THE GENERALIZED FERMAT EQUATION $X^5 + Y^3 = Z^7$

MANVIR JASWAL

Abstract. Assuming the classification of Dahmen–Siksek and Putz, we show that $X^5 + Y^3 = Z^7$ has no solution in nonzero coprime integers; equivalently, the generalized Fermat equation of signature $(3, 5, 7)$ has no nontrivial primitive solution in any arrangement of the exponents. By that classification, a solution determines one of seven septic fields: six pure fields $\mathbb{Q}\big((3^a \cdot 5)^{1/7}\big)$, $1 \le a \le 6$, and an exceptional field F. We exclude F by a fifth-power descent over $F(\sqrt{-35})$, where the equation becomes a norm identity for an explicit element; the identity and the element's valuations above 3, 5 and 7 confine it to 125 classes modulo fifth powers, none compatible with its possible fifth-power residue symbols above 11 and 19. For the pure fields we use results from recent preprints on the genus-2 Frey curves of Pacetti and Villagra Torcomian, whose Jacobians have real multiplication by $\mathbb{Q}(\sqrt{5})$. Level lowering shows that their 7-torsion is reducible, giving a rational point on a genus-15 double cover of the genus-8 curve of $\mathbb{F}_{49}$-lines in the 7-torsion. The Prym variety of this cover contains an abelian surface of rank one, and Chabauty's method at 13 confines the point to two explicit rational points, neither coming from a solution.

Contents

1. Introduction 2
2. The field classification and its inputs 7
3. The exceptional field 10
4. The Frey family and the curve $\mathcal{X}$ 19
5. The lift to C 33
6. The surface B: polarization and rank 42
7. The good model at 13 and the integral lattice 53
8. Arithmetic in the Jacobian and the two residue discs 61
Appendix A. Index of notation 65
Appendix B. The S-units of the exceptional field 67
Appendix C. Data for Section 6 68
Appendix D. The model at 13 72
Appendix E. Computations 77
Declarations 81
References 81

2020 *Mathematics Subject Classification.* Primary 11D41; Secondary 11F80, 11G10, 11G30, 11Y50, 14H40.

Key words and phrases. Generalized Fermat equation, Prym variety, Chabauty's method, real multiplication, level lowering, explicit descent.

1. Introduction

1.1. **The equation.** For integers $p, q, r \geq 2$ the *generalized Fermat equation* of signature (p, q, r) is

$$X^p + Y^q = Z^r, \qquad \gcd(X, Y, Z) = 1, \qquad XYZ \neq 0.$$

When $1/p+1/q+1/r < 1$ (the *hyperbolic* case), Darmon and Granville [17] proved that there are only finitely many solutions, and it is conjectured that for $\min(p, q, r) \geq 3$ there are none (Beal's conjecture; see [3] for its history and for a survey of the signatures that have been settled). This paper concerns the signature $(5, 3, 7)$, for which $1/5 + 1/3 + 1/7 = 71/105 < 1$. Up to the order of the exponents it is the case $(3, 5, 7)$, which the survey of solved cases by Ratcliffe and Grechuk [47, §1.1] describes as the smallest triple, ordered by the sum of the exponents, for which Beal's conjecture was then open. The signatures $(3, 4, 5)$, $(5, 5, 7)$ and $(7, 7, 5)$, with which it is often grouped, were settled by Siksek and Stoll [52] (for $(3, 4, 5)$) and by Dahmen and Siksek [14] (for the other two), using descent on curves of small genus combined with the Chabauty–Coleman method and the modular approach. For $(3, 5, 7)$, Dahmen and Siksek [15], together with the enumeration of Putz [46], reduced the problem to seven septic fields (Section 2), and it is these seven fields that we exclude. Chocian [11] has also excluded them, by different methods (see the end of Section 1.7).

We consider integers X, Y, Z, of any sign, with

$$X^5 + Y^3 = Z^7, \qquad \gcd(X, Y, Z) = 1, \qquad XYZ \neq 0. \tag{1.1}$$

Any prime dividing two of X, Y, Z divides the third, so the three are pairwise coprime. Because all three exponents are odd, changing signs and moving a term across the equation matches the solutions of (1.1) with those of each of

$$x^3 + y^5 = z^7, \qquad x^3 + y^7 = z^5, \qquad x^5 + y^7 = z^3$$

in nonzero coprime integers (for instance, $x^5 + y^7 = z^3$ becomes (1.1) with $(X, Y, Z) = (x, -z, -y)$). So a statement about all solutions of (1.1) covers every arrangement of the exponents $3, 5, 7$.

1.2. **The starting point: a septic algebra.** Dahmen and Siksek [15] attach to a solution of (1.1) the parameter ν and, through the fixed polynomial ϕ, the seventh-degree $\mathbb{Q}$-algebra A_ν:

$$\nu = \frac{X^5}{Z^7} \in \mathbb{Q} \smallsetminus \{0, 1\}, \qquad \phi(T) = 15T^7 - 35T^6 + 21T^5, \tag{1.2}$$

$$A_\nu = \mathbb{Q}[T]/(\phi(T) - \nu). \tag{1.3}$$

The polynomial ϕ is adapted to the exponents: $\phi(T) = T^5(15T^2 - 35T + 21)$ and $\phi(T) - 1 = (T-1)^3(15T^4 + 10T^3 + 6T^2 + 3T + 1)$, so as a map $\mathbb{P}^1 \to \mathbb{P}^1$ it is ramified only over 0, 1 and ∞, with ramification indices 5, 3 and 7 at $T = 0, 1, \infty$, matching the exponents in $\nu = X^5/Z^7$ and $1 - \nu = Y^3/Z^7$. Since $\phi'(T) = 105T^4(T-1)^2$, the critical values of ϕ are $\phi(0) = 0$ and $\phi(1) = 1$. As $\nu \notin \{0, 1\}$, the polynomial $\phi(T) - \nu$ is separable and A_ν is an étale algebra of dimension 7. The results of [15] restrict the completions of A_ν at 2, 3, 5 and 7 to explicit lists, determine $A_\nu \otimes \mathbb{R}$, exclude every decomposition of A_ν as a product of smaller fields, and reduce the problem to septic fields with prescribed local behaviour. Dahmen and Siksek found seven such fields in the available number-field database [15, §4.3], and Putz [46] proved that there are no others: every septic field of signature $(1, 3)$ that

is unramified outside 3, 5 and 7 and has its completions at 2, 3, 5 and 7 in these lists is isomorphic to one of the seven fields

$$L_a = \mathbb{Q}\big((3^a \cdot 5)^{1/7}\big) \quad (1 \le a \le 6) \qquad \text{or} \qquad F = \mathbb{Q}[x]/(h(x)), \tag{1.4}$$

where $h(x) = x^7 - 2x^6 + 6x^5 + 50x^4 + 35x^3 + 35x + 35$. We call the L_a the *pure fields* and F the *exceptional field*. The statements we take from [15] and [46] are listed in Section 2. This paper shows that for a solution of (1.1) the algebra A_ν cannot be isomorphic to any of the seven fields.

1.3. **Main results.**

Theorem 1.1 (The pure fields)**.** *Let (X, Y, Z) satisfy (1.1). Then A_ν is not isomorphic to L_a for any $1 \le a \le 6$.*

The proof of Theorem 1.1 uses results from the preprints [43] and [2] on the Frey family of Section 1.5 and on Darmon's curves [16], hyperelliptic curves with real multiplication. They are listed at the beginning of Section 4.

Theorem 1.2 (The exceptional field)**.** *Let (X, Y, Z) satisfy (1.1). Then A_ν is not isomorphic to F.*

Theorem 1.3. *Assume the results of Dahmen–Siksek and Putz stated in Section 2. Then there are no integers X, Y, Z satisfying (1.1). Equivalently, none of the equations $x^3+y^5 = z^7$, $x^3 + y^7 = z^5$ and $x^5 + y^7 = z^3$ has a solution in nonzero coprime integers.*

Proof. By Corollary 2.5, a solution of (1.1) has A_ν isomorphic to one of the seven fields in (1.4). Theorems 1.1 and 1.2 exclude each of them. The equivalent form follows from Section 1.1. □

Only the passage to Theorem 1.3 uses the results of [15] and [46]. Theorems 1.1 and 1.2 are proved by different methods, independently of each other.

1.4. **The exceptional field: a fifth-power descent.** Suppose $A_\nu \simeq F$. The isomorphism sends the class of T to a root $\vartheta \in F$ of $\phi(T) - \nu$; since ν is unknown, ϑ is not a fixed element of F. Put $\beta = 15Z\vartheta$. Then β is an algebraic integer with characteristic polynomial

$$T^7 - 35ZT^6 + 315Z^2T^5 - 15^6X^5 = 15^6Z^7(\phi(T/15Z) - \nu),$$

and $T^7 - 35ZT^6 + 315Z^2T^5 = T^5(T^2 - 35ZT + 315Z^2)$, whose quadratic factor splits over $\mathcal{E} = F(\sqrt{-35})$:

$$\beta^2 - 35Z\beta + 315Z^2 = (\beta - Za_+)(\beta - Za_-),$$

where $a_\pm = (35 \pm \sqrt{-35})/2$, so that $a_+a_- = 315$. Writing $V = \beta - Za_+$ and σ for the involution of $\mathcal{E}/F$, the equation becomes the norm identity $V\,\sigma(V) = 15\,(15X/\beta)^5$, and coprimality of X and Z makes V and $\sigma(V)$ coprime away from the primes above 3, 5 and 7. Consequently the class of V lies in the finite group $\mathcal{M} = \mathcal{E}(S, 5)$ of classes in $\mathcal{E}^\times/\mathcal{E}^{\times 5}$ whose valuations are divisible by 5 at every prime outside the set S of primes above 3, 5 and 7. In $\mathcal{M}$ it satisfies $(1 + \sigma)[V] = [15]$. An unconditional class-group computation shows that the class group of $\mathcal{E}$ has no 5-torsion. As $\mathcal{E}$ also contains no primitive fifth root of unity, $\dim_{\mathbb{F}_5} \mathcal{M} = 16$: the unit rank 6 of $\mathcal{E}$ plus the ten primes of S (Lemma 3.7). The norm relation and the valuations of V at the ten primes of S, which are the same modulo 5 for every solution (Propositions 3.4 and 3.6), cut the possible classes down to an explicit affine set $\mathcal{A}$ of 125 elements (Theorem 3.9). Finally, modulo a prime of $\mathcal{E}$ above 11 or 19 (all these residue fields have order congruent to 1 modulo 5), the residue of V is $\bar\beta - \bar Z\bar a_+$,

where $\bar{\beta}$ is a root of the reduction of the characteristic polynomial of β, which depends only on the residues of X and Z. Running through all residues gives, at 11 and at 19, the list of fifth-power residue symbols that the class of V can have (Lemma 3.11), and no element of $\mathcal{A}$ is compatible with both lists (Proposition 3.12). The primes of $\mathcal{E}$ of residue degree 4 above 2 and 13 would not suffice in place of those above 11 and 19 (Remark 3.13). Section 3 carries out this argument and prints every matrix and every list of residue symbols that its last step uses.

1.5. **The pure fields: a rational point that cannot exist.** Suppose $A_\nu \simeq L_a$. Here the argument passes through a family of curves. Pacetti and Villagra Torcomian [43] attach to a solution the genus-2 curve

$$H_t\colon\ y^2 = 5x^6 - 12x^5 + 10tx^3 + t^2, \qquad t = -X^5/Y^3,$$

whose Jacobian J_t has real multiplication by $\mathbb{Z}[(1+\sqrt{5})/2]$. Since 7 is inert in $K = \mathbb{Q}(\sqrt{5})$, the 7-torsion $J_t[7]$ is a 2-dimensional vector space over $k = \mathbb{F}_{49}$ with a k-linear action of $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. The hypothesis $A_\nu \simeq L_a$, through modularity (Proposition 4.4, proved from a congruence modulo $(\sqrt{5})$ with a modular elliptic curve) and level lowering, forces this representation to be reducible, with a stable line $H \subset J_t[7]$ on which G_K acts through the character $\delta\chi_7$, where χ_7 is the cyclotomic character modulo 7 and δ is the quadratic character, ramified only at (3) and $(\sqrt{5})$, of $K(\sqrt{\mathfrak{d}})/K$ with $\mathfrak{d} = 3(5+\sqrt{5})/2$ (Proposition 4.9). It is the only stable line with this character. It defines a point of a fixed curve $\mathcal{X}$ of genus 8, the curve parametrizing the k-lines in $J_t[7]$ as t varies. The point is rational over $\mathbb{Q}$ and not only over K (Proposition 4.12), and it lies over the value $t = -X^5/Y^3$ of the solution under the degree-50 map $t\colon \mathcal{X} \to \mathbb{P}^1$.

A rational point on $\mathcal{X}$ does not by itself lead to a contradiction. The reducible representation also says how the Galois group acts on the line H, and this information is recorded by an unramified double cover $q\colon C \to \mathcal{X}$ of genus 15: the fibre of C over a line consists of the two classes of its nonzero vectors modulo squares in $k^\times$, with the Galois action twisted by the quadratic character of $K/\mathbb{Q}$ (Section 5). For the stable line of a solution both points of this fibre are rational: G_K acts on H through $\delta\chi_7$, whose values lie in $\mathbb{F}_7^\times \subset (k^\times)^2$, so it fixes both classes, and the twist corrects the action of the elements of $G_\mathbb{Q}$ outside G_K, which exchange them (Lemma 5.2 and Proposition 5.3). So a solution gives a point $R \in C(\mathbb{Q})$ with $t(q(R)) = -X^5/Y^3$.

Rather than determining $C(\mathbb{Q})$ directly, we use the Prym variety of the double cover, $P = \mathrm{im}(1-\tau) \subset \mathrm{Jac}(C)$, where τ is the covering involution. It has dimension 7, and a correspondence on C that comes from the Weil pairing (Section 1.6) acts on it by an endomorphism $\mathcal{D}$ with $\mathcal{D}^2 = 49$. The image of $e_B = (\mathcal{D}+7)/2$ is an abelian surface B with a polarization of type $(1,7)$ (Section 6). A two-descent over a quintic field L, with $B[2] \simeq \ker\left(\mathrm{Res}_{L/\mathbb{Q}}\,\mu_2 \to \mu_2\right)$ (Proposition 6.5), shows $\mathrm{rank}\, B(\mathbb{Q}) = 1$. The composite $f\colon C \to P \to B$ of an Abel–Jacobi map followed by $1-\tau$ and e_B then puts us in the situation of Chabauty's method on a surface of rank one: the 13-adic logarithms of all points of $f(C(\mathbb{Q}))$ lie on a line, and there is a differential η on C, pulled back from B, whose 13-adic integral vanishes between any two rational points. (Section 1.6 explains the choice of the prime 13.)

The last step is local at 13. At $t = 1$, which corresponds to $Z = 0$, the family H_t degenerates and its local monodromy is a transvection. The line fixed by this transvection is the unique rational point $P_0 \in \mathcal{X}(\mathbb{Q})$ over $t = 1$, and C has two rational points Q_0, Q_1 over P_0, which we call the *cusps*. The line of P_0 carries the same character $\delta\chi_7$ as the line H of a

solution (proof of Lemma 5.9), so the Galois action alone does not distinguish R from the cusps. The splitting of the pure field at 13 forces $13 \mid Z$, so $t \equiv 1 \pmod{13}$, and it forces R to reduce modulo 13 to $\overline{Q_0}$ or $\overline{Q_1}$ (Section 7). With the Abel–Jacobi map based at Q_0, the point $f(Q_1)$ has infinite order in $B(\mathbb{Q})$ (Proposition 6.13), so η is determined by the integrals from Q_0 to Q_1 of the invariant differentials of B, pulled back to C (the *cusp periods*). A computation of the cusp periods modulo 169 determines η modulo 13 and shows that its value at each cusp is a 13-adic unit, so that its integral vanishes to order exactly one there. Hence each residue disc contains no rational point other than the cusp itself (Section 8):

$$C(\mathbb{Q}) \cap \mathrm{red}_{13}^{-1}\{\overline{Q_0}, \overline{Q_1}\} = \{Q_0, Q_1\}.$$

But the cusps have $t = 1$, whereas $t(q(R)) = -X^5/Y^3$, which is not 1 because $X^5 + Y^3 = Z^7$ is nonzero. This contradiction proves Theorem 1.1. Figure 1 shows the objects involved.

$$\begin{array}{ccccc} C & \xrightarrow{(1-\tau)\circ \mathrm{AJ}_{Q_0}} & P & \xrightarrow{\quad e_B \quad} & B \\ {\scriptstyle q}\downarrow{\scriptstyle \deg 2} & & & & \\ \mathcal{X} & \xrightarrow[t]{\deg 50} & \mathbb{P}^1 & & \end{array}$$

FIGURE 1. The construction for the pure fields. The curve $\mathcal{X}$ is the genus-8 curve of k-lines in $J_t[7]$, and C is its genus-15 unramified double cover carrying the point R: the quadratic twist by 5 of the cover of $\mathcal{X}$ by nonzero vectors modulo squares of scalars (Section 5.1). Here P is the 7-dimensional Prym variety, $e_B = (\mathcal{D} + 7)/2$ is the endomorphism of P whose image is the abelian surface B of rank one on which the Chabauty argument is run (Propositions 6.2 and 6.13), and τ is the covering involution. The composite $C \to B$ is the map f of (6.1).

1.6. **Why the method works.** We explain four choices made in the argument for the pure fields.

Why a genus-2 family. The hypothesis $A_\nu \simeq L_a$ is a statement about the seventh-degree algebra A_ν. Its link with geometry is the mod-7 representation of the family J_t. Comparing the factorizations of $\phi(T) - \nu$ and $x^7 - 3^a \cdot 5$ over $\mathbb{Q}_p$ for $p = 2, 3, 5, 7$ shows that $A_\nu \simeq L_a$ forces $30 \mid Z$ and $\gcd(XY, 210) = 1$ (Lemma 4.2). These are the conditions that a modularity and level-lowering argument needs: with them, the twist by δ of the mod-7 representation is unramified outside 3, 5 and 7, finite at 7, and has unipotent inertia at (3) and $(\sqrt{5})$ (Lemma 4.5). Level lowering then compares it with the 1-dimensional space of Hilbert newforms of parallel weight two and level $(3\sqrt{5})$ over K, spanned by the base change of the elliptic curve 15a1. The comparison fails at the prime (2): there the newform has Hecke eigenvalue -3, while $A_\nu \simeq L_a$ forces $2 \mid Z$, so that J_t has multiplicative reduction at (2) and the Frobenius trace of the representation is $\pm(\mathrm{N}(2) + 1) = \pm 5$ modulo 7. So the representation is reducible, and its stable line with character $\delta\chi_7$ gives a rational point on the curve $\mathcal{X}$. After this, the pure fields enter only once more, through their splitting at 13 (Lemma 7.3).

Why a double cover of $\mathcal{X}$ rather than $\mathcal{X}$ itself. Instead of determining the rational points of the genus-8 curve $\mathcal{X}$, we use more of the reducible representation: it gives not just a stable line but a line with the character $\delta\chi_7$, and this extra information lifts the point to

the unramified double cover C (Proposition 5.3). Working on C makes the Prym variety, and with it the surface B of rank one, available.

Why the surface B. Chabauty's method needs an abelian variety of rank less than its dimension. The Prym of $C \to \mathcal{X}$ has dimension 7 and we have no way to bound its rank. But the fibres of $C \to \mathbb{P}^1$ carry the Weil pairing on $J_t[7]$, which the real multiplication turns into a k-bilinear alternating pairing e_k, and whether $e_k(v, w)$ is a square in $k^\times$ does not change when v and w are multiplied by squares. Relating two classes $[v], [w]$ on distinct lines when $e_k(v, w)$ is a nonsquare defines a correspondence on C commuting with the covering involution. It acts on the Prym with square 49, and its $+7$ eigenspace is a surface (Proposition 6.2). A two-descent over the quintic field L that describes the Galois action on $B[2]$ (Proposition 6.5), whose class group and units can be determined unconditionally, shows that $B(\mathbb{Q})$ has rank one (Proposition 6.13), which is less than $\dim B = 2$.

Why 13 *and why modulo* 169. The prime 13 is the smallest prime outside $\{2, 3, 5, 7\}$ that is not a square modulo 7, and C has good reduction there (Lemma 6.12). As $13 \equiv -1 \pmod 7$, $x^7 - 3^a \cdot 5$ has one root in $\mathbb{F}_{13}$ and its other roots in $\mathbb{F}_{169}$, so $L_a \otimes \mathbb{Q}_{13}$ is the product of $\mathbb{Q}_{13}$ and three unramified quadratic extensions of $\mathbb{Q}_{13}$. If $13 \mid Y$, the three roots of $\phi(T) - \nu$ near $T = 1$ would give three factors $\mathbb{Q}_{13}$ or an unramified cubic factor, which the pure field does not have. At a prime $p \equiv 2, 4 \pmod 7$, such as 11, the pure fields have such factors and this step fails. So $t = -X^5/Y^3$ is 13-integral, and if $13 \nmid Z$ then R would reduce to a point of C over a finite value of t other than 1. But 13 happens to be a prime at which C has only ten points modulo 13, two over $t = 1$ and eight over $t = \infty$. So $13 \mid Z$, $t \equiv 1 \pmod{13}$, and the rational point is confined to two residue discs (Lemma 7.3). The annihilating differential η is built from the cusp periods I_1, I_2, and these are divisible by 13 (Lemma 7.8). To know that η has a unit value at the cusps one needs the next 13-adic digit, which is why the computation in the Jacobian in Section 8 is carried out modulo 169.

1.7. **Relation to earlier work.** The family H_t and its Frey representation are due to Pacetti and Villagra Torcomian [43], who treat the signature $(5, p, 3)$ for varying p within Darmon's program [16]. Their theorems on the equation do not cover $p = 7$, so they do not apply to (1.1) directly, but their family, its real multiplication and the properties listed at the start of Section 4 are the starting point of that section. Turning a residual Galois representation with special properties into a rational point on an explicit curve, and then determining the relevant points by descent and Chabauty's method [10, 12], is the strategy of Poonen, Schaefer and Stoll for $x^2 + y^3 = z^7$ [45], where the curves are twists of the Klein quartic $X(7)$, and of Freitas, Naskręcki and Stoll for $x^2 + y^3 = z^p$ [24]. Here the curve parametrizes the k-lines in the 7-torsion of a family of abelian surfaces with real multiplication, and the rational points are controlled on an abelian surface in a Prym variety rather than on a Jacobian. The idea of using a Prym variety as the target of Chabauty's method goes back to Bruin [9]. The main new point of the argument for the pure fields is that the parameter $t = -X^5/Y^3$ of the solution is kept through the whole construction: the rational point on C lies over this value of t, so the behaviour of the solution at 13 decides which residue discs the point can lie in. The argument for the exceptional field is a fifth-power descent of classical type and uses no modular forms. What is new there is the treatment of every possible combination of the valuations of X, Y, Z at 3, 5 and 7.

Independent work. Chocian [11] has proved the same theorem by different methods. For the pure fields he constructs an explicit Fano resolvent, descends to a smooth plane quartic of genus 3 over $\mathbb{Q}(\sqrt{-7})$ and shows that its only points with rational parameter are five points above the branch values. For the exceptional field he combines the modularity and

conductor results of Pacetti and Villagra Torcomian with level lowering over $\mathbb{Q}(\sqrt{5})$ and a Hecke comparison at 29. Apart from the classification of Dahmen–Siksek and Putz, the two proofs have in common only the Frey family of Pacetti and Villagra Torcomian with level lowering over $\mathbb{Q}(\sqrt{5})$, which he uses for the exceptional field and we use for the pure fields.

1.8. **What is assumed, and what is computed.** The proof of Theorem 1.3 relies on the following, and otherwise only on standard results cited where they are used.

(i) The local and global results of Dahmen–Siksek [15] listed in Section 2, which reduce A_ν to a septic field with prescribed local behaviour.

(ii) Putz's enumeration [46] of septic fields with that local behaviour, which yields the list (1.4).

(iii) The results of Pacetti–Villagra Torcomian [43] on the family H_t and its hypergeometric motive (the realization of the motive by J_t, potentially multiplicative reduction at 3 and 5, the congruences with the motives of the elliptic curve E_t of (4.7) modulo $(\sqrt{5})$ and of Darmon's curve C_5^+ modulo 3, and the endomorphism algebra of the generic member), Azon's description [2] of the reduction of Darmon's curves at the prime above 5 and the absence of mixed reduction for abelian varieties with real multiplication (semistable reduction is good or totally toric) [2, Proposition 2.17 and Remark 2.18], two lemmas of Dieulefait–Pacetti [21] on mod-p representations of $G_{\mathbb{Q}}$ whose restriction to $G_{\mathbb{Q}(\zeta_p)}$ is not absolutely irreducible, the modularity theorem of Freitas–Le Hung–Siksek [23], the lifting theorem of Khare–Thorne [33], the level-lowering theorem of Breuil–Diamond [8], and results of Billerey–Chen–Dieulefait–Freitas on the Galois representations of abelian surfaces with real multiplication and their reduction in families [4, Theorems 2.8, 7.1, 7.5 and Lemma 6.9]. All are used in Section 4, where the hypotheses of each are listed at the point of use.

(iv) Explicit computations, carried out with free software (PARI/GP [44], Singular [18] and Python), whose inputs, code and outputs are supplied as supplementary data [31]. Each is stated in the text as a numbered lemma, proposition or theorem, and the data it produces are printed unless they are too large to print, in which case they are in [31]. Table 16 lists these statements, and Appendix E says how each was carried out and which were repeated by separately written programs.

Theorem 1.3 assumes (i) and (ii) as stated. Neither has yet appeared in a refereed journal: [15] is a working paper and [46] is a doctoral thesis. Chocian [11] has reconstructed the arguments by which Dahmen and Siksek exclude the reducible cases (Theorem 2.1(c)–(e)). Among the results in (iii), those of [43] and [2] are recent preprints.

1.9. **Plan of the paper.** Section 2 records the classification inputs and proves Corollary 2.5. Section 3 proves Theorem 1.2. From Section 2 it uses only the prime decompositions (2.5), and it can be read first. Sections 4 to 8 prove Theorem 1.1 in the order sketched above. Section 7 also computes the lattice of integral differentials at 13 that Section 8 uses. Appendices B to D print the data used in Sections 3 and 6 to 8, and Appendix E describes the computations. Table 1 summarizes the argument for the pure fields, and Appendix A is an index of notation.

2. The field classification and its inputs

This section states what we take from Dahmen–Siksek [15] and Putz [46], proves that the polynomial h of (1.4) and the two other polynomials by which the exceptional field has been

Statement	Proved in
$A_\nu \simeq L_a$ forces $J_t[7]$ to be reducible, with a stable line of character $\delta\chi_7$	Proposition 4.9
The stable line gives a point of $\mathcal{X}(\mathbb{Q})$ over $t = -X^5/Y^3$	Proposition 4.12
The point lifts to $R \in C(\mathbb{Q})$ with the same t	Proposition 5.3
$B \subset P$ is an abelian surface with a polarization of type $(1,7)$, and rank $B(\mathbb{Q}) = 1$	Propositions 6.2 and 6.13
R reduces modulo 13 to $\overline{Q_0}$ or $\overline{Q_1}$	Lemma 7.3
The only rational points in the residue discs of $\overline{Q_0}$ and $\overline{Q_1}$ are Q_0 and Q_1	Theorem 8.6

TABLE 1. The steps of the proof of Theorem 1.1.

presented in the literature define the same field, and deduces the reduction (Corollary 2.5) used in the proof of Theorem 1.3.

2.1. **The results of Dahmen and Siksek.** Recall from (1.2)–(1.3) that $\nu = X^5/Z^7$ and $A_\nu = \mathbb{Q}[T]/(\phi(T) - \nu)$. Dahmen and Siksek work with nontrivial primitive solutions of $X^5 + Y^3 = Z^7$ of arbitrary sign, that is, with the solutions of (1.1).

Theorem 2.1 (Dahmen–Siksek)**.** *Let (X, Y, Z) be coprime nonzero integers with $X^5 + Y^3 = Z^7$, and let A_ν be as in (1.3).*

(a) ([15, Proposition 3.3, Corollary 3.4, Propositions 3.5–3.7, Lemma 4.1]) *The étale $\mathbb{Q}_p$-algebra $A_\nu \otimes \mathbb{Q}_p$ is one of those listed in* [15, Corollary 3.4] *for $p = 2$,* [15, Proposition 3.5] *for $p = 7$,* [15, Proposition 3.6] *for $p = 5$ and* [15, Proposition 3.7] *for $p = 3$; for every prime $p \notin \{3, 5, 7\}$ it is unramified* [15, Proposition 3.3 and Corollary 3.4]*, so A_ν is unramified outside $\{3, 5, 7\}$. At infinity, $A_\nu \otimes \mathbb{R} \simeq \mathbb{R} \times \mathbb{C}^3$* [15, Lemma 4.1].

(b) ([15, Lemma 4.1]) *If $A_\nu \simeq \prod_i M_i$ with fields M_i, then the degrees $[M_i : \mathbb{Q}]$ form one of the patterns (7), $(1, 6)$, $(2, 5)$, $(3, 4)$.*

(c) ([15, Proposition 6.1]) *$\phi(T) - \nu$ has no rational root; so the pattern $(1, 6)$ does not occur.*

(d) ([15, Propositions 4.2 and 5.1]) *If the pattern is $(2, 5)$ then the quadratic factor is $\mathbb{Q}(\sqrt{-35})$; and $\phi(T) - \nu$ has no root in $\mathbb{Q}(\sqrt{-35})$. So the pattern $(2, 5)$ does not occur.*

(e) ([15, Propositions 4.3 and 7.1]) *If the pattern is $(3, 4)$ then the cubic factor is $\mathbb{Q}((5^\alpha 7)^{1/3})$ with $\alpha \in \{1, 2\}$ and the quartic factor is $\mathbb{Q}[T]/(T^4 - T^3 + 3T^2 + 3T + 9)$; and this case does not occur.*

Consequently A_ν is a field of degree seven, of signature $(1, 3)$, unramified outside $\{3, 5, 7\}$, whose completions at $2, 3, 5, 7$ lie in the lists of (a).

The signature in (a) can also be seen directly: $\phi'(T) = 105T^4(T - 1)^2 \geq 0$, with equality only at $T = 0, 1$, so ϕ is strictly increasing on $\mathbb{R}$ and $\phi(T) - \nu$ has exactly one real root.

Remark 2.2. Dahmen and Siksek also state [15, Theorem 1] that either $30 \mid Z$ and $7 \nmid XY$, or $2 \nmid Z$, $3 \nmid XYZ$, $5 \nmid YZ$ and $7 \mid Y$. We need only parts of it, and these are proved directly from the local structure of the seven fields: in Lemma 4.2 for the pure fields, and in Proposition 3.4 for the exceptional field.

2.2. **Putz's enumeration.** Dahmen and Siksek [15, §4.3] examined the septic fields of signature $(1, 3)$ unramified outside 3, 5 and 7 in the available number-field database, and found

that their methods eliminate all of them except seven: the six pure fields $L_a = \mathbb{Q}((3^a \cdot 5)^{1/7})$, $1 \le a \le 6$, and the exceptional field F, defined by the polynomial

$$h(x) = x^7 - 2x^6 + 6x^5 + 50x^4 + 35x^3 + 35x + 35. \tag{2.1}$$

They note that the database was not known to be complete for the relevant discriminants. Completeness was established by Putz.

Theorem 2.3 (Putz, [46, Theorem 3.50, pp. 118–119])**.** *Let K' be a number field of degree 7 and signature $(1,3)$. Suppose that $K' \otimes \mathbb{Q}_p$ is isomorphic to one of the étale algebras in* [15, Corollary 3.4 and Propositions 3.5–3.7] *for $p = 2, 3, 5, 7$. Moreover, suppose that K' is unramified outside 3, 5, and 7. Then K' is isomorphic to $\mathbb{Q}(\sqrt[7]{3^a \cdot 5})$ with $a = 1, \dots, 6$, or K' is isomorphic to*

$$\mathbb{Q}[U]/(f_P(U)), \qquad f_P(U) = U^7 - 483U^2 + 3955U - 3945.$$

The statement is quoted from [46, p. 118], with K renamed K', t renamed U and the polynomial named $f_P(U)$ to match Section 2.3. The field $\mathbb{Q}(\sqrt[7]{3^a \cdot 5})$ is L_a. The hypotheses of Theorem 2.3 are the conclusions of Theorem 2.1: the degree is given by (b)–(e), the signature by (a), and the local conditions and the ramification by (a), which cites the same results of [15] as Theorem 2.3. So Theorem 2.3 applies to $K' = A_\nu$. The proof in the thesis is a Hunter search for each of the twelve discriminants $-3^i \cdot 5^j \cdot 7^k$ with $i \in \{2, 4, 6\}$, $j \in \{4, 6\}$ and $k \in \{5, 7\}$, allowed by [15, Lemma 4.1(ii)], followed by a check of the local conditions on the fields found [46, Appendix A.4, Tables A.9 and A.10, pp. 186–187].

2.3. **Three models of the exceptional field.** The exceptional field has been written in three ways: by h in [15], by f_P in [46], and by the polynomial f_b, whose multiple $15f_b$ appears in [15, §4.3]:

$$f_b(b) = b^7 - \tfrac{7}{3}b^6 + \tfrac{7}{5}b^5 - \tfrac{32}{1215}, \qquad \text{so that} \qquad 15f_b(b) = \phi(b) - \tfrac{32}{81}. \tag{2.2}$$

The last identity shows that $\mathbb{Q}[b]/(f_b(b))$ is the algebra A_ν of (1.3) with $\nu = 32/81$. This is how F arises from ϕ.

Lemma 2.4. *The fields $\mathbb{Q}[x]/(h(x))$, $\mathbb{Q}[b]/(f_b(b))$ and $\mathbb{Q}[U]/(f_P(U))$ are isomorphic. Explicitly, if b is a root of f_b then*

$$u(b) = \tfrac{1215}{112}b^6 - \tfrac{2025}{112}b^5 - \tfrac{729}{112}b^4 + \tfrac{171}{8}b^3 - \tfrac{369}{28}b^2 + \tfrac{15}{7}b + \tfrac{12}{7} \tag{2.3}$$

is a root of f_P, and if U is a root of f_P then

$$\begin{aligned} a(U) = &-\tfrac{2133}{2594536}U^6 - \tfrac{499}{370648}U^5 + \tfrac{6183}{2594536}U^4 + \tfrac{52351}{2594536}U^3 \\ &- \tfrac{200901}{2594536}U^2 - \tfrac{29931}{1297268}U - \tfrac{754927}{370648} \end{aligned} \tag{2.4}$$

is a root of h.

Proof. Division with remainder over $\mathbb{Q}$ shows that $f_P(u(b)) \equiv 0 \pmod{f_b(b)}$ and $h(a(U)) \equiv 0 \pmod{f_P(U)}$. Each of h, $1215f_b$ and f_P is irreducible modulo 53, hence irreducible over $\mathbb{Q}$, so each quotient is a field of degree seven. The substitutions (2.3) and (2.4) therefore define nonzero $\mathbb{Q}$-algebra homomorphisms between fields of the same degree, which are isomorphisms. □

By Lemma 2.4 all three polynomials define F. Where a concrete model is needed we use h, as in (1.4). For later reference, F has signature $(1,3)$, discriminant $-3^6 \cdot 5^6 \cdot 7^5$, and

the following decompositions of 2, 3, 5 and 7 into prime ideals, listed as pairs (ramification index, residue degree):

$$\begin{array}{c|l} 2 & (1,1),\ (1,2),\ (1,4) \\ 3 & (1,1),\ (3,2) \\ 5 & (2,1),\ (5,1) \\ 7 & (3,1),\ (4,1). \end{array} \tag{2.5}$$

They follow from Dedekind's criterion, which applies at 2, 3, 5 and 7 because the index of $\mathbb{Z}[x]/(h(x))$ in $\mathcal{O}_F$ is 7229, prime to 210. At 3, 5 and 7 the criterion is applied in Section 3.3, and at 2 it applies to $h \equiv (x+1)(x^2+x+1)(x^4+x+1) \pmod 2$.

2.4. **The reduction.**

Corollary 2.5. *Assume Theorems 2.1 and 2.3. If (X,Y,Z) satisfies (1.1), then A_ν is isomorphic to L_a for some $1 \le a \le 6$, or to F.*

Proof. By Theorem 2.1, A_ν is a field of degree seven satisfying the hypotheses of Theorem 2.3, so it is isomorphic to some L_a or to $\mathbb{Q}[U]/(f_P(U))$, and the latter is F by Lemma 2.4. □

We make two remarks on how Theorems 2.1 and 2.3 are used. First, the isomorphism $A_\nu \simeq F$ or $A_\nu \simeq L_a$ is an isomorphism of abstract fields. It sends the class of T to a root of $\phi(T) - \nu$ in the target field, and in the exceptional case that root is the element ϑ of Section 3.1. The arguments of Sections 3 and 4 use only the existence of such a root, not a particular choice of the isomorphism or a particular value of ν.

Second, the inputs to Theorems 2.1 and 2.3 are of different kinds. The local results of [15], which determine the algebras $A_\nu \otimes \mathbb{Q}_p$ and $A_\nu \otimes \mathbb{R}$, give (a), (b) and the quadratic factor in (d), and they supply the local hypotheses of Theorem 2.3. The cubic and quartic factors in (e) come from a search of the number-field database [15, Proposition 4.3], and the exclusions in (c), (d) and (e) are global computations on curves of genus 2 and 3: a two-cover descent, and Chabauty and Mordell–Weil sieve arguments [15, §§5–7]. Chocian [11, §§3–5] has redone these global computations. The proof of Theorem 2.3 is Putz's enumeration by Hunter searches, described after its statement. We use these results as stated in [15] and [46].

3. The exceptional field

This section proves Theorem 1.2. Throughout, (X,Y,Z) satisfies (1.1) and we assume, for contradiction, that $A_\nu \simeq F$. The signs of X,Y,Z play no role: $-1 = (-1)^5$ is a fifth power, and the enumeration in the proof of Lemma 3.11 runs over all residue classes.

3.1. **The element V and its norm identity.** Fix an isomorphism $A_\nu \simeq F$ and let $\vartheta \in F$ be the image of the class of T. Thus $\phi(\vartheta) = \nu = X^5/Z^7$, and ϑ generates F over $\mathbb{Q}$. Put

$$\beta = 15Z\vartheta, \qquad \Delta = 15Z - \beta = 15Z(1-\vartheta). \tag{3.1}$$

Lemma 3.1. *β and Δ are algebraic integers generating F, with minimal polynomials*

$$C_Z(T) = T^7 - 35ZT^6 + 315Z^2T^5 - 15^6X^5, \tag{3.2}$$

$$D_Z(T) = T^7 - 70ZT^6 + 1890Z^2T^5 - 23625Z^3T^4 + 118125Z^4T^3 - 15^6Y^3. \tag{3.3}$$

Proof. Substituting $T = 15Z\vartheta$ in (3.2) and $T = 15Z(1-\vartheta)$ in (3.3) gives

$$C_Z(\beta) = 15^6 Z^7(\phi(\vartheta) - \nu) = 0, \qquad D_Z(\Delta) = -15^6 Z^7(\phi(\vartheta) - \nu) = 0,$$

where the first equalities are identities of polynomials in ϑ, X, Y, Z once Y^3 is replaced by $Z^7 - X^5$. Both C_Z and D_Z are monic of degree 7 with integer coefficients, and β, Δ generate F because ϑ does. □

Since $[F : \mathbb{Q}] = 7$ is odd, F has no quadratic subfield, so -35 is not a square in F, and $\mathcal{E} = F(\sqrt{-35})$, with $\sqrt{-35}$ a fixed square root of -35, is a field of degree 14. Let σ be its nontrivial automorphism over F. Let ϖ be the class of x in $F = \mathbb{Q}[x]/(h(x))$, so that $h(\varpi) = 0$ and $F = \mathbb{Q}(\varpi)$. The element ϖ, unlike ϑ, is fixed once and for all. Every element of $\mathcal{E}$ can be written uniquely as $A(\varpi) + B(\varpi)\sqrt{-35}$ with $A, B \in \mathbb{Q}[x]$ of degree at most 6, and σ maps it to $A(\varpi) - B(\varpi)\sqrt{-35}$. Put

$$a_+ = \frac{35 + \sqrt{-35}}{2}, \qquad a_- = \frac{35 - \sqrt{-35}}{2} = \sigma(a_+),$$
$$a_+ a_- = \frac{35^2 + 35}{4} = 315. \tag{3.4}$$

Both are roots of $T^2 - 35T + 315$, hence algebraic integers, and over $\mathcal{E}$ the quadratic factor of $C_Z(T) + 15^6 X^5 = T^5(T^2 - 35ZT + 315Z^2)$ splits:

$$\beta^2 - 35Z\beta + 315Z^2 = (\beta - Za_+)(\beta - Za_-).$$

Define

$$V = \beta - Za_+ \in \mathcal{E}, \qquad \text{so that} \qquad \sigma(V) = \beta - Za_-. \tag{3.5}$$

Lemma 3.2. *$\beta \neq 0$, $V \neq 0$, and*

$$V\,\sigma(V) = 15\left(\frac{15X}{\beta}\right)^5,$$
$$\sigma(V) - V = Z\sqrt{-35}, \qquad a_- V - a_+\sigma(V) = -\beta\sqrt{-35}. \tag{3.6}$$

Proof. Since $C_Z(\beta) = 0$, we have $\beta^5(\beta^2 - 35Z\beta + 315Z^2) = 15^6 X^5$. As $X \neq 0$, this gives $\beta \neq 0$ and the first identity. The other two are immediate from (3.5) and (3.4). Finally $V \neq 0$, as otherwise $a_+ = \beta/Z \in F$. □

3.2. **The descent to $\mathcal{E}(S, 5)$.** Let S be the set of primes of $\mathcal{E}$ above 3, 5 and 7, let $\mathcal{O}_{\mathcal{E},S}$ be the ring of S-integers, and let

$$\mathcal{M} = \mathcal{E}(S, 5) = \{c \in \mathcal{E}^\times/\mathcal{E}^{\times 5} \;:\; v_\mathfrak{p}(c) \equiv 0 \pmod 5 \text{ for all primes } \mathfrak{p} \notin S\}. \tag{3.7}$$

Proposition 3.3. *The class $[V]$ of V in $\mathcal{E}^\times/\mathcal{E}^{\times 5}$ lies in $\mathcal{M}$, and*

$$(1 + \sigma)[V] = [V\,\sigma(V)] = [15] \quad \text{in } \mathcal{M}. \tag{3.8}$$

Proof. The elements V and $\sigma(V)$ are integral, as β and a_+ are. Let $\mathfrak{p} \notin S$ be a prime of $\mathcal{E}$ dividing both. By (3.6), $\mathfrak{p} \mid Z\sqrt{-35}$ and $\mathfrak{p} \mid \beta\sqrt{-35}$. As $\sqrt{-35} \cdot \sqrt{-35} = -35$ and $\mathfrak{p} \nmid 35$, we get $\mathfrak{p} \mid Z$ and $\mathfrak{p} \mid \beta$. Then $C_Z(\beta) = 0$ and $\mathfrak{p} \nmid 15$ give $\mathfrak{p} \mid X$, so the rational prime below $\mathfrak{p}$ divides X and Z, contradicting $\gcd(X, Z) = 1$. Hence at most one of $v_\mathfrak{p}(V)$, $v_\mathfrak{p}(\sigma(V))$ is nonzero. Their sum is $v_\mathfrak{p}(15(15X/\beta)^5) \equiv 0 \pmod 5$, so each is divisible by 5. This proves $[V] \in \mathcal{M}$, and (3.8) is (3.6) read modulo fifth powers. □

3.3. **The primes above 3, 5 and 7, and the divisibility of X, Y, Z.** The primes 3, 5 and 7 decompose in $\mathcal{E}$ as follows, with the primes above each listed as pairs (ramification index, residue degree):

$$\begin{array}{c|l} 3 & (1,1),\ (1,1),\ (3,2),\ (3,2) \\ 5 & (2,1),\ (10,1),\ (2,1) \\ 7 & (4,1),\ (4,1),\ (6,1). \end{array} \tag{3.9}$$

This follows from (2.5), as we now show. As $-35 \equiv 1 \pmod 3$ is a square in $\mathbb{Q}_3$, the primes above 3 split. At 5 the prime of F with $e = 2$ splits in $\mathcal{E}$, since its completion contains $\sqrt{-35}$: there $\varpi - 1$ has valuation $1/2$, and in the Taylor expansion of $h(\varpi) = 0$ at 1 the terms $h(1) = 160$ and $456(\varpi - 1)^2$ have valuation 1, while $365(\varpi - 1)$ and the terms of higher degree have larger valuation. So $-35/(\varpi - 1)^2 \equiv 35 \cdot 456/160 = 399/4 \equiv 1$ modulo the maximal ideal. The prime above 5 with $e = 5$ has a single prime of $\mathcal{E}$ above it, with $e = 10$, as $\mathbb{Q}_5(\sqrt{-35})$ and the degree-5 factor have coprime ramification indices. At 7 the prime with $e = 4$ splits: there ϖ has valuation $1/4$, and in $h(\varpi) = 0$ the terms $50\varpi^4$ and 35 have valuation 1 while all others have larger valuation, so $-35/\varpi^4 \equiv 50 \equiv 1$ modulo the maximal ideal. The prime above 7 with $e = 3$ has a single prime of $\mathcal{E}$ above it, with $e = 6$. Thus S has ten elements.

A list $(p, \dots)$ denotes the ideal generated by its entries. The primes of F above 3, 5 and 7 are $(3, \varpi + 1)$, $(3, \varpi^2 + 2\varpi + 2)$, $(5, \varpi - 1)$, $(5, \varpi)$, $(7, \varpi)$ and $(7, \varpi - 3)$, with ramification indices $1, 3, 2, 5, 4, 3$. This follows from the factorizations

$$h \equiv (x+1)(x^2+2x+2)^3 \pmod 3, \quad h \equiv x^5(x-1)^2 \pmod 5,$$
$$h \equiv x^4(x-3)^3 \pmod 7$$

by Dedekind's criterion, which applies because the index of $\mathbb{Z}[\varpi]$ in $\mathcal{O}_F$ is 7229, prime to 105 (the discriminant of h is 7229^2 times that of F). We number the primes of S as follows:

$$\begin{array}{lll} \mathfrak{p}_1 = (3, \varpi + 1, \sqrt{-35} - 1), & e = 1,\ f = 1, & v_{\mathfrak{p}_1}(a_+) = 2; \\ \mathfrak{p}_2 = (3, \varpi + 1, \sqrt{-35} + 1), & e = 1,\ f = 1, & v_{\mathfrak{p}_2}(a_+) = 0; \\ \mathfrak{p}_3 = (3, \varpi^2 + 2\varpi + 2, a_-), & e = 3,\ f = 2, & v_{\mathfrak{p}_3}(a_+) = 0; \\ \mathfrak{p}_4 = (3, \varpi^2 + 2\varpi + 2, a_+), & e = 3,\ f = 2, & v_{\mathfrak{p}_4}(a_+) = 6; \\ \mathfrak{p}_5 \text{ above } (5, \varpi - 1),\ \sqrt{-35} + \varpi - 1 \in \mathfrak{p}_5^2, & e = 2,\ f = 1, & v_{\mathfrak{p}_5}(a_+) = 1; \\ \mathfrak{p}_6 \text{ above } (5, \varpi), & e = 10,\ f = 1, & v_{\mathfrak{p}_6}(a_+) = 5; \\ \mathfrak{p}_7 = \sigma(\mathfrak{p}_5),\ \sqrt{-35} - \varpi + 1 \in \mathfrak{p}_7^2, & e = 2,\ f = 1, & v_{\mathfrak{p}_7}(a_+) = 1; \\ \mathfrak{p}_8 \text{ above } (7, \varpi),\ \sqrt{-35} - \varpi^2 \in \mathfrak{p}_8^3, & e = 4,\ f = 1, & v_{\mathfrak{p}_8}(a_+) = 2; \\ \mathfrak{p}_9 = \sigma(\mathfrak{p}_8),\ \sqrt{-35} + \varpi^2 \in \mathfrak{p}_9^3, & e = 4,\ f = 1, & v_{\mathfrak{p}_9}(a_+) = 2; \\ \mathfrak{p}_{10} \text{ above } (7, \varpi - 3), & e = 6,\ f = 1, & v_{\mathfrak{p}_{10}}(a_+) = 3. \end{array} \tag{3.10}$$

At each of the two primes above $(5, \varpi - 1)$, the element $\varpi - 1$ is a uniformizer and $\sqrt{-35}/(\varpi - 1)$ is a unit with square congruent to 1 (by the computation above). So modulo the square of each of these primes we have $\sqrt{-35} \equiv \pm(\varpi - 1)$, with opposite signs, and $\mathfrak{p}_5$ is the one with the minus sign. Likewise, at each of the two primes above $(7, \varpi)$, the element ϖ is a uniformizer and $\sqrt{-35}/\varpi^2$ is a unit with square congruent to 1, and $\mathfrak{p}_8$ is the one where $\sqrt{-35} \equiv \varpi^2$ modulo the cube. The automorphism σ acts on S by $(\mathfrak{p}_1\,\mathfrak{p}_2)(\mathfrak{p}_3\,\mathfrak{p}_4)(\mathfrak{p}_5\,\mathfrak{p}_7)(\mathfrak{p}_8\,\mathfrak{p}_9)$.

Proposition 3.4. *$2 \nmid Z$, $3 \nmid XYZ$, $5 \nmid YZ$ and $7 \nmid X$.*

Proof. As C_Z is the minimal polynomial of β, which generates F, the irreducible factors of C_Z over $\mathbb{Q}_p$ match the factors of $F \otimes \mathbb{Q}_p$ in (2.5): the factor belonging to the j-th prime of F above p, with ramification index e_j and residue degree f_j, has degree $e_j f_j$, and its roots

all have the same valuation, which lies in $\frac{1}{e_j}\mathbb{Z}$. The same holds for D_Z and Δ. We describe the Newton polygon at p of a polynomial $\sum_i c_i T^i$ by listing its vertices $(i, v_p(c_i))$.

Proof that $2 \nmid Z$. If $2 \mid Z$ then $2 \nmid X$ and

$$C_Z \equiv T^7 - 1 = (T+1)(T^3+T+1)(T^3+T^2+1) \pmod 2$$

is squarefree, so by Hensel's lemma $F \otimes \mathbb{Q}_2$ would have residue degrees $1, 3, 3$, contradicting (2.5).

Proof that $3 \nmid Z$ *and* $5 \nmid Z$. If $v_p(Z) \geq 1$ with $p \in \{3, 5\}$, then $p \nmid X$, and C_Z has vertices $(0, 6)$, $(7, 0)$: one segment of slope $-6/7$, forcing $7 \mid e$, while $e \in \{1, 3\}$ at 3 and $e \in \{2, 5\}$ at 5.

Proof that $3 \nmid X$. If $v_3(X) = 1$ the vertices are $(0, 11)$, $(6, 0)$, $(7, 0)$, and the segment of slope $-11/6$ and length 6 would force a factor of degree 6 with $6 \mid e$, whereas the degree-6 factor at 3 has $e = 3$. If $v_3(X) = m \geq 2$ the vertices are $(0, 6+5m)$, $(5, 2)$, $(6, 0)$, $(7, 0)$. The first segment has slope $-(4+5m)/5$, with denominator 5, and $5 \nmid e$.

Proof that $3 \nmid Y$. If $v_3(Y) = m \geq 1$ then $3 \nmid XZ$, and D_Z has vertices $(0, 6+3m)$, $(3, 3)$, $(6, 0)$, $(7, 0)$, with segments of lengths $3, 3, 1$ and slopes $-(1+m)$, -1, 0. The six roots of the degree-6 factor of D_Z over $\mathbb{Q}_3$ must share a valuation, but no six roots do.

Proof that $5 \nmid Y$. If $v_5(Y) = m \geq 1$ the vertices of D_Z are $(0, 6+3m)$, $(3, 4)$, $(5, 1)$, $(7, 0)$. The first segment has slope $-(2+3m)/3$ with denominator 3, and $3 \nmid e$.

Proof that $7 \nmid X$. If $v_7(X) = m \geq 1$ the vertices of C_Z are $(0, 5m)$, $(5, 1)$, $(7, 0)$. The first segment has slope $-(5m-1)/5$ with denominator 5, while $e \in \{3, 4\}$ at 7. □

Remark 3.5. Proposition 3.4 is the second alternative of the statement recalled in Remark 2.2, with $7 \mid Y$ replaced by the weaker condition $7 \nmid X$, proved here from the local structure of F.

3.4. The valuations of V at S.

Proposition 3.6. *With the numbering* (3.10),

$$\big(v_{\mathfrak{p}_i}(V) \bmod 5\big)_{i=1}^{10} = v_0 = (0, 1, 0, 3, 1, 0, 1, 0, 0, 0). \tag{3.11}$$

Proof. The valuations of the roots of C_Z over $\mathbb{Q}_p$ are normalized by $v_p(p) = 1$, and at a prime $\mathfrak{p}_i$ we write v for $v_{\mathfrak{p}_i}$, so that $v = e\, v_p$ with e as in (3.10).

At 3. By Proposition 3.4, $3 \nmid XZ$, so C_Z has vertices $(0, 6)$, $(6, 0)$, $(7, 0)$ at 3: six roots of valuation 1 and one unit root, the root in the degree-1 factor. So β is a unit at $\mathfrak{p}_1, \mathfrak{p}_2$, and $v(\beta) = 3$ at $\mathfrak{p}_3, \mathfrak{p}_4$. By (3.10), at $\mathfrak{p}_1$ we have $v(\beta) = 0 < 2 = v(Za_+)$, so $v(V) = 0$. At $\mathfrak{p}_3$, $v(\beta) = 3 > 0 = v(Za_+)$, so $v(V) = 0$, and at $\mathfrak{p}_4$, $v(\beta) = 3 < 6 = v(Za_+)$, so $v(V) = 3$. At $\mathfrak{p}_2$ both terms of V are units, and by (3.6)

$$v_{\mathfrak{p}_2}(V) + v_{\mathfrak{p}_2}(\sigma(V)) = v_{\mathfrak{p}_2}(15(15X/\beta)^5) = 1 + 5 = 6,$$

where $v_{\mathfrak{p}_2}(\sigma(V)) = v_{\mathfrak{p}_1}(V) = 0$. Hence $v_{\mathfrak{p}_2}(V) = 6 \equiv 1$.

At 5. Let $m = v_5(X) \geq 0$. By Proposition 3.4, $5 \nmid YZ$, so C_Z has vertices $(0, 6+5m)$, $(5, 1)$, $(7, 0)$ at 5: five roots of valuation $1+m$ (the degree-5 factor) and two of valuation $1/2$ (the degree-2 factor). At $\mathfrak{p}_6$ ($e = 10$), σ fixes $\mathfrak{p}_6$ and $v(a_+a_-) = v(315) = 10$, so $v(a_+) = v(a_-) = 5$. As $v(\beta) = 10(m+1) > 5$, we get $v(V) = 5 \equiv 0$. At $\mathfrak{p}_5$ and $\mathfrak{p}_7$ ($e = 2$, swapped by σ), let $v = v_{\mathfrak{p}_5}$. Then $v(\beta) = 1$, and by (3.6)

$$v(V) + v(\sigma(V)) = v\big(15(15X/\beta)^5\big) = 2 + 5(2 + 2m - 1) = 7 + 10m,$$

while $v(\sigma(V) - V) = v(Z\sqrt{-35}) = 1$. The sum is odd, so the two valuations differ, and the smaller one equals $v(\sigma(V) - V) = 1$. Hence $\{v_{\mathfrak{p}_5}(V), v_{\mathfrak{p}_7}(V)\} = \{v(V), v(\sigma(V))\} = \{1, 6+10m\}$, and both are $\equiv 1 \pmod 5$.

At 7. By Proposition 3.4, $7 \nmid X$, so the constant term of C_Z is a 7-adic unit and its other nonleading coefficients are divisible by 7. So every root is a unit, and β, hence $V\sigma(V) = 15(15X/\beta)^5$, is a unit at $\mathfrak{p}_8, \mathfrak{p}_9, \mathfrak{p}_{10}$. As V and $\sigma(V)$ are integral, both are units. □

3.5. The group $\mathcal{M}$ and the possible classes of V.

Lemma 3.7. $\dim_{\mathbb{F}_5} \mathcal{M} = 16$.

Proof. If $[c] \in \mathcal{M}$, then $c\mathcal{O}_{\mathcal{E},S} = \mathfrak{a}_c^5$ with $\mathfrak{a}_c = \prod_{\mathfrak{p}\notin S} \mathfrak{p}^{v_\mathfrak{p}(c)/5}$. The map sending $[c]$ to $[\mathfrak{a}_c]$ is well defined and surjective onto $\mathrm{Cl}(\mathcal{O}_{\mathcal{E},S})[5]$, and its kernel consists of the classes of S-units: if $\mathfrak{a}_c = w\mathcal{O}_{\mathcal{E},S}$ with $w \in \mathcal{E}^\times$, then $cw^{-5} \in \mathcal{O}_{\mathcal{E},S}^\times$. An S-unit that is a fifth power in $\mathcal{E}^\times$ is the fifth power of an S-unit. So there is an exact sequence

$$0 \longrightarrow \mathcal{O}_{\mathcal{E},S}^\times/\mathcal{O}_{\mathcal{E},S}^{\times 5} \longrightarrow \mathcal{M} \longrightarrow \mathrm{Cl}(\mathcal{O}_{\mathcal{E},S})[5] \longrightarrow 0.$$

A class-group computation for $\mathcal{E}$ [44] gives the group $\mathbb{Z}/2\mathbb{Z}$ under the generalized Riemann hypothesis, and an unconditional certificate shows that $\mathrm{Cl}(\mathcal{E})$ is a quotient of this group (Appendix E.5). Hence $\mathrm{Cl}(\mathcal{E})$ has order dividing 2, and $\mathrm{Cl}(\mathcal{O}_{\mathcal{E},S})$, a quotient of $\mathrm{Cl}(\mathcal{E})$, has no 5-torsion. As $\mathcal{E}$ has signature $(0, 7)$, its unit rank is 6, and adjoining the ten primes of S gives S-unit rank 16. As $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ does not divide 14, $\mathcal{E}$ contains no primitive fifth root of unity, so the torsion of $\mathcal{O}_{\mathcal{E},S}^\times$ has order prime to 5 and $\mathcal{O}_{\mathcal{E},S}^\times/\mathcal{O}_{\mathcal{E},S}^{\times 5} \simeq \mathbb{F}_5^{16}$. Therefore $\dim_{\mathbb{F}_5} \mathcal{M} = 16$. □

We use the S-units $g_j = (A_j(\varpi) + B_j(\varpi)\sqrt{-35})/506030$, $1 \le j \le 16$, of Table 5, with $A_j, B_j \in \mathbb{Z}[x]$ of degree at most 6. Appendix B lists them and explains the denominator.

Lemma 3.8. *The classes of $g_1, \dots, g_{16}$ form a basis of $\mathcal{M}$. With respect to this basis:*

(i) *the matrix $S_\sigma \in M_{16}(\mathbb{F}_5)$ of σ, whose column j holds the coordinates of $[\sigma g_j]$, is*

$$S_\sigma = \begin{pmatrix}
4&0&0&0&4&4&4&4&4&4&0&0&0&0&0&0\\
2&1&0&0&1&1&1&1&1&1&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
1&1&1&1&2&1&2&1&1&0&4&0&0&0&0&1\\
0&0&4&0&0&0&4&4&0&1&0&0&1&0&0&0\\
0&0&0&1&1&0&0&0&1&4&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&4&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{pmatrix}; \tag{3.12}$$

(ii) *the matrix* $\mathrm{Val} \in M_{10\times 16}(\mathbb{F}_5)$ *of the map* $[c] \mapsto (v_{\mathfrak{p}_i}(c) \bmod 5)_{i=1}^{10}$, *with the numbering* (3.10), *is*

$$\mathrm{Val} = \begin{pmatrix}
2&1&0&0&1&1&1&1&1&1&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0
\end{pmatrix}; \tag{3.13}$$

(iii) *the coordinate vector of* [15] *is*

$$e_{15} = (3, 1, 3, 3, 2, 0, 2, 0, 0, 0, 0, 3, 3, 0, 0, 2). \tag{3.14}$$

Proof. Each g_j is an S-unit: its characteristic polynomial over $\mathbb{Q}$ has integer coefficients, so $g_j \in \mathcal{O}_\mathcal{E}$, and its norm is 1, 9, 15 or 21, so every prime ideal dividing $g_j\mathcal{O}_\mathcal{E}$ lies above 3, 5 or 7. Its valuations at $\mathfrak{p}_1, \dots, \mathfrak{p}_{10}$ give the ideals in Table 5, from which Val is read off. Let $J\colon \mathcal{M} \to \mathbb{F}_5^{18}$ be the map whose coordinates are the valuations modulo 5 at the ten primes of S and the characters defined as in (3.17) of Section 3.6 at the six primes of $\mathcal{E}$ above 11 and at the two primes of $\mathcal{E}$ of residue degree 4 above 2. These two lie above the prime $(2, \varpi^4 + \varpi + 1)$ of F, and all eight primes have residue fields of order $\equiv 1 \pmod 5$. The 18×16 matrix $J(g_1, \dots, g_{16})$ has rank 16. Hence the g_j are independent in $\mathcal{M}$, by Lemma 3.7 they form a basis, and J is injective on $\mathcal{M}$. (The characters at the two primes above 2 are not printed. By the paragraph after (3.19), the printed matrices Val, L_{11} and L_{19} also give an injective map on $\mathcal{M}$, which can replace J in this proof.) The columns of the matrix S_σ and the vector e_{15} are obtained by evaluating J on $\sigma(g_j) = (A_j(\varpi) - B_j(\varpi)\sqrt{-35})/506030$ and on 15, and solving the resulting linear systems. Injectivity of J makes the solutions unique. Changing the primitive fifth roots of unity that define the eight characters multiplies rows of J by nonzero scalars, which changes neither the rank nor these solutions. □

Theorem 3.9. *Let $c \in \mathbb{F}_5^{16}$ be the coordinate vector of $[V]$ in the basis $g_1, \dots, g_{16}$. Then*

$$(I + S_\sigma)\, c = e_{15} \qquad \text{and} \qquad \mathrm{Val} \cdot c = v_0, \tag{3.15}$$

and the set $\mathcal{A}$ of solutions of (3.15) has exactly 125 elements, namely

$$c(\alpha, \gamma, \rho) = (1, 1, 0, 3, 1, 0, 1, 0, 0, 0,\ \alpha,\ \gamma,\ 4 - \gamma,\ \rho,\ -\rho,\ 1), \qquad \alpha, \gamma, \rho \in \mathbb{F}_5. \tag{3.16}$$

Proof. The first condition is (3.8) in coordinates and the second is Proposition 3.6. The 26×16 matrix stacking $I + S_\sigma$ over Val has rank 13 over $\mathbb{F}_5$, so the solution set, if nonempty, is a coset of a 3-dimensional space and has 125 elements. Direct multiplication shows that (3.16) satisfies (3.15) for all α, γ, ρ. □

Remark 3.10. That $\mathcal{A}$ is a coset of a space of dimension 3 has an intrinsic explanation. Each $\mathfrak{p}_i^2$ is principal, as $\mathrm{Cl}(\mathcal{E})$ has order dividing 2 (see the proof of Lemma 3.7), so Val is surjective and its kernel is the image of $\mathcal{O}_\mathcal{E}^\times/\mathcal{O}_\mathcal{E}^{\times 5}$, of dimension 6. The norm $\mathcal{E} \to F$ induces a map of that space onto $\mathcal{O}_F^\times/\mathcal{O}_F^{\times 5}$, which has dimension 3 because F has signature $(1, 3)$. The map is onto because the composite $\mathcal{O}_F^\times \to \mathcal{O}_\mathcal{E}^\times \to \mathcal{O}_F^\times$ is squaring, which is invertible modulo 5. So the homogeneous system $(I + S_\sigma)c = 0$, $\mathrm{Val}\, c = 0$ has a 3-dimensional solution space, in agreement with the rank computation.

3.6. **Fifth-power residues at 11 and 19.** Let $p \in \{11, 19\}$; it is unramified in $\mathcal{E}$. Modulo p, h factors into irreducibles as

$$h \equiv (x + 3)(x^2 + 3x + 9)(x^4 + 3x^3 + 3x^2 + 6x + 7) \pmod{11},$$
$$h \equiv (x - 5)(x^2 + 2x + 2)(x^2 + 4x + 5)(x^2 - 3x + 5) \pmod{19}.$$

So the residue degrees of F above 11 and 19 are $1, 2, 4$ and $1, 2, 2, 2$. As -35 is a square modulo 11 and a nonsquare modulo 19, those of $\mathcal{E}$ are $1, 1, 2, 2, 4, 4$ and $2, 2, 2, 2, 2, 2, 2$, and every prime $\mathfrak{q}$ of $\mathcal{E}$ above p has residue field $\ell_\mathfrak{q}$ of order $\equiv 1 \pmod 5$. In this subsection $\mathfrak{p}$ denotes a prime of F and $\mathfrak{q}$ a prime of $\mathcal{E}$. Every $\mathfrak{q}$ above p except $(19, \varpi - 5)$ is $(p,\ h_\mathfrak{p}(\varpi),\ \sqrt{-35} - s_\mathfrak{q}(\varpi))$, where $h_\mathfrak{p}$ is the irreducible factor of h modulo p attached to the prime $\mathfrak{p} = (p, h_\mathfrak{p}(\varpi))$ below

$\mathfrak{q}$, and $s_\mathfrak{q} \in \mathbb{Z}[x]$ reduces to a square root of -35 in $\mathbb{F}_p[x]/(h_\mathfrak{p})$. Then $\ell_\mathfrak{q} = \mathbb{F}_p[x]/(h_\mathfrak{p})$, with $\varpi \mapsto x$ and $\sqrt{-35} \mapsto s_\mathfrak{q}(x)$. The prime $(19, \varpi - 5)$ is inert in $\mathcal{E}/F$, with residue field $\mathbb{F}_{19}(\sqrt{-35}) \simeq \mathbb{F}_{361}$ and $\varpi \mapsto 5$. For $p = 19$ every residue field is generated over $\mathbb{F}_{19}$ by the residue of $\sqrt{-35}$, and in each of them the four primitive fifth roots of unity are the residues of $2 \pm \sqrt{-35}$ and $7 \pm 4\sqrt{-35}$. Table 2 lists the primes above 11 and 19, each with a chosen primitive fifth root of unity $\zeta_\mathfrak{q} \in \ell_\mathfrak{q}^\times$, which is $2^{(\#\ell_\mathfrak{q}-1)/5}$ for $\mathfrak{q} \mid 11$.

p	row	$\mathfrak{q}$	$\#\ell_\mathfrak{q}$	$\zeta_\mathfrak{q} \bmod \mathfrak{q}$
11	1	$(11,\ \varpi + 3,\ \sqrt{-35} + 3)$	11	4
	2	$(11,\ \varpi + 3,\ \sqrt{-35} - 3)$	11	4
	3	$(11,\ \varpi^2 + 3\varpi + 9,\ \sqrt{-35} - 3)$	11^2	5
	4	$(11,\ \varpi^2 + 3\varpi + 9,\ \sqrt{-35} + 3)$	11^2	5
	5	$(11,\ \varpi^4 + 3\varpi^3 + 3\varpi^2 + 6\varpi + 7,\ \sqrt{-35} + 3)$	11^4	3
	6	$(11,\ \varpi^4 + 3\varpi^3 + 3\varpi^2 + 6\varpi + 7,\ \sqrt{-35} - 3)$	11^4	3
19	1	$(19,\ \varpi^2 + 4\varpi + 5,\ \sqrt{-35} + 4\varpi + 8)$	19^2	$7 - 4\sqrt{-35}$
	2	$(19,\ \varpi^2 + 4\varpi + 5,\ \sqrt{-35} - 4\varpi - 8)$	19^2	$2 - \sqrt{-35}$
	3	$(19,\ \varpi^2 + 2\varpi + 2,\ \sqrt{-35} - 4\varpi - 4)$	19^2	$7 + 4\sqrt{-35}$
	4	$(19,\ \varpi^2 - 3\varpi + 5,\ \sqrt{-35} - 7\varpi + 1)$	19^2	$2 + \sqrt{-35}$
	5	$(19,\ \varpi - 5)$	19^2	$7 + 4\sqrt{-35}$
	6	$(19,\ \varpi^2 - 3\varpi + 5,\ \sqrt{-35} + 7\varpi - 1)$	19^2	$7 + 4\sqrt{-35}$
	7	$(19,\ \varpi^2 + 2\varpi + 2,\ \sqrt{-35} + 4\varpi + 4)$	19^2	$7 + 4\sqrt{-35}$

TABLE 2. The primes $\mathfrak{q}$ of $\mathcal{E}$ above 11 and 19, in the order of the rows of L_{11} and L_{19}, with the primitive fifth roots of unity $\zeta_\mathfrak{q} \in \ell_\mathfrak{q}^\times$ used in (3.17).

Define

$$\lambda_\mathfrak{q} \colon \mathcal{E}^\times \to \mathbb{F}_5, \qquad \lambda_\mathfrak{q}(a) = \log_{\zeta_\mathfrak{q}} \Big(\big(p^{-v_\mathfrak{q}(a)} a\big)^{(\#\ell_\mathfrak{q}-1)/5} \bmod \mathfrak{q} \Big). \tag{3.17}$$

Since p is a uniformizer at $\mathfrak{q}$, this is a homomorphism killing fifth powers, hence defined on $\mathcal{M}$. Let L_p be the matrix of these homomorphisms on the basis $g_1, \dots, g_{16}$, with rows in the order of Table 2, so that $(L_p)_{\mathfrak{q},j} = \lambda_\mathfrak{q}(g_j)$:

$$L_{11} = \begin{pmatrix} 0 & 4 & 3 & 3 & 3 & 4 & 1 & 0 & 2 & 1 & 0 & 2 & 3 & 0 & 1 & 1 \\ 3 & 4 & 1 & 1 & 3 & 3 & 0 & 4 & 2 & 3 & 0 & 3 & 2 & 1 & 0 & 1 \\ 4 & 2 & 4 & 2 & 3 & 4 & 3 & 3 & 1 & 4 & 1 & 2 & 1 & 3 & 2 & 2 \\ 1 & 3 & 1 & 1 & 4 & 3 & 1 & 3 & 3 & 4 & 4 & 1 & 2 & 2 & 3 & 3 \\ 1 & 2 & 0 & 4 & 1 & 0 & 3 & 2 & 4 & 0 & 3 & 4 & 2 & 4 & 2 & 2 \\ 1 & 0 & 3 & 0 & 2 & 4 & 4 & 4 & 3 & 0 & 2 & 2 & 4 & 2 & 4 & 0 \end{pmatrix}, \tag{3.18}$$

$$L_{19} = \begin{pmatrix} 2 & 2 & 3 & 1 & 2 & 3 & 1 & 1 & 1 & 4 & 0 & 3 & 4 & 0 & 4 & 4 \\ 1 & 1 & 4 & 1 & 0 & 4 & 2 & 4 & 0 & 2 & 0 & 2 & 4 & 2 & 0 & 2 \\ 2 & 4 & 0 & 0 & 4 & 0 & 1 & 2 & 3 & 2 & 1 & 2 & 2 & 2 & 3 & 4 \\ 2 & 4 & 1 & 1 & 2 & 0 & 3 & 4 & 2 & 0 & 4 & 0 & 2 & 4 & 4 & 4 \\ 1 & 3 & 4 & 2 & 0 & 2 & 0 & 3 & 1 & 2 & 4 & 0 & 0 & 2 & 3 & 3 \\ 0 & 1 & 0 & 4 & 0 & 2 & 4 & 1 & 4 & 0 & 2 & 4 & 0 & 3 & 3 & 1 \\ 3 & 0 & 1 & 2 & 3 & 2 & 4 & 1 & 3 & 2 & 1 & 3 & 3 & 2 & 3 & 0 \end{pmatrix}. \tag{3.19}$$

The 23×16 matrix stacking the matrices Val, L_{11} and L_{19} has rank 16. So the valuations modulo 5 at the ten primes of S and the thirteen characters $\lambda_\mathfrak{q}$ give an injective map $\mathcal{M} \to \mathbb{F}_5^{23}$, and each class $[g_j]$ is determined by its image, the j-th column of this matrix.

For $c = c(\alpha, \gamma, \rho)$ as in (3.16), multiplying out gives

$$L_{11}\, c = \big(-\gamma - \rho,\ 2 + \gamma + \rho,\ 4 + \alpha + \gamma + \rho,\ 3 - \alpha - \gamma - \rho, \tag{3.20}$$
$$4 + 3\alpha + 2\gamma + 2\rho,\ 3 + 2\alpha + 3\gamma + 3\rho\big),$$
$$L_{19}\, c = \big(-\gamma + \rho,\ 3\gamma + 2\rho,\ 3 + \alpha - \rho,\ 1 - \alpha + 3\gamma, \tag{3.21}$$
$$3 - \alpha - \rho,\ 3 + 2\alpha - \gamma,\ 3 + \alpha - \rho\big).$$

Lemma 3.11. *For $p \in \{11, 19\}$ the vector $\big(\lambda_{\mathfrak{q}}(V)\big)_{\mathfrak{q}|p}$, with the rows of L_p in the same order, agrees, at every coordinate not marked $*$, with one of the following patterns: for $p = 11$ (fifteen patterns),*

$$\begin{array}{llllllll} (0,0,3,2,4,1), & (0,2,0,2,2,0), & (0,3,1,2,1,2), & (1,1,4,3,0,2), \\ (1,3,1,3,3,1), & (1,4,2,3,2,3), & (2,0,3,4,3,4), & (2,2,0,4,1,3), \\ (2,4,2,4,4,2), & (3,0,3,0,0,3), & (3,1,4,0,4,0), & (3,3,1,0,2,4), \\ (4,1,4,1,1,4), & (4,2,0,1,0,1), & (4,4,2,1,3,0); & \end{array} \tag{3.22}$$

and for $p = 19$ (twelve patterns),

$$\begin{array}{llllllll} (*,0,2,4,2,2,2), & (0,*,2,4,2,2,2), & (1,2,1,2,3,1,1), \\ (1,2,3,1,0,3,3), & (2,4,3,3,0,4,3), & (2,4,4,1,0,3,4), \\ (3,1,*,4,2,2,0), & (3,1,0,4,2,2,*), & (3,1,2,*,2,0,2), \\ (3,1,2,0,2,*,2), & (4,3,1,3,3,4,1), & (4,3,4,2,3,1,4). \end{array} \tag{3.23}$$

Proof. Write z and n for the residues of Z and X^5 modulo p. At $\mathfrak{q}$, $V = \beta - Za_+$ has residue $\bar\beta - z\bar a_+$, where $\bar a_+$ is computed from the residue of $\sqrt{-35}$ given by the generators of $\mathfrak{q}$ in Table 2, and $\bar\beta = \bar\beta_{\mathfrak{p}}$ is the residue of β in the residue field $k_{\mathfrak{p}} = \mathbb{F}_p[x]/(h_{\mathfrak{p}}) \subseteq \ell_{\mathfrak{q}}$ of the prime $\mathfrak{p}$ below $\mathfrak{q}$. If V is a unit at $\mathfrak{q}$, then $\lambda_{\mathfrak{q}}(V)$ is the logarithm to base $\zeta_{\mathfrak{q}}$ of the fifth-power residue symbol of $\bar\beta - z\bar a_+$. If $V \equiv 0 \pmod{\mathfrak{q}}$, the coordinate is unconstrained, which is what $*$ records. So it suffices to enumerate, in each of the four cases $p \nmid XYZ$, $p \mid Z$, $p \mid X$ and $p \mid Y$, which we call the valuation strata at p, the possible families $(\bar\beta_{\mathfrak{p}})_{\mathfrak{p}|p}$, with the same $\bar\beta_{\mathfrak{p}}$ at every prime of $\mathcal{E}$ above $\mathfrak{p}$.

The stratum $p \nmid XYZ$. Then $\bar\beta_{\mathfrak{p}}$ is a root of

$$\bar C(T) = T^7 - 35zT^6 + 315z^2T^5 - 15^6 n, \qquad z, n \neq 0.$$

The polynomial $\bar C$ is separable, since $\bar C' = 7T^4(T - 15z)^2$ and a common root would force $n = 0$ or $n = z^7$, and $n = z^7$ means $p \mid Y$. As $F \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p[T]/(C_Z)$, Hensel's lemma matches the primes $\mathfrak{p} \mid p$ of F with the irreducible factors of $\bar C$ over $\mathbb{F}_p$, the factor matched with $\mathfrak{p}$ being the minimal polynomial of $\bar\beta_{\mathfrak{p}}$, of degree $f(\mathfrak{p})$. We enumerate all (z, n) and all families of roots $\bar\beta_{\mathfrak{p}}$ of $\bar C$ of degree $f(\mathfrak{p})$ with pairwise distinct minimal polynomials.

The stratum $p \mid Z$. Then $\bar C = T^7 - 15^6 n$ is separable and $\bar V = \bar\beta$. The enumeration is as before, with $z = 0$.

The stratum $p \mid X$. Write $v_p(X) = m \geq 1$, $X = p^m X_0$ and $\beta = p^m U$. Dividing $C_Z(p^m U)$ by p^{5m} shows that five roots of C_Z have $\bar\beta = 0$, with $\bar U$ a root of $315z^2U^5 - 15^6 X_0^5$, and that the other two reduce to the roots $z\bar a_+$ and $z\bar a_-$ of $T^2 - 35zT + 315z^2$. We call these five roots the small cluster and the other two the large cluster. For a root in the small cluster $\bar V = -z\bar a_+$, which is nonzero as $p \nmid 315Z$, so V is a unit at the corresponding primes. For a root in the large cluster $V \equiv 0$, giving a $*$, or $V \equiv -Z\sqrt{-35} \pmod{\mathfrak{q}}$. This is the only stratum on which V can fail to be a unit at a prime above p.

The stratum $p \mid Y$. Write $v_p(Y) = m \geq 1$, $Y = p^m Y_0$ and $\Delta = p^m U$. Dividing $D_Z(p^m U)$ by p^{3m} shows that three roots have $\bar{\Delta} = 0$, that is, $\bar{\beta} = 15z$, with $\bar{U}$ a root of $118125z^4U^3 - 15^6 Y_0^3$. These three roots form the small cluster and the other four the large cluster. The roots in the large cluster reduce to the roots of $\bar{C}(T)/(T-15z)^3$, where now $n = z^7$, and after the substitution $T = 15zs$ this polynomial is a nonzero constant multiple of $15s^4 + 10s^3 + 6s^2 + 3s + 1$. This quartic has discriminant $3^3 \cdot 5^2 \cdot 7^3$, so it is separable modulo p, and it takes the value $35 \neq 0$ at $s = 1$.

In every case the residual polynomial of each cluster is separable, so each residue lifts to a unique root in the corresponding unramified completion, and the clusters are disjoint with total degree 7. Hence the enumeration covers every solution and every $m \geq 1$. On the strata $p \mid X$ and $p \mid Y$ the primes of F above p are matched as before with the irreducible factors over $\mathbb{F}_p$ of the residual polynomials of the two clusters. A prime matched with the small cluster has $\bar{\beta}_{\mathfrak{p}} = 0$ if $p \mid X$ and $\bar{\beta}_{\mathfrak{p}} = 15z$ if $p \mid Y$, and one matched with the large cluster has $\bar{\beta}_{\mathfrak{p}}$ a root of degree $f(\mathfrak{p})$ of $T^2 - 35zT + 315z^2$, respectively of $\bar{C}(T)/(T-15z)^3$, with pairwise distinct minimal polynomials. As the stratum, the residues z, n, X_0, Y_0 and such families vary, the vectors $(\lambda_{\mathfrak{q}}(V))_{\mathfrak{q}|p}$ run through the list (3.22) for $p = 11$ and the list (3.23) for $p = 19$. At $p = 11$ all fifteen patterns come from the stratum $p \nmid XYZ$, and at $p = 19$ six come from $p \nmid XYZ$ and the six with a $*$ from $p \mid X$. On the other strata the degrees of the irreducible factors of the residual polynomials cannot match the residue degrees of F at p. If $p \mid Z$, then $\bar{C}(T) = T^7 - 15^6 n$ has factors of degrees $1, 3, 3$ at 11 and $1, 6$ at 19. If $11 \mid X$, the large cluster gives degrees $1, 1$ and the small one $1, 1, 1, 1, 1$ or 5. If $p \mid Y$, the small cluster gives $1, 2$ at 11 and $1, 1, 1$ or 3 at 19, while the quartic factors with degrees $1, 1, 2$ modulo 11 and is irreducible modulo 19. (If one also uses that $n = X^5 \bmod p$ is a fifth power and that $z^7 - n = Y^3 \bmod p$ is a cube, with the analogous conditions on the other strata, the list at $p = 11$ reduces to $(0, 2, 0, 2, 2, 0)$, $(1, 1, 4, 3, 0, 2)$, $(2, 0, 3, 4, 3, 4)$, and the list at $p = 19$ does not change.) □

3.7. **The contradiction.**

Proposition 3.12. *For no $c = c(\alpha, \gamma, \rho) \in \mathcal{A}$ do both $L_{11}\, c$ and $L_{19}\, c$ agree, at every coordinate not marked $*$, with a pattern in* (3.22)*, respectively* (3.23)*.*

Proof. At 11. In (3.20) the first two coordinates sum to 2, and the first and third sum to $4 + \alpha$. Exactly three of the fifteen patterns in (3.22) have first two coordinates summing to 2, namely

$$(0, 2, 0, 2, 2, 0), \qquad (1, 1, 4, 3, 0, 2), \qquad (2, 0, 3, 4, 3, 4),$$

and in each of them the first and third coordinates sum to 0. Hence $\alpha = 1$.

At 19. Let x_i be the i-th coordinate of (3.21). Then $x_3 = x_7$ and $x_3 - x_5 = 2\alpha$, so $\alpha = 3(x_3 - x_5)$. Every pattern in (3.23) specifies x_5 and at least one of x_3, x_7. Reading these off, the twelve patterns force $\alpha = 0, 0, 4, 4, 4, 2, 4, 4, 0, 0, 4, 3$, respectively, and in particular $\alpha \neq 1$. The two conclusions are incompatible. □

Proof of Theorem 1.2. Suppose $A_\nu \simeq F$ and construct V as in Section 3.1. By Propositions 3.3 and 3.6 and Theorem 3.9, the class of V in $\mathcal{M}$ has coordinates $c(\alpha, \gamma, \rho)$ for some $\alpha, \gamma, \rho \in \mathbb{F}_5$, and by Lemma 3.11 the vectors $L_{11}\, c = (\lambda_{\mathfrak{q}}(V))_{\mathfrak{q}|11}$ and $L_{19}\, c = (\lambda_{\mathfrak{q}}(V))_{\mathfrak{q}|19}$ agree with one pattern in each list at every coordinate not marked $*$. Proposition 3.12 excludes this. □

Remark 3.13. All finite data needed in this section are printed: the primes in (3.10) and Table 2, the S-units of Table 5, the matrices S_σ, Val, L_{11}, L_{19}, the vector e_{15} and the pattern

lists. The deductions from the matrices and lists (Theorem 3.9 and Proposition 3.12) are linear algebra over $\mathbb{F}_5$. The primes of $\mathcal{E}$ of residue degree 4 above 2 and 13 do not suffice in place of those above 11 and 19: the constraints that the enumeration in the proof of Lemma 3.11 gives at them are satisfied by all 125, respectively 100, classes of $\mathcal{A}$.

4. The Frey family and the curve $\mathcal{X}$

From here to the end of Section 8 we assume that (X, Y, Z) satisfies (1.1) and that $A_\nu \simeq L_a$ for some $1 \le a \le 6$, and we work towards a contradiction. We attach to the solution a genus-2 Frey curve with real multiplication, show that the mod-7 representation of its Jacobian is reducible with prescribed characters (Proposition 4.9), and obtain a rational point on a fixed curve $\mathcal{X}$ of genus 8 (Proposition 4.12). Proposition 4.9 rests on a modularity argument (Propositions 4.4 and 4.6), and the hypotheses of each cited theorem are checked where it is applied.

Results used from preprints. Besides published theorems, the proof of Theorem 1.1 uses, in this section only, the following statements from recent preprints. In these statements, J_t is the Jacobian of the curve H_t of (4.2) over $K = \mathbb{Q}(\sqrt{5})$, E_t is the elliptic curve (4.7), and C_5^+ is Darmon's curve recalled in the proof of Lemma 4.5(b).

- [43, §2.2, Remark 2.2, §2.3 and §7.1]: up to a Tate twist, J_t realizes the motive h^+ that Pacetti and Villagra Torcomian attach to the solution (used in Proposition 4.4 and Lemma 4.5).
- [43, Lemma 7.3 and its proof, Proposition 3.1, (19) and (23)]: the congruences between h^+ and the motives realized by E_t and by Darmon's curve C_5^+ (used in (4.8) and for the inertia at $(\sqrt{5})$ in Lemma 4.5(b)).
- [43, Proposition 7.4]: J_t has potentially multiplicative reduction at 3 and 5 (used in Lemma 4.5(b)).
- [2, Proposition 2.17 and Remark 2.18]: an abelian variety with real multiplication has no mixed reduction (applied to J_t at the primes dividing Z in Lemma 4.5(a),(b)).
- [2, Theorems 2.38, 3.5, 4.3 (case 2.b of its proof) and 4.21(4), Remark 3.21]: the reduction at $(\sqrt{5})$ of the Jacobian of C_5^+, from which the inertia character of J_t at $(\sqrt{5})$ is shown to be ramified (used in Lemma 4.5(b)).
- [43, §7.1]: the endomorphism algebra of the Jacobian of the generic member of the family is K (used in Lemma 4.10).

The other citations of these preprints are alternative sources for statements proved here, or comparisons with them. For instance, the finiteness of $J_t[7]$ at (7) [43, Theorem 2.1(4)] is obtained in Lemma 4.5(c) from [4], and so are, in Lemma 4.5(a) and with explicit models, the reduction types of J_t at primes not dividing 15 [43, Theorem 2.1(1),(2)] and the unramifiedness of the residual representation outside $3 \cdot 5 \cdot 7$ [43, Theorem 2.1(3)]. The modularity of J_t [43, Theorem 2.4(1)] is proved in Proposition 4.4, and the real multiplication is also obtained, by another construction, in [26].

4.1. **The genus-2 family and its real multiplication.** Let $K = \mathbb{Q}(\sqrt{5})$, $e = (1+\sqrt{5})/2$, and

$$\mathfrak{d} = 3(e+2) = \frac{3(5+\sqrt{5})}{2}, \qquad \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{d}) = 45. \tag{4.1}$$

Pacetti and Villagra Torcomian [43, §7.1] attach to a solution of (1.1) the genus-2 Frey curve

$$H_t\colon\ y^2 = 5x^6 - 12x^5 + 10tx^3 + t^2, \qquad t = -\frac{X^5}{Y^3}, \tag{4.2}$$

and its Jacobian J_t. Then $t \notin \{0, 1\}$ and $t - 1 = -Z^7/Y^3$.

Proposition 4.1 (Real multiplication)**.** *Over the smooth locus $t \notin \{0, 1, \infty\}$, the Jacobian J_t carries an action of $\mathcal{O}_K = \mathbb{Z}[e]$ by endomorphisms defined over K, compatible with the canonical polarization (that is, invariant under the Rosati involution). We write $[e] \in \mathrm{End}_K(J_t)$ for the endomorphism corresponding to e, so $[e]^2 - [e] - 1 = 0$.*

Proof. The family (4.2) lies in the discriminant-5 family of genus-2 curves with real multiplication of Kumar and Mukamel [36, Theorem 14]: the substitutions $z = -6/(5x)$, $q_s = (-6/5)^3/t$ and $y_1 = yz^3/t$ turn (4.2) into

$$y_1^2 = z^6 + 10q_sz^3 + 10q_s^2z + 5q_s^2, \quad \mathrm{disc} = 200000\, q_s^{10}(125q_s + 216)^2, \tag{4.3}$$

the case $p = 0$, $q = q_s$, of their family $C(p, q)$, where p and q are the two parameters of [36]. For generic (p, q) the correspondence of [36, Theorem 14] induces an endomorphism generating real multiplication by $\mathcal{O}_K$, self-adjoint for the Rosati involution. It is defined over $K(p, q)$ and not over $\mathbb{Q}(p, q)$: in the coordinates of (4.3), the differentials dz/y_1 and $z\,dz/y_1$ of $C(p, q)$, which are defined over $\mathbb{Q}(p, q)$, are eigenforms with eigenvalues $(1 \pm \sqrt{5})/2$ [36, §6 and the proof of Proposition 17], and an endomorphism is determined by its action on differentials. By (4.3) the line $p = 0$ is not in the discriminant locus, so the Jacobian of $C(p, q)$ is an abelian scheme over the discrete valuation ring of the (p, q)-plane over K at the generic point of $\{p = 0\}$. The endomorphism extends over it [40, Ch. II, Proposition 6.4 and Corollary 6.6], and its specialization to the Jacobian of (4.3) over $K(q_s)$ satisfies the same quadratic equation and is self-adjoint. (The same real multiplication is obtained from [26, Theorem 9.2, Proposition 9.5] and [43, §§2.2–2.4, 7.1].) The endomorphism extends over the open subscheme of $\mathbb{P}^1_K$ where (4.2) is smooth: over each local ring of this subscheme, restricting endomorphisms of the Jacobian scheme to its generic fibre over $K(t)$ is bijective [40, Ch. II, Proposition 6.4 and Corollary 6.6], and the local extensions agree on overlaps because they agree on the generic fibre. □

Which root of $x^2 - x - 1$ in $\mathrm{End}(J_t)$ is called $[e]$ is a convention. The results of this section hold for either choice, once it is fixed.

As 7 is inert in K, the residue field $k = \mathcal{O}_K/(7)$ is $\mathbb{F}_{49}$, and $[e]$ makes $J_t[7]$ a 2-dimensional k-vector space, on which $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acts k-linearly:

$$\bar{\rho}_{t,7}\colon G_K \longrightarrow \mathrm{GL}_2(k). \tag{4.4}$$

The Weil pairing is the trace of a k-bilinear alternating pairing on this rank-two module, so

$$\det \bar{\rho}_{t,7} = \chi_7, \tag{4.5}$$

where χ_7 is the mod-7 cyclotomic character, valued in $\mathbb{F}_7^\times \subset k^\times$. We also use the quadratic twist $A_t = J_t^{(\mathfrak{d})}$ of J_t by the character δ of $K(\sqrt{\mathfrak{d}})/K$, with mod-7 representation $\bar{\rho}_{t,7} \otimes \delta$. The character δ is unramified at every place other than (3) and $(\sqrt{5}) = (e+2)$, the real places included: $\mathfrak{d}$ is totally positive, has odd valuation exactly at (3) and $(\sqrt{5})$, and $\mathfrak{d} - (1+e)^2 = 4$, so that $\mathfrak{d} \equiv (1 + e)^2 \pmod 4$. The twist gives A_t multiplicative reduction at (3) and $(\sqrt{5})$ (Lemma 4.5(b)), which level lowering needs in the proof of Proposition 4.6.

4.2. **Local conditions for the pure fields.**

Lemma 4.2. *If $A_\nu \simeq L_a$ then $30 \mid Z$ and $\gcd(XY, 210) = 1$.*

Proof. For every prime p, $A_\nu \otimes \mathbb{Q}_p = \mathbb{Q}_p[T]/(f_\nu)$ with $f_\nu(T) = \phi(T) - \nu = 15T^7 - 35T^6 + 21T^5 - \nu$, and the degrees of the irreducible factors of f_ν over $\mathbb{Q}_p$ are those of $x^7 - 3^a \cdot 5$. Recall that $\nu = X^5/Z^7$ and $1 - \nu = Y^3/Z^7$. Expanding f_ν at $T = 1$ gives

$$f_\nu(1 + S) = (1 - \nu) + 35S^3 + 105S^4 + 126S^5 + 70S^6 + 15S^7. \tag{4.6}$$

Now $x^7 - 3^a \cdot 5$, $1 \le a \le 6$, is irreducible over $\mathbb{Q}_3$ and $\mathbb{Q}_5$, its Newton polygon being a single segment of slope $-a/7$, respectively $-1/7$, with $\gcd(a, 7) = 1$. Modulo 2 it is $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$, with distinct irreducible factors, so over $\mathbb{Q}_2$ its irreducible factors have degrees $1, 3, 3$. Over $\mathbb{Q}_7$ it is irreducible unless $3^a \cdot 5 = d^7$ with $d \in \mathbb{Q}_7$ (a binomial $x^\ell - c$ with ℓ prime is irreducible over any field in which c is not an ℓ-th power), and then it is $(x - d)\, d^6 \Phi_7(x/d)$, with the seventh cyclotomic polynomial Φ_7 irreducible over $\mathbb{Q}_7$. Hence its irreducible factors over $\mathbb{Q}_7$ have degrees 7, or 1 and 6. A segment of a Newton polygon gives a factor over $\mathbb{Q}_p$ whose degree is the horizontal length of the segment.

At 3. If $3 \nmid Z$, then $v_3(\nu) \ge 0$. The coefficient of T^6 in f_ν is a 3-adic unit, that of T^7 has valuation 1, and the others are integral. Hence the Newton polygon ends with the segment from $(6, 0)$ to $(7, 1)$, and f_ν has a linear factor over $\mathbb{Q}_3$, which is impossible. So $3 \mid Z$.

At 5. If $5 \nmid Z$, then $v_5(\nu) \ge 0$. The coefficient of T^5 is a 5-adic unit, those of T^6 and T^7 have valuation 1, and the others are integral. Hence the Newton polygon ends with the segment from $(5, 0)$ to $(7, 1)$, and f_ν has a factor of degree 2 over $\mathbb{Q}_5$, which is impossible. So $5 \mid Z$.

At 2. If $2 \nmid Z$, then exactly one of X, Y is even, because $X^5 + Y^3 = Z^7$ is odd. If $v_2(X) = m \ge 1$, then $f_\nu(2^m U) = 2^{5m} g(U)$ with

$$g(U) = 15 \cdot 2^{2m} U^7 - 35 \cdot 2^m U^6 + 21U^5 - \nu/2^{5m} \in \mathbb{Z}_2[U],$$

and $g \equiv U^5 + 1 = (U + 1)(U^4 + U^3 + U^2 + U + 1) \pmod 2$, as $\nu/2^{5m}$ is a unit. As g is primitive, Hensel's lemma [42, Ch. II, Lemma 4.6] gives a factor of g over $\mathbb{Z}_2$ of degree 4 reducing to the irreducible $U^4 + U^3 + U^2 + U + 1$, so f_ν has an irreducible factor of degree 4 over $\mathbb{Q}_2$, which is impossible. If $v_2(Y) = m \ge 1$, then, by (4.6), $f_\nu(1 + 2^m U) = 2^{3m} g(U)$ with $g \in \mathbb{Z}_2[U]$ and $g \equiv U^3 + 1 = (U + 1)(U^2 + U + 1) \pmod 2$, as 35 and $(1 - \nu)/2^{3m}$ are units and the coefficients of $U^4, \dots, U^7$ are even. In the same way f_ν has an irreducible factor of degree 2 over $\mathbb{Q}_2$, which is impossible. So $2 \mid Z$.

At 7. If $v_7(X) = m \ge 1$, then $v_7(\nu) = 5m$, and the Newton polygon of f_ν at 7 has the points $(0, 5m)$, $(5, 1)$, $(6, 1)$, $(7, 0)$. As $(1 - 5m)/5 < -1/2$ and $(6, 1)$ lies above the segment from $(5, 1)$ to $(7, 0)$, its first segment has length 5, and f_ν has a factor of degree 5 over $\mathbb{Q}_7$, which is impossible. If $v_7(Y) = m \ge 1$, then $v_7(1 - \nu) = 3m$, and, by (4.6), the Newton polygon of $f_\nu(1 + S)$ at 7 has the points $(0, 3m)$, $(3, 1)$, $(4, 1)$, $(5, 1)$, $(6, 1)$, $(7, 0)$. As $(1 - 3m)/3 < -1/4$ and $(4, 1), (5, 1), (6, 1)$ lie above the segment from $(3, 1)$ to $(7, 0)$, its first segment has length 3, and f_ν has a factor of degree 3 over $\mathbb{Q}_7$, which is impossible. So $7 \nmid XY$.

Finally, XY is prime to 30, because $30 \mid Z$ and X, Y, Z are pairwise coprime. □

In the rest of this section, therefore, $30 \mid Z$, $7 \nmid XY$, and $t = -X^5/Y^3$ is a unit at 2, 3, 5 and 7 with $v_p(t - 1) = 7v_p(Z)$ for $p \in \{2, 3, 5\}$.

4.3. **Modularity of J_t.** We use the elliptic curve

$$E_t\colon\ y^2+3xy+ty=x^3, \qquad c_4=9(9-8t), \qquad \Delta=27t^3(1-t), \tag{4.7}$$

whose point $(0,0)$ is a flex (the tangent $y=0$ meets the curve with multiplicity 3), hence a rational point of order 3.

Lemma 4.3. *$E_t[5]$ is an absolutely irreducible $G_{\mathbb{Q}}$-module, and remains absolutely irreducible on restriction to $G_{\mathbb{Q}(\zeta_5)}$.*

Proof. As $5 \mid Z$, we have $t \equiv 1 \pmod{5^7}$. Hence c_4 is a 5-adic unit and $v_5(\Delta) = v_5(1-t) = 7v_5(Z) > 0$: the model is minimal at 5 with multiplicative reduction, and $v_5(j(E_t)) < 0$. A $G_{\mathbb{Q}}$-stable line in $E_t[5]$ and the rational point of order 3 would generate a rational cyclic subgroup of order 15, i.e. a noncuspidal rational point of $X_0(15)$. The four such points have j-invariants $-25/2$, $-349938025/8$, $-121945/32$, $46969655/32768$ [5, pp. 79–80, 86], all 5-integral, contradicting $v_5(j) < 0$. So $E_t[5]$ is irreducible, hence absolutely irreducible, being odd. It remains to treat the restriction to $G_{\mathbb{Q}(\zeta_5)}$. The Serre weight w of $E_t[5]$ is 2 or 6, as E_t is semistable at 5, and by [21, Lemmas 1.13–1.14] a failure of absolute irreducibility over $\mathbb{Q}(\zeta_5)$ would require $5 = 2w-3$ or $5 = 2w-1$, which neither $w=2$ nor $w=6$ satisfies. □

Proposition 4.4 (Modularity)**.** *J_t is modular: there is a Hilbert cuspidal newform over K of parallel weight two whose compatible system of Galois representations is that of J_t with its $\mathcal{O}_K$-action.*

Proof. We use the λ-adic representations of an abelian surface A over K with $\mathcal{O}_K \subset \mathrm{End}_K(A)$, recalled from Ribet's work in [4, §2.2 and Theorem 2.8]. For a prime $\lambda \mid \ell$ of K, $V_\lambda(A) = V_\ell(A) \otimes_{K\otimes\mathbb{Q}_\ell} K_\lambda$ is 2-dimensional over K_λ, with K_λ-linear G_K-action of determinant the ℓ-adic cyclotomic character. If A has good reduction at $v \nmid \ell$, an arithmetic Frobenius at v has characteristic polynomial $T^2 - a_v(A)T + \mathrm{N}\,v$ on $V_\lambda(A)$, with $a_v(A) \in \mathcal{O}_K$ independent of λ (see also [39, Proposition 10.20], applied to the endomorphisms $c\Phi_v^n$ with $c \in \mathcal{O}_K$ and $n \geq 1$, where Φ_v is the Frobenius endomorphism of the reduction). For $\ell \in \{5,7\}$, which is not split in K, we have $K \otimes \mathbb{Q}_\ell = K_\lambda$, so $T_\ell(A)$ is free of rank two over $\mathcal{O}_{K,\lambda}$, and $A[\lambda] = T_\ell(A)/\lambda T_\ell(A)$ is a 2-dimensional $\mathcal{O}_K/\lambda$-vector space whose Frobenius characteristic polynomials are the reductions of those of $V_\lambda(A)$. For $\ell = 7$, which is inert in K, we write $\lambda_7 = (7)$, so that $A[\lambda_7] = A[7]$.

The residual representation at λ_5. Let $\lambda_5 = (\sqrt{5})$, $V_{A,\lambda_5} = V_{\lambda_5}(A_t)$ and $\overline{V}_{A,\lambda_5} = A_t[\lambda_5]$. Up to a Tate twist, J_t realizes the motive h^+ of Pacetti and Villagra Torcomian at t [43, §2.2, Remark 2.2 and §7.1], and the second congruence of [43, Lemma 7.3] compares h^+ modulo $(\sqrt{5})$ with the hypergeometric motive realized by E_t [43, Proposition 3.1 and (19)], with no quadratic twist over K (loc. cit., proof of Lemma 7.3). Taking into account the Tate twist and the twist by δ in A_t, we obtain

$$\overline{V}_{A,\lambda_5}^{\mathrm{ss}} \simeq \left(E_t[5] \otimes \bar{\chi}_5\right)\big|_{G_K} \otimes \bar{\delta}, \tag{4.8}$$

where $\bar{\chi}_5$ is the mod-5 cyclotomic character, whose restriction to G_K is the quadratic character of $K(\zeta_5)/K$, and $\bar{\delta}$ is δ with values in $\mathbb{F}_5^\times$. The factor $\bar{\chi}_5$ comes from the Tate twist, and the data of [43, Table 7.1] at the prime of norm 29, where $\bar{\chi}_5$ is nontrivial, confirm it. By Lemma 4.3, as $G_{K(\zeta_5)} = G_{\mathbb{Q}(\zeta_5)}$, the right-hand side is absolutely irreducible, so $\overline{V}_{A,\lambda_5}$ is semisimple and $\overline{V}_{A,\lambda_5} \simeq E_t'[5]$, where E_t' is the quadratic twist of E_t over K by δ times the quadratic character of $K(\zeta_5)/K$. As an elliptic curve over a real quadratic field, E_t' is modular [23, Theorem 1].

The lifting theorem. Let $W_5 = V_{A,\lambda_5}^\vee$, viewed in $\mathrm{GL}_2(\overline{\mathbb{Q}}_5)$ through an embedding $j_5\colon K_{\lambda_5} \hookrightarrow \overline{\mathbb{Q}}_5$. Following [33, §2, "Rings of coefficients"], its residual representation $\overline{W}_5$ is the semisimplification of its reduction. The hypotheses of the lifting theorem of Khare and Thorne [33, Theorem 1.1] hold:

(i) K is totally real;

(ii) $p = 5$ is odd, and W_5, dual to the λ_5-adic Tate module of an abelian surface, is continuous, 2-dimensional and unramified outside a finite set of places;

(iii) W_5 is de Rham at λ_5, with Hodge–Tate weights $\{0, 1\}$ at both embeddings $K \hookrightarrow \overline{\mathbb{Q}}_5$: in the convention of [33, §2], where the cyclotomic character has weight -1, V_{A,λ_5} has weights in $\{-1, 0\}$ and cyclotomic determinant, hence one weight of each kind, so W_5 has weights $\{0, 1\}$ and determinant ε_5^{-1}, where ε_5 is the 5-adic cyclotomic character;

(iv) $\overline{W}_5$ arises from a cuspidal automorphic representation of weight two: by (4.8), $\overline{W}_5 = (\overline{V}_{A,\lambda_5}^\vee)^{\mathrm{ss}} \simeq E_t'[5]^\vee$, and $E_t'[5]^\vee \otimes \overline{\mathbb{F}}_5$ is the residual representation of $H^1_{\text{ét}}(E_t', \overline{\mathbb{Q}}_5)$, which is attached, in the geometric normalization of [33, §2], to the weight-two automorphic representation of E_t';

(v) $\overline{W}_5|_{G_{K(\zeta_5)}}$ is irreducible over $\overline{\mathbb{F}}_5$, by Lemma 4.3, as $G_{K(\zeta_5)} = G_{\mathbb{Q}(\zeta_5)}$ and twisting by a character preserves irreducibility.

Conditions (i)–(v) are all the hypotheses of [33, Theorem 1.1]. The theorem gives a cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_K)$ of weight two and an isomorphism $\iota\colon \overline{\mathbb{Q}}_5 \simeq \mathbb{C}$ with $W_5 \simeq r_\iota(\pi)$, the representation attached to π in [33, §2].

From λ_5 to every λ. Let Σ be the set of primes of K dividing 5 or of bad reduction for A_t. At $v \notin \Sigma$, $r_\iota(\pi) \simeq W_5$ is unramified, so π_v is unramified [33, §2, property 2], and a geometric Frobenius at v has characteristic polynomial $T^2 - \iota^{-1}(t_v)T + \mathrm{N}\,v\,\iota^{-1}(s_v)$ on $r_\iota(\pi)$, where t_v, s_v are the eigenvalues of T_v, S_v on π_v [33, §2, (2.2)]. On W_5 this is $T^2 - j_5(a_v(A_t))T + \mathrm{N}\,v$, the characteristic polynomial of an arithmetic Frobenius on V_{A,λ_5}. Hence, with $\sigma_0 = \iota \circ j_5|_K\colon K \hookrightarrow \mathbb{C}$,

$$t_v = \sigma_0(a_v(A_t)), \qquad s_v = 1 \qquad (v \notin \Sigma). \tag{4.9}$$

In particular π has trivial central character. For a prime ℓ and $\iota_\ell\colon \overline{\mathbb{Q}}_\ell \simeq \mathbb{C}$, the embedding $j_\ell = \iota_\ell^{-1} \circ \sigma_0\colon K \hookrightarrow \overline{\mathbb{Q}}_\ell$ is continuous for exactly one prime $\lambda \mid \ell$ and extends to K_λ. Every $\lambda \mid \ell$ arises in this way: if $j\colon K \hookrightarrow \overline{\mathbb{Q}}_\ell$ is continuous for λ, the isomorphism $\sigma_0(K) \to j(K)$ extends to an isomorphism $\mathbb{C} \to \overline{\mathbb{Q}}_\ell$, whose inverse ι_ℓ gives $j_\ell = j$. By [33, §2] and (4.9), at every $v \notin \Sigma$ with $v \nmid \ell$, the representations $r_{\iota_\ell}(\pi)$ and $V_\lambda(A_t)^\vee \otimes_{K_\lambda, j_\ell} \overline{\mathbb{Q}}_\ell$ are unramified, and a geometric Frobenius at v has, on both, the characteristic polynomial $T^2 - j_\ell(a_v(A_t))T + \mathrm{N}\,v$. By the Chebotarev density and Brauer–Nesbitt theorems, their semisimplifications are isomorphic. For $\lambda = \lambda_7$, reduction modulo 7 and the Brauer–Nesbitt theorem over $\overline{\mathbb{F}}_7$ give $(A_t[7]^\vee \otimes_{k,\bar{j}_7} \overline{\mathbb{F}}_7)^{\mathrm{ss}} \simeq \bar{r}_{\iota_7}(\pi)$, the semisimplified reduction of $r_{\iota_7}(\pi)$, where $\bar{j}_7\colon k \hookrightarrow \overline{\mathbb{F}}_7$ is the embedding of residue fields induced by j_7, and every embedding $k \hookrightarrow \overline{\mathbb{F}}_7$ arises in this way. As $A_t[7]$ has k-determinant χ_7 by (4.5) and $\delta^2 = 1$, $A_t[7]^\vee \simeq A_t[7] \otimes \chi_7^{-1}$, and

$$\left(A_t[7] \otimes_{k,\bar{j}_7} \overline{\mathbb{F}}_7\right)^{\mathrm{ss}} \simeq \bar{r}_{\iota_7}(\pi) \otimes \chi_7 \simeq \bar{r}_{\iota_7}(\pi)^\vee. \tag{4.10}$$

Here $r_{\iota_7}(\pi)^\vee$, which is isomorphic to $r_{\iota_7}(\pi) \otimes \varepsilon_7$ with ε_7 the 7-adic cyclotomic character, has determinant ε_7, and an arithmetic Frobenius at $v \notin \Sigma$, $v \nmid 7$, has characteristic polynomial $T^2 - \iota_7^{-1}(t_v)T + \mathrm{N}\,v$ on it. Thus $r_{\iota_7}(\pi)^\vee$ is the representation attached to π in the normalization of [8, §3.1], in which the representation attached to a form of parallel weight two is realized in $H^1_{\text{ét}}(1)$ of a Shimura curve, so that its determinant is ε_7 times a character of finite order.

Finally, as $J_t = A_t \otimes \delta$, we have $V_\lambda(J_t) = V_\lambda(A_t) \otimes \delta$. With δ viewed as a Hecke character, $\pi \otimes \delta$ is cuspidal of weight two with trivial central character and $r_{\iota\ell}(\pi \otimes \delta) = r_{\iota\ell}(\pi) \otimes \delta$, so its Hilbert newform has the stated property. □

Modularity of J_t for every rational $t \notin \{0, 1\}$ is also stated in [43, Theorem 2.4(1)], whose proof refers to [25], where the statement for the motive used here is Theorem 6.2.

4.4. Local behaviour of $J_t[7]$.

Lemma 4.5. *The following hold.*

(a) *J_t has good reduction at every prime of K not dividing $15Z$, and multiplicative reduction at every prime dividing Z but not 15, in particular at (2). The representation $\bar\rho_{t,7}$ is unramified at every prime of K not dividing $3 \cdot 5 \cdot 7$, in particular at (2), where the Frobenius eigenvalues on the semisimplification are ε and 4ε for some $\varepsilon = \pm 1$.*

(b) *At (3) and $(\sqrt{5})$ the reduction of J_t is potentially multiplicative, and the inertia group acts on $J_t[7]$ through a ramified quadratic character times a unipotent transformation. Consequently the twist $A_t = J_t^{(\mathfrak{d})}$ has multiplicative reduction at (3) and $(\sqrt{5})$, and inertia acts unipotently on $A_t[7]$ there.*

(c) *If $7 \mid Z$, then $t \equiv 1 \pmod{7^7}$, the reduction at (7) is multiplicative, and $J_t[7]$ extends to a finite flat group scheme over the ring of integers of $K_{(7)}$. If $7 \nmid Z$, the reduction at (7) is good.*

Proof. Write $(a, b, c) = (X, -Z, Y)$, so that $a^5 + b^7 + c^3 = 0$ is the equation of [43] with $(q, p, r) = (5, 7, 3)$, and $t = -a^5/c^3$ is their parameter t_0. The motive h^+ of [43, §2.3] is realized by J_t up to a Tate twist [43, §2.2 and §7.1].

(a). At primes not dividing $30XYZ$, such as (7) when $7 \nmid Z$ (as $7 \nmid XY$ by Lemma 4.2), the model (4.2) is smooth: its leading coefficient 5 and discriminant $2^{12} \cdot 3^6 \cdot 5^5\, t^8(t-1)^2$ are units. Let $\mathfrak{l}$ be a prime dividing XY, so that $\mathfrak{l} \nmid 30$ by Lemma 4.2. If $\mathfrak{l} \mid X$, then $v_\mathfrak{l}(t) = 5v_\mathfrak{l}(X)$, so over an unramified extension of $K_\mathfrak{l}$ we may write $t = s^5$, and $(x, y) = (s^2x', s^5y')$ turns (4.2) into $y'^2 = 1 - 12x'^5 + 10s\,x'^3 + 5s^2x'^6$, whose reduction $y'^2 = 1 - 12x'^5$ is smooth. If $\mathfrak{l} \mid Y$, then $v_\mathfrak{l}(1/t) = 3v_\mathfrak{l}(Y)$, so we may write $t = s^{-3}$, and $(x, y) = (x'/s,\, y'/s^3)$ gives $y'^2 = 5x'^6 - 12s\,x'^5 + 10x'^3 + 1$, whose reduction $y'^2 = 5x'^6 + 10x'^3 + 1$ is smooth. (The discriminants of $1 - 12x^5$ and $5x^6 + 10x^3 + 1$ are divisible only by 2, 3 and 5.) As Néron models commute with unramified base change, J_t has good reduction at $\mathfrak{l}$. At every prime of good reduction not above 7, $\bar\rho_{t,7}$ is unramified by the Néron–Ogg–Shafarevich criterion.

At primes $\mathfrak{l}$ dividing Z but not $2 \cdot 3 \cdot 5$, among them (7) when $7 \mid Z$, we have $v_\mathfrak{l}(t-1) = 7v_\mathfrak{l}(Z) > 0$, and the hypotheses of [4, Theorem 7.5], including the standing ones of [4, §7.1], hold as in (c). By the remark following these standing hypotheses in [4, §7.1], the reduction at $\mathfrak{l}$ is multiplicative, hence totally toric, because an abelian variety with real multiplication has no mixed reduction [2, Proposition 2.17 and Remark 2.18]. For $\mathfrak{l} \neq (7)$, [4, Theorem 7.5] with $\ell \neq p$ shows that $\bar\rho_{t,7}$ is unramified at $\mathfrak{l}$. At (2), where $2 \mid Z$, the same holds for the model

$$y^2 + (x^3 + t)\, y = x^6 - 3x^5 + 2t\, x^3$$

over the ring of integers $\mathcal{O}_2$ of $K_{(2)}$, obtained from (4.2) by $y \mapsto 2y + x^3 + t$. Its discriminant [2, Definition 2.27] is $3^6 \cdot 5^5\, t^8(t-1)^2$, a unit in $\mathcal{O}_2((t-1)) = \mathcal{O}_2[[t-1]][1/(t-1)]$, with t now a variable as in (c), and its reduction modulo 2 is smooth over $\mathbb{F}_4((t-1))$ as well, since in characteristic 2 its singular points lie over $t = 0$ and $t = 1$. At $t = 1$ its fibre over $K_{(2)}$ is isomorphic to $y^2 = (x^2 - x - 1)^2(5x^2 - 2x + 1)$, and its fibre over $\mathbb{F}_4$ is the

geometrically integral curve $y^2 + (x^3+1)y = x^6 + x^5$, whose only singularities are two ordinary double points, at $x^2+x+1=0$, $y=x^2$. Both fibres have normalization of genus 0. The partial derivative $y - 2x^3$ of the equation with respect to t is a unit at the nodes, and $v_2(t-1) = 7v_2(Z)$, with $K_{(2)}/\mathbb{Q}_2$ unramified. So the reduction at (2) is multiplicative, hence totally toric, and $\bar\rho_{t,7}$ is unramified at (2) by [4, Theorem 7.5] with $\ell = 2 \neq p$. The primes above 3 and 5 are treated in (b). These reduction types agree with [43, Theorem 2.1(1),(2)] (see also [25, Theorems 2.9(4) and 4.1] away from 7), by which h^+ is unramified at every prime $\mathfrak{l} \nmid 15b$ and has multiplicative reduction at every $\mathfrak{l} \mid b$ with $\mathfrak{l} \nmid 15$.

At (2), therefore, $J_t[7]^{\mathrm{ss}} \simeq k(\gamma) \oplus k(\gamma\chi_7)$ as a $k[G_{K_{(2)}}]$-module, where the unramified character γ gives the Galois action on the character group of the torus, a rank-one $\mathcal{O}_K$-module. The values of γ are roots of unity of $\mathcal{O}_K$, so $\gamma(\mathrm{Frob}_{(2)}) = \varepsilon = \pm 1$, and $\chi_7(\mathrm{Frob}_{(2)}) = \mathrm{N}(2) = 4$.

(b). As $3 \mid Z$ and $5 \mid Z$, $v_\ell(t-1) = 7v_\ell(Z) \geq 7$ for $\ell = 3, 5$, and [43, Proposition 7.4] gives potentially multiplicative reduction at 3 and 5, totally toric after a finite extension because an abelian variety with real multiplication has no mixed reduction [2, Proposition 2.17 and Remark 2.18]. For $v \in \{(3), (\sqrt{5})\}$, inertia at v acts $\mathcal{O}_K$-linearly through a finite quotient on the character group of the torus, a rank-one $\mathcal{O}_K$-module, hence through a character ψ_v with values in the roots of unity of K, of order dividing 2. So on $J_t[7]$, and on $J_t[\lambda]$ for every λ prime to the residue characteristic of v, inertia acts as ψ_v times a unipotent transformation [27, Exp. IX]. Twisting by a quadratic character χ of G_{K_v} replaces ψ_v by $\psi_v\chi|_{I_v}$, and an abelian variety of this kind, with $\mathcal{O}_K$-action and potentially toric reduction, has toric reduction over K_v exactly when its inertia character is trivial.

At $v = (3)$, untwisting (4.8) by δ gives $J_t[\lambda_5]^{\mathrm{ss}} \simeq (E_t[5] \otimes \bar\chi_5)|_{G_K}$, and, as $5 \neq 3$, inertia acts on $J_t[\lambda_5]$ as $\psi_{(3)}$ times a unipotent transformation. As $t \equiv 1 \pmod{3^7}$, the model (4.7) has $v_3(c_4) = 2$ and $v_3(\Delta) = 3 + 7v_3(Z)$, so it is minimal with additive, potentially multiplicative reduction, and E_t is the twist of a Tate curve by a ramified quadratic character, through which inertia acts on $E_t[5]^{\mathrm{ss}}$. As $\bar\chi_5$ is unramified at 3, $\psi_{(3)}$ is ramified.

At $v = (\sqrt{5})$, the congruence (4.8) gives no information, as 5 is the residue characteristic and inertia acts on the 5-torsion of a Tate curve through $\bar\chi_5$. Instead, the first congruence of [43, Lemma 7.3], which holds over K without a quadratic twist, and [43, (23) and Proposition 3.1] show that, up to a power of the mod-3 cyclotomic character (unramified at 5), $J_t[3]^{\mathrm{ss}}$ is the semisimplified 3-torsion of the Jacobian $J_5^+(s_0)$ of Darmon's curve

$$C_5^+(s)\colon\ y^2 = (x+2)(x^5 - 5x^3 + 5x + 2 - 4s) \qquad \text{at } s_0 = 1/t.$$

This is the curve $y^2 = g_{5,s}^+(x)$ of [2, Definition 3.2] for Azon's prime $r = 5$, with $g_{5,s}^+(x) = (x+2)\, g_{5,s}^-(x)$ and $g_{5,s}^-(x) = x^5 - 5x^3 + 5x + 2 - 4s$. The Jacobian $J_5^+(s_0)$ of $C_5^+(s_0)$ has real multiplication by $\mathcal{O}_K$ over K [2, Theorem 3.5]. We show below that it has potentially toric reduction at $(\sqrt{5})$ with ramified inertia character ψ'. Then, as $3 \neq 5$, inertia at $(\sqrt{5})$ acts on the semisimplified 3-torsion of J_t and of $J_5^+(s_0)$ through $\psi_{(\sqrt{5})} \oplus \psi_{(\sqrt{5})}$ and $\psi' \oplus \psi'$ respectively, with values in $\{\pm 1\} \subset \mathbb{F}_9^\times$. As $1 \neq -1$ in characteristic 3, $\psi_{(\sqrt{5})} = \psi'$ is ramified.

The reduction of $J_5^+(s_0)$ at $(\sqrt{5})$ is given by [2, Theorem 4.3 and Figure 2]. Azon's parameters are $s_0 \in \overline{\mathbb{Q}} \smallsetminus \{0, 1\}$ and $\delta_{\mathbb{Q}} \in \overline{\mathbb{Z}} \smallsetminus \{0\}$ with $\delta_{\mathbb{Q}}^r(2 - 4s_0)$ and $\delta_{\mathbb{Q}}^2$ in $\mathbb{Z}$ [2, Definition 3.18]. For C_r^+ and $\delta_{\mathbb{Q}} \in \mathbb{Z}$, the choice of $\delta_{\mathbb{Q}}$ only changes the Weierstrass model of $C_r^+(s_0)$, which is $y^2 = g_r^+(x)$ with $g_r^+(x) = \delta_{\mathbb{Q}}^{r+1} g_{r,s_0}^+(x/\delta_{\mathbb{Q}})$ [2, Definition 3.20 and Remark 3.21]. We take $s_0 = 1/t = -Y^3/X^5$ and $\delta_{\mathbb{Q}} = X$, so $\delta_{\mathbb{Q}}^5(2 - 4s_0) = 2X^5 + 4Y^3 \in \mathbb{Z}$. For squarefree $\delta_K \in \mathcal{O}_K$, the twist $(C_r^+)^{(\delta_K)}\colon y^2 = \delta_K\, g_r^+(x)$ of [2, Definitions 2.30 and 3.26] becomes isomorphic to C_r^+ over $K(\sqrt{\delta_K})$, the nontrivial automorphism acting through the

hyperelliptic involution, which is -1 on the Jacobian. So $(J_r^+)^{(\delta_K)} \simeq J_r^+ \otimes \chi_{\delta_K}$, with χ_{δ_K} the character of $K(\sqrt{\delta_K})/K$. The reduction types of [2] refer to the identity component of the special fibre of the Néron model: "toric" means a torus and "unipotent" a unipotent group, that is, additive reduction [2, Definition 2.19].

Azon's standing Hypotheses 1–3 [2, p. 23] hold for $(s_0, \delta_{\mathbb{Q}}) = (1/t, X)$ at every prime q. Write $\nu_q = v_q(s_0(s_0-1))$, as in [2, Definition 4.1]. As $s_0(s_0-1) = Y^3Z^7/X^{10}$, $\nu_q \geq 0$ exactly when $q \nmid X$, and then $v_q(\delta_{\mathbb{Q}}) = 0$ and $v_q(2-4s_0) \geq 0$, which gives Hypothesis 1. If $q \geq 3$ and $\nu_q \leq 0$, then $q \nmid YZ$, so $v_q(\delta_{\mathbb{Q}}^{10} s_0(s_0-1)) = v_q(Y^3Z^7) = 0$, which gives Hypothesis 2. As $2 \mid Z$, $\nu_2 = 7v_2(Z) > 0$, and Hypothesis 3, which concerns $\nu_2 \leq 0$, is vacuous.

At $\mathfrak{r} = (\sqrt{5})$, above $r = 5$, we have $v_5(s_0) = 0$ and $v_5(s_0-1) = v_5(Z^7/X^5) = 7v_5(Z) \geq 7$. This is the branch of [2, Figure 2] for the prime $\mathfrak{q} = \mathfrak{r}$ with $v(s_0-1) > 2$, for either normalization of the valuation (on $K_{(\sqrt{5})}$ it is $14v_5(Z)$), treated in [2, proof of Theorem 4.3, case 2.b, p. 44]. Since $v_{(\sqrt{5})}(s_0-1) > 5$, the cluster picture of $C_5^+(s_0)$ over $K_{(\sqrt{5})}$ is that of [2, Theorem 4.21(4)]. The six roots of g_5^+ are the five roots of $g_5^-(x) = \delta_{\mathbb{Q}}^5 g_{5,s_0}^-(x/\delta_{\mathbb{Q}})$, which form a cluster $\mathcal{R}$ of depth 1 containing two twins, and $-2\delta_{\mathbb{Q}}$, which lies outside $\mathcal{R}$ at depth 0. The twins and $\mathcal{R}$ are inertia-invariant, and the splitting field has ramification index at most 2 over $K_{(\sqrt{5})}$. For the twist $(C_5^+)^{(\delta_K)}$, $\mathcal{R}$ is the only principal cluster, with invariant $\nu_{\mathcal{R}} = v_{(\sqrt{5})}(\delta_K) + 5$ in the notation of [2, §2.4.2]. By the semistability criterion [2, Theorem 2.38], $(C_5^+)^{(\delta_K)}$ is semistable exactly when $v_{(\sqrt{5})}(\delta_K) = 1$, its Jacobian then having toric reduction, while for $v_{(\sqrt{5})}(\delta_K) = 0$ the reduction is additive. Taking $\delta_K = \sqrt{5}$, we find that $J_5^+(s_0) \otimes \chi_{\sqrt{5}}$ has toric reduction at $(\sqrt{5})$ and $J_5^+(s_0)$ does not. Hence $J_5^+(s_0)$ has potentially toric reduction, with inertia character ψ' such that $\psi'\chi_{\sqrt{5}}|_I = 1$, and $\psi' = \chi_{\sqrt{5}}|_I$ is ramified, $\sqrt{5}$ being a uniformizer.

Finally, $\mathfrak{d}$ has odd valuation at (3) and $(\sqrt{5})$, so δ is ramified at both. Two ramified quadratic characters of G_{K_v}, for v of odd residue characteristic, differ by an unramified character. Hence $\delta|_{I_v} = \psi_v$, and $A_t = J_t \otimes \delta$ has unipotent inertia, that is, multiplicative reduction, at (3) and $(\sqrt{5})$. (When $\bar{\rho}_{t,7}$ is irreducible, [43, Theorem 7.8] gives its conductor exponent at (3) and $(\sqrt{5})$ as 2, that of a ramified quadratic twist of a unipotent representation.)

(c). If $7 \mid Z$, then $t \equiv 1 \pmod{7^7}$. We apply [4, Theorem 7.5], with the local field there taken to be $K_{(7)}$, whose ring of integers $\mathcal{O}$ is unramified over $\mathbb{Z}_7$ with residue field k, and with $z_0 = 1$, $\pi_0 = t-1$, A the Jacobian of the family (4.2) over $K_{(7)}(t)$, where t is now a variable, and $t_1 = -X^5/Y^3$, so that $A(t_1) = J_t$. Let $\mathcal{W}$ be the Weierstrass model over $\mathcal{O}[[\pi_0]]$ of $y^2 = f(x,t)$, with $f(x,t) = 5x^6 - 12x^5 + 10tx^3 + t^2$ as in (4.2). Its two points at infinity are smooth, as 5 is a unit. The hypotheses of [4, Theorem 7.5], including the standing ones of [4, §7.1], hold as follows.

(ii) *A extends to an abelian scheme over $\mathcal{O}((\pi_0))$.* The discriminant of f in x is $2^{12} \cdot 3^6 \cdot 5^5 t^8 (t-1)^2$, and $t = 1 + \pi_0$ is a unit in $\mathcal{O}[[\pi_0]]$, as are 2, 3 and 5, so $\mathcal{W}$ is smooth over $\mathcal{O}((\pi_0)) = \mathcal{O}[[\pi_0]][1/\pi_0]$, where its Jacobian is an abelian scheme.

(i), (iii) *A has a model over $\mathcal{O}[[\pi_0]]$ with multiplicative reduction of full toric rank at π_0, and A over $k[[\pi_0]]$ has multiplicative reduction of full toric rank at π_0.* At $\pi_0 = 0$ the model specializes to $y^2 = f(x,1) = (x^2-x-1)^2(5x^2-2x+1)$. The discriminants 5 and -16 of the two quadratic factors and their resultant 45 are units at 7. So over algebraic closures of $K_{(7)}$ and of k, $f(x,1)$ has exactly two double roots and two simple roots, the maximal number $g = 2$ of double roots. This is the criterion for bad semistable reduction recalled in [4, §2.3], by which the same hypotheses are verified in the proof of [4, Theorem 7.6]. Over both points

of $\operatorname{Spec}\mathcal{O}$, the fibre at $\pi_0 = 0$ is a geometrically integral curve of arithmetic genus 2 whose only singularities are two ordinary double points at $y = 0$, $x^2 - x - 1 = 0$. Its normalization is the conic $y'^2 = 5x^2 - 2x + 1$, $y = (x^2 - x - 1)y'$, of genus 0. Comparing units on the curve and on its normalization gives an exact sequence $0 \to \mathbb{G}_m^2 \to \mathrm{Pic}^0 \to \mathrm{Pic}^0(\text{normalization}) = 0$ over an algebraic closure, so the generalized Jacobian of the fibre is a torus of dimension $2 = \dim A$. The model $\mathcal{W}$ is regular at the two nodes. Indeed, at a node, $t = 1$ and $x \in \{e, 1 - e\}$ is a root of $x^2 - x - 1$, so $\partial f/\partial t = 10x^3 + 2t$ equals $4(5x + 3)$ there, a unit because $\mathrm{N}_{K/\mathbb{Q}}(5e + 3) = -1$. Hence, over the discrete valuation rings $K_{(7)}[[\pi_0]]$ and $k[[\pi_0]]$, $\mathcal{W}$ is regular with reduced special fibre. By Raynaud's theorem on regular models with reduced special fibre [7, §9.5, Theorem 4], the identity component of the special fibre of the Néron model of the Jacobian is Pic^0 of that fibre, the torus above. Thus A has multiplicative reduction of full toric rank at π_0 over $\mathcal{O}[[\pi_0]]$, $K_{(7)}[[\pi_0]]$ and $k[[\pi_0]]$.

(1) *A is of GL_2-type, with real multiplication by a subfield of* $\mathrm{End}_{K_{(7)}(t)}(A) \otimes \mathbb{Q}$. This is Proposition 4.1.

(2) *There is $t_1 \in \mathbb{P}^1(K_{(7)})$ such that $\mathrm{ord}_{K_{(7)}}(\pi_0(t_1))$ is positive and divisible by 7.* The valuation $v_7(t_1 - 1) = 7v_7(Z)$ is positive and divisible by 7, and $K_{(7)}/\mathbb{Q}_7$ is unramified, so $\mathrm{ord}_{K_{(7)}} = v_7$.

The theorem gives that $J_t[7]$ is finite at (7), that is, extends to a finite flat group scheme over $\mathcal{O}$, as do [43, Theorem 2.1(4)] and [25, Theorem 4.3]. By (a) the reduction at (7) is multiplicative if $7 \mid Z$. If $7 \nmid Z$, then t is a 7-adic unit with $t \not\equiv 1 \pmod 7$, and the reduction at (7) is good. □

4.5. **Reducibility and the characters.**

Proposition 4.6. *$\bar\rho_{t,7}$ is reducible.*

Proof. Suppose that $\bar\rho = \bar\rho_{t,7} \otimes \delta$, the representation of G_K on $A_t[7]$, is irreducible. Being odd, it is absolutely irreducible: otherwise its image would lie in the multiplicative group of a quadratic extension of k, a cyclic group whose elements of order at most two are the scalars ± 1, of determinant one, whereas $\det\bar\rho(c) = \chi_7(c) = -1$ for a complex conjugation c. Its restriction to $\Gamma = G_{K(\zeta_7)}$ is also absolutely irreducible. Indeed G_K/Γ is cyclic of order 6, prime to 7, so a reducible $\bar\rho|_\Gamma \otimes \overline{\mathbb{F}}_7$ would be a sum of two characters. If they were equal, $\bar\rho(\Gamma)$ would be scalar, the projective image of $\bar\rho$ cyclic, and $\bar\rho \otimes \overline{\mathbb{F}}_7$ reducible. If they were distinct, the stabilizer of one of the two lines would be the index-two subgroup G_M containing Γ, with $M = K(\sqrt{-7})$, and $\bar\rho|_{G_M}$ would not be absolutely irreducible, contradicting [4, Lemma 6.9]. The hypotheses of that lemma hold. The variety A_t is of GL_2-type with real multiplication by K, and the prime $7 > 3$ is unramified in K. A_t has good or multiplicative reduction above 7, by Lemma 4.5(a),(c), as δ is unramified at (7). The representation $\bar\rho$ is absolutely irreducible, and a prime above 7 ramifies in M/K, as 7 is unramified in K and ramified in $\mathbb{Q}(\sqrt{-7})$.

By (4.10), for every embedding $k \hookrightarrow \overline{\mathbb{F}}_7$, $\bar\rho \otimes \overline{\mathbb{F}}_7$ has the same semisimplification as the reduction of the 7-adic representation attached, in the normalization of [8, §3.1], to the automorphic representation π constructed in the proof of Proposition 4.4. As $\bar\rho$ is absolutely irreducible, the two are isomorphic.

The representation $\bar\rho$ is unramified at every prime not dividing $3 \cdot 5 \cdot 7$, by Lemma 4.5(a) and as δ is unramified outside (3) and $(\sqrt{5})$. At $v \in \{(3), (\sqrt{5})\}$, A_t has multiplicative

reduction (Lemma 4.5(b)), so by Grothendieck's description of the Tate module of an abelian variety with toric reduction [27, Exp. IX]

$$V_{\lambda_7}(A_t)|_{G_{K_v}} \simeq \begin{pmatrix} \varepsilon_7\alpha_v & * \\ 0 & \alpha_v \end{pmatrix}, \tag{4.11}$$

where α_v is the unramified character, with values ± 1, by which G_{K_v} acts on the character group of the torus, a rank-one $\mathcal{O}_K$-module. Inertia acts unipotently, and $\bar\rho$ is ramified at v exactly when the monodromy of (4.11) is nontrivial modulo 7. At (7), if $7 \mid Z$, A_t has multiplicative reduction (Lemma 4.5(a), as δ is unramified at (7)). The Mumford uniformization used in the proof of [4, Theorem 7.5] (see [4, (7.3)]) makes the 7-torsion of the torus a $G_{K_{(7)}}$-stable k-line in $A_t[7]$, with character $\bar\alpha_7\chi_7$ for an unramified character α_7 with values ± 1. So $\bar\rho|_{G_{K_{(7)}}}$ is an extension of $k(\bar\alpha_7)$ by $k(\bar\alpha_7\chi_7)$, which is finite by Lemma 4.5(c), as finiteness depends only on the restriction to inertia [4, Theorem 7.1]. If $7 \nmid Z$, the reduction at (7) is good and ordinary, as the fibres of (4.2) over $t \bmod 7 \in \{2, \dots, 6\}$ have Frobenius polynomials $T^4 + bT^2 + 49$ with $b \not\equiv 0 \pmod 7$. These polynomials are computed from the point counts in the proof of Proposition 4.8, which do not depend on the present proposition. Hence the 7-divisible group of the Néron model is an extension of an étale group by one of multiplicative type, each of height two and stable under $\mathcal{O}_K$, and

$$V_{\lambda_7}(A_t)|_{G_{K_{(7)}}} \simeq \begin{pmatrix} \varepsilon_7\tilde\alpha_1 & * \\ 0 & \tilde\alpha_2 \end{pmatrix}, \qquad \tilde\alpha_1, \tilde\alpha_2 \text{ unramified}, \quad \tilde\alpha_1\tilde\alpha_2 = 1. \tag{4.12}$$

We apply [8, Théorème 3.2.2], the level-lowering theorem of Breuil and Diamond, in their notation with $F = K$, $p = 7$, and E a sufficiently large finite extension of $\mathbb{Q}_7$ whose residue field k_E contains the quadratic extension of k, as [8, §3.1] requires. Its standing assumptions [8, §3.1], that $\bar\rho$ is continuous, irreducible, totally odd ($\det\bar\rho(c) = -1$ for the complex conjugations at both real places) and modular (it arises from a Hilbert eigenform of some weight and level), hold by the first two paragraphs of this proof. The hypotheses of [8, Théorème 3.2.2] hold as follows.

(A) Here $p = 7 > 2$, and $\bar\rho$ is modular with $\bar\rho|_{G_{K(\zeta_7)}}$ irreducible, by the first two paragraphs. The additional condition on the projective image concerns only $p = 5$.

(B) A character $\psi\colon G_K \to E^\times$ lifting $\det\bar\rho = \chi_7$ with $\psi\varepsilon_7^{-1}$ of finite order: $\psi = \varepsilon_7$.

(C) A set T of places above 7, and a finite set S of finite places containing the places above 7 and those where $\bar\rho$ or ψ is ramified: $T = \{(7)\}$ and $S = \{(7)\} \cup \{v \in \{(3), (\sqrt{5})\} : \bar\rho \text{ is ramified at } v\}$.

(D) For each $v \in S$, a Weil–Deligne type $[r_v, N_v]$, for each $v \in T \cup \{w \nmid 7 : N_w \neq 0\}$ a character $\mu_v\colon G_{K_v} \to k_E^\times$, and a lift $\rho_v\colon G_{K_v} \to \mathrm{GL}_2(E)$ of $\bar\rho|_{G_{K_v}}$ such that:

- (D1) if $v \mid 7$, ρ_v is potentially semistable with Hodge–Tate weights $\{0, 1\}$ for every embedding $K_v \hookrightarrow \overline{\mathbb{Q}}_7$;
- (D2) if $v \mid 7$, ρ_v is potentially ordinary exactly when $v \in T$;
- (D3) ρ_v is of type $[r_v, N_v]$;
- (D4) if $v \in T \cup \{w \nmid 7 : N_w \neq 0\}$, ρ_v has a 1-dimensional subrepresentation σ_v lifting $\mu_v\chi_7$ with $\sigma_v\varepsilon_7^{-1}|_{I_v}$ of finite order;
- (D5) $\det\rho_v|_{I_v} = \psi|_{I_v}$.

We verify (D) place by place.

$v \in S \smallsetminus \{(7)\}$ *(the Steinberg case).* Take r_v unramified, $N_v \neq 0$, $\mu_v = \bar\alpha_v$ and $\rho_v = V_{\lambda_7}(A_t)|_{G_{K_v}} \otimes E$ as in (4.11), which lifts $\bar\rho|_{G_{K_v}}$ as $A_t[7]$ is its reduction. Inertia acts on it

unipotently and nontrivially, as $\bar\rho$ is ramified at v, so it has type $[r_v, N_v]$. The character $\sigma_v = \varepsilon_7\alpha_v$ lifts $\mu_v\chi_7$ with $\sigma_v\varepsilon_7^{-1}|_{I_v} = 1$, and $\det\rho_v = \varepsilon_7$.

$v \in \{(3), (\sqrt{5})\} \smallsetminus S$ *(the unramified case).* No condition is imposed, and the lift produced is unramified outside S, hence at v.

$v = (7)$. Take the crystalline type, r_7 unramified and $N_7 = 0$. If $7 \nmid Z$, take μ_7 to be the reduction of $\tilde\alpha_1$ and $\rho_7 = V_{\lambda_7}(A_t)|_{G_{K_{(7)}}} \otimes E$ as in (4.12). It lifts $\bar\rho|_{G_{K_{(7)}}}$, is crystalline as A_t has good reduction [13, Introduction, Theorem], has the Hodge–Tate weights $\{0, 1\}$ of a Tate module at each embedding, and is ordinary. The character $\sigma_7 = \varepsilon_7\tilde\alpha_1$ lifts $\mu_7\chi_7$ with $\sigma_7\varepsilon_7^{-1}|_{I_7} = 1$, and $\det\rho_7 = \varepsilon_7$. If $7 \mid Z$, then $(\bar\rho \otimes \bar\alpha_7)|_{G_{K_{(7)}}} \otimes_k k_E$ is an extension of k_E by $k_E(\chi_7)$, with class

$$c \in H^1(K_{(7)}, k_E(\chi_7)) = (K_{(7)}^\times/K_{(7)}^{\times 7}) \otimes_{\mathbb{F}_7} k_E$$

by Kummer theory. This extension is finite, that is, peu ramifié [4, Theorem 7.1 and the definition preceding it]: the Kummer generators of the field it cuts out over the maximal unramified extension of $K_{(7)}$ have valuations divisible by 7. The valuation of $K_{(7)}$ extends to that unramified extension with the same value group, and the nontrivial seventh roots of unity do not lie in it. Hence $c = \sum_i \kappa(u_i) \otimes c_i$ with u_i units of the ring of integers $\mathcal{O}$ of $K_{(7)}$, κ the mod-7 Kummer map and $c_i \in k_E$. Let $\tilde c_i \in \mathcal{O}_E$ lift c_i, let $\hat\kappa$ be the 7-adic Kummer map and $\tilde c = \sum_i \hat\kappa(u_i) \otimes \tilde c_i \in H^1(K_{(7)}, \mathcal{O}_E(\varepsilon_7))$, and take $\mu_7 = \bar\alpha_7$ and

$$\rho_7 = \alpha_7 \otimes \begin{pmatrix} \varepsilon_7 & \tilde c \\ 0 & 1 \end{pmatrix},$$

with α_7 as above. It lifts $\bar\rho|_{G_{K_{(7)}}}$ and is crystalline, as Kummer classes of units span the crystalline classes in $H^1(K_{(7)}, E(\varepsilon_7))$ [6, §3, Example 3.9]: for a unit u, the representation $\left(\begin{smallmatrix} \varepsilon_7 & \hat\kappa(u) \\ 0 & 1 \end{smallmatrix}\right)$ describes the Galois action on the Tate module of the 7-divisible group over $\mathcal{O}$ attached to u. It is ordinary with Hodge–Tate weights $\{0, 1\}$. The character $\sigma_7 = \alpha_7\varepsilon_7$ lifts $\mu_7\chi_7$ with $\sigma_7\varepsilon_7^{-1}|_{I_7} = 1$, and $\det\rho_7 = \alpha_7^2\varepsilon_7 = \varepsilon_7$.

The theorem gives a lift $\rho\colon G_K \to \mathrm{GL}_2(E)$ of $\bar\rho$, unramified outside S, of type $[r_v, N_v]$ at each $v \in S$, with $\det\rho = \varepsilon_7$, coming from a Hilbert modular form of parallel weight two. Let $\mathfrak{f}$ be the associated newform and $\pi_\mathfrak{f}$ its automorphic representation. By local–global compatibility ([33, §2, property 2] at places not above 7 and [49] at (7)), the conductor of $\pi_\mathfrak{f}$ at a finite place v is that of the Weil–Deligne representation of $\rho|_{G_{K_v}}$. At (7) it is trivial: ρ is crystalline there, so its Weil–Deligne representation is unramified with $N_7 = 0$. At $v \in S \smallsetminus \{(7)\}$ it has exponent one, as r_v is unramified and $N_v \neq 0$, and at the other finite places it is trivial. As $\det\rho = \varepsilon_7$, the central character is trivial. So $\mathfrak{f}$ has trivial character and level $\mathfrak{n}$ dividing $(3\sqrt{5})$.

As $(-1,-1)_\mathbb{Q}$ is ramified exactly at 2 and ∞, and 2 is inert in K, the algebra $\mathbb{H} = (-1,-1)_K$ is ramified exactly at the two real places. As K has narrow class number one, the Jacquet–Langlands correspondence [20, Theorem 3.9] identifies the Hecke module $S_2(\mathfrak{n})$ of Hilbert cusp forms of parallel weight two, trivial character and level $\mathfrak{n}$ with the functions orthogonal to the constants on the right ideal classes of an Eichler order of level $\mathfrak{n}$ in $\mathbb{H}$ [20, Definition 3.7]. The icosian order $\mathcal{O}_\mathbb{H}$, generated over $\mathcal{O}_K$ by the binary icosahedral group $2I \subset \mathbb{H}^1$, is maximal [54, 11.5.7]. Its norm-one units form a finite group containing, hence equal to, $2I$, a maximal finite subgroup of the unit quaternions, of order 120. The reduced norms of its units are totally positive units of K, hence squares, as e has norm -1. Thus $\mathcal{O}_\mathbb{H}^\times = \mathcal{O}_K^\times \cdot 2I$ and $\mathcal{O}_\mathbb{H}^\times/\mathcal{O}_K^\times \simeq 2I/\{\pm1\} \simeq A_5$, of order 60. The Eichler mass formula [54, Main Theorem 26.1.5 and (26.1.8)] gives, for a maximal order, the mass

$2^{1-[K:\mathbb{Q}]}\,|\zeta_K(-1)|\,h_K = 1/60$, as $\zeta_K(-1) = 1/30$ and $h_K = 1$, and the class of $\mathcal{O}_{\mathbb{H}}$ alone contributes $[\mathcal{O}_{\mathbb{H}}^\times : \mathcal{O}_K^\times]^{-1} = 1/60$, so the class number is one [20, Example 4.6]. Consequently, for squarefree $\mathfrak{n}$, the right ideal classes of an Eichler order of level $\mathfrak{n}$ are the orbits of A_5 on $\prod_{v|\mathfrak{n}} \mathbb{P}^1(\mathbb{F}_v)$, with $\mathbb{F}_v$ the residue field and $\mathcal{O}_{\mathbb{H}}$ acting through a splitting $\mathcal{O}_{\mathbb{H}} \otimes \mathbb{F}_v \simeq M_2(\mathbb{F}_v)$ [20, §4], and $\dim S_2(\mathfrak{n})$ is their number minus one. Here $\mathbb{F}_{(3)} = \mathbb{F}_9$ and $\mathbb{F}_{(\sqrt{5})} = \mathbb{F}_5$. The image of A_5 in $\mathrm{PSL}_2(\mathbb{F}_v)$ is isomorphic to A_5, and a nontrivial element has two, one or no fixed points on $\mathbb{P}^1(\mathbb{F}_v)$ according as it is split semisimple, unipotent or nonsplit semisimple. Therefore elements of order 2, 3, 5 have 2, 1, 0 fixed points on $\mathbb{P}^1(\mathbb{F}_9)$ ($9 \equiv 1 \pmod 4$, $3 = \operatorname{char}\mathbb{F}_9$, $5 \mid 9+1$) and 2, 0, 1 on $\mathbb{P}^1(\mathbb{F}_5)$ ($5 \equiv 1 \pmod 4$, $3 \mid 5+1$, $5 = \operatorname{char}\mathbb{F}_5$), and by Burnside's lemma the numbers of orbits on $\mathbb{P}^1(\mathbb{F}_9)$, $\mathbb{P}^1(\mathbb{F}_5)$ and their product are $(10 + 15\cdot 2 + 20\cdot 1)/60 = 1$, $(6 + 15\cdot 2 + 24\cdot 1)/60 = 1$ and $(60 + 15\cdot 4)/60 = 2$. Hence $S_2(\mathfrak{n}) = 0$ for $\mathfrak{n} = (1), (3), (\sqrt{5})$, and $S_2((3\sqrt{5}))$ is 1-dimensional and consists of newforms. So $\mathfrak{f}$ has level $(3\sqrt{5})$ and is the unique newform of that level.

This newform is the base change to K of the elliptic curve

$$E_{15}\colon\ y^2 + xy + y = x^3 + x^2 - 10x - 10 \qquad \text{(Cremona 15a1)}.$$

Indeed E_{15} has multiplicative reduction at 3 and 5 and good reduction elsewhere, so over K it has multiplicative reduction at (3) and $(\sqrt{5})$ and conductor $(3\sqrt{5})$. It is modular over K [23, Theorem 1], so its newform, the form 2.2.5.1-45.1-a in [37], lies in the 1-dimensional space just computed. As (2) is inert in K with residue field $\mathbb{F}_4$ and $a_2(E_{15}) = -1$, the eigenvalue of $\mathfrak{f}$ at (2) is $a_{(2)} = a_2^2 - 2\cdot 2 = -3$ (equivalently, $\#E_{15}(\mathbb{F}_4) = 8$).

On the other hand, by Lemma 4.5(a) the eigenvalues of an arithmetic Frobenius at (2) on $\bar\rho$ are ε and 4ε with $\varepsilon = \pm 1$ (the twist by δ, unramified at (2), only changes the sign), so its trace is ± 5. As $\bar\rho \simeq \bar\rho_{\mathfrak{f}}$, the residual representation of $\mathfrak{f}$, and (2) does not divide the level, this trace is the reduction of $a_{(2)} = -3$. But $\pm 5 \not\equiv -3 \pmod 7$, a contradiction. □

Proposition 4.7. *The semisimplification of $\bar\rho_{t,7}$ is $k(\delta\chi_7) \oplus k(\delta)$.*

Proof. By Proposition 4.6, $J_t[7]$ contains a G_K-stable k-line, on which G_K acts through a character $\gamma\colon G_K \to k^\times$, and by (4.5) the quotient has character χ_7/γ. By Lemma 4.5, γ is unramified outside (3), $(\sqrt{5})$, (7) and the real places, and quadratic on inertia at (3) and $(\sqrt{5})$. At (7), if $7 \mid Z$, $J_t[7]$ is finite flat over an absolutely unramified base, so by Raynaud's theorem [48, Théorème 3.4.3, Corollaire 3.4.4] the inertia characters of its Jordan–Hölder constituents are powers ω_2^s of the fundamental character of level two, with $s \in \{0,1,7,8\}$ and $\omega_2^8 = \chi_7|_{I_7}$. If $7 \nmid Z$, the reduction is good and the same holds. By reciprocity, the product over all places of the local components of γ at the global unit e is 1. They are ± 1 at (3), $(\sqrt{5})$ and the real places, and $\omega_2(e)^s = \bar e^s$ at (7), where $\bar e$ is the image of e in $k^\times$. Hence $\bar e^{2s} = 1$, and as $\bar e$ has order 16, $8 \mid s$, that is, $s \in \{0, 8\}$ and $\gamma|_{I_7} \in \{1, \chi_7\}$. So exactly one of γ, χ_7/γ is unramified at (7); call it θ.

Then θ^2 is unramified at every finite place and trivial at the real places, where $\theta = \pm 1$. As the narrow class number of K is one (e has norm -1), $\theta^2 = 1$. So θ is the character of some $K(\sqrt{m})/K$, with m of odd valuation exactly at the primes where θ is ramified. Among finite primes these are (3) and $(\sqrt{5}) = (e+2)$, where θ agrees on inertia with γ or γ^{-1} (χ_7 being unramified away from 7), and at these primes γ is the ramified quadratic character of Lemma 4.5(b). As K has class number one, $m = 3(e+2)u$ up to squares, with $u \in \{1, -1, e, -e\}$. As θ is unramified at (2) by Lemma 4.5(a), m is a square modulo 4, hence so is u, since $\mathfrak{d} = 3(e+2)$ is. The unit squares in $(\mathcal{O}_K/4)^\times$ are 1, $1+e$ and $2+3e$, and none of $-1 \equiv 3$, e and $-e \equiv 3e$ is among them. Hence $u = 1$ and $\theta = \delta$. (Equivalently,

$K(\sqrt{u\mathfrak{d}})/K$ has conductor divisible by (2) for $u = -1, e, -e$, and conductor $(3\sqrt{5})$ for $u = 1$.) The other character is $\chi_7\delta^{-1} = \chi_7\delta$. □

4.6. **Divisibility by seven and the submodule.**

Proposition 4.8. $7 \mid Z$.

Proof. Suppose $7 \nmid Z$. Then t is a 7-adic unit with $t \not\equiv 1 \pmod 7$, so J_t has good reduction at (7) and $t \bmod 7 \in \{2, 3, 4, 5, 6\}$. Point counts on H_t for these five values give $\#H_t(\mathbb{F}_7) = 8$ in every case and $\#H_t(\mathbb{F}_{49}) = 44, 60, 54, 70, 34$ respectively, so the Frobenius polynomials over $\mathbb{F}_7$ are $T^4 + bT^2 + 49$ with $b = -3, 5, 2, 10, -8$. Each fibre is ordinary, as $b \not\equiv 0 \pmod 7$, and Frobenius over $\mathbb{F}_{49}$, the residue field of (7) in K, acts on the étale part of $J_t[7]$ by $-b \equiv 3, 2, 5, 4, 1 \pmod 7$ respectively. By Proposition 4.7 this étale part, the unramified constituent, has character δ, and $\delta(\mathrm{Frob}_{(7)}) = -1$ because $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{d}) = 45 \equiv 3$ is a nonsquare modulo 7. As $-1 \equiv 6$ is not among $3, 2, 5, 4, 1$, this is a contradiction. □

Proposition 4.9 (The submodule $k(\delta\chi_7)$)**.** *There is an exact sequence of $k[G_K]$-modules*

$$0 \longrightarrow k(\delta\chi_7) \longrightarrow J_t[7] \longrightarrow k(\delta) \longrightarrow 0. \tag{4.13}$$

Proof. By Proposition 4.7, $A_t[7] = J_t[7] \otimes \delta$ has Jordan–Hölder constituents $k(\chi_7)$ and the trivial representation k, distinct as χ_7 is nontrivial on G_K. If $A_t[7]$ has a G_K-stable line with character χ_7, twisting back by δ gives (4.13). Otherwise the stable line is k, and $A_t[7]$ is an extension

$$0 \longrightarrow k \longrightarrow A_t[7] \longrightarrow k(\chi_7) \longrightarrow 0$$

of $k[G_K]$-modules with class $c \in \mathrm{Ext}^1_{k[G_K]}(k(\chi_7), k) = H^1(K, M)$, where $M = k(\chi_7^{-1})$. We show that $c = 0$. Then $k(\chi_7)$ is also a submodule, and twisting back by δ again gives (4.13). Let c_v be the restriction of c to G_{K_v}.

The places (3) *and* $(\sqrt{5})$. Let $v \in \{(3), (\sqrt{5})\}$, with residue field of order $q = 9$ or 5. Then χ_7 is unramified at v with $\chi_7(\mathrm{Frob}_v) = q$, and $q \equiv 2$ or $5 \pmod 7$, so that $q \not\equiv 1$ and $q^2 \equiv 4 \pmod 7$. As $7 \nmid q$, the local Euler characteristic formula [38, Ch. I, Theorem 2.8] gives

$$\dim_k H^0(K_v, M) - \dim_k H^1(K_v, M) + \dim_k H^2(K_v, M) = 0.$$

Here $H^0(K_v, M) = 0$ as $q^{-1} \not\equiv 1 \pmod 7$, and by local duality [38, Ch. I, Corollary 2.3] $H^2(K_v, M)$ is dual to $H^0(K_v, \mathrm{Hom}(M, \mu_7)) = H^0(K_v, k(\chi_7^2))$, which vanishes as $q^2 \not\equiv 1 \pmod 7$. So $H^1(K_v, M) = 0$ and $c_v = 0$.

The place (7). By Proposition 4.8, $7 \mid Z$, so A_t has multiplicative reduction at (7) (Lemma 4.5(a), as δ is unramified at (7)). As in the proof of Proposition 4.6, $A_t[7]|_{G_{K_{(7)}}}$ contains the 7-torsion of the torus in the uniformization of A_t over $K_{(7)}$, a stable k-line on which inertia acts through χ_7, nontrivially as $K_{(7)}/\mathbb{Q}_7$ is unramified. The line k is also stable, with trivial inertia action, so $A_t[7]|_{G_{K_{(7)}}}$ is the direct sum of these two lines, and $c_{(7)} = 0$.

The other finite places. If $v \nmid 3 \cdot 5 \cdot 7$, $A_t[7]$ is unramified at v, by Lemma 4.5(a) and as δ is unramified outside (3) and $(\sqrt{5})$. So the cocycle $g \mapsto g\tilde{x} - \tilde{x}$ representing $c|_{I_v}$, where $\tilde{x} \in A_t[7]$ lifts a generator of the quotient, vanishes, and c is unramified at v.

The global step. In this paragraph, L denotes the field $K(\zeta_7) = \mathbb{Q}(\sqrt{5}, \zeta_7)$, which is totally imaginary of degree 12. As χ_7 is trivial on G_L, the restriction c_L of c lies in $H^1(L, k) = \mathrm{Hom}_{\mathrm{cont}}(G_L, k)$. It is unramified at every finite place of L: above (3), $(\sqrt{5})$ and (7) as $c_v = 0$ there, and elsewhere by the previous paragraph. As L has no real places, class field theory shows that c_L factors through the Galois group of the Hilbert class field of L,

so $c_L \in \mathrm{Hom}(\mathrm{Cl}(L), k)$. The field L, of discriminant $5^6 \cdot 7^{10}$, has class number 1, by an unconditional computation (Appendix E) with the model of L generated over $\mathbb{Q}$ by a root of

$$x^{12} - x^{11} + 2x^{10} - 3x^9 + 5x^8 - 8x^7 + 13x^6 + 8x^5 + 5x^4 + 3x^3 + 2x^2 + x + 1.$$

Hence $c_L = 0$. By inflation–restriction, c lies in the image of the group $H^1(\mathrm{Gal}(L/K), M^{G_L})$, which is killed by $[L : K] = 6$ and by 7, hence zero. So $c = 0$. □

4.7. **The curve of k-lines.** Let $U = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ with coordinate t. For the family $J_t \to U$ of (4.2) with its $\mathcal{O}_K$-action, $J_t[7]$ is a local system of 2-dimensional k-vector spaces on U, and the associated projective bundle

$$\mathcal{X}^\circ = \mathbb{P}_k(J_t[7]) \longrightarrow U$$

is a finite étale cover of degree $\#\mathbb{P}^1(k) = 50$, whose fibre over t is the set of k-lines in $J_t[7]$ (over an algebraic closure). Let $\mathcal{X}$ be the smooth projective curve containing $\mathcal{X}^\circ$, and $t\colon \mathcal{X} \to \mathbb{P}^1$ the induced map.

Lemma 4.10. *$\mathcal{X}$ and the map t are defined over $\mathbb{Q}$.*

Proof. The family is defined over $\mathbb{Q}$ and the action of $\mathcal{O}_K \subset \mathrm{End}(J_t)$ over K, so $\mathcal{X}^\circ$ is defined over K. The nontrivial automorphism of $K/\mathbb{Q}$ acts on the family and carries $[e]$ to a root of $x^2 - x - 1$ in the endomorphism ring of the generic member J_η, that is, to $[e]$ or $1 - [e]$, as $\mathrm{End}^0(J_\eta) = K$ [43, §7.1]. This image is not $[e]$. Otherwise $[e]$ would be defined over $\mathbb{Q}(t)$, hence over $\mathbb{Q}$ on the fibre J_2 at $t = 2$. This fibre has good reduction at the prime 7, which is inert in K, and the reduction of $[e]$ would commute with the Frobenius endomorphism π of J_2 modulo 7. Then π would have characteristic polynomial $\mathrm{N}_{K/\mathbb{Q}}(T^2 - aT + 7)$ with $a \in \mathcal{O}_K$, its K-linear determinant being 7 as the Weil pairing is the trace of a K-bilinear alternating form on which π acts with multiplier 7. By the proof of Proposition 4.8, $\#H_2(\mathbb{F}_7) = 8$, so π has trace 0 and $a = c\sqrt{5}$ with $c \in \mathbb{Z}$, giving $T^4 + (14 - 5c^2)T^2 + 49$. But that proof gives $T^4 - 3T^2 + 49$, and $14 - 5c^2 = -3$ has no solution. So the automorphism carries $[e]$ to $1 - [e]$. Hence elements of G_K act on $J_t[7]$ k-linearly and those of $G_\mathbb{Q} \smallsetminus G_K$ semilinearly with respect to the Frobenius of $k/\mathbb{F}_7$, so all of them preserve $\mathcal{O}_K$ and permute the k-lines in $J_t[7]$. Therefore $\mathcal{X}^\circ$, $\mathcal{X}$ and t descend to $\mathbb{Q}$. □

Proposition 4.11 (Monodromy and genus)**.** *The geometric monodromy group of $J_t[7]$ on U is $\mathrm{SL}_2(k)$, of order 117600. The local monodromies at $t = 0, 1, \infty$ have orders 5, 7 and 3, and act on $\mathbb{P}^1(k)$ with cycle types 5^{10}, $1 \cdot 7^7$ and $1^2 \cdot 3^{16}$. Consequently $\mathcal{X}$ is geometrically connected of genus 8, and $t\colon \mathcal{X} \to \mathbb{P}^1$ has degree 50 with these three branch profiles.*

Proof. At $t = 0$ the substitution $t = s^5$, $x = s^2x'$, $y = s^5y'$ gives the smooth limit $y'^2 = 1 - 12x'^5$, with an automorphism of order 5 whose cohomological eigenvalues are the primitive fifth roots of unity. Hence the k-linear monodromy has order 5 and trace α_0, where $\alpha_0^2 + \alpha_0 - 1 = 0$ in k. At $t = \infty$ the substitution $t = s^{-3}$, $x = x'/s$, $y = y'/s^3$ gives $y'^2 = 5x'^6 + 10x'^3 + 1$, with an automorphism of order 3 and no invariant cohomology, so the monodromy has order 3 and trace -1. At $t = 1$ the fibre has two nodes (see the proof of Lemma 4.5(c)), and by the Picard–Lefschetz formula [19, Exp. XV, Théorème 3.4] the monodromy is unipotent. It is nontrivial modulo 7, hence of order 7, as the two vanishing cycles are part of a symplectic basis of H_1 of a smooth fibre (see the proof of Lemma 6.1).

In a suitable k-basis of $J_t[7]$ the local monodromies are

$$G_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad G_0 = \begin{pmatrix} 0 & (1+\alpha_0)^{-1} \\ -1-\alpha_0 & \alpha_0 \end{pmatrix}, \qquad G_\infty = G_0^{-1} G_1^{-1},$$

all of determinant one. The trace condition on G_∞ and conjugation by the centralizer of G_1 fix G_0 up to the choice of α_0, and the two choices are conjugate under the Frobenius of $k/\mathbb{F}_7$. The group generated by G_0, G_1 has order $117600 = 49(49^2-1)$ (Appendix E), so it is $\mathrm{SL}_2(k)$. This group acts two-transitively on $\mathbb{P}^1(k)$, hence $\mathcal{X}$ is connected. The matrix G_0 has no eigenvector in k^2 (its eigenvalues are primitive fifth roots of unity, not in $\mathbb{F}_{49}$), so it permutes the 50 lines in ten 5-cycles. The matrix G_1 fixes exactly one line and permutes the others in seven 7-cycles, and G_∞ has two eigenlines and permutes the rest in sixteen 3-cycles. Riemann–Hurwitz gives $2g(\mathcal{X}) - 2 = -2 \cdot 50 + 40 + 42 + 32 = 14$, so $g(\mathcal{X}) = 8$. □

The same computation gives the genera, listed in Table 3, of the curve W of nonzero vectors in $J_t[7]$ and of its quotient $W/\mathbb{F}_7^\times$ by the scalars $\mathbb{F}_7^\times$. These curves are defined in Section 5.1, where their genera are recalled.

Cover of $\mathbb{P}^1$	Degree	over $t=0$	over $t=1$	over $t=\infty$	Genus
W (nonzero vectors)	2400	5^{480}	$1^{48} \cdot 7^{336}$	3^{800}	369
$W/\mathbb{F}_7^\times$	400	5^{80}	$1^8 \cdot 7^{56}$	$1^{16} \cdot 3^{128}$	57
$\mathcal{X}$ (lines)	50	5^{10}	$1 \cdot 7^7$	$1^2 \cdot 3^{16}$	8

TABLE 3. The cover W of nonzero vectors in $J_t[7]$ and its quotients $W/\mathbb{F}_7^\times$ and $\mathcal{X} = W/k^\times$: degrees, cycle types over $t = 0, 1, \infty$, and genera by Riemann–Hurwitz.

Proposition 4.12 (A rational point on $\mathcal{X}$)**.** *The line $H = k(\delta\chi_7) \subset J_t[7]$ of (4.13) is $G_\mathbb{Q}$-stable, hence defines a point $x_H \in \mathcal{X}(\mathbb{Q})$ with $t(x_H) = -X^5/Y^3$.*

Proof. As χ_7 is nontrivial on G_K, the characters $\delta\chi_7$ and δ are distinct, so H is the unique G_K-stable line with character $\delta\chi_7$, whether or not (4.13) splits. Let $g \in G_\mathbb{Q} \smallsetminus G_K$. By the proof of Lemma 4.10, g acts on $J_t[7]$ semilinearly with respect to the Frobenius of $k/\mathbb{F}_7$, so $g(H)$ is a G_K-stable line whose character is the g-conjugate of $\delta\chi_7$ composed with the Frobenius of k. This character is $\delta\chi_7$. Indeed, $\delta\chi_7$ takes values in $\mathbb{F}_7^\times$, which the Frobenius fixes, and $\chi_7|_{G_K}$ and δ are both invariant under conjugation by g: the conjugate of δ is the character of $K(\sqrt{\mathfrak{d}'})/K$, where $\mathfrak{d}' = 3(5-\sqrt{5})/2$, and $\mathfrak{d}/\mathfrak{d}' = e^2$ is a square. So $g(H) = H$: H is $G_\mathbb{Q}$-stable and defines a $\mathbb{Q}$-rational point of $\mathcal{X}^\circ$ over $t = -X^5/Y^3$. □

5. The lift to C

Proposition 4.12 produced a point $x_H \in \mathcal{X}(\mathbb{Q})$ over $t = -X^5/Y^3$. Using only the character information in (4.13), we lift it to a rational point of an unramified double cover $C \to \mathcal{X}$.

5.1. **Vectors, scalar classes and the parity cover.** We keep the notation of Section 4.7: $k = \mathbb{F}_{49}$, and $J_t[7]$ is the local system of 2-dimensional k-vector spaces over $U = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$. Besides the bundle $\mathcal{X}^\circ$ of lines we consider the cover of nonzero vectors and its quotients by subgroups of $k^\times$:

$$W^\circ = J_t[7] \smallsetminus \{0\} \longrightarrow W^\circ/\mathbb{F}_7^\times \longrightarrow W^\circ/(k^\times)^2 \longrightarrow \mathcal{X}^\circ = W^\circ/k^\times. \tag{5.1}$$

Here $(k^\times)^2$ is the subgroup of squares, of index two, and $\mathbb{F}_7^\times \subset (k^\times)^2$ as $\mathbb{F}_7^\times$ has order 6 and $(k^\times)^2$ order 24. Over $\mathcal{X}^\circ$ the three covers have degrees 48, 8 and 2. We write W, $W/\mathbb{F}_7^\times$ and $\mathcal{Z}$ for the smooth projective curves containing W°, $W^\circ/\mathbb{F}_7^\times$ and $\mathcal{Z}^\circ = W^\circ/(k^\times)^2$, respectively. The curves W and $W/\mathbb{F}_7^\times$ have genus 369 and 57 (Proposition 4.11, Table 3), and all three curves are defined over $\mathbb{Q}$, by the argument of Lemma 4.10. We call $\mathcal{Z} \to \mathcal{X}$ the *parity cover*: for generators γ of $k^\times$ and v of a line, the two classes modulo $(k^\times)^2$ in the line are those of the $\gamma^j v$ with j even and with j odd.

Lemma 5.1. *The degree-8 cover $W/\mathbb{F}_7^\times \to \mathcal{X}$ is unramified. Consequently the parity cover $q_{\mathcal{Z}}\colon \mathcal{Z} \to \mathcal{X}$ is an unramified double cover, and $g(\mathcal{Z}) = 15$.*

Proof. By the proof of Proposition 4.11, at $t = 0$ the matrix G_0 fixes no nonzero vector and no line, and all its orbits on both have length 5. At $t = 1$ the unipotent G_1 fixes the vectors of one line pointwise and has orbits of length 7 on the other vectors and lines. At $t = \infty$, G_∞ acts on each of its two eigenlines by a scalar of order 3, which lies in $\mathbb{F}_7^\times$ and so acts trivially on $W^\circ/\mathbb{F}_7^\times$ over these lines, and on the other lines and their vectors all orbits have length 3. So in each case the ramification indices agree, and $W/\mathbb{F}_7^\times \to \mathcal{X}$ is unramified at the boundary. As it is étale over U by construction, it is unramified, and then so is the intermediate cover $\mathcal{Z} \to \mathcal{X}$. Riemann–Hurwitz gives $2g(\mathcal{Z}) - 2 = 2(2 \cdot 8 - 2)$, i.e. $g(\mathcal{Z}) = 15$. □

5.2. **The fibre over x_H and the twist by 5.** Let $x_H \in \mathcal{X}(\mathbb{Q})$ be the point of Proposition 4.12, corresponding to the line $H = k(\delta\chi_7) \subset J_t[7]$, with δ as in Section 4.1. The fibres over x_H of $W^\circ \to \mathcal{X}^\circ$, of $W^\circ/\mathbb{F}_7^\times \to \mathcal{X}^\circ$ and of $\mathcal{Z} \to \mathcal{X}$ are the set $H \smallsetminus \{0\}$ of 48 vectors with its Galois action, its eight classes modulo $\mathbb{F}_7^\times$, and its two classes modulo $(k^\times)^2$.

Lemma 5.2. *Fix a generator v of H and a generator γ of $k^\times$, and index the eight scalar classes by $j \in \mathbb{Z}/8$ via $\gamma^j v$. Then G_K fixes every class, while every $g \in G_\mathbb{Q} \smallsetminus G_K$ acts by $j \mapsto m - j$ for some odd m (depending on g).*

Proof. The group G_K acts on $H = k(\delta\chi_7)$ through the character $\delta\chi_7$, whose values lie in $\mathbb{F}_7^\times$ as $\delta = \pm 1$, so it fixes every class. Let $g \in G_\mathbb{Q} \smallsetminus G_K$. It acts on $J_t[7]$ semilinearly with respect to the Frobenius $x \mapsto x^7$ of k (see the proof of Lemma 4.10) and preserves H (Proposition 4.12), so $g(v) = \alpha v$ with $\alpha \in k^\times$. Then $g^2 \in G_K$ and $g^2(v) = g(\alpha v) = \alpha^7 \alpha\, v = \mathrm{N}_{k/\mathbb{F}_7}(\alpha)\ v$, so

$$\mathrm{N}_{k/\mathbb{F}_7}(\alpha) = (\delta\chi_7)(g^2) = \delta(g^2)\,\chi_7(g)^2.$$

The extension $K(\sqrt{\mathfrak{d}})/\mathbb{Q}$ is cyclic of order four: $\sqrt{5} \mapsto -\sqrt{5}$ extends to $\sqrt{\mathfrak{d}} \mapsto 3\sqrt{5}/\sqrt{\mathfrak{d}}$, whose square is $\sqrt{\mathfrak{d}} \mapsto -\sqrt{\mathfrak{d}}$, as $\mathfrak{d}\mathfrak{d}' = 45$ for the conjugate $\mathfrak{d}'$ of $\mathfrak{d}$. So g^2 restricts to the nontrivial element of $\mathrm{Gal}(K(\sqrt{\mathfrak{d}})/K)$, and $\delta(g^2) = -1$ is a nonsquare modulo 7. Hence $\mathrm{N}_{k/\mathbb{F}_7}(\alpha)$ is a nonsquare in $\mathbb{F}_7^\times$, and $\alpha = \gamma^m$ with m odd, as the norm $x \mapsto x^8$ sends γ^m to the m-th power of a generator of $\mathbb{F}_7^\times$. Finally $g(\gamma^j v) = \gamma^{7j}\alpha v = \gamma^{7j+m} v$, and $7j + m \equiv m - j \pmod 8$. □

Proposition 5.3 (Lifting to C)**.** *Let $C = \mathcal{Z}^{(5)}$ be the quadratic twist of the parity cover $\mathcal{Z} \to \mathcal{X}$ by $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$, with covering map $q\colon C \to \mathcal{X}$ and covering involution τ. Then C is an unramified double cover of $\mathcal{X}$ of genus 15, defined over $\mathbb{Q}$, and there are exactly two points $R \in C(\mathbb{Q})$ with $q(R) = x_H$; in particular*

$$t(q(R)) = -\frac{X^5}{Y^3}.$$

Proof. By Lemma 5.2, G_K fixes both points of the fibre of $\mathcal{Z}$ over x_H (the classes with j even and with j odd), and each $g \in G_\mathbb{Q} \smallsetminus G_K$ swaps them, as $j \mapsto m - j$ with m odd changes

parity. So this fibre is $\operatorname{Spec} K$. Twisting by the quadratic character of $K/\mathbb{Q}$ multiplies the action of each $g \in G_{\mathbb{Q}} \smallsetminus G_K$ on fibres by the covering involution, so $G_{\mathbb{Q}}$ acts trivially on the fibre over x_H, and both points become rational. Over K the twist becomes isomorphic to $\mathcal{Z}$ as a cover of $\mathcal{X}$, so $C \to \mathcal{X}$ is again an unramified double cover of genus 15, and $t(q(R)) = t(x_H)$ as $q(R) = x_H$. □

Remark 5.4. A solution produces a point of $C(\mathbb{Q})$, but a rational point of C need not come from a solution. The argument of Sections 6 to 8 concerns all of $C(\mathbb{Q})$.

5.3. **The explicit model.** On $\mathbb{P}^7_{\mathbb{Q}}$ with coordinates $x_0, \dots, x_7$ we fix fifteen quadratic forms $q_1, \dots, q_{15}$, thirteen pairs (A_i, B_i) of quintic forms and a quadratic form r_0. Remark 5.6 says where they come from. Each q_i has 14 or 15 terms, with coefficients of at most 162 bits, and r_0 has 19 terms, with coefficients of at most 632 bits. With each pair scaled to be primitive integral, each A_i has 63 terms and each B_i has 51, with coefficients of at most 5828 bits. These forms, and the effective divisor E_c of degree 8 on the curve they define (Proposition 5.10), are in the supplementary data [31], and the reductions of the q_i and r_0 modulo 13 are printed in Table 11. We write $I = (q_1, \dots, q_{15}) \subset \mathbb{Q}[x] = \mathbb{Q}[x_0, \dots, x_7]$ and

$$y_0 = x_1 - 25x_0, \qquad y_1 = x_2 - 204x_0$$

(any two linear forms with the properties checked below would do).

Proposition 5.5 (Canonical model)**.** *Let $\mathcal{X}' \subset \mathbb{P}^7_{\mathbb{Q}}$ be the closed subscheme defined by $q_1, \dots, q_{15}$.*

(a) *$\mathcal{X}'$ is a smooth, geometrically integral curve of genus 8 with Hilbert polynomial $14n - 7$. It is canonically embedded and not hyperelliptic, and its homogeneous ideal is I.*

(b) *For all i, j the form $A_iB_j - A_jB_i$ vanishes on $\mathcal{X}'$, and the twenty-six forms $A_1, \dots, A_{13}, B_1, \dots, B_{13}$ have no common zero on $\mathcal{X}'$. Hence the maps $(A_i : B_i)$, each defined where $(A_i, B_i) \neq (0, 0)$, glue to a morphism $t\colon \mathcal{X}' \to \mathbb{P}^1_{\mathbb{Q}}$. (The B_i alone vanish simultaneously exactly on the fibre over $t = \infty$.)*

(c) *t has degree 50, is étale over U, and has ramification profiles 5^{10}, $1 \cdot 7^7$ and $1^2 \cdot 3^{16}$ over 0, 1 and ∞.*

(d) *The point $P_0 = (1 : 0 : \cdots : 0)$ lies on $\mathcal{X}'$, $t(P_0) = 1$, and P_0 is the unramified point of the fibre over $t = 1$. The function $u = x_1/x_0$ is a uniformizer at P_0, and $t - 1 = u + O(u^2)$.*

Proof. (a). A Gröbner basis of I over $\mathbb{Q}$ (degree reverse lexicographic order, 21 elements) shows that $\mathbb{Q}[x]/I$ has Hilbert series $(1 + 6T + 6T^2 + T^3)/(1 - T)^2$, so its Hilbert function is $1, 8$ and $14n - 7$ for $n \geq 2$. The q_i are 13-integral, and a Gröbner basis over $\mathbb{F}_{13}$ gives the same Hilbert function for the ideal $\bar{I}$ of their reductions $\bar{q}_i$. So every graded piece of $\mathbb{Z}_{(13)}[x]/(q_1, \dots, q_{15})$ is a finitely generated $\mathbb{Z}_{(13)}$-module of the same rank over $\mathbb{Q}$ and over $\mathbb{F}_{13}$, hence free. Therefore $\mathcal{X}'_{\mathbb{Z}_{(13)}} = \operatorname{Proj} \mathbb{Z}_{(13)}[x]/(q_1, \dots, q_{15})$ is flat and projective over $\mathbb{Z}_{(13)}$, with generic fibre $\mathcal{X}'$ and special fibre $\mathcal{X}'_{\mathbb{F}_{13}} = V(\bar{I})$.

In the coordinates $y_0, y_1, x_0, x_3, \dots, x_7$, a Gröbner basis of $\bar{I}$ for a block order that puts y_0, y_1 last has no leading monomial involving y_0 or y_1, and $\bar{I} + (y_0, y_1)$ has colength 14. So $\mathbb{F}_{13}[x]/\bar{I}$ is free of rank 14 over $\mathbb{F}_{13}[y_0, y_1]$, and $\mathcal{X}'_{\mathbb{F}_{13}}$ is finite and flat over both charts of the $\mathbb{P}^1$ with coordinate y_1/y_0, hence of pure dimension 1. Let $\partial\bar{q}$ be the Jacobian matrix of $(\bar{q}_1, \dots, \bar{q}_{15})$. For the 6×15 and 8×6 matrices R_k and C_k $(k = 1, \dots, 4)$ over $\mathbb{F}_{13}$ listed in the supplementary data [31], each $\det(R_k \cdot \partial\bar{q} \cdot C_k)$ lies in the ideal of 6×6 minors of $\partial\bar{q}$, by the Cauchy–Binet formula. Adjoining the four determinants to $\bar{I}$ gives an ideal defining

the empty subscheme of $\mathbb{P}^7_{\mathbb{F}_{13}}$. Hence $\partial\bar{q}$ has rank 6 on $\mathcal{X}'_{\mathbb{F}_{13}}$, which is therefore smooth. (Step (iii) of the proof of Proposition 7.1 proves this from Table 11 alone.)

By [53, Tag 01V9], $\mathcal{X}'_{\mathbb{Z}_{(13)}}$ is smooth over $\mathbb{Z}_{(13)}$ at every point of the special fibre. The locus where $\mathcal{X}'_{\mathbb{Z}_{(13)}} \to \operatorname{Spec}\mathbb{Z}_{(13)}$ is not smooth is closed. As $\mathcal{X}'_{\mathbb{Z}_{(13)}}$ is proper, the image of this locus in $\operatorname{Spec}\mathbb{Z}_{(13)}$ is closed, and it does not contain the closed point, so the locus is empty. Hence $\mathcal{X}'$ is smooth over $\mathbb{Q}$. It is of pure dimension 1, as $\mathbb{Q}[x]/I$ is free of finite rank over $\mathbb{Q}[y_0, y_1]$ (see the proof of (c)), and $\chi(\mathcal{O}_{\mathcal{X}'}) = -7$. By the proof of (c), $\mathcal{X}'$ is birational to an irreducible plane curve, so it is irreducible. It has the smooth rational point P_0 of (d), so it is geometrically irreducible: a smooth point lies on a single geometric component, which is then Galois-stable, while $G_{\mathbb{Q}}$ permutes the geometric components transitively. Hence $\mathcal{X}'$ is a smooth, geometrically integral curve of genus 8.

The curve $\mathcal{X}'$ lies in no hyperplane (the q_i are quadrics, and I is saturated, since y_0 is a nonzerodivisor on $\mathbb{Q}[x]/I$, which is free over $\mathbb{Q}[y_0, y_1]$). So $h^0(\mathcal{O}_{\mathcal{X}'}(1)) \geq 8 = g$, and $\mathcal{X}'$ has degree $14 = 2g - 2$. Riemann–Roch gives $h^0(K_{\mathcal{X}'} - \mathcal{O}_{\mathcal{X}'}(1)) = h^0(\mathcal{O}_{\mathcal{X}'}(1)) - 7 \geq 1$ for this class of degree 0, so $\mathcal{O}_{\mathcal{X}'}(1) \simeq K_{\mathcal{X}'}$. Thus $\mathcal{X}'$ is canonically embedded, hence not hyperelliptic. The fifteen q_i are linearly independent in $I(\mathcal{X}')_2$, which has dimension $(g-2)(g-3)/2 = 15$ by Max Noether's theorem. They cut out a curve and not a surface, so $\mathcal{X}'$ is not trigonal, and it is not a plane quintic, as $g \neq 6$. By Petri's theorem [55, Ch. 2 and Theorem 3.2.2] the homogeneous ideal of $\mathcal{X}'$ is therefore generated by $I(\mathcal{X}')_2$, that is, it equals I.

(b). The normal forms of the 78 forms $A_iB_j - A_jB_i$ $(i < j)$ modulo the Gröbner basis of (a) are zero, so where $(A_i : B_i)$ and $(A_j : B_j)$ are both defined, they agree. A Gröbner basis over $\mathbb{Q}$ of $I + (A_1, \ldots, A_{13}, B_1, \ldots, B_{13})$ shows that this ideal contains a power of $(x_0, \ldots, x_7)$, so the A_i and B_i have no common zero on $\mathcal{X}'$. Finally, $I + (B_1, \ldots, B_{13})$ defines a subscheme of $\mathcal{X}'$ of dimension 0 and degree 50, the fibre $t^*(\infty)$.

(c). The algebra $\mathbb{Q}[x]/(I + (y_0, y_1))$ has dimension 14, with Hilbert function $(1, 6, 6, 1)$, and a Gröbner basis of I for the block order of (a) has no leading monomial involving y_0 or y_1. Hence $\mathbb{Q}[x]/I$ is free of rank 14 over $\mathbb{Q}[y_0, y_1]$ (with a basis of monomials in $x_0, x_3, \ldots, x_7$), the forms y_0 and y_1 have no common zero on $\mathcal{X}'$, and $\varphi = y_1/y_0 \colon \mathcal{X}' \to \mathbb{P}^1$ is finite of degree 14. Let M_{A_1}, M_{B_1} be the matrices over $\mathbb{Q}[\varphi]$ of multiplication by A_1, B_1 on the dehomogenized module (chart $y_0 = 1$), and let $G(\varphi, T) \in \mathbb{Z}[\varphi, T]$ be the primitive part of $\det(T\,M_{B_1} - M_{A_1})$. The content removed, of degree 20 in φ, comes from the common zeros of A_1 and B_1. By construction G is, up to a factor in $\mathbb{Q}(\varphi)^\times$, the characteristic polynomial of t over $\mathbb{Q}(\varphi)$. It has degree 14 in T and 50 in φ and no nonconstant factor in $\mathbb{Q}[T]$, and $G(\varphi, 1/2)$ is irreducible over $\mathbb{Q}$ of degree 50; hence G is irreducible in $\mathbb{Q}[\varphi, T]$. The image of $\mathcal{X}'$ under (φ, t) is the curve $G = 0$, on which φ has degree $\deg_T G = 14$, as on $\mathcal{X}'$. Therefore $(\varphi, t) \colon \mathcal{X}' \to \{G = 0\}$ is birational (and $\mathcal{X}'$ is irreducible), and t has degree $\deg_\varphi G = 50$. At a point (φ_0, t_0) of $G = 0$ where $\partial G/\partial T \neq 0$, the plane curve is smooth, exactly one point Q of $\mathcal{X}'$ lies over it, $\varphi - \varphi_0$ is a uniformizer at Q, and the multiplicity of φ_0 as a root of $G(\varphi, t_0)$ is the ramification index $e_Q(t)$. Factorization over $\mathbb{Q}$ gives

$$G(\varphi, 0) = c_0\, h_0^5, \qquad G(\varphi, 1) = c_1\,(\varphi - \tfrac{204}{25})\, h_1^7,$$
$$(T^{14} G(\varphi, 1/T))\big|_{T=0} = c_\infty\, h_2\, h_3^3 h_4^3,$$

with $c_0, c_1, c_\infty \in \mathbb{Q}^\times$ and $h_0, \ldots, h_4 \in \mathbb{Q}[\varphi]$ irreducible of degrees $10, 7, 2, 8, 8$, each prime to the corresponding specialization of $\partial G/\partial T$ (for $t = \infty$, of the T-derivative of $T^{14}G(\varphi, 1/T)$). These fibres have total degree 50 in φ, so no point over 0, 1, ∞ lies on $y_0 = 0$, and the ramification profiles are as stated. They contribute $40 + 42 + 32 = 114 = 2 \cdot 8 - 2 + 2 \cdot 50$ to the Riemann–Hurwitz formula, so t is unramified over U.

(d). The monomial x_0^2 occurs in no q_i, so $P_0 \in \mathcal{X}'$. As $A_i(P_0) = B_i(P_0) \neq 0$ for every i, $t(P_0) = 1$. At P_0, $\varphi = 204/25$, the simple root of $G(\varphi, 1)$, so P_0 is the unramified point over $t = 1$. The linear parts of the q_i at P_0 in $x_2/x_0, \dots, x_7/x_0$ have rank 6, so u is a uniformizer, and solving $q_1 = \cdots = q_{15} = 0$ order by order in $\mathbb{Q}[[u]]$ gives $t - 1 = u + O(u^2)$. □

Remark 5.6 (Origin of the equations). The equations were obtained by interpolating the characteristic polynomial over $\mathbb{Q}(t)$ of a function on lines, computed 11-adically from $J_t[7]$, and then computing a canonical model. Proposition 5.5 is a statement about the equations themselves, and Proposition 5.8 identifies the curve they define with $\mathcal{X}$.

As in the proof of Proposition 4.11, $\alpha_0 \in k$ is a root of $x^2 + x - 1$, and G_0, G_1 are the matrices displayed there, G_0 depending on α_0. For $g \in \mathrm{GL}_2(k)$, $\bar{g}$ denotes the permutation $\ell \mapsto g(\ell)$ of $\mathbb{P}^1(k)$.

Lemma 5.7. *Let $g_0, g_1 \in \mathrm{SL}_2(k)$ with g_0 of order 5, $g_1 \neq 1$ unipotent, and $\mathrm{tr}(g_0 g_1) = -1$. Then there are $h \in \mathrm{GL}_2(k)$ and $\sigma \in \mathrm{Gal}(k/\mathbb{F}_7)$ with $h\,\sigma(g_0)\,h^{-1} = G_0$ and $h\,\sigma(g_1)\,h^{-1} = G_1$. In particular the pairs of permutations $(\bar{g}_0, \bar{g}_1)$ and $(\bar{G}_0, \bar{G}_1)$ of $\mathbb{P}^1(k)$ are simultaneously conjugate in the symmetric group of $\mathbb{P}^1(k)$.*

Proof. The eigenvalues of g_0 are $\zeta^{\pm 1}$ with ζ a primitive fifth root of unity in $\mathbb{F}_{49^2}$, so $\alpha = \mathrm{tr}\, g_0 = \zeta + \zeta^{-1}$ satisfies $\alpha^2 + \alpha - 1 = 0$, and $\alpha \in \{\alpha_0, \sigma_7(\alpha_0)\}$ with σ_7 the Frobenius of k. Replacing (g_0, g_1) by $(\sigma_7(g_0), \sigma_7(g_1))$, which satisfies the same hypotheses, we may assume $\alpha = \alpha_0$. As all nontrivial unipotent elements of $\mathrm{SL}_2(k)$ are conjugate under $\mathrm{GL}_2(k)$, we may also assume $g_1 = G_1$. Write $g_0 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then $a + d = \alpha_0$ and $ad - bc = 1$, and the condition $-1 = \mathrm{tr}(g_0 G_1) = a + c + d$ gives $c = -1 - \alpha_0$, which is nonzero as -1 is not a root of $x^2 + x - 1$. Conjugation by $\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right)$, which commutes with G_1, replaces a by $a + yc$. With $y = -a/c$ we get $a = 0$, $d = \alpha_0$ and $b = -1/c = (1 + \alpha_0)^{-1}$, that is, $g_0 = G_0$. The last assertion holds because $\mathrm{GL}_2(k)$ and σ_7 act on $\mathbb{P}^1(k)$ by permutations. □

Proposition 5.8 (Identification with $\mathcal{X}$)**.** *There is exactly one isomorphism $\mathcal{X}' \simeq \mathcal{X}$ over $\overline{\mathbb{Q}}$ that commutes with the maps t to $\mathbb{P}^1$, and it is defined over $\mathbb{Q}$.*

Proof. Let $b = 1/2$, and let γ_0, γ_1 be the anticlockwise circles of radius $1/2$ about 0 and 1, based at b. They generate the free group $\pi_1(U(\mathbb{C}), b)$. Each encircles exactly one of the points 0 and 1, and $\gamma_0\gamma_1$ is homotopic in $U(\mathbb{C})$ to a loop encircling both, that is, to a loop around ∞. For a connected finite cover $V \to U(\mathbb{C})$ and $i = 0, 1$, we write τ_i for the monodromy permutation of the fibre V_b given by path lifting along γ_i (the subscript distinguishes it from the covering involution τ of C).

The curve $\mathcal{X}$. Parallel transport along γ_0, γ_1 in $J_t[7]$ gives $g_0, g_1 \in \mathrm{SL}_2(k)$ (in a k-basis of the fibre over b), and τ_0, τ_1 for $\mathcal{X}^\circ$ are $\bar{g}_0, \bar{g}_1$. By Proposition 4.11, g_0 is conjugate to the local monodromy at 0, which has order 5, and g_1 to the local monodromy at 1, a nontrivial unipotent element. Transport along $\gamma_0\gamma_1$, which is $g_1 g_0$ or $g_0 g_1$ according to the composition convention, is conjugate to the inverse of the local monodromy at ∞. Either way $\mathrm{tr}(g_0 g_1) = \mathrm{tr}(G_\infty^{-1}) = -1$. By Lemma 5.7, (τ_0, τ_1) is simultaneously conjugate to $(\bar{G}_0, \bar{G}_1)$.

The curve $\mathcal{X}'$. For $\mathcal{X}'^\circ = t^{-1}(U)$ we computed (τ_0, τ_1) by following the 50 roots φ of $G(\varphi, t)$ (Proposition 5.5) as t runs along γ_0 and γ_1, with a rigorous enclosure of each root at every step (Appendix E.3). As (φ, t) is birational and these roots remain simple along both paths, they label the points of $\mathcal{X}'$ over t. The permutations τ_0, τ_1 and $\tau_0\tau_1$ (first τ_0, then τ_1) have cycle types 5^{10}, $1 \cdot 7^7$ and $1^2 \cdot 3^{16}$ and generate a group of order 58800, and there is a bijection $\beta\colon \mathcal{X}'_b \to \mathbb{P}^1(k)$ with $\beta\tau_i\beta^{-1} = \bar{G}_i$ for $i = 0, 1$ (for either choice of α_0). The permutations and β are printed in Table 17.

Isomorphism over $\mathbb{C}$. By the Riemann existence theorem [28, Exp. XII, Théorème 5.1], connected finite étale covers of $U_{\mathbb{C}}$ are classified by the transitive actions of $\pi_1(U(\mathbb{C}), b)$ on their fibres, which are determined by (τ_0, τ_1). Hence $\mathcal{X}'^{\circ}_{\mathbb{C}} \simeq \mathcal{X}^{\circ}_{\mathbb{C}}$ over $U_{\mathbb{C}}$, and the isomorphism extends to the smooth projective curves. Its graph is an irreducible component of $\mathcal{X}'_{\mathbb{C}} \times_{\mathbb{P}^1} \mathcal{X}_{\mathbb{C}}$ that maps birationally onto both factors. As irreducible components of schemes of finite type over the algebraically closed field $\overline{\mathbb{Q}}$ stay irreducible over $\mathbb{C}$, with the same degrees over the factors, this component is the base change of such a component of $\mathcal{X}'_{\overline{\mathbb{Q}}} \times_{\mathbb{P}^1} \mathcal{X}_{\overline{\mathbb{Q}}}$, which is the graph of an isomorphism $\mathcal{X}'_{\overline{\mathbb{Q}}} \simeq \mathcal{X}_{\overline{\mathbb{Q}}}$ over $\mathbb{P}^1$.

Uniqueness and descent. Two such isomorphisms differ by an automorphism of $\mathcal{X}_{\overline{\mathbb{Q}}}$ over $\mathbb{P}^1$, that is, a permutation of $\mathbb{P}^1(k)$ commuting with the monodromy group $\mathrm{PSL}_2(k)$. Such an automorphism is trivial: the centralizer of a transitive permutation group Γ is isomorphic to $N_\Gamma(\Gamma_\ell)/\Gamma_\ell$ for a point stabilizer Γ_ℓ, and here $\Gamma = \mathrm{PSL}_2(k)$ and Γ_ℓ is a Borel subgroup, which is its own normalizer. So the isomorphism $\iota\colon \mathcal{X}'_{\overline{\mathbb{Q}}} \to \mathcal{X}_{\overline{\mathbb{Q}}}$ is unique. The curve $\mathcal{X}'$ and its map t are defined over $\mathbb{Q}$ by construction, and $\mathcal{X}$ and its map t by Lemma 4.10, so $\sigma(\iota)$ is again such an isomorphism for every $\sigma \in G_{\mathbb{Q}}$. Hence $\sigma(\iota) = \iota$, and ι is defined over $\mathbb{Q}$. □

5.4. **The fibre of the parity cover over the cusp.** From now on we identify $\mathcal{X}$ with $\mathcal{X}'$. Let D_{x_0} be the hyperplane divisor $\{x_0 = 0\}$ on $\mathcal{X}$, of degree 14. The point $P_0 = (1 : 0 : \cdots : 0) \in \mathcal{X}(\mathbb{Q})$ is the unique unramified point over $t = 1$ (Proposition 5.5(d)), and it corresponds to the fixed line of the unipotent local monodromy at $t = 1$. We call P_0 the *rational cusp*.

Lemma 5.9. *The group G_K fixes the two points of $\mathcal{Z}$ over the rational cusp P_0, and every $g \in G_{\mathbb{Q}} \smallsetminus G_K$ interchanges them. Consequently C has exactly two points over P_0, and both are rational.*

Proof. Let $L = \mathbb{Q}((s))$ with $s = t - 1$, and $I_L \subset G_L$ its inertia group, so that $G_L/I_L = G_{\mathbb{Q}}$. As $\mathcal{X} \to \mathbb{P}^1$ is unramified at the rational point P_0, a unique L-point x_L of $\mathcal{X}$ over $t = 1 + s$ specializes to P_0. As $\mathcal{Z} \to \mathcal{X}$ is finite étale, the fibre of $\mathcal{Z}$ over x_L is an étale L-algebra of degree 2 which extends over $\mathbb{Q}[[s]]$ and reduces to the fibre over P_0. So it suffices to compute the action of G_L on the two classes of $H_L \smallsetminus \{0\}$ modulo $(k^\times)^2$, where $H_L \subset J_t[7](\overline{L})$ is the line of x_L.

As in the proof of Lemma 4.5(c), the fibre of (4.2) at $t = 1$ is the rational curve $y^2 = (x^2 - x - 1)^2(5x^2 - 2x + 1)$, with two ordinary nodes at the roots ρ, ρ' of $x^2 - x - 1$. The model defined by (4.2) over $\mathbb{Q}[[s]]$, a surface, is regular at the nodes, as the t-derivative $4(5\rho + 3)$ of the right-hand side does not vanish there. So, by [7, §9.5, Theorem 4], J_t has semistable reduction over L with a torus T of dimension 2, and by [27, Exp. IX, §12] the character group $\mathrm{X}(T)$ is, as a $G_{\mathbb{Q}}$-module, H_1 of the dual graph of the special fibre: one vertex and one loop for each node. An orientation of the loop at ρ is an ordering of the two branches there, which correspond to the points $(\rho, \pm\sqrt{5\rho^2 - 2\rho + 1}) = (\rho, \pm\sqrt{3(\rho + 2)})$ of the normalization $y'^2 = 5x^2 - 2x + 1$, $y' = y/(x^2 - x - 1)$. The $\mathcal{O}_K$-action extends to the Néron model and preserves the torus, so $T[7] \subset J_t[7]$ is a k-line. As inertia acts trivially on $\mathrm{X}(T)$ and on μ_7, I_L fixes $T[7] = \mathrm{Hom}(\mathrm{X}(T), \mu_7)$ pointwise, and as the unipotent local monodromy fixes a unique line, $H_L = T[7]$.

Hence G_L acts on $H_L = T[7]$ through $G_L/I_L = G_{\mathbb{Q}}$. Let $g \in G_K$. It fixes $\rho = e$ and $\rho' = 1 - e$ and acts on the two loops by the signs

$$g(\sqrt{3(e+2)})/\sqrt{3(e+2)} \qquad \text{and} \qquad g(\sqrt{3(3-e)})/\sqrt{3(3-e)},$$

both equal to $\delta(g)$, as $3(e+2) = \mathfrak{d}$, $3(3-e) = \mathfrak{d}'$ and $\mathfrak{d}\mathfrak{d}' = 45$ is a square in K. So g acts on $\mathrm{X}(T)$ by $\delta(g)$ and on $T[7]$ by the scalar $\delta(g)\chi_7(g) \in \mathbb{F}_7^\times \subset (k^\times)^2$, and fixes both classes. Now let $g \in G_{\mathbb{Q}} \smallsetminus G_K$. It acts on $T[7]$ semilinearly with respect to the Frobenius of k (see the proof of Lemma 4.10), say $g(v) = \alpha v$ for a generator v of $T[7]$. As in the proof of Lemma 5.2, $g^2 \in G_K$ acts by $\alpha^8 = \mathrm{N}_{k/\mathbb{F}_7}(\alpha)$, which by the previous step is $\delta(g^2)\chi_7(g)^2$, with $\delta(g^2) = -1$. As -1 is not a square in $\mathbb{F}_7$, α is not a square in k, and g interchanges the two classes.

Thus the fibre of $\mathcal{Z}$ over P_0 is $\operatorname{Spec} K$, and after the twist by the quadratic character of $K/\mathbb{Q}$ every element of $G_{\mathbb{Q}}$ acts trivially on it: the fibre of C over P_0 consists of two rational points. □

Proposition 5.10 (The double cover)**.** *Let $r = r_0/x_0^2$. Then*

$$\operatorname{div}(r) = 12P_0 + 2E_c - 2D_{x_0}, \qquad r = (t-1)^{12}(1 + O(t-1)) \text{ at } P_0, \tag{5.2}$$

where E_c is an effective divisor of degree 8 defined over $\mathbb{Q}$, consisting of eight distinct points of $\mathcal{X}(\overline{\mathbb{Q}})$ different from P_0. The smooth projective curve C' with function field $\mathbb{Q}(\mathcal{X})(w)$, $w^2 = r$, is a geometrically connected unramified double cover of $\mathcal{X}$ of genus 15, with exactly two points over P_0, both rational; we call them Q_0 and Q_1, where $w/(t-1)^6$ takes the value 1 at Q_0 and -1 at Q_1. If C' and C are isomorphic as double covers of $\mathcal{X}$ over $\overline{\mathbb{Q}}$, then they are isomorphic over $\mathbb{Q}$.

Proof. In the affine chart $x_0 = 1$, where $u = x_1$, the points of E_c are $(1 : u : g_2(u) : \cdots : g_7(u))$ with $m(u) = 0$, for an irreducible $m \in \mathbb{Q}[u]$ of degree 8 with $m(0) \neq 0$ and $g_2, \dots, g_7 \in \mathbb{Q}[u]$ of degree at most 7, which are given in the supplementary data [31]. All q_i and r_0 vanish at these points, as their values are divisible by m. Over the field $\mathbb{Q}[u]/(m)$ the Jacobian matrix of $(q_1, \dots, q_{15})$ with respect to $x_1, \dots, x_7$ has rank 6, also with the gradient of r_0 appended, so r_0 vanishes to order at least 2 at each of the eight points. At P_0, let $x_2(u), \dots, x_7(u) \in \mathbb{Q}[[u]]$ be the expansions of the coordinates found in the proof of Proposition 5.5(d). Then $r_0(1, u, x_2(u), \dots, x_7(u)) = u^{12} + O(u^{13})$ and $t - 1 = u + O(u^2)$, so $r = (t-1)^{12}(1 + O(t-1))$. As r_0 restricted to $\mathcal{X}$ is a section of $\mathcal{O}(2)$, of degree $28 = 12 + 2 \cdot 8$, these are all its zeros, which gives (5.2).

Every multiplicity in (5.2) is even, so $w^2 = r$ is unramified over $\mathcal{X}$, and Riemann–Hurwitz gives genus $2 \cdot 8 - 1 = 15$. The curve C' is geometrically connected. Otherwise $[6P_0 + E_c - D_{x_0}]$ would be trivial, and as this divisor is defined over $\mathbb{Q}$, Hilbert's Theorem 90 would give $r = cf^2$ with $c \in \mathbb{Q}^\times$ and $f \in \mathbb{Q}(\mathcal{X})$ (a function over $\overline{\mathbb{Q}}$ whose divisor is defined over $\mathbb{Q}$ is a constant multiple of one defined over $\mathbb{Q}$). The expansion at P_0 forces $c \in \mathbb{Q}^{\times 2}$, so r would be a square in $\mathbb{Q}(\mathcal{X})$. Then $r = r_0/x_0^2$ would take square values at the $\mathbb{F}_{13}$-points of the reduction of $\mathcal{X}$ modulo 13 (see the proof of Proposition 5.5(a)) where it is a unit. This contradicts Proposition D.1, where r_0 takes the nonsquare values $2, 7, 8$ at points with $x_0 = 1$. As r has even order 12 at P_0 with leading coefficient 1 with respect to $t - 1$, the two points over P_0 are rational.

If C' and C are isomorphic over $\overline{\mathbb{Q}}$ as double covers of $\mathcal{X}$, their classes in $H^1(\mathcal{X}, \mu_2)$ have the same image in $H^1(\mathcal{X}_{\overline{\mathbb{Q}}}, \mu_2)$, so they differ by a class from $H^1(\mathbb{Q}, \mu_2) = \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, and $C' \simeq C^{(d)}$ for some $d \in \mathbb{Q}^\times$. As the fibre of C over P_0 consists of two rational points (Lemma 5.9), that of $C^{(d)}$ is $\operatorname{Spec} \mathbb{Q}[w]/(w^2 - d)$, which consists of two rational points, as that of C' does, only if $d \in \mathbb{Q}^{\times 2}$. Hence $C' \simeq C$ over $\mathbb{Q}$. □

Lemma 5.11 (Comparison at 11)**.** *Let $\mathcal{X}_{\mathbb{Z}_{11}} \subset \mathbb{P}^7_{\mathbb{Z}_{11}}$ be the closed subscheme defined by $q_1, \dots, q_{15}$, whose coefficients are 11-integral, and let $\mathcal{X}_{\mathbb{F}_{11}}$ be its special fibre.*

(a) *$\mathcal{X}_{\mathbb{Z}_{11}}$ is smooth and proper over $\mathbb{Z}_{11}$ with generic fibre $\mathcal{X} \otimes \mathbb{Q}_{11}$, and $\mathcal{X}_{\mathbb{F}_{11}}$ is a smooth geometrically connected curve of genus 8. The map t extends to a finite flat morphism $t\colon \mathcal{X}_{\mathbb{Z}_{11}} \to \mathbb{P}^1_{\mathbb{Z}_{11}}$ of degree 50.*

(b) *The form r_0 is 11-integral, and its reduction $\bar{r}_0$ does not vanish identically on $\mathcal{X}_{\mathbb{F}_{11}}$. The normalization $C'_{\mathbb{Z}_{11}}$ of $\mathcal{X}_{\mathbb{Z}_{11}}$ in the function field of $C' \otimes \mathbb{Q}_{11}$ is finite étale of degree 2 over $\mathcal{X}_{\mathbb{Z}_{11}}$, and its special fibre is the étale double cover of $\mathcal{X}_{\mathbb{F}_{11}}$ given by $w^2 = \bar{r}_0/x_0^2$.*

(c) *C' and C are isomorphic as double covers of $\mathcal{X}$ over $\overline{\mathbb{Q}}$.*

Consequently $C' \simeq C$ over $\mathbb{Q}$, and $C'_{\mathbb{Z}_{11}} \to \mathcal{X}_{\mathbb{Z}_{11}}$ is a smooth proper model over $\mathbb{Z}_{11}$ of the double cover $C \to \mathcal{X}$; in particular $\mathcal{X}$ and C have good reduction at 11.

Proof. Here a bar denotes reduction modulo 11, and $U_{\mathbb{Z}_{11}} = \mathbb{P}^1_{\mathbb{Z}_{11}} \smallsetminus \{0, 1, \infty\}$. As $5 \equiv 4^2 \pmod{11}$, we fix an embedding $K \subset \mathbb{Q}_{11}$.

The model. A Gröbner basis of $\bar{I} = (\bar{q}_1, \dots, \bar{q}_{15})$ over $\mathbb{F}_{11}$ (degree reverse lexicographic order, $x_0 > \cdots > x_7$) consists of fifteen quadrics, five cubics and one quartic, and $\mathbb{F}_{11}[x]/\bar{I}$ has Hilbert series $(1 + 6T + 6T^2 + T^3)/(1 - T)^2$, as over $\mathbb{Q}$. The ideal $\bar{I} + (x_0, x_1)$ has colength 14, equal to the degree, so $\mathbb{F}_{11}[x]/\bar{I}$ is Cohen–Macaulay of dimension 2, $\mathcal{X}_{\mathbb{F}_{11}}$ is of pure dimension 1, and $H^0(\mathcal{X}_{\mathbb{F}_{11}}, \mathcal{O}) = \mathbb{F}_{11}$. For three pairs of matrices over $\mathbb{F}_{11}$ listed in the supplementary data [31], the determinants formed as in the proof of Proposition 5.5(a) generate with $\bar{I}$ an ideal of Krull dimension 0. With these data the argument of the proof of Proposition 5.5(a), including the appeal to [53, Tag 01V9], applies with 11 in place of 13: $\mathcal{X}_{\mathbb{Z}_{11}}$ is flat, projective and smooth over $\mathbb{Z}_{11}$, with generic fibre $\mathcal{X} \otimes \mathbb{Q}_{11}$ and special fibre the smooth curve $\mathcal{X}_{\mathbb{F}_{11}} = V(\bar{I})$, of genus 8 as $\chi(\mathcal{O}) = -7$. The reduced Gröbner basis of I over $\mathbb{Q}$ is 11-integral and reduces to that of $\bar{I}$, so for every d the standard monomials of degree d form a $\mathbb{Z}_{11}$-basis of $H^0(\mathcal{X}_{\mathbb{Z}_{11}}, \mathcal{O}(d))$.

The map t. We argue as in the proof of Lemma 7.2 below, with 11 in place of 13. Here $H_5 = H^0(\mathcal{X}_{\mathbb{Z}_{11}}, \mathcal{O}(5))$ is free of rank 63, and $V_{\mathbb{Z}_{11}} = (V \otimes \mathbb{Q}_{11}) \cap H_5^{\oplus 2}$ with V the $\mathbb{Q}$-span of the pairs (A_i, B_i). The image in $H_5^{\oplus 2}$ of each primitive integral pair (A_i, B_i) is divisible by 11 exactly once (its normal form has content of 11-adic valuation 1), and the reductions of the thirteen pairs $11^{-1}(A_i, B_i)$ span a space of dimension only 12. Replacing one of them by 11^{-1} times a suitable integral combination of all of them gives thirteen pairs in $V_{\mathbb{Z}_{11}}$, again written (A_i, B_i), with linearly independent reductions $(\bar{A}_i, \bar{B}_i)$, hence a basis of $V_{\mathbb{Z}_{11}}$. These reductions satisfy $\bar{A}_i\bar{B}_j \equiv \bar{A}_j\bar{B}_i \pmod{\bar{I}}$, and with $\bar{I}$ the twenty-six forms $\bar{A}_i, \bar{B}_i$ generate an ideal of Krull dimension 0. So the morphisms $(A_i : B_i)$ glue to a morphism $t\colon \mathcal{X}_{\mathbb{Z}_{11}} \to \mathbb{P}^1_{\mathbb{Z}_{11}}$ extending t, finite and flat of degree 50 because $\bar{t}$ is not constant: its fibres $\bar{I} + (\bar{A}_i)_i$, $\bar{I} + (\bar{A}_i - \bar{B}_i)_i$ and $\bar{I} + (\bar{B}_i)_i$ over 0, 1 and ∞ are finite of degree 50, with 10, 8 and 18 geometric points. This proves (a).

The cover C'. The form r_0 is 11-integral, and its normal form modulo the Gröbner basis has a coefficient prime to 11, so $\bar{r}_0 \notin \bar{I}$. Hence $r = r_0/x_0^2$ and 2 are units in the discrete valuation ring of $\mathcal{X}_{\mathbb{Z}_{11}}$ at the generic point of $\mathcal{X}_{\mathbb{F}_{11}}$, where $C'_{\mathbb{Z}_{11}} \to \mathcal{X}_{\mathbb{Z}_{11}}$ is therefore étale. It is étale over the generic fibre by Proposition 5.10, hence at all points of codimension 1, and so, by purity of the branch locus [28, Exp. X, Théorème 3.1], everywhere. Its special fibre is the étale double cover of $\mathcal{X}_{\mathbb{F}_{11}}$ given by $w^2 = \bar{r}$ at the generic point. For a closed point P of $\mathcal{X}_{\mathbb{F}_{11}}$ with residue field κ and an integral linear form y with $\bar{y}(P) \neq 0$, $r_0/y^2 = r(x_0/y)^2$ also defines C'. If $\bar{r}_0(P) \neq 0$, then r_0/y^2 is a unit near P, and the fibre of $C'_{\mathbb{F}_{11}}$ over P is split exactly when $\bar{r}_0(P)$ is a square in κ, whatever the homogeneous coordinates of P, as r_0 has even degree. If $\bar{r}_0(P) = 0$, then $\bar{r}_0/\bar{y}^2$ has even order at P, the cover being étale, and the

fibre is split exactly when its leading coefficient in a local parameter at P is a square in κ. This proves (b).

The parity cover over U. Over $U_{\mathbb{Z}_{11}}$ the curve (4.2) is smooth, as its leading coefficient 5 and its discriminant $2^{12} \cdot 3^6 \cdot 5^5\, t^8 (t-1)^2$ are units. So its Jacobian is an abelian scheme over $U_{\mathbb{Z}_{11}}$, and the 7-torsion $\mathcal{J}$ of this Jacobian is finite étale over $U_{\mathbb{Z}_{11}}$. As $U_{\mathbb{Z}_{11}}$ is normal and connected, the fundamental group of its generic point surjects onto $\pi_1(U_{\mathbb{Z}_{11}})$ [28, Exp. V, Proposition 8.2]. Hence a morphism between finite étale $U_{\mathbb{Z}_{11}}$-schemes is determined by its restriction to the generic point, and every morphism between these restrictions extends. Thus the action of $k = \mathcal{O}_K/(7)$ on $\mathcal{J} \otimes \mathbb{Q}_{11}$ given by Proposition 4.1 extends to $\mathcal{J}$, and the Weil pairing on $\mathcal{J}$ is the trace of a k-bilinear alternating pairing e_k, as over $\mathbb{Q}_{11}$ (Section 4.1). The quotients $\mathcal{X}^\circ_{\mathbb{Z}_{11}} = (\mathcal{J} \smallsetminus \{0\})/k^\times$ and $\mathcal{Z}^\circ_{\mathbb{Z}_{11}} = (\mathcal{J} \smallsetminus \{0\})/(k^\times)^2$ are finite étale over $U_{\mathbb{Z}_{11}}$, of degrees 50 and 100, with generic fibres $\mathcal{X}^\circ \otimes \mathbb{Q}_{11}$ and $\mathcal{Z}^\circ \otimes \mathbb{Q}_{11}$. They are normal, and irreducible: each connected component is finite étale over the connected scheme $U_{\mathbb{Z}_{11}}$, so it meets the generic fibre, which is connected (for $\mathcal{Z}^\circ_{\mathbb{Z}_{11}}$ because the monodromy group $\mathrm{SL}_2(k)$ of Proposition 4.11 is transitive on nonzero vectors, so $\mathcal{Z}$ is geometrically connected). Also $t^{-1}(U_{\mathbb{Z}_{11}}) \subset \mathcal{X}_{\mathbb{Z}_{11}}$ is finite over $U_{\mathbb{Z}_{11}}$ by (a), normal as it is smooth over $\mathbb{Z}_{11}$, and irreducible as it is flat over $\mathbb{Z}_{11}$ with irreducible generic fibre. A normal integral scheme finite over $U_{\mathbb{Z}_{11}}$ is the normalization of $U_{\mathbb{Z}_{11}}$ in its function field (for $\mathcal{X}^\circ_{\mathbb{Z}_{11}}$ see also [28, Exp. I, Corollaire 10.2]), and the two function fields are identified over $\mathbb{Q}_{11}(t)$ by Proposition 5.8. Therefore the isomorphism of Proposition 5.8 extends to $t^{-1}(U_{\mathbb{Z}_{11}}) \simeq \mathcal{X}^\circ_{\mathbb{Z}_{11}}$ over $U_{\mathbb{Z}_{11}}$. It follows that the normalization $\mathcal{Z}_{\mathbb{Z}_{11}}$ of $\mathcal{X}_{\mathbb{Z}_{11}}$ in the function field of $\mathcal{Z} \otimes \mathbb{Q}_{11}$ is $\mathcal{Z}^\circ_{\mathbb{Z}_{11}}$ over $t^{-1}(U_{\mathbb{Z}_{11}})$, which is finite étale over $\mathcal{X}^\circ_{\mathbb{Z}_{11}}$. By Lemma 5.1, $\mathcal{Z}_{\mathbb{Z}_{11}}$ is also étale over the generic fibre. The remaining points, the closed points of $\mathcal{X}_{\mathbb{F}_{11}}$ over $\bar{t} \in \{0, 1, \infty\}$, have codimension 2, so, by purity [28, Exp. X, Théorème 3.1], $\mathcal{Z}_{\mathbb{Z}_{11}}$ is a finite étale double cover of $\mathcal{X}_{\mathbb{Z}_{11}}$. As $\sqrt{5} \in \mathbb{Q}_{11}$, the twist by $\mathbb{Q}(\sqrt{5})$ is trivial over $\mathbb{Q}_{11}$, and $C \otimes \mathbb{Q}_{11} \simeq \mathcal{Z} \otimes \mathbb{Q}_{11}$ as double covers of $\mathcal{X} \otimes \mathbb{Q}_{11}$.

Points and fibres over $\mathbb{F}_q$. Let $q = 11^n$, $t_0 \in \mathbb{F}_q \smallsetminus \{0, 1\}$, and Fr the q-power Frobenius endomorphism of the Jacobian J_{t_0} of H_{t_0} over $\mathbb{F}_q$. On $J_{t_0}[7] = \mathcal{J}_{t_0}(\overline{\mathbb{F}}_{11})$ it acts as the arithmetic Frobenius. By the preceding paragraph, the points $P \in \mathcal{X}_{\mathbb{F}_{11}}(\mathbb{F}_q)$ over t_0 correspond bijectively to the Fr-stable lines $H \subset J_{t_0}[7]$, and the two geometric points of the special fibre $\mathcal{Z}_{\mathbb{F}_{11}}$ of $\mathcal{Z}_{\mathbb{Z}_{11}}$ over P to the two classes of $H \smallsetminus \{0\}$ modulo $(k^\times)^2$. If Fr acts on H by $\lambda_H \in k^\times$, it fixes these classes if $\lambda_H \in (k^\times)^2$ and swaps them otherwise. So the fibre of $\mathcal{Z}_{\mathbb{F}_{11}}$ over P is split if and only if $\varepsilon(\lambda_H) = 1$, with $\varepsilon\colon k^\times \to \{\pm 1\}$ the quadratic character.

Frobenius on a fibre. In this paragraph and the next, a bar on an integer denotes its image in $\mathbb{F}_7$. Let $T^4 - s_1 T^3 + s_2 T^2 - q s_1 T + q^2$ be the characteristic polynomial of Fr. As Fr commutes with k and $e_k(\mathrm{Fr}\, x, \mathrm{Fr}\, y) = q\, e_k(x, y)$ (the Weil pairing is Galois-equivariant and the trace form of $k/\mathbb{F}_7$ is nondegenerate), it acts on $J_{t_0}[7]$ k-linearly with determinant $\bar{q} \in \mathbb{F}_7^\times$. Its $\mathbb{F}_7$-linear characteristic polynomial, the reduction of the one above, is the norm to $\mathbb{F}_7[T]$ of $T^2 - cT + \bar{q}$, with $c \in k$ its k-trace. Comparing coefficients, $c + c^7 = \bar{s}_1$ and $c^8 = \bar{s}_2 - 2\bar{q}$, so c and c^7 are the roots in k of $T^2 - \bar{s}_1 T + (\bar{s}_2 - 2\bar{q})$. If $T^2 - cT + \bar{q}$ has no root in k, no line is stable. If it has two distinct roots λ_1, λ_2, exactly the two eigenlines are stable, and $\varepsilon(\lambda_1) = \varepsilon(\lambda_2)$ as $\lambda_1 \lambda_2 = \bar{q} \in \mathbb{F}_7^\times \subset (k^\times)^2$. If it has a double root λ, one line or all 50 are stable, all with eigenvalue λ, and $\varepsilon(\lambda) = \lambda^{24} = \bar{q}^{12} = 1$. So all stable lines have the same value ε_{t_0} of $\varepsilon(\lambda_H)$, unchanged if c is replaced by c^7, which replaces the eigenvalues by their seventh powers. Thus $\mathcal{X}_{\mathbb{F}_{11}}(\mathbb{F}_q)$ has 0 points, 2 points, or either 1 or 50 points over t_0, according as $T^2 - cT + \bar{q}$ has no root, two roots or a double root in k, and the fibre of $\mathcal{Z}_{\mathbb{F}_{11}}$ over each of them is split if and only if $\varepsilon_{t_0} = 1$.

The computation. Take $q = 11^3 = 1331$, the smallest power of 11 for which the estimate in the conclusion below is decisive. The set $\mathcal{X}_{\mathbb{F}_{11}}(\mathbb{F}_q)$ has 1278 points, at each of which we computed $\bar{t}$ and $\bar{r}_0$ (Appendix E.4): none lies over $\bar{t} = 0$, eight lie over $\bar{t} = 1$ (among them $\overline{P_0}$), two over $\bar{t} = \infty$, and 1268 over $U(\mathbb{F}_q)$. For each of the 1329 values $t_0 \in \mathbb{F}_q \smallsetminus \{0, 1\}$ we computed the characteristic polynomial of Frobenius of J_{t_0} and ε_{t_0}: $T^2 - cT + \bar{q}$ has no root in k for 719 of them, two roots for 560 and a double root for 50. In the last case the fibre has 1 point in 48 instances and 50 points in the other 2 ($t_0 = 6, 9 \in \mathbb{F}_{11}$, where Fr acts on $J_{t_0}[7]$ as -1). In each of the 1329 fibres the number of points of $\mathcal{X}_{\mathbb{F}_{11}}(\mathbb{F}_q)$ agrees with this prediction. At 1264 of the 1268 points over $U(\mathbb{F}_q)$, $\bar{r}_0 \neq 0$ and the quadratic character of $\bar{r}_0(P)$ is $\varepsilon_{\bar{t}(P)}$. The other four are reductions of points of E_c (one over $u = 4$, rational over $\mathbb{F}_{11}$, and three conjugate ones over the roots of $u^3 - 5u^2 - 5u + 4$); at each, $\bar{r}_0$ vanishes to order exactly 2, and the quadratic character of its leading coefficient in a local parameter is again $\varepsilon_{\bar{t}(P)}$.

Conclusion. Let $\psi\colon \pi_1(\mathcal{X}_{\mathbb{F}_{11}}) \to \{\pm 1\}$ be the product of the characters of the étale double covers $\mathcal{Z}_{\mathbb{F}_{11}}$ and $C'_{\mathbb{F}_{11}}$ of $\mathcal{X}_{\mathbb{F}_{11}}$, and Frob_P the q-power Frobenius at P. By the descriptions of the fibres above and the computation, $\psi(\mathrm{Frob}_P) = 1$ at the 1268 points $P \in \mathcal{X}_{\mathbb{F}_{11}}(\mathbb{F}_q)$ over $U(\mathbb{F}_q)$, and $\psi(\mathrm{Frob}_P) = \pm 1$ at the other ten. Hence

$$\sum_{P \in \mathcal{X}_{\mathbb{F}_{11}}(\mathbb{F}_q)} \psi(\mathrm{Frob}_P) \geq 1268 - 10 = 1258.$$

If ψ were nontrivial on $\pi_1(\mathcal{X}_{\mathbb{F}_{11}} \otimes \overline{\mathbb{F}}_{11})$, the double cover $D \to \mathcal{X}_{\mathbb{F}_{11}}$ defined by ψ would be a smooth projective geometrically connected curve of genus 15, and the sum would be $\#D(\mathbb{F}_q) - \#\mathcal{X}_{\mathbb{F}_{11}}(\mathbb{F}_q) = -\sum_{i=1}^{14} \beta_i$. Here $\beta_1, \ldots, \beta_{14}$ are the eigenvalues of Frobenius on the (-1)-eigenspace of the covering involution in $H^1(D \otimes \overline{\mathbb{F}}_{11}, \mathbb{Q}_\ell)$, for a prime $\ell \neq 11$, that is, on the Tate module of the Prym variety of D over $\mathcal{X}_{\mathbb{F}_{11}}$. By Weil's theorem [56], $|\beta_i| = \sqrt{q}$, so the sum would be at most $14\sqrt{1331} < 511$ in absolute value, a contradiction. So ψ factors through $\mathrm{Gal}(\overline{\mathbb{F}}_{11}/\mathbb{F}_{11})$, and $\psi(\mathrm{Frob}_P) = \psi(\mathrm{Frob}_{11})^3 = \psi(\mathrm{Frob}_{11})$ for every $P \in \mathcal{X}_{\mathbb{F}_{11}}(\mathbb{F}_q)$. As this is 1 at some such P, ψ is trivial, and $\mathcal{Z}_{\mathbb{F}_{11}} \simeq C'_{\mathbb{F}_{11}}$ as double covers of $\mathcal{X}_{\mathbb{F}_{11}}$. As $\mathcal{X}_{\mathbb{Z}_{11}}$ is proper over the complete local ring $\mathbb{Z}_{11}$, restriction to the special fibre is an equivalence between the categories of finite étale covers of $\mathcal{X}_{\mathbb{Z}_{11}}$ and of $\mathcal{X}_{\mathbb{F}_{11}}$ [28, Exp. IX, Théorème 1.10]. Therefore $\mathcal{Z}_{\mathbb{Z}_{11}} \simeq C'_{\mathbb{Z}_{11}}$ over $\mathcal{X}_{\mathbb{Z}_{11}}$, and on generic fibres $C \otimes \mathbb{Q}_{11} \simeq \mathcal{Z} \otimes \mathbb{Q}_{11} \simeq C' \otimes \mathbb{Q}_{11}$. Let D' be the étale double cover of $\mathcal{X} \otimes \overline{\mathbb{Q}}$ whose class in $H^1(\mathcal{X} \otimes \overline{\mathbb{Q}}, \mu_2)$ is the sum of those of C and C'; its base change to an algebraic closure $\overline{\mathbb{Q}}_{11} \supset \overline{\mathbb{Q}}$ is split. If D' were connected, it would be a proper connected smooth curve over the algebraically closed field $\overline{\mathbb{Q}}$, so $H^0(D', \mathcal{O}) = \overline{\mathbb{Q}}$ and $D' \otimes \overline{\mathbb{Q}}_{11}$ would be connected. Hence D' is split, which is (c). By the last assertion of Proposition 5.10, $C' \simeq C$ over $\mathbb{Q}$, and the final statement follows from (a) and (b). □

From now on we identify C with C', and $C_{\mathbb{Z}_{11}} = C'_{\mathbb{Z}_{11}}$ is its smooth model over $\mathbb{Z}_{11}$.

6. The surface B: polarization and rank

The double cover $q\colon C \to \mathcal{X}$ of Section 5 has a Prym variety of dimension 7. Using the Weil pairing, we obtain from it an abelian surface B, which carries a polarization of type $(1, 7)$ by Proposition 6.2, and we prove by a two-descent that $\mathrm{rank}\, B(\mathbb{Q}) = 1$ (Proposition 6.13). The data used in this section are printed in Appendix C, except those too large to print, which are in the supplementary data [31].

6.1. **The correspondence and the surface.** Let $J = \mathrm{Jac}(C)$, let τ be the covering involution of $C \to \mathcal{X}$, and let

$$P = \mathrm{im}(1 - \tau) \subset J$$

be the Prym variety of the unramified double cover, of dimension $g(C) - g(\mathcal{X}) = 7$. By Mumford [41, §3, Corollary 2], the principal polarization λ_J of J restricts to twice a principal polarization λ_P on P. We write $\mathrm{AJ}_{Q_0} \colon C \to J$, $Q \mapsto [Q - Q_0]$, for the Abel–Jacobi map with base point the rational cusp Q_0 of Proposition 5.10.

By Section 5.1 and Proposition 5.3, $\mathcal{Z} = W/(k^\times)^2$ and $C = \mathcal{Z}^{(5)}$, so the geometric fibre of C over a point of U is the set of 100 classes of nonzero vectors modulo squares of scalars. Let e_k be the k-bilinear alternating pairing on $J_t[7]$ with $\mathrm{Tr}_{k/\mathbb{F}_7} \circ e_k = e_7$, the Weil pairing (Section 4.1), once μ_7 is identified with $\mathbb{F}_7$ by a primitive seventh root of unity. A different choice of root of unity multiplies e_k by an element of $\mathbb{F}_7^\times$, which is a square in k. Let $\varepsilon \colon k^\times \to \{\pm 1\}$ be the quadratic character. For classes $[v], [w]$ in a fibre on distinct lines, $\varepsilon(e_k(v, w))$ is well defined, since scaling v or w by a square does not change it.

The monodromy group $\mathrm{SL}_2(k)$ determines e_k only up to a scalar, and a nonsquare scalar interchanges the two relations $\varepsilon(e_k(v, w)) = 1$ and $\varepsilon(e_k(v, w)) = -1$ between classes in a fibre. Lemma 6.1 tells them apart by the local monodromy at $t = 1$.

Lemma 6.1 (The transvection at $t = 1$)**.** *Let $t \in U$, let $\bar{T}$ be the image in $\mathrm{SL}_k(J_t[7])$ of a generator of the local fundamental group at 1, transported to t along any path, and let $w \in J_t[7]$ with $\bar{T}w \neq w$. Then $\bar{T}$ is a transvection and*

$$\varepsilon(e_k(w, \bar{T}w)) = -1.$$

In the coordinates of Proposition 4.11, in which $G_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, one has $e_k = \lambda \det$ with $\varepsilon(\lambda) = -1$.

Proof. We work over $\mathbb{C}$, where the monodromy of $J_t[7]$ is that on $M_t = H_1(J_t(\mathbb{C}), \mathbb{Z})$ reduced modulo 7. The Riemann form $\langle\ ,\ \rangle$ of the principal polarization is alternating and unimodular on M_t, and modulo 7 it is the Weil pairing on $J_t[7] = M_t/7M_t$, up to sign and the identification of μ_7 with $\mathbb{F}_7$. The ring $\mathcal{O}_K$ acts on M_t through $[e]$ by self-adjoint endomorphisms (Proposition 4.1). As the trace form identifies the trace dual $\mathcal{O}_K^\vee = \frac{1}{\sqrt{5}}\mathcal{O}_K$ with $\mathrm{Hom}(\mathcal{O}_K, \mathbb{Z})$, there is a unique $\mathcal{O}_K$-bilinear alternating form $E \colon M_t \times M_t \to \mathcal{O}_K^\vee$ with $\mathrm{Tr}_{K/\mathbb{Q}} \circ E = \langle\ ,\ \rangle$. As $7 \nmid [\mathcal{O}_K^\vee : \mathcal{O}_K] = 5$, reduction modulo 7 identifies $\mathcal{O}_K^\vee/7\mathcal{O}_K^\vee$ with $\mathcal{O}_K/7\mathcal{O}_K = k$ compatibly with traces, so e_k is E modulo 7 up to a factor in $\mathbb{F}_7^\times$.

By the proof of Lemma 4.5, the fibre of (4.2) at $t = 1$ is irreducible with exactly two ordinary double points and normalization of genus 0, and the total space is regular at both nodes. By the Picard–Lefschetz formula [19, Exp. XV, Théorème 3.4], the local monodromy at $t = 1$ is

$$T(x) = x + \varsigma\big(\langle x, \gamma_1\rangle\gamma_1 + \langle x, \gamma_2\rangle\gamma_2\big)$$

for a sign $\varsigma = \pm 1$, with γ_1, γ_2 the two vanishing cycles. These are disjoint with connected complement in the smooth fibre, so they are part of a symplectic basis of M_t: $\Lambda = \mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2$ is a primitive isotropic sublattice and $x \mapsto (\langle x, \gamma_1\rangle, \langle x, \gamma_2\rangle)$ maps M_t onto $\mathbb{Z}^2$. Hence $\mathcal{N} = T - 1$ has image Λ, which is an $\mathcal{O}_K$-module of rank one as $\mathcal{N}$ commutes with $\mathcal{O}_K$. Thus $\Lambda = \mathcal{O}_K\gamma$ (K has class number one), and $\gamma_i = a_i\gamma$ with $\{a_1, a_2\}$ a $\mathbb{Z}$-basis of $\mathcal{O}_K$. As Λ is primitive, $\bar{T} - 1$ has image the line $k\bar{\gamma}$, where $\bar{\gamma} = \gamma \bmod 7$, so $\bar{T}$ is a transvection. With $y = E(x, \gamma) \in \mathcal{O}_K^\vee$ we have $\langle x, \gamma_i\rangle = \mathrm{Tr}(a_i y)$, so

$$\mathcal{N}(x) = \varsigma\,\Phi(y)\,\gamma, \qquad \Phi(y) = \mathrm{Tr}(a_1 y)\,a_1 + \mathrm{Tr}(a_2 y)\,a_2.$$

Since $E(\cdot,\gamma)\colon M_t \to \mathcal{O}_K^\vee$ is onto (by unimodularity of $\langle\ ,\ \rangle$ and primitivity of Λ) and $\mathcal{N}$ is $\mathcal{O}_K$-linear, $\Phi\colon \mathcal{O}_K^\vee \to \mathcal{O}_K$ is $\mathcal{O}_K$-linear: $\Phi(y) = \pi y$ with $\pi \in K^\times$. The symmetric form $(y,z) \mapsto \operatorname{Tr}(\pi yz) = \operatorname{Tr}(a_1 y)\operatorname{Tr}(a_1 z) + \operatorname{Tr}(a_2 y)\operatorname{Tr}(a_2 z)$ on $\mathcal{O}_K^\vee$ is the standard form of $\mathbb{Z}^2$ in the coordinates $y \mapsto (\operatorname{Tr}(a_1 y), \operatorname{Tr}(a_2 y))$, an isomorphism $\mathcal{O}_K^\vee \to \mathbb{Z}^2$ by trace duality. So it is positive definite and unimodular: π is totally positive, and $\mathrm{N}_{K/\mathbb{Q}}(\pi)\cdot \operatorname{disc}(\mathcal{O}_K^\vee) = 1$ with $\operatorname{disc}(\mathcal{O}_K^\vee) = \operatorname{disc}(\mathcal{O}_K)^{-1} = 1/5$, i.e. $\mathrm{N}_{K/\mathbb{Q}}(\pi) = 5$. Now let $w = x \bmod 7$ with $\bar{T}w \neq w$. Then

$$e_k(w, \bar{T}w) \equiv E(x, \mathcal{N}x) = \varsigma\pi\, E(x,\gamma)^2 = \varsigma\pi y^2 \pmod 7$$

up to a factor in $\mathbb{F}_7^\times$, and $\bar{y} = y \bmod 7 \neq 0$. As every element of $\mathbb{F}_7^\times$, in particular ς, is a square in k, $\varepsilon(e_k(w,\bar{T}w)) = \varepsilon(\bar{\pi}) = \bar{\pi}^{24} = \mathrm{N}_{k/\mathbb{F}_7}(\bar{\pi})^3 \equiv 5^3 \equiv -1 \pmod 7$. Replacing $\bar{T}$ by $\bar{T}^j$ multiplies $e_k(w,\bar{T}w)$ by $j \in \mathbb{F}_7^\times$, and conjugation by $\mathrm{SL}_2(k)$ preserves e_k, so the value does not depend on the choices. For the last assertion, $e_k = \lambda \det$ with $\lambda \in k^\times$, as $\mathrm{SL}_2(k)$ preserves both, and for $w = (a,b)$ with $b \neq 0$, $\det(w, G_1 w) = -b^2$ is a square, so $\varepsilon(\lambda) = \varepsilon(e_k(w, G_1 w)) = -1$. Bases in which the generator has matrix G_1 differ by matrices $\left(\begin{smallmatrix}\alpha & \beta \\ 0 & \alpha\end{smallmatrix}\right)$, of square determinant α^2, so $\varepsilon(\lambda)$ does not depend on the basis. □

Proposition 6.2 (The surface and its polarization)**.** *The relation* $\{([v],[w]) : \varepsilon(e_k(v,w)) = -1\}$ *on the fibres of* $C^\circ = C \times_{\mathbb{P}^1} U \to U$ *extends to a symmetric correspondence on* C *of bidegree* $(49,49)$*, defined over* $\mathbb{Q}$*, which commutes with* τ*. Its action* $\mathcal{D}$ *on* P *satisfies* $\mathcal{D}^2 = 49$*; it acts as* $+7$ *and* -7 *on abelian subvarieties* B *and* B' *of* P*, of dimensions* 2 *and* 5*, whose rational homology groups are the corresponding eigenspaces of* $\mathcal{D}$ *on* $H_1(P,\mathbb{Q})$*, and the endomorphism* $e_B = (\mathcal{D}+7)/2$ *of* P *is integral, acting as* 7 *on* B *and as* 0 *on* B'*. Writing* $i\colon B \hookrightarrow J$ *for the inclusion:*

(a) *the polarization* λ_B *induced on* B *by* λ_P *has type* $(1,7)$*, and* $i^\vee \lambda_J i = 2\lambda_B$*;*

(b) *the addition map* $B \times B' \to P$ *is an isogeny of degree* 49 *whose kernel is isomorphic to* $(\mathbb{Z}/7)^2$ *over* $\overline{\mathbb{Q}}$*;*

(c) *with base point* Q_0*, the maps*

$$f = e_B \circ (1-\tau) \circ \mathrm{AJ}_{Q_0}\colon C \longrightarrow B, \qquad \iota = i^\vee \circ \lambda_J \circ \mathrm{AJ}_{Q_0}\colon C \longrightarrow B^\vee \tag{6.1}$$

satisfy $f = \lambda_B' \circ \iota$ *with* $\lambda_B' = 7\lambda_B^{-1}\colon B^\vee \to B$*,* $\lambda_B'\lambda_B = [7]$*, and the endomorphism* $F_B = e_B(1-\tau)$ *of* J *inducing* f *satisfies* $F_B \circ i = [14]$ *on* B*.*

Proof. On a fibre over U, for fixed $[v]$, each of the other 49 lines contains exactly one class $[w]$ with $\varepsilon(e_k(v,w)) = -1$, as $e_k(v,cw) = c\, e_k(v,w)$ and ε is nontrivial. Thus both projections have degree 49, and the relation is symmetric as e_k is alternating and $\varepsilon(-1) = 1$. It is preserved by the monodromy, which acts through $\mathrm{SL}_2(k)$ and so preserves e_k. It is preserved by $G_\mathbb{Q}$: an element of $G_\mathbb{Q}$ acts on $J_t[7]$ k-semilinearly and multiplies the Weil pairing by a cyclotomic factor, so it transforms $e_k(v,w)$ into $\chi\,\mathrm{Fr}^j(e_k(v,w))$ with $\chi \in \mathbb{F}_7^\times$, Fr the Frobenius of $k/\mathbb{F}_7$ and $j \in \{0,1\}$, and $\varepsilon(\chi\,\mathrm{Fr}^j(x)) = \varepsilon(x)$. Finally, the twist by 5 changes the Galois action on the fibres by τ, which is the scalar action of a nonsquare c, and $\varepsilon(e_k(cv,cw)) = \varepsilon(c^2 e_k(v,w)) = \varepsilon(e_k(v,w))$. Hence the relation descends to $\mathbb{Q}$ and extends to the proper curve. It commutes with τ for the same reason.

On the odd functions on a fibre (those with $F \circ \tau = -F$), the correspondence acts by the matrix H with $\mathsf{H}_{ij} = -\varepsilon(e_k(v_i,v_j))$ for $i \neq j$ and $\mathsf{H}_{ii} = 0$, indexed by the 50 lines with a chosen representative v_i on each, and the complementary relation acts by $-\mathsf{H}$. For $i \neq j$, the lines other than those of v_i and v_j are spanned by vectors $v_l = c_l(av_i + v_j)$ with $a \in k^\times$, so $\varepsilon(e_k(v_i,v_l))\,\varepsilon(e_k(v_l,v_j)) = \varepsilon(c_l^2 a\, e_k(v_i,v_j)^2) = \varepsilon(a)$, which sums to zero over a.

The diagonal entries of H^2 count the 49 lines other than that of v_i, as $\varepsilon(-1) = 1$. Hence $\mathsf{H}^2 = 49I$. On the space of all functions on the fibre, the correspondence acts by a matrix $\widetilde{\mathcal{D}}$ with $\widetilde{\mathcal{D}}^2 = 49I - 24(I + \tau) + 24\,\mathbf{1}$, where $\mathbf{1}$ is the all-ones matrix. The matrix $\mathbf{1}$ acts as zero on J, and $I + \tau$ acts as zero on P. (Each class is related to 49 classes, and $[v]$ and $\tau[v]$ have no related class in common. For $[v]$, $[u]$ on distinct lines, a class related to both lies on a line $k(xv + yu)$ with $xy \neq 0$. As $e_k(v, xv + yu)\, e_k(xv + yu, u) = xy\, e_k(v, u)^2$, such a line carries one class related to both if $\varepsilon(xy) = 1$ and none otherwise, and 24 of the 48 lines have $\varepsilon(xy) = 1$.) So $\mathcal{D}^2 = 49$ on P.

Dimensions. Let V^{odd} be the rank-50 local system of odd functions on the fibres over U, and $V_\pm \subset V^{\mathrm{odd}}$ the sub-local systems on which H acts as ± 7, both of rank 25 as $\operatorname{tr}\mathsf{H} = 0$. As $C \to \mathbb{P}^1$ is finite, $H^1(C, \mathbb{Q}) = H^1(\mathbb{P}^1, j_*\rho_*\mathbb{Q})$, with $\rho\colon C^\circ \to U$ the restriction of $t \circ q$ and $j\colon U \hookrightarrow \mathbb{P}^1$, and the odd part is $H^1(P) = H^1(\mathbb{P}^1, j_*V_+) \oplus H^1(\mathbb{P}^1, j_*V_-)$, the summands being the ± 7 eigenspaces of $\mathcal{D}$. For a local system V on U without global invariants or coinvariants, $\dim H^1(\mathbb{P}^1, j_*V) = \operatorname{rank} V - \sum_{s\in\{0,1,\infty\}} \dim V^{I_s}$ by the Euler characteristic formula. At $t = 1$, G_1 fixes the two classes on its fixed line and permutes the other 98 in fourteen 7-cycles, paired by τ. Hence the G_1-invariant odd functions form an 8-dimensional space, with basis the functions $1_O - 1_{\tau O}$ for the fixed pair and for seven pairs of 7-cycles $O, \tau O$. The trace of H on this space is

$$\sum_{7 \text{ pairs}} \sum_{j=1}^{6} -\varepsilon(e_k(w, G_1^j w)) = 7 \cdot 6 \cdot (-1) \cdot (-1) = 42,$$

where the outer sum runs over the seven pairs $\{O, \tau O\}$ of 7-cycles, w is a vector whose class lies in O, and the fixed pair contributes nothing as $\mathsf{H}_{ii} = 0$. Here $\varepsilon(e_k(w, G_1^j w)) = -1$ by the last assertion of Lemma 6.1: for $w = (a, b)$ with $b \neq 0$, $\det(w, G_1^j w) = -jb^2$ is a square in k. Thus the invariants of V_+ and V_- at $t = 1$ have dimensions 7 and 1. At $t = 0$ the dimensions are 5 and 5, and at $t = \infty$ they are 9 and 9 (Lemma 6.3(d)). The global invariants vanish since $\mathrm{SL}_2(k)$ fixes no nonzero odd function. Hence $\dim H^1(\mathbb{P}^1, j_*V_+) = 25 - 5 - 9 - 7 = 4$ and $\dim H^1(\mathbb{P}^1, j_*V_-) = 25 - 5 - 9 - 1 = 10$, and B, B' are abelian subvarieties of dimensions 2 and 5.

Integral structure. By Lemma 6.3, the intersection form restricts to $H_1(P, \mathbb{Z}) = \ker(1 + \tau_*) \subset H_1(C, \mathbb{Z})$ as twice a unimodular form, which is the Riemann form of λ_P. On the saturated ± 7 eigenlattices $H_1(B, \mathbb{Z})$ and $H_1(B', \mathbb{Z})$, the Smith forms of λ_P give polarization types $(1, 7)$ and $(1, 1, 1, 1, 7)$. Moreover $H_1(P, \mathbb{Z})/(H_1(B, \mathbb{Z}) \oplus H_1(B', \mathbb{Z})) \simeq (\mathbb{Z}/7)^2$. This gives (a) and (b): the kernel of $B \times B' \to P$ is isomorphic to this quotient, and $i^\vee \lambda_J i$ is the restriction of the intersection form, $2\lambda_B$. Every entry of $\mathcal{D} + 7$ on $H_1(P, \mathbb{Z})$ is even, so $e_B = (\mathcal{D} + 7)/2$ preserves the lattice and commutes with the complex structure, hence is an endomorphism of P. Its Galois conjugates have the same double, and Hom groups of abelian varieties are torsion-free, so it is defined over $\mathbb{Q}$. Finally (c): $1 - \tau$ acts as 2 on P and e_B as 7 on B, so $F_B \circ i = [14]$. The maps $\lambda'_B\, i^\vee \lambda_J$ and $e_B(1 - \tau)$ from J to B are both $[14]$ on B (as $i^\vee \lambda_J i = 2\lambda_B$), and both vanish on B' and on $q^* \operatorname{Jac}(\mathcal{X})$, which are λ_J-orthogonal to B because $\mathcal{D}$ and τ are self-adjoint. As $B + B' + q^* \operatorname{Jac}(\mathcal{X}) = J$, the two maps agree, and composing with AJ_{Q_0} gives $f = \lambda'_B \circ \iota$. □

Lemma 6.3 (Integral homology of C)**.** *Label the* 100 *points of a fibre of $C^\circ \to U$ by* $0, \dots, 99$ *as in Appendix C.1, let $\sigma_0, \sigma_1 \in S_{100}$ be the permutations induced by G_0, G_1 of Proposition 4.11 (Table 6), and put $\sigma_\infty = \sigma_0^{-1}\sigma_1^{-1}$; in this labelling τ exchanges $2m$ and $2m + 1$. Let Σ be the 2-dimensional Δ-complex with triangles t_x^+, t_x^- $(0 \le x \le 99)$, each with*

vertices labelled $0<1<\infty$*, in which* t_x^+ *and* t_x^- *share their edge* $[0,1]$*,* t_x^- *and* $t^+_{\sigma_1(x)}$ *share their edge* $[1,\infty]$*, and* t_x^+ *and* $t^-_{\sigma_0(x)}$ *share their edge* $[0,\infty]$*.*

(a) Σ *has* 72 *vertices (the cycles of* $\sigma_0,\sigma_1,\sigma_\infty$*),* 300 *edges and* 200 *triangles, and is homeomorphic to* $C(\mathbb{C})$ *compatibly with the maps to* $\mathbb{P}^1(\mathbb{C})$*;* τ *and the relation of Proposition 6.2 act simplicially.*

(b) $H_1(\Sigma,\mathbb{Z})\simeq\mathbb{Z}^{30}$ *with unimodular intersection form;* $\ker(1+\tau_*)$ *has rank* 14*, the intersection form restricted to it has Smith form* $(2,\dots,2)$*, so half of it is unimodular.*

(c) *On* $\ker(1+\tau_*)$*,* $\mathcal{D}^2=49$ *and* $\mathcal{D}+7\equiv 0 \pmod 2$*. The saturated sublattices* $\ker(\mathcal{D}-7)$ *and* $\ker(\mathcal{D}+7)$ *have ranks* 4 *and* 10*, the halved form restricted to them has Smith forms* $(1,1,7,7)$ *and* $(1,1,1,1,1,1,1,1,7,7)$*, and their sum has index* 49*, with quotient* $(\mathbb{Z}/7)^2$*.*

(d) *The dimensions of the inertia invariants of* G_0,G_1,G_∞ *on the* $+7$ *and* -7 *eigenspaces of the odd functions are* $(5,7,9)$ *and* $(5,1,9)$*.*

(e) *There is a basis of* $\ker(1+\tau_*)$ *in which the halved form has matrix* $\left(\begin{smallmatrix}0 & I_7\\ -I_7 & 0\end{smallmatrix}\right)$ *and* $\mathcal{D}$ *has the matrix of Table 7.*

Proof. The triangulation of $\mathbb{P}^1(\mathbb{C})$ by the closed upper and lower half-planes, with vertices $0,1,\infty$, pulls back to a triangulation of $C(\mathbb{C})$ with one triangle over each half-plane for each of the 100 points of a fibre over the upper half-plane. With the gluing rules above, the vertices over 0, 1 and ∞ are the cycles of σ_0, σ_1 and σ_∞. By Proposition 4.11, the description of $\mathcal{Z}$ in Section 5.1 and Proposition 5.3 (the twist does not change the complex points), $C^\circ(\mathbb{C})\to U(\mathbb{C})$ is the topological cover whose monodromy permutations of the classes of nonzero vectors modulo squares are σ_0 and σ_1, and it extends uniquely to the compact surface; this is (a). The remaining statements follow by linear algebra over $\mathbb{Z}$ on simplicial chains and cochains: H^1 is computed as cocycles modulo coboundaries, the cup product of 1-cocycles is the Alexander–Whitney product for the ordered simplices [29, §3.2] evaluated on the fundamental class $\sum_x(t_x^+-t_x^-)$, and Poincaré duality transports everything to H_1. The relation and τ act on chains by $t_x^\pm\mapsto\sum_y t_y^\pm$, the sum running over the points y related to x. These are chain maps, as the relation is invariant under σ_0 and σ_1. The dimensions in (d) are $\frac{1}{n}\sum_{0\le j<n}\operatorname{tr}(g^j\cdot\frac{7\pm\mathsf{H}}{14})$ on the odd functions, where g is the permutation of the fibre induced by G_0, G_1 or G_∞ and n is its order. □

Remark 6.4 (The construction in general). The construction of the correspondence in Proposition 6.2 uses only a rank-two local system of k-vector spaces on a curve, k a finite field of odd order q, with monodromy in $\mathrm{SL}_2(k)$ preserving a nondegenerate alternating form e_k, together with the curve of lines, its double cover by nonzero vectors modulo squares, and the quadratic character ε of $k^\times$. Then each of the two relations $\varepsilon(e_k(v,w))=\pm1$ is a symmetric correspondence of bidegree (q,q) commuting with τ (when $\varepsilon(-1)=1$, that is, $q\equiv1 \pmod 4$, as for $q=49$), and the computation in the proof of Proposition 6.2 shows that its matrix H on the odd functions on a fibre satisfies $\mathsf{H}^2=qI$. Hence $\mathcal{D}^2=q$ on the Prym. For q a square the eigenvalues $\pm\sqrt{q}$ are integers, the eigenspaces of $\mathcal{D}$ in homology are those of abelian subvarieties, and the relation descends to the base field if the multiplier of e_k under Galois lies in the prime field of k (whose elements are then squares in k). The two relations act with opposite signs. The square class of $e_k(w,\bar{T}w)$ for a transvection $\bar{T}$ in the local monodromy (Lemma 6.1) decides which eigenspace belongs to which relation, and the local monodromy at the branch points gives their dimensions. In the present case $q=49$, and the branch data of Table 3 make one eigenspace a surface.

6.2. **The 2-torsion of B and the quintic field.** The divisor E_L of Proposition 6.7 is defined over the quintic field L of the next proposition, and the five embeddings s of L index the five nonzero singular elements $T_s = [E_s + 13Q_0 - K_C]$ of $B[2]$, where E_s is the conjugate of E_L under s (Proposition 6.7 and Lemma 6.8).

Proposition 6.5. *Let*

$$L = \mathbb{Q}(\xi), \qquad \xi^5 - 70\xi^2 + 210\xi - 168 = 0. \tag{6.2}$$

Then L is a field of signature $(1,2)$, discriminant $43218000 = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7^4$ and class number one, with Galois group S_5; and there is an isomorphism of Galois modules

$$B[2] \simeq \ker\big(\operatorname{Res}_{L/\mathbb{Q}} \mu_2 \longrightarrow \mu_2\big), \tag{6.3}$$

where the map is the norm. In particular $B[2](\mathbb{Q}) = 0$, and for every field $M \supseteq \mathbb{Q}$,

$$H^1(M, B[2]) \simeq \ker\Big((L \otimes M)^\times/(L \otimes M)^{\times 2} \xrightarrow{\mathrm{N}} M^\times/M^{\times 2}\Big). \tag{6.4}$$

Let Δ be the set of embeddings $s\colon L \to \overline{\mathbb{Q}}$, $(e_s)_{s\in\Delta}$ the standard basis of $\mathbb{F}_2^\Delta$, and $E_\Delta \subset \mathbb{F}_2^\Delta$ the even-weight submodule.

Proof. The ring of integers, the class group and the unit group of L are determined unconditionally (Appendix E), and the index of $\mathbb{Z}[\xi]$ in $\mathcal{O}_L$ is 30. The Galois group is S_5: the polynomial is irreducible modulo 11 (a 5-cycle) and modulo 13 a quadratic times a cubic (so the Galois group contains an element of cycle type $(2,3)$, whose cube is a transposition), and a transitive subgroup of S_5 containing a 5-cycle and a transposition is S_5. As 5 is odd, $\mathbb{F}_2^\Delta = E_\Delta \oplus \langle(1,\dots,1)\rangle$. By Lemma 6.8(a), Ψ maps E_Δ onto $i(B[2])$, injectively as $\ker\Psi \subseteq \langle(1,\dots,1)\rangle$. Hence $B[2] \simeq E_\Delta = \ker(\operatorname{Res}_{L/\mathbb{Q}}\mu_2 \to \mu_2)$ as Galois modules, which is (6.3). The same decomposition shows that the sequence $0 \to B[2] \to \operatorname{Res}_{L/\mathbb{Q}}\mu_2 \to \mu_2 \to 0$ splits, and (6.4) follows by Shapiro's lemma and Kummer theory for $\operatorname{Res}_{L/\mathbb{Q}}\mu_2$. As the Galois action on Δ is transitive, the only Galois-fixed vectors in $\mathbb{F}_2^\Delta$ are 0 and the all-ones vector, of odd weight, so $B[2](\mathbb{Q}) = 0$. □

The primes ramified in L are 2, 3, 5 and 7. The following display lists the pairs (e,f) of ramification index and residue degree of the primes of L above them, which are described in Table 8, and the decomposition of $L \otimes \mathbb{R}$:

$$\begin{array}{c|l} 2 & (1,1),\ (4,1) \\ 3 & (1,1),\ (2,1),\ (2,1) \\ 5 & (1,1),\ (4,1) \\ 7 & (5,1) \end{array} \qquad \text{and} \qquad L \otimes \mathbb{R} \simeq \mathbb{R} \times \mathbb{C}^2. \tag{6.5}$$

6.3. **The descent functions.** Let $K_C = q^*D_{x_0}$, a canonical divisor of C of degree 28, and let r, w be as in Proposition 5.10, so that C is the double cover of $\mathcal{X}$ given by $w^2 = r$. The function $u = x_1/x_0$ is a uniformizer at P_0, hence at Q_0 and Q_1, and $u \circ \tau = u$.

Evaluation at divisors. For a field $F \supseteq \mathbb{Q}$, a function $h \in F(C)^\times$ and a closed point Q of C_F, choose a uniformizer π_Q at Q defined over F and put $h[Q] = \mathrm{N}_{F(Q)/F}\Big((h\pi_Q^{-\operatorname{ord}_Q h})(Q)\Big) \in F^\times$. For a divisor $\mathfrak{a} = \sum_Q n_Q Q$ on C_F put $h[\mathfrak{a}] = \prod_Q h[Q]^{n_Q}$. If Q is not a zero or pole of h, then $h[Q]$ is the norm of $h(Q)$. At Q_0 and Q_1 we always take the uniformizer u.

Lemma 6.6. *Let $h \in F(C)^\times$ have a divisor with all multiplicities even. Then the class of $h[\mathfrak{a}]$ in $F^\times/F^{\times 2}$ does not depend on the uniformizers, and $h[\mathfrak{a} + \operatorname{div} g] \equiv h[\mathfrak{a}]$ modulo $F^{\times 2}$ for every $g \in F(C)^\times$. In particular $\mathfrak{a} \mapsto h[\mathfrak{a}]$ induces a homomorphism $\operatorname{Pic}(C_F) \to F^\times/F^{\times 2}$.*

Proof. Replacing π_Q by $v\pi_Q$, with v a unit at Q, multiplies $h[Q]$ by the square $\mathrm{N}(v(Q))^{-\mathrm{ord}_Q h}$. For the second assertion it suffices to show that $h[\operatorname{div} g] \in F^{\times 2}$. Write $\operatorname{div} h = 2D$. By the moving lemma, $D = D' + \operatorname{div} h_1$ with $h_1 \in F(C)^\times$ and D' disjoint from the support of $\operatorname{div} g$. Then $h = c\, h_1^2 h'$ with $c \in F^\times$ and $\operatorname{div} h' = 2D'$. As evaluation at a divisor is multiplicative in the function, $h[\operatorname{div} g] = c^{\deg \operatorname{div} g}\, h_1[\operatorname{div} g]^2\, h'(\operatorname{div} g)$, and by Weil reciprocity for functions with disjoint divisors, $h'(\operatorname{div} g) = g(\operatorname{div} h') = g(D')^2$. □

Proposition 6.7. *There are functions a, b, c on $\mathcal{X}$ with coefficients in L, and a constant $\delta_0 \in L^\times$, such that*

$$\Theta = a + \frac{b}{w} \in L \otimes \mathbb{Q}(C), \qquad \Theta \cdot \tau(\Theta) = a^2 - \frac{b^2}{r} = \delta_0\, c^2, \qquad \operatorname{div}(\Theta) = 26Q_0 + 2E_L - 2K_C, \tag{6.6}$$

where E_L is an effective divisor of degree 15 defined over L (that is, its five conjugates E_s are effective divisors of degree 15 over $\overline{\mathbb{Q}}$). The classes $T_s = [E_s + 13Q_0 - K_C]$ are the five nonzero singular elements of $B[2]$, for the unique Galois-invariant quadratic refinement of the Weil pairing of λ_B. Here Q_0 is the cusp at which $w/(t-1)^6 = 1$ (Proposition 5.10). Let $\ell \in L^\times$ be the leading coefficient of Θ at Q_0, $\Theta = \ell u^{26}(1 + O(u))$. Then, for $M = \mathbb{Q}$ and for $M = \mathbb{Q}_p$ with p any prime, the composite

$$\begin{aligned}\kappa\colon C(M) \xrightarrow{\iota} B^\vee(M) \longrightarrow H^1(M, B^\vee[2]) &\simeq H^1(M, B[2]) \\ &\simeq \ker\left((L\otimes M)^\times/(L\otimes M)^{\times 2} \to M^\times/M^{\times 2}\right)\end{aligned}$$

is $R \mapsto \Theta[R - Q_0] = \Theta[R]/\ell$: at a point R which is not a zero or pole of Θ, this is $\Theta(R)/\ell$, and in general it is computed with the leading coefficient of Θ at R in a uniformizer defined over M (Lemma 6.6). In particular $\kappa(Q_1) = \delta_0$ modulo squares. More generally, for $x = [\mathfrak{a}] \in J(M)$ the Kummer class of $i^\vee\lambda_J(x) \in B^\vee(M)$ is $\Theta[\mathfrak{a}]$.

The functions. Here $a = a_0/x_0^2$, $b = b_0/x_0^3$ and $c = c_0/x_0^2$, where a_0 and c_0 are quadratic forms and b_0 is a cubic form in $x_0, \dots, x_7$ with coefficients in L, and $w = \sqrt{r_0}/x_0$ with $r = r_0/x_0^2$. The forms a_0, b_0, c_0 and the constants δ_0, ℓ are given in the supplementary data [31]. They are too large to print: in the basis $1, \xi, \dots, \xi^4$ of L, the coordinates of δ_0 are rationals whose numerators and denominators have about 6000 digits, and those of ℓ and of the coefficients of a_0, b_0, c_0 have up to about 3000 digits. The function Θ lies in $H^0(C_L, \mathcal{O}(2K_C - 26Q_0))$, which has dimension $56 - 26 - 15 + 1 = 16$ by the Riemann–Roch theorem. The proof of Proposition 6.7, given after Lemma 6.10, uses the following four properties of Θ, which we prove first.

(F1) $\operatorname{div}(\Theta) = 26Q_0 + 2E_L - 2K_C$ with E_L effective of degree 15.
(F2) $ra^2 - b^2 = \delta_0 r c^2$ on $\mathcal{X}$.
(F3) δ_0 is not a square in L.
(F4) $\mathrm{N}_{L/\mathbb{Q}}(\Theta)$ is a constant times a square in $\overline{\mathbb{Q}}(C)$.

Property (F2) is an identity between sections of $\mathcal{O}_{\mathcal{X}}(6) = \mathcal{O}(6K_{\mathcal{X}})$, a line bundle of degree 84. Each of the seven fibres of u over $u = -3, \dots, 3$ is reduced and consists of 14 points with $x_0 \neq 0$, and the form $r_0a_0^2 - b_0^2 - \delta_0 r_0 c_0^2$ vanishes at all of them. A section of a line bundle of degree 84 that vanishes at 98 points is zero. Property (F3) holds because δ_0 has residue 29, a nonsquare modulo 43, at the degree-one prime of L above 43 at which $\xi \equiv 18$.

Property (F1) is proved by specialization at 11, where $\mathcal{X}$ and C have good reduction (Lemma 5.11), 11 is inert in L with residue field $\mathbb{F}_{11^5}$, and the forms a_0, b_0, c_0, r_0 and the

constants δ_0, ℓ are 11-integral, with δ_0, ℓ units. Over $\mathbb{F}_{11^5}$ the norms to the u-line of $\bar{c}$, $\bar{a}$ and $\bar{r}$ are polynomials of degree 28. That of $\bar{c}$ has a zero of order exactly 13 at $u = 0$, and its remaining factor is squarefree of degree 15 and prime to the other two. The expansion at $\overline{P_0}$ gives $\bar{c} = O(u^{13})$ with nonzero u^{13}-coefficient, $\bar{\Theta} = \bar{\ell} u^{26}(1 + O(u))$ at $\overline{Q_0}$, and $\bar{\Theta}(\overline{Q_1}) \neq 0$. Over L, the expansion of c at P_0 in powers of u has zero coefficients up to u^{12} and a nonzero coefficient of u^{13}, so $\operatorname{ord}_{P_0}(c) = 13$. Hence, specializing zeros from $L \otimes \mathbb{Q}_{11}$ to $\mathbb{F}_{11^5}$, $\operatorname{div}_{\mathcal{X}}(c) = 13P_0 + E_{\mathcal{X}} - 2D_{x_0}$ with $E_{\mathcal{X}}$ reduced of degree 15, contained in the chart $x_0 \neq 0$ (its points have finite u), not containing P_0, and $a \neq 0$ at its points. The poles of Θ are bounded by $2K_C$: a has poles only along D_{x_0}, of order at most 2, and, by (F2), $(b/w)^2 = a^2 - \delta_0 c^2$, so b/w is regular away from D_{x_0} with poles of order at most 2 along it. By (F2), $\operatorname{div}\Theta + \tau \operatorname{div}\Theta = 2q^* \operatorname{div}_{\mathcal{X}}(c)$. At a point y of $E_{\mathcal{X}}$ with preimages Q and τQ, the orders of Θ at Q and τQ are nonnegative by the bound on the poles, and they add up to 2. They are not 1 and 1, as otherwise $a = (\Theta + \tau\Theta)/2$ would vanish at y. At P_0, the orders at Q_0 and Q_1 add up to 26, and they are 26 and 0 because the zeros of Θ near $\overline{Q_0}$ and $\overline{Q_1}$ specialize with their multiplicities. The bound on the poles has degree 56, the degree of the zeros found, which proves (F1), with E_L the sum of the points over $E_{\mathcal{X}}$ at which Θ vanishes.

Property (F4) is proved on the same model. The norm of $\bar{\Theta}$ is a constant times the square of an explicit element of $H^0(\bar{C}, \mathcal{O}(5K_{\bar{C}}))$: the two sides agree in their first 281 Taylor coefficients at $\overline{Q_0}$, which suffices since both are sections of $\mathcal{O}(10K_{\bar{C}})$, of degree 280. Hence the class $\sum_s T_s \in J(\mathbb{Q})[2]$ of $\frac{1}{2}\operatorname{div} \mathrm{N}_{L/\mathbb{Q}}(\Theta)$ reduces to zero modulo 11. As reduction modulo 11 is injective on $J(\mathbb{Q})[2]$, this class is zero, which gives (F4).

The value at Q_1. By (F2) and $u \circ \tau = u$, $\Theta[Q_1] \cdot (\tau\Theta)[Q_1] = \delta_0\, c[Q_1]^2$ with $(\tau\Theta)[Q_1] = \Theta[Q_0] = \ell$. Hence

$$\Theta[Q_1 - Q_0] = \Theta[Q_1]/\ell = \delta_0\,(c[Q_1]/\ell)^2 \equiv \delta_0 \pmod{L^{\times 2}}.$$

Lemma 6.8. *Let $\Psi\colon \mathbb{F}_2^{\Delta} \to J[2]$ be the Galois-equivariant map $e_s \mapsto T_s$, and $E_\Delta \subset \mathbb{F}_2^{\Delta}$ the even-weight submodule.*

(a) $\ker\Psi$ *is* 0 *or* $\langle(1,\dots,1)\rangle$, *and* $\Psi(E_\Delta) = i(B[2])$.

(b) *If* (F4) *holds, then* $\ker\Psi = \langle(1,\dots,1)\rangle$: *the T_s lie in $i(B[2])$ and span it with the single relation $\sum_s T_s = 0$, and they are the five nonzero singular vectors of the unique Galois-invariant quadratic refinement of the Weil pairing on $B[2]$.*

(c) *The characteristic polynomial of Frobenius at* 13 *on $B[2]$ is $(T+1)^2(T^2+T+1)$, and the L-polynomials of B and B' at* 13 *are those of Proposition 7.4.*

Proof. We identify B and B' with their images in $P \subset J$. For $s \in \Delta$ let Θ_s be the conjugate of Θ under s. By (F1), $\operatorname{div}\Theta_s = 2(E_s + 13Q_0 - K_C)$, so $2T_s = 0$ and Ψ is defined. The Galois group acts on Δ through S_5, and the S_5-submodules of $\mathbb{F}_2^{\Delta}$ are 0, $\langle(1,\dots,1)\rangle$, E_Δ and $\mathbb{F}_2^{\Delta}$, because E_Δ is irreducible even under a 5-cycle (2 has order 4 modulo 5). If $\ker\Psi \supseteq E_\Delta$, all T_s would equal one Galois-invariant class T_0. Choose a divisor D_T over $\mathbb{Q}$ in this class (possible as $C(\mathbb{Q}) \neq \emptyset$) and $h_T \in \mathbb{Q}(C)$ with $\operatorname{div} h_T = 2D_T$. Then $E_L + 13Q_0 - K_C = D_T + \operatorname{div} h_L$ with $h_L \in L(C)$, so $\Theta = \gamma h_T h_L^2$ with $\gamma \in L^{\times}$. By the congruence proved before this lemma, $\delta_0 \equiv \Theta[Q_1 - Q_0] \equiv h_T[Q_1 - Q_0]$ modulo $L^{\times 2}$, so δ_0 would lie in $\mathbb{Q}^{\times} L^{\times 2}$. As $\mathrm{N}_{L/\mathbb{Q}}(\delta_0)$ is a square (δ_0 is congruent modulo squares to $g_1 = (4-\xi^2)(1+4\xi-2\xi^2)$, whose norm is $2^4 \cdot 3^6 \cdot 5^6$, by the proof of Proposition 6.13), δ_0 would be a square in L, contradicting (F3). Hence $\ker\Psi \subseteq \langle(1,\dots,1)\rangle$, and $\mathcal{T} = \Psi(E_\Delta) \simeq E_\Delta$ is irreducible of dimension 4, with no nonzero Galois-equivariant map to the trivial module.

By (F2), $\operatorname{div}\Theta+\tau\operatorname{div}\Theta = 2q^*\operatorname{div}_{\mathcal{X}}(c)$, hence $\operatorname{div}_{\mathcal{X}}(c) = 13P_0+q_*E_L-2D_{x_0}$, and the norm $\mathrm{N}_{C/\mathcal{X}}\colon J\to\operatorname{Jac}(\mathcal{X})$ kills $T_s = [E_s+13Q_0-K_C]$, as $q_*K_C = 2D_{x_0}$. So $\mathcal{T}\subseteq(\ker\mathrm{N})[2]$. By Mumford [41, §3 and §6, (b)], $\ker\mathrm{N}$ has two connected components, with identity component P. The map $(\ker\mathrm{N})[2]\to\pi_0(\ker\mathrm{N})\simeq\mathbb{Z}/2$ is Galois-equivariant with trivial action on the target, so it kills $\mathcal{T}$, and $\mathcal{T}\subseteq P[2]$. Since $B\cap B'$ has odd order (Proposition 6.2(b)), $P[2] = B[2]\oplus B'[2]$ as Galois modules.

To exclude a nonzero projection of $\mathcal{T}$ to $B'[2]$, we use Frobenius at 13, where C has good reduction and L is unramified. It acts on Δ with cycle type $(2,3)$, so on $\mathcal{T}\simeq E_\Delta$ with characteristic polynomial

$$(T^2-1)(T^3-1)/(T-1)\equiv(T+1)^2(T^2+T+1)\pmod 2.$$

The characteristic polynomials $L_B, L_{B'}$ of Frobenius on the Tate modules of B, B' are Weil polynomials of degrees 4 and 10 with $L_BL_{B'} = L_P$, the characteristic polynomial of Frobenius on the Tate module of P. By (7.1), the first five power sums of the roots of L_P are $1,-23,-23,-927,-464$. By Katz's congruence formula [19, Exp. XXII, Théorème 3.1] and the Cartier matrix of Proposition 7.6, $L_B\equiv T^2h_2$ and $L_{B'}\equiv T^5h_5\pmod{13}$, where $\deg h_2 = 2$ and $h_2h_5 = (T^2+T+6)(T^5+11T^4+8T^3+T+1)$. As the quintic factor is irreducible over $\mathbb{F}_{13}$, $h_2 = T^2+T+6$. If $L_B = T^4+aT^3+bT^2+13aT+169$ lies within the Weil bounds and $(a,b)\equiv(1,6)\pmod{13}$, then $L_{B'} = L_P/L_B$ is determined by the power sums and the functional equation. An enumeration, carried out in the proof of Proposition 7.4 independently of this lemma, shows that exactly two pairs (a,b) satisfy all these conditions (integrality, the Weil bounds for $L_{B'}$ and the congruence for $L_{B'}$ modulo 13):

$$L_B = T^4+T^3-7T^2+13T+169,\qquad L_B = T^4+T^3+6T^2+13T+169,$$

the second with $L_{B'}$ as in (7.3). For the first,

$$L_P\equiv(T^4+T^3+T^2+T+1)(T+1)^{10}\pmod 2$$

is prime to T^2+T+1, which is impossible as $\mathcal{T}\subseteq P[2]$. For the second, $L_B\equiv(T+1)^2(T^2+T+1)$ and $L_{B'}\equiv T^{10}+T^7+T^5+T^3+1\pmod 2$, which is prime to $(T+1)(T^2+T+1)$. So Frobenius at 13 on $B'[2]$ has no constituent in common with $\mathcal{T}$, the projection of $\mathcal{T}$ to $B'[2]$ is zero, and $\mathcal{T}\subseteq B[2]$. By dimension, $\mathcal{T} = B[2]$. This proves (a) and (c).

For (b): if $\sum_s T_s = \Psi(1,\dots,1)$ vanishes, then $\ker\Psi = \langle(1,\dots,1)\rangle$ and $T_s = \Psi(e_s+(1,\dots,1))\in B[2]$. The Galois group acts on $B[2]\simeq E_\Delta$ through S_5, and E_Δ is absolutely irreducible. Hence the Weil pairing of λ_B, which is Galois-invariant, and nondegenerate as $\deg\lambda_B = 49$ is odd, is the unique nonzero invariant alternating form $\sum_s x_sy_s$ on E_Δ. Two invariant quadratic refinements of it differ by an invariant linear form, which is zero as E_Δ has no nonzero fixed vector. Therefore the only invariant refinement is $x\mapsto\frac12\operatorname{wt}(x)\bmod 2$, whose nonzero singular vectors are the five vectors $e_s+(1,\dots,1)$ of weight 4, which Ψ maps to the T_s. By (F4), $\sum_s T_s$ is the class of $\frac12\operatorname{div}\mathrm{N}_{L/\mathbb{Q}}(\Theta)$, which is zero. □

Lemma 6.9 (Kummer maps of Jacobians by functions)**.** *Let M be a field of characteristic zero, C as above with $C(M)\neq\emptyset$, and $T\in J[2]$ with field of definition $F\supseteq M$. Let D be a divisor on C_F with $[D] = T$ and $h\in F(C)^\times$ with $\operatorname{div}h = 2D$. For $x = [\mathfrak{a}]\in J(M)$, with $\mathfrak{a}$ a divisor of degree 0 defined over M, and for $\sigma\in G_F$,*

$$e_2^{\lambda_J}(\kappa_J(x)(\sigma),T) = \frac{\sigma\big(\sqrt{h[\mathfrak{a}]}\big)}{\sqrt{h[\mathfrak{a}]}},$$

where κ_J is the Kummer map of J and $e_2^{\lambda_J}$ the Weil pairing of the principal polarization.

Proof. Suppose first that the support of $\mathfrak{a}$ is disjoint from that of D. Then the formula is the first part of the proof of [50, Theorem 2.3], applied to multiplication by 2 on J and to the single divisor D. The spanning condition there is used only for injectivity, and, as noted after that theorem, the argument works over any field containing M. It uses the formula $e_2^{\lambda_J}([D_1],[D_2]) = h_2(D_1)/h_1(D_2)$ for $\operatorname{div} h_i = 2D_i$ with disjoint supports, which computes the Weil pairing of the principal polarization [30, Theorem 1]. In general, replace $\mathfrak{a}$ by $\mathfrak{a} + \operatorname{div} g$ with $g \in M(C)^\times$ so that the supports become disjoint. This changes neither the left-hand side nor, by Lemma 6.6, the class of $h[\mathfrak{a}]$ modulo $F^{\times 2}$. □

Lemma 6.10. *Let $\psi\colon A_1 \to A_2$ be an isogeny of odd degree between abelian varieties over a field M of characteristic zero. Then ψ induces isomorphisms $A_1[2] \to A_2[2]$ of Galois modules and $A_1(M)/2A_1(M) \to A_2(M)/2A_2(M)$ compatible with the Kummer maps. For $M = \mathbb{Q}$ it induces isomorphisms $\mathrm{Sel}_2(A_1/\mathbb{Q}) \to \mathrm{Sel}_2(A_2/\mathbb{Q})$ and $Ш(A_1/\mathbb{Q})[2] \to Ш(A_2/\mathbb{Q})[2]$, and $\operatorname{rank} A_1(\mathbb{Q}) = \operatorname{rank} A_2(\mathbb{Q})$.*

Proof. There is ψ' with $\psi'\psi = [n]$ and $\psi\psi' = [n]$, $n = \deg\psi$ odd. As $[n]$ is the identity on $A_i[2]$ and on $A_i(M)/2A_i(M)$, ψ and ψ' induce mutually inverse maps. Compatibility with the Kummer maps is functoriality of the connecting homomorphism, and the statements about Selmer groups and $Ш[2]$ follow by applying this over $\mathbb{Q}$ and every completion. □

Proof of Proposition 6.7. Properties (F1)–(F4) were proved above, and Lemma 6.8 gives the statement about the T_s. Let $M = \mathbb{Q}$ or $\mathbb{Q}_p$ and $x = [\mathfrak{a}] \in J(M)$; since $Q_0 \in C(\mathbb{Q})$, every class in $J(M)$ has this form. By functoriality of the connecting homomorphism, the Kummer class of $i^\vee\lambda_J(x)$ is the image of $\kappa_J(x)$ under $i^\vee\lambda_J\colon J[2] \to B^\vee[2]$. By functoriality of the Weil pairing $e_2\colon B[2] \times B^\vee[2] \to \mu_2$ [39, Ch. I, Proposition 13.2], for $b \in B[2]$ and $y \in J[2]$,

$$e_2(b, i^\vee\lambda_J y) = e_2(i(b), \lambda_J y) = e_2^{\lambda_J}(y, i(b))^{\pm 1}.$$

For $s \in \Delta$ let $b_s \in B[2]$ with $i(b_s) = T_s$ (Lemma 6.8(b)), and let $\mu_2^\Delta = \operatorname{Res}_{L/\mathbb{Q}}\mu_2$ be the Galois module of maps $\Delta \to \mu_2$. The map $y \mapsto (e_2(b_s, y))_s$ is injective on $B^\vee[2]$ with image the norm-one part of μ_2^Δ, because the T_s span $i(B[2])$ with the single relation $\sum_s T_s = 0$. On H^1 it gives the isomorphism of $H^1(M, B^\vee[2])$ with $\ker\left((L\otimes M)^\times/(L\otimes M)^{\times 2} \to M^\times/M^{\times 2}\right)$ used in the proposition. Now take $h = \Theta_s$, the conjugate of Θ under s, which has divisor $2(E_s + 13Q_0 - K_C)$ and is defined over $s(L)$. By Lemma 6.9, the component at s of the image of the Kummer class of $i^\vee\lambda_J(x)$ in $H^1(M, \mu_2^\Delta)$ is the class of $\Theta_s[\mathfrak{a}]$. Under Shapiro's lemma $H^1(M, \mu_2^\Delta) = (L\otimes M)^\times/(L\otimes M)^{\times 2}$ (the G_M-orbits on Δ being the factors of $L \otimes M$), the Kummer class is therefore $\Theta[\mathfrak{a}]$. For $\mathfrak{a} = R - Q_0$ we get $\kappa(R) = \Theta[R]/\Theta[Q_0] = \Theta[R]/\ell$, and $\kappa(Q_1) \equiv \delta_0$ modulo squares by the congruence proved before Lemma 6.8. The identification of $H^1(M, B^\vee[2])$ with $H^1(M, B[2])$ is induced by λ_B, an isogeny of odd degree 49 by Proposition 6.2(a), hence an isomorphism on 2-torsion (Lemma 6.10). The isogeny λ_B' induces the same identification, since $\lambda_B'\lambda_B = [7]$ is the identity on $B[2]$. □

Remark 6.11. Without (F4), Lemma 6.8(a) and the argument in the proof of Lemma 6.8(b), which uses only (a), show that the $T_s' = \Psi(e_s + (1,\dots,1))$ are the five nonzero singular vectors of the Galois-invariant quadratic refinement of the Weil pairing on $B[2]$, and $T_s = T_s' + z$ with $z = \sum_s T_s \in J(\mathbb{Q})[2]$. As $\mathrm{N}_{L/\mathbb{Q}}(\Theta)$ has divisor twice a divisor of class z, Lemma 6.9 and the argument above give the Kummer class of $i^\vee\lambda_J(x)$ as $\Theta[\mathfrak{a}] \cdot \mathrm{N}_{L\otimes M/M}(\Theta[\mathfrak{a}])$, the projection of $\Theta[\mathfrak{a}]$ to the norm-one part along $M^\times/M^{\times 2}$. For all classes used in the descent below, $\mathrm{N}_{L\otimes M/M}(\Theta[\mathfrak{a}])$ is a square in M. For δ_0 and for the images of the points of Table 10, this is part of the computation of Table 9. Therefore the descent does not use (F4).

6.4. **The two-descent.**

Lemma 6.12. *For every prime $p \notin \{2,3,5,7\}$, the curves $\mathcal{X}$ and C have good reduction at p. Consequently J, P, B and B' have good reduction at every prime $p \notin \{2,3,5,7\}$.*

Proof. The family (4.2) is smooth over $U_{\mathbb{Z}[1/30]}$, as its leading coefficient is 5 and its discriminant is $2^{12} \cdot 3^6 \cdot 5^5\, t^8(t-1)^2$. Thus $J_t[7]$ is finite étale over $U_{\mathbb{Z}[1/210]}$, and so are the covers $\mathcal{X}^\circ$ and $\mathcal{Z}^\circ$ of U built from it in Sections 4.7 and 5.1: as in the proof of Lemma 5.11 over $\mathbb{Z}_{11}$, the $\mathcal{O}_K$-action extends to this finite étale group scheme over the normal base, and the descent of Lemma 4.10 works over $\mathbb{Z}[1/210]$, where K is unramified. Let $p \notin \{2,3,5,7\}$. The divisor $D = \{0,1,\infty\}$ of $\mathbb{P}^1_{\mathbb{Z}_{(p)}}$ is a disjoint union of three sections, hence regular, and the covers are tamely ramified along D in codimension one, as the generic points of D have residue characteristic 0. By Abhyankar's lemma [53, Tags 0EYG and 0EYH], the normalization of $\mathbb{P}^1_{\mathbb{Z}_{(p)}}$ in the function field of $\mathcal{X}$, respectively $\mathcal{Z}$, is étale locally along D of the form $\operatorname{Spec} A[x]/(x^e - f)$, with f a local equation of D and e invertible in A. Such a scheme is smooth over $\mathbb{Z}_{(p)}$ [28, Exp. XIII, Proposition 5.4], and away from D the normalization is finite étale over $U_{\mathbb{Z}_{(p)}}$. So $\mathcal{X}$ and $\mathcal{Z}$ have smooth proper models over $\mathbb{Z}_{(p)}$ (see also [57, Theorem 1.2]), and so does the twist $C = \mathcal{Z}^{(5)}$, as the quadratic character of $\mathbb{Q}(\sqrt{5})$ is unramified at p. Hence J has good reduction at p, and so do its abelian subvarieties P, B and B', whose Tate modules are submodules of that of J, hence unramified at p [51, Theorem 1]. □

Let $\mathcal{S} = \{2,3,5,7\}$, outside which B has good reduction (Lemma 6.12), and let $L(\mathcal{S},2) \subset L^\times/L^{\times 2}$ be the subgroup of classes with even valuation at all primes outside $\mathcal{S}$. By Lemma 6.10, applied to $\lambda'_B\colon B^\vee \to B$ of degree 49, we may carry out the descent on $B^\vee$ with the Kummer map of Proposition 6.7. Selmer groups, Ш[2] and ranks of B and $B^\vee$ correspond, and $\kappa(R)$ corresponds to the Kummer class of $f(R) = \lambda'_B\iota(R)$.

Proposition 6.13 (Rank one)**.** $\mathrm{Sel}_2(B/\mathbb{Q})$ *is 1-dimensional, generated by $\kappa(Q_1)$. Consequently* $\operatorname{rank} B(\mathbb{Q}) = 1$*, the point $f(Q_1) \in B(\mathbb{Q})$ has infinite order, and* $Ш(B/\mathbb{Q})[2] = 0$.

Proof. The ambient space. As L has class number one, unit rank 2 and eight primes above $\mathcal{S}$ by (6.5), $L(\mathcal{S},2)$ has dimension 11. It is generated by -1, ξ, $\xi-1$, $\xi^2-\xi-1$, 2, $\xi+2$, $\xi-2$, 3, $\xi-3$, $\xi-4$, $3\xi-4$, which are independent modulo squares. The norm map $L(\mathcal{S},2) \to \mathbb{Q}(\mathcal{S},2) = \langle -1,2,3,5,7\rangle$ has rank 5, so by (6.4) the classes in $H^1(\mathbb{Q}, B[2])$ unramified outside $\mathcal{S}$ form the 6-dimensional space

$$\mathcal{V} = \ker(\mathrm{N}\colon L(\mathcal{S},2) \to \mathbb{Q}(\mathcal{S},2)) = \langle g_0, g_1, \dots, g_5\rangle_{\mathbb{F}_2},$$

$$g_0 = 2-\xi, \qquad g_1 = (4-\xi^2)(1+4\xi-2\xi^2), \qquad g_2 = 2+\xi,$$

$$g_3 = 3(\xi-1), \qquad g_4 = 4-\xi, \qquad g_5 = (\xi-1)(3-\xi),$$

with norms 2^2, $2^4\cdot 3^6\cdot 5^6$, $2^2\cdot 3^2\cdot 5^2$, 3^8, $2^6\cdot 3^2$, $3^4\cdot 5^2$. The Selmer group lies in $\mathcal{V}$: at $p \notin \mathcal{S}$ the local Kummer image is contained in the unramified subgroup, because the multiplication-by-two torsor extends over the abelian scheme, and both have dimension $\dim B[2](\mathbb{Q}_p)$, so they are equal. The element δ_0 of Proposition 6.7 satisfies $\delta_0/g_1 \in L^{\times 2}$, so $\kappa(Q_1)$ is the class of g_1.

Local images at $\mathcal{S}$. Let $p \in \mathcal{S}$. As $B^\vee(\mathbb{Q}_p)$ has a subgroup of finite index isomorphic to $\mathbb{Z}_p^{\dim B}$ [38, Ch. I, Lemma 3.3], and $B^\vee[2] \simeq B[2]$ (Lemma 6.10), $\dim_{\mathbb{F}_2} B^\vee(\mathbb{Q}_p)/2B^\vee(\mathbb{Q}_p)$ is $\dim B[2](\mathbb{Q}_p) + \dim B$ for $p = 2$ and $\dim B[2](\mathbb{Q}_p)$ otherwise. By Lemma 6.10 it equals

$\dim_{\mathbb{F}_2} B(\mathbb{Q}_p)/2B(\mathbb{Q}_p)$, and by (6.3), $\dim B[2](\mathbb{Q}_p)$ is one less than the number of primes of L above p. From (6.5):

p	2	3	5	7
$\dim B(\mathbb{Q}_p)/2B(\mathbb{Q}_p)$	3	2	1	0

(6.7)

Hilbert symbols give coordinates on $(L\otimes\mathbb{Q}_p)^\times/(L\otimes\mathbb{Q}_p)^{\times 2} = \prod_{\mathfrak{p}|p} L_\mathfrak{p}^\times/L_\mathfrak{p}^{\times 2}$. For the basis $\mathcal{B}_\mathfrak{p}$ of $L_\mathfrak{p}^\times/L_\mathfrak{p}^{\times 2}$ in Table 8, an element y has the coordinates $(y,\beta)_\mathfrak{p}$ for $\beta\in\mathcal{B}_\mathfrak{p}$, written additively (0 for $+1$, 1 for -1). They determine y, as the Hilbert pairing is perfect. The coordinates of $g_0,\dots,g_5$ and of the images of the local points below are in Table 9. Proposition 6.7 gives the images of points of $C(\mathbb{Q}_p)$. At $p=2$ we use Q_1 and the points R_2 and R_{-2} of Table 10, with $u=2$ and $u=-2$. At $p=3$ we use Q_1 and R_{-3}, with $u=-3$, and at $p=5$ only Q_1. At $p=7$ the local image is zero. On the explicit model, x_2/x_0 at a point of $\mathcal{X}$ with $u=u_0$ is a root of the fibre polynomial $m_{u_0}(T)=\prod_{u(Q)=u_0}(T-(x_2/x_0)(Q))$, of degree 14, and the other coordinates are polynomials in it. The roots used are simple, with $v_p(m'_{u_0}((x_2/x_0)(R)))=2,2,60$ for $R=R_2,R_{-2},R_{-3}$, so Hensel's lemma applies to approximations of sufficient precision. Appendix C.2 explains why the printed coordinates determine the points. The images $\Theta[R]/\ell$ are evaluated from the coordinates modulo p^{42} in Table 10. An explicit bound for the effect of the truncation on each factor $L_\mathfrak{p}$ shows that the square classes are those of the true points, and coordinates modulo p^{38} suffice. The approximations and these bounds are in the supplementary data [31]. In each case the classes span a space of the dimension in (6.7), hence the whole local image W_p:

$$W_2=\langle\kappa(Q_1),\kappa(R_2),\kappa(R_{-2})\rangle,\qquad W_3=\langle\kappa(Q_1),\kappa(R_{-3})\rangle,$$
$$W_5=\langle\kappa(Q_1)\rangle,\qquad W_7=0.$$

The Selmer group. Let $y=\prod g_i^{e_i}\in\mathcal{V}$. From Table 9, the condition at 7 is empty, as all g_i are locally trivial there. At 5, W_5 is spanned by the vector with coordinates $(0,0)$ at $\mathfrak{p}_5$ and $(0,1)$ at $\mathfrak{p}_5'$, and the first coordinate of the image of y is e_2+e_5, so the condition is $e_2=e_5$. At 3, W_3 is spanned by the second and sixth coordinate vectors, and the first, third, fourth and fifth coordinates of the image of y are $e_2+e_3+e_4+e_5$, $e_2+e_3+e_4$, $e_2+e_3+e_4+e_5$ and e_5, so the conditions are $e_5=0$ and $e_2+e_3+e_4=0$. At 2, the first, second and fourth coordinates vanish on W_2 and equal e_0+e_2, e_4 and e_0+e_2 on the image of y. Given $e_0=e_2$ and $e_4=0$, the image of y at 2 is $(e_0+e_1)\kappa(Q_1)+e_3g_3+e_5g_5$ in additive notation. As $\kappa(Q_1)\in W_2$, comparing the remaining coordinates shows that it lies in W_2 if and only if $e_3=0$. The conditions at $2,3,5,7$ have ranks $3,2,1,0$, of combined rank 5, with solution space $e_0=e_2=e_3=e_4=e_5=0$, that is $\langle g_1\rangle$. Hence $\mathrm{Sel}_2(B/\mathbb{Q})\subseteq\langle g_1\rangle=\langle\kappa(Q_1)\rangle$ (the conditions at the real place, not used here, can only make it smaller). As $\kappa(Q_1)$ lies in $\mathrm{Sel}_2(B/\mathbb{Q})$ and is nonzero, $\mathrm{Sel}_2(B/\mathbb{Q})=\langle\kappa(Q_1)\rangle$ has dimension 1. Here $\kappa(Q_1)\neq 0$ because $g_1\equiv(4-18^2)(1+72-648)\equiv 3 \pmod{\mathfrak{p}_{43}}$, where $\mathfrak{p}_{43}$ is the degree-one prime of L above 43 with $\xi\equiv 18$, and 3 is a nonsquare modulo 43.

Rank. From $0\to B(\mathbb{Q})/2B(\mathbb{Q})\to\mathrm{Sel}_2(B/\mathbb{Q})\to Ш(B/\mathbb{Q})[2]\to 0$ and $B[2](\mathbb{Q})=0$ we get $\operatorname{rank} B(\mathbb{Q})\le 1$. The point $\iota(Q_1)\in B^\vee(\mathbb{Q})$ is nontorsion: $B^\vee[2]\simeq B[2]$ (Lemma 6.10), so $B^\vee(\mathbb{Q})$ has no 2-torsion, its torsion subgroup is odd and 2-divisible, and a torsion point would have trivial Kummer image, whereas $\kappa(Q_1)\neq 0$. Hence $f(Q_1)=\lambda'_B\iota(Q_1)\in B(\mathbb{Q})$ is nontorsion, $\operatorname{rank} B(\mathbb{Q})=1$, and the exact sequence above gives $Ш(B/\mathbb{Q})[2]=0$. □

7. The good model at 13 and the integral lattice

We show that $\mathcal{X}$ and C have good reduction at 13, use this to confine the points R of Proposition 5.3 to two residue discs (Lemma 7.3), and compute the invariants of B at 13

that Section 8 needs. Appendix D lists the reductions modulo 13 of the equations, forms and differentials used here.

Throughout this section a bar denotes reduction modulo 13, and $\overline{\mathbb{F}}_{13}$ is an algebraic closure of $\mathbb{F}_{13}$. We write $I \subset \mathbb{F}_{13}[x] = \mathbb{F}_{13}[x_0, \dots, x_7]$ for the ideal generated by the fifteen quadrics $\overline{q}_1, \dots, \overline{q}_{15}$ of Table 11 (the ideal $\bar{I}$ of the proof of Proposition 5.5), put $\overline{\mathcal{X}} = \mathrm{Proj}(\mathbb{F}_{13}[x]/I)$, and let $u = x_1/x_0$ be the function of Proposition 5.5(d).

7.1. **Good reduction and point counts.**

Proposition 7.1. *The canonical model of $\mathcal{X}$ in Proposition 5.5 has good reduction at 13: its reduction modulo 13 is a smooth curve of genus 8 over $\mathbb{F}_{13}$. The double cover $C \to \mathcal{X}$ extends to an unramified double cover of smooth curves over $\mathbb{Z}_{13}$. The numbers of points over $\mathbb{F}_{13^n}$ are*

n	1	2	3	4	5
$\#\overline{\mathcal{X}}(\mathbb{F}_{13^n})$	11	223	2261	28415	371726
$\#\overline{C}(\mathbb{F}_{13^n})$	10	246	2284	29342	372190

(7.1)

Of the ten points of $\overline{C}(\mathbb{F}_{13})$, exactly two lie over $\bar{t} = 1$, namely the reductions $\overline{Q_0}, \overline{Q_1}$ of the cusps, and the other eight lie over $\bar{t} = \infty$, so that none lies over $\bar{t} = 0$ or over a value $\bar{t} \notin \{0, 1, \infty\}$.

Proof. The special fibre. The quadrics $q_1, \dots, q_{15}$ of Proposition 5.5 have 13-integral coefficients, and their reductions are the forms $\overline{q}_i$ of Table 11. The proof of Proposition 5.5(a) shows that $\overline{\mathcal{X}}$ is smooth. Gröbner-basis computations over $\mathbb{F}_{13}$ with the forms of Table 11 (Appendix D.3) prove this from the printed data and give the other facts used below.

(i) The reduced Gröbner basis of I for the reverse lexicographic order with $x_0 > \cdots > x_7$ consists of fifteen quadrics, five cubics and one quartic. The ideal I is saturated, and the Hilbert series of $\mathbb{F}_{13}[x]/I$ is $(1 + 6T + 6T^2 + T^3)/(1 - T)^2$, so $\overline{\mathcal{X}}$ has Hilbert polynomial $14n - 7$.

(ii) The forms x_0, x_1 have no common zero on $\overline{\mathcal{X}}$, and $\mathbb{F}_{13}[x]/(I + (x_0, x_1))$ has length 14, which is the multiplicity of $\mathbb{F}_{13}[x]/I$. Hence x_0, x_1 is a regular sequence and $\mathbb{F}_{13}[x]/I$ is Cohen–Macaulay of dimension 2.

(iii) Let $M_1, \dots, M_4$ be the ideals of 6×6 minors of the 6×8 Jacobian matrices of the sets $\{\overline{q}_1, \dots, \overline{q}_6\}$, $\{\overline{q}_7, \dots, \overline{q}_{12}\}$, $\{\overline{q}_{10}, \dots, \overline{q}_{15}\}$ and $\{\overline{q}_1, \overline{q}_3, \overline{q}_5, \overline{q}_7, \overline{q}_9, \overline{q}_{11}\}$. Then $I + M_1 + M_2 + M_3 + M_4$ has Krull dimension 0, that is, it has no zero in $\mathbb{P}^7(\overline{\mathbb{F}}_{13})$.

By (ii), $\overline{\mathcal{X}}$ is equidimensional of dimension 1 without embedded points, and $H^0(\overline{\mathcal{X}}, \mathcal{O}) = (\mathbb{F}_{13}[x]/I)_0 = \mathbb{F}_{13}$, as a graded Cohen–Macaulay ring of dimension 2 has depth 2. With these data the argument of the proof of Proposition 5.5(a) applies. By (i) the canonical ring of $\mathcal{X}$ over $\mathbb{Q}$ and $\mathbb{F}_{13}[x]/I$ have the same Hilbert function, so the closure $\mathcal{X}_{\mathbb{Z}_{13}}$ of $\mathcal{X}$ in $\mathbb{P}^7_{\mathbb{Z}_{13}}$ is flat and proper over $\mathbb{Z}_{13}$, with homogeneous ideal $(q_1, \dots, q_{15}) \otimes \mathbb{Z}_{13}$ and special fibre $\overline{\mathcal{X}}$. By (iii), at each geometric point of $\overline{\mathcal{X}}$ some M_k does not vanish, so $\overline{\mathcal{X}}$ is smooth. Hence $\mathcal{X}_{\mathbb{Z}_{13}}$ is a smooth proper model of $\mathcal{X}$, and $\overline{\mathcal{X}}$ is a smooth geometrically connected curve of genus 8 (as $H^0(\overline{\mathcal{X}}, \mathcal{O}) = \mathbb{F}_{13}$ and $\chi(\mathcal{O}_{\overline{\mathcal{X}}}) = -7$), whose canonical bundle is $\mathcal{O}(1)$, as $\mathcal{O}(1)$ has degree $14 = 2g - 2$ and $g = 8$ independent sections. For every d the module $H^0(\mathcal{X}_{\mathbb{Z}_{13}}, \mathcal{O}(d))$ is free, with basis the monomials of degree d that are standard for the Gröbner basis in (i), lifted to a Gröbner basis over $\mathbb{Z}_{13}$ with unit leading coefficients.

The double cover. The form r_0 of Proposition 5.10 is 13-integral and reduces to the form $\overline{r}_0$ of Table 11, which is not in I. As in the proof of Lemma 5.11(b), it follows by purity of the branch locus [28, Exp. X, Théorème 3.1] that the normalization $C_{\mathbb{Z}_{13}}$ of the regular scheme

$\mathcal{X}_{\mathbb{Z}_{13}}$ in the function field of C is étale over $\mathcal{X}_{\mathbb{Z}_{13}}$. Hence $C_{\mathbb{Z}_{13}}$ is smooth and proper over $\mathbb{Z}_{13}$, with special fibre the unramified double cover $\overline{C}$ of $\overline{\mathcal{X}}$ given by $w^2 = \overline{r}$. It is geometrically connected: otherwise it would split over $\mathbb{F}_{169}$ into two copies of $\overline{\mathcal{X}}$, and $\#\overline{C}(\mathbb{F}_{169})$ would be $2 \cdot 223$, whereas it is 246 by (7.1). So $\overline{C}$ has genus 15.

The counts. The numbers (7.1) are obtained from Table 11 by counting points fibre by fibre over the u-line (Appendix D.3). For $n = 1$ the points are listed in Proposition D.1.

The distribution over t. By Lemma 7.2, whose proof uses only the first part of this proof, t extends over $\mathbb{Z}_{13}$. Table 12 gives the values of $\bar{t}$ at the eleven points of $\overline{\mathcal{X}}(\mathbb{F}_{13})$, none of which lies over $\bar{t} = 0$, and the numbers of points of $\overline{C}$ above them. So $\overline{C}(\mathbb{F}_{13})$ consists of the two distinct points $\overline{Q_0}, \overline{Q_1}$ above the reduction $\overline{P_0}$ of the rational cusp, where $\bar{t} = 1$, and of two points above each of the four points of $\overline{\mathcal{X}}(\mathbb{F}_{13})$ where $\bar{t} = \infty$. □

Lemma 7.2 (The parameter t at 13)**.** *The map $t\colon \mathcal{X} \to \mathbb{P}^1$ extends to a finite flat morphism $t\colon \mathcal{X}_{\mathbb{Z}_{13}} \to \mathbb{P}^1_{\mathbb{Z}_{13}}$ of degree 50. On $\overline{\mathcal{X}}$ its reduction is $\bar{t} = \overline{A}/\overline{B}$ wherever the quintic forms $\overline{A}, \overline{B}$ of Table 14 do not both vanish, which includes all of $\overline{\mathcal{X}}(\mathbb{F}_{13})$, and the values of $\bar{t}$ at the eleven points of $\overline{\mathcal{X}}(\mathbb{F}_{13})$ are those of Table 12. At $\overline{P_0}$ one has $\bar{t} = 1 + u + O(u^2)$.*

Proof. Let V be the $\mathbb{Q}$-span of the thirteen pairs (A_i, B_i) of Proposition 5.5, as pairs of quintic forms modulo the ideal of $\mathcal{X}$. Every $(A, B) \in V$ satisfies $A = tB$ on $\mathcal{X}$, and $\dim V = 13$ (see below). Put $H_5 = H^0(\mathcal{X}_{\mathbb{Z}_{13}}, \mathcal{O}(5))$, free of rank 63 with reduction $H^0(\overline{\mathcal{X}}, \mathcal{O}(5))$, and $V_{\mathbb{Z}_{13}} = (V \otimes \mathbb{Q}_{13}) \cap H_5^{\oplus 2}$, a saturated lattice of rank 13. Each $(A, B) \in V_{\mathbb{Z}_{13}}$ defines a morphism $[A : B]$ to $\mathbb{P}^1_{\mathbb{Z}_{13}}$ on the open set $U_{A,B} \subset \mathcal{X}_{\mathbb{Z}_{13}}$ where A and B do not both vanish, and this morphism agrees with t on the generic fibre. A basis of $V_{\mathbb{Z}_{13}}$ is obtained from the thirteen rational pairs by 13-adic saturation (Appendix D.2). (Saturation is needed: once each of the thirteen rational pairs is scaled to be primitive in $H_5^{\oplus 2}$, their reductions are all multiples of a single pair.) Write (A_i, B_i) again for the resulting basis. The reductions $(\overline{A_i}, \overline{B_i})$ are linearly independent (so $\dim V = 13$), satisfy $\overline{A_i}\overline{B_j} \equiv \overline{A_j}\overline{B_i} \pmod{I}$, and have no common zero on $\overline{\mathcal{X}}$: with I they generate an ideal of Krull dimension 0.

So the open sets U_{A_i,B_i} cover $\mathcal{X}_{\mathbb{Z}_{13}}$: the generic fibre by Proposition 5.5(b), the special fibre by the last property. The morphisms $[A_i : B_i]$ agree on the dense generic fibre, hence on overlaps, as $\mathbb{P}^1$ is separated. They therefore glue to a morphism $\mathcal{X}_{\mathbb{Z}_{13}} \to \mathbb{P}^1_{\mathbb{Z}_{13}}$ extending t. As $\bar{t}$ is not constant (see below), this morphism is quasi-finite and proper, hence finite, and it is flat, as a finite morphism between regular schemes of dimension 2. Hence $\bar{t}$ has degree 50.

The pair $(\overline{A}, \overline{B})$ of Table 14 lies in the reduction of $V_{\mathbb{Z}_{13}}$, so $\bar{t} = \overline{A}/\overline{B}$ wherever $(\overline{A}, \overline{B}) \neq (0, 0)$. Evaluating at the eleven points gives the last two columns of Table 12: no point is a common zero, and $\bar{t}$ takes the values $1, \infty, 2, 9, 11$. Expanding at $\overline{P_0}$, where u is a local parameter, gives $\bar{t} = 1 + u + O(u^2)$. □

Lemma 7.3 (The two residue discs)**.** *Suppose that $A_\nu \simeq L_a$, and let $R \in C(\mathbb{Q})$ be one of the two points of Proposition 5.3. Then $13 \nmid XY$, $13 \mid Z$, and the reduction of R modulo 13 is $\overline{Q_0}$ or $\overline{Q_1}$.*

Proof. As $13 \equiv -1 \pmod 7$, the seventh-power map is a bijection of $\mathbb{F}_{13}^\times$, so $T^7 - 3^a \cdot 5$ has exactly one root in $\mathbb{F}_{13}$. The other six lie in $\mathbb{F}_{169}$, which contains μ_7, and pair into three quadratic factors. All factors are simple, so $L_a \otimes \mathbb{Q}_{13}$ is the product of $\mathbb{Q}_{13}$ and three unramified quadratic extensions.

Suppose $13 \mid Y$. Then $13 \nmid XZ$ and $v_{13}(\nu - 1) = 3v_{13}(Y) =: 3b > 0$, as $\nu - 1 = -Y^3/Z^7$. The factorization

$$\phi(T) - 1 = (T - 1)^3 \, (15T^4 + 10T^3 + 6T^2 + 3T + 1)$$

isolates a cluster of three roots of $\phi(T)-\nu$ near $T=1$: the quartic factor takes the 13-adic unit value 35 at $T=1$, so, writing $T=1+13^b v$, the cluster is governed by the residual cubic $35v^3-c$, with $c\neq 0$ the residue of $(\nu-1)/13^{3b}$. As $\mu_3\subset\mathbb{F}_{13}$, this cubic splits completely or is irreducible over $\mathbb{F}_{13}$, so the cluster contributes to $A_\nu\otimes\mathbb{Q}_{13}$ three copies of $\mathbb{Q}_{13}$ or one unramified cubic field, neither of which is a product of factors of $L_a\otimes\mathbb{Q}_{13}$, whose only 3-dimensional subproduct is $\mathbb{Q}_{13}\times\mathbb{Q}_{169}$, with $\mathbb{Q}_{169}$ the unramified quadratic extension of $\mathbb{Q}_{13}$. Hence $13\nmid Y$.

So $t=-X^5/Y^3$ is 13-integral. As $C_{\mathbb{Z}_{13}}$ is proper, R extends to a $\mathbb{Z}_{13}$-point and reduces to a point $\overline{R}\in\overline{C}(\mathbb{F}_{13})$, which lies over the reduction of $t(q(R))$ because t extends to $\mathcal{X}_{\mathbb{Z}_{13}}$ (Lemma 7.2). If $13\mid X$, then $t\equiv 0$, and if $13\nmid XYZ$, then t reduces to a value outside $\{0,1,\infty\}$. By Proposition 7.1, in neither case does $\overline{C}(\mathbb{F}_{13})$ have a point over it. Therefore $13\mid Z$, $t\equiv 1 \pmod{13}$, and $\overline{R}$ is one of the two points over $\bar{t}=1$, the reductions of the cusps. □

7.2. **The L-polynomials of P, B and B' at 13.** For an abelian variety G of dimension d over $\mathbb{F}_{13}$, its L-polynomial $L_G(T)=\det\left(T-\pi_G\mid V_\ell(G)\right)$ is the characteristic polynomial of its Frobenius endomorphism π_G on the ℓ-adic Tate module $V_\ell(G)$, for any prime $\ell\neq 13$. It is monic of degree $2d$, $T^{2d}L_G(13/T)=13^dL_G(T)$, and $L_G(1)=\#G(\mathbb{F}_{13})$. For P, B, B' it is applied to their reductions at 13, which are abelian varieties because C has good reduction, and $\#P(\mathbb{F}_{13})$, $\#B(\mathbb{F}_{13})$, $\#B'(\mathbb{F}_{13})$ denote the numbers of points of these reductions.

Proposition 7.4. *The L-polynomial of P at 13 factors as $L_B(T)L_{B'}(T)$ with*

$$L_B(T)=T^4+T^3+6T^2+13T+169, \tag{7.2}$$

$$\begin{aligned}L_{B'}(T)=T^{10}-2T^9+8T^8-13T^7+118T^6+79T^5\\ +1534T^4-2197T^3+17576T^2-57122T+371293,\end{aligned} \tag{7.3}$$

the factors corresponding to B and B' respectively. They are determined by the point counts (7.1), the Cartier matrix of Proposition 7.6, the Weil bounds and either the Galois structure of $P[2]$ (Lemma 6.8) or the point counts over $\mathbb{F}_{13^6}$. Hence

$$\#B(\mathbb{F}_{13})=190,\qquad \#B'(\mathbb{F}_{13})=331275,$$

$$N:=\#P(\mathbb{F}_{13})=62942250=2\cdot 3\cdot 5^3\cdot 7\cdot 19\cdot 631. \tag{7.4}$$

Proof. The addition map $B\times B'\to P$ is an isogeny of degree 49 (Proposition 6.2(b)), prime to 13, so $L_P=L_BL_{B'}$, with factors of degrees 4 and 10.

Power sums. Since $H^1(\overline{C})=H^1(\overline{\mathcal{X}})\oplus H^1(\overline{P})$ as Frobenius modules, $\#\overline{\mathcal{X}}(\mathbb{F}_{13^n})-\#\overline{C}(\mathbb{F}_{13^n})$ is the n-th power sum of the roots of L_P. By (7.1) the first five are $1,-23,-23,-927,-464$, so by Newton's identities

$$L_P=T^{14}-T^{13}+12T^{12}-4T^{11}+296T^{10}-115T^9+\cdots.$$

Reduction modulo 13. By Katz's congruence formula [19, Exp. XXII, Théorème 3.1] (for curves, Manin's theorem, see [1, §2.5 of the arXiv version]), the L-polynomials of the Jacobians satisfy

$$\begin{aligned}L_{\overline{C}}&\equiv T^{15}\det(T-F\mid H^1(\overline{C},\mathcal{O})),\\ L_{\overline{\mathcal{X}}}&\equiv T^8\det(T-F\mid H^1(\overline{\mathcal{X}},\mathcal{O}))\pmod{13},\end{aligned}$$

with F the Frobenius. As $H^1(\overline{C},\mathcal{O})=H^1(\overline{\mathcal{X}},\mathcal{O})\oplus H^1(\overline{C},\mathcal{O})^-$ compatibly with F, and $L_{\overline{C}}=L_{\overline{\mathcal{X}}}L_P$, we get $L_P\equiv T^7\det(T-F\mid H^1(\overline{C},\mathcal{O})^-)$. As F is adjoint to the Cartier

operator under Serre duality (Section 7.3), and τ-eigenspaces of opposite sign are orthogonal, Proposition 7.6(a) gives

$$L_P \equiv T^7\,(T^2+T+6)(T^5+11T^4+8T^3+T+1) \pmod{13}.$$

By the functional equation the coefficients of T^j, $j<d$, of the L-polynomial of an abelian variety of dimension d are divisible by 13. So $L_B \equiv T^2 h_2$ and $L_{B'} \equiv T^5 h_5$ with h_2, h_5 monic of degrees 2 and 5 and $h_2 h_5 = (T^2+T+6)(T^5+11T^4+8T^3+T+1)$. As the quintic is irreducible over $\mathbb{F}_{13}$, $h_2 = T^2+T+6$, which gives (7.5) below.

Candidates. Hence $L_B = T^4+aT^3+bT^2+13aT+169$ with $a \equiv 1$, $b \equiv 6 \pmod{13}$. Writing $L_B = (T^2-\beta_1 T+13)(T^2-\beta_2 T+13)$ with β_i real and $|\beta_i| \le 2\sqrt{13}$, one has $a = -(\beta_1+\beta_2)$ and $b = \beta_1\beta_2 + 26$. So $a=1$ and $b \in \{-7, 6, 19\}$ (the bounds allow $a \in \{1, -12, 14\}$, but $a=-12$ forces $b \in \{61, 62\}$ and $a=14$ forces $b=75$, none $\equiv 6 \pmod{13}$). For each b the five coefficients above determine the coefficients of $T^9, \dots, T^5$ of $L_{B'} = L_P/L_B$, and the functional equation the rest. For $b=19$ the resulting $L_{B'}$ has roots off the circle $|T| = \sqrt{13}$. For $b=6$ it is (7.3), and for $b=-7$ it is

$$T^{10} - 2T^9 + 21T^8 - 52T^7 + 352T^6 - 766T^5 \\ + 4576T^4 - 8788T^3 + 46137T^2 - 57122T + 371293.$$

Both are Weil polynomials (the real polynomials h with $L = T^d h(T+13/T)$ have all their roots in $[-2\sqrt{13}, 2\sqrt{13}]$) and satisfy the congruence modulo 13.

The choice of L_B. The candidate $b=-7$ is excluded by the proof of Lemma 6.8, which shows, independently of this proposition, that Frobenius at 13 acts on a 4-dimensional Galois submodule of $P[2]$ with characteristic polynomial $(T+1)^2(T^2+T+1)$, whereas for $b=-7$, $L_P \equiv (T^4+T^3+T^2+T+1)(T+1)^{10} \pmod 2$ is prime to T^2+T+1. Alternatively, one more point count excludes it: the two candidates give L_P with sixth power sums -3533 ($b=6$) and -7823 ($b=-7$), and the procedure used for (7.1) gives $\#\overline{\mathcal{X}}(\mathbb{F}_{13^6}) = 4823533$ and $\#\overline{C}(\mathbb{F}_{13^6}) = 4827066$, whose difference is -3533 (Appendix D.3).

So L_B and $L_{B'}$ are (7.2) and (7.3), with $L_B(1) = 190$, $L_{B'}(1) = 331275$ and $N = L_B(1)L_{B'}(1)$. Over $\mathbb{Q}$, $L_B = (T^2-4T+13)(T^2+5T+13)$ and $L_{B'}$ is irreducible. □

We record the reductions modulo 13:

$$L_B(T) \equiv T^2(T^2+T+6), \\ L_{B'}(T) \equiv T^5(T^5+11T^4+8T^3+T+1) \pmod{13}. \tag{7.5}$$

So B and B' are ordinary at 13 (the unit-root factors have degrees 2 and 5), and these factors are coprime modulo 13: the quadratic has roots 4 and 8 in $\mathbb{F}_{13}$, and the quintic is irreducible. By (7.5), $N = L_B(1)L_{B'}(1) \equiv (1+1+6)(1+11+8+1+1) \equiv 7 \pmod{13}$, so N is prime to 13, as needed in Lemma 7.8.

7.3. **Integral odd differentials and the Cartier operator.** Let Ω^- be the space of odd regular differentials on C, those with $\tau^*\omega = -\omega$, of dimension $g(C) - g(\mathcal{X}) = 7$. It is the cotangent space of P at the origin. As C has good reduction at 13, $\Omega^- \otimes \mathbb{Q}_{13}$ contains the lattice

$$\Lambda^- = H^0(C_{\mathbb{Z}_{13}}, \Omega^1)^- \subset \Omega^- \otimes \mathbb{Q}_{13}$$

of odd differentials regular on the smooth model over $\mathbb{Z}_{13}$, free of rank 7. By Abel–Jacobi it is the cotangent lattice of the Néron model of P: the Néron model of J is Pic^0 of the smooth model [7, §9.5, Theorem 4], with cotangent lattice $H^0(C_{\mathbb{Z}_{13}}, \Omega^1) = \Lambda^+ \oplus \Lambda^-$, where Λ^+ is the even part, and Λ^+ vanishes on the tangent space of P. Reduction identifies $\Lambda^- \otimes \mathbb{F}_{13}$

with $H^0(\overline{C},\Omega^1)^-$: it is injective, as an element of Λ^- with zero reduction is 13 times a differential regular along $\overline{C}$, hence on the normal scheme $C_{\mathbb{Z}_{13}}$, and both sides have dimension $g(\overline{C})-g(\overline{\mathcal{X}})=7$. The function $u=x_1/x_0$ is a local parameter at the rational cusp P_0 of $\mathcal{X}$, and its reduction is a local parameter at $\overline{P_0}$, as u is unramified at $\overline{P_0}$ (Lemma 7.5(c)). As q is unramified, the pullback of u to C is a local parameter at Q_0 and Q_1. For a differential ω regular at Q_0 we write $\omega(Q_0)$ for the value of ω/du at Q_0.

The Cartier operator. For a smooth proper curve Γ over $\mathbb{F}_{13}$, the Cartier operator $\mathcal{C}$ on $H^0(\Gamma,\Omega^1)$ is characterized by $\mathcal{C}(g^{13}\omega)=g\,\mathcal{C}(\omega)$, $\mathcal{C}(dg)=0$ and $\mathcal{C}(g^{12}dg)=dg$. In a local parameter s at a rational point,

$$\mathcal{C}\Big(\sum_{n\geq 0} a_n s^n\,ds\Big)=\sum_{m\geq 0} a_{13m+12}\,s^m\,ds,$$

see [1, §2.2], following Serre. It is $\mathbb{F}_{13}$-linear, the field being prime, and by Serre duality adjoint to the Frobenius F on $H^1(\Gamma,\mathcal{O}_\Gamma)$ [1, §2.4]. Its matrix C in a basis (ν_j) is defined by $\mathcal{C}(\nu_j)=\sum_i \mathsf{C}_{ij}\nu_i$, so that it acts on columns of coordinates [1, §1.1]. The matrix of F in the dual basis of $H^1(\Gamma,\mathcal{O}_\Gamma)$ is then $\mathsf{C}^{\intercal}$ [1, (1.1), §2.4]. The two have the same characteristic polynomial, which is what Proposition 7.4 uses. Subspaces of differentials, as in Proposition 7.7, are described by C itself. (Over a non-prime field the matrix of F is the transpose of C with a Frobenius twist of the entries [1, §2.4]. Over $\mathbb{F}_{13}$ this twist is trivial.)

The odd differentials. Let ω_0 be the regular differential on $\mathcal{X}$ corresponding to x_0 in the canonical embedding, normalized by $(\omega_0/du)(P_0)=1$, which is possible as $\operatorname{div}(\omega_0)=D_{x_0}$ does not contain P_0. Let w be the function on C with $w^2=r$ and $w/(t-1)^6=1$ at Q_0 (Proposition 5.10). For a quadratic form Q in $x_0,\dots,x_7$ put

$$\nu_Q=\frac{Q\,\omega_0}{x_0^2\,w}.$$

Lemma 7.5. (a) *ν_Q is a regular differential on C if and only if Q vanishes on the divisor $6P_0+E_c$ of Proposition 5.10, that is, if and only if $Q^2\equiv r_0 s$ modulo the ideal of $\mathcal{X}$ for some quadratic form s; it is then odd.*

(b) *Let $\mathcal{Q}_1,\dots,\mathcal{Q}_7$ be the seven quadratic forms with rational coefficients given in the supplementary data [31], whose reductions modulo 13 are the forms $\overline{\mathcal{Q}}_1,\dots,\overline{\mathcal{Q}}_7$ of Table 15. Then $\nu_j:=\nu_{\mathcal{Q}_j}$ lies in Λ^- for each j, and $\nu_1,\dots,\nu_7$ is a $\mathbb{Z}_{13}$-basis of Λ^-.*

(c) *On $\overline{\mathcal{X}}$, the map u is simply ramified at 42 geometric points, none of them rational and none over $u=\infty$; the reduction of ω_0 is $\overline{\omega}_0=x_0^3\,du/\overline{\Delta}$, where $\overline{\Delta}$ is the cubic form (D.4), the unique cubic form modulo I whose divisor is the ramification divisor of u and which takes the value 1 at $\overline{P_0}$. On the chart $x_0=1$,*

$$\overline{\nu}_j=\frac{\overline{\mathcal{Q}}_j\,du}{\overline{\Delta}\,\overline{w}},\qquad \overline{w}^{\,2}=\overline{r}_0,\qquad \overline{w}/u^6=1 \text{ at } \overline{Q_0}.$$

In particular any lifts to Λ^- of $\overline{\nu}_1,\dots,\overline{\nu}_7$ form a $\mathbb{Z}_{13}$-basis of Λ^-.

Proof. (a) On C, $\operatorname{div}(\omega_0)=q^*D_{x_0}$ and, by (5.2), $\operatorname{div}(w)=q^*(6P_0+E_c-D_{x_0})$, the cover being unramified. If H_Q is the divisor on $\mathcal{X}$ of the section Q of $\mathcal{O}(2)$, then $\operatorname{div}(\nu_Q)=q^*(H_Q-6P_0-E_c)$, so ν_Q is regular if and only if $H_Q\geq 6P_0+E_c$. As $\operatorname{div}(r_0)=12P_0+2E_c$ and $\mathcal{X}$ is projectively normal, this holds if and only if $Q^2\in r_0H^0(\mathcal{X},\mathcal{O}(2))$. The differential ν_Q is odd because $\tau^*w=-w$, while ω_0, Q and x_0 are pulled back from $\mathcal{X}$.

(b) The identities $\mathcal{Q}_j^2\equiv r_0 s_j$ modulo the ideal of $\mathcal{X}$ hold over $\mathbb{Q}$: $\mathcal{Q}_j^2$ reduces to zero modulo a Gröbner basis of the ideal generated by the fifteen quadrics and r_0. So $\nu_j\in\Omega^-$

by (a). Integrality: u is a local parameter at P_0 on both fibres, so du generates the relative differentials of $\mathcal{X}_{\mathbb{Z}_{13}}$ near the section P_0, and $(\omega_0/du)(P_0) = 1$ is a unit. Hence ω_0 has no vertical zero or pole, i.e. it is regular along $\overline{\mathcal{X}}$ with nonzero reduction. The functions x_0 and w are units at the generic point of $\overline{C}$, as $w^2 = r_0/x_0^2$ and $\overline{r}_0 \notin I$. Each $\mathcal{Q}_j$ has 13-integral coefficients, not all divisible by 13, in the basis of standard monomials of $H^0(\mathcal{X}_{\mathbb{Z}_{13}}, \mathcal{O}(2))$ (proof of Proposition 7.1), with reduction $\overline{\mathcal{Q}}_j$. Therefore ν_j is regular at the generic point of $\overline{C}$, with reduction $\overline{\nu}_j = \overline{\mathcal{Q}}_j\overline{\omega}_0/(x_0^2\overline{w}) \neq 0$, and, being regular on the generic fibre, it is regular on the normal scheme $C_{\mathbb{Z}_{13}}$: $\nu_j \in \Lambda^-$. As the $\overline{\mathcal{Q}}_j$ are linearly independent modulo I, the $\overline{\nu}_j$ form a basis of $H^0(\overline{C}, \Omega^1)^- = \Lambda^- \otimes \mathbb{F}_{13}$, and by Nakayama's lemma $\nu_1, \dots, \nu_7$, or any lifts of the $\overline{\nu}_j$, form a basis of Λ^-.

(c) On the chart $x_0 = 1$ the ramification scheme of u is cut out by I and the 6×6 minors of the Jacobian matrix of the $\overline{q}_i$ with respect to $x_2, \dots, x_7$ (the Fitting ideal of the relative differentials). It is reduced, of length 42, with closed points of degrees $2, 2, 2, 3, 4, 5, 24$. The fibre over $u = \infty$ ($x_0 = 0$) is reduced, of length 14. So u is simply ramified at $42 = 2 \cdot 8 - 2 + 2 \cdot 14$ geometric points, all with $x_0 \neq 0$, and $\operatorname{div}(du) = R_u - 2\overline{D}_{x_0}$, with R_u this ramification divisor. As $\operatorname{div}(\overline{\omega}_0) = \overline{D}_{x_0}$, $\overline{\omega}_0 = x_0^3\, du/\overline{\Delta}$ for a cubic form $\overline{\Delta}$ with divisor R_u. The cubic forms modulo I vanishing on R_u form a 1-dimensional space, spanned by (D.4), and the normalization at $\overline{P_0} = (1 : 0 : \cdots : 0)$ picks out (D.4) itself. Finally, $\overline{w}/u^6$ and $\overline{w}/(\bar{t} - 1)^6$ agree at $\overline{Q_0}$, as $\bar{t} - 1 = u + O(u^2)$ there (Lemma 7.2). □

Proposition 7.6. *Let $\nu_1, \dots, \nu_7$ be the basis of Λ^- of Lemma 7.5. With respect to this basis:*

(a) *the Cartier operator on $\Lambda^- \otimes \mathbb{F}_{13} = H^0(\overline{C}, \Omega^1)^-$ satisfies $\mathcal{C}(\overline{\nu}_j) = \sum_i \mathsf{C}_{ij}\, \overline{\nu}_i$ with*

$$\mathsf{C} = \begin{pmatrix} 11 & 3 & 8 & 1 & 5 & 11 & 5 \\ 1 & 2 & 7 & 12 & 6 & 4 & 3 \\ 8 & 11 & 2 & 9 & 1 & 8 & 6 \\ 8 & 5 & 10 & 3 & 2 & 12 & 10 \\ 8 & 0 & 12 & 8 & 10 & 1 & 10 \\ 3 & 4 & 2 & 12 & 7 & 12 & 1 \\ 9 & 5 & 9 & 0 & 12 & 11 & 0 \end{pmatrix} \quad \text{over } \mathbb{F}_{13}, \tag{7.6}$$

whose characteristic polynomial is $(T^2 + T + 6)(T^5 + 11T^4 + 8T^3 + T + 1)$;

(b) *the kernel of $\mathsf{C}^2 + \mathsf{C} + 6$ is 2-dimensional, spanned by the columns of*

$$\mathsf{K} = \begin{pmatrix} 12 & 3 \\ 5 & 5 \\ 6 & 4 \\ 0 & 4 \\ 11 & 12 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \text{on which } \mathsf{C} \text{ acts by } \begin{pmatrix} 1 & 1 \\ 5 & 11 \end{pmatrix}, \tag{7.7}$$

that is, $\mathsf{CK} = \mathsf{K}\left(\begin{smallmatrix} 1 & 1 \\ 5 & 11 \end{smallmatrix}\right)$;

(c) *the values at Q_0 are $\big(\nu_j(Q_0)\big)_{j=1}^7 \equiv (3, 4, 1, 8, 2, 9, 6) \pmod{13}$.*

Proof. All three statements concern only the $\overline{\nu}_j$ and are computed from Tables 11 and 15 together with (D.4). At $\overline{P_0}$, where u is a local parameter, solving the fifteen quadrics order by order gives $x_2, \dots, x_7$ as power series in u. Along this branch $\overline{r}_0 = u^{12}(1 + 4u + \cdots)$, so $\overline{w} = u^6(1 + 2u + \cdots)$ on the sheet $\overline{Q_0}$, and $\overline{\Delta} = 1 + O(u^7)$. Since each $\overline{\mathcal{Q}}_j$ vanishes to order exactly 6 at $\overline{P_0}$, $\overline{\nu}_j/du = \overline{\mathcal{Q}}_j/(\overline{\Delta}\,\overline{w})$ lies in $\mathbb{F}_{13}[[u]]$. The constant terms are (c). The

seven series are linearly independent already in their coefficients of $u^0, \dots, u^6$, so $\mathcal{C}(\overline{\nu}_j)$ is determined by these coefficients, which by the formula for $\mathcal{C}$ are those of $u^{12}, u^{25}, \dots, u^{90}$ in $\overline{\nu}_j/du$. Solving gives the j-th column of (7.6). The characteristic polynomial, the kernel of $\mathsf{C}^2+\mathsf{C}+6$ and the matrix of C on it follow by linear algebra over $\mathbb{F}_{13}$. (The transpose $\mathsf{C}^\intercal$, the matrix of F, would give a different plane: the kernel of $(\mathsf{C}^\intercal)^2+\mathsf{C}^\intercal+6$ is spanned by $(0,11,6,4,3,1,0)^\intercal$ and $(4,11,3,3,12,0,1)^\intercal$.) □

Proposition 7.7 (The lattice Λ_B)**.** *The pullback of invariant differentials along $f\colon C \to B$ identifies the cotangent lattice of the Néron model of B at 13 with a saturated rank-two direct summand $\Lambda_B \subset \Lambda^-$, and the reduction of Λ_B modulo 13 is the span of the columns of K.*

Proof. The maps of (6.1) extend to the Néron models at 13 by the Néron mapping property. Since $F_B \circ i = [14]$ on B (Proposition 6.2(c)) and 14 is a 13-adic unit, f^* identifies the invariant differentials of B with a summand of Λ^-. Likewise those of B' give a summand $\Lambda_{B'}$. The two summands are the ± 7 eigenlattices of $\mathcal{D}$, and they span Λ^- because 49 is a 13-adic unit.

Put $\overline{\Lambda}_B = \Lambda_B \otimes \mathbb{F}_{13}$ and $\overline{\Lambda}_{B'} = \Lambda_{B'} \otimes \mathbb{F}_{13}$. They are the $+7$ and -7 eigenspaces of $\mathcal{D}$ on $\Lambda^- \otimes \mathbb{F}_{13} = H^0(\overline{C}, \Omega^1)^-$ (distinct, as 14 is a unit), of dimensions 2 and 5. The endomorphism $\mathcal{D}$ of P extends to the Néron model and acts on $H^0(\overline{C}, \Omega^1)^- \simeq H^0(\overline{P}, \Omega^1)$ by pullback along an endomorphism of $\overline{P}$. As the Cartier operator commutes with pullback along morphisms of smooth varieties, and the Abel–Jacobi identification is itself a pullback, $\mathcal{C}$ commutes with $\mathcal{D}$ and preserves $\overline{\Lambda}_B$ and $\overline{\Lambda}_{B'}$. The characteristic polynomial of $\mathcal{C}$ on $\Lambda^- \otimes \mathbb{F}_{13}$, which is $(T^2+T+6)(T^5+11T^4+8T^3+T+1)$ by Proposition 7.6(a), is the product of those on $\overline{\Lambda}_B$ and $\overline{\Lambda}_{B'}$, of degrees 2 and 5. As the quintic is irreducible over $\mathbb{F}_{13}$, the factor on $\overline{\Lambda}_B$ is T^2+T+6. By Cayley–Hamilton, $\mathcal{C}^2+\mathcal{C}+6$ vanishes on $\overline{\Lambda}_B$, and it is invertible on $\overline{\Lambda}_{B'}$ as T^2+T+6 is prime to the quintic. Hence $\overline{\Lambda}_B = \ker(\mathcal{C}^2+\mathcal{C}+6)$, which in the basis $\overline{\nu}_1, \dots, \overline{\nu}_7$ is the span of the columns of K by Proposition 7.6(b). □

7.4. **The precision lemma.** For $R \in C(\mathbb{Q}_{13})$ and $\omega \in \Lambda^-$, write $\int_{Q_0}^R \omega$ for the abelian (Coleman) integral, that is, the value on ω of the 13-adic logarithm of $[R-Q_0] \in J(\mathbb{Q}_{13})$ [12, 58]. The two *cusp periods* of Λ_B are

$$I_j = \int_{Q_0}^{Q_1} \omega_j \qquad (j=1,2), \tag{7.8}$$

where $\omega_1, \omega_2 \in \Lambda_B$ are lifts of the two columns of K.

Lemma 7.8. *For every $\omega \in \Lambda^-$ and every $R \in C(\mathbb{Q}_{13})$, $\int_{Q_0}^R \omega \in 13\mathbb{Z}_{13}$. Consequently the periods I_1, I_2 lie in $13\mathbb{Z}_{13}$, and replacing ω_j by $\omega_j + 13\omega'$ with $\omega' \in \Lambda^-$ changes I_j by an element of $169\mathbb{Z}_{13}$.*

Proof. Put $T_R = (1-\tau)[R-Q_0] = [R-\tau R+Q_1-Q_0] \in P(\mathbb{Q}_{13})$. The Néron model $\mathcal{P}$ of P over $\mathbb{Z}_{13}$ is an abelian scheme, with module of invariant differentials Λ^-. Multiplication by $N = \#P(\mathbb{F}_{13})$ sends T_R into the kernel of reduction, the group of points of the formal group $\widehat{\mathcal{P}}$ with coordinates in $13\mathbb{Z}_{13}$: if $z_1, \dots, z_7$ are formal parameters of $\mathcal{P}$ along the zero section, $z(NT_R) \in (13\mathbb{Z}_{13})^7$.

Let $\omega \in \Lambda^-$, viewed as an invariant differential on $\mathcal{P}$. In the formal parameters, $\omega = \sum_i f_i(z)\,dz_i$ with $f_i \in \mathbb{Z}_{13}[[z]]$, and ω is closed: over $\mathbb{Q}_{13}$ the logarithm is an isomorphism of the formal group with the additive one, under which invariant differentials become constant ones. The logarithm against ω is the unique series $\lambda \in \mathbb{Q}_{13}[[z]]$ with $\lambda(0)=0$ and $d\lambda = \omega$, and its value at NT_R is $\lambda(z(NT_R))$. Write $f_i = \sum_{n \geq 1} f_{i,n-1}$ with $f_{i,n-1}$ homogeneous of

degree $n-1$, and $\omega^{(n)} = \sum_i f_{i,n-1}\,dz_i$. Closedness gives $d\omega^{(n)} = 0$, and the Euler vector field $E = \sum_i z_i\,\partial/\partial z_i$ satisfies $\mathcal{L}_E\,\omega^{(n)} = n\,\omega^{(n)}$. By Cartan's formula

$$n\,\omega^{(n)} = \mathcal{L}_E\,\omega^{(n)} = d(\iota_E\,\omega^{(n)}) + \iota_E\,d\omega^{(n)} = d\Big(\sum_i z_i f_{i,n-1}\Big).$$

Hence the homogeneous part of degree n of λ is $\lambda_n = \frac{1}{n}\sum_i z_i f_{i,n-1}(z)$, with coefficients in $\frac{1}{n}\mathbb{Z}_{13}$, of 13-adic valuation at least $-v_{13}(n)$. For $z \in (13\mathbb{Z}_{13})^7$, $\lambda_n(z)$ has valuation at least $n - v_{13}(n) \geq 1$, and these valuations tend to infinity, so $\lambda(z(NT_R)) \in 13\mathbb{Z}_{13}$. As N is prime to 13 (Section 7.2), the logarithm of T_R against ω lies in $13\mathbb{Z}_{13}$. For odd ω it is $\langle \log[R - Q_0], (1-\tau)^*\omega\rangle = 2\int_{Q_0}^{R}\omega$, and 2 is a unit. Taking $R = Q_1$ gives the statement about I_j, and the last assertion follows by linearity, from the first applied to ω'. □

So a computation modulo 169 suffices: the periods lie in $13\mathbb{Z}_{13}$, and what matters in Section 8 is $(I_1/13, I_2/13)$ modulo 13, which is determined by (I_1, I_2) modulo 169 and does not depend on the lifts ω_1, ω_2. Likewise the periods $\int_{Q_0}^{Q_1}\nu_j$ modulo 169 depend only on the reductions $\overline{\nu}_j$ of Lemma 7.5.

8. Arithmetic in the Jacobian and the two residue discs

We now compute the cusp periods I_1, I_2 of (7.8) modulo 169. From the exact periods we define a differential η on C whose abelian integral vanishes between any two rational points, and the computed congruences show that η has a unit value at both cusps. This proves Theorem 8.6, which together with Lemma 7.3 gives Theorem 1.1 (Section 8.7).

8.1. **Strategy.** Since τ interchanges Q_0 and Q_1, the Prym class of the cusp difference is

$$T_{Q_1} = (1-\tau)[Q_1 - Q_0] = 2[Q_1 - Q_0] \in P(\mathbb{Q}_{13}),$$

and by (7.4) the multiple

$$\mu := 2N = 125884500 = 169 \cdot 744878 + 118, \qquad \mu^{-1} \equiv 53 \pmod{169}, \tag{8.1}$$

sends $[Q_1 - Q_0]$ into the kernel of reduction of J at 13: $\mu[Q_1 - Q_0] = N\,T_{Q_1}$ lies in the formal group. On the formal group the 13-adic logarithm against an integral differential can be computed as a formal integral, and modulo 169 only its linear term in the formal coordinates contributes (Section 8.3). We therefore represent the divisor class $\mu[Q_1 - Q_0]$ explicitly modulo 169 by arithmetic in J (Section 8.2) and read off its formal coordinates relative to a fixed reference divisor (Section 8.3). Integrating the seven basis differentials ν_j then gives $\mu\int_{Q_0}^{Q_1}\nu_j$ modulo 169, and it remains to divide by the unit μ. Modulo 169 this division has no effect: as $\mu \equiv 1 \pmod{13}$, multiplication by $\mu^{-1} \equiv 53$ fixes an element of $\mathbb{Z}/169\mathbb{Z}$ if and only if it is divisible by 13, and the integrals are divisible by 13 by Lemma 7.8.

8.2. **Divisor arithmetic over $\mathbb{Z}/169\mathbb{Z}$.** Arithmetic in J is carried out with Khuri-Makdisi's algorithms [34, 35], in which a divisor class is represented by a subspace of sections of a fixed line bundle, and addition and subtraction of classes are multiplication and division of section spaces. Fix the divisor

$$D_0 = K_C + 3Q_0, \qquad \deg D_0 = 31,$$

and let $V_n = L(nD_0)$ for $1 \le n \le 5$ and $V_1' = L(D_0 + Q_0)$. By Riemann–Roch, since all these divisors have degree at least $2g(C) - 1 = 29$,

$$\dim V_n = 31n - 14 = 17,\ 48,\ 79,\ 110,\ 141\ (n = 1, \dots, 5), \qquad (8.2)$$
$$\dim V_1' = 18.$$

These are the spaces on the explicit model of C over $\mathbb{Q}$. Their bases are computed with rational coefficients and then saturated to give bases of the corresponding free $\mathbb{Z}_{13}$-modules of sections on the smooth model. We represent a section by its first 64 Taylor coefficients at an auxiliary closed point of residue degree 3. This gives an evaluation map to a space of dimension $192 > 155 = \deg 5D_0$, which is injective on every space used. The evaluation matrices have full rank modulo 13, so one of their maximal minors is a unit, and evaluation is injective over $\mathbb{Z}_{13}$ as well.

Khuri-Makdisi's algorithms are stated over a field. The following lemma shows that they remain valid over $\mathbb{Z}/169\mathbb{Z}$.

Lemma 8.1. *Let $\mathcal{L}$ be a line bundle on the smooth model $C_{\mathbb{Z}_{13}}$ whose restrictions to the generic and special fibres are nonspecial and base-point-free. Then $H^0(C_{\mathbb{Z}_{13}}, \mathcal{L})$ is a free $\mathbb{Z}_{13}$-module whose formation commutes with base change; in particular its reduction is $H^0(C_{\mathbb{F}_{13}}, \mathcal{L}_{\mathbb{F}_{13}})$. Consequently:*

(i) *(addition) if $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2$ and a set of products of sections of $\mathcal{L}_1$ and $\mathcal{L}_2$ reduces to a spanning set of $H^0(C_{\mathbb{F}_{13}}, \mathcal{L}_{\mathbb{F}_{13}})$, it spans $H^0(C_{\mathbb{Z}_{13}}, \mathcal{L})$ integrally;*

(ii) *(subtraction) the kernel of a linear map of free modules whose kernels on the generic and special fibres have the same dimension d is free of rank d and reduces onto the kernel on the special fibre, and after choosing d coordinates on which the reduced kernel projects isomorphically (a unit minor), the integral kernel is the graph of a map whose reduction modulo 169 is found by elimination over $\mathbb{Z}/169\mathbb{Z}$.*

Proof. For a nonspecial line bundle, H^1 vanishes on both fibres, so, by cohomology and base change, H^0 commutes with base change and is free. Part (i) follows from Nakayama's lemma. For (ii), the integral kernel is free, of rank d, the dimension of the generic kernel. As the kernel of a map of free modules it is saturated, so its reduction injects into the reduced kernel, which has dimension d, and is therefore equal to it. Hence projection to d coordinates with a unit minor is an isomorphism, by Nakayama's lemma, and the graph description follows. Since all pivots are units, the same elimination can be carried out modulo 169. □

In the algorithm the relevant bundles are $\mathcal{O}(nD_0)$ for $n \le 5$, $\mathcal{O}(2D_0 - D)$ for effective D of degree 31 in the classes that occur, and the tensor products of two of these that arise as products of section spaces. These have degrees at least 31, hence are nonspecial and base-point-free on both fibres. By Khuri-Makdisi's results over a field, the kernels computed in the algorithm are, on each fibre, spaces $L(2D_0 - D)$, of dimension $31 - 15 + 1 = 17$, so $d = 17$ in (ii). For the section ψ of Section 8.3, $d = 1$. All pivots are units of $\mathbb{Z}/169\mathbb{Z}$, and all products lie in spaces on which evaluation is injective. The addition algorithm returns the negative of the sum, so the sign of each group operation is tracked.

An effective divisor D of degree 31 is represented by $W_D = L(2D_0 - D) \subset V_2$. The zero class is $W_{D_0} = L(D_0)$, and the cusp difference is represented by $D = D_0 - Q_0 + Q_1$, with $W_D = L(D_0 + Q_0 - Q_1)$, a hyperplane in V_1'. This fixes the sign convention $[D - D_0] = [Q_1 - Q_0]$.

8.3. **The reference divisor and the formal coordinates.** Let E_0 be the residual divisor of the section of $L(D_0)$, unique up to scaling, that vanishes to order 16 at Q_1. It is effective

of degree 15, and its reduction consists of four closed points, of residue degrees $1, 3, 3, 8$. Moreover $h^0(\overline{E_0}) = 1$ and $h^1(\overline{E_0}) = 0$, since the 15×15 matrix in the proof of Proposition 8.2, the differential of the Abel–Jacobi map at $\overline{E_0}$, is invertible modulo 13. Hence $h^0(E_0) = 1$ and $h^1(E_0) = 0$ as well, the Abel–Jacobi map is étale at E_0 over $\mathbb{Z}_{13}$, and a divisor E with the same reduction as E_0 is determined by the local parameters of its points, all of which are congruent to those of E_0 modulo 13. For a closed point of $\overline{E_0}$ of degree d, let $\mathcal{O}$ be the ring of integers of the unramified extension of $\mathbb{Q}_{13}$ of degree d, and let S be a function on the smooth model whose reduction is a local parameter at that point. For such E and an integral differential $\omega = \sum_{n \geq 0} a_n S^n \, dS$, with the corresponding points of E_0 and E at $S = s_0$ and $S = s$, where $s_0, s \in 13\mathcal{O}$, the local integral is

$$\int_{s_0}^{s} \omega \equiv a_0(s - s_0) \pmod{169},$$

since every term of degree $n \geq 1$ has valuation at least $(n+1) - v_{13}(n+1) \geq 2$. The logarithm of $[E - E_0]$ against ω is the sum over the points of E_0 of the traces to $\mathbb{Q}_{13}$ of these local integrals.

If W_D represents a class in the formal group, the section ψ of $L(2D_0 - D - 16Q_1)$, unique up to scaling, has divisor $E + 16Q_1 + D - 2D_0$ with E effective and with the same reduction as E_0. Comparing with $\operatorname{div}(\psi_0) = E_0 + 16Q_1 - D_0$ for the section ψ_0 of $L(D_0)$ defining E_0 gives $[E - E_0] = -[D - D_0]$. The logarithm of $\mu[Q_1 - Q_0]$ is therefore the *negative* of the sum of the traces.

8.4. **The cusp periods.**

Proposition 8.2. *In the basis $\nu_1, \ldots, \nu_7$ of Lemma 7.5,*

$$\Big(\int_{Q_0}^{Q_1} \nu_j \Big)_{j=1}^{7} \equiv (39, 39, 156, 143, 39, 52, 26) \pmod{169}. \tag{8.3}$$

Consequently, with $\omega_1, \omega_2 \in \Lambda_B$ lifting the columns of K,

$$\begin{aligned} (I_1, I_2) &\equiv (52, 143) \pmod{169}, \\ (I_1/13, I_2/13) &\equiv (4, 11) \pmod{13}, \end{aligned} \tag{8.4}$$

and, by Proposition 7.6(c), $(\omega_1(Q_0), \omega_2(Q_0)) \equiv (2, 4) \pmod{13}$.

Proof. The class $\mu[Q_1 - Q_0]$ is computed from W_D, $D = D_0 - Q_0 + Q_1$, by a signed double-and-add chain of the operations of Section 8.2 modulo 169. For the resulting representative, the section ψ of Section 8.3 gives the divisor E. The traces of $a_0(s - s_0)$ at the four closed points of E are summed for each ν_j, and by Section 8.3 the negatives of these sums are $\mu \int_{Q_0}^{Q_1} \nu_j$ modulo 169. Division by μ uses (8.1). The inputs of this last step, namely the four residue rings (D.2), the displacements $\delta_i = s - s_0$ and, for the fifteen integral differentials ($\nu_1, \ldots, \nu_7$ and eight even ones), the constant terms a_0 and the sixty traces, are printed in Appendix D.1 (Table 13). The 15×15 matrix over $\mathbb{Z}/169\mathbb{Z}$ of the linear map $(\delta_i)_i \mapsto \big(\sum_i \operatorname{Tr}(a_0(\omega, P_i)\, \delta_i) \big)_\omega$ of (D.3), with ω running through the fifteen integral differentials and rows and columns in the order of Table 13, has determinant 9 modulo 13. So the displacements are determined by the class. The logarithms against the eight even differentials (those pulled back from $\mathcal{X}$) vanish, as they must for a class in the Prym. Since $\omega_j \equiv \sum_i \mathsf{K}_{ij} \nu_i$ modulo $13\Lambda^-$, the last assertion of Lemma 7.8 gives $I_j \equiv \sum_i \mathsf{K}_{ij} \int_{Q_0}^{Q_1} \nu_i \pmod{169}$, so $(I_1, I_2) \equiv (52, 143)$ by (8.3). The same projection applied to the values of Proposition 7.6(c) gives $(\omega_1(Q_0), \omega_2(Q_0)) \equiv (2, 4)$. □

8.5. **The annihilating differential.**

Definition 8.3. With the periods $I_1, I_2 \in 13\mathbb{Z}_{13}$ of (7.8), put

$$\eta = \frac{I_2\,\omega_1 - I_1\,\omega_2}{13} \in \Lambda_B. \tag{8.5}$$

By Lemma 7.8 both $I_j/13$ lie in $\mathbb{Z}_{13}$, so η is an integral differential, and by (8.4) its coefficients in the basis $\nu_1, \dots, \nu_7$ are congruent modulo 13 to $\mathsf{K}\,(11, -4)^{\intercal} = (3, 9, 11, 10, 8, 11, 9)^{\intercal}$. In particular, since $(\omega_1(Q_0), \omega_2(Q_0)) \equiv (2, 4)$ by Proposition 8.2,

$$\begin{aligned} \eta(Q_0) &\equiv 11 \cdot 2 - 4 \cdot 4 = 6 \pmod{13}, \\ \eta(Q_1) &= -\eta(Q_0) \equiv 7 \pmod{13}, \end{aligned} \tag{8.6}$$

the second because η is odd, τ interchanges the cusps, and u is τ-invariant. Both values are units. By (8.4), $(I_1, I_2) \neq (0, 0)$, so the abelian logarithm of $f(Q_1)$ is nonzero.

Proposition 8.4. *For every $R \in C(\mathbb{Q})$, $\int_{Q_0}^{R} \eta = 0$.*

Proof. For $\omega \in \Lambda_B$ and $R \in C(\mathbb{Q})$, the abelian integral $\int_{Q_0}^{R} \omega$ is the value on ω of the logarithm of $f(R) \in B(\mathbb{Q}) \subset B(\mathbb{Q}_{13})$, since ω is pulled back from an invariant differential on B along f and $f(Q_0) = 0$. By Proposition 6.13, $B(\mathbb{Q})$ has rank one and $f(Q_1)$ has infinite order, so for every $R \in C(\mathbb{Q})$ there are integers $m \neq 0$ and n with $m\,f(R) - n\,f(Q_1)$ torsion. The logarithm kills torsion and is linear, so $m \log f(R) = n \log f(Q_1)$ in the 2-dimensional $\mathbb{Q}_{13}$-vector space of logarithms. In coordinates, $\big(\int_{Q_0}^{R} \omega_1, \int_{Q_0}^{R} \omega_2\big)$ is proportional to (I_1, I_2). Hence

$$\int_{Q_0}^{R} \eta = \frac{1}{13}\Big(I_2 \int_{Q_0}^{R} \omega_1 - I_1 \int_{Q_0}^{R} \omega_2\Big) = 0. \qquad \square$$

8.6. **Uniqueness in the two discs.** We first prove a uniqueness statement for a single residue disc.

Proposition 8.5 (Uniqueness in a residue disc)**.** *Let Γ be a smooth projective curve over $\mathbb{Q}$ with good reduction at an odd prime p, let $Q \in \Gamma(\mathbb{Q})$, let u be a local parameter at Q whose reduction is a local parameter at $\overline{Q} = \mathrm{red}_p(Q)$ on the special fibre of the smooth model over $\mathbb{Z}_p$, and let η be a differential on Γ that is regular on the smooth model over $\mathbb{Z}_p$ with $\eta(Q) = (\eta/du)(Q) \in \mathbb{Z}_p^{\times}$. If $\int_{Q}^{R} \eta = 0$ for every $R \in \Gamma(\mathbb{Q})$, then Q is the only rational point in its residue disc: $\Gamma(\mathbb{Q}) \cap \mathrm{red}_p^{-1}(\overline{Q}) = \{Q\}$.*

Proof. On the residue disc $\{u \in p\mathbb{Z}_p\}$ write $\eta = (a_0 + a_1 u + a_2 u^2 + \cdots)\,du$ with $a_n \in \mathbb{Z}_p$ and $a_0 = \eta(Q)$ a unit. For R in the disc the abelian integral from Q to R is the formal integral

$$\int_{Q}^{R} \eta = u(R)\Big(a_0 + \sum_{n \geq 1} \frac{a_n\,u(R)^n}{n+1}\Big).$$

For $u(R) \in p\mathbb{Z}_p$ each term of the bracket with $n \geq 1$ has valuation at least $n - v_p(n+1) \geq 1$, and these valuations tend to infinity. Hence the bracket converges to a p-adic unit, and the integral vanishes only when $u(R) = 0$, that is, at $R = Q$. If R is rational the integral vanishes by hypothesis, so $R = Q$. $\square$

Theorem 8.6. *On the good model at 13,*

$$C(\mathbb{Q}) \cap \mathrm{red}_{13}^{-1}\{\overline{Q_0}, \overline{Q_1}\} = \{Q_0, Q_1\}.$$

Proof. Apply Proposition 8.5 to $\Gamma = C$ with $p = 13$ and the parameter u of Section 7.3. At $Q = Q_0$: η is integral by Lemma 7.8, $\eta(Q_0) \equiv 6$ is a unit by (8.6), and $\int_{Q_0}^{R} \eta = 0$ for all $R \in C(\mathbb{Q})$ by Proposition 8.4. At $Q = Q_1$: $\eta(Q_1) \equiv 7$ is a unit, and for $R \in C(\mathbb{Q})$,

$$\int_{Q_1}^{R} \eta = \int_{Q_0}^{R} \eta - \int_{Q_0}^{Q_1} \eta = 0 - \frac{I_2 I_1 - I_1 I_2}{13} = 0. \qquad \square$$

Remark 8.7 (Scope of the method). Apart from the identification of $\mathcal{X}$ and C (Sections 4 and 5) and the two-descent (Sections 6.2 to 6.4), which are specific to $X^5 + Y^3 = Z^7$, the method uses only four ingredients. The first is an unramified double cover $C \to \mathcal{X}$ with a rational point R attached to a solution. The second is an abelian subvariety B of the Prym with $\operatorname{rank} B(\mathbb{Q}) < \dim B$, an eigenspace of a correspondence commuting with the involution. The third is a prime p of good reduction that confines R to the residue discs of finitely many known rational points Q_i. The fourth is, for each i, an integral differential coming from B that annihilates $B(\mathbb{Q})$ and has a unit value at Q_i. The method then shows that R is one of the Q_i, but it does not determine $C(\mathbb{Q})$.

8.7. **Proof of Theorem 1.1.**

Proof. Suppose (X, Y, Z) satisfies (1.1) and $A_\nu \simeq L_a$ for some $1 \le a \le 6$. By Propositions 4.12 and 5.3 there is a point $R \in C(\mathbb{Q})$ with $t(q(R)) = -X^5/Y^3$. By Lemma 7.3, R reduces modulo 13 to $\overline{Q_0}$ or $\overline{Q_1}$, and by Theorem 8.6 it is then Q_0 or Q_1. But $q(Q_0) = q(Q_1) = P_0$ and $t(P_0) = 1$, whereas $t(q(R)) = -X^5/Y^3 \ne 1$ because $X^5 + Y^3 = Z^7 \ne 0$. This contradiction proves the theorem. $\square$

Appendix A. Index of notation

Throughout, (X, Y, Z) is a hypothetical solution of (1.1): nonzero coprime integers with $X^5 + Y^3 = Z^7$. Table 4 lists the symbols that are used in more than one section. Its first part contains the notation for the equation and the exceptional field (Sections 1 to 3 and Appendix B), and its second part the notation for the pure fields (Sections 4 to 8 and Appendices C and D). Some letters, for example Δ, F, H, L, R, S and V, also have local meanings, which are stated where they are used. Unrelated objects may share a letter and differ in their subscripts, as L_a, L_p and L_B do.

Table 4. Symbols used in more than one section.

Symbol	Meaning
t	$-X^5/Y^3$, the parameter of the Frey family H_t
ν	$X^5/Z^7 = t/(t-1)$, in $\mathbb{Q} \smallsetminus \{0, 1\}$
$\phi(T)$	$15T^7 - 35T^6 + 21T^5$
A_ν	the septic algebra $\mathbb{Q}[T]/(\phi(T) - \nu)$
L_a	the pure field $\mathbb{Q}\big((3^a \cdot 5)^{1/7}\big)$, $1 \le a \le 6$
F	the exceptional septic field, $\mathbb{Q}[x]/(h(x))$ with h as in (2.1)
ϖ	the class of x in $F = \mathbb{Q}[x]/(h(x))$; elements and ideals of $\mathcal{E}$ are written in terms of ϖ and $\sqrt{-35}$
$h,\ f_b,\ f_P$	the three defining polynomials of F (Section 2.3)
ϑ	the root of $\phi(T) - \nu$ in F supplied by an isomorphism $A_\nu \simeq F$
$\mathcal{E},\ \sigma$	$F(\sqrt{-35})$, of degree 14; its involution over F
$\sqrt{-35}$	a fixed square root of -35 in $\mathcal{E}$; $\sigma(\sqrt{-35}) = -\sqrt{-35}$

TABLE 4. (continued)

Symbol	Meaning
$a_+,\ a_-$	$(35 \pm \sqrt{-35})/2$, so $a_+a_- = 315$
$\beta,\ \Delta,\ V$	$15Z\vartheta$; $15Z - \beta$; $\beta - Za_+$
S	the ten primes of $\mathcal{E}$ above 3, 5 and 7
$\mathcal{O}_{\mathcal{E},S}$	the ring of S-integers of $\mathcal{E}$
$\mathcal{M}$	$\mathcal{E}(S,5)$, the classes in $\mathcal{E}^\times/\mathcal{E}^{\times 5}$ with valuations divisible by 5 outside S (3.7); $\dim_{\mathbb{F}_5} \mathcal{M} = 16$
$g_1, \dots, g_{16}$	the basis of $\mathcal{M}$ in Section 3; in Section 6.4, $g_0, \dots, g_5$ denote the generators of $\mathcal{V} \subset L^\times/L^{\times 2}$
$S_\sigma,\ \mathrm{Val}$	the matrices of σ and of the S-valuations on the g_j
$\mathcal{A}$	the 125-element affine set of Theorem 3.9
L_p	the matrix of the characters $\lambda_{\mathfrak{q}}$, $\mathfrak{q} \mid p$, on $g_1, \dots, g_{16}$ (Section 3.6), $p \in \{11, 19\}$
$K,\ e,\ k$	$\mathbb{Q}(\sqrt{5})$; $(1+\sqrt{5})/2$; $\mathcal{O}_K/(7) = \mathbb{F}_{49}$
U	$\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$, over which the family H_t is smooth
$H_t,\ J_t$	the genus-2 curve $y^2 = 5x^6 - 12x^5 + 10tx^3 + t^2$; its Jacobian
$[e]$	the endomorphism of J_t given by e under the real multiplication, $[e]^2 - [e] - 1 = 0$
$\mathfrak{d},\ \delta$	$3(5+\sqrt{5})/2$; the quadratic character of $K(\sqrt{\mathfrak{d}})/K$
A_t	the quadratic twist $J_t^{(\mathfrak{d})}$
E_t	the elliptic curve $y^2 + 3xy + ty = x^3$ of (4.7)
$\chi_7,\ \bar{\rho}_{t,7}$	the mod-7 cyclotomic character; the representation of G_K on $J_t[7]$
$H,\ x_H$	the stable line $k(\delta\chi_7) \subset J_t[7]$; the point of $\mathcal{X}(\mathbb{Q})$ it defines
$\mathcal{X}$	the genus-8 curve of k-lines in $J_t[7]$, with $t\colon \mathcal{X} \to \mathbb{P}^1$ of degree 50
$G_0,\ G_1,\ G_\infty$	the local monodromy matrices of $J_t[7]$ at $t = 0, 1, \infty$ in $\mathrm{SL}_2(k)$ (Proposition 4.11)
α_0	a root of $x^2 + x - 1$ in k, the trace of G_0
$W,\ \mathcal{Z}$	the covers of $\mathcal{X}$ by nonzero vectors of the lines (genus 369) and by their classes modulo squares of scalars (genus 15)
$C,\ q,\ \tau$	the twist $\mathcal{Z}^{(5)}$, of genus 15; its covering map to $\mathcal{X}$; its involution
R	a point of $C(\mathbb{Q})$ with $t(q(R)) = -X^5/Y^3$ produced by a solution
$\mathcal{X}',\ C'$	the explicit genus-8 curve in $\mathbb{P}^7$ of Proposition 5.5 and its double cover $w^2 = r$, identified with $\mathcal{X}$ and C by Proposition 5.8 and Lemma 5.11
$x_0, \dots, x_7,\ u$	coordinates of the canonical model of $\mathcal{X}$ in $\mathbb{P}^7$; the function x_1/x_0
$q_1, \dots, q_{15}$	the fifteen quadrics defining $\mathcal{X}'$ in $\mathbb{P}^7$ (Proposition 5.5)
$A_i,\ B_i$	the thirteen pairs of quintic forms with $t = A_i/B_i$ on $\mathcal{X}'$ (Proposition 5.5)
$\varphi,\ G(\varphi, t)$	the function $(x_2 - 204x_0)/(x_1 - 25x_0)$ of degree 14 on $\mathcal{X}'$; the plane model of $\mathcal{X}'$ in the coordinates φ and t, of degree 14 in t and 50 in φ (Proposition 5.5)
$\tau_0,\ \tau_1$	the monodromy permutations along the loops γ_0, γ_1 around 0 and 1 (proof of Proposition 5.8, Table 17)
$D_{x_0},\ P_0,\ E_c$	the hyperplane divisor $\{x_0 = 0\}$; the rational cusp of $\mathcal{X}$ over $t = 1$; the degree-8 divisor in $\mathrm{div}(r)$
$r_0,\ r,\ w$	the quadratic form with $r = r_0/x_0^2$; the function with $\mathrm{div}(r) = 12P_0 + 2E_c - 2D_{x_0}$; the coordinate $w^2 = r$ of C (Proposition 5.10)

TABLE 4. (continued)

Symbol	Meaning
$Q_0,\ Q_1$	the two rational cusps of C over P_0, with $w/(t-1)^6 = 1$ at Q_0 (Proposition 5.10)
e_k	the k-bilinear alternating pairing on $J_t[7]$ whose trace to $\mathbb{F}_7$ is the Weil pairing (Section 6.1)
ε	the quadratic character $k^\times \to \{\pm 1\}$
P	the Prym variety $\mathrm{im}(1-\tau) \subset J = \mathrm{Jac}(C)$ of $C \to \mathcal{X}$, of dimension 7
$\mathcal{D},\ e_B$	the action on P of the correspondence of Proposition 6.2, defined by the sign of the Weil pairing, with $\mathcal{D}^2 = 49$; $(\mathcal{D}+7)/2$
$B,\ B'$	the abelian subvarieties of P on which $\mathcal{D}$ acts as $+7$ and -7: a surface with a polarization of type $(1,7)$ and a fivefold
$f,\ \iota,\ F_B$	the maps $C \to B$, $C \to B^\vee$ of (6.1); the endomorphism of J inducing f
$\lambda_B,\ \lambda'_B$	the $(1,7)$ polarization of B; $7\lambda_B^{-1}$
L	the quintic field $\mathbb{Q}(\xi)$ with $\xi^5 - 70\xi^2 + 210\xi - 168 = 0$; $B[2] \simeq \ker(\mathrm{Res}_{L/\mathbb{Q}}\,\mu_2 \to \mu_2)$
K_C	the canonical divisor $q^*D_{x_0}$ of C, of degree 28 (Section 6.3)
$\Theta,\ \delta_0,\ \kappa$	the descent function of Proposition 6.7; the constant $\delta_0 \in L^\times$ there; the Kummer map $C(\mathbb{Q}) \to L^\times/L^{\times 2}$
$\mathcal{S}$	the set of primes $\{2,3,5,7\}$ in the two-descent of Section 6.4
$\mathcal{X}_{\mathbb{Z}_{13}},\ C_{\mathbb{Z}_{13}}$	the smooth proper models of $\mathcal{X}$ and C over $\mathbb{Z}_{13}$ (Proposition 7.1), with special fibres $\overline{\mathcal{X}}$ and $\overline{C}$
$\Omega^-,\ \Lambda^-,\ \Lambda_B$	odd differentials on C; the lattice of 13-integral ones; its rank-two summand coming from B (Section 7.3)
ω_0	the regular differential on $\mathcal{X}$ corresponding to x_0, with $(\omega_0/du)(P_0) = 1$
$\mathcal{Q}_1, \dots, \mathcal{Q}_7$	the rational quadratic forms of Lemma 7.5, with reductions $\overline{\mathcal{Q}}_j$ in Table 15
$\nu_1, \dots, \nu_7$	the basis $\nu_j = \mathcal{Q}_j\,\omega_0/(x_0^2 w)$ of Λ^-
$\overline{\Delta}$	the cubic form (D.4), with $\overline{\omega}_0 = x_0^3\,du/\overline{\Delta}$ on $\overline{\mathcal{X}}$
$\mathcal{C},\ \mathsf{C}$	the Cartier operator on regular differentials over $\mathbb{F}_{13}$; its matrix on $\overline{\nu}_1, \dots, \overline{\nu}_7$ (Proposition 7.6)
K	the 7×2 matrix whose columns span the reduction of Λ_B
$L_B,\ L_{B'},\ N$	the L-polynomials of B, B' at 13; $N = \#P(\mathbb{F}_{13})$
$\omega_1,\ \omega_2,\ I_1,\ I_2$	lifts to Λ_B of the columns of K; their cusp periods $\int_{Q_0}^{Q_1} \omega_j$
η	the annihilating differential $(I_2\omega_1 - I_1\omega_2)/13$
μ	the multiple $2N$ of Section 8.1; $\mu \equiv 1 \pmod{13}$
$D_0,\ V_n,\ V'_1,\ E_0$	$K_C + 3Q_0$; the section spaces $L(nD_0)$, $L(D_0+Q_0)$; the reference divisor of Section 8.3

APPENDIX B. THE S-UNITS OF THE EXCEPTIONAL FIELD

Table 5 lists the sixteen S-units $g_1, \dots, g_{16}$ of $\mathcal{E} = F(\sqrt{-35})$ used in Section 3.5. In the notation of Section 3.1, with $h(\varpi) = 0$ and $F = \mathbb{Q}(\varpi)$, each of them is

$$g_j = \frac{A_j(\varpi) + B_j(\varpi)\sqrt{-35}}{506030}, \qquad A_j = \sum_{i=0}^{6} a_{j,i}x^i, \quad B_j = \sum_{i=0}^{6} b_{j,i}x^i \in \mathbb{Z}[x],$$

where $506030 = 2\cdot 5\cdot 7\cdot 7229$, and the table gives the coefficient vectors $a = (a_{j,0}, \dots, a_{j,6})$ and $b = (b_{j,0}, \dots, b_{j,6})$, constant term first. The second column is the ideal $g_j\mathcal{O}_\mathcal{E}$ in terms of the

primes $\mathfrak{p}_i$ of (3.10); $g_{11}, \dots, g_{16}$ are units. Each g_j is an algebraic integer: its characteristic polynomial over $\mathbb{Q}$ has integer coefficients, and its norm is 9 for $j \le 4$, 15 for $5 \le j \le 7$, 21 for $8 \le j \le 10$ and 1 for $j \ge 11$. The denominator reflects the index of $\mathbb{Z}[\varpi, \sqrt{-35}]$ in $\mathcal{O}_{\mathcal{E}}$, which is divisible by 7229, the index of $\mathbb{Z}[\varpi]$ in $\mathcal{O}_F$. Applying σ changes the sign of b; thus $g_{13} = \sigma(g_{12})$ and $g_{15} = \sigma(g_{14})$.

TABLE 5. The S-units $g_j = (A_j(\varpi) + B_j(\varpi)\sqrt{-35})/506030$.

	$g_j\mathcal{O}_{\mathcal{E}}$		coefficients of A_j (row a) and B_j (row b), constant term first
g_1	$\mathfrak{p}_1^2$	a	(9194535, 70875, −543515, 10388350, 2005360, −679280, 238525)
		b	(152425, 414785, −403795, 513138, 173444, −56478, 15281)
g_2	$\mathfrak{p}_1\mathfrak{p}_2$	a	(1080415, −1111425, 1313130, 777245, −86275, 17990, 7945)
		b	(−725865, 19005, 152360, −913757, −187469, 64388, −21717)
g_3	$\mathfrak{p}_3$	a	(5628140, 3178875, −1765610, 7623490, 1848035, −601825, 193480)
		b	(1212260, −304885, 225990, 1355872, 207199, −73209, 28918)
g_4	$\mathfrak{p}_4$	a	(32947915, −1110515, −1795500, 35921655, 6742890, −2317595, 821905)
		b	(−1219435, −1700125, 1433320, −2640321, −825330, 262643, −75717)
g_5	$\mathfrak{p}_1\mathfrak{p}_5$	a	(6692105, 11651780, 7852285, 4238255, 2147600, −509915, 167125)
		b	(1085175, 713650, −1268215, −633345, 433154, −111527, 12333)
g_6	$\mathfrak{p}_1\mathfrak{p}_6$	a	(541100, 181825, −326690, 996135, 233625, −78995, 24675)
		b	(−154070, −12985, 52330, −170341, −40883, 13267, −4253)
g_7	$\mathfrak{p}_1\mathfrak{p}_7$	a	(5257945, 6746845, −4848025, −10552500, −1329405, 487830, −217735)
		b	(−1080135, −1713215, −1647825, −979712, −103017, 20742, −18743)
g_8	$\mathfrak{p}_1\mathfrak{p}_8$	a	(1064245, −424095, −295225, 2108750, 421120, −144060, 49595)
		b	(35, −100065, −46355, −127418, −27276, 8456, −3157)
g_9	$\mathfrak{p}_1\mathfrak{p}_9$	a	(1456945, −19810, −524790, 1977395, 496405, −148365, 50155)
		b	(119525, 101290, −95660, 176223, 55957, −17073, 4513)
g_{10}	$\mathfrak{p}_1\mathfrak{p}_{10}$	a	(1025045, 828135, 7315, 1357405, 1367485, −210, 43225)
		b	(121765, 22505, −62345, 146867, 103085, −32522, 19335)
g_{11}	(1)	a	(10112795, 4856460, −1735265, 3756095, 1007790, −316995, 96775)
		b	(280245, 1090110, 912145, 1055507, 177112, −50225, 23401)
g_{12}	(1)	a	(481530, 1984465, −696465, −3410890, −388955, 153160, −67235)
		b	(−247310, 388395, 540615, −50820, −159191, 48192, −8561)
g_{13}	(1)	a	(481530, 1984465, −696465, −3410890, −388955, 153160, −67235)
		b	(247310, −388395, −540615, 50820, 159191, −48192, 8561)
g_{14}	(1)	a	(5457795, 31479035, 49625275, 26935790, 1745765, −313320, 478905)
		b	(4240705, 5869535, −1385115, −4128516, −444401, 190570, −83033)
g_{15}	(1)	a	(5457795, 31479035, 49625275, 26935790, 1745765, −313320, 478905)
		b	(−4240705, −5869535, 1385115, 4128516, 444401, −190570, 83033)
g_{16}	(1)	a	(624820, 178535, −25830, 618240, 397425, −42840, −37625)
		b	(−90510, −66255, 17210, −110536, −84365, −6720, 2461)

These elements represent the classes used in Lemma 3.8; any element of $g_j\mathcal{E}^{\times 5}$ would serve equally well, since only the classes enter. They are also included in the supplementary data [31].

APPENDIX C. DATA FOR SECTION 6

This appendix gives the data used in Section 6: the monodromy permutations and the Prym lattice for Proposition 6.2, and the local data for the two-descent of Proposition 6.13. The

equations of $\mathcal{X}$ and C over $\mathbb{Q}$, the functions a, b, c and the constants δ_0, ℓ of Proposition 6.7, and the local points to 200 digits are in the supplementary data [31].

C.1. **The monodromy of $C \to \mathbb{P}^1$ and the Prym lattice.** Identify $k = \mathcal{O}_K/(7)$ with $\mathbb{F}_7(s)$, where $s^2 = 3$, and take $\alpha_0 = 3 + s$ in Proposition 4.11, so that

$$G_0 = \begin{pmatrix} 0 & 3+s \\ 3+6s & 3+s \end{pmatrix}, \qquad G_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$
$$G_\infty = G_0^{-1} G_1^{-1} = \begin{pmatrix} 3+s & 1+5s \\ 4+s & 3+6s \end{pmatrix}.$$

For $x = a + bs \in k$ $(0 \le a, b \le 6)$ let $\mathrm{ind}(x) = 7a + b$, and let $\mathrm{ind}(\infty) = 49$; the line through $(x, 1)$, respectively $(1, 0)$, has index $\mathrm{ind}(x)$, respectively $\mathrm{ind}(\infty)$. The class of λv, where $v = (x, 1)$ or $(1, 0)$ and $\lambda \in k^\times$, has label $2\,\mathrm{ind}(v)$ if λ is a square and $2\,\mathrm{ind}(v) + 1$ if not, where $\mathrm{ind}(v)$ is the index of the line through v; so the two classes on that line are those of v and $(1 + s)v$, as $1 + s$ is a nonsquare. Thus τ exchanges $2m$ and $2m + 1$. The permutations σ_0, σ_1 of the labels induced by G_0, G_1 are in Table 6; $\sigma_\infty = \sigma_0^{-1}\sigma_1^{-1}$ has cycle type $1^4\,3^{32}$. In these coordinates the relation of Proposition 6.2 is $\varepsilon(\det(v, w)) = +1$, where ε is the quadratic character of $k^\times$ (Lemma 6.1).

σ_0	(0 15 69 82 99)(1 14 68 83 98)(2 32 36 5 89)(3 33 37 4 88) (6 62 13 22 43)(7 63 12 23 42)(8 58 34 16 11)(9 59 35 17 10) (18 96 31 56 94)(19 97 30 57 95)(20 76 41 60 71)(21 77 40 61 70) (24 74 73 66 48)(25 75 72 67 49)(26 53 84 64 86)(27 52 85 65 87) (28 38 44 54 91)(29 39 45 55 90)(46 50 80 93 79)(47 51 81 92 78)
σ_1	(0 14 28 42 56 70 84)(1 15 29 43 57 71 85)(2 16 30 44 58 72 86) (3 17 31 45 59 73 87)(4 18 32 46 60 74 88)(5 19 33 47 61 75 89) (6 20 34 48 62 76 90)(7 21 35 49 63 77 91)(8 22 36 50 64 78 92) (9 23 37 51 65 79 93)(10 24 38 52 66 80 94)(11 25 39 53 67 81 95) (12 26 40 54 68 82 96)(13 27 41 55 69 83 97); fixed points 98, 99

TABLE 6. The monodromy permutations of $C \to \mathbb{P}^1$ at $t = 0$ and $t = 1$ on the 100 labels of Appendix C.1.

The Prym lattice $\ker(1 + \tau_*) \subset H_1(C, \mathbb{Z})$ has a basis $e_1, \dots, e_7, f_1, \dots, f_7$ in which the principal polarization λ_P has matrix $\left(\begin{smallmatrix} 0 & I_7 \\ -I_7 & 0 \end{smallmatrix}\right)$ and the correspondence $\mathcal{D}$ of Proposition 6.2 has the matrix of Table 7, whose j-th column is the image of the j-th basis vector. From this matrix alone one recovers Lemma 6.3(c): $\mathcal{D}^2 = 49$, $(\mathcal{D} + 7)/2$ is integral, $\ker(\mathcal{D} - 7)$ and $\ker(\mathcal{D} + 7)$ have ranks 4 and 10, the halved form restricted to them has Smith forms $(1, 1, 7, 7)$ and $(1^8, 7, 7)$, and their sum has index 49. The matrix also shows that $\mathcal{D}$ is self-adjoint for λ_P.

C.2. **Local data for the two-descent.** For each prime $\mathfrak{p}$ of L above 2, 3, 5 and 7 (all of residue degree one), Table 8 gives its ramification index, the residue or valuation of ξ at $\mathfrak{p}$, and the basis $\mathcal{B}_\mathfrak{p}$ of $L_\mathfrak{p}^\times / L_\mathfrak{p}^{\times 2}$ used for the coordinates $(y, \beta)_\mathfrak{p}$, $\beta \in \mathcal{B}_\mathfrak{p}$, in Proposition 6.13. Table 9 gives these coordinates for $g_0, \dots, g_5$ and for the Kummer images of the local points.

The local points are the points R of C with $x_0 = 1$, $x_1 = u$ and the coordinates of Table 10, which are correct modulo p^{42}; the value of w determines which of the two points of C over the same point of $\mathcal{X}$ is meant. Their x_2-coordinates are simple roots of the fibre

$$\left(\begin{array}{rrrrrrr|rrrrrrr}
-5 & 2 & -2 & 0 & -2 & 2 & 2 & 0 & -2 & -2 & 0 & -6 & -2 & 2 \\
8 & -3 & 4 & -8 & -2 & 4 & -10 & 2 & 0 & 14 & 10 & 6 & 14 & 2 \\
-6 & 4 & -17 & 6 & -2 & 4 & 4 & 2 & -14 & 0 & 10 & -22 & 0 & 16 \\
-18 & -4 & -10 & 7 & 4 & -4 & 10 & 0 & -10 & -10 & 0 & -16 & -10 & 10 \\
2 & 4 & 6 & -10 & -5 & 4 & -10 & 6 & -6 & 22 & 16 & 0 & 22 & 12 \\
-6 & 4 & -10 & 6 & -2 & -3 & 4 & 2 & -14 & 0 & 10 & -22 & 0 & 16 \\
-6 & -2 & -6 & 8 & 0 & -2 & 5 & -2 & -2 & -16 & -10 & -12 & -16 & 0 \\
\hline
0 & -4 & 12 & -8 & 6 & -4 & 10 & -5 & 8 & -6 & -18 & 2 & -6 & -6 \\
4 & 0 & 8 & -8 & 2 & 0 & 0 & 2 & -3 & 4 & -4 & 4 & 4 & -2 \\
-12 & -8 & 0 & 8 & 6 & -8 & 6 & -2 & 4 & -17 & -10 & 6 & -10 & -6 \\
8 & 8 & -8 & 0 & -8 & 8 & -6 & 0 & -8 & 6 & 7 & -10 & 6 & 8 \\
-6 & -2 & -6 & 8 & 0 & -2 & -2 & -2 & -2 & -2 & 4 & -5 & -2 & 0 \\
4 & 0 & 8 & -8 & 2 & 0 & 0 & 2 & 4 & 4 & -4 & 4 & -3 & -2 \\
-10 & 0 & -6 & 6 & 2 & 0 & 0 & 2 & -10 & 4 & 10 & -10 & 4 & 5
\end{array}\right)$$

TABLE 7. The matrix of $\mathcal{D}$ on the Prym lattice in a symplectic basis $e_1, \ldots, e_7, f_1, \ldots, f_7$ for λ_P.

p	prime	e	description	$\mathcal{B}_{\mathfrak{p}}$
2	$\mathfrak{p}_2$	1	$v_{\mathfrak{p}}(\xi) = 2$	$-1,\ \xi-1,\ 2$
	$\mathfrak{p}_2'$	4	ξ a uniformizer	$-1,\ \xi,\ \xi-1,\ \xi^2-\xi-1,\ 2,\ \xi-2$
3	$\mathfrak{p}_3'$	2	$\xi \equiv 1,\ \xi-1$ a uniformizer	$-1,\ \xi-1$
	$\mathfrak{p}_3$	1	$\xi \equiv 1,\ v_{\mathfrak{p}}(\xi-1) = 2$	$-1,\ \xi+2$
	$\mathfrak{p}_3''$	2	ξ a uniformizer	$-1,\ \xi$
5	$\mathfrak{p}_5$	1	$\xi \equiv 3$	$\xi,\ \xi^2-\xi-1$
	$\mathfrak{p}_5'$	4	$\xi \equiv 3,\ \xi-3$ a uniformizer	$\xi,\ \xi+2$
7	$\mathfrak{p}_7$	5	ξ a uniformizer	$-1,\ \xi$

TABLE 8. The primes of L above $\mathcal{S}$ and the bases of the local square class groups.

	$p=2$: $\mathfrak{p}_2 \mid \mathfrak{p}_2'$	$p=3$: $\mathfrak{p}_3' \mid \mathfrak{p}_3 \mid \mathfrak{p}_3''$	$p=5$: $\mathfrak{p}_5 \mid \mathfrak{p}_5'$
g_0	100 | 110000	00 | 00 | 01	00 | 00
$g_1 = \kappa(Q_1)$	001 | 001011	01 | 00 | 00	00 | 01
g_2	101 | 111011	11 | 11 | 01	10 | 10
g_3	000 | 010000	10 | 11 | 01	00 | 00
g_4	010 | 001100	10 | 11 | 00	00 | 00
g_5	001 | 011010	10 | 01 | 11	10 | 11
$\kappa(R_2)$	000 | 010100		
$\kappa(R_{-2})$	000 | 000101		
$\kappa(R_{-3})$		00 | 00 | 01	

TABLE 9. Hilbert-symbol coordinates of the generators of $\mathcal{V}$ and of the images of the local points, in the bases of Table 8 (in that order within each prime; 1 means symbol -1). At $p = 7$ all g_i have coordinates $(0, 0)$.

polynomials m_u, with $v_p(m_u'(x_2)) = 2, 2, 60$ for R_2, R_{-2}, R_{-3}; the two roots of m_{-3} in $\mathbb{Z}_3$ are congruent modulo 3^5 but not modulo 3^6, so x_2 modulo 3^6 determines the point.

	$R_2 \in C(\mathbb{Q}_2)$, $u = 2$	$R_{-2} \in C(\mathbb{Q}_2)$, $u = -2$
x_2	1943367761412	2963101284868
x_3	4061910274824	864975790840
x_4	90281580304	319731186448
x_5	156551181600	4376343543008
x_6	4118212848704	3956940531776
x_7	1961067637376	3940505116032
w	4325351937600	1686432534080
		$R_{-3} \in C(\mathbb{Q}_3)$, $u = -3$
x_2		33466286008536187455
x_3		31632976806682109922
x_4		59894551954179815625
x_5		52820431253576767422
x_6		17782590429763798698
x_7		101297974124587121118
w		106617295422845025417

TABLE 10. The local points used in Proposition 6.13: coordinates modulo 2^{42} (upper part) and 3^{42} (lower part).

Appendix D. The model at 13

This appendix gives the reductions modulo 13 of the canonical model of $\mathcal{X}$, of the double cover C, of the map t, of the differential ω_0 and of the odd differentials, so that the statements of Section 7 about the special fibre can be checked from the paper. Appendix D.3 describes the computations. The rational model is in the supplementary data [31]. As in Section 7, a bar denotes reduction modulo 13.

Table 11 is in the coordinates of Proposition 5.5, and its rows $q_1, \dots, q_{15}$ and r_0 list the coefficients of $\overline{q}_1, \dots, \overline{q}_{15}$ and $\overline{r}_0$. In each of the rows $q_1, \dots, q_{15}$ the terms of lowest weight, where x_m has weight m, form a binomial $x_i x_j - x_k x_l$ with $i+j = k+l$, for instance $x_0x_2 - x_1^2$ in the row q_1 and $x_0x_3 - x_1x_2$ in the row q_2. The rational cusp P_0 of Section 5.3 reduces to $(1:0:0:0:0:0:0:0)$, where $u = x_1/x_0$ is a local parameter.

Proposition D.1. *The eleven points of $\overline{\mathcal{X}}(\mathbb{F}_{13})$ are, in the chart $x_0 = 1$ (there are none with $x_0 = 0$),*

$$\begin{gathered}(0,0,0,0,0,0,0),\ (0,3,7,3,6,11,0),\ (1,2,10,1,0,8,8),\\ (4,10,3,4,12,10,10),\ (5,4,3,11,0,4,3),\ (5,11,7,9,10,4,0),\\ (6,10,6,3,4,1,12),\ (9,0,2,5,2,0,11),\ (9,11,3,1,8,1,0),\\ (10,1,7,10,2,4,7),\ (12,5,7,0,0,8,8),\end{gathered} \tag{D.1}$$

listed as $(x_1, \dots, x_7)$. At each of them the Jacobian matrix of $(\overline{q}_1, \dots, \overline{q}_{15})$ has rank 6, so each is a smooth point of $\overline{\mathcal{X}}$. The form $\overline{r}_0$ takes the values $1, 2, 7, 7, 2, 12, 3, 8$ at the second, fourth, fifth, sixth, eighth, ninth, tenth and eleventh points, of which $1, 12, 3$ are squares in $\mathbb{F}_{13}$ and $2, 7, 8$ are not; it vanishes at the first, third and seventh points.

Proof. The fifteen quadrics of Table 11 are evaluated at all points of $\mathbb{F}_{13}^7$ (about $6 \cdot 10^7$ points) and, in the same way, on the hyperplane $x_0 = 0$. The rank of the Jacobian matrix and the value of $\overline{r}_0$ are then computed at the points found. □

This gives $\#\overline{\mathcal{X}}(\mathbb{F}_{13}) = 11$ in (7.1). At the eight points where $\overline{r}_0 \neq 0$ there are $1 + \varepsilon_{13}(\overline{r}_0)$ points of $\overline{C}$ above, where ε_{13} is the quadratic character of $\mathbb{F}_{13}^\times$: two above each of the second, ninth and tenth points, and none above the others. At each of the three zeros P of $\overline{r}_0$, $u - u(P)$ is a local parameter, since u is unramified at all eleven points (Lemma 7.5(c)). At the cusp $(0, \dots, 0)$, $\overline{r}_0 = u^{12}(1+4u+\cdots)$ along the branch, and the unit factor takes the value 1, a square, so the two points $\overline{Q_0}, \overline{Q_1}$ lie above it. At the third point, $\overline{r}_0 = 11(u-1)^2 + \cdots$, and 11 is not a square, so no point lies above it. At the seventh, $\overline{r}_0 = 10(u-6)^2 + \cdots$, and 10 is a square, so two points lie above it. Hence $\#\overline{C}(\mathbb{F}_{13}) = 10$. On $\overline{\mathcal{X}}$ the zero scheme of $\overline{r}_0$ has length 28 and is $12\overline{P_0} + 2\overline{E_c}$, where $\overline{E_c}$ consists of the third and seventh points, a point of degree 2 over $u = 4$ and a point of degree 4. So $\operatorname{div}(\overline{r}_0)$ has even multiplicities. Table 12 collects these data and the values of $\bar{t}$ from Lemma 7.2.

D.1. **The cusp-period data.** This subsection gives the inputs of the last step of the proof of Proposition 8.2, in which four traces are summed for each of the fifteen integral differentials (sixty traces in all). The reference divisor E_0 of Section 8.3 reduces to four closed points $P_1, \dots, P_4$ of $\overline{C}$, of residue degrees $1, 3, 3, 8$. The points of E_0 and E above P_i are defined over the unramified extension of $\mathbb{Q}_{13}$ of degree $\deg P_i$, whose ring of integers

	x_0^2	x_0x_1	x_0x_2	x_0x_3	x_0x_4	x_0x_5	x_0x_6	x_0x_7	x_1^2	x_1x_2	x_1x_3	x_1x_4	x_1x_5	x_1x_6	x_1x_7	x_2^2	x_2x_3	x_2x_4
q_1	0	0	1	0	0	0	0	0	12	0	0	0	0	0	0	0	0	0
q_2	0	0	0	1	0	0	0	0	0	12	0	0	0	0	0	0	0	0
q_3	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	12	0	0
q_4	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	12	0
q_5	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
q_6	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
q_7	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	12	0	0
q_8	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	12	0
q_9	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
q_{10}	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
q_{11}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
q_{12}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
q_{13}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
q_{14}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
q_{15}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
r_0	0	0	6	7	8	5	5	7	7	6	2	3	12	1	7	3	5	7

	x_2x_5	x_2x_6	x_2x_7	x_3^2	x_3x_4	x_3x_5	x_3x_6	x_3x_7	x_4^2	x_4x_5	x_4x_6	x_4x_7	x_5^2	x_5x_6	x_5x_7	x_6^2	x_6x_7	x_7^2
q_1	0	0	9	0	0	0	1	3	7	8	0	8	2	0	0	11	8	10
q_2	0	0	8	0	0	0	12	12	2	0	12	2	1	7	6	4	12	9
q_3	0	0	5	0	0	0	10	4	5	4	4	3	5	1	7	7	6	10
q_4	0	0	2	0	0	0	12	0	4	9	8	10	3	9	9	5	1	9
q_5	0	0	0	12	0	0	2	5	10	12	12	3	1	6	11	6	11	9
q_6	0	0	12	0	12	0	9	3	11	9	2	6	5	7	3	9	11	9
q_7	0	0	8	0	0	0	5	4	0	2	0	2	6	4	1	11	0	1
q_8	0	0	1	0	0	0	10	8	0	7	6	6	1	7	9	7	6	12
q_9	0	0	4	12	0	0	8	2	0	5	1	2	12	12	1	9	6	6
q_{10}	0	0	8	0	12	0	10	6	0	5	7	4	11	12	5	1	11	0
q_{11}	0	0	4	0	0	0	6	1	12	1	10	10	11	7	4	11	2	11
q_{12}	0	0	6	12	0	0	11	10	0	9	7	11	2	1	7	10	10	8
q_{13}	1	0	10	0	12	0	8	6	0	8	2	10	2	12	6	4	12	11
q_{14}	0	1	5	0	0	0	0	1	12	8	2	5	10	1	12	4	1	5
q_{15}	0	0	11	0	0	1	6	3	12	9	8	3	6	8	5	3	3	2
r_0	5	2	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0

TABLE 11. The canonical model of $\mathcal{X}$ and the double cover C modulo 13, in two halves (monomials 1–18 above, 19–36 below). Rows $q_1, \dots, q_{15}$: coefficients in $\mathbb{F}_{13}$ of the fifteen quadrics. Row r_0: the quadratic form with $r = r_0/x_0^2$, so that C is $w^2 = r_0(x)/x_0^2$ over $\mathcal{X}$.

modulo 169 is $R_i = (\mathbb{Z}/169\mathbb{Z})[x]/(m_i(x))$, with

$$\begin{aligned} &m_1 = x + 7, \qquad m_2 = x^3 + 11x^2 + 12x + 4, \\ &m_3 = x^3 + 4x^2 + 11, \\ &m_4 = x^8 + 7x^7 + 6x^6 + 5x^5 + 4x^4 + 3x^3 + 7x^2 + 7x + 10, \end{aligned} \tag{D.2}$$

and the coefficients read as integers. The elements of R_i are written in the basis $1, x, \dots, x^{\deg m_i - 1}$. With S a local parameter at P_i as in Section 8.3, fixed in the supplementary data [31], let s and s_0, both in $13R_i$, be the coordinates of the points above P_i of the divisor E attached to $\mu[Q_1 - Q_0]$ and of E_0, and put $\delta_i = s - s_0$. For an integral differential ω, let $a_0(\omega, P_i) \in R_i$ be the constant term of ω/dS at P_i. By Section 8.3 the logarithm of

no.	point $(x_1, \dots, x_7)$	$\overline{r}_0$, or leading term	points of $\overline{C}$ above	$(\overline{A}, \overline{B})$	$\bar{t}$
1	$(0,0,0,0,0,0,0)$	u^{12}	2	$(7,7)$	1
2	$(0,3,7,3,6,11,0)$	1	2	$(6,0)$	∞
3	$(1,2,10,1,0,8,8)$	$11(u-1)^2$	0	$(3,8)$	2
4	$(4,10,3,4,12,10,10)$	2	0	$(5,2)$	9
5	$(5,4,3,11,0,4,3)$	7	0	$(3,5)$	11
6	$(5,11,7,9,10,4,0)$	7	0	$(1,7)$	2
7	$(6,10,6,3,4,1,12)$	$10(u-6)^2$	2	$(4,0)$	∞
8	$(9,0,2,5,2,0,11)$	2	0	$(3,5)$	11
9	$(9,11,3,1,8,1,0)$	12	2	$(9,0)$	∞
10	$(10,1,7,10,2,4,7)$	3	2	$(6,0)$	∞
11	$(12,5,7,0,0,8,8)$	8	0	$(7,8)$	9

TABLE 12. The eleven points of $\overline{\mathcal{X}}(\mathbb{F}_{13})$, in the order of (D.1): the value of $\overline{r}_0$, or its leading term in the local parameter $u - u(P)$ where it vanishes; the number of points of $\overline{C}(\mathbb{F}_{13})$ above; the values of the quintic forms $\overline{A}, \overline{B}$ of Table 14; and $\bar{t} = \overline{A}/\overline{B}$.

$\mu[Q_1 - Q_0]$ against ω is

$$-\sum_{i=1}^{4} \operatorname{Tr}_{R_i/(\mathbb{Z}/169\mathbb{Z})} \left(a_0(\omega, P_i)\, \delta_i\right) \pmod{169}. \tag{D.3}$$

In Table 13, $\omega_1^+, \dots, \omega_8^+$ is a basis of the even integral differentials (those pulled back from $\mathcal{X}$), fixed in the supplementary data [31]. The sums for these eight differentials vanish, and those for $\nu_1, \dots, \nu_7$ are $(130, 130, 13, 26, 130, 117, 143) \equiv -(39, 39, 156, 143, 39, 52, 26)$ (mod 169). Every δ_i is divisible by 13, so every trace, and hence every sum, is divisible by 13, as Lemma 7.8 predicts.

As $\mu \equiv 1 \pmod{13}$, multiplication by μ is the identity on $13\mathbb{Z}/169\mathbb{Z}$ (Section 8.1), so by (D.3) the negatives of these sums are the periods (8.3).

D.2. **The parameter t and the odd differentials modulo 13.** *The map t.* The thirteen rational pairs (A_i, B_i) of Proposition 5.5 were written in the standard monomials of $H_5 = H^0(\mathcal{X}_{\mathbb{Z}_{13}}, \mathcal{O}(5))$ by reduction modulo a Gröbner basis of $(q_1, \dots, q_{15})$ over $\mathbb{Z}/13^{30}\mathbb{Z}$. Since the reduced Gröbner basis over $\mathbb{Q}$ is 13-integral (Appendix E.4) and has the leading monomials of the one over $\mathbb{F}_{13}$ in Proposition 7.1, these are the reductions of the normal forms over $\mathbb{Q}$. Their $\mathbb{Z}_{13}$-span was saturated in $H_5^{\oplus 2}$ (Lemma 7.2) by repeatedly replacing a combination whose reduction vanishes by its quotient by 13 until the reductions were linearly independent (thirteen replacements in all, after which the pairs are still known modulo 13^{27}). Table 14 gives one element of the reduction of the saturated lattice with no common zero among the eleven points of $\overline{\mathcal{X}}(\mathbb{F}_{13})$. Its values there are in Table 12.

	P_1	P_2			P_3			P_4								$\mathrm{Tr}(a_0\delta_i)$				Σ
δ_i	13	0	78	156	52	39	156	104	39	91	39	143	0	130	104					
ω_1^+	109	163	87	53	85	146	43	24	34	4	20	42	122	22	21	65	91	65	117	0
ω_2^+	82	126	34	11	34	85	143	128	46	56	110	105	106	165	44	52	91	104	91	0
ω_3^+	102	73	120	77	159	115	87	103	143	41	41	20	1	163	142	143	130	39	26	0
ω_4^+	30	95	65	98	40	71	32	6	13	56	129	138	3	90	15	52	39	26	52	0
ω_5^+	15	149	163	101	81	58	146	149	85	10	128	64	52	104	99	26	130	130	52	0
ω_6^+	59	38	129	27	137	8	135	51	104	32	115	135	157	38	67	91	117	52	78	0
ω_7^+	135	19	4	43	39	42	116	32	167	68	118	155	128	98	79	65	52	78	143	0
ω_8^+	164	97	146	155	143	12	123	30	159	42	125	136	150	53	65	104	143	156	104	0
ν_1	59	39	68	160	135	80	9	160	24	156	90	149	110	121	54	91	156	78	143	130
ν_2	13	100	99	100	103	106	142	86	166	117	30	51	152	148	38	0	0	130	0	130
ν_3	76	68	48	39	23	95	139	149	158	126	47	52	116	59	77	143	156	26	26	13
ν_4	32	63	160	26	87	89	80	105	24	0	48	164	8	82	101	78	91	117	78	26
ν_5	106	134	35	3	165	79	82	28	166	160	54	142	66	72	111	26	117	13	143	130
ν_6	128	43	148	27	44	52	138	41	164	115	110	87	83	31	67	143	117	52	143	117
ν_7	89	21	62	110	131	161	59	47	96	111	64	101	134	58	121	143	78	91	0	143

TABLE 13. The cusp-period data at the reference divisor E_0, modulo 169. For each of the four points P_i of $\overline{E_0}$ the columns give the coordinates in R_i of the displacement δ_i (first row) and of the constant terms $a_0(\omega, P_i)$ of ω/dS for the fifteen integral differentials (rows); the last five columns give the traces $\mathrm{Tr}_{R_i/(\mathbb{Z}/169\mathbb{Z})}(a_0\delta_i)$ and their sum.

monomial	$\overline{A}$	$\overline{B}$	monomial	$\overline{A}$	$\overline{B}$	monomial	$\overline{A}$	$\overline{B}$
x_7^5	2	2	$x_6^3x_7^2$	12	3	$x_0^3x_6x_7$	4	0
$x_6x_7^4$	2	0	$x_5x_6^2x_7^2$	0	1	$x_0^3x_5x_7$	1	3
$x_5x_7^4$	12	2	$x_4x_6^2x_7^2$	0	5	$x_0^3x_4x_7$	9	4
$x_4x_7^4$	3	8	$x_3x_6^2x_7^2$	5	2	$x_0^3x_3x_7$	0	4
$x_3x_7^4$	1	0	$x_2x_6^2x_7^2$	2	6	$x_0^3x_2x_7$	12	8
$x_2x_7^4$	0	10	$x_1x_6^2x_7^2$	2	5	$x_0^3x_1x_7$	12	0
$x_1x_7^4$	5	3	$x_0x_6^2x_7^2$	1	9	$x_0^4x_7$	2	12
$x_0x_7^4$	12	0	$x_0^2x_6x_7^2$	0	5	x_6^5	7	9
$x_6^2x_7^3$	0	3	$x_0^2x_5x_7^2$	7	2	$x_5x_6^4$	12	6
$x_5x_6x_7^3$	7	7	$x_0^2x_4x_7^2$	7	12	$x_4x_6^4$	0	3
$x_4x_6x_7^3$	0	4	$x_0^2x_3x_7^2$	12	7	$x_3x_6^4$	7	0
$x_3x_6x_7^3$	3	8	$x_0^2x_2x_7^2$	0	7	$x_2x_6^4$	9	1
$x_2x_6x_7^3$	2	0	$x_0^2x_1x_7^2$	7	4	$x_1x_6^4$	0	0
$x_1x_6x_7^3$	0	4	$x_0^3x_7^2$	11	3	$x_0x_6^4$	12	7
$x_0x_6x_7^3$	7	0	$x_6^4x_7$	0	6	$x_0^4x_6$	9	3
$x_0x_5x_7^3$	2	5	$x_5x_6^3x_7$	0	0	$x_0^4x_5$	0	6
$x_0x_4x_7^3$	5	10	$x_4x_6^3x_7$	3	10	$x_0^4x_4$	7	7
$x_0x_3x_7^3$	9	2	$x_3x_6^3x_7$	11	10	$x_0^4x_3$	0	0
$x_0x_2x_7^3$	4	6	$x_2x_6^3x_7$	3	11	$x_0^4x_2$	0	0
$x_0x_1x_7^3$	2	0	$x_1x_6^3x_7$	0	9	$x_0^4x_1$	7	0
$x_0^2x_7^3$	1	11	$x_0x_6^3x_7$	0	0	x_0^5	7	7

TABLE 14. Two quintic forms $\overline{A}, \overline{B}$ over $\mathbb{F}_{13}$ with $\bar{t} = \overline{A}/\overline{B}$ on $\overline{\mathcal{X}}$ wherever they do not both vanish (Lemma 7.2). They have no common zero in $\overline{\mathcal{X}}(\mathbb{F}_{13})$. The forms are written in the basis of $H^0(\overline{\mathcal{X}}, \mathcal{O}(5))$ formed by the 63 monomials of degree 5 that are standard for the Gröbner basis of Proposition 7.1.

The differential ω_0. The cubic forms modulo I vanishing on the ramification scheme of u form a 1-dimensional space, spanned by

$$\begin{aligned}\overline{\Delta} = {} & x_0^3 + 12x_0^2x_7 + x_0\,(11x_1x_7 + 7x_2x_7 + 9x_3x_7 + 10x_4x_7 \\ & \qquad + 11x_6^2 + 6x_6x_7 + 12x_7^2) \\ & + x_6^2\,(x_1 + 11x_2 + 9x_3 + 11x_4 + 7x_5 + 4x_6) \\ & + x_6x_7\,(12x_1 + 4x_2 + 9x_3 + 5x_4 + 11x_5 + 4x_6) \\ & + x_7^2\,(4x_1 + 4x_2 + 4x_3 + 12x_4 + 8x_5 + 7x_6 + 12x_7),\end{aligned} \tag{D.4}$$

normalized by $\overline{\Delta}(\overline{P_0}) = 1$. Then $\overline{\omega}_0 = x_0^3\,du/\overline{\Delta}$ (Lemma 7.5(c)), and at $\overline{P_0}$, in the parameter u, $\overline{\Delta} = 1 + 12u^7 + \cdots$.

The odd differentials. The seven rational quadratic forms $\mathcal{Q}_j$ of Lemma 7.5 were written in the standard monomials of $H^0(\mathcal{X}_{\mathbb{Z}_{13}}, \mathcal{O}(2))$ in the same way. Their reductions are the forms of Table 15, from which, with Table 11 and (D.4), the data of Proposition 7.6 are computed as in its proof.

	x_0x_6	x_1x_6	x_2x_6	x_3x_6	x_4x_6	x_5x_6	x_6^2	x_0x_7	x_1x_7	x_2x_7	x_3x_7	x_4x_7	x_5x_7	x_6x_7	x_7^2
$\overline{\mathcal{Q}}_1$	3	8	6	12	0	1	11	12	11	6	12	3	3	12	6
$\overline{\mathcal{Q}}_2$	4	9	2	12	4	2	11	7	7	11	0	9	9	3	5
$\overline{\mathcal{Q}}_3$	1	8	8	5	6	9	3	4	0	8	6	3	10	2	7
$\overline{\mathcal{Q}}_4$	8	7	6	3	9	9	3	11	0	11	7	10	0	0	12
$\overline{\mathcal{Q}}_5$	2	10	3	12	0	11	1	10	6	7	5	0	11	10	4
$\overline{\mathcal{Q}}_6$	9	2	2	9	7	8	8	7	8	3	1	5	10	8	11
$\overline{\mathcal{Q}}_7$	6	11	3	6	6	9	4	4	6	5	1	4	5	4	1

TABLE 15. The quadratic forms $\overline{\mathcal{Q}}_1, \ldots, \overline{\mathcal{Q}}_7$ over $\mathbb{F}_{13}$ of Lemma 7.5: their coefficients on the monomials x_ix_6 and x_ix_7, all other coefficients being zero.

D.3. **Computations on the special fibre.** The computations that concern $\overline{\mathcal{X}}$ and $\overline{C}$ in Proposition 7.1, Lemma 7.2, Lemma 7.5 and Proposition 7.6 use only Table 11 (and, for t and the $\overline{\mathcal{Q}}_j$, the reductions of Appendix D.2). In step (iii) of the proof of Proposition 7.1, M_4 is needed: the ideal $I + M_1 + M_2 + M_3$ still has zeros.

The coordinate ring over the u-line. On the chart $x_0 = 1$, with $u = x_1$ and the order that compares the monomials in $x_2, \ldots, x_7$ first (reverse lexicographically) and then the powers of u, no leading monomial of the Gröbner basis of the dehomogenized ideal involves u. So the fourteen standard monomials $1, x_2, \ldots, x_7, x_2x_7, \ldots, x_6x_7, x_7^2, x_7^3$ form a basis over $\mathbb{F}_{13}[u]$ of the coordinate ring A of the chart, on which $x_2, \ldots, x_7$ act by commuting 14×14 matrices over $\mathbb{F}_{13}[u]$ satisfying the fifteen quadrics. The same holds on the chart $x_1 = 1$ over $\mathbb{F}_{13}[v]$, $v = x_0/x_1$, which is used only for the fibre over $u = \infty$.

Good fibres. Let $y = x_4 + 2x_5 + 3x_6 + 5x_7$ and let $\chi(u, T)$ be the characteristic polynomial of multiplication by y on A. Its discriminant in T has degree 182 in u, and $1, y, \ldots, y^{13}$ is a basis of $A \otimes_{\mathbb{F}_{13}[u]} \mathbb{F}_{13}(u)$, in which $\overline{r}_0 = \sum_{i=0}^{13} \rho_i(u)\, y^i$. Let $\beta(u)$ be the product of this discriminant, the norm of $\overline{r}_0$ from A to $\mathbb{F}_{13}[u]$ and the common denominator of the ρ_i. The norm of $\overline{r}_0$ is $10\,u^{12}(u-6)^2(u-4)^4(u-1)^2(u^4+3u^2+2u+8)^2$. For $a \in \mathbb{F}_{13^n}$ with $\beta(a) \neq 0$, the fibre over a is étale and y separates its points, so its $\mathbb{F}_{13^n}$-points correspond to the roots $y_0 \in \mathbb{F}_{13^n}$ of $\chi(a, T)$, and above such a point there are $1 + \varepsilon_{13^n}\big(\sum_i \rho_i(a) y_0^i\big)$ points of $\overline{C}$, with ε_{13^n} the quadratic character of $\mathbb{F}_{13^n}^\times$.

The other fibres. The irreducible factors of β have degrees $1, 1, 1, 1$ (namely u, $u-1$, $u-4$, $u-6$), $2, 2, 2, 3, 4, 4, 4, 5, 15, 24, 51$, so for $n \le 6$ only those of degree at most 5 matter. For each of them, and for the fibre over $u = \infty$, the closed points of $\overline{\mathcal{X}}$ in the fibre were determined by linear algebra in the fibre algebras, with their degrees e over $\mathbb{F}_{13}$ and the quadratic character $\varepsilon \in \{\pm 1\}$ of the value of $\overline{r}_0$ in the residue field or, where $\overline{r}_0$ vanishes, of a quadratic form s with $Q^2 - \overline{r}_0 s \in I$ for some quadratic form Q (for instance $\overline{\mathcal{Q}}_1$ of Table 15), since s/x_0^2 and $\overline{r}$ differ by a square. The fibre over $u = \infty$, $\overline{\mathcal{X}} \cap \{x_0 = 0\}$, is reduced and consists of two closed points, of degrees 2 and 12, at both of which $\overline{r}_0$ is nonzero with nonsquare value in the residue field. A closed point of degree e contributes e to $\#\overline{\mathcal{X}}(\mathbb{F}_{13^n})$ and $e\,(1 + \varepsilon^{n/e})$ to $\#\overline{C}(\mathbb{F}_{13^n})$ if $e \mid n$, and nothing otherwise, which gives the following contributions.

	good fibres		other fibres		total	
n	$\#\overline{\mathcal{X}}$	$\#\overline{C}$	$\#\overline{\mathcal{X}}$	$\#\overline{C}$	$\#\overline{\mathcal{X}}$	$\#\overline{C}$
1	6	4	5	6	11	10
2	202	224	21	22	223	246
3	2250	2272	11	12	2261	2284
4	28366	29284	49	58	28415	29342
5	371701	372164	25	26	371726	372190
6	4823476	4827020	57	46	4823533	4827066

For $n = 1$ this agrees with the exhaustive search of Proposition D.1. The totals for $n \le 5$ are (7.1), and the row $n = 6$ is used in the proof of Proposition 7.4.

Appendix E. Computations

Appendix E.1 lists the computational statements of the paper, and Appendix E.2 describes the computations that were repeated by separately written programs. Appendices E.3 and E.4 give the details of the computations behind Proposition 5.8 and Lemma 5.11, Appendix E.5 names the software, and Appendix E.6 says where the data are.

E.1. **List of computational statements.** Table 16 lists the statements whose proofs rest on machine computation, and what was computed for each; the programs in the supplementary data also recheck several smaller statements that can be verified by hand. All arithmetic is exact (integers, rationals, number fields, finite fields and rings $\mathbb{Z}/p^k\mathbb{Z}$), with one exception: the continuation of Appendix E.3 uses ball arithmetic, in which every quantity carries a rigorous error bound.

All computations were carried out on one computer with an Apple M5 processor. The longest computation used in the proofs, the certified continuation of Appendix E.3, takes about one hour of processor time, and each of the others a quarter of an hour or less. The running time of each program is recorded with the supplementary data [31].

E.2. **Independent second computations.** The following computations were repeated by separately written programs, which share with the first ones only the data printed in the paper or deposited with it.

The exceptional field (Section 3). Every printed matrix, e_{15}, the affine set $\mathcal{A}$, the two pattern lists and the incompatibility of Proposition 3.12 were recomputed from the primes (3.10), Table 2 and the S-units of Table 5 alone, by two programs: one in PARI/GP with a different defining polynomial of $\mathcal{E}$, and one in integer arithmetic only, which enumerates the

Statement	What is computed
Lemma 2.4	polynomial identities between the three models of F; irreducibility modulo 53
Lemmas 3.7 and 3.8; Theorem 3.9	the class-group certificate for $\mathcal{E}$; the S-units g_j, their valuations, and the matrices S_σ and Val; the affine set $\mathcal{A}$
Lemma 3.11; Proposition 3.12	the fifth-power residue patterns at 11 and 19, by enumeration of all residue classes and valuation strata; the final linear algebra over $\mathbb{F}_5$
Proposition 4.1	the change of variables to the Kumar–Mukamel form and its discriminant
Proposition 4.8	point counts of H_t over $\mathbb{F}_7$ and $\mathbb{F}_{49}$
Proposition 4.9	the class number of $\mathbb{Q}(\sqrt{5}, \zeta_7)$
Proposition 4.11	the local monodromy matrices in $\mathrm{SL}_2(\mathbb{F}_{49})$ and the group they generate
Propositions 5.5, 5.8 and 5.10	Gröbner bases of the canonical ideal over $\mathbb{Q}$ and $\mathbb{F}_{13}$; the normal forms of the products $A_iB_j - A_jB_i$; the expansion at P_0; the plane model $G(\varphi, t)$ and its factorizations; the certified monodromy of $\mathcal{X}' \to \mathbb{P}^1$ (Appendix E.3); the divisor of r
Lemma 5.11	Gröbner bases over $\mathbb{F}_{11}$, and the 11-integrality of the reduced Gröbner basis over $\mathbb{Q}$; normal forms modulo 11^{40}; the 11-adic saturation of the pairs (A_i, B_i); the points of $\mathcal{X}_{\mathbb{F}_{11}}(\mathbb{F}_{1331})$ with the values of $\bar{t}$ and $\bar{r}_0$; the Frobenius polynomials of H_{t_0} for $t_0 \in \mathbb{F}_{1331} \smallsetminus \{0, 1\}$
Proposition 6.2; Lemma 6.3	the integral homology of C from its triangulation; the Prym lattice and its eigenlattices, with their Smith forms
Propositions 6.5, 6.7 and 6.13; Lemma 6.8	the field L; the properties (F1)–(F4) of Θ; $\delta_0/g_1 \in L^{\times 2}$; local points and Kummer images at 2, 3 and 5; the Selmer group
Propositions 7.1 and 7.4; Lemma 7.2; Proposition D.1	smoothness of the reduction at 13; the map t over $\mathbb{Z}_{13}$; point counts over $\mathbb{F}_{13^n}$, $n \le 6$; the L-polynomials of B and B'; the enumeration of $\overline{\mathcal{X}}(\mathbb{F}_{13})$
Lemma 7.5; Propositions 7.6 and 7.7	the integral odd differentials; the Cartier matrix and its kernel
Proposition 8.2	the class $\mu[Q_1 - Q_0]$ by divisor arithmetic modulo 169, and its logarithm

TABLE 16. The computational statements of the paper.

valuation strata at 11 and 19 by listing the elements of the residue fields. The class-group certificate of Lemma 3.7 was obtained for both defining polynomials of $\mathcal{E}$.

The surface B (Section 6). The integral homology of C, the Prym lattice, its eigenlattices and their Smith forms were computed from two cell structures on $C(\mathbb{C})$, the triangulation of Lemma 6.3 and a dessin d'enfant of $t \circ q \colon C \to \mathbb{P}^1$. The Smith forms were also computed from the printed Table 7. The field L, the group $\mathcal{V}$, properties (F1)–(F3), the local points, their Kummer images and the Selmer group were recomputed from the model, with the local points in different local coordinates.

The good model at 13 (Section 7). The point counts (7.1) were computed twice, and the closed points of the other fibres (Appendix D.3) were determined both by linear algebra in the fibre algebras and by primary decomposition. The Cartier matrix (7.6) was recomputed by the program for the cusp periods.

The cusp periods (Section 8). A second program computed the values (8.3), sharing with the first only the deposited model of C. It uses the base divisor $2K_C$ instead of D_0 and stores sections by their u-adic expansions to length 145 at the two cusps, which determine the sections of $\mathcal{O}(10K_C)$, a line bundle of degree $280 < 2 \cdot 145$. It multiplies $[Q_1 - Q_0]$ by

its exact order $8392300 = \mu/15$ in $J(\mathbb{F}_{13})$, by twice this number and by μ, and reads off the resulting classes at four reference divisors supported on the cusps. For several independent random choices it gives the values (8.3), and the logarithms against the even differentials vanish. For one such choice, every intermediate state of the three double-and-add chains is deposited [31], together with a program that uses linear algebra modulo 169 to check each step and the values read off.

The same program gives the value of N in (7.4) without point counts over extensions of $\mathbb{F}_{13}$. The orders of the classes $(1-\tau)[c - \overline{Q_0}]$ with $c \in \overline{C}(\mathbb{F}_{13})$ have a least common multiple divisible by $N/5$, and the 5-primary parts of two of these classes, of orders 25 and 5, generate a group of order 125. Hence N divides $\#P(\mathbb{F}_{13})$. On the other hand, $\#P(\mathbb{F}_{13}) = \prod_{i=1}^{7}(14 - 2\operatorname{Re}\alpha_i)$, where $\alpha_1, \dots, \alpha_7$ are Frobenius eigenvalues on P, one from each pair of complex conjugates, and $\sum_i 2\operatorname{Re}\alpha_i = \#\overline{\mathcal{X}}(\mathbb{F}_{13}) - \#\overline{C}(\mathbb{F}_{13}) = 1$. By the inequality of arithmetic and geometric means, $\#P(\mathbb{F}_{13}) \le (97/7)^7 < 9.82 \cdot 10^7 < 2N$, so $\#P(\mathbb{F}_{13}) = N$.

E.3. **The certified continuation.** For the monodromy of $\mathcal{X}' \to \mathbb{P}^1$ in Proposition 5.8, the loops γ_0, γ_1 were replaced by the inscribed regular 32-gons with vertices rounded to points of $2^{-40}(\mathbb{Z} + i\mathbb{Z})$. The rounded polygons lie in the annuli $0.49 < |t| < 0.51$ and $0.49 < |t-1| < 0.51$, so they are homotopic in $U(\mathbb{C})$ to γ_0 and γ_1. Along each edge $[v_0, v_1]$, parametrized as $t = v_0 + \theta(v_1 - v_0)$ with $0 \le \theta \le 1$, the 50 roots of $G(\varphi, t)$ were followed in ball arithmetic (Arb [32], at 1000 bits). At a dyadic parameter θ_0 the roots are isolated in pairwise disjoint balls, each containing exactly one root of the exact polynomial. For each centre c_j one computes in ball arithmetic the coefficients g_{mn} of

$$G\bigl(c_j + w,\ t(\theta_0) + (v_1 - v_0)h\bigr) = \sum_{m,n \ge 0} g_{mn} w^m h^n$$

and chooses a radius $r_j \le 0.45 \min_{i \ne j} |c_i - c_j|$. The step is a dyadic number Δ, the same for all j, such that for every j

$$|g_{00}| + \sum_{m \ge 2} |g_{m0}| r_j^m + \sum_{n \ge 1} \Delta^n \sum_m |g_{mn}| r_j^m < |g_{10}|\, r_j.$$

By Rouché's theorem (comparison with $g_{10}w$ on $|w| = r_j$), for every $h \in [0, \Delta]$ the disc $|w| < r_j$ contains exactly one root, and the discs are pairwise disjoint. So each root moves continuously inside its own disc over the step, and at $\theta_0 + \Delta$ it is identified with the unique newly isolated ball in that disc. Comparing the final balls of each loop with the initial ones at $t = 1/2$ gives τ_0, τ_1. Table 17 prints them and the labelling β of Proposition 5.8. In the coordinates of Appendix C.1, where $k = \mathbb{F}_7(s)$ with $s^2 = 3$ and $\alpha_0 = 3 + s$, one has $\beta(\tau_i(j)) = G_i \cdot \beta(j)$ for $i = 0, 1$ and all j, where the matrices G_0, G_1 of Proposition 4.11 act on $\mathbb{P}^1(k)$ by Möbius transformations.

E.4. **The comparison at 11.** For Lemma 5.11, the normal forms of the thirteen pairs (A_i, B_i) and of r_0 were computed modulo 11^{40} with a Gröbner basis over $\mathbb{Z}/11^{40}\mathbb{Z}$ that has unit leading coefficients and the same leading monomials as the reduced Gröbner basis of I over $\mathbb{Q}$. As the latter is 11-integral (checked in exact arithmetic, together with its 13-integrality, which is used in Appendix D.2), these are the reductions of the normal forms over $\mathbb{Q}$. The points of $\mathcal{X}_{\mathbb{F}_{11}}(\mathbb{F}_{1331})$ were found fibre by fibre over the u-line: in each of the charts $x_0 = 1$ and $x_1 = 1$ the coordinate ring is free of rank 14 over the polynomial ring in the base coordinate, and over a base value the rational points correspond to the joint eigenvectors, with eigenvalues in $\mathbb{F}_{1331}$, of the transposed matrices of multiplication

τ_0	(0 45 35 11 33)(1 34 12 36 44)(2 40 38 37 39)(3 21 20 28 6)(4 5 27 19 22) (7 42 17 13 9)(8 10 14 18 43)(15 25 31 23 29)(16 30 24 32 26)(41 49 46 47 48)
τ_1	(0 5 13 18 16 10 8)(1 7 9 15 17 14 6)(2 19 21 35 36 22 20)(3 26 49 46 40 27 23) (4 24 28 39 47 48 25)(11 31 37 45 34 30 42)(12 43 29 33 44 38 32); fixed point 41
ind $\beta(j)$	$0 \mapsto 4$, $1 \mapsto 37$, $2 \mapsto 45$, $3 \mapsto 35$, $4 \mapsto 6$, $5 \mapsto 11$, $6 \mapsto 30$, $7 \mapsto 44$, $8 \mapsto 46$, $9 \mapsto 2$, $10 \mapsto 39$, $11 \mapsto 8$, $12 \mapsto 33$, $13 \mapsto 18$, $14 \mapsto 23$, $15 \mapsto 9$, $16 \mapsto 32$, $17 \mapsto 16$, $18 \mapsto 25$, $19 \mapsto 3$, $20 \mapsto 38$, $21 \mapsto 10$, $22 \mapsto 31$, $23 \mapsto 28$, $24 \mapsto 13$, $25 \mapsto 48$, $26 \mapsto 42$, $27 \mapsto 21$, $28 \mapsto 20$, $29 \mapsto 47$, $30 \mapsto 43$, $31 \mapsto 15$, $32 \mapsto 26$, $33 \mapsto 5$, $34 \mapsto 36$, $35 \mapsto 17$, $36 \mapsto 24$, $37 \mapsto 22$, $38 \mapsto 19$, $39 \mapsto 27$, $40 \mapsto 14$, $41 \mapsto 49$, $42 \mapsto 1$, $43 \mapsto 40$, $44 \mapsto 12$, $45 \mapsto 29$, $46 \mapsto 7$, $47 \mapsto 34$, $48 \mapsto 41$, $49 \mapsto 0$

TABLE 17. The monodromy of $\mathcal{X}' \to \mathbb{P}^1$ in Proposition 5.8: the permutations τ_0, τ_1 of the 50 points of $\mathcal{X}'$ over $t = 1/2$, numbered $0, \dots, 49$ in order of increasing real part and then increasing imaginary part of the root φ of $G(\varphi, 1/2)$, and the labelling β, listed as $j \mapsto \operatorname{ind}\beta(j)$, where ind is the index of lines in $\mathbb{P}^1(k)$ defined in Appendix C.1.

by $x_2, \dots, x_7$, the eigenvalues being the coordinates of the point. A joint eigenspace has dimension at most one, so every point is found exactly once. At each point, $\bar{t}$ was evaluated as $\bar{A}_i/\bar{B}_i$ for each of the thirteen pairs of the basis of $V_{\mathbb{Z}_{11}}$ constructed in the proof of Lemma 5.11, and these values agree wherever they are defined. The value of $\bar{r}_0$ was obtained by substitution, and at the four points over U where $\bar{r}_0$ vanishes, the coordinates were expanded as power series in a local parameter. The Frobenius polynomials of the 1329 curves H_{t_0} were computed with PARI's `hyperellcharpoly` and checked against direct point counts. Independently, a primary decomposition over $\mathbb{F}_{11}$ of the fibres of $\bar{t}$ over 0, 1, ∞ gives closed points of degrees $5, 5$; $1, 1, 3, 3$; and $1, 1$ and eight of degree 2, hence 0, 8 and 2 points over $\mathbb{F}_{1331}$.

The reductions modulo 11 of the q_i and of r_0 are in the supplementary data [31].

E.5. **Software.** The computations used PARI/GP 2.17.3 [44] (partly through its Python interface cypari2 2.2.4), FLINT [22] through python-flint 0.8.0, SymPy 1.14.0 and NumPy 2.5.2 under Python 3.12, with the ball arithmetic of Arb [32] through python-flint for Appendix E.3. The Gröbner-basis computations of Sections 5 and 7, of Appendix D and of Appendix E.4 were done with SINGULAR 4.4.1 [18]. The maximal order of the quintic field L of Section 6.2 is certified with PARI's `nfcertify`, and the class groups and unit groups of L and of $\mathbb{Q}(\sqrt{5}, \zeta_7)$ (proof of Proposition 4.9) with `bnfcertify`. Neither assumes the generalized Riemann hypothesis. For $\mathcal{E}$ only the statement that the class group is a quotient of the computed one is certified (`bnfcertify(·,1)`, Lemma 3.7), and the units that PARI/GP computes for $\mathcal{E}$ are not used. Finite-field enumerations and the linear algebra modulo 5 and modulo 169 are implemented directly, without a computer algebra system.

E.6. **Data availability.** The inputs, programs and outputs of all computations are deposited at Zenodo [31]. The deposit also contains, in machine-readable form, the data that are too large to print here: the canonical model of $\mathcal{X}$ over $\mathbb{Q}$ with the map t and the function r; the plane model $G(\varphi, t)$ of Proposition 5.5; the descent function Θ and the local points of Section 6; the rational forms $\mathcal{Q}_j$ and the other data at 13 of Section 7; and the intermediate states of the period computation of Appendix E.2.

Declarations

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

Competing interests. The author declares no competing interests.

Research methodology. The author designed and operated the multi-agent research system used in this work, built on OpenAI GPT-6 Astra. The system carried out literature analysis, mathematical development and computation, with checks assigned to agents separate from those developing the arguments.

Use of generative AI in the manuscript. Anthropic Claude Opus 5.5 was used to draft and revise the manuscript. The author reviewed the material and takes full responsibility for the article.

References

1. Jeffrey D. Achter and Everett W. Howe, *Hasse–Witt and Cartier–Manin matrices: a warning and a request*, Arithmetic geometry: computation and applications (Yves Aubry, Everett W. Howe, and Christophe Ritzenthaler, eds.), Contemp. Math., vol. 722, Amer. Math. Soc., Providence, RI, 2019, https://doi.org/10.1090/conm/722/14534. Corrected version: arXiv:1710.10726v5 (2020), which fixes an error in §2.5 of the published text, pp. 1–18.
2. Martin Azon, *Effective Darmon's program for the generalised Fermat equation*, 2025, Preprint, arXiv:2504.01967v2.
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, https://doi.org/10.1007/978-3-319-32162-2_3, pp. 173–205.
4. Nicolas Billerey, Imin Chen, Luis V. Dieulefait, and Nuno Freitas, *On Darmon's program for the generalized Fermat equation, I*, 2025, Extended version, arXiv:2205.15861v5, whose numbering is used here. A shorter version, numbered differently, is published in J. Reine Angew. Math. **822** (2025), 107–146, https://doi.org/10.1515/crelle-2025-0014.
5. Bryan J. Birch and Willem Kuyk (eds.), *Modular functions of one variable IV*, Lecture Notes in Math., vol. 476, Springer, Berlin, 1975, Proceedings of the International Summer School, University of Antwerp, RUCA, 1972, https://doi.org/10.1007/BFb0097580.
6. Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I (Pierre Cartier, Luc Illusie, Nicholas M. Katz, Gérard Laumon, Yuri Manin, and Kenneth A. Ribet, eds.), Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.
7. Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21, Springer-Verlag, Berlin, 1990, https://doi.org/10.1007/978-3-642-51438-8.
8. Christophe Breuil and Fred Diamond, *Formes modulaires de Hilbert modulo p et valeurs d'extensions entre caractères galoisiens*, Ann. Sci. Éc. Norm. Supér. (4) **47** (2014), no. 5, 905–974, https://doi.org/10.24033/asens.2230; arXiv:1208.5367.
9. Nils Bruin, *The arithmetic of Prym varieties in genus 3*, Compos. Math. **144** (2008), no. 2, 317–338, https://doi.org/10.1112/S0010437X07003314.
10. Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.
11. Peter Chocian, *The primitive generalized Fermat equation $x^3 + y^5 = z^7$: a computer-assisted proof*, 2026, Preprint, arXiv:2609.26996v1.
12. Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770, https://doi.org/10.1215/S0012-7094-85-05240-8.
13. Robert F. Coleman and Adrian Iovita, *The Frobenius and monodromy operators for curves and abelian varieties*, Duke Math. J. **97** (1999), no. 1, 171–215, https://doi.org/10.1215/S0012-7094-99-09708-9; arXiv:math/9701229.
14. 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, https://doi.org/10.4064/aa164-1-5.

15. ———, *On the generalized Fermat equation $x^5+y^3=z^7$*, July 2024, Working paper, https://few.vu.nl/~sdn249/GFE357.pdf.
16. Henri Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's last theorem*, Duke Math. J. **102** (2000), no. 3, 413–449, https://doi.org/10.1215/S0012-7094-00-10233-5.
17. Henri Darmon and Andrew Granville, *On the equations $z^m = F(x,y)$ and $Ax^p + By^q = Cz^r$*, Bull. Lond. Math. Soc. **27** (1995), no. 6, 513–543, https://doi.org/10.1112/blms/27.6.513.
18. Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, *Singular 4.4.1: a computer algebra system for polynomial computations*, 2025, https://www.singular.uni-kl.de.
19. Pierre Deligne and Nicholas M. Katz, *Groupes de monodromie en géométrie algébrique (SGA 7 II)*, Lecture Notes in Math., vol. 340, Springer, Berlin, 1973, Séminaire de géométrie algébrique du Bois-Marie 1967–1969, https://doi.org/10.1007/BFb0060505.
20. Lassina Dembélé and John Voight, *Explicit methods for Hilbert modular forms*, Elliptic curves, Hilbert modular forms and Galois deformations (Henri Darmon, Fred Diamond, Luis V. Dieulefait, Bas Edixhoven, and Víctor Rotger, eds.), Adv. Courses Math. CRM Barcelona, Birkhäuser/Springer, Basel, 2013, https://doi.org/10.1007/978-3-0348-0618-3_4, pp. 135–198.
21. Luis V. Dieulefait and Ariel Pacetti, *A simplified proof of Serre's conjecture*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM **117** (2023), no. 4, Paper No. 153, https://doi.org/10.1007/s13398-023-01478-8; arXiv:2108.07577.
22. The FLINT team, *FLINT: Fast Library for Number Theory*, 2025, https://flintlib.org.
23. Nuno Freitas, Bao V. Le Hung, and Samir Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math. **201** (2015), no. 1, 159–206, https://doi.org/10.1007/s00222-014-0550-z.
24. Nuno Freitas, Bartosz Naskręcki, and Michael Stoll, *The generalized Fermat equation with exponents 2, 3, n*, Compos. Math. **156** (2020), no. 1, 77–113, https://doi.org/10.1112/S0010437X19007693.
25. Franco Golfieri Madriaga and Ariel Pacetti, *Hypergeometric motives and the generalized Fermat equation*, 2025, Preprint, arXiv:2412.08804v2; with an appendix by A. Pacetti and F. Rodriguez Villegas.
26. Franco Golfieri Madriaga, Ariel Pacetti, and Fernando Rodriguez Villegas, *On rank 2 hypergeometric motives*, 2026, Preprint, arXiv:2603.17978v1; with an appendix by E. Lorenzo García and A. Pacetti.
27. Alexander Grothendieck, *Groupes de monodromie en géométrie algébrique (SGA 7 I)*, Lecture Notes in Math., vol. 288, Springer, Berlin, 1972, Séminaire de géométrie algébrique du Bois-Marie 1967–1969, avec la collaboration de M. Raynaud et D. S. Rim, https://doi.org/10.1007/BFb0068688; Exposé IX (A. Grothendieck, *Modèles de Néron et monodromie*), pp. 313–523.
28. Alexander Grothendieck and Michèle Raynaud, *Revêtements étales et groupe fondamental (SGA 1)*, Doc. Math. (Paris), vol. 3, Soc. Math. France, Paris, 2003, Séminaire de géométrie algébrique du Bois-Marie 1960–1961; updated and annotated reprint of Lecture Notes in Math. 224, Springer, 1971; arXiv:math/0206203.
29. Allen Hatcher, *Algebraic topology*, Cambridge University Press, Cambridge, 2002.
30. Everett W. Howe, *The Weil pairing and the Hilbert symbol*, Math. Ann. **305** (1996), no. 2, 387–392, https://doi.org/10.1007/BF01444229.
31. Manvir Jaswal, *Supplementary data and programs for "The generalized Fermat equation $X^5+Y^3=Z^7$"*, Zenodo, 2026, https://doi.org/10.5281/zenodo.22949370.
32. Fredrik Johansson, *Arb: efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Trans. Comput. **66** (2017), no. 8, 1281–1292, https://doi.org/10.1109/TC.2017.2690633.
33. Chandrashekhar B. Khare and Jack A. Thorne, *Automorphy of some residually S_5 Galois representations*, Math. Z. **286** (2017), no. 1-2, 399–429, https://doi.org/10.1007/s00209-016-1766-y; arXiv:1503.03796.
34. Kamal Khuri-Makdisi, *Linear algebra algorithms for divisors on an algebraic curve*, Math. Comp. **73** (2004), no. 245, 333–357, https://doi.org/10.1090/S0025-5718-03-01567-9.
35. ———, *Asymptotically fast group operations on Jacobians of general curves*, Math. Comp. **76** (2007), no. 260, 2213–2239, https://doi.org/10.1090/S0025-5718-07-01989-8.
36. Abhinav Kumar and Ronen E. Mukamel, *Real multiplication through explicit correspondences*, LMS J. Comput. Math. **19** (2016), suppl. A, 29–42, https://doi.org/10.1112/S1461157016000188; arXiv:1602.01924.
37. The LMFDB Collaboration, *The L-functions and modular forms database*, 2026, https://www.lmfdb.org, accessed 23 September 2026.
38. James S. Milne, *Arithmetic duality theorems*, second ed., BookSurge, LLC, Charleston, SC, 2006.
39. ———, *Abelian varieties*, 2008, Course notes, v2.00, https://www.jmilne.org/math/CourseNotes/av.html.

40. ———, *Complex multiplication*, 2020, Course notes, v0.10, https://www.jmilne.org/math/CourseNotes/cm.html.
41. David Mumford, *Prym varieties I*, Contributions to analysis (a collection of papers dedicated to Lipman Bers) (Lars V. Ahlfors, Irwin Kra, Bernard Maskit, and Louis Nirenberg, eds.), Academic Press, New York, 1974, pp. 325–350.
42. Jürgen Neukirch, *Algebraic number theory*, Grundlehren Math. Wiss., vol. 322, Springer, Berlin, 1999, https://doi.org/10.1007/978-3-662-03983-0.
43. Ariel Pacetti and Lucas Villagra Torcomian, *On the generalized Fermat equation of signature* $(5, p, 3)$, 2025, Preprint, arXiv:2512.17845v1.
44. The PARI Group, *PARI/GP version 2.17.3*, Univ. Bordeaux, 2025, https://pari.math.u-bordeaux.fr/.
45. Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of $X(7)$ and primitive solutions to $x^2+y^3 = z^7$*, Duke Math. J. **137** (2007), no. 1, 103–158, https://doi.org/10.1215/S0012-7094-07-13714-1.
46. Piet Hein Casper Putz, *Enumeration of local and global étale algebras applied to generalized Fermat equations*, Ph.D. thesis, Vrije Universiteit Amsterdam, 2024, https://doi.org/10.5463/thesis.832; full text at https://research.vu.nl/ws/portalfiles/portal/367784086/Thesis_CasperPutz.pdf.
47. Ashleigh Ratcliffe and Bogdan Grechuk, *Generalized Fermat equation: a survey of solved cases*, Expo. Math. **43** (2025), no. 4, Paper No. 125688, https://doi.org/10.1016/j.exmath.2025.125688; arXiv:2412.11933.
48. Michel Raynaud, *Schémas en groupes de type* $(p, \dots, p)$, Bull. Soc. Math. France **102** (1974), 241–280, https://doi.org/10.24033/bsmf.1779.
49. Takeshi Saito, *Hilbert modular forms and p-adic Hodge theory*, Compos. Math. **145** (2009), no. 5, 1081–1113, https://doi.org/10.1112/S0010437X09004175.
50. Edward F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), no. 3, 447–471, https://doi.org/10.1007/s002080050156. Erratum: Math. Ann. **339** (2007), no. 1, 1, https://doi.org/10.1007/s00208-007-0091-5. Corrected version: arXiv:1507.08325.
51. Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517, https://doi.org/10.2307/1970722.
52. Samir Siksek and Michael Stoll, *Partial descent on hyperelliptic curves and the generalized Fermat equation $x^3 + y^4 + z^5 = 0$*, Bull. Lond. Math. Soc. **44** (2012), no. 1, 151–166, https://doi.org/10.1112/blms/bdr086.
53. The Stacks project authors, *The Stacks project*, 2026, https://stacks.math.columbia.edu.
54. John Voight, *Quaternion algebras*, Grad. Texts in Math., vol. 288, Springer, Cham, 2021, https://doi.org/10.1007/978-3-030-56694-4.
55. John Voight and David Zureick-Brown, *The canonical ring of a stacky curve*, Mem. Amer. Math. Soc. **277** (2022), no. 1362, v+144 pp., https://doi.org/10.1090/memo/1362.
56. André Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041, Hermann, Paris, 1948.
57. Stefan Wewers, *Stable reduction of three point covers*, J. Théor. Nombres Bordeaux **17** (2005), no. 1, 405–421, https://doi.org/10.5802/jtnb.498.
58. Yuri G. Zarhin, *p-adic abelian integrals and commutative Lie groups*, J. Math. Sci. (New York) **81** (1996), no. 3, 2744–2750, https://doi.org/10.1007/BF02362339; arXiv:alg-geom/9603006.

Independent researcher, Toronto, Canada
Email address: manvirjaswal@icloud.com