hexagon:2611.00591v1

THE RATIONAL POINTS OF THE NON-SPLIT CARTAN MODULAR CURVE OF LEVEL 25

MANVIR JASWAL

Abstract. We prove that the modular curve $X_{\mathrm{ns}}^{+}(25)$ of the normalizer of a non-split Cartan subgroup of level 25, of genus 14 and Jacobian rank 14, has exactly nine rational points, all of them CM. This is the level 25 case of a conjecture of Rouse, Sutherland and Zureick-Brown, and with their theorem it determines the 5-adic images of Galois of elliptic curves over $\mathbb{Q}$ without complex multiplication. A descent by the modular units of the curve, using no information on the Mordell–Weil group, places every rational point in the residue disc of a CM point at the prime 1151. Quadratic Chabauty at 1151, with two correspondences that change only the level structure, then shows that each of these discs holds one rational point. The local term at 5 of these correspondences vanishes, by a formula of Betts and Dogra, because their eigenvalues lie in $\sqrt{5}\,\mathbb{Q}$, and the height pairing is fixed by the nine CM points alone.

Contents

1. Introduction 1
2. The curve 6
3. The descent 7
4. Modular units at level 25 8
5. The labels and the residue discs 10
6. Correspondences that change only the Cartan subring 11
7. The term at 5 15
8. Heights at the auxiliary prime 17
9. Control equations and the disc of a known point 18
10. The rank 20
11. The prime 1151 20
Declarations 23
References 23

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Its Galois image on torsion is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ by Serre [39], and Mazur's Program B [34, p. 109] asks which images occur. Write $N_{\mathrm{ns}}(m)$ for the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/m)$ and $X_{\mathrm{ns}}^{+}(m)$ for its modular curve. For a prime ℓ, Rouse, Sutherland and Zureick-Brown [36, Theorem 1.6] show that the ℓ-adic image H of E falls in one of four cases: X_H is $\mathbb{P}^1$ or an

Date: November 18, 2026.
2020 *Mathematics Subject Classification.* Primary 11G18; Secondary 11G05, 11F80, 11G50, 11R27, 14G05.
Key words and phrases. Non-split Cartan modular curves, modular units, Kummer descent, quadratic Chabauty, p-adic heights, Galois images of elliptic curves.

elliptic curve of rank one; X_H has an exceptional rational point and H is in an explicit list; $H \leq N_{\mathrm{ns}}(m)$ for $m = 3^3, 5^2, 7^2, 11^2$ or a prime $m = \ell \geq 19$; or H lies in one of two groups of level 49. They conjecture that in the last two cases X_H has no exceptional rational points, that is, none other than cusps and CM points [36].

For $m = 25$ the curve $X := X_{\mathrm{ns}}^+(25)$ has genus 14, rational CM points and no rational cusps, and every isogeny factor of its Jacobian has analytic rank equal to its dimension [36, pp. 3–4 and Table 2]. Rouse, Sutherland and Zureick-Brown computed a canonical model of X and, searching the points of $X_{\mathrm{ns}}^+(5) \cong \mathbb{P}^1$ of height at most 1000 with a test on traces of Frobenius, found eight rational points, all CM [36, §9.2]; the CM point of discriminant -8, with j-invariant 8000, is a ninth. They could not determine $X(\mathbb{Q})$ [36]. The neighboring cases are settled: $m = 27$ by Balakrishnan, Betts, Hast, Jha and Müller [4, Theorem 1.3], $m = 49$ by Furio and Lombardo [18, Theorem 1.4], and the two groups of level 49 by Arango-Piñeros and Zureick-Brown [1, Theorem 2]. The case $m = 121$ is treated in [23].

Let $\mathcal{D} := \{-3, -7, -8, -12, -27, -28, -43, -67, -163\}$. For $D \in \mathcal{D}$ let $y_D \in X(\mathbb{Q})$ be the CM point of discriminant D (Lemma 2.2).

Theorem 1.1. *The curve $X_{\mathrm{ns}}^+(25)$ has exactly nine rational points, the CM points y_D, $D \in \mathcal{D}$.*

The proof does not use the classification of imaginary quadratic orders of class number one, so, as each such order of conductor prime to 5 in whose field 5 is inert gives a rational point of X (proof of Lemma 2.2), Theorem 1.1 recovers that these orders are exactly those with discriminant in $\mathcal{D}$. That rational points on non-split Cartan curves bear on the class number one problem in this way was noted by Serre [40, Appendix].

Corollary 1.2. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acting on $E[25]$ is not contained in a conjugate of $N_{\mathrm{ns}}(25)$. So the case $H \leq N_{\mathrm{ns}}(5^2)$ of* [36, Theorem 1.6 (iii)] *does not occur, and the 5-adic image of E is, up to conjugacy, one of the 25 subgroups of $\mathrm{GL}_2(\mathbb{Z}_5)$ counted in* [36, Table 3]*, each of level at most 25 and index at most 120.*

Proof. Such an E would give a rational point of X with j-invariant $j(E)$, which is not a CM j-invariant, against Theorem 1.1. The groups in cases (iii) and (iv) of [36, Theorem 1.6] other than $N_{\mathrm{ns}}(5^2)$ are proper subgroups of level prime to 5, so none contains H, which there is, up to conjugacy, the inverse image in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of the 5-adic image of E and so maps onto $\mathrm{GL}_2(\mathbb{Z}/m)$ for every m prime to 5. By the first part the 5-adic image therefore falls under case (i) or (ii); at $\ell = 5$ these are the 23 groups H of 5-power level with $X_H(\mathbb{Q})$ infinite and the two exceptional groups of [36, Table 1] counted in [36, Table 3], where the count assumes only, at $\ell = 5$, that $N_{\mathrm{ns}}(5^2)$ does not occur. □

Karabiyik has announced a determination of $X(\mathbb{Q})$ by quadratic Chabauty in the framework of p-adic adelic metrics of Besser, Müller and Srinivasan [24], [6, §7].

The obstacle. The Jacobian J of X has rank 14, its genus (Proposition 10.1), so the method of Chabauty and Coleman does not apply, while quadratic Chabauty [5] does. For modular curves of rank equal to genus it works as follows [2, §1.5], [3, Algorithm 3.12]. At an auxiliary prime q of good reduction, a correspondence Z of trace zero gives a locally analytic function on $X(\mathbb{Q}_q)$, the local height at q minus a bilinear form in the abelian logarithm, which on $X(\mathbb{Q})$ takes only the values allowed by the local heights at the bad primes. It is expanded as a power series on every residue disc modulo q, and $X(\mathbb{Q})$ lies among the

points where it takes one of these values. The bilinear form is fixed by the heights at known rational points, each of which gives a linear equation, and the Hecke action reduces the number of points needed [2, §1.7], [4, §2.5]; generators of $J(\mathbb{Q})$ are not needed. In this way the rational points were determined at levels 13 and 17 [2, 3] and 27 [4]. Hashimoto, Lido, Lombardo, Mascot and Parent work from the moduli interpretation instead of an equation of the curve, at prime level [20]. At the bad prime the local term has to be controlled: at level 27 it vanishes because every local point reduces to the one Galois-stable component of a stable model [4, §3.6], and at level 17 the correspondences were chosen, through a known stable model, so that it vanishes [3, §5.5].

Our last step is a first-order argument modulo q^2 at a known rational point: it expands the height identity only at a point y_D, so it can only show that the residue disc of y_D contains no second rational point. So every other disc has to be excluded first, by the descent below. At 5 the Jacobian has potentially good reduction (Lemma 7.1), and we choose correspondences for which the local term vanishes without a stable model. Leonhardt and Rendell computed a basis of H^1_{dR} of X from modular forms and the Hodge filtration for a correspondence on it, the first steps of quadratic Chabauty for this curve [32, Theorem A]. We do not use them: the local heights at the auxiliary prime q that enter are, modulo q^2, logarithms of values of functions (Lemma 8.1), so no splitting of the Hodge filtration is computed. Working modulo q^2 with integral data rather than with q-adic power series is also the point of view of geometric quadratic Chabauty [17].

Residue discs from modular units. The ten cusps of X are defined over $K := \mathbb{Q}(\zeta_{25})^+$, and $G := \mathrm{Gal}(K/\mathbb{Q})$ permutes them simply transitively. Products of Siegel functions along the orbits of $N_{\mathrm{ns}}(25) \cap \mathrm{SL}_2(\mathbb{Z}/25)$ give functions on X over K with divisors supported on the cusps. Those whose divisor is divisible by 5, modulo fifth powers and constants, form an $\mathbb{F}_5[G]$-module V of dimension 8 (Section 4). For rational points x and y the quotient $u(x)/u(y)$ of the values of such a unit has valuation divisible by 5 at every prime of K not above 5, because X has a smooth model over $\mathbb{Z}[1/5]$. As $5 \nmid h(K)$, it is a 5-unit up to a fifth power, and the 5-units modulo fifth powers form a free $\mathbb{F}_5[G]$-module of rank one on $\eta := (1-\zeta_{25})(1-\zeta_{25}^{-1})$. So x has a label in $\mathrm{Hom}(V, \mathbb{F}_5)$, one of 5^8, and at a prime $q \equiv 1 \bmod 25$ the label is read off the reduction of x by fifth-power residue symbols. The general statement is the following.

Theorem 1.3. *Let $X/\mathbb{Q}$ be a smooth projective geometrically connected curve, $m \geq 2$ an integer, $F/\mathbb{Q}$ a finite Galois extension with group G, and S a finite G-stable set of primes of F. Let Λ be a $\mathbb{Z}[G]$-module that is finitely generated over $\mathbb{Z}$, and $e \mapsto u_e$ a homomorphism $\Lambda \to F(X)^\times$, such that:*

(U1) *the divisors of the u_e are supported on a finite set $\Sigma \subset X(F)$ with $\Sigma \cap X(\mathbb{Q}) = \emptyset$, and $\sigma(u_e) \in F^\times u_{\sigma e}$ for $\sigma \in G$, acting on coefficients;*

(U2) *for each prime $\mathfrak{q} \notin S$ of F, the curve X_F has a regular proper model over $\mathcal{O}_{F,\mathfrak{q}}$ with irreducible special fiber.*

Let $\Lambda_m := \{e \in \Lambda : \operatorname{div} u_e \in m\operatorname{Div}(X_F)\}$ and $\Lambda_0 := \{e \in \Lambda : u_e \in F^\times\}$, and put $V := \Lambda_m/(m\Lambda + \Lambda_0)$ and

$$F(S,m) := \{a \in F^\times/F^{\times m} : m \mid v_{\mathfrak{q}}(a) \text{ for every prime } \mathfrak{q} \notin S\}.$$

Fix $y \in X(\mathbb{Q})$.

(a) *For $x \in X(\mathbb{Q})$, the map $e \mapsto u_e(x)/u_e(y)$ induces a G-equivariant homomorphism $\Phi_x \colon V \to F(S,m)$.*

(b) *Let $\mathfrak{q} \notin S$ be a prime of F, unramified and of degree one over a prime q at which X has good reduction, let $\chi_{\mathfrak{q}}\colon F(S,m) \to \mathbb{F}_q^\times/\mathbb{F}_q^{\times m}$ be the m-th power residue symbol at $\mathfrak{q}$, and let $\bar{x}$ denote reduction modulo q. Then $\chi_{\mathfrak{q}}(\Phi_x(e)) = \tilde{u}_e(\bar{x})/\tilde{u}_e(\bar{y})$ for $e \in \Lambda_m$, where $\tilde{u}_e(\bar{x}) \in \mathbb{F}_q^\times/\mathbb{F}_q^{\times m}$ is the leading coefficient of u_e at $\bar{x}$ (the value of $\bar{u}_e$ at $\bar{x}$ when no point of Σ reduces to $\bar{x}$), defined in Section 3.*

So if Q is a finite set of such primes, Φ_x lies in the set of $\Phi \in \mathrm{Hom}_G(V, F(S,m))$ such that for each $\mathfrak{q} \in Q$ some $\bar{z} \in X(\mathbb{F}_q)$ has $\chi_{\mathfrak{q}}(\Phi(e)) = \tilde{u}_e(\bar{z})/\tilde{u}_e(\bar{y})$ for all e; and $\bar{x}$ is one such $\bar{z}$. On a modular curve X_H of level M with no rational cusp, the modular units give (U1), with F the field of the cusps, and the smooth model of Deligne and Rapoport over $\mathbb{Z}[1/M]$ gives (U2) with S the primes above M. To use the theorem one needs $F(S,m)$ explicitly, and Remark 3.1 gives a condition under which it is. At level 25, with $m = 5$, $F = K$ and S the prime above 5, it gives:

Theorem 1.4. *For every $x \in X(\mathbb{Q})$ there is $D \in \mathcal{D}$ such that x and y_D have the same reduction modulo* 1151.

The proof uses no rank, generator or Shafarevich–Tate group of J and no integrality of j. Evaluating functions whose divisors are m-th multiples, modulo m-th powers, is the classical descent by functions [38, §2.1, Lemma 2.1], [8, §2]. For $e \in \Lambda_5$ put $T_e := [\frac{1}{5}\operatorname{div} u_e] \in J(K)[5]$. By Weil reciprocity, a rational divisor A of degree 0 away from the cusps gives $e \mapsto u_e(A)$ modulo fifth powers, depending only on the class of A modulo $5J(\mathbb{Q})$; this is the descent map attached to the classes T_e. So the label Φ_x is the value at $[x-y]$ of a homomorphism $J(\mathbb{Q})/5 \to \mathrm{Hom}_G(V, K(S,5))$, computed without knowing $J(\mathbb{Q})$. The sieve at the primes q has the shape of the Mordell–Weil sieve [9], with $\mathrm{Hom}_G(V, K(S,5))$ in place of $J(\mathbb{Q})/5$. Here the functions are the modular units of the curve, their classes form a module over the Galois group of the field of the cusps, and the local conditions are fifth-power residue symbols at split primes. The proof at level 49 of Arango-Piñeros and Zureick-Brown is also a descent of Kummer type, on the superelliptic equations $F(x,y) = kw^7$ of Furio and Lombardo, where F is the binary cubic whose roots are the non-rational cusps of $X_{\mathrm{ns}}^+(7)$ or of $X_{\mathrm{sp}}^+(7)$ [1, pp. 2–3, 6].

The term at 5. To finish we use quadratic Chabauty at $q = 1151$, with correspondences that fix the elliptic curve and change only the level structure. As $q \equiv 1 \bmod 25$, the labels can be read at q (Section 5), and as $q \equiv 11 \bmod 12$, the fixed points of the correspondences are supersingular modulo q; so are eight of the nine y_D, as their D are not squares modulo q, and all computations except those at y_{-163} stay over $\mathbb{F}_{q^2}$ (Section 11). For $\nu \in \mathbb{F}_5^\times$, S_ν sends a Cartan subring $(\mathbb{Z}/25)[x]$, with $\operatorname{tr} x = 0$ and $x^2 = 2$, to the six $(\mathbb{Z}/25)[x']$ with $x' = x + 5w$, where w anticommutes with x modulo 5 and $w^2 \equiv \nu$. On the Cartan subrings congruent to a given one modulo 5, S_ν is a Cayley graph on $\mathbb{F}_{25}$, whose eigenvalues other than its degree 6 are the sums $\Upsilon(m) := \sum_{\mathrm{N}\,\gamma = m} \zeta_5^{\operatorname{Tr}\gamma}$ over $\gamma \in \mathbb{F}_{25}$, which are minus the Kloosterman sums $\sum_{x \in \mathbb{F}_5^\times} \zeta_5^{x+m/x}$. Put $Z_1 := S_2 - S_3$ and $Z_2 := S_1 - S_4$. For the quartic character χ of $\mathbb{F}_5^\times$ with $\chi(2) = i$, $Z_2 - iZ_1 = \sum_\nu \bar{\chi}(\nu) S_\nu$, and by Hasse–Davenport its non-zero eigenvalues are squares of Gauss sums up to fourth roots of unity; so Z_1 and Z_2 have their eigenvalues in $\sqrt{5}\,\mathbb{Q}$ (Proposition 6.4). So the local term at 5 vanishes, with no stable model, by the following criterion.

Proposition 1.5. *Let p be a prime and $X/\mathbb{Q}_p$ a smooth projective geometrically connected curve of genus at least 2 whose Jacobian J has potentially good reduction. Let $C = \sum_i n_i C_i$ be a symmetric correspondence over $\mathbb{Q}_p$, where the $C_i \subset X \times X$ are distinct irreducible curves other than the diagonal and the n_i are non-zero integers, with non-zero endomorphism Z of J; let $\operatorname{Fix} C$ and $C(y)$ be its pull-backs by the diagonal $X \to X \times X$ and, for $y \in X$, by $x \mapsto (y, x)$. Let $\ell \neq p$ be a prime and $H := H^1_{\acute{e}t}(X_{\bar{\mathbb{Q}}_p}, \bar{\mathbb{Q}}_\ell)$. Suppose there is $\alpha \in \bar{\mathbb{Q}}_\ell$ with $\alpha \notin \mathbb{Q}$ such that Z acts on each isotypic component of H under the inertia group of $\mathbb{Q}_p$ by a scalar in $\mathbb{Q}\alpha$. Then for all $y, z \in X(\mathbb{Q}_p)$ such that none of (y, y), (z, z), (y, z) lies on a C_i,*

$$i_p(z - y,\ \operatorname{Fix} C - C(y) - C(z)) = 0,$$

where i_p is the Néron local symbol.

The proof (Section 7) rests on the formula of Betts and Dogra for this local term [7, Corollary 12.1.3, Remark 12.1.4]. It expresses the term as a pairing with a measure on the stable reduction graph. Potentially good reduction makes the graph a tree; then the mass of the measure on each inertia orbit of vertices is half the trace of an endomorphism of an abelian variety, so rational, and also lies in $\mathbb{Q}\alpha$, so it is 0; the masses are constant on orbits, so the measure is 0. Betts and Dogra treat $X^+_{\mathrm{ns}}(p)$ for primes $p > 3$ with $p \equiv 3 \bmod 4$ through the components of its special fiber [7, §12.2.1]. The hypothesis of Proposition 1.5 holds for Z_1 and Z_2 (Section 7), which act on the ℓ-adic representation $\sigma(\pi)$ of each automorphic representation π occurring in the cohomology of X through the restriction $\pi_5|_{\mathrm{GL}_2(\mathbb{Z}_5)}$ of its local component at 5. It does not hold for Hecke operators such as T_2, whose eigenvalues are not determined by $\pi_5|_{\mathrm{GL}_2(\mathbb{Z}_5)}$.

The height pairing from the CM points. With all local terms away from q zero, the height identity for a pair of known rational points becomes a linear equation on the height pairing, with a right side in $q\mathbb{Z}_q$. The pairing is determined by a linear functional on the Hecke algebra modulo q, and at $q = 1151$ the equations from the nine CM points (the control equations), for Z_1 and Z_2, have rank 14 on the 14-dimensional space of such functionals; one correspondence would give at most eight (Remark 9.2). So they show that the pairing is integral on $J(\mathbb{Q}) \otimes \mathbb{Z}_q$ and determine it modulo q^2. On the disc of y_D, a second rational point would satisfy a congruence for each of Z_1 and Z_2, with coefficients that we compute, and at each of the nine discs the two congruences have no common solution (Table 1). The general form is Proposition 9.1.

Outline.

1. **Discs** (Sections 3, 4 and 5). Every $x \in X(\mathbb{Q})$ has the reduction modulo 1151 of some y_D.
2. **Rank** (Section 10). $\operatorname{rank} J(\mathbb{Q}) = 14$.
3. **Correspondences** (Section 6). Z_1 and Z_2 have eigenvalues in $\sqrt{5}\,\mathbb{Q}$ and fixed points over $j = 0$ and 1728.
4. **The term at 5** (Section 7). Their local term at 5 vanishes.
5. **Heights** (Sections 8 and 9). The control equations fix the height pairing, and Proposition 9.1 gives a criterion for a known point to be alone in its disc.
6. **The prime 1151** (Section 11). The hypotheses hold at $q = 1151$, and the criterion holds at each of the nine points.

Computations. The computations on which the proofs rest use PARI/GP and Python and are exact, except for the L-values of Proposition 10.1, which are computed in FLINT's ball arithmetic. The programs, which run in about three hours on one thread, are deposited with their outputs at [22].

2. The curve

Let $\mathcal{G} := \mathrm{GL}_2(\mathbb{Z}/25)$, let $\xi := \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right)$, so that $\xi^2 = 2$, and let $\mathcal{C} := (\mathbb{Z}/25)[\xi] \subset M_2(\mathbb{Z}/25)$. As 2 is not a square modulo 5, $\mathcal{C}$ is the unramified quadratic extension of $\mathbb{Z}/25$, and $\mathcal{C}^\times$ has order 600. Let $N \subset \mathcal{G}$ be the stabilizer of the subring $\mathcal{C}$ under conjugation. It is the normalizer $N_{\mathrm{ns}}(25)$ of the non-split Cartan subgroup $\mathcal{C}^\times$, it has order 1200, and $N = \mathcal{C}^\times \sqcup \mathcal{C}^\times s$ with $s := \mathrm{diag}(1, -1)$, which induces the non-trivial automorphism of $\mathcal{C}$. The elements of $\mathcal{C}^\times s$ are the matrices $\left(\begin{smallmatrix} a & -2b \\ b & -a \end{smallmatrix}\right)$, all of trace 0, and $\det(N) = (\mathbb{Z}/25)^\times$. Let Ω be the set of conjugates of $\mathcal{C}$, which we call Cartan subrings; $|\Omega| = 250$. Each contains exactly two elements x with $\operatorname{tr} x = 0$ and $x^2 = 2$, namely $\pm x$, and every such $x \in M_2(\mathbb{Z}/25)$ generates a Cartan subring, since $t^2 - 2$ is irreducible modulo 5.

Let Y be the compactified moduli scheme over $\mathbb{Z}[1/5]$ of pairs (E, ϕ) with $\phi\colon (\mathbb{Z}/25)^2 \to E[25]$ an isomorphism, with the right action $r_g(E, \phi) := (E, \phi \circ g)$ of $\mathcal{G}$. The quotient $X := Y/N$, through $(E, \phi) \mapsto (E, \phi\mathcal{C}\phi^{-1})$, is the curve of pairs (E, R) with $R \subset \mathrm{End}(E[25])$ a Cartan subring, meaning that $\phi^{-1}R\phi \in \Omega$ for one, hence every, ϕ. It is $X_{\mathrm{ns}}^+(25)$, it is geometrically connected because $\det(N) = (\mathbb{Z}/25)^\times$, it has degree 250 over the j-line, and its genus is 14 [36, Table 2]. As ξ is conjugate to its transpose, N is conjugate to its transpose, so the usual conventions for level structures give the same curve. By Deligne and Rapoport [16, VI, Proposition 6.7], X has a smooth proper model $\mathcal{X}$ over $\mathbb{Z}[1/5]$, the coarse moduli scheme of the same problem. For $\mathbb{Q}(X)$ we use Shimura's model [42, Theorem 6.6, Proposition 6.9]: the field $\mathcal{F}$ of modular functions for $\Gamma(25)$ whose $q^{1/25}$-expansions have coefficients in $\mathbb{Q}(\zeta_{25})$ is Galois over $\mathbb{Q}(j)$ with group $\mathcal{G}/\{\pm 1\}$, an element of $\mathrm{SL}_2(\mathbb{Z}/25)$ acting by composition with a lift to $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{diag}(1, d)$ by $\zeta_{25} \mapsto \zeta_{25}^d$ on coefficients, and $\mathbb{Q}(X) = \mathcal{F}^N$.

Lemma 2.1. *The curve X has ten cusps, each of width 25. They are defined over $K := \mathbb{Q}(\zeta_{25})^+$, and $G := \mathrm{Gal}(K/\mathbb{Q})$ acts on them simply transitively. For $d \in (\mathbb{Z}/25)^\times$ choose $g_d \in N$ with $\det g_d = d$ and put $B_d := g_d^{-1}\,\mathrm{diag}(1, d) \in \mathrm{SL}_2(\mathbb{Z}/25)$. Then $\sigma_d(\infty) = B_d\infty$, where $\sigma_d \in G$ is induced by $\zeta_{25} \mapsto \zeta_{25}^d$.*

Proof. The width of the cusp $\gamma\infty$ is the least $h > 0$ with $\pm\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \gamma^{-1}N\gamma$. A conjugate of such an element is not in $\mathcal{C}^\times s$, whose elements have trace 0. In $\mathcal{C}^\times$ the elements $a + b\xi$ with characteristic polynomial $(t \mp 1)^2$ have $a = \pm 1$ and $5 \mid b$, so $a + b\xi \mp 1 = b\xi$ is 5 times a matrix that is 0 or invertible modulo 5, whereas, for $0 < h < 25$, $\left(\begin{smallmatrix} 0 & h \\ 0 & 0 \end{smallmatrix}\right)$ is non-zero modulo 5 if $5 \nmid h$ and is 5 times a non-zero nilpotent if $5 \mid h$. So every width is 25, and there are $250/25 = 10$ cusps.

Let $f \in K(X) = \mathcal{F}^{N_\pm}$, where $N_\pm := \{g \in N : \det g = \pm 1\}$. The element g_d fixes $\mathbb{Q}(X)$ and acts on $\mathbb{Q}(\zeta_{25})$ as σ_d, so it acts on $K(X)$ as σ_d; and $\mathrm{diag}(1, d) = g_dB_d$. If f and $\sigma_d f$ are regular at the relevant cusps, $\sigma_d(f(\infty))$ is the constant term of f with σ_d applied to its coefficients, that is, the value at ∞ of $f^{\mathrm{diag}(1,d)} = (\sigma_d f) \circ B_d$, which is $(\sigma_d f)(B_d\infty)$. As $\sigma_d(f(\infty)) = (\sigma_d f)(\sigma_d\infty)$ for all such f, $\sigma_d\infty = B_d\infty$. Now $B_d\infty = \infty$ on X if and only if $\mathrm{diag}(1, d) \in N \cdot \{\pm\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)\}$, so if and only if N contains an upper triangular matrix with diagonal $\pm(1, d)$. The upper triangular elements of N are the $\mathrm{diag}(a, \pm a)$, so this happens exactly for $d = \pm 1$. Hence ∞ is defined over K with stabilizer $\{1\}$ in G, and its orbit has ten elements. □

For $d \in (\mathbb{Z}/25)^\times/\{\pm 1\}$ we write $c_d := \sigma_d(\infty)$ for the cusps.

Lemma 2.2. *Let $D \in \mathcal{D}$ and let $E_D/\mathbb{Q}$ have complex multiplication by the order $\mathcal{O}_D$ of discriminant D. The image of $\mathcal{O}_D$ in $\mathrm{End}(E_D[25])$ is a Cartan subring stable under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, so it defines a point $y_D \in X(\mathbb{Q})$ with $j(y_D) = j_D$. For D in the order of $\mathcal{D}$, $j_D = 0$, -3375, 8000, 54000, -12288000, 16581375, -884736000, -147197952000 and -262537412640768000. The map $X \to X(1)$ is unramified at each y_D, so $j - j_D$ is a local parameter at y_D. For $D = -3$ this holds modulo every prime $q \geq 7$, and for $D \neq -3$ modulo every prime $q \geq 7$ with $j_D \not\equiv 0, 1728 \bmod q$.*

Proof. As 5 is inert in $\mathbb{Q}(\sqrt{D})$ and prime to the conductor of $\mathcal{O}_D$, $\mathcal{O}_D/25$ is the unramified quadratic extension of $\mathbb{Z}/25$. Since $E_D[25]$ is free of rank one over $\mathcal{O}_D/25$, the image of $\mathcal{O}_D$ is a Cartan subring. Galois conjugation carries $\mathcal{O}_D \subset \mathrm{End}(E_{D,\bar{\mathbb{Q}}})$ to itself, so the subring is Galois-stable. For $j_D \neq 0$, $\mathrm{Aut}(E_D) = \{\pm 1\}$ and $X \to X(1)$ is unramified. For $D = -3$ the automorphism of order 6 lies in $\mathcal{O}_{-3}$, so it normalizes the Cartan subring and the ramification index is again 1. Modulo a prime $q \geq 7$ the reduction of E_{-3} has automorphism group μ_6, and that of E_D, $D \neq -3$, has automorphism group $\{\pm 1\}$ when $j_D \not\equiv 0, 1728$. □

3. The descent

We prove Theorem 1.3. For $\mathfrak{q} \notin S$ let $\mathcal{X}_\mathfrak{q}$ be the model of (U2), and write its special fiber as $r\,\mathcal{X}_{\mathfrak{q},s}$ with $\mathcal{X}_{\mathfrak{q},s}$ integral. A point $x \in X(\mathbb{Q})$ extends to a section $\tilde{x}$ of $\mathcal{X}_\mathfrak{q}$, as $\mathcal{X}_\mathfrak{q}$ is proper, and $r\,\tilde{x}^*\mathcal{X}_{\mathfrak{q},s}$ is the pull-back of the divisor of a uniformizer, of degree 1. So $r = 1$: the special fiber is reduced and $\deg \tilde{x}^*\mathcal{X}_{\mathfrak{q},s} = 1$.

Proof of Theorem 1.3 (a). As $x, y \notin \Sigma$, the values $u_e(x)$, $u_e(y)$ are defined and non-zero. For $e \in m\Lambda$ the quotient $u_e(x)/u_e(y)$ is an m-th power, and for $e \in \Lambda_0$ it is 1, so Φ_x is well defined on V. For $\sigma \in G$, as x and y are rational, $\sigma(u_e(x)/u_e(y)) = (\sigma u_e)(x)/(\sigma u_e)(y) = u_{\sigma e}(x)/u_{\sigma e}(y)$, the constant in (U1) cancelling. Let $e \in \Lambda_m$, with $\operatorname{div} u_e = mD_e$, and let $\mathfrak{q} \notin S$. On the regular scheme $\mathcal{X}_\mathfrak{q}$ the divisor of u_e is $m\overline{D}_e + n\mathcal{X}_{\mathfrak{q},s}$, with $\overline{D}_e$ the closure of D_e and $n \in \mathbb{Z}$, since $\mathcal{X}_{\mathfrak{q},s}$ is irreducible. Neither $\tilde{x}$ nor $\tilde{y}$ lies in its support, so

$$v_\mathfrak{q}(u_e(x)/u_e(y)) = \deg \tilde{x}^*(\operatorname{div} u_e) - \deg \tilde{y}^*(\operatorname{div} u_e) = m(\deg \tilde{x}^*\overline{D}_e - \deg \tilde{y}^*\overline{D}_e) \in m\mathbb{Z}. \quad \square$$

For (b), let $\mathcal{X}$ be a smooth proper model of X over $\mathbb{Z}_q$, unique if the genus is positive, on which reductions are taken; let $\bar{x} \in \mathcal{X}(\mathbb{F}_q)$, and τ a parameter at $\bar{x}$ over $\mathbb{Z}_q$, so that $\widehat{\mathcal{O}}_{\mathcal{X},\bar{x}} = \mathbb{Z}_q[[\tau]]$. As $\mathfrak{q}$ has degree one, $u_e \in \mathbb{Q}_q(X)$. The prime ideals of height one of $\mathbb{Z}_q[[\tau]]$ are (q) and those generated by irreducible distinguished polynomials, and $\mathbb{Z}_q[[\tau]]$ is factorial. For $e \in \Lambda_m$ the multiplicity of each horizontal prime in $\operatorname{div} u_e$ lies in $m\mathbb{Z}$, so

$$u_e = q^c \prod_P P^{n_P} \cdot w, \qquad n_P \in m\mathbb{Z},\ w \in \mathbb{Z}_q[[\tau]]^\times,$$

with c the order of u_e along the special fiber, which does not depend on $\bar{x}$. We put $\tilde{u}_e(\bar{x}) := w(0) \bmod q$ in $\mathbb{F}_q^\times/\mathbb{F}_q^{\times m}$. Another parameter changes each P by a unit factor, which enters to a power in $m\mathbb{Z}$, so $\tilde{u}_e(\bar{x})$ is well defined. When no point of Σ reduces to $\bar{x}$, no P occurs, and $\tilde{u}_e(\bar{x})$ is the value at $\bar{x}$ of the reduction $\bar{u}_e$ of $q^{-c}u_e$. No condition on the reductions of the points of Σ is needed.

Proof of Theorem 1.3 (b). For $a \in F(S, m)$, $\chi_\mathfrak{q}(a)$ is the class of $aq^{-v_\mathfrak{q}(a)}$ modulo $\mathfrak{q}$; as $m \mid v_\mathfrak{q}(a)$, any other uniformizer in place of q gives the same class. Let x reduce to $\bar{x}$ and $t := \tau(x) \in q\mathbb{Z}_q$. Then $u_e(x) = q^c \prod_P P(t)^{n_P} w(t)$ with $\prod_P P(t)^{n_P} \in \mathbb{Q}_q^{\times m}$ and

$w(t) \equiv w(0) \bmod q$. The same holds at y with the same c, so $u_e(x)/u_e(y)$ is $w_{\bar{x}}(0)/w_{\bar{y}}(0)$ times a unit congruent to 1 modulo q times an m-th power, and its symbol is $\tilde{u}_e(\bar{x})/\tilde{u}_e(\bar{y})$. □

Remark 3.1. There is an exact sequence $0 \to \mathcal{O}_{F,S}^\times/m \to F(S,m) \to \mathrm{Cl}_S(F)[m] \to 0$, where the second map sends a to the class of the ideal $\mathfrak{a}$ with $(a) = \mathfrak{a}^m$ away from S. So $F(S,m)$ is explicit when $\#\,\mathrm{Cl}_S(F)$ is prime to m and a subgroup of $\mathcal{O}_{F,S}^\times$ of index prime to m is known.

4. Modular units at level 25

With the modular units of X, the hypotheses of Theorem 1.3 hold for $m = 5$, $F = K$ and S the prime above 5, and we determine V and $K(S,5)$, so that the theorem attaches to each rational point of X a label in $\mathrm{Hom}(V, \mathbb{F}_5)$.

For $a = (a_1, a_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ let g_a be the Siegel function, as in [33, §3.1]. On row vectors $v = (v_1, v_2) \in (\mathbb{Z}/25)^2$ put $Q(v) := v_2^2 - 2v_1^2$. Then $Q(vg) = \det(g)Q(v)$ for $g \in \mathcal{C}^\times$ and $Q(vs) = Q(v)$, so $Q(vg) = \pm\det(g)Q(v)$ for $g \in N$. For n in $I := \{1,2,3,4,6,7,8,9,11,12\}$, a set of representatives of $(\mathbb{Z}/25)^\times/\{\pm 1\}$, let O_n be the set of the 30 classes $\pm v$ with $Q(v) = \pm n$, and

$$U_n := \prod_{\pm v \in O_n} g_{v/25}, \qquad A(n) := 25 \sum_{\pm v \in O_n} \tfrac{1}{2} B_2(\{v_1/25\}),$$

with $B_2(t) = t^2 - t + \frac{1}{6}$. By [33, Proposition 6 (i), (ii)] the choice of representatives changes U_n only by a constant, and by [33, Proposition 7] U_n has order $A(n)$ at ∞ in the parameter $q^{1/25}$. A computation in PARI/GP gives

$$(A(n))_{n \in I} = (\tfrac{1}{2}, \tfrac{11}{2}, -\tfrac{9}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{11}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, -\tfrac{19}{2}),$$

all in $\frac{1}{2} + \mathbb{Z}$, of sum 0. Let $\Lambda := \{e \in \mathbb{Z}^I : 2 \mid \sum_n e_n\}$, with G acting by $(\sigma_d e)_n := e_{n/d}$. Carlucci [11] writes $t = t_1 + t_2\sqrt{\epsilon}$ and $[t] := (t_1, t_2)/p^k$, for a squarefree $\epsilon \equiv 3 \bmod 4$ that is not a square modulo p. For $\epsilon \equiv 1/2 \bmod 25$, for instance $\epsilon = -37$, his Cartan group at level 25 is $\mathcal{C}^\times$, and $t = v_1 + v_2\sqrt{\epsilon}$ has $[t] \equiv \pm v/25 \bmod \mathbb{Z}^2$ and $|t| = -Q(v)/2$. So the functions U_n are, up to constants, his $G_{n/2}^+$, and Lemma 4.1 is the case $p^k = 25$ of his results: for $p \neq 2, 3$, modulo constants, the modular units of $X_{\mathrm{ns}}^+(p^k)$ are exactly the products $\prod_h (G_h^+)^{e_h}$ with $12/\gcd(12, p+1)$ dividing $\sum_h e_h$ [11, Theorem 6.5], a condition that at $p = 5$ defines Λ. A constant multiple of each is defined over $\mathbb{Q}(\cos(2\pi/p^k))$, which is K at $p^k = 25$, and the Galois action permutes the G_h^+ up to constants [11, Remark 6.6]. He describes the group of their divisors by a Stickelberger element built from the same sums of B_2 as the numbers $A(n)$ [11, Main Theorem 7.1]. We include a proof in our notation, which gives the orders at the cusps c_d in the labeling used below.

Lemma 4.1. *For each $e \in \Lambda$ there is $u_e \in K(X)^\times$, unique up to $K^\times$, with*

$$\mathrm{ord}_{c_d} u_e = \sum_{n \in I} e_n A(n/d) \qquad (d \in I),$$

and u_e is a constant multiple of $\prod_n U_n^{e_n}$. The choices can be made so that $e \mapsto u_e$ is a homomorphism, and then $\sigma(u_e) \in K^\times u_{\sigma e}$ for $\sigma \in G$.

Proof. Let $f := \prod_n U_n^{e_n}$. We first show that $S(n) := \sum_{\pm v \in O_n} v^{\mathsf{T}} v \equiv 0 \bmod 25$, where $v^{\mathsf{T}} v$ is the matrix $(v_i v_j)$. For $g \in \mathcal{C}^\times$ of determinant 1, $v \mapsto vg$ permutes O_n, so $g^{\mathsf{T}} S(n) g = S(n)$. With $\Delta := \mathrm{diag}(-2, 1)$ one has $g^{\mathsf{T}} \Delta^{-1} g = \det(g)\Delta^{-1}$ for $g \in \mathcal{C}$, and an element of order 3 in the group of determinant-one elements of $\mathcal{C}^\times$, a cyclic group of order 30, has a one-dimensional space of invariant symmetric matrices over $\mathbb{F}_5$. As its order is prime to 5,

its invariant symmetric matrices over $\mathbb{Z}/25$ are the multiples of Δ^{-1}. So $S(n) = c\Delta^{-1}$. The matrix $s' := \left(\begin{smallmatrix} 1 & -2 \\ 1 & -1 \end{smallmatrix}\right) = (1+\xi)s \in N$ has determinant 1, permutes O_n, and satisfies $s'^{\mathsf{T}}\Delta^{-1}s' = -\Delta^{-1}$. So $S(n) = -S(n)$ and $S(n) \equiv 0$. Also f has $30\sum_n e_n \equiv 0 \bmod 12$ factors, counted with sign. By the theorem of Kubert and Lang [28, Chapter 3, Theorem 5.2], [33, Theorem 8], f is a modular unit for $\Gamma(25)$.

Let $\Gamma_X \subset \mathrm{SL}_2(\mathbb{Z})$ be the preimage of $N \cap \mathrm{SL}_2(\mathbb{Z}/25)$. For $\gamma \in \Gamma_X$, $v \mapsto v\gamma$ permutes the classes in each O_n up to sign, so $f \circ \gamma = c_e(\gamma) f$ with $c_e(\gamma) \in \mathbb{C}^\times$ [33, Proposition 6]. As f is invariant under $\Gamma(25)$, c_e is a character of $(N \cap \mathrm{SL}_2(\mathbb{Z}/25))/\{\pm 1\}$, a dihedral group of order 30, so it is trivial on the rotations, a subgroup of odd order 15. The reflection s' fixes $1+i$ in the upper half plane, and $f(1+i) \neq 0$, so $c_e(s') = 1$ and $c_e = 1$. Thus f is a function on $X_{\mathbb{C}}$ with divisor supported on the cusps. Its divisor is K-rational by Lemma 2.1, and the line bundle it defines is trivial over $\mathbb{C}$, so it has a non-zero section over K: the divisor is that of some $u_e \in K(X)^\times$, and $f \in \mathbb{C}^\times u_e$.

For the orders, $\mathrm{ord}_{c_d} f = \mathrm{ord}_{B_d\infty} f = \mathrm{ord}_\infty f \circ B_d$, and by [33, Proposition 6 (iii)] $f \circ B_d$ is a constant times $\prod_n \prod_{\pm v \in O_n} g_{vB_d/25}^{e_n}$. The first coordinate of $vB_d = vg_d^{-1}\,\mathrm{diag}(1,d)$ is that of vg_d^{-1}, and $v \mapsto vg_d^{-1}$ carries O_n onto $O_{n/d}$. So $\mathrm{ord}_{c_d} U_n = A(n/d)$ by [33, Proposition 7]. Choosing u_e on a basis of Λ gives a homomorphism. Finally $\operatorname{div} \sigma_d(u_e) = \sigma_d(\operatorname{div} u_e)$ has order $\sum_n e_n A(n/d')$ at $c_{dd'}$, which is the order of $u_{\sigma_d e}$ there; two functions over K with the same divisor differ by a factor in $K^\times$. □

A computation in PARI/GP shows that the divisor map $\Lambda \to \mathbb{Z}^I$, $e \mapsto (\mathrm{ord}_{c_d} u_e)_d$, has elementary divisors $1, 5, 5, 5, 5, 5, 5, 355, 355$ and a kernel of rank 1, spanned by $(1, \dots, 1)$ (the product of all the G_h^+ is constant, as Carlucci notes after [11, Theorem 6.5]). So in the notation of Theorem 1.3, with $m = 5$, Λ_5 has index 5 in Λ, $\Lambda_0 = \mathbb{Z}(1, \dots, 1)$, and $V := \Lambda_5/(5\Lambda + \Lambda_0)$ has dimension 8 over $\mathbb{F}_5$. At 71, the only other prime dividing these elementary divisors, V would have dimension 2.

The group $K(S, 5)$. Let $\mathfrak{p}_5$ be the prime of K above 5 and $S := \{\mathfrak{p}_5\}$. Let $\zeta := \zeta_{25}$, $\eta := (1-\zeta)(1-\zeta^{-1})$, and for a prime to 5 let $\vartheta_a := \zeta^{(1-a)/2}(1-\zeta^a)/(1-\zeta)$, a unit of K with $\vartheta_a^2 = \sigma_a(\eta)/\eta$.

Proposition 4.2. *The class number of K is prime to 5, and $K(S,5) = \mathcal{O}_{K,S}^\times/5$, a free $\mathbb{F}_5[G]$-module of rank one on η.*

Proof. The extension $K/\mathbb{Q}(\sqrt{5})$ is cyclic of degree 5, with group Γ. It is totally ramified at the prime $(\sqrt{5})$, as 5 is totally ramified in $\mathbb{Q}(\zeta_{25})$, unramified at the other finite primes, and both fields are totally real. By the ambiguous class number formula [31, Theorem 1 (1)], with one ramified place and $h(\mathbb{Q}(\sqrt{5})) = 1$, the group $\mathrm{Cl}(K)^\Gamma$ of ambiguous classes has order $1/(E : E \cap \mathrm{N}\, K^\times)$, where E is the unit group of $\mathbb{Q}(\sqrt{5})$; so it is trivial. A group of order 5 acting on a non-trivial finite 5-group has a non-trivial fixed point, so $\mathrm{Cl}(K)[5^\infty] = 0$. By Remark 3.1, $K(S,5) = \mathcal{O}_{K,S}^\times/5$.

The prime $\mathfrak{p}_5$ is (η), so $\mathcal{O}_{K,S}^\times = \mathcal{O}_K^\times \times \eta^{\mathbb{Z}}$. By [43, Lemma 8.1 (a)] the cyclotomic units of K are generated by -1 and the nine ϑ_a, $1 < a < 25/2$, $5 \nmid a$, and by [43, Theorem 8.2] they have index $h(K)$ in $\mathcal{O}_K^\times$. As $\vartheta_a^2 = \sigma_a(\eta)/\eta$, the group generated by -1 and the conjugates of η is generated by -1, η and the ϑ_a^2, of index 2^9 in the group generated by -1, η and the ϑ_a. So it has index $2^9 h(K)$ in $\mathcal{O}_{K,S}^\times$, prime to 5. As $\mathcal{O}_{K,S}^\times$ has rank $10 = |G|$, the map $\mathbb{Z}[G] \to \mathcal{O}_{K,S}^\times/\{\pm 1\}$, $x \mapsto \eta^x$, is injective, and as -1 is a fifth power it induces $\mathbb{F}_5[G] \cong \mathcal{O}_{K,S}^\times/5$. □

By Lemmas 2.1 and 4.1, (U1) holds with $F = K$, Σ the cusps and Λ, u_e as above; (U2) holds for $\mathfrak{q} \neq \mathfrak{p}_5$ with the model $\mathcal{X} \otimes \mathcal{O}_{K,\mathfrak{q}}$, whose fibers are smooth and connected. For $x \in X(\mathbb{Q})$, Theorem 1.3 and Proposition 4.2 give a G-map $\Phi_x \colon V \to \mathbb{F}_5[G]\eta$. Writing $\Phi_x(e) = \sum_{d \in I} \phi_x(\sigma_d^{-1} e)\, \sigma_d \eta$ identifies $\mathrm{Hom}_G(V, \mathbb{F}_5[G]\eta)$ with $\mathrm{Hom}(V, \mathbb{F}_5)$; we call $\phi_x \in \mathrm{Hom}(V, \mathbb{F}_5)$ the *label* of x. We fix a base point $y \in X(\mathbb{Q})$; any rational point would do, and in the computations it is the point v_{-7} of Section 5.

5. The labels and the residue discs

We read the label of a rational point off its reductions modulo primes $q \equiv 1 \bmod 25$ and prove Theorem 1.4.

Let $q \equiv 1 \bmod 25$ be prime. Then q splits completely in K, and $\mathbb{F}_q$ contains the 25-th roots of unity, which is why we use these primes: for $q \equiv -1 \bmod 25$ the group $\mathbb{F}_q^\times / \mathbb{F}_q^{\times 5}$ is trivial. Fix a prime of $\mathbb{Q}(\zeta)$ above q, let $\bar\zeta \in \mathbb{F}_q$ be the reduction of ζ and $\mathfrak{q}$ the prime of K below it. Identify $\mathbb{F}_q^\times / \mathbb{F}_q^{\times 5}$ with $\mathbb{F}_5$ by dlog, where $\mathrm{dlog}(t) = k$ if $t^{(q-1)/5} = \bar\zeta^{5k}$, and put

$$h_d := \mathrm{dlog}\big((1 - \bar\zeta^d)(1 - \bar\zeta^{-d})\big), \qquad (\Theta_q \phi)(e) := \sum_{d \in I} h_d\, \phi(\sigma_d^{-1} e),$$

for $\phi \in \mathrm{Hom}(V, \mathbb{F}_5)$. For $\bar x \in \mathcal{X}(\mathbb{F}_q)$ let $r_{\bar x} \in \mathrm{Hom}(V, \mathbb{F}_5)$ be $e \mapsto \mathrm{dlog}\big(\tilde u_e(\bar x)/\tilde u_e(\bar y)\big)$. By Theorem 1.3 (b), every $x \in X(\mathbb{Q})$ satisfies

$$\Theta_q \phi_x = r_{\bar x}. \tag{5.1}$$

The map $r_{\bar x}$ is the Tate pairing over $\mathbb{F}_q$ of $\bar x - \bar y$ with the classes $\frac{1}{5} \operatorname{div} \bar u_e$, so with 5^8 labels and about q points, heuristically a label that is not that of a rational point survives a prime with probability about $q/5^8$.

The model. We compute on the canonical model. For $v \in (\mathbb{Z}/25)^2$ not divisible by 5, Hecke's Eisenstein series e_v of weight one, defined as in [23, §5] with 121 replaced by 25, has its expansion in $\frac{1}{50}\mathbb{Z}[\zeta_{25}][[q^{1/25}]]$ and satisfies $e_v^g = e_{vg}$ for the semilinear action of $\mathcal{G}$. So, for v' also not divisible by 5 and $s \in \mathbb{Z}/25$, $\sum_{g \in N/\{\pm 1\}} \zeta_{25}^{s \det g}\, e_{vg} e_{v'g}$ is invariant under N, a form of weight 2 on X over $\mathbb{Q}$. A computation shows that forty of these span the forms of weight 2 on X, a space of dimension 23. As G permutes the cusps transitively, the combinations with constant term 0 at ∞ are cusp forms, and a basis of those with expansions in $\mathbb{Z}[\zeta_{25}][[q^{1/25}]]$ gives fourteen cusp forms of weight 2 on X, defined over $\mathbb{Q}$ and integral away from 5. They are independent modulo each of the eighteen primes $q \equiv 1 \bmod 25$ with $q \leq 2351$, so their reductions are a basis of $H^0(\mathcal{X}_{\mathbb{F}_q}, \Omega^1)$. Integrality and identities of forms of weight 2 are decided by finitely many coefficients: a form of weight 2 is a section of $\Omega^1(\text{cusps})$, of degree $2g - 2 + 10 = 36$, on X and on its reduction at each prime $\ell \neq 5$, so a form whose first 37 coefficients at ∞ vanish modulo ℓ vanishes modulo ℓ, and likewise modulo ℓ^2. These are checked on 160 coefficients, and on 60 in Section 11.

The products of the fourteen forms span a space of dimension $39 = 3g - 3$ in weight 4, so $\mathcal{X}_{\mathbb{F}_q}$ is not hyperelliptic, the forms embed it in $\mathbb{P}^{13}$, and the image lies on $66 = 105 - 39$ quadrics. By the theorem of Noether, Enriques and Petri [37, p. 157], the forms map the symmetric algebra onto the canonical ring of X, with kernel generated in degrees 2 and 3. So the cubics through X form a space of dimension $560 - 5 \cdot 13 = 495$, and as the products of the quadrics with the coordinates have rank 495 modulo 1151, they span it. Hence the quadrics generate the ideal of X and cut out X. The values of the forms at a CM point of discriminant D in the upper half plane (at $D = -3$, where every form vanishes to order at

least 2, their second derivatives) are proportional, to at least 90 digits, to an integer vector v_D that satisfies the quadrics, so $v_D \in X(\mathbb{Q})$.

An exhaustive search on the quadrics over $\mathbb{F}_q$ finds $q+1-\sum_f a_q(f)$ points, the sum over the fourteen newforms f of Proposition 10.1; by [12, Theorem 1.4] this is $\#\mathcal{X}(\mathbb{F}_q)$, so the search finds every point. Each u_e, for e in a basis of Λ_5, is a quotient of two sections of $2K_X$, found modulo q from the first coefficients of its expansion. This determines it, by Riemann–Roch: the pairs of sections with quotient u_e form a space of dimension 39 minus the degree of the poles of u_e, as that degree is at most 25, and the pairs that the coefficients allow form a space of the same dimension. Then $\tilde{u}_e(\bar{x})$ is computed at every $\bar{x} \in \mathcal{X}(\mathbb{F}_q)$ from the reductions of two such sections. Away from the cusps it is the quotient of their values, for a pair whose second section does not vanish at $\bar{x}$, and at the reduction of a cusp the quotient of their leading coefficients in a parameter there.

Proof of Theorem 1.4. The two smallest primes $q \equiv 1 \bmod 25$ are 101 and 151. A computation shows that Θ_{101} and Θ_{151} are invertible; that the 114 points of $\mathcal{X}(\mathbb{F}_{101})$ have 114 distinct values of $\Theta_{101}^{-1} r_{\bar{x}}$; that the 139 points of $\mathcal{X}(\mathbb{F}_{151})$ have 136 distinct values of $\Theta_{151}^{-1} r_{\bar{x}}$; and that exactly nine values are common to both lists, the labels ϕ_{v_D}. So by (5.1) every $x \in X(\mathbb{Q})$ has $\phi_x = \phi_{v_D}$ for some $D \in \mathcal{D}$, and at each of the eighteen primes a computation shows that the only $\bar{x} \in \mathcal{X}(\mathbb{F}_q)$ with $r_{\bar{x}} = \Theta_q \phi_{v_D}$ is $\bar{v}_D$, so $\bar{x} = \bar{v}_D$. The nine points y_D are rational and distinct modulo 1151, as their j-invariants are (Section 11), and each of the nine labels has one point in its fiber at 1151; so each of the nine labels is that of exactly one y_D, and $\bar{x}$ is the reduction of that y_D at each of the eighteen primes. □

The proof gives more: x and the same y_D have the same reduction modulo each of the eighteen primes $q \equiv 1 \bmod 25$ with $q \le 2351$.

6. Correspondences that change only the Cartan subring

For $\nu \in \mathbb{F}_5^\times$ let $R_\nu \subset \Omega \times \Omega$ be the set of pairs $((\mathbb{Z}/25)[x], (\mathbb{Z}/25)[x'])$ with $\operatorname{tr} x = \operatorname{tr} x' = 0$, $x^2 = x'^2 = 2$ and $x' = x + 5w$, where $wx \equiv -xw$ and $w^2 \equiv \nu \bmod 5$. Here w is determined modulo 5. The relation is invariant under conjugation by $\mathcal{G}$ and symmetric, as $x = x' - 5w$ and $-w$ anticommutes with x' modulo 5. Let S_ν be the correspondence $(E, R) \mapsto \sum(E, R')$ on X, the sum over the R' with $(\phi^{-1} R \phi, \phi^{-1} R' \phi) \in R_\nu$ for some ϕ. It is symmetric, defined over $\mathbb{Q}$ and, by the same moduli description, over $\mathbb{Z}[1/5]$, and it commutes with the Hecke operators T_n, $5 \nmid n$, because an isogeny of degree prime to 5 carries $E[25]$, its Cartan subrings and R_ν isomorphically. Put

$$Z_1 := S_2 - S_3, \qquad Z_2 := S_1 - S_4.$$

They are the real and imaginary parts of $\sum_\nu \bar{\chi}(\nu) S_\nu$ for a quartic character χ of $\mathbb{F}_5^\times$, whose non-zero eigenvalues on the Cartan subrings are squares of Gauss sums up to fourth roots of unity; that is what puts their eigenvalues in $\sqrt{5}\,\mathbb{Q}$, as Proposition 1.5 needs. Hypothesis (C) of Proposition 9.1 needs both here (Remark 9.2).

The fibers modulo 5. Fix x_1 with $\operatorname{tr} x_1 = 0$ and $x_1^2 = 2$, and let $\bar{x}_1$ be its reduction, $\mathbb{F}_{25} := \mathbb{F}_5[\bar{x}_1]$, and $\mathfrak{A} := \{u \in M_2(\mathbb{F}_5) : u\bar{x}_1 = -\bar{x}_1 u\}$.

Lemma 6.1. (a) $\mathfrak{A} = \mathbb{F}_{25}u_0$ *for any non-zero* $u_0 \in \mathfrak{A}$*, and* u_0 *may be chosen with* $u_0^2 = 1$*. Then* $(\gamma u_0)^2 = \mathrm{N}\,\gamma$*, and for* $a = \alpha u_0$*,* $u = \gamma u_0$ *in* $\mathfrak{A}$ *the product* $au = \alpha\bar{\gamma}$ *lies in* $\mathbb{F}_{25}$*, with* $\mathrm{tr}(au) = \mathrm{Tr}_{\mathbb{F}_{25}/\mathbb{F}_5}(\alpha\bar{\gamma})$*.*

(b) *The Cartan subrings congruent to* $\mathbb{F}_{25}$ *modulo* 5 *are the* $(\mathbb{Z}/25)[x_1 + 5u]$ *with* $u \in \mathfrak{A}$ *(lifted), and they are* 25 *distinct ones. In this parametrization* R_ν *is the relation* $u' - u \in \mathfrak{A}_\nu := \{u \in \mathfrak{A} : u^2 = \nu\}$*, a set of* 6 *elements.*

(c) *For* $a \in \mathfrak{A}$ *the function* $\psi_a(u) := \zeta_5^{\mathrm{tr}(au)}$ *on* $\mathfrak{A}$ *is an eigenfunction of the adjacency operator of* R_ν *on this fiber, with eigenvalue* 6 *if* $a = 0$ *and* $\Upsilon(a^2\nu)$ *otherwise, where* $\Upsilon(m) := \sum_{\gamma\in\mathbb{F}_{25},\ \mathrm{N}\,\gamma=m} \zeta_5^{\mathrm{Tr}\,\gamma}$*. The* 25 *functions* ψ_a *are a basis.*

Proof. (a) Conjugation by $\bar{x}_1$ is an involution of $M_2(\mathbb{F}_5)$ with fixed space $\mathbb{F}_{25}$ and (-1)-eigenspace $\mathfrak{A}$, both of dimension 2. For $u_0 \in \mathfrak{A}$ non-zero, $\mathbb{F}_{25}u_0 \subset \mathfrak{A}$ has dimension 2, and $u_0\gamma = \bar{\gamma}u_0$ for $\gamma \in \mathbb{F}_{25}$. Elements of $\mathfrak{A}$ have trace 0, so $u_0^2 = -\det u_0$ is a scalar, and it is non-zero, as one sees on $\bar{x}_1 = \xi$, $u_0 = s$. Then $(\gamma u_0)^2 = \mathrm{N}(\gamma)u_0^2$ takes every value in $\mathbb{F}_5^\times$, so we may take $u_0^2 = 1$, and $\alpha u_0 \gamma u_0 = \alpha\bar{\gamma}$. The trace of multiplication by an element of $\mathbb{F}_{25}$ on $\mathbb{F}_5^2$, a one-dimensional $\mathbb{F}_{25}$-space, is its trace to $\mathbb{F}_5$.

(b) Such a Cartan subring has a unique generator $x \equiv \bar{x}_1 \bmod 5$ with $\mathrm{tr}\,x = 0$ and $x^2 = 2$. Writing $x = x_1 + 5u$, $x^2 = 2$ means $x_1u + ux_1 \equiv 0 \bmod 5$, and then $\mathrm{tr}\,u \equiv 0$. For $x' = x + 5w$ the parameter becomes $u + w$. By (a), $\mathfrak{A}_\nu = \{\gamma u_0 : \mathrm{N}\,\gamma = \nu\}$, which has $24/4 = 6$ elements.

(c) $\sum_{w\in\mathfrak{A}_\nu} \psi_a(u + w) = \psi_a(u) \sum_{w\in\mathfrak{A}_\nu} \zeta_5^{\mathrm{tr}(aw)}$. For $a = \alpha u_0 \neq 0$ and $w = \gamma u_0$, $\beta := \alpha\bar{\gamma}$ runs over the β with $\mathrm{N}\,\beta = \mathrm{N}(\alpha)\nu = a^2\nu$, and $\mathrm{tr}(aw) = \mathrm{Tr}\,\beta$. The pairing $(a, u) \mapsto \mathrm{tr}(au)$ is non-degenerate on $\mathfrak{A}$, so the ψ_a are distinct characters. □

The fibers of Ω over the ten Cartan subrings of $M_2(\mathbb{F}_5)$ are preserved by every R_ν, so on $\mathbb{Q}[\Omega]$ the adjacency operators A_ν of the R_ν commute. Put $A_{Z_1} := A_2 - A_3$ and $A_{Z_2} := A_1 - A_4$, and let χ be the character of $\mathbb{F}_5^\times$ with $\chi(2) = i$. Then $A_{Z_2} - iA_{Z_1} = \sum_\nu \bar{\chi}(\nu)A_\nu$ is 0 on ψ_0, and on ψ_a, $a \neq 0$, it is by Lemma 6.1 (c) the scalar $\chi(a^2)\sum_{\gamma\neq 0} \bar{\chi}(\mathrm{N}\,\gamma)\zeta_5^{\mathrm{Tr}\,\gamma}$. By Hasse–Davenport [14] this sum is $-g(\bar{\chi})^2$, where g is the Gauss sum over $\mathbb{F}_5$, and $g(\bar{\chi})^2 = g(\bar{\chi}^2)\sum_x \bar{\chi}(x)\bar{\chi}(1-x) = \sqrt{5}\,(-1+2i)$, with $\sqrt{5} := \zeta_5 + \zeta_5^{-1} - \zeta_5^2 - \zeta_5^{-2}$ the quadratic Gauss sum. So $A_{Z_2} - iA_{Z_1}$ acts on ψ_a by $\chi(a^2)\sqrt{5}\,(1 - 2i)$. As A_{Z_1} and A_{Z_2} are real and symmetric, their eigenvalues on ψ_a are non-zero and lie in $\{\pm\sqrt{5}, \pm 2\sqrt{5}\}$. So the minimal polynomial $P_Z \in \mathbb{Q}[t]$ of A_Z has distinct roots, all in $\sqrt{5}\,\mathbb{Q}$.

From the Cartan subrings to cohomology. Section 7 needs two facts about $H := H^1_{\text{ét}}(X_{\bar{\mathbb{Q}}}, \bar{\mathbb{Q}}_\ell)$: the eigenvalues of Z_1 and Z_2 on H lie in $\sqrt{5}\,\mathbb{Q}$, which makes their traces vanish, and the scalar $z(\pi)$ by which they act on the part $\sigma(\pi)$ of H attached to an automorphic representation π depends only on $\pi_5|_{\mathrm{GL}_2(\mathbb{Z}_5)}$, which Lemma 7.2 and Corollary 7.3 use. Both come from the action on the Cartan subrings.

Let k be a field of characteristic 0. For a $\mathcal{G}$-stable subset $R \subset \Omega \times \Omega$ let A_R be its adjacency operator on $k[\Omega]$, $\mathcal{C}' \mapsto \sum_{(\mathcal{C}',\mathcal{C}'')\in R} \mathcal{C}''$, and $D_R := \{g \in \mathcal{G} : (\mathcal{C}, g\mathcal{C}g^{-1}) \in R\}$, a union of double cosets of N.

Lemma 6.2. *For a* $k[\mathcal{G}]$*-module* W*,* $w \mapsto (g\mathcal{C}g^{-1} \mapsto gw)$ *is an isomorphism* $W^N \to \mathrm{Hom}_{\mathcal{G}}(k[\Omega], W)$*, with inverse* $\Psi \mapsto \Psi(\mathcal{C})$*. Under it,* $\Psi \mapsto \Psi \circ A_R$ *corresponds to* $w \mapsto \sum_{hN\subset D_R} hw$*.*

Proof. The map is well defined on W^N, as N is the stabilizer of $\mathcal{C}$, and $\mathcal{G}$-equivariance gives the inverse. Then $(\Psi \circ A_R)(\mathcal{C}) = \sum_{(\mathcal{C},\mathcal{C}'')\in R} \Psi(\mathcal{C}'') = \sum_{hN\subset D_R} hw$. □

Let $H(\cdot) := H^1_{\text{ét}}(\cdot_{\bar{\mathbb{Q}}}, \bar{\mathbb{Q}}_\ell)$ for a prime ℓ, let $\mathrm{pr}\colon Y \to X$ be the quotient map, and let $\mathcal{G}$ act on $H(Y)$ on the left by $g \cdot v := r_g^* v$. Write S_R for the correspondence of R on X, so that $S_\nu = S_{R_\nu}$, and S_R^* for its action on $H(X)$.

Lemma 6.3. *The map* pr^* *is an isomorphism* $H(X) \to H(Y)^N$*, and* $\mathrm{pr}^* S_R^* v = \sum_{hN \subset D_R} h \cdot \mathrm{pr}^* v$.

Proof. The group $N/\{\pm 1\}$ acts faithfully on Y with quotient X, as $(E,\phi) \cong (E,-\phi)$, so pr^* is an isomorphism onto the invariants and $\mathrm{pr}^*\mathrm{pr}_* = \sum_{n \in N/\{\pm1\}} r_n^*$. For $g \in D_R$, the map $(\mathrm{pr}, \mathrm{pr} \circ r_g)\colon Y \to X \times X$ sends (E,ϕ) to $\big((E,\phi\mathcal{C}\phi^{-1}),(E,\phi g\mathcal{C}g^{-1}\phi^{-1})\big)$. Its image S_g depends only on NgN, it has degree $|N \cap gNg^{-1}|/2$ onto S_g, since (E,ϕ) and $(E,\phi n)$ have the same image exactly when $n \in N \cap gNg^{-1}$, and $S_R = \sum S_g$ over representatives g of the double cosets in D_R. So $S_g^* = \frac{2}{|N \cap gNg^{-1}|}\mathrm{pr}_* r_g^* \mathrm{pr}^*$, and as $r_n^* r_g^* = (ng)\cdot$,

$$\mathrm{pr}^* S_g^* v = \frac{1}{|N \cap gNg^{-1}|} \sum_{n \in N} (ng) \cdot \mathrm{pr}^* v = \sum_{hN \subset NgN} h \cdot \mathrm{pr}^* v,$$

because $ngN = n'gN$ if and only if $n^{-1}n' \in N \cap gNg^{-1}$. □

By Lemmas 6.2 and 6.3, $\mathrm{pr}^* Z^* = \rho(A_Z)\mathrm{pr}^*$ on $H(X)$ for $Z \in \{Z_1, Z_2\}$, where $\rho(A)$ is $\Psi \mapsto \Psi \circ A$ on $\mathrm{Hom}_{\mathcal{G}}(\bar{\mathbb{Q}}_\ell[\Omega], H(Y)) = H(Y)^N$. As $A \mapsto \rho(A)$ reverses products and $\bar{\mathbb{Q}}_\ell[A_Z]$ is commutative, $P_Z(Z^*) = 0$ on $H(X)$.

Proposition 6.4. *Let* $Z \in \{Z_1, Z_2\}$ *and* $H := H^1_{\acute{e}t}(X_{\bar{\mathbb{Q}}}, \bar{\mathbb{Q}}_\ell)$.

(a) *Z acts semisimply and injectively on H with eigenvalues in $\sqrt{5}\,\mathbb{Q}$, and* $\mathrm{Tr}(Z \mid H) = 0$.

(b) $H = \bigoplus_{\pi \in P} \sigma(\pi)$ *for a set P of fourteen cuspidal automorphic representations π of* $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ *of weight 2 whose central characters are trivial on $\mathbb{Z}_5^\times$, where $\sigma(\pi)$ is the two-dimensional ℓ-adic representation attached to π. The correspondence Z acts on $\sigma(\pi)$ by a scalar $z(\pi) \in \sqrt{5}\,\mathbb{Q}$ that depends only on the restriction of the local component π_5 to* $\mathrm{GL}_2(\mathbb{Z}_5)$.

Proof. (a) $P_Z(Z) = 0$ with P_Z as above. As A_Z is 0 on ψ_0 and has non-zero eigenvalues on the ψ_a, $a \neq 0$, the kernel of A_Z on $\bar{\mathbb{Q}}_\ell[\Omega]$ consists of the functions constant on the fibers over the Cartan subrings of $M_2(\mathbb{F}_5)$. If Z kills $v \in H(X)$, the Ψ corresponding to $w := \mathrm{pr}^* v$ (Lemmas 6.2 and 6.3) vanishes on the image of A_Z, which contains $\mathcal{C}' - \mathcal{C}''$ whenever $\mathcal{C}' \equiv \mathcal{C}''$ mod 5 (as A_Z is symmetric, its image is the orthogonal of its kernel). So $w = \Psi(\mathcal{C})$ is invariant under the preimage N' of $N_{\mathrm{ns}}(5)$ in $\mathcal{G}$, the stabilizer of $\mathcal{C}$ modulo 5, and as in Lemma 6.3, $H(Y)^{N'}$ is the pull-back of $H(X^+_{\mathrm{ns}}(5))$, which is 0 as $X^+_{\mathrm{ns}}(5)$ has genus 0. Hence $w = 0$, so $v = 0$, and Z is injective on H. The trace is an integer, since Z acts on $H^1(X(\mathbb{C}), \mathbb{Z})$, and it lies in $\sqrt{5}\,\mathbb{Q}$, so it is 0.

(b) Let $\mathcal{K}(25) := \ker(\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathcal{G})$. By [10, §2.3, p. 421] (see [30] for $\mathbb{Q}$), there is an isomorphism of $\mathcal{G} \times \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules

$$H(Y) \cong \bigoplus_\pi V_\pi^\theta \otimes \sigma(\pi), \qquad V_\pi := \pi_{\mathrm{fin}}^{\mathcal{K}(25)},$$

over the cuspidal automorphic representations π of GL_2 of weight 2, where V^θ denotes V with $\mathcal{G}$ acting through an automorphism θ of $\mathcal{G}$ that depends only on the conventions for the two actions; nothing below depends on θ. As a $\mathcal{G}$-module, V_π is 0 unless π is unramified outside 5, and then it is $\pi_5^{\ker(\mathrm{GL}_2(\mathbb{Z}_5) \to \mathcal{G})}$ tensored with lines, so it depends only on $\pi_5|_{\mathrm{GL}_2(\mathbb{Z}_5)}$. Taking N-invariants, $H(X) \cong \bigoplus_\pi (V_\pi^\theta)^N \otimes \sigma(\pi)$. By Chen's isogeny [12, Theorem 1.4] (proof

of Lemma 7.1), H is the sum of the irreducible representations $\sigma(f)$ over the fourteen newforms f of level 625 with trivial character and Fricke eigenvalue $+1$, and these are pairwise non-isomorphic by strong multiplicity one. Hence $(V_\pi^\theta)^N$ has dimension at most 1 for every π; let P be the fourteen π for which it is a line. The center of $\mathcal{G}$ lies in N, is preserved by θ, and acts on V_π through the central character of π_5, so that character is trivial on $\mathbb{Z}_5^\times$ for $\pi \in P$. By Lemmas 6.2 and 6.3, Z acts on $(V_\pi^\theta)^N \otimes \sigma(\pi) = \mathrm{Hom}_{\mathcal{G}}(\bar{\mathbb{Q}}_\ell[\Omega], V_\pi^\theta) \otimes \sigma(\pi)$ through $\rho(A_Z)$ on the first factor, a line, so by a scalar $z(\pi)$ that depends only on the $\mathcal{G}$-module V_π^θ. It lies in $\sqrt{5}\,\mathbb{Q}$ by (a). □

Fixed points. For $\mu \in \mathbb{F}_5^\times$, the six Cartan subrings S_μ-related to that of y_{-3} form two orbits of size three under the automorphism of order 3 of E_{-3} (see the proof below), so $S_\mu(y_{-3}) = 3Q_\mu + 3Q'_\mu$ with $Q_\mu \neq Q'_\mu$ over $j = 0$. For $\nu \in \{1, 4\}$ let Φ_ν be the sum of the ten points over $j = 1728$ described in (c) below.

Proposition 6.5. (a) $\mathrm{Fix}\, S_\nu$ *has no point over* $j \neq 0, 1728, \infty$.

(b) *Over* $j = 0$, $\mathrm{Fix}\, S_\nu = 2Q_{2\nu} + 2Q'_{2\nu}$.

(c) *Over* $j = 1728$, $\mathrm{Fix}\, S_\nu = 0$ *for* $\nu = 2, 3$, *and* $\mathrm{Fix}\, S_\nu = \Phi_\nu$, *ten distinct points of multiplicity one, for* $\nu = 1, 4$.

(d) *Each cusp has multiplicity* 2 *in* $\mathrm{Fix}\, S_1$ *and* $\mathrm{Fix}\, S_4$, *and* 0 *in* $\mathrm{Fix}\, S_2$ *and* $\mathrm{Fix}\, S_3$.

Hence $\mathrm{Fix}\, Z_1 = 2(Q_4 + Q'_4 - Q_1 - Q'_1)$ *and* $\mathrm{Fix}\, Z_2 = 2(Q_2 + Q'_2 - Q_3 - Q'_3) + \Phi_1 - \Phi_4$. *The same holds over* $\bar{\mathbb{F}}_q$ *for every prime* $q \geq 7$, *for the reductions of these points.*

Proof. A point (E, R) is fixed when some $R' = \alpha R \alpha^{-1}$ with $\alpha \in \mathrm{Aut}(E)$ is S_ν-related to R; as $(R, R) \notin R_\nu$, $\alpha \neq \pm 1$. This gives (a). As $\mathrm{Aut}(E)/\{\pm 1\}$ has order 2 or 3 and $\alpha R \alpha^{-1} \neq R$, only ± 1 fixes R, so a parameter t of X at (E, R) is a parameter of the stack. Each such α, up to sign, gives a branch of S_ν through $((E, R), (E, R))$ which, in t, is the graph of $t \mapsto \epsilon t$ with $\epsilon \neq 1$ the root of unity by which α acts on the tangent space of the stack; it meets the diagonal with multiplicity one.

(b) Let $\omega \in \mathrm{Aut}(E_{-3})$ have order 3, and let $R_0 = (\mathbb{Z}/25)[\omega]$, the Cartan subring of y_{-3}, generated by x_0. If $\omega R \omega^{-1}$ is S_ν-related to R, then ω normalizes R modulo 5, and an element of order 3 of the normalizer of a non-split Cartan subring of $M_2(\mathbb{F}_5)$ lies in it; so $R \equiv R_0 \bmod 5$, and R is generated by $x = x_0 + 5\tilde{w}$ with $\tilde{w}$ anticommuting with x_0 modulo 5. Then $\omega \tilde{w} \omega^{-1} = \omega \bar{\omega}^{-1} \tilde{w} = \omega^2 \tilde{w}$ modulo 5, so $\omega x \omega^{-1} = x + 5(\omega^2 - 1)\tilde{w}$, and $((\omega^2 - 1)\tilde{w})^2 = \mathrm{N}(\omega^2 - 1)\tilde{w}^2 = 3\tilde{w}^2$. So the condition is $\tilde{w}^2 = \nu/3 = 2\nu$, which describes $S_{2\nu}(R_0)$. The map $\tilde{w} \mapsto \omega^2 \tilde{w}$ has no non-zero fixed point, so these six subrings give the two points $Q_{2\nu}$, $Q'_{2\nu}$, each with the two branches of ω and ω^2.

(c) Let $\iota \in \mathrm{Aut}(E_{1728})$ have order 4, and write a generator as $x = a_0 \iota + w$ with w anticommuting with ι. Then $\iota x \iota^{-1} = a_0 \iota - w$. It is congruent to x modulo 5 only if $w \equiv 0$, which would give $x^2 \equiv -a_0^2 \equiv 2$, impossible; so the generator of $\iota R \iota^{-1}$ congruent to x is $-\iota x \iota^{-1}$, which needs $a_0 = 5a'$, and then $-\iota x \iota^{-1} = x + 5(-2a'\iota)$ with $(-2a'\iota)^2 = -4a'^2 = a'^2$. So $\nu = a'^2$ with $a' \not\equiv 0$, which excludes $\nu = 2, 3$. For $\nu \in \{1, 4\}$ the subrings $(\mathbb{Z}/25)[5a'\iota + w]$ with $a'^2 = \nu$ and $w^2 = 2$ are twenty, and ι pairs them into ten points, each with the single branch of ι.

(d) Near a cusp, X is described by the Tate curve with parameter t, t^{25} the Tate parameter, and $u := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ acts on level structures as $t \mapsto \zeta_{25} t$. So the branches of S_ν through (cusp, cusp) come from the $m \not\equiv 0 \bmod 25$ with $(R, u^m R u^{-m}) \in R_\nu$. Let $x = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ generate R; then $5 \nmid c$, as $\bar{x}$ has no eigenvector. With $n := u - 1$, $u^m x u^{-m} = x + m(nx - xn) - m^2 c\, n$, and $nx - xn$ has diagonal $(c, -c)$, so $u^m x u^{-m} \equiv x \bmod 5$ forces $m = 5m'$; congruence to

$-x$ is excluded by the lower left entry. Then $u^m x u^{-m} = x + 5m'(nx - xn)$, where $nx - xn$ anticommutes with x and has square c^2. So $\nu = (m'c)^2$: there is no solution for $\nu = 2, 3$ and two values of m' for $\nu = 1, 4$, with branches $t \mapsto \zeta_5^{\pm m'} t$.

The same arguments apply over $\bar{\mathbb{F}}_q$, $q \geq 7$, where the automorphism groups at $j = 0$, 1728 and elsewhere are the same and the Tate curve describes the cusps. □

7. The term at 5

We prove Proposition 1.5 and show that its hypotheses hold for X over $\mathbb{Q}_5$ and the correspondences Z_1 and Z_2 (Corollary 7.3).

Proof of Proposition 1.5. Let d be the degree of $C(y)$, and write Z also for the action of the endomorphism on H. By the Lefschetz fixed point formula, $\deg \operatorname{Fix} C = 2d - \operatorname{Tr}(Z \mid H)$. This trace is an integer, since the characteristic polynomial of an endomorphism of J has integer coefficients and is its characteristic polynomial on the Tate module [35, Theorem 10.9, Proposition 10.20]. It also lies in $\mathbb{Q}\alpha$, and $\mathbb{Q} \cap \mathbb{Q}\alpha = 0$ as $\alpha \notin \mathbb{Q}$. So $\operatorname{Tr}(Z \mid H) = 0$, and $D := \operatorname{Fix} C - C(y) - C(z)$ has degree 0. As C is symmetric, transposition permutes the C_i, so by the hypotheses on y and z neither lies on $\operatorname{Fix} C_i$, $C_i(y)$ or $C_i(z)$ for any i, and neither lies in the support of D.

The reduction graph. Let K_0 be the completion of the maximal unramified extension of $\mathbb{Q}_p$, with inertia group $I = \operatorname{Gal}(\bar{K}_0/K_0)$. By [15, Corollary (2.7)] there is a finite Galois extension L of K_0 over which X has a stable model $\mathcal{X}_L$, and we take L so large that J has good reduction over L. By a theorem of Raynaud [15, Theorem (2.5)], the identity component of the special fiber of the Néron model of J_L is Pic^0 of the special fiber of the minimal regular model of X_L, which is that of $\mathcal{X}_L$ with each node replaced by a chain of rational curves [15, proof of Lemma (1.12)]. As for any nodal curve, this Pic^0 is an extension of $\prod_v \operatorname{Jac}(C_v)$ by a torus of dimension $b_1(\Gamma)$. Here Γ is the dual graph of the special fiber, v runs over its vertices and C_v is the normalization of the component v. Good reduction leaves no torus, so Γ is a tree and J reduces to $\bar{J} = \prod_v \operatorname{Jac}(C_v)$. This decomposes $H = \bigoplus_v H(v)$ with $H(v) := H^1_{\text{ét}}(C_v, \bar{\mathbb{Q}}_\ell)$, and we let e_v be the projection onto $H(v)$. The group I acts on H through its finite quotient $\operatorname{Gal}(L/K_0)$. For σ in this quotient, the conjugate of $\mathcal{X}_L$ by σ is a stable model of the same curve, so by [15, Lemma (1.12)] the action of σ on X_L extends to $\mathcal{X}_L$. Hence I acts on Γ, and $\sigma H(v) = H(\sigma v)$.

The formula of Betts and Dogra. The endomorphism Z is fixed by the Rosati involution, as C is symmetric, and has trace 0. By [7, Remark 12.1.4], the function $z \mapsto i_p(z - y, \operatorname{Fix} C - C(y) - C(z))$ is a non-zero constant multiple of the coordinate j_C of the unipotent Kummer map with base point y. By [7, Theorem 1.1.2, Corollary 12.1.3] (in the form of [3, Theorem 3.2]), in the case of a tree [7, §12.2.1],

$$j_C(z) = \langle \operatorname{red}(z) - \operatorname{red}(y), \mu \rangle, \qquad \mu = \frac{1}{2} \sum_v \operatorname{Tr}(e_v Z e_v \mid H(v))\, v,$$

where $\operatorname{red}\colon X(\mathbb{Q}_p) \to \Gamma$ is the reduction map and $\langle\,,\rangle$ is the height pairing on the metrized graph Γ.

Each mass vanishes. Write $\mu = \sum_v \mu_v v$. Let O be an orbit of I on the vertices of Γ, and $H_O := \bigoplus_{v \in O} H(v)$. It is stable under I. As I acts on H semisimply, H_O is the sum of its intersections with the isotypic components of H under I, and Z acts on each of these by a scalar in $\mathbb{Q}\alpha$. Hence Z preserves H_O, and

$$2 \sum_{v \in O} \mu_v = \sum_{v \in O} \operatorname{Tr}(e_v Z e_v \mid H(v)) = \operatorname{Tr}(Z \mid H_O) \in \mathbb{Q}\alpha.$$

On the other hand, $\mathrm{Tr}(Z \mid H_O)$ is the trace on H^1 of an endomorphism of the abelian variety $\prod_{v\in O} \mathrm{Jac}(C_v)$, namely the reduction of Z on $\bar{J}$ restricted to this factor and projected back onto it, so it is an integer [35, Theorem 10.9, Proposition 10.20], and therefore 0. As Z commutes with I (C is defined over $\mathbb{Q}_p$) and $\sigma e_v \sigma^{-1} = e_{\sigma v}$, the masses μ_v are constant on O, so each is 0. Hence $\mu = 0$, so $j_C(z) = 0$ and $i_p(z - y, D) = 0$. □

Lemma 7.1. *The Jacobian J has potentially good reduction at 5.*

Proof. By Chen [12, Theorem 1.4], J is isogenous over $\mathbb{Q}$ to the new quotient of the Jacobian of $X_0^+(625)$, as $X_0^+(25)$ has genus 0. So its Tate module is a sum of the ℓ-adic representations of the newforms of weight 2 and level 625 with trivial character and Fricke eigenvalue $+1$. The local component at 5 of such a newform is not a twist $\mathrm{St} \otimes \chi$ of the Steinberg representation: its central character χ^2 would be trivial, and then its conductor would be 5 or 5^2. So these representations have no monodromy at 5 [10, Théorème (A)], inertia at 5 acts on them through a finite quotient, and J has potentially good reduction [41, §2, Theorem 2(i)]. □

Lemma 7.2. *Let $\pi, \pi' \in P$ (Proposition 6.4) and let I be the inertia group at 5. If $\sigma(\pi)|_I$ and $\sigma(\pi')|_I$ have a common irreducible constituent, then π_5 and π'_5 have isomorphic restrictions to $\mathrm{GL}_2(\mathbb{Z}_5)$.*

Proof. Let W_5 be the Weil group of $\mathbb{Q}_5$, and $\sigma(\pi_5)$ the representation of the Weil–Deligne group of $\mathbb{Q}_5$ attached to π_5 by the correspondence normalized as in [10, (0.5)]. By Carayol's theorem [10, Théorème (A)] it is the Weil–Deligne representation of $\sigma(\pi)$ restricted to a decomposition group at 5. As $\sigma(\pi) \subset H$, inertia acts on it through a finite quotient (Lemma 7.1), so $\sigma(\pi_5)$ has monodromy 0 and $\sigma(\pi_5)|_I = \sigma(\pi)|_I$ is semisimple. The same holds for π', so $\mathrm{Hom}_I(\sigma(\pi_5), \sigma(\pi'_5)) \neq 0$. A Frobenius element $\Phi \in W_5$ acts on this space by $\phi \mapsto \sigma(\pi'_5)(\Phi) \circ \phi \circ \sigma(\pi_5)(\Phi)^{-1}$, and an eigenvector ϕ, with eigenvalue c, is a non-zero W_5-map $\sigma(\pi_5) \otimes \mu \to \sigma(\pi'_5)$, where μ is the unramified character with $\mu(\Phi) = c$.

If $\sigma(\pi_5)$ or $\sigma(\pi'_5)$ is irreducible, ϕ is an isomorphism, and $\sigma(\pi'_5) \cong \sigma(\pi_5) \otimes \mu = \sigma(\pi_5 \otimes \mu^{-1})$ by [10, (0.5) (b)], where $\pi_5 \otimes \mu^{-1}$ means $\pi_5 \otimes (\mu^{-1} \circ \det)$. The correspondence [29] is injective by the local converse theorem of Jacquet and Langlands [21, Corollary 2.19], so $\pi'_5 \cong \pi_5 \otimes (\mu^{-1} \circ \det)$, and $\mu \circ \det$ is trivial on $\mathrm{GL}_2(\mathbb{Z}_5)$.

Otherwise both are reducible. As the monodromy is 0, neither π_5 nor π'_5 is a twist of the Steinberg representation, and as $\sigma(\pi_5)$ is reducible, π_5 is not supercuspidal. So $\pi_5 = \mathrm{Ind}(\xi_1, \xi_2)$ and $\pi'_5 = \mathrm{Ind}(\xi'_1, \xi'_2)$ are irreducible principal series, and $\sigma(\pi_5) = \xi_1^{-1}\lambda \oplus \xi_2^{-1}\lambda$ with λ unramified [10, (0.5)], and likewise for π'_5. Through local class field theory, a common constituent gives, after renumbering, $\xi'_1 = \xi_1$ on $\mathbb{Z}_5^\times$. The central characters $\xi_1\xi_2$ and $\xi'_1\xi'_2$ are trivial on $\mathbb{Z}_5^\times$ (Proposition 6.4), so also $\xi'_2 = \xi_2$ on $\mathbb{Z}_5^\times$. By the Iwasawa decomposition $\mathrm{GL}_2(\mathbb{Q}_5) = B(\mathbb{Q}_5)\,\mathrm{GL}_2(\mathbb{Z}_5)$, with B the upper triangular subgroup, the restriction of $\mathrm{Ind}(\xi_1, \xi_2)$ to $\mathrm{GL}_2(\mathbb{Z}_5)$ is induced from the character $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \mapsto \xi_1(a)\xi_2(d)$ of $B(\mathbb{Z}_5)$, so it depends only on ξ_1 and ξ_2 on $\mathbb{Z}_5^\times$. □

Corollary 7.3. *Let $Z = S_\nu - S_{4\nu} \in \{Z_1, Z_2\}$, and let $y, z \in X(\mathbb{Q}_5)$ be such that none of (y, y), (z, z), (y, z) lies on S_ν or $S_{4\nu}$. Then $i_5(z - y, \mathrm{Fix}\, Z - Z(y) - Z(z)) = 0$.*

Proof. The correspondence Z is symmetric, and its components lie on S_ν or $S_{4\nu}$, none of them the diagonal, as R_ν is symmetric and contains no pair (R, R). It is non-zero, being injective on H by Proposition 6.4 (a), and J has potentially good reduction at 5 by Lemma 7.1. By Proposition 6.4 (b), $H = \bigoplus_{\pi\in P} \sigma(\pi)$, with Z acting on $\sigma(\pi)$ by $z(\pi) \in \sqrt{5}\,\mathbb{Q}$, and each $\sigma(\pi)|_I$ is semisimple. The isotypic component of an irreducible representation

τ of I is the sum of the τ-isotypic parts of the $\sigma(\pi)$ that contain τ, and by Lemma 7.2 and Proposition 6.4 (b) all these π have the same $z(\pi)$. So Proposition 1.5 applies with $\alpha = \sqrt{5}$. □

8. Heights at the auxiliary prime

The argument of this section and the next works on any modular curve, and we state it in that generality. Let $\mathcal{H} \subset \mathrm{GL}_2(\mathbb{Z}/N_X)$ contain the scalars, with $\det \mathcal{H} = (\mathbb{Z}/N_X)^\times$, let $X = X_{\mathcal{H}}$ have genus $g \geq 2$ and Jacobian J, and let $\mathbb{T} \subset \mathrm{End}\, J$ be generated by the Hecke operators T_n, n prime to N_X. Let $q \geq 5$ be a prime not dividing N_X, let $\mathcal{X}$ be the smooth model of X over $\mathbb{Z}_q$ [16, VI, Proposition 6.7], and put

$$\mathcal{L} := H^0(\mathcal{X}, \Omega^1), \quad \mathrm{Lie} := \mathrm{Hom}(\mathcal{L}, \mathbb{Z}_q), \quad \mathbb{T}_q := \mathbb{T} \otimes \mathbb{Z}_q, \quad M := J(\mathbb{Q}) \otimes \mathbb{Z}_q, \quad N_q := \#\bar{J}(\mathbb{F}_q).$$

We assume

(B) $q \nmid N_q$;
(M) Lie is free of rank one over $\mathbb{T}_q$.

These are the hypotheses (B) and (M) of [23, Theorem 1.2], with its prime p replaced by q, and we use [23, §§2–3] in that form. None of the results we use there needs its other hypothesis (Φ), which gives the integrality of the height pairing [23, Proposition 2.9]; here integrality comes from the control equations instead (Proposition 9.1 (a)). By (M), $\mathcal{L}$ has a $\mathbb{T}_q$-stable complement W in $H^1_{\mathrm{dR}}(\mathcal{X}/\mathbb{Z}_q)$, and W is isotropic [23, Lemma 2.1]. For a divisor b of degree 0 over a finite extension L of $\mathbb{Q}_q$, let ω_b be the form of the third kind over L with residue divisor b and class in $W \otimes L$ [23, §2], and let $h = \sum_v h_v$ be the height of Coleman and Gross [13] for W, with

$$h_q(a,b) := \int_a \omega_b, \qquad h_v(a,b) := -i_v(a,b) \log_q v \quad (v \neq q)$$

for divisors a, b of degree 0 with disjoint supports, and $\log_q q = 0$. We never need W explicitly: modulo q^2, the values of h_q that enter are given by Lemma 8.1 through values of functions. The local term h_q is symmetric, as W is isotropic, and $\mathbb{T}$ acts on M by self-adjoint operators for h [23, Lemma 2.2], as in [4, Lemma 2.13]. By (B), M is torsion-free and $\log M \subset q\,\mathrm{Lie}$, so

$$\kappa := q^{-1} \log \colon M \to \mathrm{Lie}$$

is defined. A symmetric integer combination Z of double cosets $\mathcal{H}\gamma\mathcal{H}$ commutes with $\mathbb{T}$, so by (M) it acts on M and on Lie through an element of $\mathbb{T}_q$, and it is self-adjoint for h [23, §3].

A residue disc is a fiber of the reduction map $X(\mathbb{C}_q) \to \mathcal{X}(\bar{\mathbb{F}}_q)$. For a residue point $\bar{x}$ rational over $\mathbb{F}_{q^f}$, let O be the ring of Witt vectors of $\mathbb{F}_{q^f}$; an integral parameter at $\bar{x}$ is a function τ with $\widehat{\mathcal{O}}_{\mathcal{X}_O,\bar{x}} = O[[\tau]]$. For a $\mathbb{Q}_q$-rational divisor D of degree 0, (B) gives a function $\bar{f}_D$ on $\mathcal{X}_{\mathbb{F}_q}$ with divisor $N_q\bar{D}$, and it lifts to a function f_D over $\mathbb{Q}_q$ whose zeros and poles lie in the residue discs of the points of D and for which $D_1 := N_q D - \mathrm{div}\, f_D$ has degree 0 on every residue disc [23, proof of Lemma 2.8]. We fix such an f_D. For a divisor $A = \sum n_P P$ at whose points a function f is a unit, $\log f(A) := \sum n_P \log f(P)$.

Lemma 8.1. *Assume* (B), *and let D be a $\mathbb{Q}_q$-rational divisor of degree* 0.

(a) *On a residue disc that contains no point of D, with integral parameter τ, $\omega_D \in O[[\tau]]\,d\tau$ and $\omega_D \equiv N_q^{-1}\, df_D/f_D$ modulo q.*
(b) *If D is rational over $\mathbb{Q}$, then $\langle \kappa[D], \omega \rangle = (qN_q)^{-1} \int_{D_1} \omega$ for $\omega \in \mathcal{L}$, and $\int_{D_1} \omega$ is a sum of integrals over residue discs, each in qO.*

(c) *Let $y, y' \in X(\mathbb{Q}_q)$ lie in residue discs that contain no point of D, and put $A := y' - y$. Then $N_q h_q(A, D) \in q\mathbb{Z}_q$ and*

$$N_q h_q(A, D) \equiv \log f_D(A) + N_q^{-1} \log f_A(D_1) \pmod{q^2}.$$

Proof. (a) By the proof of [23, Lemma 2.8], $N_q \omega_D = \omega_{D_1} + df_D/f_D$. The divisor D_1 lies in the residue discs of the points of D, so ω_{D_1} is q times an integral form on the disc [23, Proposition 2.6 (a)], and f_D is a unit there.

(b) As $[\operatorname{div} f_D] = 0$, $N_q[D] = [D_1]$, and $\langle \log[D_1], \omega \rangle = \int_{D_1} \omega$. As D_1 has degree 0 on every disc, this is the sum over the discs of the integrals of ω over the part of D_1 in the disc, and each lies in qO by [23, Lemma 2.3], as ω is integral.

(c) By (a), $N_q h_q(A, D) = \int_A \omega_{D_1} + \log f_D(A)$, and $\log f_D(A)$ is the logarithm of a unit of $\mathbb{Z}_q$, so it lies in $q\mathbb{Z}_q$. As h_q is symmetric, $\int_A \omega_{D_1} = h_q(A, D_1) = \int_{D_1} \omega_A$. On the discs of the points of D, which contain no point of A, (a) gives $\omega_A \equiv N_q^{-1} df_A/f_A$ modulo q, with both forms integral. As D_1 has degree 0 on each of these discs, [23, Lemma 2.3] gives $\int_{D_1} \omega_A \in q\mathbb{Z}_q$ and $\int_{D_1} \omega_A \equiv N_q^{-1} \int_{D_1} df_A/f_A = N_q^{-1} \log f_A(D_1)$ modulo q^2. □

9. Control equations and the disc of a known point

We keep the setting of Section 8 and assume (B) and (M). Let $y_1, \dots, y_n \in X(\mathbb{Q})$, and let $\mathcal{Z}$ be a finite set of correspondences Z on X, each a symmetric integer combination of double cosets $\mathcal{H}\gamma\mathcal{H}$ with $\gamma \notin \mathcal{H}$, with $\operatorname{Tr}(Z \mid \mathcal{L}) = 0$, and such that:

(F) for all i, j, the closure of each term of Z in $\mathcal{X} \times \mathcal{X}$ does not contain $(\bar{y}_i, \bar{y}_j)$;

(V) at each prime $v \mid N_X$, $i_v(z - y, \operatorname{Fix} Z - Z(y) - Z(z)) = 0$ for all $y, z \in X(\mathbb{Q})$ whose reductions modulo q lie in $\{\bar{y}_1, \dots, \bar{y}_n\}$.

For $Z \in \mathcal{Z}$ and $i < j$, $B_{ij}^Z := \operatorname{Fix} Z - Z(y_i) - Z(y_j)$ is a rational divisor of degree 0. Fix a generator e of Lie over $\mathbb{T}_q$, and define $a_{ij}, b_{ij}^Z \in \mathbb{T}_q$ by

$$\kappa[y_j - y_i] = a_{ij}\, e, \qquad \kappa[B_{ij}^Z] = b_{ij}^Z\, e.$$

For each Z and $i < j$, the height identity for $y_j - y_i$ and B_{ij}^Z is a linear equation on the height pairing, with right side $q^{-1} h_q(y_j - y_i, B_{ij}^Z)$ (proof of (a) below); we call these the control equations. As B_{ij}^Z is symmetric in i and j, the pairs with $i > j$ give nothing new.

Proposition 9.1. *In this setting, assume also:*

(R) $\operatorname{rank} J(\mathbb{Q}) \le g$;

(C) the products $a_{ij} b_{ij}^Z$, for $Z \in \mathcal{Z}$ and $i < j$, span $\mathbb{T}_q/q$ over $\mathbb{F}_q$.

Then:

(a) *The map $\kappa\colon M \to \operatorname{Lie}$ is an isomorphism, and $h(M, M) \subset q\mathbb{Z}_q$. There is a unique linear map $\bar{\lambda}\colon \mathbb{T}_q/q \to \mathbb{F}_q$ with $\bar{\lambda}(a_{ij} b_{ij}^Z) = q^{-1} h_q(y_j - y_i, B_{ij}^Z) \bmod q$ for all Z and $i < j$, and the form $\tilde{b}$ on Lie/q with $\tilde{b}(\kappa a, \kappa a') \equiv q^{-1} h(a, a') \bmod q$ is $\tilde{b}(te, t'e) = \bar{\lambda}(tt')$.*

(b) *Let $y := y_i$, let $\delta \ne 0$ be a tangent vector to $\mathcal{X}_{\mathbb{F}_q}$ at $\bar{y}$, and let $\operatorname{ev}_\delta \in \operatorname{Lie}/q = \operatorname{Hom}(\mathcal{L}/q, \mathbb{F}_q)$ be $\omega \mapsto \omega(\delta)$. For $Z \in \mathcal{Z}$ let $D_Z := \operatorname{Fix} Z - 2Z(y)$ and $\bar{\omega}_{D_Z} := N_q^{-1}\, d\bar{f}_{D_Z}/\bar{f}_{D_Z}$, and put*

$$L_Z := \bar{\omega}_{D_Z}(\delta) - \tilde{b}(\operatorname{ev}_\delta, \kappa[D_Z]), \qquad Q_Z := \tilde{b}(\operatorname{ev}_\delta, Z \operatorname{ev}_\delta).$$

If there is no $c \in \mathbb{F}_q$ with $L_Z = cQ_Z$ for every $Z \in \mathcal{Z}$, for instance if $L_Z Q_{Z'} \ne L_{Z'} Q_Z$ for some $Z, Z' \in \mathcal{Z}$, then y is the only rational point in its residue disc.

Proof. (a) By (B), M is torsion-free, and κ is $\mathbb{T}_q$-linear. The ideal of $\mathbb{T}_q/q$ generated by the a_{ij} contains every $a_{ij}b_{ij}^Z$, so by (C) it is the unit ideal. Hence $\kappa(M)+q\,\mathrm{Lie}=\mathrm{Lie}$, and $\kappa(M)=\mathrm{Lie}$ by Nakayama's lemma. As M is free of rank at most g by (R) and Lie is free of rank g, κ is an isomorphism. So $\beta(x,x'):=q^{-1}h(\kappa^{-1}x,\kappa^{-1}x')$ is a symmetric $\mathbb{Q}_q$-valued form on Lie with $\beta(tx,x')=\beta(x,tx')$ for $t\in\mathbb{T}_q$, and $\beta(te,t'e)=\lambda(tt')$ for $\lambda(t):=\beta(e,te)$.

Fix Z and $i<j$, and put $A:=y_j-y_i$ and $B:=B_{ij}^Z$. By (F), no term of Z passes through (y_i,y_i), (y_i,y_j), (y_j,y_i) or (y_j,y_j), and no residue disc meets the supports of both A and B. In $h([A],[B])=\sum_v h_v(A,B)$, the terms at $v\nmid qN_X$ vanish by [23, Lemma 3.1], as X has good reduction at v [16, VI, Proposition 6.7], and those at $v\mid N_X$ vanish by (V). So

$$\lambda(a_{ij}b_{ij}^Z)=\beta(\kappa[A],\kappa[B])=q^{-1}h_q(A,B),$$

which lies in $\mathbb{Z}_q$ by Lemma 8.1 (c). By (C) and Nakayama's lemma the $a_{ij}b_{ij}^Z$ span $\mathbb{T}_q$ over $\mathbb{Z}_q$, so $\lambda(\mathbb{T}_q)\subset\mathbb{Z}_q$. Thus β is $\mathbb{Z}_q$-valued, $h(M,M)\subset q\mathbb{Z}_q$, and the reduction $\bar\lambda$ of λ is as stated; (C) makes it unique.

(b) Let $z\in X(\mathbb{Q})$, $z\neq y$, with $\bar z=\bar y$. Let w be a parameter of $\mathcal{X}$ at $\bar y$ over $\mathbb{Z}_q$ with $w(y)=0$ and $d\bar w(\delta)=1$, and put $u:=w(z)$ and $k:=v_q(u)\geq 1$. Fix $Z\in\mathcal{Z}$, and let $P:=[z-y]$ and $D:=\mathrm{Fix}\,Z-Z(y)-Z(z)$. By (F), no point of D_Z or of $Z(z)-Z(y)$ lies in the residue disc of $\bar y$, and no term of Z passes through (y,y), (y,z), (z,y) or (z,z). As in (a), all local terms of $h(P,[D])$ other than h_q vanish, and $[D]=[D_Z]-ZP$, so

$$h_q(z-y,D)=h(P,[D_Z])-h(P,ZP). \tag{9.1}$$

Below, the product of u or of u^2/q with an element of $\mathbb{F}_q$ is the product with any lift; modulo q^{k+1} it does not depend on the lift, as $v_q(u^2/q)=2k-1\geq k$.

The divisor $Z(z)-Z(y)$ is rational and misses the disc of $\bar y$, and it has degree 0 on every residue disc, as $\bar z=\bar y$ and each term of Z extends to a finite flat correspondence on $\mathcal{X}$. Hence $\omega_{Z(z)-Z(y)}$ is q times an integral form on the disc of $\bar y$ [23, Proposition 2.6 (a)]. By Lemma 8.1 (a), ω_{D_Z} is integral there, with reduction $\bar\omega_{D_Z}$. Integrating from y to z term by term [23, (3.1)],

$$h_q(z-y,D)\equiv u\,\bar\omega_{D_Z}(\delta)\pmod{q^{k+1}}.$$

For $\omega\in\mathcal{L}$, $\langle\log P,\omega\rangle=\int_y^z\omega\equiv u\,(\omega/dw)(y)$ modulo q^{k+1}, in the same way. So $\kappa P\equiv(u/q)\,\widetilde{\mathrm{ev}}$ modulo $q^k\,\mathrm{Lie}$, where $\widetilde{\mathrm{ev}}\in\mathrm{Lie}$ is $\omega\mapsto(\omega/dw)(y)$, a lift of ev_δ. As β is $\mathbb{Z}_q$-valued by (a) and $2k\geq k+1$, modulo q^{k+1}

$$h(P,[D_Z])=q\beta(\kappa P,\kappa[D_Z])\equiv u\,\tilde b(\mathrm{ev}_\delta,\kappa[D_Z]),\qquad h(P,ZP)=q\beta(\kappa P,Z\kappa P)\equiv\frac{u^2}{q}\,Q_Z.$$

So (9.1) becomes

$$uL_Z+\frac{u^2}{q}\,Q_Z\equiv 0\pmod{q^{k+1}}.$$

If $k\geq 2$, this says $L_Z=0$. If $k=1$, then $s:=u/q \bmod q$ is non-zero and $L_Z+sQ_Z=0$. So $L_Z=cQ_Z$ for every $Z\in\mathcal{Z}$, with $c=0$ or $c=-s$, contrary to the hypothesis. □

The numbers in (b) depend on δ only through a scalar: replacing δ by $\mu\delta$, $\mu\in\mathbb{F}_q^\times$, multiplies L_Z by μ and Q_Z by μ^2. So the hypothesis of (b) does not depend on δ, and, when $Q_Z\neq 0$, the one value $s_Z:=-L_Z/Q_Z$ of $w(z)/q \bmod q$ that Z allows becomes s_Z/μ. Hence the ratio $s_Z/s_{Z'}$ does not depend on δ, and the condition $s_Z\neq s_{Z'}$ is that this ratio is not 1.

In the language of quadratic Chabauty, the left side $uL_Z+(u^2/q)\,Q_Z$ of the last congruence in the proof, with $u=w(z)$ and $k=v_q(u)$, is the expansion at y modulo q^{k+1} of the quadratic

Chabauty function of Z with base point y: $L_Z \neq 0$ implies that y is a simple zero of it, and $s_Z \neq s_{Z'}$ that the functions of Z and Z' have no common zero z with $v_q(w(z)) = 1$.

Remark 9.2. One correspondence cannot satisfy (C) when $n - 1 < g$. Write $\kappa[y_i - y_1] = \alpha_i e$ and $\kappa[\operatorname{Fix} Z - 2Z(y_1)] = c\,e$, and let $t_Z \in \mathbb{T}_q$ be the action of Z on Lie. Then $a_{ij} = \alpha_j - \alpha_i$ and $b_{ij}^Z = c - t_Z(\alpha_i + \alpha_j)$, so $a_{ij}b_{ij}^Z = \varphi_j - \varphi_i$ with $\varphi_i := c\alpha_i - t_Z\alpha_i^2$, and these span at most $n - 1$ dimensions. At level 25, $n = 9$ and $g = 14$, which is why we use two correspondences. The trivial and quadratic characters of $\mathbb{F}_5^\times$ give rational eigenvalues, so Z_1 and Z_2 span the combinations of the S_ν with eigenvalues in $\sqrt{5}\,\mathbb{Q}$, and $2(n-1) = 16$ leaves two equations to spare. That several correspondences give more equations from the same rational points is observed in [4, Remark 2.15].

10. The rank

Proposition 10.1. $\operatorname{rank} J(\mathbb{Q}) = 14$.

Proof. By Chen's isogeny (proof of Lemma 7.1), J is isogenous over $\mathbb{Q}$ to $\prod_f A_f$, over the Galois orbits of newforms f of weight 2 and level 625 with Fricke eigenvalue $+1$, where A_f is the quotient of $J_0(625)$ attached to f. A computation in PARI/GP gives four orbits, of dimensions 2, 2, 2 and 8. The root number of such an f is -1, so

$$L'(f,1) = 2\sum_{n\geq 1} \frac{a_n}{n} E_1\Big(\frac{2\pi n}{25}\Big), \qquad E_1(x) := \int_1^\infty e^{-xt}\frac{dt}{t}.$$

A computation in ball arithmetic with python-flint gives $L'(f,1) > 0$ for all fourteen f; the smallest of these values is $0.782729318982775 \pm 1.7 \cdot 10^{-16}$. By S.-W. Zhang's theorem [44, Theorem A], which generalizes results of Gross and Zagier [19] and of Kolyvagin [27] to totally real fields, $\operatorname{rank} A_f(\mathbb{Q}) = [\mathcal{O}_f : \mathbb{Z}] \cdot \operatorname{ord}_{s=1} L(f,s) = \dim A_f$ for these f, where $\mathcal{O}_f$ is the ring generated by the coefficients of f. So $\operatorname{rank} J(\mathbb{Q}) = 2 + 2 + 2 + 8 = 14$. □

11. The prime 1151

We apply Proposition 9.1 to X, with $\mathcal{H} = N$, $N_X = 25$, $q := 1151$, the nine points y_D, $D \in \mathcal{D}$, and $\mathcal{Z} := \{Z_1, Z_2\}$.

The points y_D modulo q^2. The computations below use v_D (Section 5) for y_D modulo q^2; we now show that $v_D \equiv y_D \bmod q^2$. By the proof of Theorem 1.4, each $\bar{y}_D$ is one of the $\bar{v}_{D'}$. For $D \neq -3$, the moduli description of (C) below, on a curve E with j-invariant j_D over the Witt vectors of $\mathbb{F}_{q^2}$ (of $\mathbb{F}_{q^5}$ for $D = -163$) on which $E[25]$ is rational, finds a point over j_D at which the values of the forms are proportional to v_D modulo q^2. So $j(v_D) \equiv j_D \bmod q^2$ for $D \neq -3$; as the j_D are distinct modulo q, $\bar{y}_D = \bar{v}_D$ for every D, including -3, and as $j - j_D$ is a parameter at $\bar{y}_D$ (Lemma 2.2), $v_D \equiv y_D \bmod q^2$ for $D \neq -3$.

At y_{-3} the fourteen values vanish, as the automorphisms of E_{-3} fix its Cartan subring, so we use a unit instead. Let $e \in \Lambda$ have $e_n = -2$ for $n \equiv \pm 2 \bmod 5$ and $e_n = 0$ otherwise. By Lemma 4.1 and the values of $A(n)$, the divisor of u_e is $5\sum_{d\equiv\pm1} c_d - 5\sum_{d\equiv\pm2} c_d$. The map $X \to X_{\mathrm{ns}}^+(5)$, $(E,R) \mapsto (E, R \bmod 5)$, is defined over $\mathbb{Q}$, and σ_d fixes or swaps the two cusps of $X_{\mathrm{ns}}^+(5)$, which are conjugate over $\mathbb{Q}(\sqrt{5})$, according as $d \equiv \pm1$ or $\pm2 \bmod 5$. So this divisor is the pull-back of the difference of the two cusps (each cusp of X, of width 25, has ramification index 5 over its image, of width 5), and as $X_{\mathrm{ns}}^+(5)$ has genus 0, u_e is constant on the fibers of $X \to X_{\mathrm{ns}}^+(5)$. Each $S_\nu(x)$ lies in the fiber of x. A computation of u_e modulo q^2, as a quotient of two forms of weight 4, shows that $u_e(v_{-3}) \equiv u_e(P) \bmod q^2$ at every point P of $S_\nu(y_{-3})$, $\nu \in \mathbb{F}_5^\times$, found by the moduli description on a curve E with j-invariant 0 over

the Witt vectors of $\mathbb{F}_{q^2}$ on which $E[25]$ is rational, and that u_e is regular with non-zero differential at $\bar{y}_{-3}$ modulo q. So $u_e - u_e(y_{-3})$ is a parameter at $\bar{y}_{-3}$, and $v_{-3} \equiv y_{-3} \bmod q^2$.

Why 1151. As $q \equiv 1 \bmod 25$, the labels can be read at q, and Theorem 1.4 puts every rational point in the residue disc of some y_D at q. As $q \equiv 11 \bmod 12$, the curves with $j = 0$ and $j = 1728$ are supersingular modulo q, and so are the y_D with $D \neq -163$, as these D are not squares modulo q; while $4q = 23^2 + 163 \cdot 5^2$, so y_{-163} is ordinary. A supersingular curve $\bar{E}$ over $\mathbb{F}_q$ has $\pi_q^2 = -q$, which acts on $\bar{E}[25]$ as -1 because $q \equiv 1 \bmod 25$. So every point of $\mathcal{X}$ over a supersingular $j \in \mathbb{F}_q$ is defined over $\mathbb{F}_{q^2}$: the fixed points of the S_ν, over $j = 0$ and 1728, and the points of $S_\nu(\bar{y}_D)$ for $D \neq -163$. This keeps the computations at q over $\mathbb{F}_{q^2}$, except at y_{-163}: its Frobenius $\pm(23 + 5\sqrt{-163})/2$ is a scalar modulo 5, so the points of $S_\nu(\bar{y}_{-163})$ are defined over $\mathbb{F}_q$, and they are computed from $\bar{E}[25]$ over $\mathbb{F}_{q^5}$. At 101, the curve with $j = 1728$ is ordinary and the points Φ_ν are not all defined over $\mathbb{F}_{101^2}$, so over $\mathbb{F}_{101^2}$ only Z_1 is usable, and one correspondence gives control equations of rank at most 8 (Remark 9.2). At 151, (B) fails: 151 divides $\#\bar{J}(\mathbb{F}_{151})$. Below 1151, the only other prime $\equiv 1 \bmod 25$ and $\equiv 11 \bmod 12$ is 251, where three of the y_D are ordinary, none with Frobenius scalar modulo 5, unlike y_{-163} at 1151.

The hypotheses. The correspondences Z_1 and Z_2 are symmetric integer combinations of double cosets NgN with $g \notin N$ (proof of Lemma 6.3), and $\operatorname{Tr}(Z \mid \mathcal{L}) = \frac{1}{2}\operatorname{Tr}(Z \mid H) = 0$ by Proposition 6.4.

(B) A computation in PARI/GP gives

$$\begin{aligned} N_q = \#\bar{J}(\mathbb{F}_{1151}) &= 816405849409688448555694726295528686523437 5 \\ &= 3^6 \cdot 5^{13} \cdot 71^2 \cdot 89^2 \cdot 56149 \cdot 60029 \cdot 72211 \cdot 943985489, \end{aligned}$$

which is prime to q.

(M) The characteristic polynomial of T_7 on $\mathcal{L}/q$ is square-free, with six linear and four quadratic factors over $\mathbb{F}_q$ (a computation in PARI/GP). So $\mathbb{Z}_q[T_7] \subset \operatorname{End}\mathcal{L}$ is étale of rank 14 over $\mathbb{Z}_q$, and $\mathcal{L}$ and its dual Lie are free of rank one over it. As $\mathbb{T}_q$ is commutative and contains T_7, $\mathbb{T}_q = \mathbb{Z}_q[T_7]$, and (M) holds.

(R) This is Proposition 10.1.

(F) The closure of S_ν in $\mathcal{X} \times \mathcal{X}$ is the correspondence $\bar{S}_\nu$ given by the same moduli description over $\mathbb{Z}_q$, which lies over the diagonal of the j-line. In the order of $\mathcal{D}$, the j_D are 0, 78, 1094, 1054, 76, 69, 868, 1114 and 658 modulo q, distinct, and $1728 \equiv 577$. So a point $(\bar{y}_D, \bar{y}_{D'})$ of $\bar{S}_\nu$ has $D = D'$ and is a fixed point of $\bar{S}_\nu$, which by Proposition 6.5 lies over $j = 0$, 1728 or ∞. Only $D = -3$ remains, and the fixed points over $j = 0$ are the reductions of Q_μ and Q'_μ, which differ from $\bar{y}_{-3}$: the automorphisms of E_{-3} fix the Cartan subring of y_{-3} and not those of Q_μ, Q'_μ.

(V) This is Corollary 7.3: by (F), for points $y, z \in X(\mathbb{Q})$ with reductions among the $\bar{y}_D$, none of (y, y), (z, z), (y, z) lies on an S_ν.

(C) A computation in Python gives the a_{ij} and b_{ij}^Z modulo q and the right sides of the control equations, with the points of $\operatorname{Fix} S_\nu$ and $S_\nu(\bar{y}_D)$ found as above. The matrices of the S_ν on $\mathcal{L}/q^2$ come from the moduli description: over a supersingular j, the values of the fourteen forms at the 250 points (E, R), for a fixed differential on E, are computed over the Witt vectors of $\mathbb{F}_{q^2}$ modulo q^2 from the values of the weight-one Eisenstein series at the points of $E[25]$ [26], as in [20, §§4.1, 6.1], since modulo q^2 the fourteen forms are combinations of the averaged products of Section 5 (an identity checked on 60 coefficients); and S_ν is the matrix that sends the values at each point to the sum of the values at its six S_ν-related points. These matrices have traces $-11, 4, 4, -11$, as Proposition 6.5 and the

Lefschetz formula require, and $1 + S_1 + S_2 + S_3 + S_4 = 0$ on $\mathcal{L}/q^2$, as $1 + \sum_\nu S_\nu$ factors through $X^+_{\mathrm{ns}}(5)$, of genus 0.

For each divisor D that enters, the function f_D is computed on the canonical curve over $\mathbb{Z}/q^2$ by linear algebra in the sections of $4K_X$, in the manner of Khuri-Makdisi [25]: an effective divisor of degree 28 is represented by the sections of $4K_X$ that vanish on it. Products of sections are read on their first 30 coefficients at ∞, which lie in $(\mathbb{Z}/q^2)[\zeta_{25}]$ and determine a section of $8K_X$: its expansions at the ten cusps are the conjugates of that at ∞, it vanishes at a cusp to order 8 less than its expansion there, and $\deg 8K_X = 208 < 10 \cdot (30 - 8)$. A double-and-add chain along N_q keeps, for each n it reaches, an effective divisor of degree 28 linearly equivalent to $nD + D_0$, and a product of quotients of sections of $4K_X$ whose divisor is the difference, starting from D_0 itself at $n = 0$. Here D_0 is a sum of 28 points over a supersingular $j \in \mathbb{F}_q$ other than 0, 1728 and the j-invariants of the nine CM points (in the computation $j = 62$); every divisor D that enters lies over these, so the residue discs of D_0 contain no point of D. At $n = N_q$ the reduction of the divisor kept is linearly equivalent to $\bar{D}_0$, as $N_q[\bar{D}] = 0$, and one more quotient replaces it by a divisor $D'_0 \equiv D_0 \bmod q$ with one point in the residue disc of each point of D_0. This gives f_D, with $\operatorname{div} f_D = N_q D + D_0 - D'_0$, so that $D_1 = D'_0 - D_0$ has degree 0 on every residue disc, and $\bar{f}_D$, with divisor $N_q \bar{D}$. For the two divisors of each control equation, the divisors D_0 lie in disjoint sets of residue discs. The proof of Lemma 8.1 (a)–(c) then applies with the residue discs of D_0 counted among those of the points of D, and gives κ and h_q modulo q^2.

The 36 products $a_{ij} b_{ij}^{Z_1}$ span a space of dimension 8, and together with the 36 for Z_2 they span $\mathbb{T}_q/q$. The right sides telescope like the products (Remark 9.2), so the 72 control equations reduce to 16 in 14 unknowns, and they are consistent: two conditions modulo q that a non-zero local term at 5 would be expected to break. So Proposition 9.1 (a) gives $h(M, M) \subset q\mathbb{Z}_q$ and the form $\tilde{b}$.

The disc coordinate. For $D \neq -3$ let $k_D := j_D(j_D - 1728)$, $a_D := -3k_D$ and $b_D := -2k_D(j_D - 1728)$, so that $y^2 = x^3 + a_D x + b_D$ has j-invariant j_D. As $X \to X(1)$ is unramified at $\bar{y}_D$ (Lemma 2.2), the family $y^2 = x^3 + a_D x + b_D + t$ over $\mathbb{F}_q[[t]]$ lifts to a unique formal curve through $\bar{y}_D$ on $\mathcal{X}_{\mathbb{F}_q}$, and we let δ_D be its tangent vector at $t = 0$. Equivalently, $dj(\delta_D) = \partial j/\partial b\,(a_D, b_D)$ for $j(a, b) = 6912a^3/(4a^3 + 27b^2)$. At $\bar{y}_{-3}$, where $a_D = b_D = 0$, we take δ_{-3} with $\mathrm{ev}_{\delta_{-3}} = 716\,\bar{v}_{-3}$ in the basis dual to the fourteen forms, for the primitive vector v_{-3} of the deposit [22]; at each $\bar{y}_D$, ev_δ is a multiple of $\bar{v}_D$, as the forms give the canonical embedding.

The proof of Theorem 1.1. Let $x \in X(\mathbb{Q})$. By Theorem 1.4, x has the reduction modulo 1151 of some y_D, $D \in \mathcal{D}$. The hypotheses of Proposition 9.1 hold at $q = 1151$, as checked above. In every row of Table 1, L_{Z_1} and L_{Z_2} are non-zero and $s_{Z_1}/s_{Z_2} \neq 1$, that is, $L_{Z_1} Q_{Z_2} \neq L_{Z_2} Q_{Z_1}$. So Proposition 9.1 (b) gives $x = y_D$. The nine points y_D are distinct, as their j-invariants are. □

D	L_{Z_1}	Q_{Z_1}	s_{Z_1}	L_{Z_2}	Q_{Z_2}	s_{Z_2}	s_{Z_1}/s_{Z_2}
-3	289	286	494	920	718	983	230
-7	954	412	1009	481	546	465	970
-8	1132	794	1051	492	153	561	761
-12	256	222	1098	203	1087	201	57
-27	679	290	1105	44	918	509	18
-28	957	87	1140	423	832	1008	974
-43	1001	1057	929	674	754	1144	525
-67	201	700	248	675	1116	677	388
-163	1064	249	874	378	184	636	823

TABLE 1. The numbers of Proposition 9.1 (b) at $q = 1151$ for the tangent vectors δ_D, as residues in $[0, 1150]$, with $s_Z = -L_Z/Q_Z$.

DECLARATIONS

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

Data availability. The programs and data used in this paper, with instructions for rerunning them, are deposited at Zenodo [22].

REFERENCES

1. Santiago Arango-Piñeros and David Zureick-Brown, *7-adic Galois representations of elliptic curves over the rationals via Kummer descent*, 2026, Preprint, arXiv:2610.06521v1.
2. Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Explicit Chabauty–Kim for the split Cartan modular curve of level 13*, Ann. of Math. (2) **189** (2019), no. 3, 885–944, doi:10.4007/annals.2019.189.3.6.
3. ———, *Quadratic Chabauty for modular curves: algorithms and examples*, Compos. Math. **159** (2023), no. 6, 1111–1152, doi:10.1112/S0010437X23007170.
4. Jennifer S. Balakrishnan, L. Alexander Betts, Daniel Rayor Hast, Aashraya Jha, and J. Steffen Müller, *Rational points on the non-split Cartan modular curve of level 27 and quadratic Chabauty over number fields*, 2025, Preprint, arXiv:2501.07833v1.
5. Jennifer S. Balakrishnan and Netan Dogra, *Quadratic Chabauty and rational points, I: p-adic heights*, Duke Math. J. **167** (2018), no. 11, 1981–2038, doi:10.1215/00127094-2018-0013.
6. Amnon Besser, J. Steffen Müller, and Padmavathi Srinivasan, *p-adic adelic metrics and quadratic Chabauty I*, J. Reine Angew. Math. **828** (2025), 223–305, doi:10.1515/crelle-2025-0063, arXiv:2112.03873v4.
7. L. Alexander Betts and Netan Dogra, *The local theory of unipotent Kummer maps and refined Selmer schemes*, 2020, Preprint, arXiv:1909.05734v2.
8. Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370, doi:10.1090/S0025-5718-09-02255-8, arXiv:0803.2052v2.
9. ———, *The Mordell–Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306, doi:10.1112/S1461157009000187.
10. Henri Carayol, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 3, 409–468, doi:10.24033/asens.1512.

11. Pierfrancesco Carlucci, *Cuspidal divisor class groups of non-split Cartan modular curves*, Acta Arith. **187** (2019), 301–327, doi:10.4064/aa8516-6-2018, arXiv:1605.00375v1.
12. Imin Chen, *Jacobians of modular curves associated to normalizers of Cartan subgroups of level p^n*, C. R. Math. Acad. Sci. Paris **339** (2004), no. 3, 187–192, doi:10.1016/j.crma.2004.04.027.
13. Robert F. Coleman and Benedict H. Gross, *p-adic heights on curves*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 73–81, doi:10.2969/aspm/01710073.
14. Harold Davenport and Helmut Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1935), 151–182, doi:10.1515/crll.1935.172.151.
15. Pierre Deligne and David Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109, doi:10.1007/BF02684599.
16. Pierre Deligne and Michael Rapoport, *Les schémas de modules de courbes elliptiques*, Modular Functions of One Variable II, Lecture Notes in Math., vol. 349, Springer, 1973, doi:10.1007/978-3-540-37855-6_4, pp. 143–316.
17. Bas Edixhoven and Guido Lido, *Geometric quadratic Chabauty*, J. Inst. Math. Jussieu **22** (2023), no. 1, 279–333, doi:10.1017/S1474748021000244.
18. Lorenzo Furio and Davide Lombardo, *On 7-adic Galois representations for elliptic curves over $\mathbb{Q}$*, Proc. Lond. Math. Soc. (3) **133** (2026), no. 2, Paper No. e70193, doi:10.1112/plms.70193, arXiv:2507.17967v3.
19. Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320, doi:10.1007/BF01388809.
20. Sachi Hashimoto, Guido Maria Lido, Davide Lombardo, Nicolas Mascot, and Pierre Parent, *Equationless quadratic Chabauty for non-split Cartan modular curves*, 2026, Preprint, arXiv:2608.10919v1.
21. Hervé Jacquet and Robert P. Langlands, *Automorphic forms on* GL(2), Lecture Notes in Math., vol. 114, Springer, Berlin, 1970, doi:10.1007/BFb0058988.
22. Manvir Jaswal, *Programs and data for "The rational points of the non-split Cartan modular curve of level 25"*, 2026, Zenodo, doi:10.5281/zenodo.24061908.
23. ———, *The rational points of the non-split Cartan modular curve of level 121*, 2026, Preprint, Zenodo, doi:10.5281/zenodo.24061906.
24. Eray Karabiyik, *Classifying 5-adic and 7-adic Galois representations of elliptic curves*, 2026, Talk, FGC-HRI-IPM Number Theory Webinar, October 21, 2026, https://researchseminars.org/talk/FGC-IPM/72/.
25. Kamal Khuri-Makdisi, *Linear algebra algorithms for divisors on an algebraic curve*, Math. Comp. **73** (2004), no. 245, 333–357, doi:10.1090/S0025-5718-03-01567-9, arXiv:math/0105182v3.
26. ———, *Moduli interpretation of Eisenstein series*, Int. J. Number Theory **8** (2012), no. 3, 715–748, doi:10.1142/S1793042112500418, arXiv:0903.1439v6.
27. Viktor A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser, Boston, MA, 1990, doi:10.1007/978-0-8176-4575-5_11, pp. 435–483.
28. Daniel S. Kubert and Serge Lang, *Modular units*, Grundlehren Math. Wiss., vol. 244, Springer, New York, 1981, doi:10.1007/978-1-4757-1741-9.
29. Philip Kutzko, *The Langlands conjecture for* GL_2 *of a local field*, Ann. of Math. (2) **112** (1980), no. 2, 381–412, doi:10.2307/1971151.
30. Robert P. Langlands, *Modular forms and ℓ-adic representations*, Modular Functions of One Variable II, Lecture Notes in Math., vol. 349, Springer, 1973, doi:10.1007/978-3-540-37855-6_6, pp. 361–500.
31. Franz Lemmermeyer, *The ambiguous class number formula revisited*, J. Ramanujan Math. Soc. **28** (2013), no. 4, 415–421, arXiv:1309.1071v1.
32. Marius Leonhardt and Isabel Rendell, *Aspects of quadratic Chabauty via modular forms*, 2026, Preprint, arXiv:2610.30703v1.
33. Elvira Lupoian, *Modular units on $X_1(p)$ and quotients of the cuspidal group*, J. Algebra **713** (2027), 1061–1094, doi:10.1016/j.jalgebra.2026.10.008, arXiv:2502.04084v1.
34. Barry Mazur, *Rational points on modular curves*, Modular functions of one variable, V, Lecture Notes in Math., vol. 601, Springer, Berlin, 1977, pp. 107–148, doi:10.1007/BFb0063947.
35. James S. Milne, *Abelian varieties*, 2008, Course notes, version 2.0, https://www.jmilne.org/math/CourseNotes/av.html.
36. Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight)*, Forum Math. Sigma **10** (2022), Paper No. e62, doi:10.1017/fms.2022.38, arXiv:2106.11141v6.
37. Bernard Saint-Donat, *On Petri's analysis of the linear system of quadrics through a canonical curve*, Math. Ann. **206** (1973), 157–175.

38. Edward F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), no. 3, 447–471, doi:10.1007/s002080050156, arXiv:1507.08325v1.
39. Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331, doi:10.1007/BF01405086.
40. ———, *Lectures on the Mordell–Weil theorem*, Aspects of Mathematics, vol. E15, Vieweg, 1989.
41. Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), no. 3, 492–517, doi:10.2307/1970722.
42. Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan, vol. 11, Iwanami Shoten and Princeton University Press, Tokyo and Princeton, 1971.
43. Lawrence C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Grad. Texts in Math., vol. 83, Springer, 1997, Ch. 8: doi:10.1007/978-1-4612-1934-7_8.
44. Shou-Wu Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27–147, doi:10.2307/2661372, arXiv:math/0101269.

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