over $\mathbb{F}_{q^n}$ with these characters and the Hasse–Davenport relation [26, (0.8)] shows, as in Weil [76], that the eigenvalues of Frob_λ on $V_r \operatorname{Jac} D_0$ are the $4(p-1)$ numbers $-J(\theta_p^j, \theta_5^i)$, $i \in (\mathbb{Z}/5)^\times$, $j \in (\mathbb{Z}/p)^\times$, where $J(\chi_1, \chi_2) = \sum_x \chi_1(x)\chi_2(1-x)$. By Stickelberger's theorem [49, Chapter 1, §2], for $N = 5p$ and $m_1, m_2, m_1 + m_2 \not\equiv 0 \pmod N$,

$$J(\chi_\lambda^{m_1}, \chi_\lambda^{m_2})\mathcal{O}_M = \prod_{t \in (\mathbb{Z}/5p)^\times / D_\ell} \sigma_t^{-1}(\lambda)^{n_t},$$

$$n_t = \#\{d \in D_\ell : \langle -m_1 td/N \rangle + \langle -m_2 td/N \rangle \geq 1\},$$

where $D_\ell \subset (\mathbb{Z}/5p)^\times$ is the decomposition group of ℓ and $\langle \cdot \rangle$ the fractional part. Take $m_1 = 5j$, $m_2 = pi$. As $\ell \equiv 1 \pmod p$, every $d \in D_\ell$ is $\equiv 1 \pmod p$, so $n_t = \#\{d \in D_\ell :$

$\langle -itd/5\rangle \geq 1 - \langle -jt/p\rangle\}$. Given t, choose $s_1, s_2 \equiv 1 \pmod 5$ with $jts_1 \equiv -1$ and $jts_2 \equiv 1 \pmod p$; since $\langle -itd/5\rangle \in [1/5, 4/5]$, $n_{ts_1} = 0$ and $n_{ts_2} = |D_\ell| \geq 1$. So the ideal of $J(\theta_p^j, \theta_5^i)$ is not stable under $H = \mathrm{Gal}(M/\mathbb{Q}(\zeta_5)) = \{\sigma_s : s \equiv 1 \pmod 5\}$, whereas an element of $\mathbb{Q}(\zeta_5)$ generates an H-stable ideal. So no root of P_0 lies in $\mathbb{Q}(\zeta_5)$.

The solution side. By Proposition 5.6, $\operatorname{Jac} C'$ has good reduction at λ and $P_{\mathrm{new}}(\gamma) = 0$ for some $\gamma \in \mathbb{Q}(\zeta_5)$. By the proof of Lemma 5.9, $e \cdot V_r(\operatorname{Jac} C') \cong V_r(\operatorname{Jac} D_{\mathrm{sol}})^{\oplus 2}$ as $\mathbb{Q}_r[G_M]$-modules, so $\operatorname{Jac} D_{\mathrm{sol}}$ has good reduction at λ (Néron–Ogg–Šafarevič [67, Theorem 1]) and $P_{\mathrm{sol}}^2 = P_{\mathrm{new}}$, so $P_{\mathrm{sol}}(\gamma) = 0$. A $\mathbb{Z}_5[G_M]$-isomorphism $T' \cong T_0$ would give $P_{\mathrm{sol}} = P_0$ with $r = 5$, which is allowed as $\ell \neq 5$. □

5.9. **Isometries.** Fix a prime λ' of M' above 5 and put $\mathcal{O} = \mathcal{O}_{M',\lambda'}$, $\mathfrak{a} = \mathfrak{D}^{-1}$ its inverse different. Complex conjugation c fixes λ' (every prime of L^+ above 5 ramifies in M'), and $\mathcal{O}/\mathcal{O}^{\mathsf{c}}$ is ramified. For an $\mathcal{O}$-lattice Λ with a c-sesquilinear form h put $\Lambda^\vee = \{y : h(\Lambda, y) \subset \mathfrak{a}\}$; Λ is *self-dual* if $\Lambda^\vee = \Lambda$. The Weil pairings make T' and T_0 self-dual for skew-Hermitian forms h', h_0, with $h(ax, by) = a\,\mathsf{c}(b)\,h(x, y)$ for $a, b \in \mathcal{O}$ and $\mathrm{Tr} \circ h$ the Weil pairing. Indeed, by [59, Chapter I, §14], $e(ax, y) = e(x, \mathsf{c}(a)y)$, and by trace duality $\mathrm{Hom}_{\mathbb{Z}_5}(\Lambda, \mathbb{Z}_5) \cong \mathrm{Hom}_{\mathcal{O}}(\Lambda, \mathfrak{a})$, $f \mapsto \mathrm{Tr} \circ f$. Here $\mathbb{Z}_5(1)$ is identified with $\mathbb{Z}_5$ by a generator $(\zeta_{5^n})_{n\geq 1}$ with $\zeta_{5^1} = \zeta_5$.

Lemma 5.12. *(a) Let T', T_0 be free $\mathcal{O}$-modules of rank n with self-dual ϵ-Hermitian forms h', h_0, the same $\epsilon = \pm 1$. Every $\mathcal{O}$-linear isomorphism $F_k \colon T'/\varpi^k \to T_0/\varpi^k$ ($k \geq 1$) that is isometric modulo $\varpi^k\mathfrak{a}$, that is, $h_0(F_k x, F_k y) \equiv h'(x, y) \pmod{\varpi^k\mathfrak{a}}$ for all $x, y \in T'$, lifts to an isometry $T' \to T_0$.*

(b) ι_{can} is isometric modulo $\varpi\mathfrak{a}$ for h' and h_0.

(c) Let $\varphi \colon T' \to T_0$ be an isometry of lattices over $\mathcal{O}_{M'} \otimes \mathbb{Z}_5$ with $\varphi \equiv \iota_{\mathrm{can}} \pmod\varpi$ and $\varphi\rho'(g)\varphi^{-1} \equiv \rho_0(g) \pmod{\varpi^D}$ for all $g \in G_K$, $D \geq 1$. Then for some $s \in 1 + \varpi^D(\mathcal{O}_{M'} \otimes \mathbb{Z}_5)$ with $s\,\mathsf{c}(s) = 1$, the isometry $s\varphi$ has the same two properties, and $X(g) = s\varphi\rho'(g)(s\varphi)^{-1}\rho_0(g)^{-1} - 1$, which we call the difference cocycle *of $s\varphi$, satisfies $\det(1 + X(g)) = 1$ for all $g \in G_K$; hence $\mathrm{tr}\, X \equiv 0$ and $X^* \equiv -X \pmod{\varpi^{2D}}$.*

Proof. (a) For $F \in \mathrm{Hom}_{\mathcal{O}}(T', T_0)$ let F^* be the adjoint, $h_0(Fx, z) = h'(x, F^*z)$, integral by self-duality. Then F is an isometry modulo $\varpi^j\mathfrak{a}$ if and only if $F^*F \equiv 1 \pmod{\varpi^j}$. Given F_j with $F_j^*F_j \equiv 1 \pmod{\varpi^j}$, the lifts modulo ϖ^{j+1} form a torsor under $\varpi^j \operatorname{End}(T_0)/\varpi^{j+1}$, and $\tau(F) = (F^*)^{-1}$ acts on it as an involution with $\tau((1+Y)F) = (1 - Y^*)\tau(F)$. Writing $\tau(F') = (1 + Y_0)F'$ for one lift F', $\tau^2 = 1$ gives $Y_0^* = Y_0$, and $F_{j+1} = (1 + Y_0/2)F'$ is τ-fixed, that is, $F_{j+1}^*F_{j+1} \equiv 1 \pmod{\varpi^{j+1}}$. Iterate and take the limit.

(b) Let (A, λ) be a principally polarized abelian variety with $\mathcal{O}_{M'} \subset \operatorname{End} A$, on which the Rosati involution is c, let $\Lambda = T_5(A) \otimes \mathcal{O}$, and let e_{5^∞} be the 5-adic Weil pairing of λ on Λ [59, Chapter I, p. 58], read in $\mathbb{Z}_5$ as above, and h the form with $\mathrm{Tr}_{M'_{\lambda'}/\mathbb{Q}_5} \circ h = e_{5^\infty}$ and $h(ax, by) = a\,\mathsf{c}(b)\,h(x, y)$. By the definition of e_{5^∞}, $e_5(x_1, \lambda y_1) = \zeta_5^{e_{5^\infty}(x,y)}$ for $x, y \in \Lambda$ with images $x_1, y_1 \in A[5]$. Put $\varepsilon_0 = \varpi/\mathsf{c}(\varpi) = -\zeta_5$; then $\mathsf{c}(\varepsilon_0) = \varepsilon_0^{-1}$ and $5/\varpi = \varepsilon_0^{-1}\varpi'$. So the points $\varpi^{-1}x$ and $\varpi^{-1}y$ of $A[\varpi]$ are $(5/\varpi)x_1$ and $\varpi'(\varepsilon_0^{-1}y_1)$, and (5.3) with $Q = \varepsilon_0^{-1}y_1$ gives

$$e_\varpi(\varpi^{-1}x, \varpi^{-1}y) = \zeta_5^{e_{5^\infty}((5/\varpi)x,\, \varepsilon_0^{-1}y)} = \zeta_5^{\mathrm{tr}_0(\varepsilon_0 h(x,y))}, \qquad \mathrm{tr}_0(a) = 5\,\mathrm{Tr}_{M'_{\lambda'}/\mathbb{Q}_5}(\varpi^{-1}a) \bmod 5,$$

since $h((5/\varpi)x, \varepsilon_0^{-1}y) = 5\varpi^{-1}\varepsilon_0\,h(x, y)$. The form $a \mapsto \mathrm{tr}_0(\varepsilon_0 a)$ is a nonzero $\mathbb{F}_5$-linear form on the line $\mathfrak{a}/\varpi\mathfrak{a}$ over the residue field, so $h \bmod \varpi\mathfrak{a}$ is determined by the values $e_\varpi(\alpha\varpi^{-1}x, \varpi^{-1}y)$, $\alpha \in \mathcal{O}_{M'}$. As ι_{can} is $\mathcal{O}_{M'}$-linear and e_ϖ-isometric (Lemma 5.2), it is isometric modulo $\varpi\mathfrak{a}$.

(c) By Lemma 5.9(b) with $r = 5$, the cocycle $\delta(g) = \det(\varphi\rho'(g)\varphi^{-1}\rho_0(g)^{-1})$ of G_K with values in $(\mathcal{O}_{M'} \otimes \mathbb{Z}_5)^\times$ is trivial on G_M; it is $\equiv 1 \pmod{\varpi^D}$ and unitary, $\delta\,\mathsf{c}(\delta) = 1$. So it is inflated from $\mathrm{Gal}(M/K)$, of order $2(p-1)$, prime to 5, with values in the pro-5 group $1 + \varpi^D(\mathcal{O}_{M'} \otimes \mathbb{Z}_5)$; hence $\delta(g) = g(\beta)/\beta$ with $\beta \equiv 1 \pmod{\varpi^D}$. Since $\mathrm{Gal}(M/\mathbb{Q})$ is abelian, $\beta\,\mathsf{c}(\beta)$ is G_K-fixed, and after dividing β by the square root of $\beta\,\mathsf{c}(\beta)$ we may assume $\beta\,\mathsf{c}(\beta) = 1$. Then $s = \beta^{1/2}$ works: $s\varphi$ is an isometry, $\equiv \varphi \pmod{\varpi^D}$, and its determinant cocycle is $\delta \cdot (s/g(s))^2 = 1$. As $1 + X$ is then unitary of determinant 1, $X^* \equiv -X$ and $\operatorname{tr} X \equiv \det(1 + X) - 1 = 0$ modulo ϖ^{2D}. □

6. The CM point at 5: graded pieces and Selmer groups

The criterion of Section 7 compares T' with T_0 one power of ϖ at a time. Each step produces a class in a Selmer group of a graded piece of the adjoint of T_0, and this section computes those Selmer groups. The outcome (Theorem 6.11 for $f = \mathrm{ord}_p 5$ even, Proposition 6.13 for f odd, and Corollary 6.14) is that they vanish as soon as $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$. Everything here concerns the CM point alone. For a place v of K we write K_v for the completion of K at v, and $K_5 = K_{\mathfrak{q}_5}$.

6.1. **The CM type and the Hodge–Tate weights.** Let $B_0 = \mathrm{Jac}\, D_0$, with $\mathcal{O}_M = \mathbb{Z}[\zeta_{5p}]$ acting by $[\zeta_p] = (R \mapsto \zeta_p R)_*$ and $[\zeta_5] = (Y \mapsto \zeta_5^3 Y)_*$ (Section 5.3). Then $T_0 = T_5(B_0)$ is free of rank one over $\mathcal{O}_M \otimes \mathbb{Z}_5$; fix a generator v_0 and write $g(xv_0) = g(x)\tilde{\psi}(g)v_0$ for $g \in G_{\mathbb{Q}}$, with $\tilde{\psi}(g) \in (\mathcal{O}_M \otimes \mathbb{Z}_5)^\times$. On G_M the cocycle $\tilde{\psi}$ is a character $\psi\colon G_M \to (\mathcal{O}_M \otimes \mathbb{Z}_5)^\times$, the CM character of B_0. Put $\Psi = \psi/(\sigma_m \circ \psi)$. Fix an embedding $\iota\colon \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_5$, and let w_0 be the prime of L above 5 induced by ι. Hodge–Tate weights are normalized so that the cyclotomic character has weight $+1$. For $t \in (\mathbb{Z}/5p)^\times$ let $y(t) = \langle (t \bmod p)/p \rangle$ and $\alpha(t) = \langle 3t/5 \rangle$, where $\langle\cdot\rangle$ is the fractional part, and $\varrho(t) = \min(\alpha, 1-\alpha)$, which is $2/5$ if $t \equiv \pm 1$ and $1/5$ if $t \equiv \pm 2 \pmod 5$.

Lemma 6.1. *(a) The CM type of B_0 (the σ_t occurring in $\mathrm{Lie}(B_0) \otimes \overline{\mathbb{Q}}$) is $\Phi = \{t \in (\mathbb{Z}/5p)^\times : y(t) < \alpha(t)\}$.*

(b) The Hodge–Tate weight of $\iota \circ \sigma_r \circ \psi$ at the embedding $\iota \circ \sigma_s$ is $[rs^{-1} \in \Phi]$.

(c) The weight of $\iota \circ \Psi$ at $\iota \circ \sigma_s$ is, with $t = s^{-1}$, $n(s) = [t \in \Phi] - [mt \in \Phi]$, which is $+1$ if $y(t) < \varrho(t)$, -1 if $y(t) > 1 - \varrho(t)$, and 0 otherwise.

(d) $n(-s) = -n(s)$. At the two embeddings of L above one embedding of a residue field of L at 5 (a residue component*) the weights $n(s)$ form the unordered pairs $\{+1,+1\}$, $\{+1,0\}$, $\{0,0\}$, $\{0,-1\}$, $\{-1,-1\}$ for y in $(0,\frac{1}{5})$, $(\frac{1}{5},\frac{2}{5})$, $(\frac{2}{5},\frac{3}{5})$, $(\frac{3}{5},\frac{4}{5})$, $(\frac{4}{5},1)$; in particular no residue component has both weights $+1$ and -1.*

(e) The weight $n(s)$ is $+1$ at exactly $d_+ = \lfloor 2p/5 \rfloor + \lfloor p/5 \rfloor$ of the $2(p-1)$ embeddings of L, and -1 at d_+ of them. For $r \in (\mathbb{Z}/5p)^\times$, at the prime $w = \sigma_r^{-1}(w_0)$ of L the number of $+1$'s is $d_w = \#\{x \in r^{-1}\langle 5\rangle : x < 2p/5\} + \#\{x \in r^{-1}\langle 5\rangle : x < p/5\}$, with $r^{-1}\langle 5\rangle$ read in $(\mathbb{Z}/p)^\times$ and $x \in [1, p-1]$ the representatives.

Proof. (a) The forms $\omega_{i,j} = R^{j-1}dR/Y^i$, $1 \le i \le 4$, $j \ge 1$, are regular at the finite branch points and at the other affine points, and at the point at infinity, where $R = z^{-5} \cdot \text{unit}$ and $Y = z^{-p} \cdot \text{unit}$, they have order $pi - 5j - 1$, which is ≥ 0 exactly when $j/p < i/5$. There are $\sum_{i=1}^4 \lfloor ip/5 \rfloor = 2(p-1)$ such pairs, with distinct characters under $\mu_5 \times \mu_p$, so they form a basis of $H^0(D_0, \Omega^1)$. The pull-backs multiply $\omega_{i,j}$ by ζ_p^j and ζ_5^{-3i}; push-forwards act on $\mathrm{Lie}(B_0)$ by the transpose. So $\mathcal{O}_M$ acts on $\mathrm{Lie}(B_0)$ through the σ_t with $t \equiv j \pmod p$ and $t \equiv 2i \pmod 5$, that is, $i = 5\alpha(t)$, $j = py(t)$, and $j/p < i/5$ means $y(t) < \alpha(t)$. (b) B_0 has

complex multiplication, so it has potentially good reduction at 5 [67, §5, Theorem 6(a)], and the Hodge–Tate decomposition $V_5(B_0) \otimes \mathbb{C}_5 \cong (\operatorname{Lie} B_0 \otimes \mathbb{C}_5)(1) \oplus (\operatorname{Lie} B_0^\vee)^\vee \otimes \mathbb{C}_5$ [70, §4, Corollary 2], applied over a finite extension where B_0 has good reduction, is equivariant for the endomorphisms, all defined over M. So the τ-component of $V_5 \otimes \mathbb{C}_5$ for a coefficient embedding $\tau = \iota \circ \sigma_r$ has weight 1 exactly when $r \in \Phi$; this is (b) for $s = 1$. For general s, choose $\tilde{g} \in G_{\mathbb{Q}}$ restricting to σ_s; the cocycle relation gives $\psi(\tilde{g}^{-1} h \tilde{g}) = \sigma_s^{-1}(\psi(h))$ for $h \in G_M$, and transport along $h \mapsto \tilde{g} h \tilde{g}^{-1}$ gives (b). (c) Weights add. With $t = s^{-1}$: $mt \equiv t \pmod 5$ and $mt \equiv -t \pmod p$, so $y(mt) = 1 - y$, $\alpha(mt) = \alpha$, and $[mt \in \Phi] = [y > 1 - \alpha]$; the case analysis gives the rule. (d) $t \mapsto -t$ sends y to $1 - y$ and fixes ϱ. The two embeddings of L above one residue embedding have the same $s \bmod p$ (the inertia group of 5 in $\operatorname{Gal}(L/\mathbb{Q})$ is $\{\sigma_s : s \equiv 1 \pmod p\}$) and s-values with one $\equiv \pm 1$ and the other $\equiv \pm 2 \pmod 5$, so one has $\varrho = 2/5$ and the other $\varrho = 1/5$. (e) Counting over $x = t \bmod p$ gives $\#\{x < 2p/5\} + \#\{x < p/5\} = d_+$ and, by $x \mapsto p - x$, the same number of -1's. The embedding $\iota \circ \sigma_s|_L$ induces $w = \sigma_r^{-1}(w_0)$ exactly when $s \in r\langle 5 \rangle$. □

The number d_w depends on w: for $p = 19$ ($f = 9$, $g = 2$) it is 6 at one prime above 5 and 4 at the other.

The next lemma solves the cyclic recurrence that fixes the exponents t_j in the proof of Proposition 6.8 and a_j in Section 8.4.

Lemma 6.2. *Let $p \geq 7$ be prime with $p \not\equiv 1 \pmod 5$, let $f = \operatorname{ord}_p 5$, and fix $r \in (\mathbb{Z}/p)^\times$. For $j \in \mathbb{Z}/f$ put $y_j = (r^{-1} 5^{-j} \bmod p)/p$, taking representatives in $[1, p-1]$, and $\Delta_j = 2p(2 - \lfloor 5y_j \rfloor)$. The unique cyclic rational solution of $5t_{j+1} - t_j = \Delta_j$ is $t_j = p - 2p\, y_{j-1}$. It is an odd integer and $0 < |t_j| < p$, for either parity of f.*

Proof. As $py_{j-1} \equiv 5py_j \pmod p$, the number $5y_j - y_{j-1}$ is an integer; since $0 < y_{j-1} < 1$, it equals $\lfloor 5y_j \rfloor$. Substitution proves the formula. The homogeneous cyclic recurrence has only the zero rational solution, since $5^f - 1 \neq 0$. Finally $1 \leq py_{j-1} \leq p - 1$, so t_j is odd (hence nonzero) and $|t_j| \leq p - 2$. □

6.2. **The residual character and crystallinity.** Let $\bar{\mathcal{O}}_M = \mathcal{O}_M/\varpi\mathcal{O}_M = \mathbb{F}_5[\bar{\zeta}_p] \cong \mathbb{F}_5[x]/\Phi_p(x)$, a product of g copies of $\mathbb{F}_{5^f}$, and ω_5 the mod-5 cyclotomic character.

In this subsection and the next, all rings are tensored with $\mathbb{Z}_5$. Let $\theta = \zeta_p - \zeta_p^{-1}$, a unit above 5 with $\sigma_m(\theta) = -\theta$ and $\theta^2 \in M'$. Then $\mathcal{O}_M = \mathcal{O}_{M'}[\theta]$ is étale over $\mathcal{O}_{M'}$ with group $\langle \sigma_m \rangle$, so $\operatorname{End}_{\mathcal{O}_{M'}}(T_0) = \mathcal{O}_M \oplus \mathcal{O}_M \sigma_m$. The Rosati involution of the principal polarization is c on $\mathcal{O}_M$, so the Weil pairing is $e_{5\infty}(xv_0, yv_0) = \operatorname{Tr}_{M \otimes \mathbb{Q}_5/\mathbb{Q}_5}(x\, \mathsf{c}(y) \gamma_M)$ for some γ_M with $\mathsf{c}(\gamma_M) = -\gamma_M$ and $\gamma_M \mathcal{O}_M = \mathfrak{D}_M^{-1} = \varpi^{-3}\mathcal{O}_M$. The *polarized adjoint* is the set $\mathrm{ad}^{\mathrm{pol}}$ of $Z \in \operatorname{End}_{\mathcal{O}_{M'}}(T_0)$ of trace zero that are skew for the skew-Hermitian form h_0 of Section 5.9. It splits as

$$\mathrm{ad}^{\mathrm{pol}} = \mathrm{diag} \oplus \mathcal{T}\sigma_m,$$

$$\mathrm{diag} = \{\alpha \in \mathcal{O}_M : \sigma_m \alpha = -\alpha,\ \mathsf{c}\alpha = -\alpha\} = \theta \cdot \mathcal{O}_{L^+}, \qquad \mathcal{T} = \{\beta \in \mathcal{O}_M : \beta^\dagger = \beta\},$$

where $\beta^\dagger = -(\sigma_m(\gamma_M)/\gamma_M) \cdot \sigma_m \mathsf{c}(\beta)$. We call $\mathcal{T}$ the *off-diagonal module*. The group G_K acts on $\mathrm{ad}^{\mathrm{pol}}$ by conjugation through ρ_0: $g \cdot \alpha = g(\alpha)$ on diag and $g \cdot \beta = (\tilde{\psi}(g)/\sigma_m(\tilde{\psi}(g)))\, g(\beta)$ on $\mathcal{T}$; so G_L acts on $\mathcal{T}$ through a character $\Psi^\flat$ extending Ψ.

Lemma 6.3. *(a) $B_0[\varpi]$ is free of rank one over $\bar{\mathcal{O}}_M$ on $\bar{e} = [(1,0)-\infty]$, with $g(x\bar{e}) = \bar{g}(x)\bar{e}$ for $g \in G_{\mathbb{Q}}$, where $\bar{g}$ acts on $\bar{\mathcal{O}}_M$ through $\bar{\zeta}_p \mapsto \bar{\zeta}_p^{a(g)}$, $g(\zeta_p) = \zeta_p^{a(g)}$. The map $t \mapsto \varpi^{-1}t$ identifies $T_0/\varpi T_0$ with $B_0[\varpi] \otimes \omega_5$, and for a generator v_0 with $\varpi^{-1}v_0 \equiv \bar{e}$ the residual cocycle is $\tilde{\psi}(g) \bmod \varpi = \omega_5(g) \in \mathbb{F}_5^\times$ for every $g \in G_{\mathbb{Q}}$. Hence $\Psi \equiv 1 \pmod{\varpi}$ on G_M and $\Psi^\flat \equiv \omega_5 \pmod{\sqrt{5}}$ on G_L.*

(b) For every prime $w \mid 5$ of L and every uniformizer $\pi \in \sqrt{-5}\cdot(\mathcal{O}_{L_w}^\times)^2$ (for $\pi = \sqrt{-5} = \nu^{2p}$, $L_w(\pi^{1/2p}) = \tilde{F}L_w$, over which B_0 has good reduction), the restriction of $\Psi^\flat$ to $G_{L_w(\pi^{1/2p})}$ is crystalline, with the weights of Lemma 6.1(c).

Proof. (a) By Lemma 5.2(a) at $u = 0$, $B_0[\varpi]$ is spanned by the $e_j = [(\zeta_p^j, 0) - \infty]$ with the single relation $\sum_j e_j = 0$, so it is $\mathbb{F}_5[\mathbb{Z}/p]/\mathbb{F}_5 \cdot (1,\dots,1) \cong \bar{\mathcal{O}}_M$, with $[\zeta_p]$ acting by translation, and g sends $(\zeta_p^j, 0)$ to $(\zeta_p^{a(g)j}, 0)$. Since $g(\varpi) \equiv \omega_5(g)\varpi \pmod{\varpi^2}$, the map $t \mapsto \varpi^{-1}t$ satisfies $\varpi^{-1}g(t) = \omega_5(g)g(\varpi^{-1}t)$. For v_0 as stated, $\tilde{\psi}(g)\bar{e} = \omega_5(g)g(\bar{e}) = \omega_5(g)\bar{e}$, and freeness gives $\tilde{\psi}(g) \equiv \omega_5(g) \pmod{\varpi}$; so on G_M, $\Psi = \tilde{\psi}/\sigma_m(\tilde{\psi}) \equiv 1$. For $g \in G_L$, g fixes ζ_p, so acts trivially on $\bar{\mathcal{O}}_M$, and acts on $\mathcal{T}/\sqrt{5}\mathcal{T} = \varpi\bar{\mathcal{O}}_M$ (Proposition 6.4(a)) by $\omega_5(g)$. (b) By Proposition 8.1(a) at $u = 0$, B_0 has good reduction over $\tilde{F} = \mathbb{Q}_{5^f}(\nu)$, $\nu^{4p} = -5$, so $V_5(B_0)$ is crystalline over $\tilde{F}$ and over every finite extension. As $\mathbb{Q}_5((-5)^{1/4}) = \mathbb{Q}_5(\zeta_5)$, $\tilde{F}L_w$ contains $L_w(\zeta_5)$, a completion of M. So the coefficient components of $V_5(B_0) \otimes \overline{\mathbb{Q}}_5$ (its τ-components for the embeddings τ of M into $\overline{\mathbb{Q}}_5$, as in the proof of Lemma 6.1(b), on which G_M acts through $\tau \circ \psi$) are crystalline over $\tilde{F}L_w = L_w(\pi_0^{1/2p})$, $\pi_0 = \nu^{2p}$, and so is $\Psi^\flat$, which on $G_{\tilde{F}L_w} \subset G_M$ is $\Psi = \psi/(\sigma_m \circ \psi)$, a quotient of two of their characters. For $\pi = \pi_0 v^2$ with $v \in \mathcal{O}_{L_w}^\times$, the field $L_w(v^{1/p})$ is unramified over L_w ($\zeta_p \in L_w$, $p \neq 5$), and $L_w(\pi^{1/2p})L_w(v^{1/p}) = \tilde{F}L_wL_w(v^{1/p})$; crystallinity descends along unramified extensions. □

6.3. **The graded pieces of the polarized adjoint.** For a submodule X write $\mathrm{gr}^k X = (X \cap \varpi^k)/(X \cap \varpi^{k+1})$, where ϖ^k means $\varpi^k \operatorname{End}_{\mathcal{O}_{M'}}(T_0)$. The *depth* of an element, or of a set of elements, of $\operatorname{End}_{\mathcal{O}_{M'}}(T_0)$ is the largest k such that ϖ^k contains it (∞ for 0).

Proposition 6.4. *Let $p \geq 7$, $p \not\equiv 1 \pmod 5$, $W = \bar{\mathcal{O}}_M \otimes_{\mathbb{F}_5} \mu_5 \cong \operatorname{Ind}_{G_L}^{G_K} \mu_5$ and $\Theta = \bar{\mathcal{O}}_M^{\bar{\mathsf{c}}=-1} \cong \operatorname{Ind}_{G_{L^+}}^{G_K} \mathbb{F}_5(\chi_{L/L^+})$, χ_{L/L^+} the character of L/L^+.*

(a) $\mathrm{gr}^k \mathcal{T} \cong \bar{\mathcal{O}}_M$ for k odd and 0 for k even; $\mathrm{gr}^{2j}(\mathrm{diag}) \cong \bar{\mathcal{O}}_M^{\bar{\mathsf{c}}=-1}$ and $\mathrm{gr}^{2j+1}(\mathrm{diag}) = 0$. Multiplication by $\sqrt{5}$ is a G_K-isomorphism $\mathrm{gr}^k \to \mathrm{gr}^{k+2}$ on both, and $\mathcal{T}/\sqrt{5}\mathcal{T} = \mathrm{gr}^1 \mathcal{T}$. For $b \in \mathcal{O}_M$ and $k \geq 0$,

$$(\varpi^k b)^\dagger \equiv -(-1)^k \varpi^k b \pmod{\varpi^{k+1}}. \tag{6.1}$$

(b) As G_K-modules, $\mathrm{gr}^{2j+1}\mathcal{T} \cong W$ and $\mathrm{gr}^{2j}(\mathrm{diag}) \cong \Theta$ for every $j \geq 0$.

(c) $H^0(G_K, W) = H^0(K_5, W) = 0$, and $H^0(K_5, \Theta)$ is 0 if f is even and has dimension $g/2$ if f is odd.

Proof. (a) From $\mathsf{c}(\gamma_M) = -\gamma_M$ and $\mathsf{c}(\varpi) = -\zeta_5^{-1}\varpi$, the unit $\varpi^3\gamma_M$ is congruent to its image under c modulo ϖ; on $\bar{\mathcal{O}}_M$ both σ_m and c act by $\bar{\zeta}_p \mapsto \bar{\zeta}_p^{-1}$, and σ_m fixes ϖ, so $\sigma_m(\gamma_M)/\gamma_M \equiv 1 \pmod{\varpi}$. The element $\sigma_m\mathsf{c}$ fixes ζ_p and sends ϖ to $1 - \zeta_5^{-1} \equiv -\varpi \pmod{\varpi^2}$. Hence (6.1) holds. Also $(\beta^\dagger)^\dagger = \beta$, and $\beta \mapsto \beta^\dagger$ preserves each $\varpi^k\mathcal{O}_M$ and is $\mathcal{O}_L$-linear. With $P(\beta) = (\beta+\beta^\dagger)/2$, $\mathcal{T} = P(\mathcal{O}_M)$ and $\varpi^k\mathcal{O}_M = P(\varpi^k\mathcal{O}_M) \oplus (1-P)(\varpi^k\mathcal{O}_M)$, so $\mathrm{gr}^k \mathcal{T} = \mathrm{gr}^k \mathcal{O}_M \cong \bar{\mathcal{O}}_M$ for k odd and 0 for k even. Elements of $L^+ \otimes \mathbb{Q}_5$ have even ϖ-valuation and θ is a unit, so $\mathrm{diag} \cap \varpi^{2j} = \sqrt{5}^j \,\mathrm{diag}$ and $\mathrm{gr}^{2j}(\mathrm{diag}) \cong (\mathcal{O}_L/\sqrt{5})^{\bar{\mathsf{c}}=-1} = \bar{\mathcal{O}}_M^{\bar{\mathsf{c}}=-1}$.

$\sqrt{5}$ is fixed by G_K, σ_m and $\sigma_m\mathsf{c}$, so multiplication by it commutes with $\beta \mapsto \beta^\dagger$ and the action, and raises the depth by 2. Finally $\mathcal{T} \subset \varpi\mathcal{O}_M$ and $\mathrm{gr}^2\,\mathcal{T} = 0$ give $\mathcal{T}/\sqrt{5}\mathcal{T} = \mathrm{gr}^1\,\mathcal{T}$. (b) By Lemma 6.3(a), $g\cdot(\varpi b) \equiv \omega_5(g)\varpi\,\bar g(b) \pmod{\varpi^2}$ for $g \in G_K$, so $\mathrm{gr}^1\,\mathcal{T} \cong \bar{\mathcal{O}}_M \otimes \omega_5 = \bar{\mathcal{O}}_M \otimes \mu_5$. The elements $\bar\zeta_p^a$, $a \in (\mathbb{Z}/p)^\times$, form a basis of $\bar{\mathcal{O}}_M$ permuted simply transitively by G_K through $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/p)^\times$, so $\bar{\mathcal{O}}_M \cong \mathrm{Ind}_{G_L}^{G_K}\mathbb{F}_5$; and c is the central element -1 of $\mathrm{Gal}(L/K)$, so $\bar{\mathcal{O}}_M^{\bar{\mathsf{c}}=-1} \cong \mathrm{Ind}_{G_{L^+}}^{G_K}\mathbb{F}_5(\chi_{L/L^+})$. (c) By Shapiro's lemma, $H^0(G_K, W) = \mu_5(L) = 0$. Locally, $W|_{G_{K_v}} \cong \bigoplus_{w|v}\mathrm{Ind}_{G_{L_w}}^{G_{K_v}}\mu_5$, so $H^0(K_v, W) = \bigoplus_{w|v}\mu_5(L_w)$. At $w \mid 5$, $e(L_w/\mathbb{Q}_5) = 2 < 4$, so $\zeta_5 \notin L_w$. For Θ at 5: the decomposition group $D_5 = \langle\mathrm{Frob}\rangle \subset \mathrm{Gal}(L/K)$ acts on $\bar{\mathcal{O}}_M \cong \prod_{w|5}\mathbb{F}_{5^f}$ by the fifth power map, so $\bar{\mathcal{O}}_M^{D_5} = \prod_w \mathbb{F}_5$, on which $\bar{\mathsf{c}}$ permutes the factors; c fixes every w if and only if $-1 \in \langle 5\rangle \subset (\mathbb{Z}/p)^\times$, that is, if and only if f is even. So $H^0(K_5, \Theta) = (\bar{\mathcal{O}}_M^{D_5})^{\bar{\mathsf{c}}=-1}$ is 0 for f even and of dimension $g/2$ for f odd. □

6.4. **Selmer groups.** Let S be the set of places of K above 2, 5, p and ∞. For $w \mid 5$ a prime of L, $L_w \cong \mathbb{Q}_{5^f}(\sqrt{5})$. Let $E_L = L_{w_0}$ (w_0 as in Section 6.1) and $k = \mathcal{O}_{E_L}/\sqrt{5} = \mathbb{F}_{5^f}$. For a prime $w \mid 5$ let $\mathcal{F}_w \subset H^1(L_w, k(\omega_5)) = k \otimes_{\mathbb{F}_5} L_w^\times/L_w^{\times 5}$ be the image of $H^1_f(L_w, \mathcal{O}_{E_L}(\Psi^\flat))$, the Bloch–Kato subgroup [8, §3], with $\Psi^\flat$ restricted to a decomposition group at w. Let

$$G = \{x \in L^\times/L^{\times 5} : v_w(x) \equiv 0 \pmod 5 \text{ for every prime } w \nmid 5 \text{ of } L\},$$

and $\mathrm{loc}_5 \colon G \to \bigoplus_{w|5} L_w^\times/L_w^{\times 5}$ the localization.

Definition 6.5. Let $\mathcal{L}_5 \subset H^1(K_5, W)$ be the image of $H^1_f(K_5, \mathcal{T})$ in $H^1(K_5, \mathcal{T}/\sqrt{5}\mathcal{T}) = H^1(K_5, W)$. Let $\mathrm{Sel}(W) \subset H^1(G_{K,S}, W)$ be the subgroup of classes that are unramified at the places above 2 and p and lie in $\mathcal{L}_5$ at $\mathfrak{q}_5$, and $\mathrm{Sel}(\Theta) \subset H^1(G_{K,S}, \Theta)$ the subgroup of classes that are unramified at the places above 2, 5 and p.

Proposition 6.6. *Let $p \geq 7$, $p \not\equiv 1 \pmod 5$.*

(a) $H^1(K_5, \mathcal{T})$ is free over $\mathcal{O}_{K_5}$ of rank $2(p-1)$, and $\dim_{\mathbb{F}_5}\mathcal{L}_5 = d_+$. Multiplication by $\sqrt{5}^j$ identifies $\mathcal{L}_5$ with the image of $H^1_f(K_5, \sqrt{5}^j\mathcal{T})$ in $H^1(K_5, \mathrm{gr}^{2j+1}\,\mathcal{T})$. Over k, $\mathcal{L}_5 \otimes k = \bigoplus_{w|5}\mathcal{F}_w$, with $\dim_k \mathcal{F}_w = d_w$.

(b) $\mathrm{Sel}(W) = \{x \in G : \mathrm{loc}_5 x \in \mathcal{L}_5\}$, under the identifications $H^1(G_{K,S}, W) = H^1(G_{L,S}, \mu_5)$ and $H^1(K_5, W) = \bigoplus_{w|5} L_w^\times/L_w^{\times 5}$ of Shapiro's lemma and Kummer theory; and $\mathrm{Sel}(W) \otimes k = \{x \in k \otimes G : x_w \in \mathcal{F}_w \text{ for every } w \mid 5\}$.

(c) The image of $H^1_f(K_5, \mathrm{diag})$ in $H^1(K_5, \Theta)$ is $H^1_{\mathrm{ur}}(K_5, \Theta)$, of dimension 0 if f is even and $g/2$ if f is odd; and $\mathrm{Sel}(\Theta) = \mathrm{Hom}(\mathrm{Cl}(L), \mathbb{F}_5)^{\mathsf{c}=-1}$, which vanishes if and only if $5 \nmid h^-(L)$.

Proof. Coefficients. The map $\beta \mapsto \beta^\dagger$ is an involution of $\mathcal{O}_M \otimes \mathbb{Z}_5$, semilinear for $\sigma_m\mathsf{c}$, which generates $\mathrm{Gal}(M/L)$; by Galois descent $\mathcal{T} \otimes \mathbb{Q}$ is free of rank one over $L \otimes \mathbb{Q}_5$, so the lattice $\mathcal{T}$ is free of rank one over $\mathcal{O}_L \otimes \mathbb{Z}_5$. As L/K is unramified above 5, $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{E_L} \cong \prod_{\sigma\in\mathrm{Gal}(L/K)}\mathcal{O}_{E_L}$, and $\mathcal{T} \otimes_{\mathcal{O}_{K_5}} \mathcal{O}_{E_L} \cong \mathrm{Ind}_{G_L}^{G_K}\mathcal{O}_{E_L}(\Psi^\flat)$; by Mackey's formula its restriction to G_{K_5} is $\bigoplus_{w|5}\mathrm{Ind}_{G_{L_w}}^{G_{K_5}}$, compatibly with Shapiro's lemma. (a) The torsion of $H^1(K_5, \mathcal{T})$ comes from $H^0(K_5, W) = 0$. $H^0(K_5, V) = 0$ for $V = \mathcal{T} \otimes \mathbb{Q}$, and $H^2(K_5, V)$ is dual to $H^0(K_5, V^*(1))$, which vanishes because at each $w \mid 5$ not all weights of $\Psi^\flat$ are $+1$: by Lemma 6.1(e) that would put the coset $r^{-1}\langle 5\rangle$ below $p/5$, but its largest element x has $5x \bmod p \leq x$, so $x > p/5$. The local Euler characteristic formula gives the rank. The subgroup $H^1_f(K_5, \mathcal{T})$, the preimage of $H^1_f(K_5, V)$, is saturated, and $H^1_f(K_5, V) \otimes_{K_5} E_L \cong$

$\bigoplus_{w|5} H^1_f(L_w, E_L(\Psi^\flat))$. As $\Psi^\flat$ is de Rham at w (Lemma 6.3(b)), the dimension formula of [8, Corollary 3.8.4] gives $\dim_{E_L} H^1_f(L_w, E_L(\Psi^\flat)) = h^0 + \dim D_{\mathrm{dR}}/\operatorname{Fil}^0 = 0 + d_w$. Summing gives d_+, and a saturated submodule of rank d_+ reduces injectively. Multiplication by $\sqrt{5}$ is a G_K-isomorphism $\mathcal{T} \cong \sqrt{5}\mathcal{T}$ carrying H^1_f to H^1_f. (b) W is inflated from $G_{K,S}$, and Shapiro's lemma with Kummer theory gives $H^1(G_{K,S}, W) = \{x \in L^\times/L^{\times 5} : v_q(x) \equiv 0 \pmod 5 \text{ for } q \nmid 10p\}$. At $v \mid p$, L_w/K_v is totally ramified, so $\mathrm{Res}_{I_{K_v}} \mathrm{Ind}_{G_{L_w}}^{G_{K_v}} = \mathrm{Ind}_{I_{L_w}}^{I_{K_v}}$; at $v \mid 2$ it is unramified, so $I_{K_v} = I_{L_w}$ and $\mathrm{Res}_{I_{K_v}} \mathrm{Ind}_{G_{L_w}}^{G_{K_v}}$ is the sum of the $[L_w : K_v]$ conjugates of the restriction to I_{L_w}. In both cases a class of $H^1(L_w, \mu_5)$ is unramified at v if and only if its restriction to I_{L_w} vanishes, that is, $v_w(x) \equiv 0 \pmod 5$ for $w \mid v$, which cuts out G. The description over k follows from (a). (c) G_{K_5} acts on $\mathrm{diag} \otimes \mathbb{Q}$ through the unramified group D_5 with all weights 0, so $H^1_f = H^1_{\mathrm{ur}}$; $H^1(K_5, \mathrm{diag})$ is torsion-free as $|D_5|$ is prime to 5, and $H^1_{\mathrm{ur}}(K_5, \mathrm{diag})$ reduces onto $H^1_{\mathrm{ur}}(K_5, \Theta) = \Theta/(\mathrm{Frob} - 1)\Theta$, of dimension $h^0(K_5, \Theta)$ (Proposition 6.4(c)). By Shapiro's lemma and inflation-restriction for $\mathrm{Gal}(L/L^+)$, $H^1(G_{K,S}, \Theta) = \mathrm{Hom}(G_{L,S}, \mathbb{F}_5)^{\mathsf{c}=-1}$. At $v \mid p$, $H^1(K_v, \Theta) = 0$ ($h^0(K_v, \Theta) = h^0(K_v, \Theta^\vee(1)) = 0$, as χ_{L/L^+} is ramified and μ_5 unramified there), so there is no condition at p; L^+/K is unramified at 2 and 5. For $\varphi \in \mathrm{Hom}(G_{L,S}, \mathbb{F}_5)^{\mathsf{c}=-1}$ and f odd, the conditions say that φ is unramified everywhere. For f even the condition at 5 is $\varphi|_{G_{L_w}} = 0$, which for c-odd φ follows from unramifiedness, since $\mathsf{c}(w) = w$ gives $\varphi([w]) = -\varphi([w])$. So $\mathrm{Sel}(\Theta) = \mathrm{Hom}(\mathrm{Cl}(L), \mathbb{F}_5)^{\mathsf{c}=-1}$ by class field theory (L is totally imaginary), and this is zero exactly when the minus part of the 5-class group of L is zero, that is, when $5 \nmid h^-(L)$. □

Remark 6.7. Let $W^\vee = \mathrm{Hom}(W, \mu_5)$ and $\mathrm{Sel}^*(W^\vee)$ its Selmer group for the dual local conditions. The Greenberg–Wiles formula [22, Theorem 2.19] gives $\dim \mathrm{Sel}(W) - \dim \mathrm{Sel}^*(W^\vee) = d_+ - p < 0$ for every $p \not\equiv 1 \pmod 5$. Indeed, the global invariants contribute -1, since $h^0(G_K, W) = 0$ by Proposition 6.4(c) and $W^\vee \cong \mathrm{Ind}_{G_L}^{G_K} \mathbb{F}_5$ has $h^0(G_K, W^\vee) = 1$ by Shapiro's lemma; the two real places contribute $-(p-1)$, the place above 5 contributes d_+, and the places above 2 and p contribute 0. So the count does not force a Selmer class, and the vanishing of $\mathrm{Sel}(W)$ is a question about global units and class groups, which Section 6.6 answers.

6.5. **The local condition at 5.** Fix $w \mid 5$, $q = 5^f$, $k_0 = \mathbb{F}_q$, and a uniformizer $\pi \in \sqrt{-5} \cdot (\mathcal{O}_{L_w}^\times)^2$. Let $F = L_w(\pi_F)$ with $\pi_F^{2p} = \pi$: it is cyclic of degree $2p$ over L_w and totally ramified, $e(F/\mathbb{Q}_5) = 4p$, $\mathrm{Gal}(F/L_w) \cong \mu_{2p}$ via $g \mapsto \omega_g = g(\pi_F)/\pi_F$, and $F \supset L_w(\sqrt{\pi}) = L_w(\zeta_5)$. For $\pi = \sqrt{-5}$, F is the field $\tilde{F} = \mathbb{Q}_{5^f}(\nu)$ of Section 1.5. Let $F_\infty = F(\pi_F^{1/5^\infty})$, and

$$\mathrm{res}\colon H^1(L_w, k(\omega_5)) \to H^1(G_{F_\infty}, k) = k \otimes k_0((u))/(\phi - 1),$$

where the right side is computed by the field of norms [44, (1.1.12)], [30, A1.2.6], in its variable $u = (\pi_F^{1/5^n})_n$ (a formal variable, not the parameter u of D_u). Write (j, N) for the class of u^{-N} on the component $j \in \mathbb{Z}/f$ of $k \otimes k_0((u))$, where, for $w = \sigma_r^{-1}(w_0)$, the component j is that of the residue embedding induced by the $\iota \circ \sigma_s$ with $s \equiv r5^j \pmod p$. Let $J_+(j)$, $J_-(j)$ be the sets of embeddings of L_w above the residue embedding j at which $\Psi^\flat$ has weight $+1$, resp. -1 (Lemma 6.1). For a character χ of G_{L_w} with values in $\mathcal{O}_{E_L}^\times$ and $\chi \equiv \omega_5 \pmod{\sqrt{5}}$ let $\mathcal{F}_w(\chi)$ be the image of $H^1_f(L_w, \mathcal{O}_{E_L}(\chi))$ in $H^1(L_w, k(\omega_5))$, so that $\mathcal{F}_w = \mathcal{F}_w(\Psi^\flat)$.

Proposition 6.8. *(a)* $\mathrm{res}(\mathcal{F}_w(\Psi^\flat))$ *is the span* $\mathcal{S}_\pi = \mathrm{span}\{(j,p) : \#J_+(j) \geq 1\} \oplus \mathrm{span}\{(j,3p) : \#J_+(j) = 2\}$, res *is injective on* $\mathcal{F}_w(\Psi^\flat)$, *and* $\dim_k \mathcal{F}_w(\Psi^\flat) = d_w$.

(b) $\mathcal{F}_w(\Psi^\flat) \cap \mathcal{F}_w(\Psi^\flat \circ \mathsf{c}) = 0$.

(c) If f is even, then c fixes every $w \mid 5$, and $\mathcal{L}_5 \cap H^+ = 0$, where H^+ is the c-fixed part of $H^1(K_5, W) = \bigoplus_{w|5} L_w^\times / L_w^{\times 5}$.

Proof. (a) By Lemma 6.3(b), $\Psi^\flat|_{G_F}$ is crystalline with weights in $\{-1, 0, 1\}$. Let χ be a crystalline character of G_{L_w} with weight 1 exactly at the embeddings in J_-; then χ and $\chi\Psi^\flat$ have weights in $\{0, 1\}$ with weight-1 sets J_- and J_+, which are disjoint. Let $\mathfrak{S} = W(k_0)[[u]]$ with the Eisenstein polynomial $E(u) = (u^{2p} - \pi)(u^{2p} - \bar\pi)$ of π_F, $\bar\pi$ the conjugate of π over $\mathbb{Q}_{5^f}$. By [36, Lemma 2.2.3], which allows any finite extension of $\mathbb{Q}_5$, the Breuil–Kisin modules of $\chi|_{G_F}$ and $\chi\Psi^\flat|_{G_F}$ with respect to π_F have rank one, $\phi(e_{i,j+1}) = \lambda_{i,j} e_{i,j}$, with $\lambda_{i,j}$ a unit times the product of the $u - \tau(\pi_F)$ over the weight-1 embeddings τ above j. Modulo the maximal ideal, $\bar\lambda_{2,j} = c_2 u^{s_j^+}$ and $\bar\lambda_{1,j} = c_1 u^{s_j^-}$ with $s_j^+ = 2p\,\#J_+(j)$ and $s_j^- = 2p\,\#J_-(j)$. The roots of $E(u)$ are the $4p$ conjugates $\tau(\pi_F)$, and J_+, J_- are disjoint, so $\lambda_1\lambda_2$ is, up to a unit, a product of distinct factors $u - \tau(\pi_F)$ of $E(u)$ and divides $E(u)$. Hence every h defines a Breuil–Kisin module $\mathfrak{M}_h$ of height ≤ 1, $\phi(e_2) = \lambda_2 e_2 + h e_1$, which by Kisin's theorem ($5 > 2$) comes from a 5-divisible group over $\mathcal{O}_F$ [43, Theorem (2.2.7)]. The Tate module of this 5-divisible group is a lattice in a crystalline extension of χ by $\chi\Psi^\flat$, and this gives a class in $H^1_f(F, \mathcal{O}_{E_L}(\Psi^\flat))$ whose restriction to G_{F_∞} is the étale class of $\bar h$ ([44, Proposition (1.1.13)], applied to $\mathfrak{M}_h/\sqrt{5}\mathfrak{M}_h$). Let $\mathcal{F}_F$ be the image of $H^1_f(F, \mathcal{O}_{E_L}(\Psi^\flat))$ in $H^1(F, k)$. In the étale ϕ-module of the extension, $\phi(\varepsilon_2) = \bar\lambda_2\varepsilon_2 + \bar h\varepsilon_1$, and replacing ε_2 by $\varepsilon_2 + x\varepsilon_1$ replaces $\bar h$ by $\bar h + \phi(x)\bar\lambda_1 - \bar\lambda_2 x$. Compare [35, Proposition 7.4] and [36, Proposition 5.1.3]. The residual characters of χ and $\chi\Psi^\flat$ agree on G_F, so there is ϑ with $\phi(\vartheta)\bar\lambda_1 = \bar\lambda_2\vartheta$; on component j, $\vartheta_j = \text{const}\cdot u^{t_j}$ with $5t_{j+1} + s_j^- = t_j + s_j^+$, that is, $t_j = \sum_{i\ge1}(s^+ - s^-)_{j-i}/5^i$. With $x = \vartheta\Xi$ the change is $\bar\lambda_2\vartheta\,(\phi(\Xi) - \Xi)$, so the class of the extension in $k \otimes k_0((u))/(\phi - 1)$ is that of $\bar h/(\bar\lambda_2\vartheta)$. For $\bar h = u^n$ on component j this is $\text{const}\cdot u^{n - s_j^+ - t_j}$, the class $(j, s_j^+ + t_j - n)$. So $(j, N) \in \mathrm{res}(\mathcal{F}_F)$ for $0 < N \le s_j^+ + t_j$, $5 \nmid N$. Now $\mathcal{F}_w(\Psi^\flat) = \mathcal{F}_F^{\mu_{2p}}$: as $[F : L_w] = 2p$ is prime to 5, restriction identifies $H^1(L_w, -)$ with $H^1(F, -)^{\mu_{2p}}$, for the coefficients $\mathcal{O}_{E_L}(\Psi^\flat)$ and $k(\omega_5)$, and $H^1_f(L_w, -)$ with $H^1_f(F, -)^{\mu_{2p}}$ (corestriction after restriction is $2p$), and μ_{2p}-invariants are exact. Here $g \in \mu_{2p}$ acts through a lift $\tilde g \in G_{L_w}$ fixing the 5^n-th roots $(\pi_F^{1/5^n})^{2p}$ of π, which exists as $[F : L_w]$ is prime to 5; it preserves F_∞, which these roots generate over F, so res is equivariant. As $\tilde g(\pi_F^{1/5^n}) = \omega_g^{5^{-n}}\pi_F^{1/5^n}$ (exponent modulo $2p$), $\tilde g$ multiplies the variable u of the field of norms by the residue of ω_g, and so u^{-N} on component j by $\omega_g^{-5^j N}$; it acts on the coefficients by $\omega_5(\tilde g) = \omega_g^p$, as $L_w(\zeta_5) = L_w(\pi_F^p)$. So g acts on (j, N) by $\omega_g^{p - 5^j N}$, the invariant classes have $N \equiv p \pmod{2p}$, and each of them in $\mathrm{res}(\mathcal{F}_F)$ is the restriction of an element of $\mathcal{F}_F^{\mu_{2p}}$, the average of a preimage over μ_{2p}. Let $y_j = \langle (r^{-1}5^{-j} \bmod p)/p \rangle$ be the value y of Lemma 6.1 on component j. By Lemma 6.1(d), $(s^+ - s^-)_j = 2p(2 - \lfloor 5y_j \rfloor)$, so Lemma 6.2 (with r read modulo p) gives $t_j = p - 2py_{j-1}$, an odd integer with $|t_j| < p$. So $s_j^+ + t_j$ lies in $(-p, p)$, $(p, 3p)$ or $(3p, 5p)$ according as $\#J_+(j) = 0, 1, 2$, and the stated span lies in $\mathrm{res}(\mathcal{F}_w)$. It has dimension $d_w = \dim_k \mathcal{F}_w$ (Proposition 6.6(a)), and $H^1_f(L_w, \mathcal{O}_{E_L}(\Psi^\flat))$ is torsion-free, so the inclusion is an equality and res is injective. (b) As c carries $\sqrt{-5}\cdot(\mathcal{O}_{L_w}^\times)^2$ to $\sqrt{-5}\cdot(\mathcal{O}_{L_{\mathsf{c}(w)}}^\times)^2$, Lemma 6.3(b) at $\mathsf{c}(w)$, transported along c, shows that $\Psi^\flat \circ \mathsf{c}$ is crystalline over F. It has the weights $-n(s)$ of Lemma 6.1(c) and residual character ω_5, so the same argument places $\mathrm{res}(\mathcal{F}_w(\Psi^\flat \circ \mathsf{c}))$ on the components with a weight -1. By Lemma 6.1(d) no component has weights of both signs, so the two images meet in 0, and res is injective.

(c) If f is even, c lies in the decomposition group of every $w \mid 5$. Transport of structure along a lift of c normalizing G_{L_w} carries $\mathcal{F}_w(\Psi^\flat)$ to $\mathcal{F}_w(\Psi^\flat \circ \mathsf{c})$ and acts on $k \otimes L_w^\times/L_w^{\times 5}$ as $1 \otimes \mathsf{c}$. If $x \in \mathcal{L}_5$ is c-fixed, each component of $x \otimes 1$ lies in $\mathcal{F}_w(\Psi^\flat)$ by Proposition 6.6(a), and, applying $1 \otimes \mathsf{c}$, in $\mathcal{F}_w(\Psi^\flat \circ \mathsf{c})$; by (b), $x = 0$. □

6.6. **Global units and class groups.** Let $\Delta = \mathrm{Gal}(L/\mathbb{Q})$, of order $2(p-1)$, prime to 5, and write $X^\pm$ for the $\mathsf{c} = \pm 1$ parts of an $\mathbb{F}_5[\Delta]$-module X. Let S_5 be the set of primes of L above 5 and $\mathrm{Cl}_{S_5}(L) = \mathrm{Cl}(L)/\langle [w] : w \in S_5 \rangle$.

Lemma 6.9. *Let $p \geq 7$, $p \not\equiv 1 \pmod 5$. There is an exact sequence of $\mathbb{F}_5[\Delta]$-modules $0 \to \mathcal{O}_{L,S_5}^\times/5 \to G \to \mathrm{Cl}_{S_5}(L)[5] \to 0$, and $(\mathcal{O}_{L,S_5}^\times/5)^-$ is zero if f is even. Hence, if f is even and $5 \nmid h^-(L)$, then $G = G^+$ and $\mathrm{loc}_5(G) \subset H^+$.*

Proof. The map sends x with $(x) = \mathfrak{a}^5 \prod_{w|5} w^{a_w}$ to the class of $\mathfrak{a}$. As $\mathbb{F}_5[\Delta]$ is semisimple, $\mathcal{O}_{L,S_5}^\times/5$ has the composition factors of $\mathcal{O}_{L,S_5}^\times \otimes \mathbb{Q} \cong (\mathcal{O}_L^\times \otimes \mathbb{Q}) \oplus \mathbb{Q}[S_5]$ (and $\mu_5(L) = 1$); the first summand is c-fixed since L is CM, and $\mathbb{Q}[S_5]^- = 0$ when c fixes every $w \mid 5$, that is, when f is even. If $5 \nmid h^-(L)$, the minus part of the 5-primary part of $\mathrm{Cl}(L)$ is 0, and so is that of its quotient $\mathrm{Cl}_{S_5}(L)$ (the classes of the $w \mid 5$ generate a Δ-stable subgroup); hence $(\mathrm{Cl}_{S_5}(L)[5])^- = 0$. As loc_5 is Δ-equivariant and c fixes every w, it maps G^+ into H^+. □

Proposition 6.10. *Let $p \geq 7$, $p \not\equiv 1 \pmod 5$. Then*

$$\dim_{\mathbb{F}_5} \ker(\mathrm{loc}_5 |_{G^+}) = \dim_{\mathbb{F}_5} (\mathrm{Cl}(M')/5)^-.$$

In particular $\ker(\mathrm{loc}_5 |_{G^+}) \neq 0$ if and only if $5 \mid h^-(M')$.

Proof. This is the Kummer-theoretic argument behind Leopoldt's reflection theorem [53] (see [75, §10.2]), written out because the local condition at 5 must be followed through it. Let $B \subset M^\times/M^{\times 5}$ be the group of the classes y with $M(y^{1/5})/M$ unramified at every prime. By Kummer theory and class field theory, $(y, [\mathfrak{A}]) \mapsto \sigma_{\mathfrak{A}}(y^{1/5})/y^{1/5}$, with $\sigma_{\mathfrak{A}}$ the Artin symbol, is a perfect $\mathrm{Gal}(M/\mathbb{Q})$-equivariant pairing $B \times \mathrm{Cl}(M)/5 \to \mu_5$, and, for a prime $\mathfrak{P}$ of M, $y \in B$ is a fifth power in $M_{\mathfrak{P}}$ exactly when it pairs trivially with the class of $\mathfrak{P}$ (as $\mathfrak{P}$ is unramified in $M(y^{1/5})$ and $\sigma_{\mathfrak{P}}$ is its Frobenius). Restriction maps $\ker(\mathrm{loc}_5 |_{G^+})$ into B, as its elements are fifth powers at every $w \mid 5$ and have $v_q \equiv 0 \pmod 5$ elsewhere, and injectively, as $[M : L] = 2$ is prime to 5. Now extend scalars from $\mathbb{F}_5$ to a finite field containing the values of the characters of $\mathrm{Gal}(M/\mathbb{Q})$, a group of order $4(p-1)$, prime to 5, and decompose into eigenspaces: the pairing identifies the χ-eigenspace of B with the dual of the $\omega_5\chi^{-1}$-eigenspace of $\mathrm{Cl}(M)/5$. Let χ_x be a character of Δ, trivial on c (no other character occurs in the kernel, which lies in G^+). Then $\omega_5\chi_x^{-1}$ is odd, and trivial on σ_m as $m \equiv 1 \pmod 5$ and $\chi_x(\sigma_m) = \chi_x(\sigma_m\mathsf{c}) = 1$. So the χ_x-eigenspace of the kernel injects into the dual of the $\omega_5\chi_x^{-1}$-eigenspace of $\mathrm{Cl}(M)/5$, which equals that of $\mathrm{Cl}(M')/5$, an odd eigenspace. Conversely, let χ be an odd character of $\mathrm{Gal}(M'/\mathbb{Q})$ with $(\mathrm{Cl}(M')/5)^\chi \neq 0$, so that the $\omega_5\chi^{-1}$-eigenspace of B is nonzero. The character $\omega_5\chi^{-1}$ is trivial on $\mathrm{Gal}(M/L) = \langle \sigma_m\mathsf{c} \rangle$, as $\omega_5(\sigma_m\mathsf{c}) = \chi(\sigma_m\mathsf{c}) = -1$, so the eigenspace comes from the classes $x \in L^\times/L^{\times 5}$ with $M(x^{1/5})/M$ unramified (the classes in $M^\times/M^{\times 5}$ fixed by $\mathrm{Gal}(M/L)$ come from $L^\times/L^{\times 5}$, as $[M : L] = 2$ is prime to 5); these have $v_q(x) \equiv 0 \pmod 5$ at every prime, and the character is even, so the eigenspace lies in G^+. The class of a prime $\mathfrak{P} \mid 5$ of M lies in eigenspaces trivial on the inertia group $\mathrm{Gal}(M/\mathbb{Q}(\zeta_p))$, while χ is not, as $\mathrm{Gal}(M/\mathbb{Q}(\zeta_p))$ contains $\sigma_m\mathsf{c}$ and $\chi(\sigma_m\mathsf{c}) = \chi(\mathsf{c}) = -1$. So the eigenspace pairs trivially with the class of every $\mathfrak{P} \mid 5$, and by the local criterion, tensored with the scalars, it lies in the kernel of the localization to $M_{\mathfrak{P}}^\times/M_{\mathfrak{P}}^{\times 5}$, hence in that of the localization to $L_w^\times/L_w^{\times 5}$, which injects into $M_{\mathfrak{P}}^\times/M_{\mathfrak{P}}^{\times 5}$ as

$[M_{\mathfrak{P}} : L_w] = 2$, w the prime of L below $\mathfrak{P}$; so it lies in the kernel. Counting dimensions eigenspace by eigenspace gives the equality. □

6.7. **The criterion in terms of class numbers.**

Theorem 6.11. *Let $p \geq 7$ be a prime with $p \not\equiv 1 \pmod 5$ and $f = \operatorname{ord}_p 5$ even.*

(a) $\mathrm{Sel}(\Theta) = 0$ *if and only if* $5 \nmid h^-(L)$.

(b) If $5 \nmid h^-(L)$, *then* $\mathrm{Sel}(W) = \ker(\mathrm{loc}_5 |_G)$, *of dimension* $\dim_{\mathbb{F}_5}(\mathrm{Cl}(M')/5)^-$.

(c) $h^-(\mathbb{Q}(\zeta_{5p})) = h^-(L)\, h^-(M')/(Q_L Q_{M'})$, *where* $Q_L, Q_{M'} \in \{1, 2\}$ *are the unit indices; so* $v_5 h^-(\mathbb{Q}(\zeta_{5p})) = v_5 h^-(L) + v_5 h^-(M')$.

Hence, if $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$, *then* $\mathrm{Sel}(W) = \mathrm{Sel}(\Theta) = 0$.

Proof. (a) is Proposition 6.6(c). (b) By Proposition 6.6(b), $\mathrm{Sel}(W) = \{x \in G : \mathrm{loc}_5 x \in \mathcal{L}_5\}$. By Lemma 6.9, $G = G^+$ and $\mathrm{loc}_5(G) \subset H^+$, and $\mathcal{L}_5 \cap H^+ = 0$ by Proposition 6.8(c); so $\mathrm{Sel}(W) = \ker(\mathrm{loc}_5 |_{G^+})$, and Proposition 6.10 gives its dimension. (c) Since σ_m has order 2 and c acts by -1 on odd characters, the odd characters of $\mathrm{Gal}(M/\mathbb{Q})$ are the disjoint union of those trivial on $\sigma_m \mathsf{c}$ (the odd characters of L) and those trivial on σ_m (the odd characters of M'). The analytic class number formula $h^-(F) = Q_F w_F \prod_{\chi \text{ odd}} (-\frac{1}{2} B_{1,\chi})$ [75, Theorem 4.17] with $w_M = 10p$, $w_L = 2p$, $w_{M'} = 10$ and $Q_M = 2$ [75, Corollary 4.13], as $5p$ is not a prime power, gives the formula. It is also the case M/L^+ of [52, Proposition 2]. Then (a) and (b) give the last statement. □

The hypothesis $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$ is decided without computing a class group: by the analytic class number formula used in (c), $h^-(\mathbb{Q}(\zeta_{5p}))$ is $Q_M w_M$ times the product of the numbers $-\frac{1}{2} B_{1,\chi}$ over the odd characters χ of $(\mathbb{Z}/5p)^\times$, and its 5-adic valuation can be computed exactly from these generalized Bernoulli numbers (Section 10). The condition is the analogue, for the field $\mathbb{Q}(\zeta_{5p})$ and the prime 5, of Kummer's regularity condition $p \nmid h^-(\mathbb{Q}(\zeta_p))$. For the field in our hypothesis, $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$ is equivalent to $5 \nmid h(\mathbb{Q}(\zeta_{5p}))$ by (F1) of Section 4. For the classical condition, $p \nmid h^-(\mathbb{Q}(\zeta_p))$ is equivalent to regularity of p.

6.8. **Odd order of 5.** In this subsection $f = \operatorname{ord}_p 5$ may be odd. If f is odd, then f divides $(p-1)/2$, so 5 is a square modulo p and, by reciprocity, p is a square modulo 5: as $p \not\equiv 1 \pmod 5$, $p \equiv -1 \pmod 5$. Moreover $-1 \notin \langle 5 \rangle$, so complex conjugation $\mathsf{c} = \sigma_{-1}$ lies outside the decomposition group of $\mathfrak{q}_5$, the subgroup $\langle 5 \rangle$ of $(\mathbb{Z}/p)^\times \cong \mathrm{Gal}(L/K)$, and moves every prime of L above 5: the g primes above 5 fall into $g/2$ pairs $\{w, \mathsf{c}(w)\}$. So the last two assertions of Lemma 6.9 and Proposition 6.8(c), which use that c fixes these primes, do not apply (the exact sequence of Lemma 6.9 holds for every f). We replace them by a statement on valuations (Proposition 6.12), which holds for either parity of f. The reduction $\bar{\Psi}^\flat = \omega_5$ of the character $\Psi^\flat$, which extends $\Psi = \psi/(\sigma_m \circ \psi)$ (Section 6.2), is the cyclotomic case treated in [36, §6] using $(\phi, \widehat{G})$-modules. Here Proposition 6.12 uses unramified twists to show that the crystalline classes have zero valuation; Theorem 8.15 excludes the possible component along the Kummer class of the uniformizer (the très ramifiée line) in the diagonal part of the leading digit (Section 7.1) through finite flat models, as in Theorem 8.12(ii).

Fix $w \mid 5$ and a uniformizer $\pi \in \sqrt{-5} \cdot (\mathcal{O}_{L_w}^\times)^2$, let $F = L_w(\pi_F)$, $\pi_F^{2p} = \pi$, and $F_\infty = F(\pi_F^{1/5^\infty})$ be as in Section 6.5, and write res_π for the map $\mathrm{res}\colon H^1(L_w, k(\omega_5)) \to H^1(G_{F_\infty}, k)$ defined there. Let $\kappa_F(g) = g(\pi_F^{1/5})/\pi_F^{1/5}$, read in k through a fixed ζ_5. As $[F : L_w] = 2p$ is prime to 5, restriction $H^1(L_w, k(\omega_5)) \to H^1(F, k)$ is injective and maps the class $[\pi]$ of π in $k \otimes L_w^\times / L_w^{\times 5} = H^1(L_w, k(\omega_5))$ to $2p\, \kappa_F$. Since $\zeta_5 \in F$ and F_∞ is generated by one compatible

system of 5-power roots of the uniformizer π_F, the kernel of $\mathrm{Hom}(G_F,k)\to\mathrm{Hom}(G_{F_\infty},k)$ is the très ramifiée line $k\kappa_F$ of π_F [36, Lemma 5.4.2], after enlarging the coefficients. Here the residual cyclotomic character is trivial. Since $2p$ is nonzero in k, this gives

$$\ker \mathrm{res}_\pi = k\cdot[\pi]. \tag{6.2}$$

For an unramified character $\mu\colon G_{L_w}\to\mathcal{O}_{E_L}^\times$ with $\mu\equiv 1 \pmod{\sqrt{5}}$ let $\mathcal{F}_{w,\mu}\subset H^1(L_w,k(\omega_5))$ be the image of $H^1_f(L_w,\mathcal{O}_{E_L}(\Psi^\flat\mu))$; thus $\mathcal{F}_{w,1}=\mathcal{F}_w$ is the space of Proposition 6.6. Let U_w be the unit group of L_w and $\mathcal{U}_w = k\otimes U_w/U_w^5$, the kernel of the valuation $v\colon k\otimes L_w^\times/L_w^{\times 5}\to k$.

Proposition 6.12. *Let $p\geq 7$ be a prime with $p\not\equiv 1 \pmod 5$, w a prime of L above 5, and $\mu\colon G_{L_w}\to\mathcal{O}_{E_L}^\times$ an unramified character with $\mu\equiv 1 \pmod{\sqrt{5}}$. Then $\mathcal{F}_{w,\mu}\subset\mathcal{U}_w$ (the classes are peu ramifiées). In particular $\mathcal{L}_5\subset\bigoplus_{w|5}U_w/U_w^5$ inside $H^1(K_5,W)=\bigoplus_{w|5}L_w^\times/L_w^{\times 5}$.*

Proof. Inputs. (V1) $\dim_k\mathcal{F}_{w,\mu}=d_w<2f$. For $\mu=1$ this is Proposition 6.6(a) with its proof, which shows that not all weights of $\Psi^\flat$ at w are $+1$; the twist by μ changes neither the weights nor the residual character, so the count of Proposition 6.6(a) is the same. (V2) For every uniformizer $\pi\in\sqrt{-5}\cdot(\mathcal{O}_{L_w}^\times)^2$, $\mathrm{res}_\pi(\mathcal{F}_{w,\mu})$ is the span $\mathcal{S}_\pi$ of Proposition 6.8(a), of dimension d_w, for every μ. Indeed, the proof of Proposition 6.8(a) uses $\Psi^\flat$ only through its weights, its residual character and its crystallinity over F, which $\Psi^\flat\mu$ shares, and the twist multiplies the Frobenius entries $\lambda_{i,j}$ of that proof only by units congruent to 1 modulo $\sqrt{5}$. The dimension count of Proposition 6.6(a) used there is (V1).

Local duality pairs $H^1(L_w,k(\omega_5))$ perfectly with $H^1(L_w,k)=\mathrm{Hom}(G_{L_w},k)$ by $(x,h)=h(\mathrm{Art}(x))$. Let $\mathrm{unr}\in\mathrm{Hom}(G_{L_w},k)$ be the unramified homomorphism with $\mathrm{unr}(\mathrm{Frob})=1$; then $(x,\mathrm{unr})=v(x)$ and $\mathrm{unr}^\perp=\mathcal{U}_w$.

The idea. By (V2) all the $\mathcal{F}_{w,\mu}$ lie in one space $\mathcal{V}_\pi$ of dimension d_w+1, and the twists serve to move a linear condition on them: for the twists μ of step (1), $\mathcal{F}_{w,\mu}$ is orthogonal to a class $\bar{y}_\mu=\bar{y}-b_\mu\,\mathrm{unr}$, where b_μ takes every value in k (steps (1) and (3)). If $\bar{y}$ were nonzero on $\mathcal{V}_\pi\cap\mathcal{U}_w$, two of the $\mathcal{F}_{w,\mu}$ would span $\mathcal{V}_\pi$, which would then contain $[\pi u]$ for every principal unit u, so that $\mathcal{V}_\pi\cap\mathcal{U}_w$, of dimension d_w, would contain $\mathcal{U}_w$, of dimension $2f>d_w$ (step (4), with (V1)). So $\bar{y}$ vanishes there, and, unless $\bar{y}$ is unramified (step (2)), the orthogonality of $\mathcal{F}_{w,1}$ to $\bar{y}$ removes the $[\pi]$-component for a π with $\bar{y}(\mathrm{Art}(\pi))\neq 0$ (step (5)).

(1) *Torsion classes of the dual character.* Let χ_{cyc} be the 5-adic cyclotomic character and $\chi_\mu^*=\chi_{\mathrm{cyc}}(\Psi^\flat\mu)^{-1}$; it is $\equiv 1 \pmod{\sqrt{5}}$, as $\Psi^\flat\equiv\omega_5$ (Lemma 6.3(a)). It is not trivial: its weight $1-n$ is nonzero at an embedding where $\Psi^\flat$ has weight $n\neq+1$, which exists by (V1). Let $s=\min_g v_{\sqrt{5}}(\chi_1^*(g)-1)$ and $\bar{y}=(\chi_1^*-1)/\sqrt{5}^s \bmod\sqrt{5}$, a nonzero element of $\mathrm{Hom}(G_{L_w},k)$. For $\mu\equiv 1 \pmod{\sqrt{5}^s}$ write $\mu(\mathrm{Frob})=1+\sqrt{5}^s\beta_\mu$ and $b_\mu=\beta_\mu \bmod\sqrt{5}$; then $(\chi_\mu^*-1)/\sqrt{5}^s\equiv\bar{y}_\mu:=\bar{y}-b_\mu\,\mathrm{unr} \pmod{\sqrt{5}}$. As $\chi_\mu^*\equiv 1 \pmod{\sqrt{5}^s}$, the element $\sqrt{5}^{-s}$ of $(E_L/\mathcal{O}_{E_L})(\chi_\mu^*)$ is invariant, and its image $y_\mu\in H^1(L_w,\mathcal{O}_{E_L}(\chi_\mu^*))$ under the connecting map of $0\to\mathcal{O}_{E_L}\to E_L\to E_L/\mathcal{O}_{E_L}\to 0$ (twisted by χ_μ^*) is killed by $\sqrt{5}^s$ and reduces to $\bar{y}_\mu$. For $x\in H^1_f(L_w,\mathcal{O}_{E_L}(\Psi^\flat\mu))$, the cup product $x\cup y_\mu$ lies in $H^2(L_w,\mathcal{O}_{E_L}(\chi_{\mathrm{cyc}}))\cong\mathcal{O}_{E_L}$, which is torsion-free, and is killed by $\sqrt{5}^s$, so it is 0. Reducing modulo $\sqrt{5}$: $(\mathcal{F}_{w,\mu},\bar{y}_\mu)=0$ for every $\mu\equiv 1 \pmod{\sqrt{5}^s}$; and as μ runs over these characters, b_μ runs over all of k.

(2) If $\bar{y}\in k\cdot\mathrm{unr}$, then $\mathcal{F}_{w,1}\subset\bar{y}^\perp=\mathrm{unr}^\perp=\mathcal{U}_w$. Otherwise $\bar{y}$ is ramified. It vanishes on the image under Art of the roots of unity of order prime to 5, so $\bar{y}\circ\mathrm{Art}$ is nonzero on $U_w^{(1)}=1+\sqrt{5}\mathcal{O}_{L_w}$.

(3) Let $\pi_0 = \sqrt{-5}$, a uniformizer of L_w (-1 is a square in $\mathbb{Q}_5$), and $\pi \in \pi_0 U_w^{(1)}$; then $\pi \in \sqrt{-5}\cdot(\mathcal{O}_{L_w}^\times)^2$, as principal units are squares. Let $\mathcal{V}_\pi = \mathrm{res}_\pi^{-1}(\mathcal{S}_\pi)$. By (V2) and (6.2), $\mathcal{V}_\pi \supseteq \mathcal{F}_{w,\mu}$ for every μ, $[\pi] \in \mathcal{V}_\pi$ and $\dim_k \mathcal{V}_\pi = d_w + 1$, as $\mathcal{S}_\pi = \mathrm{res}_\pi(\mathcal{F}_{w,1})$ lies in the image of res_π. As $v([\pi]) = 1$, $\mathcal{V}_\pi = \mathcal{V}'_\pi \oplus k[\pi]$ with $\mathcal{V}'_\pi = \mathcal{V}_\pi \cap \mathcal{U}_w$ of dimension d_w.

(4) *Claim:* $(\mathcal{V}'_\pi, \bar{y}) = 0$ *for every* $\pi \in \pi_0 U_w^{(1)}$. Suppose $x_0 \in \mathcal{V}'_\pi$ has $(x_0, \bar{y}) \neq 0$. Then $(x_0, \bar{y}_\mu) = (x_0, \bar{y}) \neq 0$, as $x_0 \in \mathrm{unr}^\perp$; so $\bar{y}_\mu$ is nonzero on $\mathcal{V}_\pi$, and by (1) and dimensions $\mathcal{F}_{w,\mu} = \mathcal{V}_\pi \cap \bar{y}_\mu^\perp$ for every $\mu \equiv 1 \pmod{\sqrt{5}^s}$. Put $\delta_\pi = \bar{y}(\mathrm{Art}(\pi))$, so that $([\pi], \bar{y}_\mu) = \delta_\pi - b_\mu$. Choose μ with $b_\mu = \delta_\pi$ and μ' with $b_{\mu'} \neq \delta_\pi$. Then $[\pi] \in \mathcal{F}_{w,\mu}$, $\mathcal{F}_{w,\mu} \supseteq \mathcal{V}'_\pi \cap \bar{y}^\perp$, and $x_0 - (x_0, \bar{y})(\delta_\pi - b_{\mu'})^{-1}[\pi] \in \mathcal{F}_{w,\mu'}$. This element pairs with $\bar{y}_\mu$ to $(x_0, \bar{y}) \neq 0$, so it lies outside $\mathcal{F}_{w,\mu}$, which has dimension $d_w = \dim_k \mathcal{V}_\pi - 1$. So $\mathcal{F}_{w,\mu} + \mathcal{F}_{w,\mu'} = \mathcal{V}_\pi$. For $u \in U_w^{(1)}$, (3) applied to $\pi' = \pi u$ gives $\mathcal{V}_\pi = \mathcal{F}_{w,\mu} + \mathcal{F}_{w,\mu'} \subseteq \mathcal{V}_{\pi'}$, and as the dimensions agree, $\mathcal{V}_\pi = \mathcal{V}_{\pi'} \ni [\pi']$. Hence $[u] = [\pi'] - [\pi] \in \mathcal{V}_\pi \cap \mathcal{U}_w = \mathcal{V}'_\pi$ for every $u \in U_w^{(1)}$. As $k \otimes U_w^{(1)}/(U_w^{(1)})^5 = \mathcal{U}_w$ has dimension $2f$, this gives $2f \leq d_w$, against (V1).

(5) In the second case of (2), since $\delta_{\pi u} = \delta_\pi + \bar{y}(\mathrm{Art}(u))$, we may choose $\pi \in \pi_0 U_w^{(1)}$ with $\delta_\pi \neq 0$. Every $z \in \mathcal{V}_\pi$ is $x + a[\pi]$ with $x \in \mathcal{V}'_\pi$, and $(z, \bar{y}) = a\delta_\pi$ by (4). For $z \in \mathcal{F}_{w,1}$, $(z, \bar{y}) = 0$ by (1), so $a = 0$ and $z \in \mathcal{V}'_\pi \subset \mathcal{U}_w$. This proves $\mathcal{F}_{w,1} \subset \mathcal{U}_w$. For a general μ, the same argument applies with $\Psi^\flat\mu$ in place of $\Psi^\flat$: its unramified twists congruent to 1 modulo $\sqrt{5}$ are such twists of $\Psi^\flat$, so (V1) and (V2) hold for them. Finally $\mathcal{L}_5 \otimes k = \bigoplus_{w|5} \mathcal{F}_w$ by Proposition 6.6(a), so $\mathcal{L}_5$ lies in $\bigoplus_{w|5} U_w/U_w^5$. □

Proposition 6.13. *Let $p \geq 7$ be a prime with $p \not\equiv 1 \pmod 5$ and $f = \mathrm{ord}_p 5$ odd. Let $H = H^1(K_5, W) = \bigoplus_{w|5} L_w^\times/L_w^{\times 5}$, and $H^\pm$, $G^\pm$ the $\mathsf{c} = \pm 1$ parts.*

(a) $\mathcal{L}_5 \cap H^+ = 0$.

(b) If $5 \nmid h^-(L)$, *then* $\mathrm{Sel}(W) = \ker(\mathrm{loc}_5|_{G^+})$, *of dimension* $\dim_{\mathbb{F}_5}(\mathrm{Cl}(M')/5)^-$.

(c) If $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$, *then* $\mathrm{Sel}(W) = \mathrm{Sel}(\Theta) = 0$.

Proof. As c has order 2, prime to 5, it acts semisimply on G and on H (carrying the w-summand to the $\mathsf{c}(w)$-summand), and loc_5 is c-equivariant. (a) Let $y \in \mathcal{L}_5 \cap H^+$, and write $y \otimes 1 = (y_w)_w$ with $y_w \in \mathcal{F}_w(\Psi^\flat)$ (Proposition 6.6(a)). Transport of structure along a lift of c to G_K carries $H^1_f(L_w, \mathcal{O}_{E_L}(\Psi^\flat))$ to $H^1_f(L_{\mathsf{c}(w)}, \mathcal{O}_{E_L}(\Psi^\flat \circ \mathsf{c}))$, so it carries $\mathcal{F}_w(\Psi^\flat)$ to $\mathcal{F}_{\mathsf{c}(w)}(\Psi^\flat \circ \mathsf{c})$ (whether c acts on $H \otimes k$ as $1 \otimes \mathsf{c}$ or as its negative does not matter for subspaces). As y is c-fixed, $y_{\mathsf{c}(w)}$ is the image of y_w, so $y_{\mathsf{c}(w)} \in \mathcal{F}_{\mathsf{c}(w)}(\Psi^\flat) \cap \mathcal{F}_{\mathsf{c}(w)}(\Psi^\flat \circ \mathsf{c}) = 0$ by Proposition 6.8(b). As w runs over the primes above 5, so does $\mathsf{c}(w)$; hence $y = 0$. (b) Let $x = x^+ + x^- \in \mathrm{Sel}(W)$, so $\mathrm{loc}_5 x \in \mathcal{L}_5$ (Proposition 6.6(b)). By Proposition 6.12, $v(\mathrm{loc}_5 x) = 0$, where $v\colon H \to \mathbb{F}_5[S_5]$ is the vector of valuations, which is c-equivariant, so $v(x^+) = v(x^-) = 0$. We show that v is injective on G^-. As $5 \nmid h^-(L)$, $(\mathrm{Cl}(L) \otimes \mathbb{Z}_5)^- = 0$ (proof of Lemma 6.9), hence $(\mathrm{Cl}_{S_5}(L) \otimes \mathbb{Z}_5)^- = 0$, and the exact sequence of Lemma 6.9 gives $G^- = (\mathcal{O}^\times_{L,S_5}/5)^-$. Let $\Lambda = v(\mathcal{O}^\times_{L,S_5}) \subset \mathbb{Z}[S_5]$. The map $(n_w) \mapsto [\prod_w w^{n_w}]$ embeds $\mathbb{Z}[S_5]/\Lambda$ in $\mathrm{Cl}(L)$, so $((\mathbb{Z}[S_5]/\Lambda) \otimes \mathbb{Z}_5)^- = 0$, that is, $(\Lambda \otimes \mathbb{Z}_5)^- = \mathbb{Z}_5[S_5]^-$. The kernel of v on $\mathcal{O}^\times_{L,S_5}$ is $\mathcal{O}^\times_L$, and $(\mathcal{O}^\times_L \otimes \mathbb{Z}_5)^- = 0$, since $\mathcal{O}^\times_L \otimes \mathbb{Z}_5 = \mathcal{O}^\times_{L^+} \otimes \mathbb{Z}_5$ (the roots of unity of L have order $2p$, and the unit index is at most 2). So $v\colon (\mathcal{O}^\times_{L,S_5} \otimes \mathbb{Z}_5)^- \to \mathbb{Z}_5[S_5]^-$ is an isomorphism, and so is its reduction modulo 5, as $\mathcal{O}^\times_{L,S_5} \otimes \mathbb{Z}_5$ is torsion-free ($\zeta_5 \notin L$). Hence $x^- = 0$, and $\mathrm{loc}_5 x = \mathrm{loc}_5 x^+ \in \mathcal{L}_5 \cap H^+ = 0$ by (a): $x \in \ker(\mathrm{loc}_5|_{G^+})$. Conversely $\ker(\mathrm{loc}_5|_{G^+}) \subset \mathrm{Sel}(W)$, as $0 \in \mathcal{L}_5$. The dimension is given by Proposition 6.10. (c) The proof of Theorem 6.11(c) does not use f, so $v_5 h^-(\mathbb{Q}(\zeta_{5p})) = v_5 h^-(L) + v_5 h^-(M')$. Hence

$5 \nmid h^-(L)$, so $\mathrm{Sel}(\Theta) = 0$ by Proposition 6.6(c); and $5 \nmid h^-(M')$, so $\mathrm{Sel}(W) = 0$ by (b) and Proposition 6.10. □

Corollary 6.14. *Let $p \geq 7$ be a prime with $p \not\equiv 1 \pmod 5$ and $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$. Then $\mathrm{Sel}(W) = \mathrm{Sel}(\Theta) = 0$, whatever the parity of $\mathrm{ord}_p 5$.*

Proof. For $\mathrm{ord}_p 5$ even this is Theorem 6.11; for $\mathrm{ord}_p 5$ odd, Proposition 6.13(c). □

7. The criterion

This section proves that class (d) is empty whenever the two Selmer groups of Section 6 vanish, given two local inputs at 5, which Section 8 supplies. The argument, outlined at the start of Section 5, is the tangent-space computation of Mazur's deformation theory (see [22, Lemmas 2.39 and 2.40]), carried out on the two lattices T', T_0 and the polarized adjoint. The two local inputs, (L1) and (L2) of Theorem 7.2, are properties of the pair (T', T_0) with the fixed identification ι_{can}: at each depth the comparison is induced by finite flat models. Rather than identifying these inputs with the tangent condition of a deformation functor, we compare the two lattices directly through isometries inducing ι_{can}, and at each depth the only obstruction to improving the comparison is the class of one leading digit (Section 7.1) in the Selmer group of a graded piece of $\mathrm{ad}^{\mathrm{pol}}$. The polarization and the normalization $\det(1+X) = 1$ (Lemma 5.12(c)) keep the digit in $\mathrm{ad}^{\mathrm{pol}}$. The isomorphism $T' \cong T_0$ that the induction would produce is excluded by Proposition 5.11.

7.1. **Difference cocycles.** Fix a class-(d) solution. On $\mathrm{End} = \mathrm{End}_{\mathcal{O}_{M'}}(T_0)$ (over $\mathcal{O}_{M'} \otimes \mathbb{Z}_5$) let G_K act by $g \cdot Z = \rho_0(g) Z \rho_0(g)^{-1}$, which is again $\mathcal{O}_{M'}$-linear because $\rho_0(g)$ is semilinear. As in Lemma 5.12(c), the difference cocycle of an $\mathcal{O}_{M'}$-linear isometry $\varphi\colon T' \to T_0$ is

$$X(g) = \varphi \rho'(g) \varphi^{-1} \rho_0(g)^{-1} - 1 \qquad (g \in G_K),$$

and $1 + X(gh) = (1 + X(g))\, g \cdot (1 + X(h))$. The isometry is *normalized* if $\det(1 + X(g)) = 1$ for all g, and its *depth* is the depth of $X(G_K)$ (Section 6.3). The *diagonal part* and the *off-diagonal part* of an element of End are its components in $\mathcal{O}_M$ and in $\mathcal{O}_M \sigma_m$ under $\mathrm{End} = \mathcal{O}_M \oplus \mathcal{O}_M \sigma_m$ (Section 6.2), and likewise in each $\mathrm{gr}^k \mathrm{End}$. On $\mathrm{ad}^{\mathrm{pol}}$ they are the components in diag and in $\mathcal{T}\sigma_m$. If φ is normalized of depth $D \geq 1$, then $X^* \equiv -X$ and $\mathrm{tr}\, X \equiv 0 \pmod{\varpi^{2D}}$ (Lemma 5.12(c)), so $X \in \mathrm{ad}^{\mathrm{pol}}$ modulo ϖ^{2D}, and its *leading digit* $x = X \bmod \varpi^{D+1}$, the class of X in $\mathrm{gr}^D \mathrm{ad}^{\mathrm{pol}}$, is a 1-cocycle of G_K. Here $\mathrm{gr}^D \mathrm{ad}^{\mathrm{pol}}$ is $\mathrm{gr}^D \mathcal{T}\sigma_m \cong W$ for D odd and $\mathrm{gr}^D \mathrm{diag} \cong \Theta$ for D even (Proposition 6.4). Let $\Gamma = G_{K_5}$.

7.2. **Depth two.** At depth 2 the leading digit is diagonal. Theorem 8.12(ii) and Theorem 8.15, which treat the diagonal part, need $D \geq 4$, so this depth is treated separately, with the isomorphism (L2), stated in Lemma 7.1 below, given by finite flat models (Proposition 8.5).

Lemma 7.1. *Let φ be a normalized isometry inducing ι_{can} with $X(G_K) \subset \varpi^2 \mathrm{End}$, and x the class of X in $\mathrm{gr}^2 \mathrm{ad}^{\mathrm{pol}} = \mathrm{gr}^2 \mathrm{diag} \cong \Theta$. Suppose* (L2)*: there is an $\mathcal{O}_{M'}$-linear Γ-equivariant isomorphism $\varphi_3\colon T'/\varpi^3 \to T_0/\varpi^3$ with $\varphi_3 \equiv \iota_{\mathrm{can}} \pmod{\varpi}$. Then $x|_\Gamma$ is a coboundary.*

Proof. Step 1: $H^0(\Gamma, \mathrm{gr}^1 \mathrm{End}) = 0$. We have $\mathrm{gr}^1 \mathrm{End} \cong (\mathrm{End}/\varpi) \otimes (\varpi\mathcal{O}/\varpi^2\mathcal{O})$. An element g of the inertia group I_{K_5} acts trivially on the residue rings of $\mathcal{O}_{M'} \otimes \mathbb{Z}_5$; on T_0/ϖ by the scalar $\omega_5(g)$ (Lemma 6.3(a); the points $(\zeta_p^j, 0)$ are fixed by g as $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is unramified at 5), hence trivially on End/ϖ; and on $\varpi\mathcal{O}/\varpi^2\mathcal{O}$ by $\omega_5(g)$. As I_{K_5} maps onto $\mathrm{Gal}(\mathbb{Q}_5(\zeta_5)/\mathbb{Q}_5(\sqrt{5}))$, some g has $\omega_5(g) = -1$ and acts by -1. *Step 2.* Let $B = \varphi\varphi_3^{-1}$, an $\mathcal{O}_{M'}$-linear automorphism

of T_0/ϖ^3 with $B \equiv 1 \pmod{\varpi}$; write $B = 1+Y$. For $g \in \Gamma$, $1+X(g) \equiv B\,(g\cdot B)^{-1} \pmod{\varpi^3}$. As $X \equiv 0 \pmod{\varpi^2}$, the class of Y in $\mathrm{gr}^1 \mathrm{End}$ is Γ-invariant, hence 0; so $Y \in \varpi^2 \mathrm{End}$ and $x(g) = y - g\cdot y$ for $g \in \Gamma$, where y is the class of Y in $\mathrm{gr}^2 \mathrm{End}$. *Step 3.* Let $Z \mapsto Z^*$ be the adjoint for the skew-Hermitian form of T_0, and $P(Z) = Z_s - \frac{1}{2}\operatorname{tr}(Z_s)\cdot 1$ with $Z_s = (Z - Z^*)/2$. Then P is an idempotent onto $\mathrm{ad}^{\mathrm{pol}}$, preserves each $\varpi^k \mathrm{End}$, and is Γ-equivariant, because $\rho_0(g)$ is a similitude. So $x(g) = \bar{P}x(g) = \bar{P}y - g\cdot\bar{P}y$ on Γ. □

7.3. **The criterion.**

Theorem 7.2 (the criterion)**.** *Let $p \geq 7$ be a prime with $p \not\equiv 1 \pmod 5$, and suppose that $\mathrm{Sel}(W) = 0$ and $\mathrm{Sel}(\Theta) = 0$. Suppose that at every class-(d) solution the following hold.*

(L1) For every $D \geq 1$ and every normalized $\mathcal{O}_{M'}$-linear isometry $\varphi\colon T' \to T_0$ with $\varphi \equiv \iota_{\mathrm{can}} \pmod{\varpi}$ whose difference cocycle satisfies $X(\Gamma) \subset \varpi^D \mathrm{End}$: (i) the class of the off-diagonal part of $X|_\Gamma \bmod \varpi^{D+1}$, an element of $H^1(K_5, \mathrm{gr}^D \mathcal{T}\sigma_m)$, lies in the image of $H^1_f(K_5, \sqrt{5}^{\lfloor D/2\rfloor}\mathcal{T})$; (ii) if $D \geq 4$ is even, the class of the diagonal part lies in $H^1_{\mathrm{ur}}(K_5, \mathrm{gr}^D \mathrm{diag})$.

(L2) There is an $\mathcal{O}_{M'}$-linear Γ-equivariant isomorphism $T'/\varpi^3 \to T_0/\varpi^3$ congruent to ι_{can} modulo ϖ.

Then no solution lies in class (d).

At every class-(d) solution, (L2) holds by Proposition 8.5, and (L1) holds by Theorem 8.12 when $\mathrm{ord}_p 5$ is even; when $\mathrm{ord}_p 5$ is odd, Corollary 8.16 draws the same conclusion by the proof below, with Proposition 8.14 and Theorem 8.15 as the inputs at 5.

Proof. Let (a, b, c) be a class-(d) solution. In outline: the leading digit of a normalized isometry of maximal depth would have its class in $\mathrm{Sel}(W)$ or $\mathrm{Sel}(\Theta)$, which vanish, so a Cayley transform would remove it. Hence the depth is unbounded, and a limit gives $T' \cong T_0$, which Proposition 5.11 excludes. *Choice of φ.* By Lemma 5.12(b) and (a), applied at each $\lambda' \mid 5$, ι_{can} lifts to an $\mathcal{O}_{M'}$-linear isometry $T' \to T_0$; it is G_K-equivariant modulo ϖ, so by Lemma 5.12(c) with $D = 1$ a unitary scalar $s \equiv 1 \pmod{\varpi}$ makes it normalized. Let $D \in \{1, 2, \ldots, \infty\}$ be the supremum of the depths of the normalized isometries inducing ι_{can}. Suppose $D < \infty$, and fix such a φ of depth D, with leading digit x.

The leading digit is unramified outside S. By Lemma 5.7, ρ' and ρ_0 are unramified outside $5, p$, and M'/K is unramified outside $5p$; so x is a cocycle of $G_{K,S}$, unramified at the places above 2.

At $v \mid p$. By Proposition 5.5 there is an isometry $\iota_v\colon T' \to T_0$ commuting with G_{K_v}; with $U = \varphi\iota_v^{-1}$, $1 + X(g) = U\rho_0(g)U^{-1}\rho_0(g)^{-1}$ on G_{K_v}, a function of $\rho_0(g)$. The group $H_v = \rho_0(I_{K_v})$ of semilinear automorphisms of T_0 is finite, I_{K_v} acts on $\mathrm{gr}^D \mathrm{ad}^{\mathrm{pol}}$ through it, by conjugation, and $x|_{I_{K_v}}$ is inflated from a cocycle $\tilde{x}$ of H_v. Here $\mathrm{Jac}\, D_0$ has good reduction over $\mathbb{Q}_p(\zeta_p, (\zeta_p - 1)^{1/5})$ (proof of Proposition 5.5), whose inertia group over $\mathbb{Q}_p^{\mathrm{ur}}$ is cyclic of order $5(p-1)$; an element of 5-power order fixes ζ_p (as $5 \nmid p-1$) and ζ_5 and acts on the special fiber $Y''^5 = V^p - V$ by $Y'' \mapsto \zeta_5^k Y''$, the reduction of a power of $[\zeta_5]$, so it acts on T_0 by a scalar in $\mu_5 \subset \mathcal{O}_{M'}$, which commutes with U. So $\tilde{x}$ vanishes on a Sylow 5-subgroup of H_v, and as restriction to it is injective on cohomology with 5-primary coefficients, $x|_{I_{K_v}}$ is a coboundary: the class of $x|_{G_{K_v}}$ is unramified.

At 5. The isometry φ is Γ-equivariant modulo ϖ^D. If D is odd, then $\mathrm{gr}^D \mathrm{diag} = 0$ and (L1)(i) puts the class of $x|_\Gamma$ in $\mathcal{L}_5$, under the identification of Proposition 6.6(a). If $D = 2$,

the class of $x|_\Gamma$ is 0 by Lemma 7.1 and (L2). If $D \geq 4$ is even, then x is diagonal, and (L1)(ii) puts the class of $x|_\Gamma$ in $H^1_{\mathrm{ur}}(K_5, \Theta)$.

Conclusion. So the class of x lies in $\mathrm{Sel}(W)$ (D odd) or in $\mathrm{Sel}(\Theta)$ (D even), hence is 0: $x(g) = g \cdot \bar{z} - \bar{z}$ for some $\bar{z} \in \mathrm{gr}^D \mathrm{ad}^{\mathrm{pol}}$. Lift $\bar{z}$ to $\tilde{z} \in \mathrm{ad}^{\mathrm{pol}} \cap \varpi^D \mathrm{End}$ and put $\varphi' = (1 - \tilde{z}/2)^{-1}(1 + \tilde{z}/2)\varphi$. As $\tilde{z}$ is skew, this Cayley transform is unitary, so φ' is an isometry. As T_0 has rank 2 over $\mathcal{O}_{M'} \otimes \mathbb{Z}_5$ and $\mathrm{tr}\, \tilde{z} = 0$, $\det(1 \pm \tilde{z}/2) = 1 + \det(\tilde{z})/4$, so φ' is normalized. Also $\varphi' \equiv \varphi \pmod{\varpi^D}$ induces ι_{can}, and its difference cocycle X' is $\equiv X - (g \cdot \tilde{z} - \tilde{z}) \equiv 0 \pmod{\varpi^{D+1}}$. Indeed, with $\mathrm{Cay}(\tilde{z}) = (1 - \tilde{z}/2)^{-1}(1 + \tilde{z}/2)$ we have $1 + X'(g) = \mathrm{Cay}(\tilde{z})\,(1 + X(g))\,(g \cdot \mathrm{Cay}(\tilde{z}))^{-1}$. The map $Z \mapsto g \cdot Z$ is a ring automorphism of End fixing $\mathbb{Z}_5$ and preserving each $\varpi^k \mathrm{End}$, as $g \cdot (\varpi Z) = g(\varpi)\,(g \cdot Z)$ and $g(\varpi) \in \varpi(\mathcal{O}_{M'} \otimes \mathbb{Z}_5)^\times$; so $\mathrm{Cay}(\tilde{z}) \equiv 1 + \tilde{z}$ and $(g \cdot \mathrm{Cay}(\tilde{z}))^{-1} \equiv 1 - g \cdot \tilde{z} \pmod{\varpi^{2D}}$. A product of two elements of $\varpi^D \mathrm{End}$ lies in $\varpi^{2D} \mathrm{End} \subset \varpi^{D+1} \mathrm{End}$, as $D \geq 1$. So φ' has depth at least $D + 1$, which contradicts the choice of D. So $D = \infty$. For each n the set of G_K-equivariant $\mathcal{O}_{M'}$-linear isomorphisms $T'/\varpi^n \to T_0/\varpi^n$ that are isometric modulo $\varpi^n \mathfrak{a}$ (Lemma 5.12(a)) and induce ι_{can} is finite and nonempty, and these sets form an inverse system under reduction. An element of the limit is a G_K-equivariant isomorphism $T' \cong T_0$, which Proposition 5.11 excludes. □

Remark 7.3. The trivial solution $(1, 0, 1)$ has $10p \mid b$ but $b = 0$, so it is not in class (d). For it $T' = T_0$, and the induction runs forever without contradiction. So the hypothesis $b \neq 0$ enters only through Lemma 5.10 and Proposition 5.11. For coprime a, b with $a^p + b^p = c^5$ and $10p \mid b$, $a \neq 0$ and $c \neq 0$ are automatic. No bound on the size of the solution and no starting depth are used: the induction starts at ι_{can}, which exists for every class-(d) solution.

8. The local conditions at 5

This section proves the local inputs (L1) and (L2) of Theorem 7.2. Both say that the comparison of T' with T_0 over $\Gamma = G_{K_5}$ is controlled by finite flat models. The reason is geometric: over a tamely ramified extension $\tilde{F}$ of $\mathbb{Q}_5$ the curves D_u, for all u with $v_5(u) > 5/(2p)$, have smooth models with one and the same special fiber, and at every solution with $10p \mid ab$, labeled so that $5 \mid b$, $u_0 = b/a$ has $v_5(u_0) \geq 2$. So D_{u_0} and D_0 are fibers of one family over a disc, and the 5-torsion group schemes of their Jacobians can be identified through the family (Proposition 8.5). Now consider a Γ-equivariant isomorphism $T'/\varpi^D \to T_0/\varpi^D$ that is isometric modulo $\varpi^D \mathfrak{a}$ and reduces to ι_{can}. Kisin's classification turns it into an isomorphism of Breuil–Kisin modules (Proposition 8.11), and the leading digit of the difference cocycle into a crystalline class (Theorem 8.12). Section 8.1 constructs the model, and Section 8.2 proves a rigidity lemma for Breuil–Kisin modules (Lemma 8.3) and, from it, specialization in a family of finite flat group schemes (Lemma 8.4); Section 8.3 deduces (L2) (Proposition 8.5). For $f = \mathrm{ord}_p 5$ even, Sections 8.4, 8.5 and 8.6 compute the Breuil–Kisin modules of the CM point and prove (L1) (Theorem 8.12); Section 8.7 treats f odd.

8.1. **The model at 5.** Recall that $\nu = (-5)^{1/4p}$ and $\tilde{F} = \mathbb{Q}_{5f}(\nu)$ (Section 1.5), and put $\lambda_5 = \nu^p$ (so $\lambda_5^4 = -5$, and $\mathbb{Q}_5(\lambda_5) = \mathbb{Q}_5(\zeta_5)$ as $(1 - \zeta_5)^4$ is -5 times a fourth power). Note that $\tilde{F} = \mathbb{Q}_5(\nu, \mu_{4p})$ is a tamely ramified Galois extension of $\mathbb{Q}_5$ with $e(\tilde{F}/\mathbb{Q}_5) = 4p$, containing ζ_5 and ζ_p, of degree $2pf$ over K_5 (prime to 5). For u algebraic over $\mathbb{Q}_5$ with $v_5(u) > 5/(2p)$ let $K_u = \tilde{F}(u)$, $w = u/\nu^{10} \in \mathfrak{m}_{K_u}$, $\epsilon = (1 + u^p)^{1/5}$ and $\gamma_u = -(1 - u^p)^{1/5}$ the

principal fifth roots, and

$$\mathcal{Q}_u(t,\tilde W) = \tilde W^5 - \lambda_5^3\tilde W^4 - 2\lambda_5^2\tilde W^3 - 2\lambda_5\tilde W^2 - \tilde W - (u^p-1)^{-1}D_p(t,-w).$$

Proposition 8.1. *(a) The closure $\mathcal{C}_u$ of $\{\mathcal{Q}_u = 0\}$ in $\mathbb{P}_{\mathcal{O}_{K_u}}(5,p,1)$ is a smooth proper curve with geometrically connected fibers and one point ∞ at infinity. Its generic fiber is D_u, via $R = \nu^5 t$ and $Y = \epsilon^4\gamma_u(1+\lambda_5\tilde W)$, and its special fiber is the curve $\bar C\colon \tilde W^5 - \tilde W = -t^p$, the same for every such u and for $u = 0$.*

(b) The reductions of Φ_a and $[\zeta_5]$ are $[\bar\zeta_p^a]_* + [\bar\zeta_p^{-a}]_*$, with $[\bar\zeta_p^a](t,\tilde W) = (\bar\zeta_p^a t, \tilde W)$, and $\tilde W \mapsto \tilde W + \bar c$, where $\bar c \in \mathbb{F}_5^\times$ is the residue of $(\zeta_5^3-1)/\lambda_5$; they do not depend on u.

(c) For $u \in 5\mathbb{Z}_5$ and every prime $\ell \neq 5$, $T_\ell(\operatorname{Jac} D_u) \cong T_\ell(\operatorname{Jac} D_0)$ as $\mathcal{O}_{M'}$-semilinear $\mathbb{Z}_\ell[G_{\mathbb{Q}_5}]$-modules, compatibly with the Weil pairings.

(d) For $u \in 5\mathbb{Z}_5$, $V_5(\operatorname{Jac} D_u)$ is crystalline over $\tilde F$, and its Weil–Deligne representation, as an $(M'\otimes\mathbb{Q}_5)$-semilinear representation, is that of $V_5(\operatorname{Jac} D_0)$.

Proof. (a) By homogeneity of the Dickson polynomial, $D_p(\nu^5 t, -\nu^{10}w) = \nu^{5p}D_p(t,-w)$, so $F_u(\nu^5 t) = \gamma_u^5 + \lambda_5^5 D_p(t,-w)$ with $\gamma_u^5 = u^p - 1$. Expanding $(1+\lambda_5\tilde W)^5$ with $5 = -\lambda_5^4$ gives

$$Y^5 - (1+u^p)^4 F_u(R) = \epsilon^{20}\lambda_5^5\gamma_u^5\,\mathcal{Q}_u(t,\tilde W).$$

The polynomial $\mathcal{Q}_u$ has integral coefficients, leading form $\tilde W^5 - (u^p-1)^{-1}t^p$, and all other monomials of weighted degree less than $5p$. The affine curve $\mathcal{Q}_u = 0$ is smooth over $\mathcal{O}_{K_u}$: on the special fiber $\partial\mathcal{Q}_u/\partial\tilde W \equiv -1$, and the generic fiber is D_u, smooth as $\operatorname{disc} F_u = (-1)^{(p-1)/2}p^p(1+u^p)^{p-1} \neq 0$. Lemma 5.3 gives the smooth proper model. Modulo the maximal ideal, $\lambda_5 \equiv 0$, $(u^p-1)^{-1} \equiv -1$ and $D_p(t,-w) \equiv t^p$, so the special fiber is $\bar C$. (b) By (5.2), $\Phi_1 = Z_{u*}$, and $q_u(\nu^5 t, \nu^5 t') = \nu^{10}q_w(t,t')$; the correspondence lies in $(\mathcal{C}_u \smallsetminus \infty)^2$ because $D_p(t',-w) - D_p(t,-w)$ is divisible by $q_w(t,t')$, and $q_w(t,X) \equiv (X-\zeta_p t)(X-\zeta_p^{-1}t)$ modulo the maximal ideal. Lemma 5.4 gives $\bar\Phi_1 = [\bar\zeta_p]_* + [\bar\zeta_p^{-1}]_*$, and $\Phi_a = D_a(\Phi_1, 1)$ gives $\bar\Phi_a$. The automorphism $[\zeta_5]$ maps $(t,\tilde W)$ to $(t, \zeta_5^3\tilde W + (\zeta_5^3-1)/\lambda_5)$. (c) For $u \in 5\mathbb{Z}_5$, $K_u = \tilde F$ and $\epsilon, \gamma_u \in \mathbb{Q}_5$, so $\sigma \in G_{\mathbb{Q}_5}$ acts on the model by $t \mapsto (\nu/\sigma(\nu))^5 t$, $\tilde W \mapsto (\lambda_5/\sigma(\lambda_5))\tilde W$, independently of u. Specialization through the abelian scheme $\operatorname{Pic}^0(\mathcal{C}_u/\mathcal{O}_{\tilde F})$ identifies $T_\ell(\operatorname{Jac} D_u)$ with $T_\ell(\operatorname{Jac}\bar C)$, equivariantly for these descent data, linearly for the reductions of (b), and isometrically. Composing it with the inverse identification for $u = 0$ gives (c). (d) $V_5(\operatorname{Jac} D_u)$ is the Tate module of the 5-divisible group of an abelian scheme over $\mathcal{O}_{\tilde F}$, so it is crystalline over $\tilde F$; the crystalline comparison theorem identifies D_{cris} with H^1_{cris} of the special fiber, with its Frobenius, the reductions of the endomorphisms and the descent data, all independent of u by (a)–(c), and the Weil–Deligne representation is built from these data [31, 2.3.7]. □

At every solution with $10p \mid abc$, labeled so that $5 \mid b$, Lemma 8.2 gives $25 \mid b$, so $u_0 = b/a$ has $v_5(u_0) \geq 2 > 5/(2p)$ and the proposition applies to u_0.

Lemma 8.2. *Let $p \geq 7$ and a, b, c integers with $\gcd(a,b) = 1$, $a^p + b^p = c^5$, $p \nmid c$ and $5 \mid b$. Then $25 \mid b$.*

Proof. Let $\zeta = \zeta_p$, and let c, σ_s ($s \in (\mathbb{Z}/p)^\times$, written σ_k there) and θ_{Stick} be as in Lemma 4.3. The ideals $(a+\zeta^i b)$ are pairwise coprime, since a common prime would divide $(\zeta^i - \zeta^j)\gcd(a,b)$, hence p, and then $p \mid a+b \mid c^5$, so $p \mid c$. As $\prod_i(a+\zeta^i b) = c^5$, $(a+\zeta b) = \mathfrak{A}^5$. As $5 \mid b$, $a+\zeta b$ is prime to 5 and $(a+\zeta b)/(a+\zeta^{-1}b) \equiv 1 + (\zeta-\zeta^{-1})b/a \pmod{25}$. If $b = 5b'$ with $5 \nmid b'$, Lemma 4.3, applied to $a+\zeta b$ with $y = (b'/a)(\zeta-\zeta^{-1})$, gives $\big((1-\mathsf{c})p\theta_{\mathrm{Stick}}\big)\zeta \equiv 0 \pmod 5$ (as $p\theta_{\mathrm{Stick}}y = (b'/a)\big((1-\mathsf{c})p\theta_{\mathrm{Stick}}\big)\zeta$ and b'/a is a 5-adic unit), where $(1-\mathsf{c})p\theta_{\mathrm{Stick}} =$

$\sum_s (2s-p)\sigma_s^{-1}$; as $\{\sigma(\zeta)\}$ is a basis of $\mathbb{Z}[\zeta]$, every $2s-p$ would be divisible by 5. The coefficients for $s=1,2$ differ by 2, so this is false. □

Under $5 \nmid h^-(\mathbb{Q}(\zeta_p))$ this is the case $q=5$ of the congruence $x \equiv 0 \pmod{q^2}$, one of the three congruences modulo q^2 of [57, Theorem 2]. The proof is Mihăilescu's Stickelberger argument for $q^2 \mid x$ in Catalan's equation [56], [7, Theorem 3.2 and §3.1], which needs no class-number hypothesis.

8.2. **Breuil–Kisin modules killed by a prime.** In this subsection ℓ is any prime, k a finite field of characteristic ℓ, $e \geq 1$, and ϕ the Frobenius of $k[[u]]$, where u is a formal variable (not the parameter u of D_u). A *Breuil–Kisin module of height* ≤ 1 killed by ℓ is a finite free $k[[u]]$-module with a ϕ-semilinear endomorphism whose linearization has cokernel killed by u^e. In a basis it is $x \mapsto A\phi(x)$ for a matrix A such that $u^e A^{-1}$ is integral. A morphism is a matrix H with $HA = A'\phi(H)$.

Lemma 8.3. *(a) If $H_0 A \equiv A'\phi(H_0) \pmod{u^N}$ with $N > e\ell/(\ell-1)$, there is exactly one morphism H with $H \equiv H_0 \pmod{u^{N-e}}$.*

(b) A morphism Δ with $\Delta \equiv 0 \pmod{u^s}$, $s > e/(\ell-1)$, is zero.

(c) If $A \equiv A' \pmod{u^N}$ with $N > e\ell/(\ell-1)$, the morphism of (a) with $H_0 = 1$ is an isomorphism, and these isomorphisms commute with morphisms that are congruent modulo u^{N-e}, and likewise with g-semilinear maps $x \mapsto Cg(x)$ that commute with the Frobenius maps and are congruent modulo u^{N-e}, for automorphisms g of $k[[u]]$ with $g(u) \in k^\times u$.

Proof. Parts (a) and (b) are, after extending the coefficients from $\mathbb{F}_\ell$ to a finite field containing k, the case of height one and no descent data of [12, Lemma 3.1.10(2) and (1)]; the morphism of (a) is unique, so it is defined over $\mathbb{F}_\ell$. In (a), $H \equiv H_0 \pmod{u^{N-e}}$ because a matrix whose product with A is $\equiv 0 \pmod{u^N}$ is $\equiv 0 \pmod{u^{N-e}}$, as $u^e A^{-1}$ is integral (as in the proof of [12, Lemma 3.1.10(2)]). (c) $\det H \equiv 1 \pmod{u}$, so H is invertible. For compatibility, the two composites around the square (the isomorphism after one morphism, and the other morphism after the isomorphism) differ by a morphism $\equiv 0 \pmod{u^{N-e}}$, and $N-e > e/(\ell-1)$, so the difference is 0 by (b). A g-semilinear map $x \mapsto Cg(x)$ commutes with the Frobenius maps if and only if C is a morphism from the module with matrix $g(A)$, again of height ≤ 1, and $g(H)$ is the isomorphism of (a) for $g(A) \equiv g(A')$; so the semilinear case is the linear one. □

The bound is sharp when $(\ell-1) \mid e$: for $N = e\ell/(\ell-1)$ the modules with matrices $\left(\begin{smallmatrix} 1 & cu^N \\ 0 & u^e \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & u^e \end{smallmatrix}\right)$ are isomorphic if and only if $c = y^\ell - y$ for some $y \in k$.

Lemma 8.4 (specialization in a family)**.** *Let ℓ be an odd prime, $K/\mathbb{Q}_\ell$ a finite extension with residue field k, ramification index e and uniformizer π, $R = \mathcal{O}_K[[z]]$, and m an integer with $m > e\ell/(\ell-1)$. Let $\mathrm{FF}_\ell(R)$ be the category of commutative finite flat group schemes over R killed by ℓ, with all homomorphisms of group schemes over R, and for $t \in \{\pi^m, 0\}$ write $\mathcal{Y} \mapsto \mathcal{Y}_t$ for base change along the $\mathcal{O}_K$-algebra map $s_t\colon R \to \mathcal{O}_K$, $z \mapsto t$. There is an isomorphism F from the functor $\mathcal{Y} \mapsto \mathcal{Y}_{\pi^m}$ to the functor $\mathcal{Y} \mapsto \mathcal{Y}_0$ on $\mathrm{FF}_\ell(R)$, that is, a family of isomorphisms $F_\mathcal{Y}\colon \mathcal{Y}_{\pi^m} \to \mathcal{Y}_0$ of group schemes over $\mathcal{O}_K$, such that:*

(a) $F_{\mathcal{Y}'} \circ j_{\pi^m} = j_0 \circ F_\mathcal{Y}$ for every homomorphism $j\colon \mathcal{Y} \to \mathcal{Y}'$ in $\mathrm{FF}_\ell(R)$; in particular $F_\mathcal{Y}$ commutes with the endomorphisms of $\mathcal{Y}$, $F_\mathcal{Y}(y_{\pi^m}) = y_0$ for every $y \in \mathcal{Y}(R)$, and $F_\mathcal{Y}$ is the identity if $\mathcal{Y} = \mathcal{Z} \otimes_{\mathcal{O}_K} R$ for a group scheme $\mathcal{Z}$ over $\mathcal{O}_K$;

(b) let $\zeta \in K$ be a root of unity of order prime to ℓ, and γ a ring automorphism of R with $\gamma(\mathcal{O}_K) = \mathcal{O}_K$, $\gamma(\pi) = \zeta\pi$ and $\gamma(z) = \zeta^m z$. Then γ preserves the ideals $(z - \pi^m)$

and (z), and for every γ-semilinear automorphism c of $\mathcal{Y}$ (an isomorphism $\mathcal{Y} \to \gamma^*\mathcal{Y}$ of group schemes over R), with induced $\gamma|_{\mathcal{O}_K}$-semilinear automorphisms $c_{z=t}$ of $\mathcal{Y}_t$, $F_{\mathcal{Y}} \circ c_{z=\pi^m} = c_{z=0} \circ F_{\mathcal{Y}}$.

Proof. Steps 1–2: the frames and the classification. Let $E(u) \in W(k)[u]$ be the Eisenstein polynomial of π, write $E(0) = \ell c_0$ with $c_0 \in W(k)^\times$, and set $E_1 = E/c_0$, whose constant term is ℓ. Put $\mathfrak{S}_R = W(k)[[u, z]]$ and $\mathfrak{S} = W(k)[[u]]$, with the endomorphisms σ that extend the Frobenius of $W(k)$ by $\sigma(u) = u^\ell$ and $\sigma(z) = z^\ell$. The surjections $\mathfrak{S}_R \to R$ $(u \mapsto \pi,\ z \mapsto z)$ and $\mathfrak{S} \to \mathcal{O}_K$ $(u \mapsto \pi)$ send u, z, resp. u, to regular systems of parameters and have kernels generated by E_1, and k is perfect of characteristic $\ell \geq 3$. These are the hypotheses of [50, §7] for the complete regular local rings R and $\mathcal{O}_K$, with Lau's E taken to be E_1 (constant term ℓ, image 0), and the only further condition for a κ-frame, that $(\sigma^2(E_1) - \sigma(E_1)^\ell)/\ell$ is a unit, is checked in the proof of [50, Lemma 7.1]. So [50, §7, Lemma 7.1] give the κ-frames $\mathcal{B}_R = (\mathfrak{S}_R, E_1\mathfrak{S}_R, R, \sigma, \sigma_1)$ and $\mathcal{B} = (\mathfrak{S}, E_1\mathfrak{S}, \mathcal{O}_K, \sigma, \sigma_1)$, where $\sigma_1(E_1 y) = \sigma(y)$, and frame homomorphisms with units $\kappa\colon \mathcal{B}_R \to \mathcal{D}_R$ and $\kappa\colon \mathcal{B} \to \mathcal{D}_{\mathcal{O}_K}$ to the Dieudonné frames, functorial for strict frame homomorphisms and crystalline, that is, base change of windows along κ is an equivalence [50, Definition 3.1, Proposition 6.3, Corollary 6.5, Theorem 7.2]. For an ℓ-divisible group X over R let $Q(X)$ be the Breuil window (a free $\mathfrak{S}_R$-module Q of finite rank with a linear map $\phi_Q\colon Q \to Q^{(\sigma)} = \mathfrak{S}_R \otimes_{\sigma,\mathfrak{S}_R} Q$ whose cokernel is killed by E_1) whose base change along κ is the Dieudonné display $\Phi_R(X)$ [51, Theorem 3.19, Lemma 2.16, Corollary 5.5]; $X \mapsto Q(X)$ is a covariant equivalence of exact categories [50, Definition 8.1, Lemma 8.2, Corollary 8.3], [51, Corollary 6.7]. For a finite flat group scheme $\mathcal{Y}$ over R of ℓ-power order, let $M(\mathcal{Y}) = \operatorname{coker}(Q(G_0) \to Q(G_1))$ for an isogeny $G_0 \to G_1$ of ℓ-divisible groups with kernel $\mathcal{Y}$. This gives a covariant equivalence with Breuil modules (M, ϕ_M, ψ_M): M is a finitely generated $\mathfrak{S}_R$-module killed by a power of ℓ, of projective dimension at most one, and $\phi_M\colon M \to M^{(\sigma)}$, $\psi_M\colon M^{(\sigma)} \to M$ are linear maps with $\phi_M\psi_M = \psi_M\phi_M = E_1$ [50, Definition 8.4, Theorem 8.5 and its proof], [51, Corollary 6.8]. All of this holds over $\mathcal{O}_K$ with $\mathcal{B}$.

Step 3: base change. For $t \in \{\pi^m, 0\}$ let $\alpha_t\colon \mathfrak{S}_R \to \mathfrak{S}$ be the $W(k)$-algebra map with $u \mapsto u$ and $z \mapsto u^m$, resp. $z \mapsto 0$; it lies over s_t. It fixes $E_1 \in W(k)[u]$, so $\alpha_t(E_1\mathfrak{S}_R) \subseteq E_1\mathfrak{S}$; it commutes with σ, as both composites send z to $u^{m\ell}$, resp. 0; and $\sigma_1(\alpha_t(E_1 y)) = \sigma(\alpha_t(y)) = \alpha_t(\sigma(y)) = \alpha_t(\sigma_1(E_1 y))$. So α_t is a frame homomorphism $\mathcal{B}_R \to \mathcal{B}$ with unit 1, that is, strict [50, Definition 2.7]. This holds for every $m \geq 1$: the bound $m > e\ell/(\ell - 1)$ is used only in Steps 5 and 6, as the hypothesis of Lemma 8.3(a) and (c) with $N = m$ (and of Lemma 8.3(b) with $s = m - e$, the same inequality), since the specialized matrices $A(u, u^m)$ and $A(u, 0)$ of Step 4 are congruent only modulo u^m. The same check shows that every ring map α between the rings $\mathfrak{S}_R$, $\mathfrak{S}$ that commutes with σ, fixes E_1 and lies over a ring map s between R, $\mathcal{O}_K$ is a strict frame homomorphism; we use the α_t, the inclusion $\iota\colon \mathfrak{S} \to \mathfrak{S}_R$ (over $\mathcal{O}_K \to R$), and in (b) two automorphisms $\hat{\gamma}$, $\hat{\gamma}'$. For such an $\alpha\colon \mathfrak{S}_1 \to \mathfrak{S}_2$ over $s\colon R_1 \to R_2$: (i) base change of windows [50, Lemma 2.10] takes the Breuil window (Q, ϕ_Q) to $(\mathfrak{S}_2 \otimes_\alpha Q, 1 \otimes \phi_Q)$, by the explicit normal representation in the proof of [50, Lemma 2.10] and the dictionary of [50, Lemma 8.2], as $\alpha(E_1) = E_1$; (ii) $\alpha_* Q(X) \cong Q(X \otimes_s R_2)$, naturally in X: by the functoriality of [50, Proposition 6.3], $\kappa \circ \alpha = \mathcal{D}(s) \circ \kappa$ with matching units, so $\kappa_*\alpha_* Q(X) \cong \mathcal{D}(s)_* \Phi_{R_1}(X) \cong \Phi_{R_2}(X \otimes_s R_2)$, the second isomorphism being the compatibility of Φ with base change [51, Theorem 3.19], applied to $R_1/\mathfrak{m}_{R_1}^n \to R_2/\mathfrak{m}_{R_2}^n$ and passed to the limit [51, Lemma 2.16]; and κ_* is an equivalence. These isomorphisms are transitive for composites of such α, as those of Φ are (they are those of the Dieudonné crystal, [51, Construction 3.16 and proof of Theorem 3.19])

and κ_* is fully faithful; (iii) $M(\mathcal{Y}\otimes_s R_2)\cong\mathfrak{S}_2\otimes_\alpha M(\mathcal{Y})$, with $1\otimes\phi_M$ and $1\otimes\psi_M$, naturally in $\mathcal{Y}$ and transitively: base change keeps $0\to\mathcal{Y}\to G_0\to G_1\to 0$ exact as fppf sheaves, tensor products are right exact, and M of a morphism is built from isogenies.

Step 4: matrices, and the canonical identification. Let $\mathcal{Y}\in\mathrm{FF}_\ell(R)$. As M is additive, $M(\mathcal{Y})$ is killed by ℓ; it has projective dimension ≤ 1 over the regular local ring $\mathfrak{S}_R$ of dimension 3, hence depth ≥ 2 (Auslander–Buchsbaum), so it is free over the regular local ring $\mathfrak{S}_R/\ell=k[[u,z]]$ of dimension 2. Fix a basis (e_i) and let $A=A(u,z)$ be the matrix of ψ_M in the bases $(1\otimes e_i)$ of $M^{(\sigma)}$ and (e_i) of M; as $\phi_M\psi_M=E_1\equiv\bar c_0^{-1}u^e \pmod\ell$, u^eA^{-1} is integral. Over $\mathfrak{S}$, likewise, a Breuil module killed by ℓ is free over $k[[u]]$, and $x\mapsto\psi_M(1\otimes x)$ makes it a Breuil–Kisin module of height ≤ 1 in the sense of Section 8.2, with matrix A; a $k[[u]]$-linear map commuting with the maps ψ commutes with the maps ϕ (apply the injective $\psi_{M'}$ to $\phi_{M'}H-H^{(\sigma)}\phi_M$), so the morphisms of Breuil modules killed by ℓ are the morphisms of these Breuil–Kisin modules. By Step 3(iii), $M(\mathcal{Y}_t)=\mathfrak{S}\otimes_{\alpha_t}M(\mathcal{Y})$ has the basis $(1\otimes e_i)$, in which ψ has the matrix $\alpha_t(A)$: $A(u,u^m)$ for $t=\pi^m$ and $A(u,0)$ for $t=0$, which are congruent modulo u^m. The maps α_{π^m} and α_0 agree modulo u^m: both reduce to $\bar\alpha\colon\mathfrak{S}_R\to\mathfrak{S}/u^m$, $u\mapsto u$, $z\mapsto 0$. Hence $M(\mathcal{Y}_{\pi^m})/u^m$ and $M(\mathcal{Y}_0)/u^m$ are both $(\mathfrak{S}/u^m)\otimes_{\bar\alpha}M(\mathcal{Y})=M(\mathcal{Y})/(z,u^m)$, with the same reduction of ψ; we call this identification $\eta_{\mathcal{Y}}$. It involves no choice, and in the bases $(1\otimes e_i)$ it is the identity matrix (for another basis $(e_i)P$ of $M(\mathcal{Y})$ both bases change by $\alpha_t(P)$, and $\alpha_{\pi^m}(P)\equiv\alpha_0(P) \pmod{u^m}$). For $j\colon\mathcal{Y}\to\mathcal{Y}'$ with matrix $J(u,z)$, $M(j_{\pi^m})$ and $M(j_0)$ have the matrices $J(u,u^m)$ and $J(u,0)$.

Step 5: the isomorphism, and (a). As $A(u,u^m)\equiv A(u,0) \pmod{u^m}$ and $m>e\ell/(\ell-1)$, Lemma 8.3(a) and (c), with $N=m$, give a unique morphism $H_{\mathcal{Y}}\colon M(\mathcal{Y}_{\pi^m})\to M(\mathcal{Y}_0)$ congruent to $\eta_{\mathcal{Y}}$ modulo u^{m-e}, and it is an isomorphism; by Step 4 it is an isomorphism of Breuil modules, so $H_{\mathcal{Y}}=M(F_{\mathcal{Y}})$ for a unique isomorphism $F_{\mathcal{Y}}\colon\mathcal{Y}_{\pi^m}\to\mathcal{Y}_0$ [50, Theorem 8.5]. For $j\colon\mathcal{Y}\to\mathcal{Y}'$ in $\mathrm{FF}_\ell(R)$, the morphisms $H_{\mathcal{Y}'}M(j_{\pi^m})$ and $M(j_0)H_{\mathcal{Y}}$ both have matrices $\equiv J(u,0) \pmod{u^{m-e}}$, so their difference vanishes by Lemma 8.3(b), as $m-e>e/(\ell-1)$; M being faithful, $F_{\mathcal{Y}'}j_{\pi^m}=j_0F_{\mathcal{Y}}$. If $\mathcal{Y}=\mathcal{Z}\otimes_{\mathcal{O}_K}R$, then $M(\mathcal{Y})=\mathfrak{S}_R\otimes_\iota M(\mathcal{Z})$ (Step 3), so a basis of $M(\mathcal{Z})$ gives one of $M(\mathcal{Y})$ in which A does not involve z. As $\alpha_t\iota=\mathrm{id}$, transitivity identifies both $M(\mathcal{Y}_t)$ with $M(\mathcal{Z})$, compatibly with $\mathcal{Y}_t=\mathcal{Z}$, and $\eta_{\mathcal{Y}}$ with the identity. So $H_{\mathcal{Y}}=\mathrm{id}$ and $F_{\mathcal{Y}}=\mathrm{id}$. This applies to $(\mathbb{Z}/\ell)_R$, and a point $y\in\mathcal{Y}(R)$ is a homomorphism $(\mathbb{Z}/\ell)_R\to\mathcal{Y}$, as $\ell\mathcal{Y}=0$; so $F_{\mathcal{Y}}(y_{\pi^m})=y_0$.

Step 6: (b). As ζ has order prime to ℓ and K is totally ramified over $W(k)[1/\ell]$, $\zeta\in W(k)$; and $\gamma(z-\pi^m)=\zeta^m(z-\pi^m)$. Let $\hat\gamma$ be the automorphism of $\mathfrak{S}_R$ that acts on $W(k)$ as γ does on $W(k)\subset\mathcal{O}_K$, with $\hat\gamma(u)=\zeta u$ and $\hat\gamma(z)=\zeta^m z$, and $\hat\gamma'$ that of $\mathfrak{S}$ with $\hat\gamma'(u)=\zeta u$; they lie over γ and $\gamma|_{\mathcal{O}_K}$, $\alpha_t\hat\gamma=\hat\gamma'\alpha_t$, and they commute with σ, as $\sigma(\zeta)=\zeta^\ell$. They fix E_1: applying γ to the coefficients of E gives the minimal polynomial of $\gamma(\pi)=\zeta\pi$ over $W(k)[1/\ell]$, which is $\zeta^eE(\zeta^{-1}u)$; so the image of E under $\hat\gamma$ is $\zeta^eE(u)$, comparing constant terms $\gamma(c_0)=\zeta^ec_0$, and $\hat\gamma(E_1)=E_1$. So they are strict frame automorphisms (Step 3). By Step 3(iii) along $\hat\gamma$, c gives a $\hat\gamma$-semilinear automorphism of $M(\mathcal{Y})$ commuting with ψ_M, $x\mapsto C\hat\gamma(x)$ in the basis (e_i), and by transitivity $M(c_{z=\pi^m})$ and $M(c_{z=0})$ are $x\mapsto C(u,u^m)\hat\gamma'(x)$ and $x\mapsto C(u,0)\hat\gamma'(x)$, which are congruent modulo u^m. As $\hat\gamma'$ reduces modulo ℓ to an automorphism g of $k[[u]]$ with $g(u)\in k^\times u$, Lemma 8.3(c) in its semilinear form gives $H_{\mathcal{Y}}M(c_{z=\pi^m})=M(c_{z=0})H_{\mathcal{Y}}$, hence $F_{\mathcal{Y}}c_{z=\pi^m}=c_{z=0}F_{\mathcal{Y}}$. □

8.3. **The residual identification comes from models.** Keep the notation of Section 8.1, with ν the uniformizer of $\tilde F$; its Eisenstein polynomial over $W(k)$, $k=\mathbb{F}_{5^f}$, is $u^{4p}+5$. For $g\in\mathrm{Gal}(\tilde F/\mathbb{Q}_5)$ put $\zeta_g=g(\nu)/\nu\in\mu_{4p}$. For $u_0\in\mathbb{Q}_5$ with $v_5(u_0)>5/(2p)$ let $\mathcal{J}_{u_0}$ be the

abelian scheme $\mathrm{Pic}^0(\mathcal{C}_{u_0}/\mathcal{O}_{\tilde F})$, the Néron model of $\mathrm{Jac}\, D_{u_0}$ over $\mathcal{O}_{\tilde F}$, with its action of $\mathcal{O}_{M'}$ and the descent data of $\mathrm{Gal}(\tilde F/\mathbb{Q}_5)$.

Proposition 8.5. *Let $u_0 \in \mathbb{Q}_5$ with $v_5(u_0) \geq 2$. There is an isomorphism of finite flat group schemes $F\colon \mathcal{J}_{u_0}[5] \to \mathcal{J}_0[5]$ over $\mathcal{O}_{\tilde F}$ that commutes with $\mathcal{O}_{M'}$ and with the descent data, and satisfies $F(e_j(u_0)) = e_j(0)$ for every j. Hence F induces an $\mathcal{O}$-linear Γ-equivariant isomorphism $T'/5T' \cong T_0/5T_0$ that is $\equiv \iota_{\mathrm{can}} \pmod{\varpi}$, and* (L2) *of Theorem 7.2 holds at every solution with $10p \mid ab$, labeled so that $5 \mid b$.*

Proof. We put D_{u_0} and D_0 into one family over $\mathcal{O}_{\tilde F}[[z]]$, as its fibers at $z = \nu^{5p+1}$ and $z = 0$, and apply Lemma 8.4 to the 5-torsion of its Jacobian. We may assume $u_0 \neq 0$. Let $m = 5p+1$, $r = u_0/\nu^m$ and $R = \mathcal{O}_{\tilde F}[[z]]$. Then $v_5(r) = v_5(u_0) - (5p+1)/4p \geq (3p-1)/4p > 5/(2p)$, so $w = rz/\nu^{10}$ lies in the maximal ideal of R, and the equation $\mathcal{Q}_{rz}$ of Section 8.1 has coefficients in R. Let $\mathcal{C}_R$ be its closure in $\mathbb{P}_R(5, p, 1)$. The affine part is free over $R[t]$ (the equation is monic in $\tilde W$) and Lemma 5.3 applies near ∞, so $\mathcal{C}_R$ is flat and proper over R; its fiber over the closed point is the smooth curve $\bar C$, so its non-smooth locus, closed with closed image in $\operatorname{Spec} R$, is empty. Thus $\mathcal{C}_R$ is a smooth proper curve over R with a section ∞. Its fibers are geometrically connected, since $\bar C$ is and the number of geometric connected components of the fibers of a smooth proper morphism is locally constant on the base, so $\mathcal{J}_R = \mathrm{Pic}^0(\mathcal{C}_R/R)$ is an abelian scheme. Its fibers at $z = \nu^m$ and $z = 0$ are $\mathcal{J}_{u_0}$ and $\mathcal{J}_0$. The points $P_j = [\zeta_p^j - rz\zeta_p^{-j} : -1 : \nu]$ (weights $5, p, 1$; in the coordinates of D_u this is the point $(\zeta_p^j - rz\zeta_p^{-j}, 0)$) are R-points, and $e_j = [P_j - \infty] \in \mathcal{J}_R[\varpi](R)$ specializes to $e_j(u_0)$ and $e_j(0)$. The automorphism $[\zeta_5]$ is given by a formula independent of u. The endomorphism Φ_1 of the generic fiber extends to $\mathcal{J}_R$ [28, Chapter I, Proposition 2.7], and its specializations are the Φ_1 of the two fibers. Indeed, for a point $P = (t_1, \tilde W_1)$ of the fiber at a point $z = z_1$ of the open unit disc, with z_1 and P defined over a finite extension K_1 of $\tilde F$, Hensel's lemma ($\partial\mathcal{Q}_{rz}/\partial\tilde W \equiv -1$) lifts it to $\tilde P = (t_1, \tilde W(z)) \in \mathcal{C}_R(R_1)$, $R_1 = \mathcal{O}_{K_1}[[z]]$. The divisor $\{q_w(t_1, t) = 0,\ \tilde W = \tilde W(z)\}$, finite flat of degree 2, represents $\Phi_1[\tilde P - \infty] + 2\infty$ at the generic point by (5.2), hence over R_1 by separatedness of $\mathcal{J}_R$. At $z = z_1$ this is $\Phi_1[P - \infty]$, and a morphism from a curve to its Jacobian that vanishes at infinitely many points is zero. So the family carries the $\mathcal{O}_{M'}$-action of both fibers. The group $\mathrm{Gal}(\tilde F/\mathbb{Q}_5)$ acts on R by $\sum a_n z^n \mapsto \sum g(a_n)(\zeta_g^m z)^n$ (as rz is fixed and $g(r) = \zeta_g^{-m} r$), and on $\mathcal{C}_R$ by the descent formulas of Proposition 8.1(c).

Apply Lemma 8.4 with $\ell = 5$, $K = \tilde F$ (residue field $\mathbb{F}_{5^f}$), $e = 4p$, $\pi = \nu$, $E(u) = u^{4p} + 5$ (constant term ℓ) and $\mathcal{Y} = \mathcal{J}_R[5]$; its only numerical condition is $m = 5p + 1 > 5e/4$. Let $F = F_{\mathcal{Y}}$. By (a), applied to the endomorphisms $[\zeta_5]$ and Φ_1 of $\mathcal{Y}$, which specialize to those of both fibers, F commutes with $\mathcal{O}_{M'} = \mathbb{Z}[\zeta_5, \Phi_1]$; applied to the R-points e_j, it gives $F(e_j(u_0)) = e_j(0)$. By (b), with $\zeta = \zeta_g$ (of order dividing $4p$) and $(\zeta_g u)^{4p} + 5 = u^{4p} + 5$, F commutes with the descent data. On points over an algebraic closure of $\tilde F$, F is therefore $G_{\mathbb{Q}_5}$-equivariant and $\mathcal{O}_{M'}$-linear. As the e_j generate the ϖ-torsion (Lemma 5.2(a)), F restricts to $e_j(u_0) \mapsto e_j(0)$ there. As ω_5 is trivial on $G_{\tilde F}$ and the identifications $t \mapsto 5^{-1}t$, $t \mapsto \varpi^{-1}t$ are compatible through multiplication by $5/\varpi \in \mathcal{O}_{M'} \otimes \mathbb{Z}_5$, the induced map $T'/5T' \to T_0/5T_0$ reduces to ι_{can} modulo ϖ. Since $5\mathcal{O} = \varpi^4\mathcal{O}$, its reduction modulo ϖ^3 is the isomorphism required in (L2); at every solution with $10p \mid ab$, labeled so that $5 \mid b$, Lemma 8.2 gives $v_5(u_0) \geq 2$. □

Remark 8.6. The family is what makes the identification canonical. Two abelian schemes over $\mathcal{O}_{\tilde F}$ that are congruent modulo an ideal of valuation greater than $5/4$ have isomorphic 5-torsion Galois modules by Fontaine's lemma, but when $e(\tilde F/\mathbb{Q}_5) = 4p \geq 4$ a Galois

module can have several finite flat models, and the argument of Proposition 8.11 needs the isomorphism of models. For the ℓ-torsion of ℓ-divisible groups, such as $\mathcal{J}_R[5]$, the statement of Lemma 8.4(a) on points also follows from Fontaine's lifting lemma [29, Proposition 1.7], which lifts a point given modulo ℓI, for an ideal I with topologically nilpotent divided powers, to a unique point congruent to it modulo I, and so compares Galois modules; Lemma 8.4 compares the finite flat models themselves, naturally in $\mathcal{Y}$ and compatibly with semilinear automorphisms, which is what carries the action of $\mathcal{O}_{M'}$ and the descent data in Proposition 8.5. Kisin's moduli of finite flat models [44, §§1.2, 2.1] vary the coefficient ring of a fixed Galois representation over a fixed base; here the base varies, along $\mathcal{O}_{\tilde{F}}[[z]]$, and the Galois modules of the two fibers are not given in advance. We know of no reference for Lemma 8.4 in this form. The parameter is normalized so that the solution sits at $z = \nu^m$, $m = 5p+1$, the least integer above the bound $e\ell/(\ell-1) = 5p$ of Lemma 8.4 ($e = 4p$, $\ell = 5$), which is Fontaine's ramification bound for group schemes killed by ℓ [29, Théorème A]. The family exists when $r = u_0/\nu^m$ satisfies $v_5(r) > 5/(2p) = v_5(\nu^{10})$, so that $w = rz/\nu^{10}$ lies in the maximal ideal of R; as $v_5(r) = v_5(u_0) - (5p+1)/4p$, this holds whenever $v_5(u_0) > (5p+11)/4p$, and $(5p+11)/4p < 2$ for $p \geq 7$. At every solution with $10p \mid ab$, labeled so that $5 \mid b$, Lemma 8.2 gives $25 \mid b$, so $v_5(u_0) \geq 2$ and the precision $m = 5p+1$ is available.

8.4. **Breuil–Kisin modules of the CM point.** We first give the set-up for f even; the variant for f odd is recorded below after the definition of the tangent space. The results in this subsection and the next two assume f even, except Example 8.8 and Lemma 8.9; Section 8.7 treats the odd case. Fix a prime λ of M above λ' and put $E = M_\lambda = \mathbb{Q}_{5^f}(\zeta_5)$, $\mathcal{O}_E = W(k)[\zeta_5]$, with uniformizer ϖ. Over G_E everything is $\mathcal{O}_E$-linear, and $T_0 \otimes_{\mathcal{O}} \mathcal{O}_E = \mathcal{O}_E v_1 \oplus \mathcal{O}_E v_2$ with G_E acting by ψ and $\sigma_m \circ \psi$ (Section 6.1), both crystalline over $\tilde{F}$ with weights in $\{0,1\}$ and both $\equiv 1 \pmod{\varpi}$ on G_E (Lemma 6.3). Let $\mathfrak{S} = W(k)[[u]]$ with $u \mapsto \nu$ and $E(u) = u^{4p} + 5$, $\mathfrak{S}_{\mathcal{O}_E} = \mathfrak{S} \otimes_{\mathbb{Z}_5} \mathcal{O}_E = \prod_{j \in \mathbb{Z}/f} \mathcal{O}_E[[u]]$ (component j belongs to the embedding Frob^j of $W(k)$ into $\mathcal{O}_E$), with ϕ mapping component j to component $j-1$, and descent data of $\mathrm{Gal}(\tilde{F}/E) \cong \mu_p$ given by $u \mapsto \zeta_g u$, with $\zeta_g = g(\nu)/\nu$ as in Section 8.3. For $g \in \mathrm{Gal}(\tilde{F}/E)$, ζ_g lies in $\mu_p \subset W(k) \subset \mathcal{O}_E$, and on component j of $\mathfrak{S}_{\mathcal{O}_E}$ the element ζ_g of $W(k)$ is $\mathrm{Frob}^j(\zeta_g) = \zeta_g^{5^j}$, so g acts there by $u \mapsto \zeta_g^{5^j} u$. A descent datum on a Breuil–Kisin module is a family of $\mathcal{O}_E$-linear, g-semilinear automorphisms $\hat{g}$ commuting with ϕ. We use Kisin's theory of Breuil–Kisin modules for crystalline representations and for finite flat group schemes [43], [44, §1] over the base $\tilde{F}$, in the form (K1)–(K4) below. Its hypotheses hold here: the residue characteristic 5 is odd, the residue field $k = \mathbb{F}_{5^f}$ is finite, and $\tilde{F}$ is totally ramified over $W(k)[1/5]$, of degree $e = 4p$, with uniformizer ν and Eisenstein polynomial $E(u)$; no bound on e is needed. Let $\tilde{F}_\infty = \bigcup_n \tilde{F}(\nu_n)$ with $\nu_0 = \nu$ and $\nu_{n+1}^5 = \nu_n$, let ϕ act on $\mathfrak{S}$ by the Frobenius of $W(k)$ and $u \mapsto u^5$, let $\mathcal{O}_{\mathcal{E}}$ be the 5-adic completion of $\mathfrak{S}[1/u]$ and $\mathcal{E} = \mathcal{O}_{\mathcal{E}}[1/5]$, and let $\mathcal{O}_{\mathcal{E}^{\mathrm{ur}}} \subset \mathcal{E}^{\mathrm{ur}}$, $\widehat{\mathcal{O}}_{\mathcal{E}^{\mathrm{ur}}}$ and $\mathfrak{S}^{\mathrm{ur}} \subset \widehat{\mathcal{O}}_{\mathcal{E}^{\mathrm{ur}}}$ be the rings of [43, (2.1.1)], with their actions of $G_{\tilde{F}_\infty}$. A *Breuil–Kisin module of finite height* is a finite free $\mathfrak{S}$-module $\mathfrak{M}$ with a ϕ-semilinear map $\phi\colon \mathfrak{M} \to \mathfrak{M}$ whose linearization $1 \otimes \phi\colon \phi^*\mathfrak{M} \to \mathfrak{M}$ has cokernel killed by a power $E(u)^h$ (*height* $\leq h$) [43, (2.1.3)]; a *torsion Breuil–Kisin module of height* ≤ 1 is a finite $\mathfrak{S}$-module killed by a power of 5, of projective dimension 1, with such a ϕ whose linearization has cokernel killed by $E(u)$ [43, (2.3.1)]. Hodge–Tate weights are normalized so that the cyclotomic character has weight 1.

(K1) (a) For $\mathfrak{M}$ of finite height, $T_{\mathfrak{S}}(\mathfrak{M}) = \mathrm{Hom}_{\mathfrak{S},\phi}(\mathfrak{M}, \mathfrak{S}^{\mathrm{ur}})$ is a free $\mathbb{Z}_5$-module of rank $\mathrm{rank}_{\mathfrak{S}} \mathfrak{M}$ with a continuous action of $G_{\tilde{F}_\infty}$, the functor $T_{\mathfrak{S}}$ is exact, and restriction identifies $T_{\mathfrak{S}}(\mathfrak{M})$ with $\mathrm{Hom}_{\mathcal{O}_{\mathcal{E}},\phi}(\mathcal{O}_{\mathcal{E}} \otimes_{\mathfrak{S}} \mathfrak{M}, \widehat{\mathcal{O}}_{\mathcal{E}^{\mathrm{ur}}})$ [43, Corollary (2.1.4)]. This is Fontaine's contravariant functor, an anti-equivalence from finite free étale ϕ-modules over $\mathcal{O}_{\mathcal{E}}$ to finite free $\mathbb{Z}_5$-modules with a continuous action of $G_{\tilde{F}_\infty}$, compatible with tensor products [30, A1.2.6, A1.2.7], [44, (1.1.12)]. As $\mathfrak{M} \mapsto \mathcal{O}_{\mathcal{E}} \otimes_{\mathfrak{S}} \mathfrak{M}$ is fully faithful [43, Proposition (2.1.12)], $T_{\mathfrak{S}}$ is fully faithful on the category of all Breuil–Kisin modules of finite height, whatever their heights; and $\mathfrak{M} \otimes_{\mathfrak{S}} \mathfrak{N}$, with $\phi \otimes \phi$, has finite height and $T_{\mathfrak{S}}(\mathfrak{M} \otimes_{\mathfrak{S}} \mathfrak{N}) = T_{\mathfrak{S}}(\mathfrak{M}) \otimes_{\mathbb{Z}_5} T_{\mathfrak{S}}(\mathfrak{N})$.

(b) If $\mathfrak{M}$ has finite height, $\mathfrak{N} \mapsto T_{\mathfrak{S}}(\mathfrak{N})$ is a bijection from the ϕ-stable finite free $\mathfrak{S}$-submodules $\mathfrak{N}$ of finite height of $\mathcal{E} \otimes_{\mathfrak{S}} \mathfrak{M}$ with $\mathcal{E} \otimes \mathfrak{N} = \mathcal{E} \otimes \mathfrak{M}$ onto the $G_{\tilde{F}_\infty}$-stable $\mathbb{Z}_5$-lattices in $T_{\mathfrak{S}}(\mathfrak{M})[1/5]$ [43, Lemma (2.1.15)]. It reverses inclusions: if $\mathfrak{M} \subset \mathfrak{N} \subset \mathfrak{M}[1/5]$ are such modules, restriction identifies $T_{\mathfrak{S}}(\mathfrak{N})$ with the set of $x \in T_{\mathfrak{S}}(\mathfrak{M})$ which, extended to $\mathfrak{M}[1/5]$, map $\mathfrak{N}$ into $\mathfrak{S}^{\mathrm{ur}}$.

(c) Let T be a $G_{\tilde{F}}$-stable $\mathbb{Z}_5$-lattice in a crystalline representation V of $G_{\tilde{F}}$ with Hodge–Tate weights ≥ 0. Then $T|_{G_{\tilde{F}_\infty}} \cong T_{\mathfrak{S}}(\mathfrak{M}(T))$ for a Breuil–Kisin module $\mathfrak{M}(T)$ of finite height [43, Corollary (1.3.15), Proposition (2.1.5), Lemma (2.1.15)], unique up to unique isomorphism by (a), and restriction to $G_{\tilde{F}_\infty}$ is fully faithful on crystalline representations [43, Corollary (2.1.14)]. Tensor products and exterior powers are compatible with these functors: [45, Theorem (1.2.1)] states this in Kisin's covariant normalization, and applying it to the dual Galois lattices gives it in our contravariant one. We use tensor products for weights in $[0, 2]$. If the weights lie in $\{0, 1\}$, every such T is the Tate module of a 5-divisible group over $\mathcal{O}_{\tilde{F}}$ [10, Theorem 3.2.5 and its proof]; then $\mathfrak{M}(T)$ has height ≤ 1 [43, Theorem (2.2.7) and its proof]. Moreover, as $5 > 2$, $\mathcal{G} \mapsto \mathfrak{M}(\mathcal{G})$ is an anti-equivalence from 5-divisible groups over $\mathcal{O}_{\tilde{F}}$ to Breuil–Kisin modules of height ≤ 1, with $T_{\mathfrak{S}}(\mathfrak{M}(\mathcal{G}))$ the Tate module of $\mathcal{G}$, naturally in $\mathcal{G}$ [43, Theorem (2.2.7) and its proof].

(K2) As $5 > 2$, there is an exact anti-equivalence $\mathcal{H} \mapsto \mathfrak{M}(\mathcal{H})$ from commutative finite flat group schemes of 5-power order over $\mathcal{O}_{\tilde{F}}$ to torsion Breuil–Kisin modules of height ≤ 1, under which the kernel of an isogeny $\mathcal{G}_1 \to \mathcal{G}_2$ of 5-divisible groups goes to the cokernel of $\mathfrak{M}(\mathcal{G}_2) \to \mathfrak{M}(\mathcal{G}_1)$ [43, Theorem (2.3.5) and its proof]; in particular $\mathfrak{M}(\mathcal{G}[\varpi^n]) = \mathfrak{M}(\mathcal{G})/\varpi^n$ for a 5-divisible group $\mathcal{G}$ with an action of $\mathcal{O}_E$. On Galois modules, write $T_{\mathfrak{S}}(\mathfrak{M}) = \mathrm{Hom}_{\mathfrak{S},\phi}(\mathfrak{M}, \mathcal{E}^{\mathrm{ur}}/\mathcal{O}_{\mathcal{E}^{\mathrm{ur}}})$ for torsion $\mathfrak{M}$; then $\mathcal{H}(\overline{\mathbb{Q}}_5)$ restricted to $G_{\tilde{F}_\infty}$ is $T_{\mathfrak{S}}(\mathfrak{M}(\mathcal{H}))$, naturally in $\mathcal{H}$. Indeed, if $\mathcal{H} = \ker(\mathcal{G}_1 \to \mathcal{G}_2)$, then $\mathcal{H}(\overline{\mathbb{Q}}_5)$ is the cokernel of $T_5\mathcal{G}_1 \to T_5\mathcal{G}_2$, that is, by (K1)(c), of $T_{\mathfrak{S}}(\mathfrak{M}(\mathcal{G}_1)) \to T_{\mathfrak{S}}(\mathfrak{M}(\mathcal{G}_2))$. Fontaine's contravariant functors are the $\mathbb{Z}_5$-dual and the Pontryagin dual of an exact functor [30, A1.2.6, A1.2.7], so they turn the exact sequence $0 \to \mathfrak{M}(\mathcal{G}_2) \to \mathfrak{M}(\mathcal{G}_1) \to \mathfrak{M}(\mathcal{H}) \to 0$, tensored with $\mathcal{O}_{\mathcal{E}}$, into an isomorphism of that cokernel with $T_{\mathfrak{S}}(\mathfrak{M}(\mathcal{H}))$. This isomorphism is natural in the isogeny, hence in $\mathcal{H}$ by the proof of [43, Theorem (2.3.5)], where sending an isogeny to its kernel is shown to be an equivalence of categories (compare [44, Proposition (1.1.13)], for Breuil's construction). Moreover, $T_{\mathfrak{S}}(\mathfrak{M}(\mathcal{H}))$ is $\mathrm{Hom}_{\mathfrak{S},\phi}(\mathfrak{M}(\mathcal{H}), \mathfrak{S}^{\mathrm{ur}}[1/5]/\mathfrak{S}^{\mathrm{ur}})$ when $\mathfrak{M}(\mathcal{H})$ is a direct sum of modules $\mathfrak{S}/5^n\mathfrak{S}$, as for the reductions modulo ϖ^n of free modules below [43, Lemma (2.1.2)].

(K3) As $5 > 2$, restriction from finite flat $G_{\tilde{F}}$-modules (the $G_{\tilde{F}}$-modules $\mathcal{H}(\overline{\mathbb{Q}}_5)$, $\mathcal{H}$ a commutative finite flat group scheme of 5-power order over $\mathcal{O}_{\tilde{F}}$) to $G_{\tilde{F}_\infty}$-modules is

fully faithful, and its essential image is stable under subobjects and quotients [10, Theorem 3.4.3]; here $\tilde{F}_\infty$ is the field of [10, §3.3] for the uniformizer ν.

(K4) Let $\mathcal{H}$ be a finite flat group scheme over $\mathcal{O}_{\tilde{F}}$ and $H \subset \mathcal{H}(\overline{\mathbb{Q}}_5)$ a $G_{\tilde{F}}$-submodule. The scheme-theoretic closure in $\mathcal{H}$ of the subgroup scheme of $\mathcal{H}_{\tilde{F}}$ with points H is a closed subgroup scheme, finite and flat over $\mathcal{O}_{\tilde{F}}$, and the fppf quotient of $\mathcal{H}$ by it is represented by a finite $\mathcal{O}_{\tilde{F}}$-scheme [65, §2.1], which is flat over $\mathcal{O}_{\tilde{F}}$, as $\mathcal{H}$ is flat over $\mathcal{O}_{\tilde{F}}$ and faithfully flat over the quotient.

Coefficients. $\mathcal{O}_E$ acts on all these objects by functoriality, and all the maps above are $\mathcal{O}_E$-linear. For a Breuil–Kisin module $\mathfrak{M}$ over $\mathfrak{S}_{\mathcal{O}_E}$ (an $\mathcal{O}_E$-action commuting with ϕ), this action makes $\mathfrak{M}$ free over $\mathfrak{S}_{\mathcal{O}_E}$, and we use $\mathrm{Hom}_{\mathfrak{S}_{\mathcal{O}_E},\phi}(\mathfrak{M}, \mathfrak{S}^{\mathrm{ur}} \otimes_{\mathbb{Z}_5} \mathcal{O}_E)$ for $T_{\mathfrak{S}}$ [35, Proposition 3.4(3)], whose proof does not use the standing assumption there that E contains the images of all embeddings of $\tilde{F}$. It is isomorphic to $T_{\mathfrak{S}}(\mathfrak{M})$ as an $\mathcal{O}_E[G_{\tilde{F}_\infty}]$-module by trace duality ($\mathrm{Hom}_{\mathbb{Z}_5}(X, \mathbb{Z}_5) \cong \mathrm{Hom}_{\mathcal{O}_E}(X, \mathfrak{d}^{-1})$, $\mathfrak{d}$ the different of $\mathcal{O}_E$), naturally after fixing an isomorphism $\mathcal{O}_E \cong \mathfrak{d}^{-1}$ [35, Remark 3.6]. We abbreviate the target to $\mathfrak{S}^{\mathrm{ur}}$. Then (K1)–(K4) hold for this form of $T_{\mathfrak{S}}$, with $\otimes_{\mathfrak{S}_{\mathcal{O}_E}}$ and $\otimes_{\mathcal{O}_E}$ in (K1). Indeed, such an $\mathfrak{M}$ is projective over $\mathfrak{S}_{\mathcal{O}_E} = \prod_j \mathcal{O}_E[[u]]$, being free over $\mathfrak{S}$ (Auslander–Buchsbaum), and $T_{\mathfrak{S}}(\mathfrak{M} \otimes_{\mathfrak{S}_{\mathcal{O}_E}} \mathfrak{N})$ is the submodule of $T_{\mathfrak{S}}(\mathfrak{M}) \otimes_{\mathbb{Z}_5} T_{\mathfrak{S}}(\mathfrak{N})$ on which the two actions of $\mathcal{O}_E$ agree. For free $\mathcal{O}_E$-modules this submodule is isomorphic to $T_{\mathfrak{S}}(\mathfrak{M}) \otimes_{\mathcal{O}_E} T_{\mathfrak{S}}(\mathfrak{N})$ as an $\mathcal{O}_E[G_{\tilde{F}_\infty}]$-module: the corresponding submodule of $\mathcal{O}_E \otimes_{\mathbb{Z}_5} \mathcal{O}_E$ is free of rank one over $\mathcal{O}_E$, and multiplication by a generator η of it, $x \otimes y \mapsto \eta \cdot (x \otimes y)$, is such an isomorphism, natural in $\mathfrak{M}$ and $\mathfrak{N}$ and compatible with exchanging the factors, which fixes η (the quotient map has image $\mathfrak{d} \cdot T_{\mathfrak{S}}(\mathfrak{M}) \otimes_{\mathcal{O}_E} T_{\mathfrak{S}}(\mathfrak{N})$). As 5 is odd, this isomorphism also gives $T_{\mathfrak{S}}(\wedge^2_{\mathfrak{S}_{\mathcal{O}_E}} \mathfrak{M}) \cong \wedge^2_{\mathcal{O}_E} T_{\mathfrak{S}}(\mathfrak{M})$. The descent data are treated in the paragraph *Descent data* below.

Write $n_\tau \in \{-1, 0, 1\}$ for the weight of $\Psi = \psi/(\sigma_m \circ \psi)$ at an embedding τ of E (Lemma 6.1(c)). Over each component j there are four embeddings τ_a of E, one for each $a \in (\mathbb{Z}/5)^\times$, with $\tau_a(\zeta_5) = \zeta_5^a$. By Lemma 6.1(d) the numbers n_τ over one component are never both $+1$ and -1. More precisely, let w_0 be the prime of L induced by ι (Lemma 6.1(e)), take Γ to be the decomposition group given by ι, and let $s_0 \in (\mathbb{Z}/5p)^\times$ be such that λ lies above the prime $\sigma_{s_0}(w_0)$ of L. We identify E with the closure of $\iota(M)$ in $\overline{\mathbb{Q}}_5$ through $\iota \circ \sigma_{s_0}^{-1}$, an embedding of M that induces λ, and number the components from the embedding of $W(k)$ into $\mathcal{O}_E$ that this gives. By transport of structure (Lemma 6.1(b)), the weights over λ are those at the prime $\sigma_{s_0}^{-1}(w_0)$ in Lemma 6.1(e), each twice. So, with $x_j = \langle (s_0^{-1} 5^{-j} \bmod p)/p \rangle$, the pair $(\#\{n = +1\}, \#\{n = -1\})$ over component j is $(4,0)$, $(2,0)$, $(0,0)$, $(0,2)$, $(0,4)$ for x_j in $(0, \frac{1}{5})$, $(\frac{1}{5}, \frac{2}{5})$, $(\frac{2}{5}, \frac{3}{5})$, $(\frac{3}{5}, \frac{4}{5})$, $(\frac{4}{5}, 1)$. Let χ_m be a crystalline character of G_E with weight 1 exactly where $n_\tau = -1$ (one exists by [19, Propositions B.3 and B.4]), and $\xi = (\sigma_m \circ \psi)^{-1} \chi_m$. After twisting by ξ, G_E acts on v_1, v_2 by $\Psi\chi_m$ and χ_m, which have weights in $\{0, 1\}$ with disjoint weight-1 sets. Their Breuil–Kisin modules have rank one, with bases f_1, f_2 such that $\phi(f_i) = A_i f_i$, where on component j ([36, Lemma 2.2.3] for $\tilde{F}$ and ν, after enlarging the coefficients; the p embeddings of $\tilde{F}$ above an embedding τ of E give $u^p - \tau(\lambda_5)$),

$$A_1^{(j)} = c_1 \prod (u^p - \tau(\lambda_5)), \qquad A_2^{(j)} = c_2 \prod (u^p - \tau(\lambda_5)),$$

the products over the weight-1 embeddings above j. These polynomials have degrees $s_1(j) = p\,\#\{n = +1\}$ and $s_2(j) = p\,\#\{n = -1\}$, and on each component one of them is a unit. The weight-1 sets are unions of pairs $\{\tau_a, \tau_{-a}\}$, as $n_{\tau_a} = n_{\tau_{-a}}$ (Lemma 6.1(c)), and $\tau_{-a}(\lambda_5) = -\tau_a(\lambda_5)$; so each pair contributes the factor $u^{2p} - \tau_a(\lambda_5)^2$, and as $\tau_a(\lambda_5)^2 \in \varpi^2 \mathcal{O}_E$, both polynomials are congruent to monomials $c_i u^{s_i(j)}$ modulo ϖ^2, in particular modulo

ϖ. The two residual characters agree, and the residual étale ϕ-modules are identified by $\bar f_2 \mapsto u^{a_j}\bar f_1$ on component j (with f_1, f_2 the basis, $\phi(f_i) = A_i f_i$, of the twisted Breuil–Kisin module $\mathfrak{M}_0$ defined below), where

$$a_{j-1} = 5a_j + s_1(j-1) - s_2(j-1), \qquad \text{i.e.} \qquad a_j = -\frac{1}{5^f-1}\sum_{i=0}^{f-1} 5^i\,(s_1-s_2)(j+i).$$

Take $r = s_0 \bmod p$ in Lemma 6.2; then $x_j = y_j$, and the table above gives $(s_1 - s_2)(j) = 2p(2 - \lfloor 5x_j \rfloor) = \Delta_j$. So $-a$ solves the recurrence of Lemma 6.2, and $a_j = p(2x_{j-1} - 1)$, an odd integer with $0 < |a_j| < p$, for either parity of f.

The tangent space. Let $\mathfrak{M}_0 = \mathfrak{S}_{\mathcal{O}_E} f_1 \oplus \mathfrak{S}_{\mathcal{O}_E} f_2$ be the twisted Breuil–Kisin module of the CM point, $\phi(f_i) = A_i f_i$, and $\bar{\mathfrak{M}}_0 = \mathfrak{M}_0/\varpi$. As the A_i are polynomials in u^p and ϕ is $\mathcal{O}_E$-linear, the bases can be chosen with $\hat g(f_i) = \zeta_g^{t_i} f_i$ on every component, with $t_i \in \mathbb{Z}/p$ independent of j (the type of f_i). An entry H_{ab} of a matrix H in the basis (f_1, f_2) has descent type $t_b - t_a$ if $\hat g(H_{ab}) = \zeta_g^{t_b - t_a} H_{ab}$ for all g; on component j the monomial u^n has type $5^j n$. As the residual characters agree on G_E, the identification $\bar f_2 \mapsto u^{a_j}\bar f_1$ commutes with the descent data, so $t_2 - t_1 \equiv 5^j a_j \pmod p$ for every j (consistently, $a_{j-1} \equiv 5a_j \pmod p$, as $p \mid s_i(j-1)$). Hence the monomials of H_{aa} have exponents divisible by p, and those of H_{12} on component j have exponents $\equiv a_j \pmod p$. As $T_{\mathfrak{S}}$ is contravariant, v_i spans $T_{\mathfrak{S}}(\mathfrak{S}_{\mathcal{O}_E} f_i)$, the set of elements of $T_{\mathfrak{S}}(\mathfrak{M}_0)$ that vanish on f_{3-i}. Let $D \ge 1$. Inside a fixed étale ϕ-module killed by ϖ^{D+1}, the lattices free over $\mathfrak{S}_{\mathcal{O}_E}/\varpi^{D+1}$ with the same image modulo ϖ^D as a given torsion Breuil–Kisin module $\mathfrak{L} \equiv \bar{\mathfrak{M}}_0$ (the lifts of that image to the next power of ϖ) are the $(1 + \varpi^D H)\mathfrak{L}$ with $H = (H_{ab})$, $H_{ab} \in \mathbb{F}((u))/\mathbb{F}[[u]]$ on each component ($\mathbb{F} = \mathcal{O}_E/\varpi$). Such a lift is ϕ-stable of height ≤ 1 and stable under the descent data exactly when, on each component, $B_{ab} = \phi(H_{ab})A_a - A_b H_{ab}$ is integral (a condition on the principal part of H_{ab}, as integral entries give integral B_{ab}) and H_{ab} has descent type $t_b - t_a$. The height condition follows: for the off-diagonal entries because $E(u)/(A_1A_2)$ is integral, as the weight-1 sets are disjoint and $E(u) = \prod_\tau (u^p - \tau(\lambda_5))$ over the four embeddings τ above each component, so that $s_1 + s_2 \le 4p$; and the diagonal entries vanish by Lemma 8.7(a). We call the space of such H the *tangent space* $\mathbb{T}$ at $\bar{\mathfrak{M}}_0$. Equivalently, $\mathbb{T}$ is the tangent space at $\bar{\mathfrak{M}}_0$ of the moduli of finite flat models with fixed generic fiber and identification, as in [44, §2.1], with the coefficient action and the prescribed tame descent data: over $\mathbb{F}[\epsilon]/(\epsilon^2)$ the lifts of $\bar{\mathfrak{M}}_0$ are the lattices $(1 + \epsilon H)(\bar{\mathfrak{M}}_0 \otimes_{\mathbb{F}} \mathbb{F}[\epsilon])$, and the conditions above are those of [44, Proposition (2.1.7) and its proof], with the descent data. This interpretation is not used below. The tensor product of $\mathbb{T}$ with $\varpi^D\mathcal{O}_E/\varpi^{D+1}\mathcal{O}_E$ describes the differences between two lifts to depth $D+1$ of the same depth-D module. Lemmas 8.10 and 8.13 say that no nonzero such difference satisfies all the required coefficient, descent and polarization symmetries.

The set-up for f odd. Let f be odd. In $\mathrm{Gal}(M/\mathbb{Q}) \cong (\mathbb{Z}/5)^\times \times (\mathbb{Z}/p)^\times$ the decomposition group of the primes above 5 is $(\mathbb{Z}/5)^\times \times \langle 5\rangle$; it contains neither σ_m nor c, as $-1 \notin \langle 5\rangle$, but contains $\mathsf{c}\sigma_m$. So λ' splits in M as $\lambda_1 \ne \lambda_2 = \sigma_m(\lambda_1) = \mathsf{c}(\lambda_1)$, and c fixes λ' and acts trivially on its residue field $k = \mathbb{F}_{5^f}$. Thus $\mathcal{O} = \mathcal{O}_{M',\lambda'} = \mathcal{O}_{M,\lambda_1}$, and $T_0 = \mathcal{O}e_1 \oplus \mathcal{O}e_2$, where e_i spans the λ_i-component. With $E = M_{\lambda_1}$, so that $\mathcal{O}_E = \mathcal{O}$, and $v_i = e_i$, the set-up above applies as written: G_E acts on e_1, e_2 by ψ and $\sigma_m \circ \psi$, and the twist ξ, the Breuil–Kisin modules $\mathfrak{M}_0$, the exponents a_j and the tangent space $\mathbb{T}$ are defined in the same way. In addition, Γ preserves both lines, as its image in the abelian group $\mathrm{Gal}(M/K)$ lies in the common decomposition group of λ_1 and λ_2. The Weil pairing on T_0 is the trace of the skew-Hermitian form of Section 5.3. Its λ'-component h, with values in the inverse different $\mathfrak{D}^{-1}$ of $\mathcal{O}$ over $\mathbb{Z}_5$, is $h(xv_0, yv_0) = \mathrm{Tr}_{M/M'}(x\,\mathsf{c}(y)\gamma_M)$, with γ_M as in Section 6.2. So

$h(ax,by)=a\,\mathsf{c}(b)\,h(x,y)$ for $a,b\in\mathcal{O}$, and $h(y,x)=-\mathsf{c}(h(x,y))$. As $\mathsf{c}(\lambda_1)=\lambda_2$, h pairs e_1 with e_2 only: $h(e_1,e_1)=h(e_2,e_2)=0$, and $h_{12}=h(e_1,e_2)$ generates $\mathfrak{D}^{-1}$, so $v_\varpi(h_{12})=-3$.

Untwisting. The twist by ξ, a character of G_E, changes no endomorphism; the structures that it destroys, the descent data of $\mathrm{Gal}(\tilde{F}/K_5)$, the $\mathcal{O}$-structure $(1\otimes\sigma_m)$ and the duality, live on the untwisted modules, which we now define. Let $\mathfrak{N}_+$, $\mathfrak{N}_-$ be the Breuil–Kisin modules of χ_m and of $\sigma_m\circ\psi$ (rank one, weights in $\{0,1\}$), $\mathfrak{N}_\xi=\mathfrak{N}_+\otimes\mathfrak{N}_-^{-1}$, a rank-one lattice in the étale ϕ-module of ξ, and, for $T=T_0$ and for $T=T'$ with u_0 as in Proposition 8.11, $\mathfrak{M}(T)$ the Breuil–Kisin module of $T\otimes_{\mathcal{O}}\mathcal{O}_E$. By (K1)(c), applied to lattices with weights in $[0,2]$, $\mathfrak{M}(T\chi_m)=\mathfrak{M}(T)\otimes\mathfrak{N}_+$ and, as $T\chi_m=T\xi\otimes(\sigma_m\circ\psi)$, $\mathfrak{M}(T\chi_m)=\mathfrak{M}(T\xi)\otimes\mathfrak{N}_-$; so $\mathfrak{M}(T\xi)=\mathfrak{M}(T)\otimes\mathfrak{N}_\xi$ inside the étale ϕ-module. So $\mathfrak{M}_0=\mathfrak{M}(T_0)\otimes\mathfrak{N}_\xi$ and $f_i=\mathring{f}_i\otimes n_\xi$, with $\mathring{f}_i$ a basis of the Breuil–Kisin module of $\mathcal{O}_E v_i$ and n_ξ one of $\mathfrak{N}_\xi$ of pure descent type (that is, $\hat{g}(n_\xi)=\zeta_g^t n_\xi$ for all g, with one $t\in\mathbb{Z}/p$), so that each $\mathring{f}_i$ has a pure descent type. Such an n_ξ exists, as for the f_i: $\mathfrak{N}_\xi$ has rank one and its ϕ-matrix is a ratio of polynomials in u^p. The map $H\mapsto H\otimes 1$ identifies the endomorphisms of $\mathfrak{M}(T_0)[1/u]$ with those of $\mathfrak{M}_0[1/u]$, and $(1+\varpi^D H)\mathfrak{M}_0$ is the twist of $(1+\varpi^D H)\mathfrak{M}(T_0)$. *Descent data:* as T_0, T' are Γ-modules, $\mathfrak{M}(T_0)$, $\mathfrak{M}(T')$ carry descent data of $\mathrm{Gal}(\tilde{F}/K_5)$ [12, Definition 2.1.2] ($\tilde{F}/K_5$ is tame and $\nu^{2p}\in K_5$), semilinear also for the action of Γ on $\mathcal{O}_E$. Here $g\in G_{K_{5,\infty}}$, with $K_{5,\infty}=K_5((\nu^{1/5^n})^{2p}:n\geq 1)$, acts on the étale ϕ-module by $g\otimes g$, which preserves the Breuil–Kisin lattice by the uniqueness in (K1). Maps of Γ-modules induce maps commuting with these descent data [12, Lemma 2.2.4]. The descent data preserve the Breuil–Kisin modules of the two lines, which are Γ-stable ($g\in\Gamma$ acts coordinatewise through the isomorphism $\mathcal{O}_M\otimes_{\mathcal{O}_{M'}}\mathcal{O}_E\to\mathcal{O}_E\times\mathcal{O}_E$, $x\otimes y\mapsto(xy,\sigma_m(x)y)$). *Duality:* the dual of a torsion Breuil–Kisin module of height ≤ 1 is one, with $T_{\mathfrak{S}}(\mathfrak{M}^\vee)=T_{\mathfrak{S}}(\mathfrak{M})^\vee(1)$ [55, Lemma 3.1.2(3) and Proposition 3.1.7]; passing to the limit and using (K1), $\mathfrak{M}(T_0)^\vee$ is the Breuil–Kisin module of $(T_0\otimes_{\mathcal{O}}\mathcal{O}_E)^\vee(1)$. So the pairing $\mathrm{Tr}\circ\tilde{h}_0$ on $T_0\otimes_{\mathcal{O}}\mathcal{O}_E$, where $\tilde{h}_0(x\otimes a,y\otimes b)=a\,\mathsf{c}(b)\,h_0(x,y)$ is the extension of scalars of h_0, induces a perfect pairing $\langle\,,\rangle$ on $\mathfrak{M}(T_0)$. This pairing is compatible with ϕ and the descent data and c-sesquilinear for $\mathcal{O}_E$, and $\mathfrak{M}(T_0)$ is self-dual for it. Each $\mathfrak{M}(T_0)/\varpi^n$ is self-dual for $\langle x,y\rangle_n=\langle\tilde{x},\mathsf{c}(\varpi)^{-n}\tilde{y}\rangle \bmod \mathfrak{S}$, where $\tilde{x},\tilde{y}\in\mathfrak{M}(T_0)$ are any lifts of x,y (this tilde marks a lift; the one on $\tilde{h}_0$ marks the extension of scalars). The Galois counterpart of $\langle\,,\rangle_n$ is the pairing $e_{0,n}(x,y)=\mathrm{Tr}(\varpi^{-n}\tilde{h}_0(\tilde{x},\tilde{y})) \bmod \mathbb{Z}_5$ on $(T_0\otimes_{\mathcal{O}}\mathcal{O}_E)/\varpi^n$, for lifts $\tilde{x},\tilde{y}\in T_0\otimes_{\mathcal{O}}\mathcal{O}_E$ of x,y. For T' the same construction, with the form h' and its extension of scalars $\tilde{h}'$, gives a perfect pairing on $\mathfrak{M}(T')$ with the same properties and the pairings $e'_n(x,y)=\mathrm{Tr}(\varpi^{-n}\tilde{h}'(\tilde{x},\tilde{y})) \bmod \mathbb{Z}_5$ on $(T'\otimes_{\mathcal{O}}\mathcal{O}_E)/\varpi^n$. For f even, the two lines are orthogonal for $\langle\,,\rangle$, as they are for $\tilde{h}_0$ by the formula for h_0 in Section 6.2. By trace duality, as in Section 5.9, $\langle\,,\rangle=\mathrm{Tr}\circ\mathring{h}_0$ for a c-sesquilinear form $\mathring{h}_0$ on $\mathfrak{M}(T_0)$ with values in $\mathfrak{S}\otimes_{\mathbb{Z}_5}\mathfrak{a}\mathcal{O}_E$. Conditions (b) and (c) of Lemma 8.10 below refer to the action $H\mapsto\hat{g}H\hat{g}^{-1}$ of Γ on endomorphisms of $\mathfrak{M}(T_0)[1/u]$ modulo integral ones, through these descent data and on the coefficients, and to the adjoint H^* for this pairing; H is $\mathcal{O}$-linear if it commutes with $1\otimes\sigma_m$.

Lemma 8.7. *(a) $H_{11}=H_{22}=0$ for $H\in\mathbb{T}$.*

(b) The H_{12}-part of $\mathbb{T}$ is spanned over $\mathbb{F}$ by the elements $H_{\mathcal{R}}=\sum_{j\in\mathcal{R}}u^{a_j}$, one for each maximal cyclic run $\mathcal{R}$ of consecutive components with $a_j<0$; the H_{21}-part likewise, with $-a$ in place of a.

Proof. (a) As H_{aa} has descent type 0, the poles of H_{aa} have orders divisible by p. If $N\geq p$ is the largest pole order, attained on component j, the term u^{-5N} of $\phi(H_{aa})$ cannot be cancelled by H_{aa} on component $j-1$ (pole order $\leq N$) nor absorbed by A_a (of degree

$s_a(j-1) \le 4p < 5p \le 5N$). (b) Write $H_{12} = u^{a_j}\delta_j$ on component j. As H_{12} has descent type $t_2 - t_1$, δ_j lies in $\mathbb{F}((v))$, $v = u^p$, and as $|a_j| < p$, δ_j matters modulo $v^{[a_j<0]}\mathbb{F}[[v]]$. Integrality of B_{12} on component $i = j-1$ reads $\phi(\delta_{i+1}) - \delta_i \in v^{b_i}\mathbb{F}[[v]]$ with $b_i = [a_i < 0] - s_2(i)/p \in [-4, 1]$. If $N' \ge 1$ is the largest v-pole order of the δ_i, attained at i, the term $v^{-5N'}$ of $\phi(\delta_i)$ forces a pole of order $5N' > N'$ in δ_{i-1}; so all δ_i are integral, $\delta_i \equiv \kappa_i$ (a constant) if $a_i < 0$ and $\delta_i \equiv 0$ if $a_i > 0$. The remaining condition, where $b_i = 1$ (that is, $a_i < 0$ and $s_2(i) = 0$, so that $a_{i+1} = (a_i - s_1(i))/5 < 0$), is $\kappa_{i+1} = \kappa_i$; and if $a_i < 0$ and $s_2(i) > 0$, then $s_1(i) = 0$ and $a_i = 5a_{i+1} - s_2(i)$ forces $a_{i+1} > 0$, so i ends its run. Hence the solutions are the κ constant along each run. □

The residual endomorphism $\bar\sigma_m$ of T_0/ϖ, which exchanges the lines of $\bar v_1$ and $\bar v_2$, corresponds under $T_{\mathfrak{S}}$ to an endomorphism of the residual étale ϕ-module that exchanges the lines of $\bar f_1$ and $\bar f_2$. As the ϕ-compatible maps from either line to the other form one $\mathbb{F}$-line, this endomorphism is $\bar f_2 \mapsto u^{a_j}\bar f_1$, $\bar f_1 \mapsto u^{-a_j}\bar f_2$ on component j, after multiplying f_2 by a constant ($\bar\sigma_m^2 = 1$ makes the two constants inverse to each other). Its class in the tangent space, the principal parts, is H_σ with $H_{\sigma,12} = \sum_{a_j<0} u^{a_j} = \sum_{\mathcal{R}} H_{\mathcal{R}}$, $H_{\sigma,21} = \sum_{a_j>0} u^{-a_j}$ and zero diagonal, as $0 < |a_j| < p$.

Example 8.8. We list these data at $p = 7$ and $p = 19$; e_j is the idempotent of component j, so that $u^n e_j$ is the monomial u^n on component j. They were computed exactly, together with the linear conditions defining $\mathbb{T}$ (Appendix B, (C9)).

At $p = 7$, $f = 6$, and there is one prime of M above 5 (with $s_0 = 1$):

j	0	1	2	3	4	5
$7x_j$	1	3	2	6	4	5
$(\#\{n=+1\}, \#\{n=-1\})$	$(4,0)$	$(0,0)$	$(2,0)$	$(0,4)$	$(0,0)$	$(0,2)$
a_j	3	-5	-1	-3	5	1

There is one run $\mathcal{R} = \{1,2,3\}$ with $a_j < 0$, and $\mathbb{T}$ has the $\mathbb{F}$-basis $H_{\mathcal{R}} = u^{-5}e_1 + u^{-1}e_2 + u^{-3}e_3$ in the $(1,2)$-entry and $u^{-5}e_4 + u^{-1}e_5 + u^{-3}e_0$ in the $(2,1)$-entry; H_σ has these two entries. As $a_{j+3} = -a_j$, $1 \otimes \sigma_m$ maps the first to the second.

At $p = 19$, $f = 9$; at the prime of M above 5 with $s_0 = 1$ (and $d_w = 6$):

j	0	1	2	3	4	5	6	7	8
$19x_j$	1	4	16	7	9	17	11	6	5
$(\#\{n=+1\}, \#\{n=-1\})$	$(4,0)$	$(2,0)$	$(0,4)$	$(2,0)$	$(0,0)$	$(0,4)$	$(0,0)$	$(2,0)$	$(2,0)$
a_j	-9	-17	-11	13	-5	-1	15	3	-7

The runs with $a_j < 0$ are $\{8,0,1,2\}$ and $\{4,5\}$, those with $a_j > 0$ are $\{3\}$ and $\{6,7\}$, and $\mathbb{T}$ has the $\mathbb{F}$-basis $u^{-7}e_8 + u^{-9}e_0 + u^{-17}e_1 + u^{-11}e_2$, $u^{-5}e_4 + u^{-1}e_5$ in the $(1,2)$-entry and $u^{-13}e_3$, $u^{-15}e_6 + u^{-3}e_7$ in the $(2,1)$-entry. At the other prime ($s_0 = 2$, $d_w = 4$) the exponents are $-a_{j+4}$.

In both cases the diagonal part of $\mathbb{T}$ is 0, and by Lemma 8.9 the descent datum of $\tilde r$, an element of the inertia subgroup of Γ with $\tilde r(\zeta_5) = \zeta_5^{-1}$, acts on every basis element of $\mathbb{T} \otimes (\varpi^D\mathcal{O}_E/\varpi^{D+1}\mathcal{O}_E)$ by $(-1)^D$. So does the adjoint at $p = 19$; at $p = 7$, where f is even and the adjoint exchanges the two entries, the adjoint followed by $H \mapsto H_{12}$ acts on $\varpi^D H_{\mathcal{R}}$ by $(-1)^D$.

8.5. **Isometries and Breuil–Kisin modules.**

Lemma 8.9 (the action of $\tilde r$ and of the adjoint)**.** *Let $\tilde r$ be an element of the inertia subgroup of Γ with $\tilde r(\zeta_5) = \zeta_5^{-1}$, let $D \ge 0$, and for a component j and $\kappa \in \mathbb{F}$ let $X_j(\kappa)$ be the*

off-diagonal principal part, at depth D, whose only nonzero entry is $\kappa\varpi^D u^{a_j}$ in position $(1,2)$ on component j if $a_j<0$, resp. $\kappa\varpi^D u^{-a_j}$ in position $(2,1)$ if $a_j>0$, read modulo ϖ^{D+1} and modulo integral entries.

(a) Conjugation by the descent datum of $\tilde r$ maps $X_j(\kappa)$ to $X_j((-1)^D\kappa)$.

(b) For f even, the adjoint followed by the identification of an $\mathcal{O}$-linear H with H_{12}, $H_{12}\mapsto(H^*)_{12}$, maps $X_j(\kappa)$ to $X_j((-1)^D\kappa)$ ($a_j<0$). For f odd, the adjoint maps $X_j(\kappa)$ to $X_j((-1)^D\kappa)$ for every j.

In particular both maps act on $\varpi^D H_{\mathcal{R}}$ by $(-1)^D$, and the descent datum of $\tilde r$, and for f odd the adjoint, act by $(-1)^D$ on the $(2,1)$-analogue of $\varpi^D H_{\mathcal{R}}$.

Proof. The maps are diagonal on monomials. $\tilde r$ lies in the inertia subgroup, so it acts trivially on $W(k)$ and on $\mathbb{F}$, and $\tilde r(\varpi)=1-\zeta_5^{-1}=-\zeta_5^{-1}\varpi$. Its descent datum preserves the components and the two lines (which are Γ-stable), and it commutes with the descent data of $\mathrm{Gal}(\tilde F/E)$, as the inertia group of $\tilde F/K_5$ is cyclic and contains $\mathrm{Gal}(\tilde F/E)$; so conjugation by it preserves descent types. Write $\hat{\tilde r}(\mathring f_i)=d_i\mathring f_i$; conjugation maps a $(1,2)$-entry y to $(d_1/d_2)\tilde r(y)$, where $\tilde r$ acts on coefficients and on u through its descent datum ($u\mapsto\zeta u$ for a root of unity ζ), and likewise in position $(2,1)$ with d_2/d_1. For f even, the adjoint followed by the identification of (b) preserves the components and the descent types and is $\sigma_m\mathsf{c}$-semilinear, as the lines are orthogonal and c, σ_m agree on $W(k)$. It multiplies $\sigma_m\mathsf{c}(y)$ by a unit built from $\mathring h_0(\mathring f_a,\mathring f_a)$ and the matrix of $1\otimes\sigma_m$. Moreover, $\sigma_m\mathsf{c}$ fixes $W(k)$, hence acts trivially on $\mathbb{F}$, and maps ϖ to $1-\zeta_5^{-1}$. For f odd, the lines are isotropic and $\mathring h_{12}=\mathring h_0(\mathring f_1,\mathring f_2)$ is h_{12} times a unit of $\mathfrak{S}_{\mathcal{O}}$ (Section 8.7); the adjoint of the endomorphism with $(1,2)$-entry y has $(1,2)$-entry $-\mathsf{c}(y\mathring h_{12})/\mathring h_{12}$, and likewise in position $(2,1)$ with $\mathsf{c}(\mathring h_{12})$. All these multipliers have descent type 0, so beyond their constant terms they involve only u^{np} with $n\geq 1$, and $u^{\pm a_j+np}$ is integral as $|a_j|<p$. Hence each map sends $X_j(\kappa)$ to $X_j(c_j\epsilon_D\kappa)$, where $c_j\in\mathbb{F}^\times$ does not depend on κ or D, and $\epsilon_D\in\mathbb{F}^\times$ is the image of the factor that ϖ^D contributes. Here $\tilde r(\varpi)^D\equiv(-1)^D\varpi^D$, $(\sigma_m\mathsf{c})(\varpi)^D\equiv(-1)^D\varpi^D$, and, for f odd, as $v_\varpi(y\mathring h_{12})=D-3$ and $\mathsf{c}(\varpi)\equiv-\varpi \pmod{\varpi^2}$, $-\mathsf{c}(y\mathring h_{12})/\mathring h_{12}\equiv-(-1)^{D-3}y=(-1)^D y \pmod{\varpi^{D+1}}$. So $\epsilon_D=(-1)^D$ (for f odd the congruence also shows that the adjoint has $c_j=1$).

The constants are 1. Take $D=0$. For f even, $\bar\sigma_m$ commutes with Γ, as $\tilde\psi\equiv\omega_5 \pmod{\varpi}$ (Lemma 6.3(a)), and it is self-adjoint, its adjoint being $(\sigma_m(\gamma_M)/\gamma_M)\bar\sigma_m=\bar\sigma_m$ (Section 6.2; $\sigma_m(\gamma_M)/\gamma_M\equiv 1$ by the proof of Proposition 6.4(a)). For f odd, both residual lines are ω_5 on the inertia subgroup of Γ (Lemma 6.3(a)), so the residual maps $\bar v_2\mapsto\bar v_1$ and $\bar v_1\mapsto\bar v_2$ commute with $G_{\tilde F}$ and with $\tilde r$; and they are self-adjoint up to the factor $-\mathsf{c}(\mathring h_{12})/\mathring h_{12}\equiv 1$ at depth 0, by the computation above. Let F_r be the fixed field of $\tilde r$ in $\tilde F$: as $\tilde r$ lies in the inertia group, $\tilde F/F_r$ is Galois, cyclic, totally and tamely ramified of degree n, the order of $\tilde r(\nu)/\nu\in\mu_{2p}$, and $\nu^n\in F_r$; so [12, §§2.1–2.2] applies with $K'=\tilde F$, $K=F_r$, $\pi'=\nu$. The maps above commute with G_{F_r}, which $G_{\tilde F}$ and $\tilde r$ generate, hence with $G_{F_{r,\infty}}$, where $F_{r,\infty}=F_r((\nu^{1/5^m})^n : m\geq 1)$ contains $K_{5,\infty}$; and $G_{F_{r,\infty}}$ contains the elements of $G_{K_{5,\infty}}$ that induce $\tilde r$ on $\tilde F$ (they multiply $\nu^{1/5^m}$ by a root of unity of order n). By [12, Lemma 2.2.4], with coefficients $\mathbb{F}$, the induced endomorphisms of the residual étale ϕ-module commute with the descent datum of $\tilde r$, and their classes are fixed by both maps. These classes are H_σ, with $(1,2)$-entry $\sum_{a_j<0}u^{a_j}$ and $(2,1)$-entry $\sum_{a_j>0}u^{-a_j}$ (Section 8.4), resp. $\sum_{a_j<0}\kappa_j u^{a_j}$ and $\sum_{a_j>0}\kappa'_j u^{-a_j}$ with all $\kappa_j,\kappa'_j\neq 0$: each has a nonzero coefficient on every component of the relevant sign. At $D=0$ each map sends $\sum_j X_j(\kappa_j)$ to $\sum_j X_j(c_j\kappa_j)$ (with κ'_j for κ_j

where $a_j > 0$, and only the j with $a_j < 0$ for the adjoint when f is even), as it preserves the components, so a fixed class with $\kappa_j \neq 0$ gives $c_j = 1$; as c_j does not depend on D, this holds at every depth. □

Lemma 8.10. *Let f be even and $D \geq 0$. No nonzero $H \in \mathbb{T} \otimes (\varpi^D \mathcal{O}_E / \varpi^{D+1} \mathcal{O}_E)$ is at the same time* (a) *$\mathcal{O}$-linear (that is, descends from $\mathcal{O}_E$ to $\mathcal{O} = \mathcal{O}_{M',\lambda'}$),* (b) *invariant under Γ, acting through the descent data and on the coefficients, and* (c) *compatible with the skew-Hermitian form h_0, that is, $H + H^*$ is integral, $*$ the adjoint for the pairing induced by h_0 (Section 8.4).*

Proof. By Lemma 8.7(a), H is off-diagonal. As f is even, $\mathcal{O}_E/\mathcal{O}$ is unramified quadratic with group $\langle \sigma_m \rangle$, and $1 \otimes \sigma_m$ maps component j to component $j + f/2$; so an $\mathcal{O}$-linear H has $H_{21,j+f/2} = \sigma_m(H_{12,j})$ (consistent with $a_{j+f/2} = -a_j$) and is determined by $H_{12} \in \operatorname{span}\{H_{\mathcal{R}}\}$. Let $\tilde{r}$ be as in Lemma 8.9. By that lemma, at depth D the descent datum of $\tilde{r}$, and the adjoint followed by $H_{12} \mapsto (H^*)_{12}$, act on every $H_{\mathcal{R}}$ by $(-1)^D$. Hence for D odd $\tilde{r}$ acts by -1 on every $H_{\mathcal{R}}$, and (b) fails unless $H = 0$; for D even every $H_{\mathcal{R}}$ is self-adjoint, so $H + H^* = 2H$, and (c) fails unless $H = 0$. □

Proposition 8.11. *Let f be even, $u_0 \in \mathbb{Q}$ with $v_5(u_0) \geq 2$ (with T' and ι_{can} as in Sections 5.3 and 5.4 for this u_0), $D \geq 1$, and $\varphi_D \colon T'/\varpi^D \to T_0/\varpi^D$ a Γ-equivariant $\mathcal{O}$-linear isomorphism, isometric modulo $\varpi^D \mathfrak{a}$, with $\varphi_D \equiv \iota_{\mathrm{can}} \pmod{\varpi}$. Then the restriction of φ_D to $G_{\tilde{F}}$, after the twist by ξ, is induced by an isomorphism of torsion Breuil–Kisin modules $\mathfrak{M}'/\varpi^D \cong \mathfrak{M}_0/\varpi^D$, where $\mathfrak{M}'$, $\mathfrak{M}_0$ are the Breuil–Kisin modules of $T'\xi$ and $T_0\xi$.*

Proof. Both $T'\xi$ and $T_0\xi$ are Barsotti–Tate over $\tilde{F}$: $V_5(\operatorname{Jac} D_{u_0})$ is crystalline over $\tilde{F}$ with the Weil–Deligne representation of T_0 (Proposition 8.1(d)), and its Hodge–Tate weights at each embedding are those of T_0, being $\{0,0\}$, $\{0,1\}$ or $\{1,1\}$ and fixed by the determinant (Lemma 5.9(b)). By Section 8.4 it suffices to show that φ_D is induced by an isomorphism $\alpha_D \colon \mathfrak{M}(T')/\varpi^D \cong \mathfrak{M}(T_0)/\varpi^D$ of untwisted torsion Breuil–Kisin modules: its twist $\alpha_D \otimes 1_{\mathfrak{N}_\xi}$ is then the required isomorphism $\mathfrak{M}'/\varpi^D \cong \mathfrak{M}_0/\varpi^D$. We induct on D. For $D = 1$, Proposition 8.5 gives an isomorphism of finite flat group schemes over $\mathcal{O}_{\tilde{F}}$ that induces ι_{can} on $G_{\tilde{F}}$-points and maps λ'-components to λ'-components; by (K2) it gives α_1. For the step from D to $D+1$, let $\mathfrak{L}$ be the model of T'/ϖ^{D+1} transported by φ_{D+1}, that is, the lattice corresponding to $\mathfrak{M}(T')/\varpi^{D+1}$ in the étale ϕ-module of $\mathfrak{M}(T_0)/\varpi^{D+1}$, and let $\mathfrak{L}_0 = \mathfrak{M}(T_0)/\varpi^{D+1}$. By induction, applied to $\varphi_{D+1} \bmod \varpi^D$, which satisfies the hypotheses at level D (an isometry modulo $\varpi^{D+1}\mathfrak{a}$ is one modulo $\varpi^D\mathfrak{a}$), they have the same image modulo ϖ^D, so $\mathfrak{L} = (1 + \varpi^D H)\mathfrak{L}_0$. Both are stable under the descent data of $\operatorname{Gal}(\tilde{F}/K_5)$, as φ_{D+1} is Γ-equivariant, so $\varpi^D H$ is Γ-invariant. Both are $\mathcal{O}$-lattices tensored with $\mathcal{O}_E$, so $\varpi^D H$ is $\mathcal{O}$-linear. Both are self-dual for $\langle\,,\rangle_{D+1}$ ($\mathfrak{L}$ because φ_{D+1} is isometric modulo $\varpi^{D+1}\mathfrak{a}$ and so carries e'_{D+1} to $e_{0,D+1}$), so $\varpi^D H + (\varpi^D H)^*$ is integral. Their twists by $\mathfrak{N}_\xi$, the transport of $\mathfrak{M}'/\varpi^{D+1}$ and $\mathfrak{M}_0/\varpi^{D+1}$, have height ≤ 1 and the descent data of $\operatorname{Gal}(\tilde{F}/E)$, so $\varpi^D H \in \mathbb{T} \otimes (\varpi^D \mathcal{O}_E / \varpi^{D+1} \mathcal{O}_E)$. By Lemma 8.10, $\varpi^D H = 0$, so $\mathfrak{L} = \mathfrak{L}_0$, which gives α_{D+1}. □

8.6. **The leading digit at 5.**

Theorem 8.12. *Let $p \geq 7$, $p \not\equiv 1 \pmod 5$, f even, $u_0 \in \mathbb{Q}$ with $v_5(u_0) \geq 2$, and $\varphi \colon T' \to T_0$ an $\mathcal{O}$-linear isometry with $\varphi \equiv \iota_{\mathrm{can}} \pmod{\varpi}$ and $\varphi\rho'(g)\varphi^{-1} \equiv \rho_0(g) \pmod{\varpi^D}$ for $g \in \Gamma$, $D \geq 1$; write $\varphi\rho'\varphi^{-1} = (1 + X)\rho_0$.*

(i) The class of the off-diagonal part X_β of X modulo ϖ^{2D} in $H^1(K_5, \sqrt{5}^{\lfloor D/2\rfloor}\mathcal{T}/\sqrt{5}^{D}\mathcal{T})$ is the reduction of a class of $H^1_f(K_5, \sqrt{5}^{\lfloor D/2\rfloor}\mathcal{T})$.

(ii) If $D \geq 4$ is even, the diagonal part of the class of X in $\mathrm{gr}^D \mathrm{End}$ is a coboundary on Γ.

Hence (L1) *of Theorem 7.2 holds at every solution with $10p \mid ab$, labeled so that $5 \mid b$ ($u_0 = b/a$, $v_5(u_0) \geq 2$ by Lemma 8.2).*

Proof. Work over G_E after the twist by ξ. By Proposition 8.11 there is an isomorphism $\iota_{\mathfrak{M}}\colon \mathfrak{M}'/\varpi^D \cong \mathfrak{M}_0/\varpi^D$ with $T_{\mathfrak{S}}(\iota_{\mathfrak{M}}) = \varphi^{-1} \bmod \varpi^D$ on $G_{\tilde{F}_\infty}$ ($T_{\mathfrak{S}}$ is contravariant). Choose lifts $f_1', f_2' \in \mathfrak{M}'$ of $\iota_{\mathfrak{M}}^{-1}(\bar{f}_1), \iota_{\mathfrak{M}}^{-1}(\bar{f}_2)$; the ϕ-matrix of $\mathfrak{M}'$ in this basis is $A' = \mathrm{diag}(A_1, A_2) + \varpi^D Y$. By Lemma 5.9(b) and (K1), $\wedge^2\mathfrak{M}' \cong \wedge^2\mathfrak{M}_0$, so $\det A' = wA_1A_2$ with w a unit. On each component $E(u) = (\text{unit}) \cdot A_1A_2A_3$, where A_3 is the product of the factors $u^p - \tau(\lambda_5)$ over the embeddings τ of E in neither weight-1 set.

(i) Let Λ_D be the preimage in $T'\xi$ of $\varphi^{-1}((\mathcal{O}_E/\varpi^D)\bar{v}_2)$. It is G_E-stable, and $\Lambda_D/\varpi^D\Lambda_D$ is an extension of $(\mathcal{O}_E/\varpi^D)(\chi_m)$ by $(\mathcal{O}_E/\varpi^D)(\Psi\chi_m)$ whose class is $[\varpi^{-D}X_{12} \bmod \varpi^D]$, which multiplication by ϖ^D identifies with $[X_{12} \bmod \varpi^{2D}]$. As $T_{\mathfrak{S}}$ reverses inclusions (K1), the Breuil–Kisin module of Λ_D is $\mathfrak{N}_D = \mathfrak{S}_{\mathcal{O}_E}\varpi^{-D}f_1' + \mathfrak{S}_{\mathcal{O}_E}f_2' \supset \mathfrak{M}'$: the set of $x \in T'\xi = T_{\mathfrak{S}}(\mathfrak{M}')$ with $x(f_1') \in \varpi^D\mathfrak{S}^{\mathrm{ur}}$ is Λ_D, because $T_{\mathfrak{S}}(\iota_{\mathfrak{M}}) = \varphi^{-1} \bmod \varpi^D$ and the elements of $T_{\mathfrak{S}}(\mathfrak{M}_0/\varpi^D)$ that vanish on $\bar{f}_1$ are the multiples of $\bar{v}_2$. In the basis $(\varpi^{-D}f_1', f_2')$ the matrix of $\mathfrak{N}_D$ is $\left(\begin{smallmatrix} A_1+\varpi^D Y_{11} & \varpi^{2D}Y_{12} \\ Y_{21} & A_2+\varpi^D Y_{22}\end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} A_1 & 0 \\ Y_{21} & A_2\end{smallmatrix}\right) \pmod{\varpi^D}$, and $E(u)Y_{21}/(A_1A_2) = (\text{unit}) \cdot A_3Y_{21}$. The module $\mathfrak{F}$ with matrix exactly $\left(\begin{smallmatrix} A_1 & 0 \\ \tilde{Y}_{21} & A_2\end{smallmatrix}\right)$ in a basis (f_1'', f_2''), $\tilde{Y}_{21}$ a lift of Y_{21} with its descent type, therefore has height ≤ 1, so by (K1) it is the Breuil–Kisin module of a lattice in a crystalline representation. As $T_{\mathfrak{S}}$ turns the ϕ-stable line of $\mathfrak{F}$, with matrix A_2, into the quotient, this is an extension of χ_m by $\Psi\chi_m$, with class $c_{\mathfrak{F}} \in H^1_f(\tilde{F}, \mathcal{O}_E(\Psi))$ after untwisting. The map $f_1'' \mapsto \varpi^{-D}f_1'$, $f_2'' \mapsto f_2'$ is an isomorphism $\mathfrak{F}/\varpi^D \cong \mathfrak{N}_D/\varpi^D$ carrying $\mathfrak{S}_{\mathcal{O}_E}f_2''$ onto $\mathfrak{S}_{\mathcal{O}_E}f_2'$, and the elements of $\Lambda_D/\varpi^D\Lambda_D$ that vanish on f_2' form a line containing the image of $\varpi^D\varphi^{-1}(v_1)$, that is, the sub-line $(\mathcal{O}_E/\varpi^D)(\Psi\chi_m)$ above. So the identification $\mathfrak{F}/\varpi^D \cong \mathfrak{N}_D/\varpi^D$ gives, by (K3), an isomorphism of extensions over $G_{\tilde{F}}$, so $[X_{12} \bmod \varpi^{2D}]$ restricted to $G_{\tilde{F}}$ is the reduction of $\varpi^D c_{\mathfrak{F}}$.

Descent to K_5. Let $\mathcal{A} = \varpi^D\mathcal{O}_M\sigma_m$, the off-diagonal part of $\varpi^D\,\mathrm{End}_{\mathcal{O}}(T_0)$; over G_E, $\beta\sigma_m \mapsto \beta$ is the $(1,2)$-entry and identifies $\mathcal{A}$ with $\varpi^D\mathcal{O}_E(\Psi)$. So $c_{\tilde{F}} = \varpi^D c_{\mathfrak{F}} \in H^1_f(\tilde{F}, \mathcal{A})$ reduces to the restriction of $[X_\beta] \in H^1(K_5, \mathcal{A}/\varpi^D\mathcal{A})$, the class of $X_\beta \bmod \varpi^{2D}$. Let $\bar{\Gamma} = \mathrm{Gal}(\tilde{F}/K_5)$, of order $2pf$, prime to 5. By Hochschild–Serre, restriction identifies $H^1(K_5, \mathcal{A})$ with $H^1(\tilde{F}, \mathcal{A})^{\bar{\Gamma}}$, and likewise for $\mathcal{A}/\varpi^D\mathcal{A}$. So the average $|\bar{\Gamma}|^{-1}\sum_{g\in\bar{\Gamma}} g \cdot c_{\tilde{F}}$ is the restriction of some $c_K \in H^1(K_5, \mathcal{A})$. This average lies in $H^1_f(\tilde{F}, \mathcal{A})$, as each $g \cdot c_{\tilde{F}}$ does, and reduces to the restriction of $[X_\beta]$, which is $\bar{\Gamma}$-invariant. Hence c_K reduces to $[X_\beta]$, and $c_K \in H^1_f(K_5, \mathcal{A})$, as a class that is crystalline on $G_{\tilde{F}}$ is crystalline ($H^1(\bar{\Gamma}, -)$ vanishes on $\mathbb{Q}_5$-vector spaces). Finally, $\beta\sigma_m \mapsto \beta^\dagger\sigma_m$ is $Z \mapsto -Z^*$ (from the formula for h_0 in Section 6.2), which commutes with Γ, as each $\rho_0(g)$ is a similitude of h_0. So $P(\beta) = (\beta + \beta^\dagger)/2$ is a Γ-equivariant projection of $\mathcal{A}$ onto $\mathcal{T} \cap \varpi^D\mathcal{O}_M = \sqrt{5}^{\lfloor D/2\rfloor}\mathcal{T}$, mapping $\varpi^D\mathcal{A}$ onto $\sqrt{5}^D\mathcal{T}$ (Proposition 6.4(a) and its proof). Hence $P_*c_K \in H^1_f(K_5, \sqrt{5}^{\lfloor D/2\rfloor}\mathcal{T})$ reduces to $P_*[X_\beta] = [X_\beta]$: X_β is fixed by P modulo ϖ^{2D}, because $1 + X$ is unitary (φ is an isometry), so that $X^* \equiv -X \pmod{\varpi^{2D}}$.

(ii) *Step 1.* On a component where A_1 is not a unit, A_2 is a unit, so $\det A' = wA_1A_2$ gives $v_\varpi(Y_{11}(x)) \geq D$ at each root x of A_1. The roots of $E(u)$ are ν times distinct $4p$-th roots of

unity, whose differences have ϖ-valuation $1/p$, so Lagrange interpolation over at most $4p$ roots loses less than 4 in valuation. Hence the remainder of Y_{11} modulo A_1 vanishes modulo ϖ when $D \geq 4$: $Y_{11} \equiv qA_1 \pmod{\varpi}$ for some $q \in \mathfrak{S}_{\mathcal{O}_E}$ (on a component where A_1 is a unit, $q = Y_{11}A_1^{-1}$). *Step 2.* Let N be the preimage in $T'\xi$ of $\varphi^{-1}((\mathcal{O}_E/\varpi^D)\bar{v}_1)$, with basis $w_1 = \varphi^{-1}(v_1)$, $w_2 = \varpi^D\varphi^{-1}(v_2)$. Modulo $\varpi^{2D}N$ the line $\mathcal{O}_E w_2$ is G_E-stable, with quotient character $(1 + X_{11})\Psi\chi_m$. As in (i), with f_1' and f_2' exchanged, the Breuil–Kisin module of N is $\mathfrak{S}_{\mathcal{O}_E} f_1' + \mathfrak{S}_{\mathcal{O}_E}\varpi^{-D} f_2'$, with matrix $\left(\begin{smallmatrix} A_1+\varpi^D Y_{11} & Y_{12} \\ \varpi^{2D}Y_{21} & A_2+\varpi^D Y_{22}\end{smallmatrix}\right)$ in the basis $(f_1', \varpi^{-D}f_2')$. So $\mathfrak{S}_{\mathcal{O}_E} f_1'$ is ϕ-stable modulo ϖ^{2D}, with matrix $A_1 + \varpi^D Y_{11}$; it and the quotient by it have height ≤ 1, as $E(u)$ times the inverse of the matrix above is integral (its determinant is wA_1A_2) and the matrix is upper triangular modulo ϖ^{2D}. By (K2), (K3) the elements of $N/\varpi^{2D}N$ that vanish on f_1' form a $G_{\tilde{F}}$-stable line ℓ_K, and the quotient by ℓ_K is $T_{\mathfrak{S}}$ of $\mathfrak{S}_{\mathcal{O}_E} f_1'$ mod ϖ^{2D}, with character χ_K. *Step 3.* As $T_{\mathfrak{S}}(\iota_{\mathfrak{M}}) = \varphi^{-1}$ mod ϖ^D, and $\iota_{\mathfrak{M}}$ maps f_1' mod ϖ^D to $\bar{f}_1$, on which $\bar{v}_2$ vanishes, $\varphi^{-1}(v_2)(f_1') \in \varpi^D\mathfrak{S}^{\mathrm{ur}}$. So $w_2(f_1') \in \varpi^{2D}\mathfrak{S}^{\mathrm{ur}}$, and the line $\mathcal{O}_E w_2$ mod $\varpi^{2D}N$ lies in ℓ_K. Both are free of rank one over $\mathcal{O}_E/\varpi^{2D}$. Indeed, w_2 is part of a basis of N, and ℓ_K is the kernel of a surjection from $N/\varpi^{2D}N$, which is free of rank two, onto the quotient by ℓ_K, which is free of rank one. So the two are equal, and $\chi_K \equiv (1 + X_{11})\Psi\chi_m \pmod{\varpi^{2D}}$ on $G_{\tilde{F}}$, in particular modulo ϖ^{D+1}. *Step 4.* By Step 1 the matrix $A_1 + \varpi^D Y_{11}$ of $\mathfrak{S}_{\mathcal{O}_E} f_1'$ mod ϖ^{2D} is $A_1(1 + \varpi^D q)$ modulo ϖ^{D+1}. Write $q = q_0 + q_+$ with q_0 constant on each component and $q_+ \in u\mathfrak{S}_{\mathcal{O}_E}$; the change of basis by $1 + \varpi^D \sum_{n\geq 0} \phi^n(q_+)$, a convergent sum as $\phi(u) = u^5$, replaces q by q_0. A rank-one module with a constant matrix $1 + \varpi^D q_0$ is that of an unramified character $\mu \equiv 1 \pmod{\varpi^D}$, so, by (K1)(a), the étale ϕ-module of χ_K modulo ϖ^{D+1} is that of $\Psi\chi_m$ times μ; both are finite flat, the first by (K4), as a quotient of $N/\varpi^{2D}N$ by a $G_{\tilde{F}}$-submodule (Step 2), the second as the ϖ^{D+1}-torsion of a 5-divisible group ((K1)(c)), so by (K3) $1 + X_{11} \equiv \mu \pmod{\varpi^{D+1}}$ on $G_{\tilde{F}}$, and the digit is unramified on $G_{\tilde{F}}$. *Step 5.* The inertia index of $\tilde{F}/K_5$ is $2p$, prime to 5, so the digit is unramified on Γ, that is, lies in $H^1_{\mathrm{ur}}(K_5, \mathrm{gr}^D \operatorname{diag})$, which is 0 for f even (Proposition 6.6(c)). The same argument with the roles of the lines exchanged treats X_{22}. □

8.7. **Odd order of 5.** In Sections 8.4, 8.5 and 8.6 we assumed that $f = \mathrm{ord}_p 5$ is even. This subsection removes that assumption. The bound $|a_j| < p$ holds for either parity (Section 8.4). For f odd, Lemma 8.10 takes a different form (Lemma 8.13); Lemma 8.7, Proposition 8.11 and part (i) of Theorem 8.12 carry over (Proposition 8.14); and the proof of part (ii) of Theorem 8.12 shows that the class of the diagonal part is unramified (Theorem 8.15); for f odd this does not make it vanish (Proposition 6.6(c)). With Proposition 6.13 this proves the criterion for f odd (Corollary 8.16).

Lemma 8.13. *Let f be odd and $D \geq 0$. No nonzero $H \in \mathbb{T} \otimes (\varpi^D\mathcal{O}/\varpi^{D+1}\mathcal{O})$ is at the same time* (b) *invariant under Γ, acting through the descent data and on the coefficients, and* (c) *compatible with h, that is, $H + H^*$ is integral, $*$ the adjoint for the pairing induced by h (Section 8.4). The labels are those of Lemma 8.10; its condition* (a)*, $\mathcal{O}$-linearity, holds here automatically, as $\mathcal{O}_E = \mathcal{O}$.*

Proof. By Lemma 8.7, $H = H_{12} + H_{21}$ is off-diagonal, and H_{12}, H_{21} are linear combinations of the elements $H_{\mathcal{R}}$. As c is trivial on k, it is trivial on $W(k)$. So the descent data of Γ (Section 8.4) and the adjoint act componentwise on $\mathfrak{S}_{\mathcal{O}} = \prod_j \mathcal{O}[[u]]$, and on H_{12} and H_{21} separately, since the lines are Γ-stable and isotropic. For an off-diagonal endomorphism X with $Xe_2 = \beta e_1$ and $Xe_1 = 0$, the condition $h(Xe_2, e_2) + h(e_2, Xe_2) = 0$ reads $\beta h_{12} -$

$\mathsf{c}(\beta h_{12}) = 0$. If β has ϖ-valuation D, then βh_{12} has valuation $D-3$, and as $\mathsf{c}(\varpi) \equiv -\varpi \pmod{\varpi^2}$ and c is trivial on k, $\mathsf{c}(\beta h_{12}) \equiv (-1)^{D-3}\beta h_{12}$ modulo ϖ^{D-2}. The same computation applies on the Breuil–Kisin side, to $\beta = \kappa u^{a_j}$ on component j with $\kappa \in \varpi^D\mathcal{O}$, with the value $\mathring{h}_{12}$ on $\mathring{f}_1, \mathring{f}_2$ of the form $\mathring{h}_0$ of Section 8.4, built from h, in place of h_{12}. That form is skew-Hermitian, as h is. As the lines are isotropic and $\mathfrak{M}(T_0)$ is self-dual, $\mathring{h}_{12}$ is h_{12} times a unit of $\mathfrak{S}_\mathcal{O}$, on which c acts trivially modulo ϖ. So at depth D the elements of the H_{12}-part of $\mathbb{T}$ (Lemma 8.7(b)) are skew for D odd and self-adjoint for D even, and likewise for H_{21}, with $\mathsf{c}(h_{12})$ in place of h_{12}. This is the parity found for f even in Lemma 8.10.

Let $\tilde{r}$ be as in Lemma 8.9. By that lemma, at depth D the descent datum of $\tilde{r}$ acts on every $H_\mathcal{R}$, and on every $(2,1)$-analogue, by $(-1)^D$. Hence for D odd, $\tilde{r}$ acts by -1 on every $H_\mathcal{R}$, and (b) fails unless $H = 0$; for D even, every $H_\mathcal{R}$ is self-adjoint, so $H + H^* = 2H$, and (c) fails unless $H = 0$. This holds for H_{12} and H_{21} separately. □

When f is odd, $\mathrm{End}_\Gamma(T_0/\varpi)$ is $M_2(\mathbb{F}_5)$ rather than $\mathbb{F}_5 \oplus \mathbb{F}_5\bar{\sigma}_m$. This does not enlarge what Lemma 8.13 must treat: the difference of two models lies in $\mathbb{T}$ whatever the residual endomorphisms are. As in Section 8.4, the class in $\mathbb{T}$ of an off-diagonal residual endomorphism is an $\mathbb{F}_5$-linear combination of $\sum_\mathcal{R} H_\mathcal{R}$ and its H_{21}-analogue, since the ϕ-compatible maps from either line to the other form one $\mathbb{F}$-line. A diagonal one, which is a scalar on each of the two lines, corresponds to an integral endomorphism, with class 0 in $\mathbb{T}$, so it preserves the CM model $\mathfrak{M}_0/\varpi$.

Proposition 8.14. *Let f be odd. Then Lemma 8.7, Proposition 8.11 and part* (i) *of Theorem 8.12 hold in the set-up for f odd of Section 8.4, whose exponents again satisfy $0 < |a_j| < p$, with Lemma 8.13 in place of Lemma 8.10.*

Proof. The proof of Lemma 8.7 uses the parity of f only through $a_j \neq 0$ and $|a_j| < p$, which hold for either parity (Section 8.4). The proof of Proposition 8.11 uses the parity of f only through Lemma 8.10: its base case is Proposition 8.5, which holds for every $p \geq 7$, and in the inductive step the difference of the two models is an H as in Lemma 8.13, hence 0 ($\mathcal{O}$-linearity is automatic, as $\mathcal{O}_E = \mathcal{O}$). In the proof of Theorem 8.12(i), with $T_0 = \mathcal{O}e_1 \oplus \mathcal{O}e_2$, the off-diagonal part of X is the pair (X_{12}, X_{21}), with the skewness conditions that $X_{12}h_{12}$ and $X_{21}\mathsf{c}(h_{12})$ are fixed by c modulo $\varpi^{2D}\mathfrak{D}^{-1}$. The argument applies to X_{12} as written. For X_{21} it applies to the lattice N of Step 2 of the proof of Theorem 8.12(ii), the preimage of $\varphi^{-1}((\mathcal{O}/\varpi^D)\bar{e}_1)$. Modulo ϖ^D, N is an extension of $(\mathcal{O}/\varpi^D)(\Psi\chi_m)$ by $(\mathcal{O}/\varpi^D)(\chi_m)$ with class $[\varpi^{-D}X_{21} \bmod \varpi^D]$, and its Breuil–Kisin module has the matrix $\left(\begin{smallmatrix} A_1 & Y_{12} \\ 0 & A_2 \end{smallmatrix}\right)$ modulo ϖ^D in the basis $(f_1', \varpi^{-D}f_2')$. The module $\mathfrak{F}'$ with matrix $\left(\begin{smallmatrix} A_1 & \tilde{Y}_{12} \\ 0 & A_2 \end{smallmatrix}\right)$ in a basis (f_1'', f_2''), $\tilde{Y}_{12}$ a lift of Y_{12} with its descent type, has height ≤ 1, as $E(u)\tilde{Y}_{12}/(A_1A_2) = (\text{unit}) \cdot A_3\tilde{Y}_{12}$. Its lattice is an extension of $\Psi\chi_m$ by χ_m, with class $c'_\mathfrak{F} \in H^1_f(\tilde{F}, \mathcal{O}(\Psi^{-1}))$ after untwisting. The map $f_1'' \mapsto f_1'$, $f_2'' \mapsto \varpi^{-D}f_2'$ identifies the two modules modulo ϖ^D, and the elements of $N/\varpi^D N$ that vanish on f_1' form the line of w_2 (Step 3 there), the sub-line $(\mathcal{O}/\varpi^D)(\chi_m)$. So, by (K3), $[X_{21} \bmod \varpi^{2D}]$ restricted to $G_{\tilde{F}}$ is the reduction of $\varpi^D c'_\mathfrak{F}$. The descent to K_5 is unchanged, with $\mathcal{A} = \varpi^D(\mathcal{O}e_{12} \oplus \mathcal{O}e_{21}) = \varpi^D(\mathcal{O}_M\sigma_m) \otimes_{\mathcal{O}_{M'}} \mathcal{O}$, whose two summands are Γ-stable and are $\varpi^D\mathcal{O}(\Psi)$ and $\varpi^D\mathcal{O}(\Psi^{-1})$ over G_E, and with $c_{\tilde{F}} = \varpi^D(c_\mathfrak{F}, c'_\mathfrak{F})$. Here $[\tilde{F} : K_5] = 2pf$ is prime to 5 for either parity. □

Theorem 8.15. *Let $p \geq 7$ be a prime with $p \not\equiv 1 \pmod 5$ and f odd, λ' a prime of M' above 5, $u_0 \in \mathbb{Q}$ with $v_5(u_0) \geq 2$, $D \geq 4$ even, and $\varphi\colon T' \to T_0$ an $\mathcal{O}$-linear isometry with $\varphi \equiv \iota_{\mathrm{can}} \pmod{\varpi}$ and $\varphi\rho'(g)\varphi^{-1} \equiv \rho_0(g) \pmod{\varpi^D}$ for $g \in \Gamma$; write $\varphi\rho'\varphi^{-1} = (1+X)\rho_0$,*

and let x be the class of X in $\mathrm{gr}^D \mathrm{End}$. Then the diagonal part of x is $(x_{11}, -x_{11})$, and its class lies in $H^1_{\mathrm{ur}}(K_5, \mathrm{gr}^D \mathrm{diag})$.

Proof of Theorem 8.15. Let $k_D = \varpi^D\mathcal{O}/\varpi^{D+1}\mathcal{O}$. The field $\tilde{F}$ contains E, so $G_{\tilde{F}}$ fixes $\mathcal{O}$ and acts $\mathcal{O}$-linearly; $\tilde{F}/\mathbb{Q}_5$ is Galois and $e(\tilde{F}/K_5) = 2p$.

Step 0: the diagonal part. As Γ preserves the lines, $Z \mapsto Z_{ii}$ is Γ-equivariant from $\mathrm{gr}^D \mathrm{End}$ onto k_D, with Γ acting on k_D through its action on $\mathcal{O}$; so x_{11} and x_{22} are cocycles of Γ in k_D, and $G_{\tilde{F}}$ acts trivially on k_D. As φ is an isometry and $\rho'(g)$, $\rho_0(g)$ are similitudes with the same multiplier, $1 + X$ is unitary for h. So $h(Xe_1, e_2) + h(e_1, Xe_2) \equiv 0 \pmod{\varpi^{2D}\mathfrak{D}^{-1}}$, $\mathfrak{D}^{-1} = h_{12}\mathcal{O}$ the inverse different, which gives $X_{22} \equiv -\mathsf{c}(X_{11}) \pmod{\varpi^{2D}}$. As D is even, c is trivial on k_D, since $\mathsf{c}(\varpi) \equiv -\varpi \pmod{\varpi^2}$ and c is trivial on k. So $x_{22} = -x_{11}$. The diagonal part of x is therefore $(x_{11}, -x_{11})$, in $\mathrm{gr}^D \mathrm{diag} = \{(b, -b)\}$, a Γ-stable direct summand of $k_De_{11} \oplus k_De_{22}$ with complement $\{(b, b)\}$. So it suffices to show that $x_{11}|_{I_{K_5}}$ is a coboundary.

Steps 1–4. In the set-up for f odd ($\mathcal{O}_E = \mathcal{O}$, $v_i = e_i$), the first paragraph of the proof of Theorem 8.12 and Steps 1–4 of its part (ii) apply to x_{11} as written: they use $D \geq 4$, (K1)–(K4) and the isomorphism $\iota_{\mathfrak{M}}$, which Proposition 8.14 supplies for f odd, but not the parity of f, and they show that x_{11} vanishes on $I_{\tilde{F}}$.

Step 5: descent. As $I_{\tilde{F}}$ is normal of index $e(\tilde{F}/K_5) = 2p$, prime to 5, in I_{K_5}, inflation-restriction shows that $x_{11}|_{I_{K_5}}$ is a coboundary. By Step 0 the class of the diagonal part of x lies in $\ker\bigl(H^1(K_5, \mathrm{gr}^D \mathrm{diag}) \to H^1(I_{K_5}, \mathrm{gr}^D \mathrm{diag})\bigr) = H^1_{\mathrm{ur}}(K_5, \mathrm{gr}^D \mathrm{diag})$. □

Corollary 8.16. *Let $p \geq 7$ be a prime with $p \not\equiv 1 \pmod 5$ and $\mathrm{ord}_p 5$ odd, and suppose that $\mathrm{Sel}(W) = \mathrm{Sel}(\Theta) = 0$. Then no solution lies in class (d).*

Proof. We follow the proof of Theorem 7.2. The choice of φ, the argument away from 5 and the conclusion do not use the local inputs at 5, and the steps at 5 are supplied as follows. Put $u_0 = b/a$, which has $v_5(u_0) \geq 2$ by Lemma 8.2. At each prime λ' of M' above 5, the λ'-component of φ is an $\mathcal{O}$-linear isometry, congruent to ι_{can} modulo ϖ and Γ-equivariant modulo ϖ^D. For D odd, Proposition 8.14 gives (L1)(i). For $D = 2$, Lemma 7.1 applies with (L2), which holds by Proposition 8.5. For $D \geq 4$ even, x is diagonal ($\mathrm{gr}^D \mathcal{T} = 0$), and Theorem 8.15 puts the class of $x|_\Gamma$ in $H^1_{\mathrm{ur}}(K_5, \Theta)$, the sum over λ' of the groups $H^1_{\mathrm{ur}}(K_5, \mathrm{gr}^D \mathrm{diag})$ (Proposition 6.4). □

9. Proof of the main theorems

This section proves Theorem 1.2, as Theorem 9.2, and then Theorem 1.1, as Theorem 9.3.

9.1. **Every solution with $10p \mid abc$.** Class (d) asks that $10p$ divide one of a, b. The argument for class (d) applies more generally to every solution with $10p \mid abc$, whichever variables 2, 5 and p divide; this includes classes (a), (b) and (c) of case (B) and the solutions in case (A) with $p \mid abc$. The reason is a symmetry of the quotient curves and the observation that the local comparison at p need not reduce to ι_{can} modulo ϖ.

For coprime nonzero integers a, b with $a^p + b^p \neq 0$ write $D_{\mathrm{sol}}(a, b)\colon Y^5 = D_p(R, -abc) - a^p + b^p$ (the curve of Proposition 5.1(d)), $e_j(a, b) = [(a\zeta_p^j - b\zeta_p^{-j}, 0) - \infty]$ for $j \in \mathbb{Z}/p$, and $\iota_{\mathrm{can}}(a, b)$ for the residual identification of Section 5.4 built from $e_j(a, b) \mapsto e_j(0)$; at a solution (a, b, c), under the isomorphism $D_{b/a} \cong D_{\mathrm{sol}}(a, b)$ of Proposition 5.1(d), $e_j(b/a)$ corresponds to $e_j(a, b)$.

Lemma 9.1 (the symmetry)**.** *Let a, b be coprime nonzero integers with $a^p + b^p \neq 0$. The map $s(R, Y) = (-R, -Y)$ is an isomorphism over $\mathbb{Q}$ from $D_{\mathrm{sol}}(a, b)$ onto $D_{\mathrm{sol}}(b, a)$. It*

commutes with $[\zeta_5]$ *and with* Φ_1*, respects the principal polarizations, and maps* $e_j(a,b)$ *to* $e_{-j}(b,a)$*. Hence* $\iota_{\mathrm{can}}(b,a)\circ s_* = \tau_0\circ\iota_{\mathrm{can}}(a,b)$ *on the* ϖ*-torsion, where* τ_0 *is the automorphism* $e_j(0)\mapsto e_{-j}(0)$ *of* $\mathrm{Jac}(D_0)[\varpi]$*.*

Proof. As p is odd, $D_p(-R,\alpha) = -D_p(R,\alpha)$ (from $D_p(z+\alpha/z,\alpha) = z^p+\alpha^p/z^p$ and $z\mapsto -z$). So $f_{b,a}(-R) = D_p(-R,-ab)-b^p+a^p = -f_{a,b}(R)$, where $f_{a,b}(R) = D_p(R,-ab)-a^p+b^p$, and s maps $Y^5 = f_{a,b}(R)$ onto $Y^5 = f_{b,a}(R)$, fixing the unique point at infinity; it is an isomorphism of curves over $\mathbb{Q}$, so it respects the principal polarizations. It commutes with $[\zeta_5]\colon Y\mapsto \zeta_5^3 Y$, and with Φ_1, the correspondence $\{Y' = Y,\ R'^2-(\zeta_p+\zeta_p^{-1})RR'+R^2+ab(2-\zeta_p^2-\zeta_p^{-2}) = 0\}$ ((5.2) transported to D_{sol}), whose equation is even in (R,R') and symmetric in a,b. The roots of $f_{a,b}$ are $R_j(a,b) = a\zeta_p^j - b\zeta_p^{-j}$, and $-R_j(a,b) = b\zeta_p^{-j} - a\zeta_p^j = R_{-j}(b,a)$, so s maps $e_j(a,b)$ to $e_{-j}(b,a)$. The last statement follows from the definition of ι_{can}. □

Theorem 9.2. *Let* $p\geq 7$ *be a prime with* $p\not\equiv 1 \pmod 5$ *and* $5\nmid h^-(\mathbb{Q}(\zeta_{5p}))$*. Then there are no integers* a,b,c *with* $\gcd(a,b) = 1$*,* $abc\neq 0$*,* $a^p+b^p = c^5$ *and* $10p\mid ab$*.*

Proof. Let (a,b,c) be such a triple; it is a solution, and each of 2, 5, p divides exactly one of a,b.

Class (d). If $10p$ divides a or b, the solution is in class (d) (Section 2.3); label it so that $10p\mid b$. By Corollary 6.14, $\mathrm{Sel}(W) = \mathrm{Sel}(\Theta) = 0$. If $\mathrm{ord}_p 5$ is even, then at a class-(d) solution (L1) holds by Theorem 8.12 and (L2) by Proposition 8.5; so Theorem 7.2 applies. If $\mathrm{ord}_p 5$ is odd, Corollary 8.16 applies.

The general case. Using the symmetry $(a,b,c)\mapsto(b,a,c)$ we label the solution so that $5\mid b$; then 2 and p may divide either variable. We run the proof of Theorem 7.2 (for $\mathrm{ord}_p 5$ even) or of Corollary 8.16 (for $\mathrm{ord}_p 5$ odd), at this solution, with $T' = T_5(\mathrm{Jac}\, D_{\mathrm{sol}}(a,b))$ and with isometries $\varphi\equiv\iota_{\mathrm{can}}(a,b) \pmod\varpi$. We check each place where the class-(d) hypothesis $10p\mid b$ is used.

The choice of φ*.* In the proof of Theorem 7.2, ι_{can} enters only through the choice of φ and through the local inputs at 5: (L1), (L2) and Lemma 7.1 (and, for $\mathrm{ord}_p 5$ odd, the statements of Section 8.7 used in Corollary 8.16). At the places $v\mid p$ the proof uses Proposition 5.5 only to provide *some* $\mathcal{O}_{M'}$-linear G_{K_v}-equivariant isomorphism $\iota_v\colon T'\to T_0$. Indeed, with $U = \varphi\iota_v^{-1}$ the proof uses only that U is $\mathcal{O}_{M'}$-linear, so that it commutes with the scalars in $\mu_5\subset\mathcal{O}_{M'}$ by which a Sylow 5-subgroup of $\rho_0(I_{K_v})$ acts. Neither $U\equiv 1 \pmod\varpi$ nor the residual identification induced by ι_v is used.

At 5. As $5\mid b$ and $p\mid ab$, $p\nmid c$, so $25\mid b$ by Lemma 8.2, and $u_0 = b/a\in\mathbb{Q}$ has $v_5(u_0)\geq 2$; the isomorphism $D_{u_0}\cong D_{\mathrm{sol}}(a,b)$ carries $e_j(u_0)$ to $e_j(a,b)$, hence $\iota_{\mathrm{can}}(u_0)$ to $\iota_{\mathrm{can}}(a,b)$. So Proposition 8.5, Proposition 8.11 and Theorem 8.12 (for $\mathrm{ord}_p 5$ even) and Proposition 8.14 and Theorem 8.15 (for $\mathrm{ord}_p 5$ odd), which are stated for such u_0, give (L1), (L2) and the inputs of Corollary 8.16.

At $v\mid p$*.* If $p\mid b$, Proposition 5.5 applies as at class (d). If $p\mid a$, then $a/b\in p\mathbb{Z}_{(p)}$, and Proposition 5.5 at $D_{a/b}\cong D_{\mathrm{sol}}(b,a)$ gives an $\mathcal{O}_{M'}$-linear isometric $G_{\mathbb{Q}_p}$-equivariant isomorphism $\iota_v'\colon T_5(\mathrm{Jac}\, D_{\mathrm{sol}}(b,a))\to T_0$. By Lemma 9.1, $\iota_v = \iota_v'\circ s_*\colon T'\to T_0$ is $\mathcal{O}_{M'}$-linear, isometric and $G_{\mathbb{Q}_p}$-equivariant, which is all the step at v needs. The isomorphism ι_v induces $\tau_0\circ\iota_{\mathrm{can}}(a,b)$ modulo ϖ, so $U\not\equiv 1 \pmod\varpi$ here, as the choice of φ above allows.

The global inputs. Lemma 5.2 and Lemma 5.12 hold for every u with $u^p\neq -1$. Lemma 5.9(b) holds at every $u_0\in\mathbb{Q}$ with $u_0^p\neq -1$. Lemma 5.7, Lemma 5.10 and Proposition 5.11 are stated for every solution with $10p\mid ab$. The Selmer groups depend on p only.

So the proof of Theorem 7.2, resp. Corollary 8.16, runs at (a, b, c) and ends with a G_K-equivariant isomorphism $T' \cong T_0$, which Proposition 5.11 excludes. So there is no such triple. □

The proof of Theorem 9.2 uses no result of [14] or [41] and nothing about J^-. At class (d) its inputs from Section 5 are Lemma 5.2 and Lemma 5.12 for the start of the induction, Proposition 5.5 at p, Lemma 5.7 for the ramification, Lemma 5.9 for the determinant, Lemmas 5.3 and 5.4 for the model at 5 (Section 8.1), and Proposition 5.11 at the end.

9.2. **The main theorems.**

Theorem 9.3. *Let $p \geq 13$ be a prime with $p \not\equiv 1 \pmod 5$ and $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$. Then the equation $x^p + y^p = z^5$ has no solution in coprime integers with $xyz \neq 0$. If $p \equiv \pm 2 \pmod 5$, only* (CK1)*, the results of* [14] *on J^+ used in Theorem 3.8, and the results for case (C) listed in* (CK4) *are used.*

Proof. Let (a, b, c) be a solution; by Lemma 2.2 it lies in exactly one of the four sets listed there.

1. The solutions for which exactly one of $2, 5$ divides ab are excluded by (CK1).
2. Case (C) is excluded by Theorem 4.1 ($p \geq 13$, $p \not\equiv 1 \pmod 5$, $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$).
3. The solutions with $10 \mid ab$ and $p \nmid ab$: if $p \equiv \pm 2 \pmod 5$, they are excluded by Theorem 3.8 ($p \geq 7$), with no input on J^-. If $p \equiv -1 \pmod 5$, then $p \geq 19$ and p splits in K; case (A) is excluded by Proposition 2.3 ($p \geq 11$); in case (B), $p \nmid c$ by Proposition 3.9, and then $p \nmid abc$, which Proposition 3.10 excludes ($p \geq 17$).
4. The solutions with $10p \mid ab$ are excluded by Theorem 9.2, which uses no result of [14]. □

No condition on 2^{p-1} or 5^{p-1} modulo p^2 is used. The hypotheses enter as follows: $p \geq 13$ only through Theorem 4.1 (as $11 \equiv 1 \pmod 5$, this is $p \geq 11$, the bound of Proposition 4.4); $p \not\equiv 1 \pmod 5$ and $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$ through Steps 2 and 4, and $p \not\equiv 1 \pmod 5$ also through Step 3. Steps 1 and 3 of the proof do not use the hypothesis on $h^-(\mathbb{Q}(\zeta_{5p}))$: every solution at a prime $p \geq 13$ with $p \not\equiv 1 \pmod 5$ lies in case (C) or has $10p \mid ab$.

Remark 9.4. At $p = 7$ (where $5 \nmid h^-(\mathbb{Q}(\zeta_{35}))$), Steps 1, 3 and 4 of the proof of Theorem 9.3 exclude every solution outside case (C), and Theorem 4.6(b) excludes the solutions in case (C) with $5 \mid c$; Proposition 4.4 needs $p \geq 11$, so case (C) with $5 \nmid c$ is left. The equation $x^7 + y^7 = z^5$ was solved by Dahmen and Siksek [20, Theorem 2].

10. Where the theorem applies

Table 3. Primes $13 \leq p < 10^3$ and $13 \leq p < 10^5$ with $p \not\equiv 1 \pmod 5$, by residue of p modulo 5: the number of primes, the number at which the hypotheses of Theorem 1.1 hold, and how many of these have $\mathrm{ord}_p 5$ odd.

range, residue of p	primes	covered	of which $\mathrm{ord}_p 5$ odd
$p < 10^3$, $p \equiv \pm 2 \pmod 5$	86	27	0
$p < 10^3$, $p \equiv -1 \pmod 5$	38	14	11
$p < 10^5$, $p \equiv \pm 2 \pmod 5$	4811	1632	0
$p < 10^5$, $p \equiv -1 \pmod 5$	2390	800	681

Let $\mathcal{E}_h$ be the set of primes p with $5 \mid h^-(\mathbb{Q}(\zeta_{5p}))$. Theorem 1.1 applies at every prime $p \geq 13$ with $p \not\equiv 1 \pmod 5$ and $p \notin \mathcal{E}_h$. Membership in $\mathcal{E}_h$ is decided by the generalized Bernoulli numbers $B_{1,\chi}$ of the odd characters of $(\mathbb{Z}/5p)^\times$ (Section 6.7), without computing a class group. Item (C1) of Appendix B describes the computation, which gives, among the 7202 primes $7 \leq p < 10^5$ with $p \not\equiv 1 \pmod 5$, exactly 2433 with $p \notin \mathcal{E}_h$; one of them is 7, so 2432 of them are at least 13. Table 3 gives the resulting counts. Below 1000 the theorem applies at the 41 primes 13, 19, 23, 29, 43, 59, 67, 107, 167, 193, 199, 233, 263, 283, 307, 317, 353, 359, 379, 383, 397, 419, 449, 467, 499, 503, 547, 563, 587, 607, 647, 659, 709, 719, 743, 827, 839, 859, 863, 883, 953, of which 27 are $\equiv \pm 2$ and 14 are $\equiv -1 \pmod 5$; below 10^5 it applies at 2432 primes (1632 and 800). Among them, those with $\operatorname{ord}_p 5$ odd, all $\equiv -1 \pmod 5$, number 11 below 1000 (19, 59, 199, 359, 379, 419, 499, 659, 719, 839, 859) and 681 below 10^5; the other 30, resp. 1751, have $\operatorname{ord}_p 5$ even. The prime 17 lies in $\mathcal{E}_h$ (Remark 11.1).

Remark 10.1 (a heuristic). A heuristic of Cohen–Lenstra type is consistent with the counts above; it is not a proof. Let $p \geq 7$ be a prime with $p \not\equiv 1 \pmod 5$. As $5 \nmid |(\mathbb{Z}/5p)^\times| = 4(p-1)$, the 5-part of the minus class group of $\mathbb{Q}(\zeta_{5p})$ is the direct sum of components A_O, one for each orbit O of $\operatorname{Gal}(\overline{\mathbb{Q}}_5/\mathbb{Q}_5)$ on the odd characters of $(\mathbb{Z}/5p)^\times$, A_O a module over the unramified extension of $\mathbb{Z}_5$ of degree $|O|$; so $p \notin \mathcal{E}_h$ if and only if every A_O is 0. Write an odd character as $\chi = \chi^{(5)}\chi^{(p)}$, with $\chi^{(5)}$ modulo 5 and $\chi^{(p)}$ modulo p of order d. For $d = 1$, $A_O = 0$, as $h^-(\mathbb{Q}(\zeta_5)) = 1$. Each divisor $d > 1$ of $p-1$ gives $2|(\mathbb{Z}/d)^\times|/o_d$ orbits of size $o_d = \operatorname{ord}_d 5$. Indeed, two of the four $\chi^{(5)}$ make χ odd, and the orbit of χ is $\{\chi^{(5)}(\chi^{(p)})^{5^j}\}$. Model the A_O, for all orbits and all primes p, as independent, with $A_O = 0$ with probability $\eta_\infty(5^{|O|})$, where $\eta_\infty(q) = \prod_{i\geq 1}(1 - q^{-i})$ is the probability that a finite module over the unramified extension of $\mathbb{Z}_5$ with residue field $\mathbb{F}_q$, weighted by $1/|\operatorname{Aut}|$ [16, 17], is 0. Then $p \notin \mathcal{E}_h$ with probability

$$P(p) = \prod_{d \mid p-1,\ d>1} \eta_\infty\big(5^{o_d}\big)^{2|(\mathbb{Z}/d)^\times|/o_d}.$$

Orbits of size 1 come only from $d = 2$ and $d = 4$, so $P(p) \leq \eta_\infty(5)^2 \approx 0.578$, and $P(p) \leq \eta_\infty(5)^6 \approx 0.193$ when $p \equiv 1 \pmod 4$. Over the 7202 primes $7 \leq p < 10^5$ with $p \not\equiv 1 \pmod 5$, $P(p)$ has average 0.333 and sum about 2397, against the 2433 primes of (C1). The sums are about 1893 against 1882 for $p \equiv 3 \pmod 4$, and 505 against 551 for $p \equiv 1 \pmod 4$. Over $13 \leq p < 1000$ the sum is about 42.5, against 41. A model as in Siegel's heuristic for regular primes [68], with each $B_{1,\chi}$ uniformly distributed modulo a prime above 5, that is, $A_O = 0$ with probability $1 - 5^{-|O|}$, predicts about 2793.

11. Remarks and an open question

This section explains where the criterion fails and how the condition $p \not\equiv 1 \pmod 5$ and the parity of $\operatorname{ord}_p 5$ enter the proof; it ends with an open question.

Remark 11.1 (where the criterion fails). The criterion of Theorem 7.2 asks for two Selmer groups to vanish, and Proposition 6.10 shows that the first does not when $5 \mid h^-(M')$: the classes in $\ker(\operatorname{loc}_5|_{G^+})$ are unramified at 2 and p and vanish at 5, so they lie in $\operatorname{Sel}(W)$ for every choice of local condition at 5. So for these primes Theorem 7.2 does not apply. Among the primes $7 \leq p < 60$ with $p \not\equiv 1 \pmod 5$, $5 \mid h^-(M')$ exactly for $p = 17, 37, 53$, with $v_5 h^-(M') = 1$ in each case (Appendix B). By Theorem 6.11(c), $5 \mid h^-(M')$ implies $5 \mid h^-(\mathbb{Q}(\zeta_{5p}))$, so these primes are already outside Theorem 1.1. The obstruction is analogous

to that for Kummer's irregular primes: a nonzero part of the class group in the eigenspaces the Selmer group sees.

The second Selmer group, $\mathrm{Sel}(\Theta)$, is nonzero exactly when $5 \mid h^-(L)$ (Proposition 6.6(c)). Among the primes $7 \le p < 60$ with $p \not\equiv 1 \pmod 5$, this occurs at $p = 37, 47, 53$ (Appendix B). Thus, for every prime $p \ge 7$ with $p \not\equiv 1 \pmod 5$, both Selmer groups vanish if and only if $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$: if $5 \mid h^-(\mathbb{Q}(\zeta_{5p}))$, then $5 \mid h^-(L)$ or $5 \mid h^-(M')$ by Theorem 6.11(c), whose proof does not use the parity of f (Proposition 6.13(c)), so one of the two groups is nonzero; the converse is Corollary 6.14.

Remark 11.2 ($\mathrm{ord}_p 5$ odd). Every $p \equiv \pm 2 \pmod 5$ has $\mathrm{ord}_p 5$ even, so, for $p \not\equiv 1 \pmod 5$, $\mathrm{ord}_p 5$ odd forces $p \equiv -1 \pmod 5$. When it is odd, complex conjugation moves the primes above 5, and Sections 6.8 and 8.7 replace the two steps of the argument for $\mathrm{ord}_p 5$ even that use the parity: the computation of the Selmer groups and the local condition at 5.

Remark 11.3 ($p \equiv 1 \pmod 5$). For $p \equiv 1 \pmod 5$, the solutions of case (B) with $p \nmid abc$ are excluded at split $p \ge 17$ (Proposition 3.10). Step 1 of the proof of Theorem 9.3 and Proposition 2.3 apply unchanged. The rest of the proof does not apply as it stands: Proposition 4.4 uses $p \not\equiv 1 \pmod 5$ in Step 4, Theorem 4.6(b) uses $-1 \in \langle p \bmod 5 \rangle$, Proposition 3.9 is stated for $p \not\equiv 1 \pmod 5$, and Sections 5, 6, 7 and 8 assume $p \not\equiv 1 \pmod 5$ throughout (for example, the step at the places above p in the proof of Theorem 7.2 uses $5 \nmid p - 1$).

An open question. At the primes with $5 \mid h^-(M')$ the condition $\mathrm{Sel}(W) = 0$, which governs the odd depths, fails (Remark 11.1). Can a test one depth deeper, deciding which classes of $\mathrm{Sel}(W)$ can be the leading digit of the comparison for an actual solution, exclude class (d) at these primes, much as Vandiver's criteria for irregular primes [74] go beyond Kummer's theorem for regular ones?

Appendix A. Case (C): the place 2, the primes above 11 and inertia at $\sqrt{5}$

This appendix proves Theorem A.9, which gives Lemma 4.2: a case-(C) solution has $ab \equiv \pm 1 \pmod 5$, and the $\mathfrak{l}$-adic representations of J^-, $\mathfrak{l} \nmid 5$, have conductor exponent 3 at $\mathfrak{q}_5$. It uses (CK4), the published results cited where they are used, and the computations (C6)–(C8) of Appendix B. The arguments are those of [41, §§2–5], in the form needed here.

Conventions. In this appendix $p \ge 13$ is prime and (a, b, c) is a case-(C) solution, so $2 \nmid ab$, $5 \nmid ab$ and $2 \mid c$. As $a^p \equiv a$ and $b^p \equiv b \pmod 8$, $a + b \equiv c^5 \equiv 0 \pmod 4$; exchanging a and b, which keeps ab and replaces C^- by its twist by -1, a square in K_5, we assume $a \equiv -1 \pmod 4$. Put $A = a^p$, $B = b^p$ and $\Phi(x) = x^5 - 5c^2x^3 + 5c^4x - 2(A - B)$, so $C^-\colon y^2 = \Phi(x)$, and $d = \Phi(-A - 2c)$. Let $\zeta = \zeta_5$ and $\omega = \zeta + \zeta^{-1} = (-1 + \sqrt{5})/2$, so $\mathcal{O}_K = \mathbb{Z}[\omega]$ and $\sigma(\omega) = -1 - \omega$; for $n \in \mathbb{Z}$ let $P_n(\omega) = \zeta^n + \zeta^{-n} \in \mathcal{O}_K$, so that $P_{\pm 1}(\omega) = \omega$, $P_{\pm 2}(\omega) = \sigma(\omega) = P_{\pm 1}(\omega)^2 - 2$, $P_{2n}(\omega) = \sigma(P_n(\omega))$, and $P_1(\omega) - P_2(\omega) = \sqrt{5}$. For $D \in \mathbb{Z} \smallsetminus \{0\}$ let $H_D\colon y^2 = x^5 + D$ and $J_D = \mathrm{Jac}\, H_D$, with ω acting by $[\zeta] + [\zeta^{-1}]$, $[\zeta](x, y) = (\zeta x, y)$, and let J_D^σ be J_D with $\mathcal{O}_K$ acting through σ. For an abelian surface $\mathcal{A}$ over K with $\mathcal{O}_K \subseteq \mathrm{End}_K(\mathcal{A})$ and a prime $\mathfrak{l} \mid \ell$ of K, $\rho_{\mathcal{A},\mathfrak{l}}$ is the representation of G_K on $V_\ell(\mathcal{A}) \otimes_{K \otimes \mathbb{Q}_\ell} K_\mathfrak{l}$, and $\bar\rho_{\mathcal{A},\mathfrak{p}}$ that on $\mathcal{A}[\mathfrak{p}]$. For $\mathcal{A} \in \{J^-, J_D\}$ and a prime $\mathfrak{q} \nmid 10\ell$ of good reduction, $a_\mathfrak{q}(\mathcal{A}) = \mathrm{tr}\, \rho_{\mathcal{A},\mathfrak{l}}(\mathrm{Frob}_\mathfrak{q}) \in \mathcal{O}_K$ does not depend on $\mathfrak{l}$; as $\mathcal{A}$ is defined over $\mathbb{Q}$ and a lift of σ to $G_\mathbb{Q}$ conjugates the action of ω to that of $\sigma(\omega)$, $a_{\sigma(\mathfrak{q})}(\mathcal{A}) = \sigma(a_\mathfrak{q}(\mathcal{A}))$, and $a_\mathfrak{q}(J_D^\sigma) = \sigma(a_\mathfrak{q}(J_D))$. We write $K_2 = K_{\mathfrak{q}_2} = \mathbb{Q}_2(\sqrt{5})$, $K_5 = K_{\mathfrak{q}_5} = \mathbb{Q}_5(\sqrt{5})$, K_5^{ur} for the

maximal unramified extension of K_5, $I_5 = G_{K_5^{\mathrm{ur}}}$, $\mathcal{U} = K_5^{\mathrm{ur}}(\zeta)$, which is quadratic over K_5^{ur} and totally ramified of degree 4 over $\mathbb{Q}_5^{\mathrm{ur}}$, and $\mathcal{U}_6 = \mathcal{U}(6^{1/5})$.

The input from [14]. Let $\mathfrak{p} \mid p$ be a prime of K. By (CK4) (Lemma 2.1(b) and its proof) there are $\chi_0 \in K(S_2, 2)^*$ such that $\bar{\rho}_{J^-,\mathfrak{p}} \otimes \chi_0$ is irreducible with Serre level dividing $\mathfrak{q}_2^2\mathfrak{q}_5^{\varepsilon}$ [14, Theorems 7.1(2), 7.9 and 8.7], a newform g of parallel weight 2, trivial character and level $\mathfrak{q}_2^2\mathfrak{q}_5^{\varepsilon}$, and a prime $\mathfrak{B} \mid p$ of its coefficient field, with $\bar{\rho}_{J^-,\mathfrak{p}} \otimes \chi_0 \cong \bar{\rho}_{g,\mathfrak{B}}$ over $\overline{\mathbb{F}}_p$. Here $\varepsilon \in \{2, 3\}$ is the conductor exponent at $\mathfrak{q}_5$ of $\rho_{J^-,\mathfrak{l}}$, $\mathfrak{l} \nmid 5$, and $\varepsilon = 3$ exactly when $v_5(d) = 1$ [14, Propositions 7.23 and 7.24]. For $p \neq 19$, g is the form g_1 attached to J_1, of level $\mathfrak{q}_2^2\mathfrak{q}_5^2$, or a form g_D attached to J_D, of level $\mathfrak{q}_2^2\mathfrak{q}_5^3$, with $D \in \{4, 16, 64\}$ (Lemma 2.1(b)). Here J_1 is the twist of $J^-(-8, 8, 0)$, the Jacobian of H_{32}, by 2. The forms g_1, g_4, g_{16}, g_{64} are 2.2.5.1-400.1-b and 2.2.5.1-2000.1-e, -d, -b in [72], and their eigensystems are those of J_1, J_4, J_{16}, J_{64} (C7). For $p = 19$ the same comparison of traces leaves, besides these, only the newform $f =$ 2.2.5.1-2000.1-h, of level $\mathfrak{q}_2^2\mathfrak{q}_5^3$ and without complex multiplication (C7). The coefficient field of g_D is K, for an identification under which $\rho_{g_D,\mathfrak{B}} \cong \rho_{J_D,\mathfrak{l}}$. As the two ring homomorphisms $\mathcal{O}_K \to \overline{\mathbb{F}}_p$ differ by σ, an isomorphism $\bar{\rho}_{J^-,\mathfrak{p}} \otimes \chi_0 \cong \bar{\rho}_{g_D,\mathfrak{B}}$ over $\overline{\mathbb{F}}_p$ can be written, through one embedding of $\mathbb{F}_{\mathfrak{p}}$ into $\overline{\mathbb{F}}_p$, as $\bar{\rho}_{J^-,\mathfrak{p}} \otimes \chi_0 \cong \bar{\rho}_{J_D,\mathfrak{p}}$ or $\bar{\rho}_{J^-,\mathfrak{p}} \otimes \chi_0 \cong \bar{\rho}_{J_D^{\sigma},\mathfrak{p}}$. Then $\operatorname{tr} \rho_{J^-,\mathfrak{p}}(\gamma)\, \chi_0(\gamma)$ is congruent modulo $\mathfrak{p}$ to $\operatorname{tr} \rho_{J_D,\mathfrak{p}}(\gamma)$, resp. $\operatorname{tr} \rho_{J_D^{\sigma},\mathfrak{p}}(\gamma)$, for every $\gamma \in G_K$ whose traces lie in $\mathcal{O}_K$ (compare [14, §9.1]).

Lemma A.1. *Let E be a finite extension of $\mathbb{Q}_r$, r prime, $E' \subset \overline{\mathbb{Q}}_r$ a finite Galois extension of E, and C a curve of genus 2 over E with affine coordinates x, y. Suppose that $C_{E'}$ is the generic fiber of a smooth proper curve $\mathcal{C}$ over $\mathcal{O}_{E'}$, the closure in $\mathbb{P}(1, 3, 1)$ of $Y^2 + Q_1(X)Y = Q_0(X)$ with $Q_0, Q_1 \in \mathcal{O}_{E'}[X]$, $\deg Q_0 = 5$, $\deg Q_1 \leq 2$, where $x \in E' + E'^{\times} X$ and $y \in E'^{\times} Y + E'[X]$. For $g \in G_E$ write $X(gP) = u_g\, g(X(P)) + t_g$ and $Y(gP) = v_g\, g(Y(P)) + s_g(g(X(P)))$ $(P \in C(\overline{\mathbb{Q}}_r))$, with $u_g, v_g \in E'^{\times}$, $t_g \in E'$, $s_g \in E'[X]$, and suppose that u_g, v_g are units and t_g, s_g integral for every g. Let $\tilde{g}$ be the map of the special fiber $\tilde{C}$ given by the reductions of these formulas, g acting on the residue field. Then for every prime $\ell \neq r$, reduction is an isomorphism $T_\ell(\operatorname{Jac} C) \to T_\ell(\operatorname{Jac} \tilde{C})$ that carries the action of $g \in G_E$ to the map induced by $\tilde{g}$ and every endomorphism of $\operatorname{Jac} C_{E'}$ to its reduction.*

Proof. By [9, §9.4, Proposition 4], $\operatorname{Pic}^0_{\mathcal{C}/\mathcal{O}_{E'}}$ is an abelian scheme with fibers $\operatorname{Jac} C_{E'}$ and $\operatorname{Jac} \tilde{C}$; reduction is therefore a bijection on ℓ^n-torsion [67, §1, Lemma 2], and every endomorphism of the generic fiber extends to this abelian scheme, which is its Néron model [9, §1.2, Proposition 8]. A point P with $X(P)$ integral has $Y(P)$ integral, and the formulas show that gP reduces to $\tilde{g}(\tilde{P})$; if $X(P)$ is not integral, P and gP both reduce to the point at infinity, which $\tilde{g}$ fixes. Sections of $\mathcal{C}$ through points of C are Cartier divisors, so the class of a divisor reduces to the class of its reduction, and the action of g corresponds to that of $\tilde{g}$. □

The characteristic polynomial on $V_{\mathfrak{l}}$ of an automorphism γ of finite order of a curve of genus 2 over a finite field, commuting with an action of $\mathcal{O}_K$ on its Jacobian, lies in $K[x]$ and does not depend on $\mathfrak{l}$: the traces of $t\gamma$ on V_ℓ, $t \in \mathcal{O}_K$, are rational integers independent of ℓ (Lefschetz), and the trace form of $K \otimes \mathbb{Q}_\ell$ is nondegenerate. If γ acts trivially on one $V_{\mathfrak{l}}$ it acts trivially on H^1, so $\gamma = 1$, as an automorphism $\neq 1$ has $1 - \operatorname{tr}(\gamma \mid H^1) + 1 = 2 - 4 < 0$ fixed points otherwise. For the automorphism $[\bar{\zeta}]$ of a curve on whose Jacobian ω acts by $[\bar{\zeta}] + [\bar{\zeta}]^{-1}$, the polynomial is $x^2 - \omega x + 1$ (compute it at a $\mathfrak{l}$ at which this polynomial is irreducible), so $[\bar{\zeta}]^n$ has trace $P_n(\omega)$ on every $V_{\mathfrak{l}}$.

Proposition A.2 (the place 2). *(a) For every prime $\mathfrak{l} \nmid 2$ of K, $\rho_{J^-,\mathfrak{l}}|_{G_{K_2}} \cong \rho_{J_4,\mathfrak{l}}|_{G_{K_2}}$; the inertia group of K_2 acts through a cyclic group of order 5, with no nonzero invariants.*

(b) Let γ be an element of the inertia group of K_2 acting on $V_{\mathfrak{l}}(J^-)$ with order 5. Then $\operatorname{tr}\rho_{J^-,\mathfrak{l}}(\gamma) = P_k(\omega)$ for some $k \not\equiv 0 \pmod 5$, and $\operatorname{tr}\rho_{J_D,\mathfrak{l}}(\gamma)$ is $P_k(\omega)$ for $D = 4, 16$ and $\sigma(P_k(\omega))$ for $D = 64, 1$.

(c) In the input above, $\chi_0 = 1$; and if $\bar\rho_{J^-,\mathfrak{p}}$ is isomorphic to $\bar\rho_{J_D,\mathfrak{p}}$ or to $\bar\rho_{J_D^\sigma,\mathfrak{p}}$ with $D \in \{1, 4, 16, 64\}$, then that surface is J_4, J_{16}, J_{64}^σ or J_1^σ.

Proof. (a) Let $t_2 = 2^{1/5}$ and $E' = \mathbb{Q}_2(\zeta, t_2)$, finite and Galois over $\mathbb{Q}_2$ and containing K_2. As $-A \equiv 1 \pmod 4$ and 5 is a square in K_2, $-A$ is a square in K_2; write $-A = \varsigma^2$ with $\varsigma \in \mathcal{O}_{K_2}^\times$, so that $\varsigma \equiv 1 \pmod 2$, and let $n_2 = v_2(c) \geq 1$. The substitution $x = t_2^4 X$, $y = 2(\varsigma + 2w)$ gives, as $A + B = c^5$,

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

of 2-adic valuations $2n_2 - \frac{8}{5}$, $4n_2 - \frac{16}{5}$ and $5n_2 - 3$, all positive. So $w^2 + \varsigma w = X^5 + c_3 X^3 + c_1 X + c_0$ is a smooth model of C^- over $\mathcal{O}_{E'}$ with special fiber $\tilde C\colon w^2 + w = X^5$. The same substitution turns $C_0^-\colon y^2 = x^5 - 4A$ into $w^2 + \varsigma w = X^5$. For $g \in G_{K_2}$ let $\zeta_g = g(t_2)/t_2 \in \mu_5$; on points of either curve, $X(gP) = \zeta_g^4\, g(X(P))$ and $w(gP) = g(w(P))$, as $g(\varsigma) = \varsigma$. By Lemma A.1, applied to both curves with $E = K_2$, $T_\ell(J^-)$ and $T_\ell(\operatorname{Jac} C_0^-)$ are isomorphic $\mathbb{Z}_\ell[G_{K_2}]$-modules, each identified with $T_\ell(\operatorname{Jac}\tilde C)$ with the same maps $\tilde g$. By [71, Proposition 3 and §3.1], C^- is the quotient of $\mathcal{D}\colon W^2 = c^5 u(u^{10} + \tau u^5 + 1)$, $\tau = -2(A - B)/c^5$, by $(u, W) \mapsto (u^{-1}, W/u^6)$, through $x = c(u + u^{-1})$, $y = W/u^3$, and ω acts by the correspondence induced by $[\zeta] + [\zeta^{-1}]$, $[\zeta](u, W) = (\zeta u, \zeta^3 W)$. As $[\zeta]$ multiplies W and u^3 by ζ^3, this correspondence keeps y, hence w, and sends $x = c(u + u^{-1})$ to $x', x'' = c(\zeta^{\pm1} u + \zeta^{\mp1} u^{-1})$, the roots of $x'^2 - \omega x x' + x^2 + c^2(\omega^2 - 4) = 0$. Indeed, their sum is ωx and their product $x^2 + c^2(\zeta^2 + \zeta^{-2} - 2)$. In the coordinate X this equation reads $X'^2 - \omega X X' + X^2 + c^2 t_2^{-8}(\omega^2 - 4) = 0$, whose constant has valuation $2n_2 - \frac{8}{5} > 0$ ($\omega^2 - 4$ has norm 5). So it reduces to $(X' - \bar\zeta X)(X' - \bar\zeta^{-1} X) = 0$, $w' = w$. As in the proof of Lemma A.1, if $X(P)$ is integral, X' and X'' are integral and reduce to $\bar\zeta^{\pm1} X(\tilde P)$; otherwise all the points reduce to ∞. The reduction of ω is therefore $[\bar\zeta] + [\bar\zeta^{-1}]$, the reduction of $[\zeta] + [\zeta^{-1}]$ on C_0^-. So $\rho_{J^-,\mathfrak{l}}|_{G_{K_2}} \cong \rho_{\operatorname{Jac} C_0^-,\mathfrak{l}}|_{G_{K_2}}$, K-linearly. Every unit of K_2 is a fifth power; with $\varrho^5 = -A$, $x = \varrho x_1$ turns C_0^- into $y^2 = -A(x_1^5 + 4)$, the twist of H_4 by $-A = \varsigma^2$, so $C_0^- \cong H_4$ over K_2, compatibly with $[\zeta]$. This gives the isomorphism of (a). On $\tilde C$ the inertia group acts through $X \mapsto \bar\zeta_g^4 X$, and ζ_g runs through μ_5 on it, as $K_2^{\mathrm{ur}}(t_2)/K_2^{\mathrm{ur}}$ is cyclic of degree 5. The quotient of $\tilde C$ by this group of order 5 has genus 0 (its function field is $\overline{\mathbb{F}}_2(X^5, w)$ with $w^2 + w = X^5$), so the group has no nonzero invariants on $H^1(\tilde C)$.

(b) For $D = 2^j$, $j \in \{0, 2, 4, 6\}$, the substitution $x = t_2^{j+2} X$, $y = 2^{j/2}(1 + 2w)$ turns H_D into $w^2 + w = X^5$ exactly, $[\zeta]$ into $X \mapsto \zeta X$, and for $g \in G_{K_2}$, $X(gP) = \zeta_g^{j+2} g(X(P))$ and $w(gP) = g(w(P))$. Let $\bar\zeta_\gamma^4 = \bar\zeta^k$, $k \not\equiv 0 \pmod 5$; then γ acts on the special fiber of C^- as $[\bar\zeta]^k$ and on that of H_D as $[\bar\zeta]^{km}$, where $4m \equiv j + 2 \pmod 5$, that is $m \equiv 1, 4, 2, 3$ for $D = 4, 16, 64, 1$. By Lemma A.1 and the paragraph before the proposition, the traces are $P_k(\omega)$ and $P_{km}(\omega)$, which is $P_k(\omega)$ for $m \equiv \pm1$ and $P_{2k}(\omega) = \sigma(P_k(\omega))$ for $m \equiv \pm2$.

(c) By (a), the restriction of $\bar\rho_{J^-,\mathfrak{p}}$ to the inertia group of K_2 is the sum of two characters of order 5 (the order is prime to p), which are tamely ramified. If χ_0 were ramified at $\mathfrak{q}_2$, it would be wildly ramified, of conductor exponent at least 2, since a quadratic character of

$K_2^\times$ that is ramified is nontrivial on $1+2\mathcal{O}_{K_2}$, as $\mathbb{F}_4^\times$ has odd order. Then both characters of $\bar\rho_{J^-,\mathfrak{p}}\otimes\chi_0$ on the inertia group would have that conductor exponent, and the Serre level of $\bar\rho_{J^-,\mathfrak{p}}\otimes\chi_0$ would have $\mathfrak{q}_2$-exponent twice that, at least 4, against the bound $\mathfrak{q}_2^2$ of the input. So χ_0 is unramified at $\mathfrak{q}_2$; as it lies in $K(S_2,2)^*$, it is unramified at every finite prime, so trivial, as K has narrow class number 1 (class number 1, and ϕ has norm -1). If $\bar\rho_{J^-,\mathfrak{p}}$ is isomorphic to $\bar\rho_{J_D,\mathfrak{p}}$ or to $\bar\rho_{J_D^\sigma,\mathfrak{p}}$, then for γ as in (b) the trace of $\rho_{J^-,\mathfrak{p}}(\gamma)$ is congruent modulo $\mathfrak{p}$ to that of $\rho_{J_D,\mathfrak{p}}(\gamma)$, resp. $\rho_{J_D^\sigma,\mathfrak{p}}(\gamma)$. By (b) the first is $P_k(\omega)$ and the second is $P_k(\omega)$ or $\sigma(P_k(\omega))$, or for J_D^σ their conjugates; as $P_k(\omega)-\sigma(P_k(\omega))=\pm\sqrt{5}$ is a unit at $\mathfrak{p}$, they must be equal, which leaves J_4, J_{16}, J_{64}^σ and J_1^σ. □

Lemma A.3 (traces by point counts)**.** *Let $q\equiv 1 \pmod 5$ be prime, $\mathfrak{q}\mid q$ a prime of K, $\bar\zeta\in\mathbb{F}_q$ of order 5 with $\omega\equiv\bar\zeta+\bar\zeta^{-1}\pmod{\mathfrak{q}}$, and $u_j\in\mathbb{F}_q^\times$ with $u_j^{(q-1)/5}=\bar\zeta^j$. Suppose $q\nmid AB$.*

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

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

Proof. (a) The map $x=c(X+X^{-1})$, $y=W/X^3$ exhibits C^- modulo q as the quotient $\pi\colon\mathcal{D}\to C^-$ by the involution $\upsilon(X,W)=(X^{-1},W/X^6)$, as $\Phi(c(X+X^{-1}))=c^5(X^5+X^{-5})-2(A-B)$, and ω acts as $\pi_*[\bar\zeta]\pi^*$ [71, §3.1]. Over $\overline{\mathbb{Q}}_\ell$, $H^1(\mathcal{D})$ is the sum of the invariants H_1^1 of $[\bar\zeta]^*$ and of its eigenspaces H_ξ^1, $\xi^5=1\neq\xi$, each of dimension 2; π^* identifies $H^1(C^-)$ with $\{v+\upsilon^*v:v\in H_\xi^1\oplus H_{\xi^2}^1\}$, on which ω acts through $\xi+\xi^{-1}$ on the image of H_ξ^1. Hence $\mathrm{tr}(\mathrm{Frob}^*\mid H_\xi^1)=\jmath_\xi(a_{\mathfrak{q}}(J^-))$, where $\jmath_\xi\colon K\to\mathbb{Q}_\ell(\xi)$ maps ω to $\xi+\xi^{-1}$, and H_ξ^1, $H_{\xi^{-1}}^1$ give the same trace, as υ exchanges them. The Lefschetz formula $q+1-\nu_j=\sum_\xi\xi^{-j}\,\mathrm{tr}(\mathrm{Frob}^*\mid H_\xi^1)$ for $[\bar\zeta]^{-j}\circ\mathrm{Frob}$, the sum over all ξ with $\xi^5=1$ (the term $\xi=1$ does not depend on j), gives, for $a_{\mathfrak{q}}(J^-)=s+t\omega$, $q+1-\nu_j=\mathrm{tr}(\mathrm{Frob}^*\mid H_1^1)+(4s-2t,-s+3t,-s-2t)$ for $j=0,1,2$, so $\nu_2-\nu_0=5s$ and $\nu_2-\nu_1=5t$. (b) Modulo q the curve is $y^2=x^5+D$ (for C^- with $q\mid c$, $\Phi(x)\equiv x^5-4A$), with ω acting by $[\bar\zeta]+[\bar\zeta^{-1}]$. Its H^1 is the sum of lines L_ξ, $\xi\neq1$, on which $[\bar\zeta]^*$ acts by ξ; the fixed points of $[\bar\zeta]^{-j}\circ\mathrm{Frob}$ are ∞ and points corresponding to the affine points of $y^2=u_jx^5+D$ over $\mathbb{F}_q$, so $\mu_j=\sum_\xi\xi^{-j}\,\mathrm{tr}(\mathrm{Frob}^*\mid L_\xi)$, and $\jmath_\xi(a_{\mathfrak{q}})=\mathrm{tr}(\mathrm{Frob}^*\mid L_\xi)+\mathrm{tr}(\mathrm{Frob}^*\mid L_{\xi^{-1}})=\frac15\sum_j(\xi^j+\xi^{-j})\mu_j$, which is the formula, as $P_2(\omega)=-1-\omega$. □

Proposition A.4 (the primes above 11)**.** *Let $\mathfrak{p}\mid p$ be a prime of K.*

(a) $\bar\rho_{J^-,\mathfrak{p}}\not\cong\bar\rho_{J_1^\sigma,\mathfrak{p}}$.

(b) If $p=19$, then $\bar\rho_{J^-,\mathfrak{p}}\not\cong\bar\rho_{f,\mathfrak{B}}$ over $\overline{\mathbb{F}}_p$ for the newform $f=$ 2.2.5.1-2000.1-h and every prime $\mathfrak{B}\mid p$ of its coefficient field.

Proof. We compare traces at both primes of K above 11, as in [6, (9.5), Remark 9.12]: $\mathfrak{q}=(3\omega+1)$, at which $\omega\equiv7$, and $\mathfrak{q}'=\sigma(\mathfrak{q})=(3\omega+2)$. The residue $r=(A \bmod 11, c \bmod 11)$ of the solution determines, by Lemma A.3, the traces of J^- at $\mathfrak{q}$ and $\mathfrak{q}'$ when $11\nmid AB$. (a) Suppose $\bar\rho_{J^-,\mathfrak{p}}\cong\bar\rho_{J_1^\sigma,\mathfrak{p}}$. If $11\nmid AB$, J^- has good reduction at $\mathfrak{q}$ and $\mathfrak{q}'$, and $x=a_{\mathfrak{q}}(J^-)-a_{\mathfrak{q}}(J_1^\sigma)$ and $\sigma(x)=a_{\mathfrak{q}'}(J^-)-a_{\mathfrak{q}'}(J_1^\sigma)$ lie in $\mathfrak{p}$; so $x\in\mathfrak{p}\cap\sigma(\mathfrak{p})=p\mathcal{O}_K$, and p divides the content m_r of x (the greatest common divisor of its coordinates in $\mathbb{Z}[\omega]$). If $11\mid AB$, J^- has purely toric reduction at $\mathfrak{q}$ and $\mathfrak{q}'$ [14, Lemma 7.5 and its proof], $\bar\rho_{J^-,\mathfrak{p}}$ is unramified

there, being isomorphic to $\bar\rho_{J_1^\sigma,\mathfrak{p}}$, and by the rigid-analytic uniformization of abelian varieties with purely toric reduction the eigenvalues of $\mathrm{Frob}_\mathfrak{q}$ on it are ±1, $\pm\,\mathrm{N}\,\mathfrak{q}$ with one sign; so $a_\mathfrak{q}(J_1^\sigma)^2 - 144 \in \mathfrak{p}$ and likewise at $\mathfrak{q}'$, and p divides the content m_r of $a_\mathfrak{q}(J_1^\sigma)^2 - 144$ [14, (9.10)]. Over the 121 residues r, $\operatorname{lcm}_r m_r = 240 = 2^4 \cdot 3 \cdot 5$ (C6), so $p \le 5$, a contradiction. (b) The coefficient field K_f of f has degree 4 and contains K; let $\theta = 2a_\mathfrak{q}(f) - 5$, which satisfies $\theta^2 = 5$ (C8), and $\jmath_0 \colon K \to K_f$ the embedding with $\jmath_0(\sqrt{5}) = \theta$. The eigenvalues of f at $\mathfrak{q}$ and $\mathfrak{q}'$ are $\jmath_0(3+\omega)$ and $\jmath_0(2-\omega) = \jmath_0(\sigma(3+\omega))$ (C8). An isomorphism over $\overline{\mathbb{F}}_p$ gives an embedding $\jmath \in \{\jmath_0, \jmath_0\circ\sigma\}$ of K into K_f with $a_\mathfrak{q}(f) - \jmath(a_\mathfrak{q}(J^-))$ and $a_{\mathfrak{q}'}(f) - \jmath(\sigma(a_\mathfrak{q}(J^-)))$ in $\mathfrak{B}$ if $11 \nmid AB$, and $a_\mathfrak{q}(f) \mp 12$, $a_{\mathfrak{q}'}(f) \mp 12$ in $\mathfrak{B}$, with independent signs, if $11 \mid AB$ (as in (a)). Both elements lie in $\jmath_0(\mathcal{O}_K)$, so p divides the norm of the ideal of $\mathcal{O}_K$ that their preimages generate. Over the 121 residues and both $\jmath$, the primes dividing these norms are 2, 3, 5 and 7 (C8), so $p \ne 19$. □

Lemma A.5 (inertia at $\sqrt{5}$)**.** *Let C be C^- or H_D with $D \in \{4, 16, 64\}$, $\mathcal{A} = \operatorname{Jac} C$ with its action of $\mathcal{O}_K$, and $\mathcal{W}$ the set of Weierstrass points of C. For a prime $\mathfrak{l} \nmid 5$ of K let $L_\mathcal{A}$ be the fixed field of the kernel of $\rho_{\mathcal{A},\mathfrak{l}}|_{I_5}$.*

(a) $L_\mathcal{A}$ does not depend on $\mathfrak{l}$.

(b) $L_\mathcal{A}$ contains $K_5^{\mathrm{ur}}(\mathcal{W})$, and $[L_\mathcal{A} : K_5^{\mathrm{ur}}]$ divides $2 \cdot 6!$.

(c) For $p \ge 7$ and $\mathfrak{p} \mid p$, the kernel of $\bar\rho_{\mathcal{A},\mathfrak{p}}|_{I_5}$ is $G_{L_\mathcal{A}}$.

Proof. There are a finite Galois extension E' of K_5 and a model of $C_{E'}$ as in Lemma A.1 with $Q_1 = 0$: for C^-, the model of [14, proof of Proposition 7.23], given by $x = \alpha + \pi^k X$, $y = \pi^{5k/2} Y$ with $\alpha \in E'$, $k \in \{2, 10\}$ and π a uniformizer of a totally ramified extension of K_5 of degree 4 or 20; for H_D, $x = \eta(\lambda X - 1)$, $y = \mu Y$ with $\eta^5 = D$, $\lambda^4 = 5$ and $\mu^2 = D\lambda^5$, as $x^5 + D = D\lambda^5(X^5 - 5\lambda^{-1}X^4 + 10\lambda^{-2}X^3 - 10\lambda^{-3}X^2 + X)$, whose special fiber is $Y^2 = X^5 + X$. For $g \in G_{K_5}$ the hypotheses of Lemma A.1 hold with $E = K_5$: $s_g = 0$; u_g and v_g are units, as g preserves valuations; and t_g is integral, as g permutes the five finite Weierstrass points of C, whose X-coordinates are the roots of Q_0, integral with distinct reductions. So the special fiber $\tilde C$ is a curve of genus 2 over a finite field, and I_5 acts on $V_\ell(\mathcal{A})$ through automorphisms $\tilde g$ of $\tilde C$ commuting with $\mathcal{O}_K$ (Lemma A.1). By the paragraph before Proposition A.2, such an automorphism is trivial on one $V_\mathfrak{l}$ only if it is the identity; so $G_{L_\mathcal{A}}$ is the kernel of $I_5 \to \operatorname{Aut}\tilde C$, which gives (a). Reduction maps $\mathcal{W}$ bijectively, compatibly with I_5, onto the Weierstrass points of $\tilde C$, so $G_{L_\mathcal{A}}$ fixes $\mathcal{W}$; and $\operatorname{Aut}\tilde C/\langle\iota\rangle$, ι the hyperelliptic involution, acts faithfully on these six points, which gives (b). (c) $\rho_{\mathcal{A},\mathfrak{p}}(I_5)$ is finite of order prime to p by (b), and the kernel of reduction on $\mathrm{GL}_2(\mathcal{O}_{K_\mathfrak{p}})$ is a pro-p group. □

For a unit u of $\mathbb{Q}_5^{\mathrm{ur}}$ let $\hat u$ be the root of unity of order prime to 5 with $u \equiv \hat u \pmod 5$, and $\kappa_5(u) \in \overline{\mathbb{F}}_5$ the residue of $(u/\hat u - 1)/5$; so $\kappa_5(6) = 1$, and κ_5 depends only on u mod 25.

Lemma A.6 (Kummer classes)**.** *Let u, u' be units of $\mathbb{Q}_5^{\mathrm{ur}}$.*

(a) $u \in \mathcal{U}^{\times 5}$ if and only if $\kappa_5(u) = 0$; if $\kappa_5(u), \kappa_5(u') \ne 0$, then $\mathcal{U}(u^{1/5}) = \mathcal{U}(u'^{1/5})$ if and only if $\kappa_5(u') \in \mathbb{F}_5^\times \kappa_5(u)$.

(b) If $u \in \mathbb{Z}_5^\times$, then $\kappa_5(u) \in \mathbb{F}_5$, and $\kappa_5(u) = 0$ if and only if $u^4 \equiv 1 \pmod{25}$.

(c) If u is a unit of the unramified quadratic extension $\mathbb{Q}_{25}$ of $\mathbb{Q}_5$ and its norm to $\mathbb{Q}_5$ lies in $\mathbb{Z}_5^{\times 5}$, then $\kappa_5(u) \in \zeta_8\mathbb{F}_5$, where $\zeta_8 \in \mathbb{F}_{25}$ has order 8.

Proof. Let π be a uniformizer of $\mathcal{U}$ and v its valuation, so $v(5) = 4$; let $\mathcal{O}$ be the ring of integers, $U_n = 1 + \pi^n\mathcal{O}$ and $\eta = 5/\pi^4$, a unit. Then $1 + 5y \mapsto \bar y$ gives $U_4/U_5 \cong \overline{\mathbb{F}}_5$, and $U_1^5 \subseteq U_5$. For $t \in \mathcal{O}$, $(1 + \pi t)^5 \equiv 1 + \pi^5(t^5 + \eta t) \pmod{\pi^6}$, and $\bar t \mapsto \bar t^5 + \bar\eta \bar t$ is onto $\overline{\mathbb{F}}_5$, so

every element of U_5 is a fifth power times an element of U_6. For $j \geq 2$, $(1+\pi^j t)^5 \equiv 1+\eta\pi^{j+4}t \pmod{\pi^{j+5}}$, so every element of U_{j+4} is a fifth power times one of U_{j+5}. Moreover, $U_9 \subseteq \mathcal{U}^{\times 5}$ by Hensel's lemma, as $9 > 2v(5)$. So $U_5 \subseteq \mathcal{U}^{\times 5}$. Conversely, if $(\xi x)^5 \in U_4$ with $x \in U_1$ and ξ a root of unity of order prime to 5, then $\xi^5 \equiv 1 \pmod{\pi^4}$, so $\xi = 1$ and $(\xi x)^5 \in U_5$. Hence $U_4 \cap \mathcal{U}^{\times 5} = U_5$, and as $\hat{u}$ is a fifth power, the class of u in $\mathcal{U}^\times/\mathcal{U}^{\times 5}$ is that of $u/\hat{u} \in U_4$, given by $\kappa_5(u)$; Kummer theory, with $\zeta \in \mathcal{U}$, gives (a). (b) Here $\hat{u}^4 = 1$, so $\hat{u} \in \mathbb{Z}_5$ and $w = u/\hat{u} \in 1 + 5\mathbb{Z}_5$, so $\kappa_5(u) \in \mathbb{F}_5$; and $w \mapsto w^4$ maps $1 + 5y$ to $1 + 20y \pmod{25}$, so $w \in 1 + 25\mathbb{Z}_5$ if and only if $u^4 = w^4 \equiv 1 \pmod{25}$. (c) Write $u = \hat{u}(1 + 5y)$ and let Fr be the Frobenius of $\mathbb{Q}_{25}/\mathbb{Q}_5$. The norm of u is $\hat{u}\,\mathrm{Fr}(\hat{u})(1 + 5y)(1 + 5\,\mathrm{Fr}(y))$, and a fifth power in $\mathbb{Z}_5^\times$ is a root of unity times an element of $1 + 25\mathbb{Z}_5$; so $y + \mathrm{Fr}(y) \equiv 0 \pmod 5$, that is $\kappa_5(u)^5 = -\kappa_5(u)$. □

Proposition A.7 (the Weierstrass points)**.** *Let $\mathcal{W}$ be the set of Weierstrass points of C^-.*

(a) There is $\delta \in \mathbb{Q}_5^{\mathrm{ur}}$ with $\delta^2 = -AB$ such that $\beta = A - B + 2\delta$ is a unit; $\beta' = A - B - 2\delta$ satisfies $\beta\beta' = c^{10}$; with $v^5 = \beta$, the roots of Φ are $v\zeta^k + c^2v^{-1}\zeta^{-k}$ ($k \in \mathbb{Z}/5$); and $\mathcal{U}\,K_5^{\mathrm{ur}}(\mathcal{W}) = \mathcal{U}(\beta^{1/5})$.

(b) If $\varepsilon = 3$, then $\kappa_5(\beta) \neq 0$, so $\mathcal{U}(\beta^{1/5})$ is cyclic of degree 5 over $\mathcal{U}$.

(c) If $(\frac{ab}{5}) = -1$, then $5 \nmid c$ and $\kappa_5(\beta) \in \zeta_8\mathbb{F}_5$.

(d) For $D \in \{4, 16, 64\}$, the Weierstrass points $\mathcal{W}_D$ of H_D satisfy $\mathcal{U}\,K_5^{\mathrm{ur}}(\mathcal{W}_D) = \mathcal{U}_6$.

Proof. (a) As $\beta+\beta' = 2(A-B)$ and $\beta\beta' = (A-B)^2+4AB = c^{10}$, β and β' are units if $5 \nmid c$, and if $5 \mid c$ the sign of δ can be chosen with β a unit, as then $A-B \equiv 2A$ is one. With $w = c^2/v$, the identity $(v+w)^5-5vw(v+w)^3+5(vw)^2(v+w) = v^5+w^5$ gives $\Phi(v+w) = \beta+\beta'-2(A-B) = 0$, and likewise for $(v\zeta^k, w\zeta^{-k})$; these five roots are distinct, as $\beta \neq \beta'$ ($AB \neq 0$). They lie in $\mathcal{U}(v)$, and if $v \notin \mathcal{U}$ the generator $v \mapsto \zeta v$ of $\mathrm{Gal}(\mathcal{U}(v)/\mathcal{U})$ moves each of them, so each generates $\mathcal{U}(v)$. (b) By [14, Proposition 7.24], $v_5(d) = 1$. With $x_0 = -A - 2c$, $\Phi(x + x_0) = x^5 + 5x_0x^4 + (10x_0^2 - 5c^2)x^3 + (10x_0^3 - 15c^2x_0)x^2 + 5(x_0^4 - 3c^2x_0^2 + c^4)x + d$, so $\Phi(x + x_0)$ is Eisenstein over $\mathbb{Z}_5^{\mathrm{ur}}$. So 5 divides $[K_5^{\mathrm{ur}}(\mathcal{W}) : K_5^{\mathrm{ur}}]$, hence $[\mathcal{U}(\beta^{1/5}) : \mathcal{U}]$, as $[\mathcal{U} : K_5^{\mathrm{ur}}] = 2$, and $\kappa_5(\beta) \neq 0$ by Lemma A.6(a). (c) If $5 \mid c$, then $-AB \equiv A^2 \pmod 5$ would be a square, so $(\frac{AB}{5}) = (\frac{ab}{5}) = +1$. So $5 \nmid c$, $-AB$ is not a square modulo 5, $\delta \in \mathcal{O}_{\mathbb{Q}_{25}} \smallsetminus \mathbb{Z}_5$, $\mathrm{Fr}(\beta) = \beta'$, and the norm of β is $c^{10} = (c^2)^5$; apply Lemma A.6(c). (d) The roots of $x^5 + D$ generate $\mathcal{U}((-D)^{1/5})$. As $D^4 \equiv 6, 11, 16 \pmod{25}$ for $D = 4, 16, 64$, and $6^4 \equiv 21 \pmod{25}$, $\kappa_5(-D)$ and $\kappa_5(6)$ lie in $\mathbb{F}_5^\times$ (Lemma A.6(b)); apply Lemma A.6(a). □

Proposition A.8. *Suppose $(\frac{ab}{5}) = -1$ and $\varepsilon = 3$. Then for every prime $\mathfrak{p} \mid p$ and every $D \in \{4, 16, 64\}$, the restriction of $\bar{\rho}_{J^-,\mathfrak{p}}$ to I_5 has a kernel different from those of the restrictions of $\bar{\rho}_{J_D,\mathfrak{p}}$ and $\bar{\rho}_{J_D^\sigma,\mathfrak{p}}$.*

Proof. Fix $D \in \{4, 16, 64\}$. By Lemma A.5(c) the kernels are $G_{L_{J^-}}$ and $G_{L_{J_D}}$. Here the representation $\bar{\rho}_{J_D^\sigma,\mathfrak{p}}$ is $\bar{\rho}_{J_D,\sigma(\mathfrak{p})}$, with the action of $\mathcal{O}_K$ composed with σ, so it has the same kernel. The field $L_{J^-}\mathcal{U}$ contains $\mathcal{U}(\beta^{1/5})$ and $L_{J_D}\mathcal{U}$ contains $\mathcal{U}_6$ (Lemma A.5(b), Proposition A.7(a), (d)). By Proposition A.7(b), (c), $\kappa_5(\beta) \in \zeta_8\mathbb{F}_5^\times$, an $\mathbb{F}_5$-line other than $\mathbb{F}_5 = \mathbb{F}_5\kappa_5(6)$, so $\mathcal{U}(\beta^{1/5}) \neq \mathcal{U}_6$ (Lemma A.6(a)), and their compositum has degree 25 over $\mathcal{U}$. If $L_{J^-} = L_{J_D}$, then $L_{J^-}\mathcal{U}$ would contain it; but $[L_{J^-}\mathcal{U} : \mathcal{U}]$ divides $[L_{J^-} : K_5^{\mathrm{ur}}]$, whose 5-part is at most 5 (Lemma A.5(b)). □

Theorem A.9. *Let $p \geq 13$ be prime and (a, b, c) a case-(C) solution with $a \equiv -1 \pmod 4$. For every prime $\mathfrak{p} \mid p$ of K, $\bar{\rho}_{J^-,\mathfrak{p}}$ is isomorphic to $\bar{\rho}_{J_4,\mathfrak{p}}$, $\bar{\rho}_{J_{16},\mathfrak{p}}$ or $\bar{\rho}_{J_{64}^\sigma,\mathfrak{p}}$; the conductor exponent ε of $\rho_{J^-,\mathfrak{l}}$ at $\mathfrak{q}_5$ ($\mathfrak{l} \nmid 5$) is 3, that is $v_5(d) = 1$; and $ab \equiv \pm 1 \pmod 5$.*

Proof. Take χ_0, g and $\mathfrak{B}$ as in (CK4); $\chi_0 = 1$ by Proposition A.2(c). If $p = 19$ and $g = f$, Proposition A.4(b) gives a contradiction. So $g = g_D$ with $D \in \{1, 4, 16, 64\}$, and $\bar\rho_{J^-,\mathfrak{p}}$ is isomorphic to $\bar\rho_{J_D,\mathfrak{p}}$ or to $\bar\rho_{J_D^\sigma,\mathfrak{p}}$. By Proposition A.2(c) that surface is J_4, J_{16}, J_{64}^σ or J_1^σ, and Proposition A.4(a) excludes J_1^σ. So $D \in \{4, 16, 64\}$, the level of g is $\mathfrak{q}_2^2\mathfrak{q}_5^3$, and $\varepsilon = 3$, as the level is $\mathfrak{q}_2^2\mathfrak{q}_5^\varepsilon$. If $(\frac{ab}{5}) = -1$, Proposition A.8 contradicts this isomorphism. So $(\frac{ab}{5}) = +1$. □

This is the part of [41, Theorem 6.7] that we use. That theorem shows more: $ab \equiv -1 \pmod 5$, through a Frobenius trace over a totally ramified extension of K_5 of degree 20 [41, Proposition 6.3], which Proposition 4.4 does not need.

Appendix B. Computations

Each computation below was repeated by a separately written program. The proof of Proposition 3.10 uses the computation (C3), Appendix A uses (C6)–(C8), and (C2) recomputes the dimensions of Lemma 3.5 (as in [21, Table 2]). (C1) decides at which primes $7 \le p < 10^5$ with $p \not\equiv 1 \pmod 5$ the hypothesis $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$ holds, and (C5) counts these primes for Table 3 and evaluates the heuristic of Remark 10.1; (C4) gives the valuations of Remark 11.1, and (C9) checks the worked examples of Example 8.8. All were done with exact arithmetic in PARI/GP 2.17.3 [73] and Python 3.12, except three computations in floating point: the probabilities of Remark 10.1 and their sums, a second evaluation of the exact products of (C4) by its second program, and one cross-check of (C1), which computes $h^-(\mathbb{Q}(\zeta_{5p}))$ for $p \le 109$ as a product of complex numbers and rounds it. The running times below are those of one core of an Apple-silicon Mac, or, where marked "server", of one core of a Linux server. The programs of each item are deposited with their outputs and running times at [42]. Its README lists the first and the separately written programs of each item in its section "Second programs", and its account of each item says how they differ.

(C1) *The primes with* $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$ (Section 10). Let $7 \le p < 10^5$ be a prime with $p \not\equiv 1 \pmod 5$. The analytic class number formula [75, Theorem 4.17] gives $h^-(\mathbb{Q}(\zeta_{5p})) = h^-(\mathbb{Q}(\zeta_p)) \prod_\chi (-\frac12 B_{1,\chi})$, the product over the odd characters χ of $(\mathbb{Z}/5p)^\times$ of conductor $5p$. Fix a prime $\mathfrak{l}$ above 5 of $\mathbb{Q}(\mu_{4(p-1)})$, in which 5 is unramified. Then $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$ if and only if no $B_{1,\chi}$, for χ odd of conductor p or $5p$, lies in $\mathfrak{l}$. For conductor p, $B_{1,\chi} = \frac1p \sum_{x=1}^{p-1} x\chi(x)$. For conductor $5p$ we use $\sum_a \lfloor ca/5p \rfloor \chi(a) = (c - \bar\chi(c))B_{1,\chi}$, the sum over $1 \le a < 5p$ prime to $5p$, with $c \equiv 1 \pmod 5$ a primitive root modulo p, for which $c - \bar\chi(c) \notin \mathfrak{l}$. Indeed, in this item write the odd characters of conductor p as ϕ and those of conductor $5p$ as $\omega^j\phi$, with ω the Teichmüller character modulo 5, $j \in \{1, 2, 3\}$ and $\phi \ne 1$ a character modulo p; then $c \equiv 1 \pmod{\mathfrak{l}}$, while $\bar\chi(c) = \bar\phi(c)$ (as $\omega(c) = 1$) is a root of unity $\ne 1$ of order dividing $p - 1$, which is prime to 5. For both conductors, the condition $B_{1,\chi} \in \mathfrak{l}$ becomes the vanishing modulo $\mathfrak{l}$ of explicit polynomials over $\mathbb{F}_5$ at $\phi(c)$: of $P(T) = \sum_{k=0}^{p-2} (c^k \bmod p)\, T^k$ for conductor p, and of $H_j(T) = \sum_a \lfloor ca/5p \rfloor\, (a^j \bmod 5)\, T^{k(a)}$, with $c^{k(a)} \equiv a \pmod p$, for conductor $5p$. The values $\phi(c)$ for odd ϕ, respectively odd $\omega^j\phi$, are the roots of $T^{(p-1)/2} + 1$, respectively the roots other than 1 of $T^{(p-1)/2} - (-1)^{j+1}$, distinct modulo $\mathfrak{l}$ as $5 \nmid p - 1$; so the conditions are decided by greatest common divisors. Result: 2433 of the 7202 primes have $5 \nmid h^-(\mathbb{Q}(\zeta_{5p}))$; the counts drawn from them are in Section 10. For the 39 primes $p \le 257$ the class number $h^-(\mathbb{Q}(\zeta_{5p}))$ was also computed exactly from the analytic class number formula; the decision agrees at each of them, and for the nine with $5p \le 256$ the values are the terms $a(5p)$ of [62, A061653]. Running time: 8 to 11 minutes for each of four ranges of p (server).

(C2) *Hilbert cusp forms of level* $\mathfrak{q}_5^e$, $e \le 2$ (Lemma 3.5). By the Jacquet–Langlands correspondence, $\dim S_2(\mathfrak{q}_5^e)$ is one less than the number of right ideal classes of an Eichler order of level $\mathfrak{q}_5^e$ in the totally definite quaternion algebra over K unramified at all finite places [27, Definition 3.7, Theorem 3.9 and §4]. As the icosian ring is a maximal order of class number 1 with unit group modulo $\mathcal{O}_K^\times$ isomorphic to A_5 [21, pp. 438–439], the number of right ideal classes of the Eichler order is the number of orbits of A_5 on $\mathbb{P}^1(\mathcal{O}_K/\mathfrak{q}_5^e)$. The 120 icosians are mapped to $\mathrm{GL}_2(\mathcal{O}_K/\mathfrak{q}_5^e)$, and the orbits are counted: one for each $e \le 2$, so $\dim S_2(\mathfrak{q}_5^e) = 0$ for $e \le 2$, as in [21, Table 2]. For $e = 3$ the programs find 3 orbits, so $\dim S_2(\mathfrak{q}_5^3) = 2$, also as in [21, Table 2]. Running time: 1 second.

(C3) *The primes* 19 *and* 79 (Proposition 3.10). For every $t_0 \in \mathbb{F}_p \smallsetminus \{0, 1\}$ the Frobenius polynomial $X^4 - a_1X^3 + a_2X^2 - pa_1X + p^2$ of $\mathrm{Jac}(y^2 = D_5(x) + 2 - 4t_0)$ over $\mathbb{F}_p$ is computed in PARI/GP. The 94 pairs (a_1, a_2) are listed below, in the order $t_0 = 2, \dots, p-1$; none is $(0, p-1)$, so no polynomial is $X^4 + (p-1)X^2 + p^2$. Running time: under 1 second.
$p = 19$, $t_0 = 2, \dots, 18$: $(5,33)$, $(-8,34)$, $(-3,29)$, $(2,34)$, $(-2,34)$, $(12,74)$, $(1,7)$, $(-7,39)$, $(0,38)$, $(7,39)$, $(-1,7)$, $(-12,74)$, $(2,34)$, $(-2,34)$, $(3,29)$, $(8,34)$, $(-5,33)$.
$p = 79$, $t_0 = 2, \dots, 78$: $(10,178)$, $(23,289)$, $(-1,127)$, $(20,258)$, $(9,167)$, $(0,-22)$, $(-13,199)$, $(-4,82)$, $(2,114)$, $(14,162)$, $(-3,149)$, $(-15,113)$, $(-16,142)$, $(4,162)$, $(-5,63)$, $(-24,302)$, $(4,-18)$, $(16,202)$, $(-6,122)$, $(-10,138)$, $(14,202)$, $(24,302)$, $(-13,169)$, $(11,187)$, $(6,122)$, $(13,139)$, $(14,202)$, $(-8,154)$, $(-2,154)$, $(-7,69)$, $(4,-18)$, $(23,279)$, $(10,138)$, $(-8,174)$, $(19,237)$, $(13,139)$, $(1,157)$, $(13,189)$, $(0,158)$, $(-13,189)$, $(-1,157)$, $(-13,139)$, $(-19,237)$, $(8,174)$, $(-10,138)$, $(-23,279)$, $(-4,-18)$, $(7,69)$, $(2,154)$, $(8,154)$, $(-14,202)$, $(-13,139)$, $(-6,122)$, $(-11,187)$, $(13,169)$, $(-24,302)$, $(-14,202)$, $(10,138)$, $(6,122)$, $(-16,202)$, $(-4,-18)$, $(24,302)$, $(5,63)$, $(-4,162)$, $(16,142)$, $(15,113)$, $(3,149)$, $(-14,162)$, $(-2,114)$, $(4,82)$, $(13,199)$, $(0,-22)$, $(-9,167)$, $(-20,258)$, $(1,127)$, $(-23,289)$, $(-10,178)$.

(C4) *The kernel of localization at* 5 (Remark 11.1). For the eleven primes $7 \le p < 60$ with $p \not\equiv 1 \pmod 5$, $v_5 h^-(M')$ and $v_5 h^-(L)$ were computed from the analytic class number formula, evaluating the generalized Bernoulli numbers of the odd characters exactly. The first valuation is 1 at $p = 17, 37, 53$ and 0 otherwise; the second is 1 at $p = 37, 47, 53$ and 0 otherwise. By Proposition 6.10, the localization kernel has dimension 1 at the first three primes and 0 otherwise; by Proposition 6.6(c), $\mathrm{Sel}(\Theta)$ is nonzero at exactly the second three primes in this range. Running time: under 1 second.

(C5) *The counts of Section 10*, computed from the list of (C1): for each range and residue class of p modulo 5, the number of primes, the number in the list and the number of these with $\mathrm{ord}_p 5$ odd (Table 3). The probabilities in Remark 10.1 are computed at each of the 7202 primes of (C1), and the counts they are compared with are taken from the list. Running time: under 1 second for the counts and under 10 seconds for the probabilities (server).

(C6) *Traces at the primes above* 11 (Proposition A.4(a)). For each of the 100 residues $(A \bmod 11, c \bmod 11)$ with $11 \nmid AB$ the trace $a_\mathfrak{q}(J^-) \in \mathcal{O}_K$ at $\mathfrak{q} = (3\omega + 1)$ is computed by Lemma A.3, and again, by a separately written program, from the Jacobian of C^- over $\mathbb{F}_{11}$; with the traces of J_1^σ at $\mathfrak{q}$, the least common multiple over all 121 residues of the contents of $a_\mathfrak{q}(J^-) - a_\mathfrak{q}(J_1^\sigma)$ ($11 \nmid AB$) or of $a_\mathfrak{q}(J_1^\sigma)^2 - 144$ ($11 \mid AB$) is $240 = 2^4 \cdot 3 \cdot 5$.

(C7) *The newforms at the levels dividing* $\mathfrak{q}_2^2\mathfrak{q}_5^3$ (the input of Appendix A). With the Hecke eigenvalues of [72] (as returned by its API on October 1, 2026, and stored in [42]) at the primes above 3, 7 and 11, and again with those of the Brandt module of the icosian ring at the levels $\mathfrak{q}_2^2\mathfrak{q}_5^3$ and $\mathfrak{q}_2^2\mathfrak{q}_5^2$ (every eigensystem, old ones included), the comparison

of [14, §9.3] at the primes above 3, 7, 11, with squared traces (so for every χ_0 at once), leaves for $p \geq 11$ only 2.2.5.1-400.1-b, 2.2.5.1-2000.1-b, -d, -e and 2.2.5.1-125.1-a, which have complex multiplication, and, for $p = 19$ only, 2.2.5.1-2000.1-h. The form 2.2.5.1-125.1-a has level $\mathfrak{q}_5^3$, so it is not a form g of the input of Appendix A. The eigensystems of the first four are those of J_1, J_{64}, J_{16}, J_4 at the 12 primes of K above 3, 7, 11, 19, 29, 31 and 41 (from the Brandt module and from [72]), and, up to the order of the two primes above q, at the 40 primes $q \equiv 1 \pmod 5$ below 1000 (from [72]).

(C8) *The newform 2.2.5.1-2000.1-h* (Proposition A.4(b)). Its eigenvalues at $(3\omega + 1)$ and $(3\omega + 2)$ are $\jmath_0(3 + \omega)$ and $\jmath_0(2 - \omega)$, for the embedding $\jmath_0$ of K into its coefficient field $\mathbb{Q}(\sqrt{5}, \sqrt{6})$ with $\jmath_0(\sqrt{5}) = \theta = 2a_{\mathfrak{q}}(f) - 5$, whose square is 5; the Brandt module confirms the matching of primes and eigenvalues. Over the 121 residues and both embeddings of K, the primes dividing the norms of the ideals in the proof of Proposition A.4(b) are 2, 3, 5 and 7.

Items (C6)–(C8) repeat computations of [41, Appendix A, items A1, A8–A10], whose programs we reran; together they take about four minutes (server).

(C9) *The worked examples* (Example 8.8). For $p = 7$ and $p = 19$ and each prime of M above 5, the numbers x_j, the pairs $(\#\{n = +1\}, \#\{n = -1\})$ and the exponents a_j are computed from their definitions in Section 8.4 and compared with the formula $a_j = p(2x_{j-1} - 1)$ there, and the space $\mathbb{T}$ is computed by solving its defining linear conditions over $\mathbb{F}_5$, for poles of order at most p, $2p$ and $6p$, and compared with Lemma 8.7. Running time: under 1 second (server).

The elimination of the two newforms of level (10) in (CK3) is that of [14, §10], by the method of [14, §9.3]; [41, Table 5] repeats it, as a check, with the same outcome for $p \geq 11$.

Declarations

Use of AI. This paper and its results were produced by an AI research system that the author designed, built and directs, running on Anthropic's Claude Opus 5.5 in Claude Code and OpenAI's GPT-6 Astra in Codex. The author chooses the problems and prioritizes the work. Separate AI agents checked each result, and a second program confirmed the computations the proofs use, with any exceptions listed in the public deposit. The system also searched the literature and checked the citations against reliable sources. The author read the paper, reran the computations from the deposit and takes full responsibility for all of the paper's contents.

Data availability. The programs and data used in this paper, with instructions for rerunning them, are deposited at Zenodo [42].

References

1. Martin Azon, *Effective Darmon's program for the generalised Fermat equation*, 2025, Preprint, arXiv:2504.01967v2.
2. Michael A. Bennett, *The equation $x^{2n} + y^{2n} = z^5$*, J. Théor. Nombres Bordeaux **18** (2006), no. 2, 315–321, doi:10.5802/jtnb.546.
3. 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, doi:10.1007/978-3-319-32162-2_3.
4. Alex J. Best, Sander R. Dahmen, and Nuno Freitas, *On the generalized Fermat equation $x^{13} + y^{13} = z^n$*, 2025, Preprint, arXiv:2510.12092v1.
5. Nicolas Billerey, Imin Chen, Luis Dieulefait, and Nuno Freitas, *A result on the equation $x^p + y^p = z^r$ using Frey abelian varieties*, Proc. Amer. Math. Soc. **145** (2017), no. 10, 4111–4117, doi:10.1090/proc/13475.

6. ———, *On Darmon's program for the generalized Fermat equation, I*, J. Reine Angew. Math. **822** (2025), 107–146, doi:10.1515/crelle-2025-0014, Numbering as in the full version, arXiv:2205.15861v5.
7. Yuri F. Bilu, *Catalan's conjecture [after Mihăilescu]*, Séminaire Bourbaki, Vol. 2002/2003, Astérisque, vol. 294, Soc. Math. France, Paris, 2004, pp. 1–26, Exp. No. 909.
8. Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.
9. Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21, Springer-Verlag, Berlin, 1990, doi:10.1007/978-3-642-51438-8.
10. Christophe Breuil, *Integral p-adic Hodge theory*, Algebraic Geometry 2000, Azumino (Hotaka), Adv. Stud. Pure Math., vol. 36, Math. Soc. Japan, Tokyo, 2002, pp. 51–80, doi:10.2969/aspm/03610051.
11. Nils Bruin, *On powers as sums of two cubes*, Algorithmic Number Theory (Leiden, 2000) (Wieb Bosma, ed.), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 169–184, doi:10.1007/10722028_9.
12. Ana Caraiani, Matthew Emerton, Toby Gee, and David Savitt, *Components of moduli stacks of two-dimensional Galois representations*, Forum Math. Sigma **12** (2024), Paper No. e31, doi:10.1017/fms.2024.4.
13. Imin Chen and Angelos Koutsianas, *Darmon's program: a survey*, 2025, Preprint, arXiv:2507.15149v1.
14. ———, *A modular approach to Fermat equations of signature* $(p, p, 5)$ *using Frey hyperelliptic curves*, 2025, To appear in Algebra & Number Theory; we cite statement numbers of arXiv:2210.02316v2.
15. Imin Chen and Lucas Villagra Torcomian, *A note on conductors of Frey representations at 2*, 2025, Preprint, arXiv:2509.23540v1.
16. Henri Cohen and Hendrik W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number Theory, Noordwijkerhout 1983 (H. Jager, ed.), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62, doi:10.1007/BFb0099440.
17. Henri Cohen and Jacques Martinet, *Étude heuristique des groupes de classes des corps de nombres*, J. Reine Angew. Math. **404** (1990), 39–76, doi:10.1515/crll.1990.404.39.
18. Paula Cohen and Jürgen Wolfart, *Modular embeddings for some nonarithmetic Fuchsian groups*, Acta Arith. **56** (1990), 93–110, doi:10.4064/aa-56-2-93-110.
19. Brian Conrad, *Lifting global representations with local properties*, 2011, Preprint, https://math.stanford.edu/~conrad/papers/locchar.pdf.
20. Sander R. Dahmen and Samir Siksek, *Perfect powers expressible as sums of two fifth or seventh powers*, Acta Arith. **164** (2014), no. 1, 65–100, doi:10.4064/aa164-1-5.
21. Henri Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's last theorem*, Duke Math. J. **102** (2000), no. 3, 413–449, doi:10.1215/S0012-7094-00-10233-5.
22. Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's Last Theorem*, Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), Int. Press, Cambridge, MA, 1997, pp. 2–140, Numbering as in the authors' revised version of 9 September 2007.
23. 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, doi:10.1112/blms/27.6.513.
24. Henri Darmon and Loïc Merel, *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. **490** (1997), 81–100, doi:10.1515/crll.1997.490.81.
25. Henri Darmon and Jean-François Mestre, *Courbes hyperelliptiques à multiplications réelles et une construction de Shih*, Canad. Math. Bull. **43** (2000), no. 3, 304–311, doi:10.4153/CMB-2000-037-x.
26. Harold Davenport and Helmut Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1935), 151–182, doi:10.1515/crll.1935.172.151.
27. Lassina Dembélé and John Voight, *Explicit methods for Hilbert modular forms*, Elliptic curves, Hilbert modular forms and Galois deformations, Adv. Courses Math. CRM Barcelona, Birkhäuser/Springer, Basel, 2013, pp. 135–198, doi:10.1007/978-3-0348-0618-3_4, Numbering as in arXiv:1010.5727v2.
28. Gerd Faltings and Ching-Li Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 22, Springer-Verlag, Berlin, 1990, doi:10.1007/978-3-662-02632-8.
29. Jean-Marc Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbf{Z}$, Invent. Math. **81** (1985), 515–538, doi:10.1007/BF01388584.
30. ———, *Représentations p-adiques des corps locaux. I*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 249–309.
31. ———, *Représentations ℓ-adiques potentiellement semi-stables*, Périodes p-adiques, Astérisque, vol. 223, Soc. Math. France, 1994, pp. 321–347, Exposé VIII.

32. 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, doi:10.1090/memo/1361.
33. Nuno Freitas and Samir Siksek, *The asymptotic Fermat's last theorem for five-sixths of real quadratic fields*, Compos. Math. **151** (2015), no. 8, 1395–1415, doi:10.1112/S0010437X14007957.
34. Kazuhiro Fujiwara, *Level optimization in the totally real case*, 2006, Preprint, arXiv:math/0602586v1.
35. Toby Gee, Tong Liu, and David Savitt, *The Buzzard–Diamond–Jarvis conjecture for unitary groups*, J. Amer. Math. Soc. **27** (2014), no. 2, 389–435, doi:10.1090/S0894-0347-2013-00775-4.
36. ———, *The weight part of Serre's conjecture for* GL(2), Forum Math. Pi **3** (2015), Paper No. e2, doi:10.1017/fmp.2015.1.
37. Franco Golfieri Madriaga and Ariel Pacetti, *Hypergeometric motives and the generalized Fermat equation*, 2025, with an appendix by Ariel Pacetti and Fernando Rodriguez Villegas. Preprint, arXiv:2412.08804v2.
38. Franco Golfieri Madriaga, Ariel Pacetti, and Fernando Rodriguez Villegas, *On rank 2 hypergeometric motives*, 2026, Preprint, arXiv:2603.17978v1.
39. Alexander Grothendieck, *Modèles de Néron et monodromie*, Groupes de monodromie en géométrie algébrique (SGA 7 I), Lecture Notes in Math., vol. 288, Springer-Verlag, Berlin, 1972, pp. 313–523, doi:10.1007/BFb0068694, Exposé IX.
40. Frazer Jarvis, *Correspondences on Shimura curves and Mazur's principle at p*, Pacific J. Math. **213** (2004), no. 2, 267–280, doi:10.2140/pjm.2004.213.267.
41. Manvir Jaswal, *The generalized Fermat equation* $x^{11} + y^{11} = z^5$, 2026, Preprint, Zenodo, doi:10.5281/zenodo.23149242.
42. ———, *Programs and data for "The generalized Fermat equation* $x^p + y^p = z^5$ *and relative class numbers"*, 2026, Zenodo, doi:10.5281/zenodo.23753558.
43. Mark Kisin, *Crystalline representations and F-crystals*, Algebraic geometry and number theory, Progr. Math., vol. 253, Birkhäuser Boston, Boston, MA, 2006, pp. 459–496, doi:10.1007/978-0-8176-4532-8_7.
44. ———, *Moduli of finite flat group schemes, and modularity*, Ann. of Math. (2) **170** (2009), no. 3, 1085–1180, doi:10.4007/annals.2009.170.1085.
45. ———, *Integral models for Shimura varieties of abelian type*, J. Amer. Math. Soc. **23** (2010), no. 4, 967–1012, doi:10.1090/S0894-0347-10-00667-3.
46. Alain Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. **49** (1997), no. 6, 1139–1161, doi:10.4153/CJM-1997-056-2.
47. ———, *On the equation* $x^r + y^r = z^p$, 1998, Notes for a talk given at IEM, Universität Duisburg-Essen; a copy is at https://github.com/NicolasBillerey/xhyper.
48. ———, *Sur l'équation* $a^3 + b^3 = c^p$, Experiment. Math. **7** (1998), no. 1, 1–13, doi:10.1080/10586458.1998.10504355.
49. Serge Lang, *Cyclotomic fields I and II*, combined second ed., Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990, doi:10.1007/978-1-4612-0987-4.
50. Eike Lau, *Frames and finite group schemes over complete regular local rings*, Doc. Math. **15** (2010), 545–569, doi:10.4171/DM/306.
51. ———, *Relations between Dieudonné displays and crystalline Dieudonné theory*, Algebra Number Theory **8** (2014), 2201–2262, doi:10.2140/ant.2014.8.2201.
52. Franz Lemmermeyer, *Ideal class groups of cyclotomic number fields I*, Acta Arith. **72** (1995), no. 4, 347–359, doi:10.4064/aa-72-4-347-359, Numbering as in arXiv:1202.5777v1.
53. Heinrich-Wolfgang Leopoldt, *Zur Struktur der l-Klassengruppe galoisscher Zahlkörper*, J. Reine Angew. Math. **199** (1958), 165–174, doi:10.1515/crll.1958.199.165.
54. Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, doi:10.1093/oso/9780198502845.001.0001.
55. Tong Liu, *Torsion p-adic Galois representations and a conjecture of Fontaine*, Ann. Sci. École Norm. Sup. (4) **40** (2007), no. 4, 633–674, doi:10.1016/j.ansens.2007.05.002.
56. Preda Mihăilescu, *A class number free criterion for Catalan's conjecture*, J. Number Theory **99** (2003), 225–231, doi:10.1016/S0022-314X(02)00101-4.
57. ———, *A cyclotomic investigation of the Fermat–Catalan equation*, 2007, Preprint, arXiv:math/0702766v1.
58. ———, *The strong Fermat–Catalan equation*, 2025, Preprint, arXiv:2509.18275v1.
59. James S. Milne, *Abelian varieties (v2.00)*, 2008, Available at https://www.jmilne.org/math/.

60. 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, doi:10.1007/978-3-642-57916-5.
61. Tadao Oda, *The first de Rham cohomology group and Dieudonné modules*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 63–135, doi:10.24033/asens.1175.
62. OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, 2026, https://oeis.org, accessed October 28, 2026.
63. Ali Rajaei, *On the levels of mod ℓ Hilbert modular forms*, J. Reine Angew. Math. **537** (2001), 33–65, doi:10.1515/crll.2001.058.
64. Ashleigh Ratcliffe and Bogdan Grechuk, *Generalized Fermat equation: a survey of solved cases*, Expo. Math. **43** (2025), no. 4, Paper No. 125688, doi:10.1016/j.exmath.2025.125688.
65. Michel Raynaud, *Schémas en groupes de type* $(p, \dots, p)$, Bull. Soc. Math. France **102** (1974), 241–280, doi:10.24033/bsmf.1779.
66. Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331, doi:10.1007/BF01405086.
67. Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), no. 3, 492–517, doi:10.2307/1970722.
68. Carl Ludwig Siegel, *Zu zwei Bemerkungen Kummers*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II **1964** (1964), 51–57.
69. Christopher M. Skinner and Andrew J. Wiles, *Residually reducible representations and modular forms*, Inst. Hautes Études Sci. Publ. Math. **89** (1999), 5–126, doi:10.1007/BF02698855.
70. John Tate, *p-divisible groups*, Proc. Conf. Local Fields (Driebergen, 1966), Springer-Verlag, Berlin, 1967, pp. 158–183, doi:10.1007/978-3-642-87942-5_12.
71. Walter Tautz, Jaap Top, and Alain Verberkmoes, *Explicit hyperelliptic curves with real multiplication and permutation polynomials*, Canad. J. Math. **43** (1991), no. 5, 1055–1064, doi:10.4153/CJM-1991-061-x.
72. The LMFDB Collaboration, *The L-functions and modular forms database*, 2026, https://www.lmfdb.org, accessed October 23, 2026.
73. The PARI Group, *PARI/GP version 2.17.3*, 2025, Univ. Bordeaux, https://pari.math.u-bordeaux.fr.
74. Harry Schultz Vandiver, *On Fermat's last theorem*, Trans. Amer. Math. Soc. **31** (1929), no. 4, 613–642, doi:10.1090/S0002-9947-1929-1501503-0.
75. Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997, doi:10.1007/978-1-4612-1934-7.
76. André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508, doi:10.1090/S0002-9904-1949-09219-4.
77. Zhong-Peng Zhou, *The inter-universal Teichmüller theory and new Diophantine results over rational numbers. II*, 2025, Preprint, arXiv:2510.05448v1.

Toronto, Canada
Email address: manvirjaswal@icloud.com
URL: https://manvirjaswal.github.io