hexagon:2611.00255v1

THE RATIONAL POINTS OF THE NON-SPLIT CARTAN MODULAR CURVE OF LEVEL 121

MANVIR JASWAL

Abstract. We prove that the modular curve $X_{\mathrm{ns}}^{+}(121)$ of the normalizer of a non-split Cartan subgroup of level 121, of genus 511, has exactly seven rational points, all of them CM. This is the level 121 case of a conjecture of Rouse, Sutherland and Zureick-Brown, and with their theorem it determines the 11-adic images of Galois of non-CM elliptic curves over $\mathbb{Q}$. The Jacobian has rank equal to the genus. We work at the primes 17 and 43, at each of which one Hecke block of the Mordell–Weil group has logarithm divisible by p^2 while its p-adic height has valuation exactly one. A comparison of valuations in the quadratic Chabauty identity then shows that the residue disc of each CM point holds no other rational point, with no computation of the local height at p, no basis of the Mordell–Weil group and no model of the curve. The inputs come from expansions of differentials at CM points and from a formula we prove for intersection numbers of CM divisors under Hecke correspondences on $X_{\mathrm{ns}}^{+}(\ell^e)$, at every prime $v \neq \ell$, and at $v = \ell$ when $\ell \geq 7$, $\ell \equiv 3 \bmod 4$ and $e \leq 2$.

Contents

1. Introduction 1
2. Heights and integrality 6
3. The method 9
4. The height formula 12
5. Correspondences that change only the Cartan subgroup 21
6. Differentials without an equation 22
7. The seven classes 28
8. One residue disc 30
9. The term at 11 31
10. The rank 34
11. The primes 17 and 43 34
Appendix A. Computations 37
Declarations 38
References 38

1. Introduction

Let A 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 [60], and Mazur's Program B [54, p. 109] asks which

Date: November 8, 2026.
2020 *Mathematics Subject Classification.* Primary 11G18; Secondary 11G05, 11F80, 11G50, 14G05.
Key words and phrases. Non-split Cartan modular curves, quadratic Chabauty, p-adic heights, Hecke correspondences, complex multiplication, Galois images of elliptic curves.

images occur. Write $N_{\mathrm{ns}}(m)$ for the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/m)$. Rouse, Sutherland and Zureick-Brown [58, Theorem 1.6] show that the ℓ-adic image H of A is in one of four cases: X_H has infinitely many rational points; H is on an explicit list; $H \subset N_{\mathrm{ns}}(m)$ for $m = 3^3, 5^2, 7^2, 11^2$ or a prime $m \geq 19$; or H lies in one of two groups of level 49. They conjecture that in the last two cases all points of $X_H(\mathbb{Q})$ are cusps or CM.

The case $m = 27$ has since been settled by Balakrishnan, Betts, Hast, Jha and Müller [6, Theorem 1.3], the case $m = 49$ by Furio and Lombardo [26, Theorem 1.4], and the two groups of level 49 by Arango-Piñeros and Zureick-Brown [1, Theorem 2]. At $\ell = 11$, Bisatt, Furio and Lombardo [10, Theorem 1.1] show that an image inside $N_{\mathrm{ns}}(11)$ is the full preimage of $N_{\mathrm{ns}}(11^n)$ for some $n \geq 1$. So the question is whether $n \geq 2$ can occur, that is, whether $X^+_{\mathrm{ns}}(121)$ has a non-CM rational point.

Theorem 1.1. *The curve $X^+_{\mathrm{ns}}(121)$ has exactly seven rational points, all CM, of discriminants $-27, -16, -12, -67, -4, -3, -163$. Consequently, by* [10, Theorem 1.1]*, if $A/\mathbb{Q}$ has no complex multiplication and its mod 11 image lies in $N_{\mathrm{ns}}(11)$, then its 11-adic image is the full preimage of $N_{\mathrm{ns}}(11)$.*

Put $X := X^+_{\mathrm{ns}}(121)$, of genus 511, and let $\pi\colon X \to E := X^+_{\mathrm{ns}}(11)$ be the natural map. Here E is the elliptic curve $y^2 + y = x^3 - x^2 - 7x + 10$ (121b1 in Cremona's tables), with $E(\mathbb{Q}) = \mathbb{Z}P_0$ and $P_0 = (4, 5)$, identified with $X^+_{\mathrm{ns}}(11)$ so that the CM points of discriminants -12 and -67 are the origin and P_0; the seven points lie over kP_0 for $k = -2, \dots, 4$, in the order above.

This is the level 121 case of the conjecture above, and with [58, Theorem 1.6] it completes the 11-adic part of Program B. Of the conjectured cases, $N_{\mathrm{ns}}(\ell)$, $\ell \geq 19$, remain; Balakrishnan, Müller and Vonk have announced $\ell = 19$ and 23 (see [50, §1]). Karabiyik has announced $N_{\mathrm{ns}}(5^2)$ [40], and a proof is given in [39].

The obstacle. The Jacobian J of X has rank 511, its genus (Proposition 10.1), so the method of Chabauty and Coleman [12, 17] does not apply. Quadratic Chabauty [7, 23], a case of Kim's non-abelian method [46, 47], allows this rank, but it needs the local height at a prime p as a function on a residue disc, computed from a plane model [3] or from arithmetic in J and a Mumford torsor [33]. It has settled levels 13 and 17, of genus 3 and 6 [2, 3]; the announced levels 19 and 23 have genus 8 and 13; and Leonhardt and Rendell compute its first steps from modular forms at genus 14 and 24 [50, Theorem A]. The Mordell–Weil sieve of Rouse et al. on E leaves the seven CM points and multiples of P_0 of enormous size [58, §9.2], and no sieve can finish, because each class it leaves holds a rational point.

The idea. Fix a prime $p \geq 7$, $p \neq 11$, with $p \nmid \#\bar{J}(\mathbb{F}_p)$, and put $M := J(\mathbb{Q}) \otimes \mathbb{Z}_p$. The logarithm sends M into $p\,\mathrm{Lie}$, where Lie is the Lie algebra of the Néron model of J over $\mathbb{Z}_p$. Both split into blocks, one for each maximal ideal of the Hecke algebra $\mathbb{T}_p$. We call a block $\mathfrak{n}$ *saturated* if $p^{-1}\log\colon M_{\mathfrak{n}} \to \mathrm{Lie}_{\mathfrak{n}}$ is an isomorphism; equationless quadratic Chabauty assumes that every block is [33, (4.4.1), Assumption 6.2(1)]. We use the opposite case: a block $\mathfrak{m}$ of rank one whose generator G has $\log G \in p^2\,\mathrm{Lie}_{\mathfrak{m}}$, one layer deeper than reduction forces. On the block of an elliptic quotient this says that p is an elliptic Wieferich prime [62, 63]. For (E, P_0) it happens at $p = 17$, where $18 = \#E(\mathbb{F}_{17})$ and $18P_0 \in E_2(\mathbb{Q}_{17})$. The Coleman–Gross height h does not see this: it maps $M \times M$ into $p\mathbb{Z}_p$, and on the blocks we use $h(G, G)$ has valuation exactly 1.

So let $y \neq z$ in $X(\mathbb{Q})$ be congruent exactly modulo p^v, and put $a := v_p(\log G) \geq 2$. In the identity of quadratic Chabauty the local height at p has valuation at least v, by integrality alone, while the global term on the block has valuation exactly $v - a + 1 < v$.

This is impossible, so $z = y$. We never compute the local height or find a basis of $J(\mathbb{Q})$. If instead $a = 1$, the global term has valuation v and the valuations decide nothing: this is the saturated case, where one needs the local height as a function on the disc.

In detail, put $P := z - y$. For a symmetric correspondence Z on X with trace 0 on differentials and divisor of fixed points $\operatorname{Fix} Z$, put $D_Z := \operatorname{Fix} Z - 2Z(y)$ and $D(y,z) := \operatorname{Fix} Z - Z(y) - Z(z)$, both of degree 0. If no component of Z has reduction through $(\bar{y},\bar{y})$ and the local terms at bad primes vanish, then

$$h_p(P, D(y,z)) = h(P, [D_Z]) - h(P, ZP). \tag{1.1}$$

If the form on $\mathfrak{m}$ does not vanish at $\bar{y}$ and every other block is saturated, then $P = \tau G + p^{v-1}Q'$ with $v_p(\tau) = v - a$ and $Q' \in M$ off the block. Blocks are orthogonal, so

$$h_p(P, D(y,z)) = \tau\, h(G, [D_Z]) + h(p^{v-1}Q', [D_Z]) - \tau^2 \tilde{Z}\, h(G,G) - p^{2v-2} h(Q', ZQ'), \tag{1.2}$$

where $\tilde{Z} \in \mathbb{Z}_p$ is the eigenvalue of Z on the block. We choose Z with $\tilde{Z} \in p\mathbb{Z}_p$ and $v_p h(G, [D_Z]) = 1$, so the terms of (1.2), in order, have valuations at least v, exactly $v-a+1$, at least v, at least $2(v-a)+2$ and at least $2v-1$. As $a \geq 2$ and $v \geq a$, the second is strictly the smallest.

The method. The argument needs only a block of this kind on the Jacobian of a modular curve X_H; Remark 3.2 says how often to expect one. Let $H \subset \mathrm{GL}_2(\mathbb{Z}/N)$ contain the scalars, with $\det H = (\mathbb{Z}/N)^\times$, let $X = X_H$ over $\mathbb{Q}$ have genus $g \geq 1$ and Jacobian J, and let $\mathbb{T} \subset \operatorname{End} J$ be generated by the T_q, $q \nmid N$, where T_n sums over all subgroups of order n. Let $p \geq 5$ be a prime not dividing N, let $\mathcal{X}/\mathbb{Z}_p$ be the smooth model, put $\mathcal{L} := H^0(\mathcal{X}, \Omega^1)$, $S := \mathcal{L}/p\mathcal{L}$, $\mathrm{Lie} := \operatorname{Hom}(\mathcal{L}, \mathbb{Z}_p)$, $\mathbb{T}_p := \mathbb{T} \otimes \mathbb{Z}_p$ and $M := J(\mathbb{Q}) \otimes \mathbb{Z}_p$, and assume:

(B) $p \nmid \#\bar{J}(\mathbb{F}_p)$;

(Φ) p does not divide the exponent of the component group of J at any bad prime;

(M) Lie is free of rank one over $\mathbb{T}_p$, which holds if every block of $\mathbb{T}_p$ on S is étale.

By (B), M is torsion-free and $\log M \subset p\,\mathrm{Lie}$. By (M), $\mathcal{L}$ has a $\mathbb{T}_p$-stable complement in $H^1_{\mathrm{dR}}(\mathcal{X}/\mathbb{Z}_p)$, and every such complement is isotropic. Let $h = \sum_v h_v$ be the Coleman–Gross height [18] for one of them, with $\log_p p = 0$. Then $h(M,M) \subset p\mathbb{Z}_p$ (Section 2).

Besides the T_n we use correspondences that fix the elliptic curve and change only the level structure: a double coset $H\gamma H$ sends the class of $(A, H\phi)$, $\phi\colon A[N] \cong (\mathbb{Z}/N)^2$, to the sum of the classes of $(A, H\gamma'\phi)$ over $H\gamma' \subset H\gamma H$. It commutes with $\mathbb{T}_p$ on Lie, so it lies in $\mathbb{T}_p$ by (M).

Theorem 1.2. *Assume* (B), (Φ) *and* (M). *Let* $\mathfrak{m}$ *be a block with* $\mathbb{T}_\mathfrak{m} = \mathbb{Z}_p$ *and character* $\theta\colon \mathbb{T}_p \to \mathbb{F}_p$ *such that:*

(a) $M_\mathfrak{m} = \mathbb{Z}_p G$ *with* $\log G \in p^2\,\mathrm{Lie}_\mathfrak{m}$, *and every other block is saturated, so that* $\operatorname{rank} J(\mathbb{Q}) = g$;

(b) $y \in X(\mathbb{Q})$, *and the nonzero forms in* $S[\mathfrak{m}]$ *do not vanish at* $\bar{y}$;

(c) Z *is a symmetric integer combination of double cosets* $H\gamma H$, $\gamma \notin H$, *and of* T_n *with* n *non-square and prime to* Np, *with* $\operatorname{Tr}(Z \mid \mathcal{L}) = 0$, $\theta(Z) = 0$ *and* $v_p h(G, [\operatorname{Fix} Z - 2Z(y)]) = 1$, *and no term of* Z *has reduction through* $(\bar{y},\bar{y})$.

If $z \in X(\mathbb{Q})$ *has* $\bar{z} = \bar{y}$ *and* $h_\ell(z - y, \operatorname{Fix} Z - Z(y) - Z(z)) = 0$ *at each prime* $\ell \mid N$, *then* $z = y$.

Section 3 proves this, and tests (a) and the height condition in (c) with two functionals modulo p (Step 6 below).

The height formula. Of the two functionals, λ_u comes from Taylor coefficients of differentials at CM points and $c_{\mathfrak{m}}$ from intersection numbers of CM divisors under Hecke operators, which we compute at every prime, 11 included. Let D_1, D_2 be coprime negative fundamental discriminants, $n \geq 1$, $D := D_1 D_2$, $F := \mathbb{Q}(\sqrt{D})$, $L := \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ and $w_i := \#\mathcal{O}_{D_i}^{\times}$. For $x \in \mathbb{Z}$ with $|x| < n\sqrt{D}$ and $x \equiv nD \bmod 2$ put

$$\nu_x := \frac{x + n\sqrt{D}}{2}, \qquad m_x := \frac{Dn^2 - x^2}{4},$$

and for a prime $\mathfrak{q}$ of F, which does not ramify in L, put

$$r_{\mathfrak{q}}(x) := \begin{cases} \operatorname{ord}_{\mathfrak{q}} \nu_x + 1 & \text{if } \mathfrak{q} \text{ splits in } L, \\ 1 & \text{if } \mathfrak{q} \text{ is inert in } L \text{ and } \operatorname{ord}_{\mathfrak{q}} \nu_x \text{ is even}, \\ 0 & \text{if } \mathfrak{q} \text{ is inert in } L \text{ and } \operatorname{ord}_{\mathfrak{q}} \nu_x \text{ is odd}. \end{cases}$$

Only those x count for which exactly one prime $\mathfrak{v}$ has $r_{\mathfrak{v}}(x) = 0$. For such x let $v(x)$ be the residue characteristic of $\mathfrak{v}$, and put $b(x) := \operatorname{ord}_{\mathfrak{v}} \nu_x$ and $R(x) := \prod_{\mathfrak{q} \neq \mathfrak{v}} r_{\mathfrak{q}}(x)$. For an odd prime $\ell \nmid n$ and $e \geq 1$ with $(D_i/\ell) = -1$, let $y(D_i)$ on $X_{\mathrm{ns}}^{+}(\ell^e)$ be the sum, over A with $\operatorname{End} A = \mathcal{O}_{D_i}$, of the point whose Cartan structure on $A[\ell^e]$ is the action of $\mathcal{O}_{D_i}/\ell^e$.

Theorem 1.3. *Let $n \geq 1$ with $\ell \nmid n$.*

(a) (Non-split level.) *For every prime $v \neq \ell$, including $v \mid nD$, with i_v the intersection number on the smooth model,*

$$i_v(y(D_1), T_n y(D_2)) = \frac{w_1 w_2}{8} \sum_{v(x) = v,\ \ell^{2e} \mid m_x} R(x)\, \frac{b(x) + 1}{2}.$$

(b) (The prime ℓ.) *Let $\ell \geq 7$, $\ell \equiv 3 \bmod 4$ and $e \in \{1, 2\}$. The Jacobian of $X_{\mathrm{ns}}^{+}(\ell^e)$ has potentially good reduction at ℓ ([24, Theorem 3.5] for $e = 1$, Section 4 for $e = 2$), so the Berkovich space of $X_{\mathrm{ns}}^{+}(\ell^e)$ over $\mathbb{C}_\ell$, with the valuation normalized to be 1 at ℓ, is contractible. Exactly one of its points lies over the Gauss point of the j-line. Take it as the root, let $(P|Q)$ be the Gromov product and let $i_\ell(\sum n_P P, \sum n'_Q Q) := \sum n_P n'_Q (P|Q)$, which on divisors of degree 0 is the Néron symbol. Then*

$$i_\ell(y(D_1), T_n y(D_2)) = \frac{w_1 w_2}{8} \sum_{v(x) = \ell} R(x)\, g_e\Big(\frac{b(x) + 1}{2}\Big),$$

where, for integers $r \geq 1$, $g_1(r) = r - 1 + \frac{1}{\ell - 1}$, $g_2(1) = \frac{1}{\ell^2(\ell - 1)}$ and $g_2(r) = r - 2 + \frac{1}{\ell} + \frac{1}{\ell^2(\ell - 1)}$ for $r \geq 2$.

At $n = 1$, part (a) is the local form of [52, Theorem C], and on the j-line the proof of (a) recovers [30, Theorem 1.3] and the finite part of [29, Ch. V, §1, (1), p. 552]; Section 4 compares them. In the proof of Theorem 1.1, which uses the primes 17 and 43, the formulas of Theorem 1.3 enter only at $p = 43$, through a single value of $c_{\mathfrak{m}}$; at $p = 17$ the height is computed on E.

The proof of Theorem 1.1. Again $X = X_{\mathrm{ns}}^{+}(121)$. Let $z \in X(\mathbb{Q})$, $p \in \{17, 43\}$, and let y_k be the CM point over kP_0. Our correspondences change only the Cartan subgroup. As -1 is a non-residue modulo 11, a point of X off the cusps is a class $[A, \pm x]$ with $x \in \operatorname{End} A[121]$, $x^2 = -1$, and R_C replaces $\pm x$ by the sum of all $\pm x'$ with $\pm\frac{1}{2}\operatorname{tr}(xx') = \pm C$; S_ν does the same for $x' = \pm(x + 11w)$, $w^2 = \nu$ (Section 5).

1. **Classes** (Section 7). The denominator of $j(z)$ is a 121st power [26, Proposition 2.9], from [25, Proposition 5.14], and X has no rational cusps. So a modular unit on E over $K := \mathbb{Q}(\zeta_{11})^+$, with divisor on the five cusps of E, takes a value in $\mathcal{O}_K^\times K^{\times 11}$ at $\pi(z)$. A computation with 11th-power symbols gives $\pi(z) = mP_0$ with $m \equiv k$ modulo $\operatorname{lcm}(18, 44, 2 \cdot 11^3)$ for one $k \in \{-2, \dots, 4\}$.
2. **One residue disc** (Section 8). As $\#E(\mathbb{F}_{17}) = 18$ and $\#E(\mathbb{F}_{43}) = 44$, $\pi(z)$ and kP_0 agree modulo p. When p splits in the CM field of y_k, Frobenius permutes the points over $k\bar{P}_0$ through its class modulo 11, and fixes only $\bar{y}_k$. Hence $\bar{z} = \bar{y}_k$, at $p = 17$ for $k = -1, 1, 2$ and at $p = 43$ for $k = -2, 0, 3, 4$; the CM fields of the last four are inert at 17.
3. **The term at 11** (Section 9). The only bad prime is 11. Since $m \equiv k \bmod 2 \cdot 11^3$, the points y_k and z lie in one closed disc of X^{an} over $\mathbb{C}_{11}$, on which the j-invariant is injective. As Z preserves it, a point of $D(y_k, z)$ in the disc would be a fixed point of a term of Z, and the disc holds none. Thus $h_{11}(z - y_k, D(y_k, z)) = 0$.
4. **The rank** (Section 10). By [13, Theorem 1.4] and [58, Table 14], J is isogenous to a product over nine Galois orbits of newforms of levels 121 and 14641. A computation gives $L'(f, 1) \neq 0$ for one form in each orbit, and [21, Proposition 7.1], which rests on Gross–Zagier [31] and Kolyvagin–Logachev [48], gives $\operatorname{rank} J(\mathbb{Q}) = 511$.
5. **Differentials without an equation** (Section 6). Products of two weight-one Eisenstein series, averaged over the Cartan subgroup, span $H^0(\mathcal{X}, \Omega^1(\text{cusps}))$ modulo p, so S and the T_q are explicit on q-expansions. A computation gives (B) and étale blocks, hence (M). Inertia at 11 acts on J through a group of order prime to p, which gives (Φ).
6. **Heights as intersection numbers** (Sections 2 and 3). If divisors b, b' have degree 0 on every residue disc at p and no disc meets both, then $h_p(b, b') \in p^2\mathbb{Z}_p$, so
$$h(b, b') \equiv -\sum_{v \neq p} i_v(b, b') \log_p v \pmod{p^2}. \tag{1.3}$$
As $B := p + 1 - T_p$ gives any rational divisor u degree 0 on every disc, we can compute
$$\lambda_u(\omega) := p^{-1} \int_{Bu} \omega \bmod p \quad (\omega \in S), \qquad c_{\mathfrak{m}}(u, u') := p^{-1} h(e_{\mathfrak{m}} Bu, Bu') \bmod p.$$
If $\operatorname{rank} J(\mathbb{Q}) \leq g$, λ_u vanishes on $S[\mathfrak{m}]$ and on no other $S[\mathfrak{n}]$, and $c_{\mathfrak{m}}(u, \operatorname{Fix} Z) \neq 0$, then (a) of Theorem 1.2 holds with $G = (Bu)_{\mathfrak{m}}$, and so does the height condition in (c).
7. **Computing λ and $c_{\mathfrak{m}}$** (Sections 6, 4 and 5). At a CM point y with p split and $j(y) \not\equiv 0, 1728 \bmod p$, $\lambda_y(\omega)$ is a unit times the Taylor coefficient of order $p - 2$ of ω at y in the disc coordinate rescaled so that j has derivative 1 at y, which an extension of Ramanujan's equations to these Eisenstein series computes from their values at y. For CM divisors, Theorem 1.3 and (1.3) make $c_{\mathfrak{m}}$ a finite sum over the x above, weighted by Fermat quotients of $v(x)$; the relations among the T_n that isolate $\mathfrak{m}$ are found on S. By hand, $\operatorname{Fix} R_C$ and $\operatorname{Fix} S_\nu$ are sums of images of $y(-4)$, $y(-3)$ under such operators, each a scalar on a block, and multiples of the sum $\mathbf{C}$ of the cusps, which B kills.
8. **The prime 17** (Section 11). Take $\mathfrak{m}$ the block of E and $u = y(-67)$. A computation shows that λ_u vanishes only on $\mathfrak{m}$. For a suitable integer combination Z of the R_C and S_ν, pushing to E, where the height is explicit, gives $c_{\mathfrak{m}}(u, \operatorname{Fix} Z) \equiv 12 \bmod 17$, and Theorem 1.2 gives $z = y_k$ for $k = -1, 1, 2$.
9. **The prime 43** (Section 11). The same happens on a block $\mathfrak{m}$ of a five-dimensional factor of J, and $u = y(-163)$ detects it: λ_u vanishes on $\mathfrak{m}$ and on no other block. For $Z = R_2$,

the divisor $\operatorname{Fix} R_2$ and the eigenvalues on $\mathfrak{m}$ of the operators in it reduce $c_{\mathfrak{m}}(u, \operatorname{Fix} Z)$ to Step 7, and a computation gives $c_{\mathfrak{m}}(u, \operatorname{Fix} Z) \equiv 24 \bmod 43$. Theorem 1.2 gives $z = y_k$ for $k = -2, 0, 3, 4$, so $X(\mathbb{Q})$ is the seven y_k.

Sections 2 and 3 hold for general X_H and Section 4 for non-split Cartan level. Appendix A says what was computed and where the programs are deposited [38].

2. Heights and integrality

We keep the setting of Theorem 1.2: $X = X_H$, J, p, $\mathcal{X}$, $\mathcal{L}$, S, Lie, $\mathbb{T}_p$ and M. All residue points named below are rational over a finite field $\mathbb{F}_q$, and we put $O := W(\mathbb{F}_q)$ and $\mathbb{Q}_q := O[1/p]$. A *residue disc* is a fiber of the reduction map $X(\mathbb{C}_p) \to \mathcal{X}(\bar{\mathbb{F}}_p)$. An *integral parameter* at $\bar{x} \in \mathcal{X}(\mathbb{F}_q)$ is a function τ with $\widehat{\mathcal{O}}_{\mathcal{X}_O, \bar{x}} = O[[\tau]]$, so that the disc of $\bar{x}$ is $\{v(\tau) > 0\}$.

Let W be an isotropic $\mathbb{Z}_p$-direct summand of $H^1_{\mathrm{dR}}(\mathcal{X}/\mathbb{Z}_p)$ complementary to $\mathcal{L}$. For a divisor D of degree 0 on X over a finite extension K of $\mathbb{Q}_p$, let ω_D be the form of the third kind over K with residue divisor D and $\Psi(\omega_D) \in W \otimes K$, where Ψ is the homomorphism of [18, Proposition 2.5]. For divisors a, b of degree 0 with disjoint supports, put

$$h_p(a, b) := \int_a \omega_b, \qquad h_v(a, b) := -i_v(a, b) \log_p v \quad (v \neq p),$$

a Coleman integral and the Néron symbol at v, with $\log_p p = 0$. Over $\mathbb{Q}$ the sum $h = \sum_v h_v$ is the Coleman–Gross height [18]. It is a symmetric bilinear form on $J(\mathbb{Q})$, because W is isotropic [18, Proposition 5.2], and it extends to $M \times M$.

Lemma 2.1. *Assume* (M). *Then $\mathcal{L}$ has a $\mathbb{T}_p$-stable complement in $H^1_{\mathrm{dR}}(\mathcal{X}/\mathbb{Z}_p)$, and every such complement is isotropic.*

Proof. The quotient $H^1_{\mathrm{dR}}(\mathcal{X}/\mathbb{Z}_p)/\mathcal{L} = H^1(\mathcal{X}, \mathcal{O}) = \mathrm{Lie}$ is free of rank one over $\mathbb{T}_p$, so the surjection onto it splits $\mathbb{T}_p$-linearly. Let W be a stable complement, with generator w. Each T_q is self-adjoint for the cup product, since $qI \in H$. So $\langle w, tw\rangle = \langle tw, w\rangle = -\langle w, tw\rangle$ for $t \in \mathbb{T}_p$, and $\langle w, tw\rangle = 0$ as p is odd. □

If every block of $\mathbb{T}_p$ on S is étale, that is, $\dim S_{\mathfrak{n}}$ is the residue degree of $\mathfrak{n}$ for each $\mathfrak{n}$, then (M) holds. Indeed $\mathcal{L}_{\mathfrak{n}}$ is free of rank one over the unramified ring $W(k_{\mathfrak{n}}) \subset \mathbb{T}_{\mathfrak{n}}$, and $\mathbb{T}_{\mathfrak{n}}$ acts faithfully on it and commutes with $W(k_{\mathfrak{n}})$, so $\mathbb{T}_{\mathfrak{n}} = W(k_{\mathfrak{n}})$.

Lemma 2.2. *Let W be stable under T_q, $q \nmid N$. Then $T_q^* \omega_D = \omega_{T_q D}$, and $h(T_q a, c) = h(a, T_q c)$ on $J(\mathbb{Q})$. So $\mathbb{T}_p$ acts on M by self-adjoint operators for h, and distinct blocks of M are orthogonal.*

Proof. By [18, Proposition 2.5], Ψ is the logarithm of the universal vectorial extension $\mathcal{E}$ of J, whose $\mathbb{Q}_p$-points are the forms with simple poles and integral residues modulo the forms df/f. Such a form ω with residue divisor D is the point of $\mathcal{E}$ given by $\mathcal{O}(D)$ with its connection. The correspondence $T_q = (\pi_1)_* \pi_2^*$ acts on line bundles with connection by pull-back and trace, so it acts on $\mathcal{E}$ as a homomorphism of algebraic groups. It sends ω to $T_q^* \omega$, of residue divisor $T_q D$, and it acts on $\mathrm{Lie}\, \mathcal{E} = H^1_{\mathrm{dR}}$ as T_q^*. A logarithm commutes with homomorphisms, so $\Psi(T_q^* \omega) = T_q^* \Psi(\omega)$, and uniqueness gives $T_q^* \omega_D = \omega_{T_q D}$. For $q \neq p$ the correspondence T_q has good reduction at p, so $h_p(a, T_q c) = \int_a T_q^* \omega_c = \int_{T_q a} \omega_c$, as T_q is symmetric and Coleman integration is functorial. At $v \neq p$ the Néron symbol satisfies the projection formula. So T_q is self-adjoint for $q \neq p$. By strong multiplicity one, the

eigenvalues of the T_q, $q \nmid Np$, on $\mathcal{L} \otimes \mathbb{Q}_p$ determine those of T_p; hence T_p is a polynomial over $\mathbb{Q}_p$ in these T_q, and it is self-adjoint because h is $\mathbb{Q}_p$-bilinear. □

Divisors of degree zero on every disc. The next three statements say that a divisor of degree 0 on every residue disc has a form of the third kind divisible by p away from its support. Their source is that a divisor stable under Galois over an unramified ring has power sums divisible by p.

Lemma 2.3. *Let A be an effective divisor on the residue disc of $\bar{x} \in \mathcal{X}(\mathbb{F}_q)$, stable under $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_q)$, and let τ be an integral parameter at $\bar{x}$. Then $m^{-1}\sum_{y\in A}\tau(y)^m \in pO$ for all $m \geq 1$. Hence for $\rho = \sum_{n\geq 0} r_n \tau^n d\tau \in O[[\tau]]d\tau$ with primitive R and $R(0) = 0$, we have $\sum_{y\in A} R(\tau(y)) \in pO$.*

Proof. Write $\prod_{y\in A}(\tau - \tau(y)) = \tau^d(1+u)$ with $u = \sum_{j=1}^{d} a_j \tau^{-j}$. The a_j lie in $\mathbb{Q}_q$ and have positive valuation, and $\mathbb{Q}_q$ is unramified, so $a_j \in pO$. In $\mathbb{Q}_q[[1/\tau]]$,

$$-\sum_{m\geq 1}\Big(\sum_{y\in A}\tau(y)^m\Big)\frac{\tau^{-m}}{m} = \log(1+u) = \sum_{k\geq 1}(-1)^{k-1}\frac{u^k}{k} \in pO[[1/\tau]],$$

since $p^k/k \in p\mathbb{Z}_p$ for $k \geq 1$, and the coefficient of τ^{-m} gives the first claim. The second follows by summing over the terms of R. □

We use a kernel for ω_b that is integral in both variables.

Lemma 2.4. *Let $\bar{x}' \in \mathcal{X}(\mathbb{F}_q)$, let τ' be an integral parameter there, $R' := O[[\tau']]$, and let z be the tautological section of $\mathcal{X}_{R'} := \mathcal{X} \times_{\mathbb{Z}_p} \operatorname{Spec} R'$, with local equation $t := \tau' \otimes 1 - 1 \otimes \tau'$, the parameter on $\mathcal{X}$ minus the variable of R'. There is a unique $\psi \in H^0(\mathcal{X}_{R'}, \Omega^1(2z))$ with $\psi \equiv dt/t^2$ modulo forms regular along z and with class in $W \otimes R'$. Its expansion at $\bar{u} \neq \bar{x}'$ in an integral parameter τ lies in $O[[\tau', \tau]]d\tau$. For z_0 in the disc of $\bar{x}'$, the specialization ψ_{z_0} at $\tau' = \tau'(z_0)$ is the form with principal part dt/t^2 at z_0 and class in W.*

Proof. Let $\Omega^1(2z)_0 := \Omega^1 + d(\mathcal{O}(z))$, the forms in $\Omega^1(2z)$ of residue 0 along z; here $d(a/t) = -a|_z\, dt/t^2 +$ (regular) with no denominator, for any p. So d induces an isomorphism $\mathcal{O}(z)/\mathcal{O} \to \Omega^1(2z)_0/\Omega^1$, and the map of complexes $[\mathcal{O} \to \Omega^1] \to [\mathcal{O}(z) \to \Omega^1(2z)_0]$ is a quasi-isomorphism. Hence each global section of $\Omega^1(2z)_0$ has a class in $H^1_{\mathrm{dR}}(\mathcal{X}/\mathbb{Z}_p) \otimes R'$, which on the generic fiber is the class of a form of the second kind. Fiberwise $H^1(\Omega^1(z)) = 0$, so there is a section $\psi^1 = (t^{-2} + ct^{-1} + \cdots)dt$, and $c = 0$ by the residue theorem on the generic fiber. Write $[\psi^1] = \eta + w$ in $(\mathcal{L} \oplus W) \otimes R'$ and put $\psi := \psi^1 - \eta$. Uniqueness holds since $\mathcal{L} \cap W = 0$. The section z does not meet the closed point over $\bar{u}$, so ψ is regular there, which gives the expansion. Each step is compatible with base change along $\tau' \mapsto \tau'(z_0)$, and uniqueness over the point gives the last claim. □

Lemma 2.5. *Let b be a divisor of degree 0 on X over a finite extension L of $\mathbb{Q}_q$, let $z_0 \in X(L)$ lie outside $\operatorname{Supp} b$, and let τ be an integral parameter at $\bar{z}_0$, used as τ' in Lemma 2.4. Then $(\omega_b/d\tau)(z_0) = \int_b \psi_{z_0}$.*

Proof. We use the local symbols of Besser [9, Proposition 4.10], [4, Definition 2.4, Proposition 2.5], with the sign of [5, (2)]: for ω meromorphic and ρ of the second kind, $\Psi(\omega) \cup [\rho]$ is the sum over the singular points A of $-\operatorname{Res}_A(\omega(\int \rho + \int_{Q_0}^{A} \rho))$, where the first integral is the formal one with no constant term and Q_0 is a fixed base point. Take $\omega = \omega_b$ and $\rho = \psi_{z_0}$. Both classes lie in the isotropic $W \otimes L$, so the sum vanishes. At $A \in \operatorname{Supp} b$

the residue is $n_A \int_{Q_0}^{A} \psi_{z_0}$, and these add up to $\int_b \psi_{z_0}$ since $\deg b = 0$. At $A = z_0$ we have $\omega = (\omega/d\tau)(z_0)dt + O(t)dt$ and $\int \rho = -1/t + O(t)$, so the residue is $-(\omega_b/d\tau)(z_0)$. □

Proposition 2.6. *Let b be a $\mathbb{Q}_p$-rational divisor of degree 0 on every residue disc.*

(a) *If U' is a residue disc missing* $\operatorname{Supp} b$*, with integral parameter τ', then $\omega_b|_{U'} \in pO[[\tau']]d\tau'$.*

(b) *If b' is another such divisor and no residue disc meets both supports, then $h_p(b', b) \in p^2\mathbb{Z}_p$.*

Proof. (a) Let b_i be the part of b on a residue disc U_i. It is stable under $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_q)$ and of degree 0, so $b_i = A_i^+ - A_i^-$ with $A_i^{\pm}$ effective, stable and of equal degree. Let $\sum_{m,n} \kappa_{mn}^{(i)} \tau'^m \tau_i^n d\tau_i$ be the kernel of Lemma 2.4 at the pair of discs. For $z_0 \in U'$, a Coleman primitive of ψ_{z_0} on U_i is a local primitive, so by degree 0

$$\int_{b_i} \psi_{z_0} = \sum_{m,n} \kappa_{mn}^{(i)} \tau'(z_0)^m \, e_{n+1}^{(i)}, \qquad e_k^{(i)} := \frac{1}{k}\Big(\sum_{y \in A_i^+} \tau_i(y)^k - \sum_{y \in A_i^-} \tau_i(y)^k \Big).$$

By Lemma 2.3, $e_k^{(i)} \in pO$, and $e_k^{(i)} \to 0$. By Lemma 2.5, $\omega_b/d\tau'$ takes at z_0 the value of a power series in $\tau'(z_0)$ with coefficients in pO.

(b) The discs meeting $\operatorname{Supp} b'$ miss $\operatorname{Supp} b$, so on each of them $\omega_b = p\rho$ with ρ integral by (a). Coleman integration on a disc is local, so Lemma 2.3 gives $\int_{b'} \omega_b \in p^2 O$, and this lies in $\mathbb{Q}_p$. □

Corollary 2.7. *If b, b' are $\mathbb{Q}$-rational divisors of degree 0 on every residue disc at p and no residue disc meets both supports, then*

$$h([b], [b']) \equiv -\sum_{v \neq p} i_v(b, b') \log_p v \pmod{p^2\mathbb{Z}_p},$$

whenever the right side is p-integral. So h modulo p^2 does not depend on W at such b, b'.

In the language of the Poincaré biextension [55], the height $h([b], [b'])$ is the logarithm map of [23, §9.3] evaluated at the integral point over $([b], [b'])$, when $[b']$ lies in the identity component at every prime [22, Propositions 3.10 and 3.11], with $h_p(b, b')$ as its term at p; Proposition 2.6 (b) says that this term vanishes modulo p^2 when b, b' have degree 0 on every disc and no disc meets both.

Forms of the third kind and the height. The rest of the section assumes (B). By (B) the integer $N_p := \#\bar{J}(\mathbb{F}_p)$ is a unit, and it carries any $\mathbb{Q}_p$-rational divisor of degree 0 to one of degree 0 on every disc, up to the divisor of a function.

Lemma 2.8. *Assume* (B)*. Let D be a $\mathbb{Q}_p$-rational divisor of degree 0 and U a residue disc containing no point of D, with integral parameter τ. Then $\omega_D|_U \in O[[\tau]]d\tau$.*

Proof. As N_p kills $\bar{J}(\mathbb{F}_p)$, we have $N_p \bar{D} = \operatorname{div} \bar{f}$ with $\bar{f} \in \mathbb{F}_p(\bar{X})$. We lift $\bar{f}$ to a rational function f over $\mathbb{Q}_p$ with zeros and poles only in the discs of points of D. If $\bar{f}$ is constant take $f = 1$. Otherwise, points of $\bar{X}$ lift to horizontal divisors, as $\mathcal{X}$ is smooth, so there is a horizontal effective divisor $\mathcal{A}$ on $\mathcal{X}$ such that $\bar{\mathcal{A}}$ is supported on the poles of $\bar{f}$, is at least the polar divisor of $\bar{f}$, and has $H^1(\bar{X}, \mathcal{O}(\bar{\mathcal{A}})) = 0$. Then $H^0(\mathcal{X}, \mathcal{O}(\mathcal{A}))$ surjects onto $H^0(\bar{X}, \mathcal{O}(\bar{\mathcal{A}}))$, so $\bar{f}$ lifts to f. The poles of f lie on $\mathcal{A}$, and its zeros reduce to the zeros of the section $\bar{f}$ of $\mathcal{O}(\bar{\mathcal{A}})$, which are supported at residue points of D. On each disc the degree

of $\operatorname{div} f$ is the order of $\bar f$ at the residue point, so $D_1 := N_pD - \operatorname{div} f$ has degree 0 on every disc.

The form $N_p\omega_D - df/f$ has residue divisor D_1, and its image under Ψ lies in $W \otimes \mathbb{Q}_p$ since $\Psi(df/f) = 0$. So $N_p\omega_D = \omega_{D_1} + df/f$. On U, ω_{D_1} is divisible by p by Proposition 2.6, and f is a unit, so df/f is integral. As N_p is a unit, we are done. □

The classes we need come from the operator $B := p + 1 - T_p \in \mathbb{T}_p$. The curve of the correspondence T_p has fiber at p two copies of $\bar X$, the graphs of Frobenius F and of its transpose [19, VI, Theorem 6.9]. So $\bar T_p = F_* + F^*$ on divisors of $\bar X$, which is the congruence of Eichler and Shimura, and $\det(B \mid \mathcal{L}) = \prod_i (p + 1 - \alpha_i - \bar\alpha_i) = N_p$, where the $\alpha_i, \bar\alpha_i$ are the eigenvalues of Frobenius. Thus (B) says that B is a unit of $\mathbb{T}_p$. A rational divisor u, of any degree, is stable under Frobenius modulo p, so $\bar T_p \bar u = (1 + p)\bar u$. Hence Bu reduces to 0: it has degree 0 on every residue disc, and its class lies in $J(\mathbb{Q})$.

Proposition 2.9. *Assume* (B) *and* (Φ). *Then* $h(M, M) \subset p\mathbb{Z}_p$.

Proof. As B is a unit on M, it is enough to bound $h([b], c)$ for $b := Bu$, with u a rational divisor of degree 0 and $c \in J(\mathbb{Q})$. We move c away from b. Let $\mathcal{D}$ and $\mathcal{A}$ be horizontal divisors over $\mathbb{Z}_{(p)}$, $\mathcal{D}$ of class c and $\mathcal{A}$ effective of large degree with reduction missing the residue points of b. A section of $\mathcal{O}(\mathcal{D} + \mathcal{A})$ not vanishing at these points gives $c = [D']$ with no point of D' in a disc of b. By Lemma 2.8, $\omega_{D'}$ is integral on the discs of b, so $h_p(b, D') = \int_b \omega_{D'} \in p\mathbb{Z}_p$ by Lemma 2.3. For $\ell \neq p$ we have $\log_p \ell \in p\mathbb{Z}_p$. The symbol $i_\ell(b, D')$ is an integer at good ℓ, and at bad ℓ its denominator divides the exponent of the component group, which is prime to p by (Φ). □

The moving also shows that h modulo p^2 on $M \times M$ does not depend on W. For $a = [u]$ and $c = [u']$ take D' as above, with $b = Bu$ and class c; then BD' has class Bc, it has degree 0 on every disc, and its support lies over that of $\bar D'$, so Corollary 2.7 applies to Bu and BD'. As B is a unit, this covers $M \times M$.

3. The method

We prove Theorem 1.2, and then give a criterion that tests its hypotheses with two functionals modulo p. Assume (B), (Φ), (M), and let W be a $\mathbb{T}_p$-stable complement. Write $e_{\mathfrak{n}} \in \mathbb{T}_p$ for the idempotent of a block $\mathfrak{n}$, so that $M = \bigoplus_{\mathfrak{n}} M_{\mathfrak{n}}$ and $\mathrm{Lie} = \bigoplus_{\mathfrak{n}} \mathrm{Lie}_{\mathfrak{n}}$. Let $\mathfrak{m}$ be a block with $\mathbb{T}_{\mathfrak{m}} = \mathbb{Z}_p$. By (M), $\mathcal{L}_{\mathfrak{m}}$ is free of rank one over $\mathbb{Z}_p$, generated by a form $\omega_{\mathfrak{m}}$, and $S_{\mathfrak{m}} = S[\mathfrak{m}]$ is the line spanned by its reduction. Evaluation on $\omega_{\mathfrak{m}}$ identifies $\mathrm{Lie}_{\mathfrak{m}}$ with $\mathbb{Z}_p$, and $v_p(\log G)$ is taken through it.

Let $y \in X(\mathbb{Q})$ and let w be a parameter of $\mathcal{X}$ at $\bar y$ over $\mathbb{Z}_p$ vanishing at y. A rational point z in the disc of y has $w(z) \in p\mathbb{Z}_p$. Since $p \geq 5$, for $\rho = \sum_n r_n w^n dw \in \mathbb{Z}_p[[w]]dw$ and $v := v_p(w(z))$,

$$\int_y^z \rho = r_0 w(z) + \sum_{n \geq 1} \frac{r_n w(z)^{n+1}}{n+1}, \qquad v_p\Big(\frac{w(z)^{n+1}}{n+1}\Big) > v \quad (n \geq 1). \tag{3.1}$$

Let Z be an integer combination of double cosets $H\gamma H$, $\gamma \notin H$, and of T_n with n non-square and prime to Np (for n a square, T_n contains the diagonal, through the isogeny $[\sqrt{n}]$, the scalars lying in H; n non-square and $\gamma \notin H$ say that Z has no diagonal component, so that $\operatorname{Fix} Z$ is a divisor). It commutes with the T_q, $q \nmid N$, because an isogeny of degree prime to N is an isomorphism on $A[N]$. So on Lie it lies in $\mathrm{End}_{\mathbb{T}_p}(\mathrm{Lie}) = \mathbb{T}_p$, by (M), and as

$\operatorname{End} J \otimes \mathbb{Z}_p$ acts faithfully on $\operatorname{Lie} \otimes \mathbb{Q}_p$, it is an element of $\mathbb{T}_p$. In particular it is self-adjoint for h by Lemma 2.2, and $\theta(Z)$ has a meaning.

Lemma 3.1. *Let Z be as above and symmetric, let $y, z \in X(\mathbb{Q})$, and suppose that no term of Z passes through (y, y), (y, z), (z, y) or (z, z). At a prime $v \nmid N$, we have $i_v(z - y, \operatorname{Fix} Z - Z(y) - Z(z)) = 0$.*

Proof. The argument is local on the regular scheme $\mathcal{X} \times \mathcal{X}$ over the unramified closure of $\mathbb{Z}_v$. As $\gamma \notin H$ and n is not a square, the diagonal is not a component of Z. The closure of Z is a Cartier divisor, as the scheme is regular; let f be a local equation of it near the relevant points. Up to multiples of the irreducible fiber, $\operatorname{Fix} Z$ is the pull-back along the diagonal, and $Z(c)$ the pull-back along $c \times \mathrm{id}$. Multiples of the fiber do not change a symbol with $z - y$, which has degree 0. Hence $i_v(z, \operatorname{Fix} Z) = i_v(z, Z(z)) = \operatorname{ord}_v f(z, z)$ and $i_v(y, \operatorname{Fix} Z) = i_v(y, Z(y)) = \operatorname{ord}_v f(y, y)$, and $i_v(z, Z(y)) = \operatorname{ord}_v f(y, z)$, $i_v(y, Z(z)) = \operatorname{ord}_v f(z, y)$. As Z is symmetric, these last two agree, and all six terms cancel. □

This is the vanishing at good places behind the identity of Balakrishnan and Dogra [7, Theorem 6.3 and the proof of Theorem 1.2], who identify the height of a mixed extension attached to Z with $h(z - y, D)$, for the divisor D below. We need only the height, so the argument above is enough.

Proof of Theorem 1.2. Let $z \neq y$ satisfy the hypotheses, and put $P := z - y$, $v := v_p(w(z))$, $D_Z := \operatorname{Fix} Z - 2Z(y)$ and $D := \operatorname{Fix} Z - Z(y) - Z(z)$. As $\bar{z} = \bar{y}$ and the closure of each term of Z misses $(\bar{y}, \bar{y})$, no point of the disc of y is a fixed point of a term or the image of y or z under one, so the disc contains no point of D. By the Lefschetz formula $\deg \operatorname{Fix} Z = 2 \deg Z(c) - 2 \operatorname{Tr}(Z \mid \mathcal{L})$, as Z is symmetric, so D and D_Z have degree 0 by $\operatorname{Tr}(Z \mid \mathcal{L}) = 0$. We have $[D] = [D_Z] - ZP$. The points (y, y), (y, z), (z, y), (z, z) reduce to $(\bar{y}, \bar{y})$, so they lie on no term of Z. By Lemma 3.1 and the hypothesis at the primes dividing N, $h(P, [D]) = h_p(P, D)$. So

$$h_p(P, D) = h(P, [D_Z]) - h(P, ZP). \tag{3.2}$$

The left side. The disc of y contains no point of D, so ω_D is integral there by Lemma 2.8, and by (3.1), $v_p h_p(P, D) \geq v$.

The block. Let $\tau \in \mathbb{Z}_p$ with $e_{\mathfrak{m}} P = \tau G$. We have $\langle \log P, \omega_{\mathfrak{m}} \rangle = \int_y^z \omega_{\mathfrak{m}}$, and by (b) the coefficient r_0 of $\omega_{\mathfrak{m}}$ is a unit, so by (3.1) this has valuation exactly v. Since it equals $\tau \langle \log G, \omega_{\mathfrak{m}} \rangle$, we get $\log G \neq 0$. So $a := v_p(\log G) < \infty$, and $a \geq 2$ by (a), with $v_p(\tau) = v - a$ and $v \geq a$.

Off the block. Let $P' := (1 - e_{\mathfrak{m}})P$. By (3.1), $\log P' \in p^v (1 - e_{\mathfrak{m}}) \operatorname{Lie}$. By (a) the map $p^{-1} \log$ is an isomorphism from $(1 - e_{\mathfrak{m}})M$ onto $(1 - e_{\mathfrak{m}}) \operatorname{Lie}$, so $P' = p^{v-1} Q'$ with $Q' \in (1 - e_{\mathfrak{m}})M$.

The valuations. By Lemma 2.2 the blocks are orthogonal and Z is self-adjoint. It acts on G by some $\tilde{Z} \in \mathbb{Z}_p$, with $\tilde{Z} \in p\mathbb{Z}_p$ by $\theta(Z) = 0$. So (3.2) becomes (1.2):

$$h_p(P, D) = \tau\, h(G, [D_Z]) + p^{v-1} h(Q', [D_Z]) - \tau^2 \tilde{Z}\, h(G, G) - p^{2v-2} h(Q', ZQ').$$

By Proposition 2.9 and (c) the valuations of the terms, in order, are at least v; exactly $v - a + 1$; at least v; at least $2(v - a) + 2$; at least $2v - 1$. Since $a \geq 2$ and $v \geq a \geq 2$, the value $v - a + 1$ is strictly below the four others, which is a contradiction. □

Remark 3.2. Theorem 1.2 works at any genus at which the rank equals the genus, which (a) forces; what it needs is a Wieferich-type event on one block. The event in (a) makes the Mordell–Weil group one of bad reduction modulo p in the sense of [34, Definition 3.9] and

[22, Definition 8.3], one of the two cases in which, by [22, Theorem 8.5], the cohomological quadratic Chabauty set can be larger than the geometric one. At $a = 1$, the saturated case, one needs the local height as a function on the disc [23, 33], so the two methods are complementary. We apply Dogra's heuristic [20, §1.2], after Katz [43], to one block. Under (B), by Poonen's congruence [20, Lemma 3], a block of residue degree d is non-saturated exactly when the Wieferich class of a generator vanishes on it, a condition of codimension d; if these classes are random, this has chance p^{-d}. The Hecke field of an orbit of newforms, like any number field, has on average one prime of degree one over p, so the heuristic expects about $1/p$ non-saturated blocks at p from each orbit, whatever its dimension, and about $r \log\log x$ such primes up to x for r orbits. For (E, P_0) and primes $5 \le p \le 2 \cdot 10^7$, $p \ne 11$, a computation finds $p = 17$ and $p = 32411$. A non-saturated block at p settles only the classes whose CM field splits at p (Proposition 8.1), so at another level the heuristic turns on the number of orbits and on how the CM fields split.

A criterion. We now test (a) and the height condition in (c) without a generator. For a rational divisor u of any degree, Bu has degree 0 on every residue disc, so $\log[Bu] \in p\,\mathrm{Lie}$, and by Lemma 2.3 the functional

$$\lambda_u(\omega) := p^{-1} \int_{Bu} \tilde{\omega} \bmod p \qquad (\omega \in S)$$

does not depend on the lift $\tilde{\omega} \in \mathcal{L}$. It is the reduction of $p^{-1}\log[Bu]$ in $\mathrm{Lie}\,/p = \mathrm{Hom}(S, \mathbb{F}_p)$. For a block $\mathfrak{m}$ with $\mathbb{T}_\mathfrak{m} = \mathbb{Z}_p$ and rational divisors u, u', put

$$c_\mathfrak{m}(u, u') := p^{-1} h(e_\mathfrak{m}[Bu], [Bu']) \bmod p.$$

By Proposition 2.9 this lies in $\mathbb{F}_p$, and it does not depend on W. The map $T \mapsto p^{-1}h([Bu], T[Bu']) \bmod p$ is a functional on $\mathbb{T}/p$, and $c_\mathfrak{m}(u,u')\,\theta$ is its $\mathfrak{m}$-component, which is how we compute $c_\mathfrak{m}$. An element $t \in \mathbb{T}_p$ is self-adjoint and commutes with B, so when tu' is again a rational divisor,

$$c_\mathfrak{m}(u, tu') = \theta(t)\, c_\mathfrak{m}(u, u'). \tag{3.3}$$

Proposition 3.3. *Assume* (B), (Φ), (M) *and* $\operatorname{rank} J(\mathbb{Q}) \le g$. *Let* $\mathfrak{m}$ *be a block with* $\mathbb{T}_\mathfrak{m} = \mathbb{Z}_p$ *and character* θ. *Let* u *be a rational divisor with* $\lambda_u = 0$ *on* $S[\mathfrak{m}]$ *and* $\lambda_u \ne 0$ *on* $S[\mathfrak{n}]$ *for every other* $\mathfrak{n}$. *Let* Z *be a symmetric integer combination of double cosets* $H\gamma H$, $\gamma \notin H$, *and of* T_n *with* n *non-square and prime to* Np, *with* $\mathrm{Tr}(Z \mid \mathcal{L}) = 0$, $\theta(Z) = 0$ *and* $c_\mathfrak{m}(u, \operatorname{Fix} Z) \ne 0$. *Then* (a) *of Theorem 1.2 holds with* $G = e_\mathfrak{m}[Bu]$. *Also* $v_p h(G, G) = 1$, *and* $v_p h(G, [\operatorname{Fix} Z - 2Z(y)]) = 1$ *for every* $y \in X(\mathbb{Q})$.

Proof. For $\mathfrak{n} \ne \mathfrak{m}$ the image of λ_u in $\mathrm{Hom}(S_\mathfrak{n}, \mathbb{F}_p)$ is non-zero on the socle $S[\mathfrak{n}]$, so it generates this cyclic module over $\mathbb{T}_\mathfrak{n}/p$. By Nakayama, $p^{-1}\log e_\mathfrak{n}[Bu]$ generates $\mathrm{Lie}_\mathfrak{n}$ over $\mathbb{T}_\mathfrak{n}$, so $p^{-1}\log\colon M_\mathfrak{n} \to \mathrm{Lie}_\mathfrak{n}$ is surjective. By (M) the ranks of the $\mathrm{Lie}_\mathfrak{n}$ over $\mathbb{Z}_p$ add up to g, and $\mathrm{Lie}_\mathfrak{m}$ has rank one. Hence $\sum_{\mathfrak{n}\ne\mathfrak{m}} \operatorname{rank} M_\mathfrak{n} \ge g - 1$. As $c_\mathfrak{m}(u, \operatorname{Fix} Z) \ne 0$, also $M_\mathfrak{m} \ne 0$. With $\operatorname{rank} J(\mathbb{Q}) \le g$ and the absence of torsion in M, we get $M_\mathfrak{m} \cong \mathbb{Z}_p$ and $\operatorname{rank} M_\mathfrak{n} = \operatorname{rank} \mathrm{Lie}_\mathfrak{n}$ for $\mathfrak{n} \ne \mathfrak{m}$. Thus every $\mathfrak{n} \ne \mathfrak{m}$ is saturated.

Let G_0 generate $M_\mathfrak{m}$, and write $e_\mathfrak{m}[Bu] = \beta G_0$ and $e_\mathfrak{m}[B \operatorname{Fix} Z] = \beta' G_0$. Then $c_\mathfrak{m}(u, \operatorname{Fix} Z)$ is the reduction of $\beta\beta' p^{-1} h(G_0, G_0)$, where $h(G_0, G_0) \in p\mathbb{Z}_p$ by Proposition 2.9. Since it is non-zero, β and β' are units and $v_p h(G_0, G_0) = 1$. So $G := e_\mathfrak{m}[Bu]$ generates $M_\mathfrak{m}$ and $v_p h(G, G) = 1$. Since $\lambda_u = 0$ on $S_\mathfrak{m} = S[\mathfrak{m}]$, we have $\log G \in p^2\,\mathrm{Lie}_\mathfrak{m}$. This is (a).

Let $y \in X(\mathbb{Q})$ and $D_Z := \operatorname{Fix} Z - 2Z(y)$. As B is a unit acting on $M_\mathfrak{m}$ by a scalar, $v_p h(G, [D_Z]) = v_p h(G, B[D_Z])$. Now $B[D_Z] = [B \operatorname{Fix} Z] - 2Z[By]$, and $h(G, Z[By]) =$

$\tilde{Z}h(G,[By]) \in p^2\mathbb{Z}_p$ since $\tilde{Z} \in p\mathbb{Z}_p$. So $h(G, B[D_Z]) \equiv \beta' h(G, G_0)$ modulo p^2, of valuation 1. □

4. The height formula

We prove Theorem 1.3. An intersection number at v is a sum of lifting lengths over homomorphisms between reductions modulo v. The homomorphisms form a hermitian $\mathcal{O}_L$-module, and a count of Howard and Yang tells how many have a given x. The lifting length is a function of x by Gross's theorem on canonical liftings.

Fix D_1, D_2, n as in the theorem. Put $K_i := \mathbb{Q}(\sqrt{D_i})$ and $\mathcal{O}_i := \mathcal{O}_{D_i}$, and let σ be complex conjugation on L and $\mathrm{N} := \mathrm{N}_{L/F}$, so that $\mathrm{N}(\lambda) = \lambda\sigma(\lambda)$. Write $\sqrt{D} := \sqrt{D_1}\sqrt{D_2}$. As the discriminants are coprime, $\mathcal{O}_L = \mathcal{O}_1 \otimes \mathcal{O}_2$, $d_L = D^2$, and L/F is unramified at all finite primes [35, (19), p. 259]. Also $\mu_L = \mu_{K_1}\mu_{K_2}$ has order $w_1w_2/2$, since ζ_5, ζ_8 and ζ_{12} do not lie in such a field except for ζ_{12} at $\{D_1, D_2\} = \{-3, -4\}$, where $w_1w_2/2 = 12$. Let $\mathrm{CM}(D_i)$ be the set of A with $\mathrm{End}\, A = \mathcal{O}_i$, each with its action $[\cdot]$ on which $[a]^*\omega = a\omega$ for invariant differentials ω.

Homomorphisms as a hermitian module. Fix a prime v and a place of $\bar{\mathbb{Q}}$ over v, and reduce at it. If v splits in K_1 or K_2, then $\bar{A}_1$ and $\bar{A}_2$ are not isogenous, and the primes of F over v split in L, so no x has $v(x) = v$ and every number in the theorem at v is 0. From now on v is nonsplit in K_1 and K_2, so $\bar{A}_1, \bar{A}_2$ are supersingular. Put

$$\mathbf{H} = \mathbf{H}(A_1, A_2) := \mathrm{Hom}(\bar{A}_2, \bar{A}_1), \qquad (a \otimes b)\varphi := [a]\varphi[b],$$

a module over $\mathcal{O}_L$, and $\langle \varphi, \psi \rangle := \mathrm{Trd}(\varphi\hat{\psi})$, the polar form of deg, on $\mathbf{H} \otimes \mathbb{Q}$. Dual isogenies give $\langle \lambda\varphi, \psi \rangle = \langle \varphi, \sigma(\lambda)\psi \rangle$, so there is a unique form $\mathbf{h}$ with values in L, linear in the first variable and σ-hermitian, such that $\langle \varphi, \psi \rangle = \mathrm{Tr}_{L/\mathbb{Q}}\, \mathbf{h}(\varphi, \psi)$. Put

$$\nu(\varphi) := \sqrt{D}\, \mathbf{h}(\varphi, \varphi) \in F, \qquad x(\varphi) := \mathrm{Tr}_{F/\mathbb{Q}}\, \nu(\varphi).$$

Lemma 4.1. (a) $\mathbf{H}$ *is a projective* $\mathcal{O}_L$*-module of rank one, and* $\nu(\lambda\varphi) = \mathrm{N}(\lambda)\nu(\varphi)$ *for* $\lambda \in \mathcal{O}_L$.

(b) $x(\varphi) = \frac{1}{2}\,\mathrm{Trd}([\sqrt{D_1}]\varphi[\sqrt{D_2}]\hat{\varphi})$ *and* $\nu(\varphi) = \frac{1}{2}(x(\varphi) + \deg(\varphi)\sqrt{D})$.

(c) $x(\varphi) \in \mathbb{Z}$ *and* $x(\varphi) \equiv \deg(\varphi)D \bmod 2$, *so* $\nu(\varphi) \in \mathcal{O}_F$. *If* $\varphi \neq 0$ *then* $x(\varphi)^2 < \deg(\varphi)^2 D$, *so* $\nu(\varphi)$ *has opposite signs at the two real places.*

(d) *The ideal* $\mathfrak{c}(\mathbf{H})$ *of* $\mathcal{O}_F$ *generated by* $\nu(\mathbf{H})$ *is a prime of norm* v.

Proof. (a) $\mathbf{H}$ has rank 4 over $\mathbb{Z}$, since supersingular curves are isogenous, and $\mathbf{H} \otimes \mathbb{Q}$ is a module over the field L. The rest is the definition of $\mathbf{h}$.

(b) As $\mathbf{h}(\varphi, \varphi) \in F$, we have

$$\mathrm{Tr}_{F/\mathbb{Q}}\, \mathbf{h}(\varphi, \varphi) = \tfrac{1}{2}\langle \varphi, \varphi \rangle = \deg \varphi, \qquad x(\varphi) = \tfrac{1}{2}\,\mathrm{Tr}_{L/\mathbb{Q}}\, \mathbf{h}(\sqrt{D}\varphi, \varphi) = \tfrac{1}{2}\langle \sqrt{D}\varphi, \varphi \rangle.$$

Both claims follow.

(c) Put $n_0 := \deg \varphi$, $\alpha := [(D_1 + \sqrt{D_1})/2]$, $\beta := \varphi[(D_2 + \sqrt{D_2})/2]\hat{\varphi}$. Then $\mathrm{Trd}\, \alpha = D_1$, $\mathrm{Trd}\, \beta = n_0 D_2$, and expanding gives $x(\varphi) = 2\,\mathrm{Trd}(\alpha\beta) - n_0 D$. The element $y := [\sqrt{D_1}]\varphi[\sqrt{D_2}]\hat{\varphi}$ has reduced trace $2x(\varphi)$ and reduced norm $n_0^2 D$. It is not rational, as D_1/D_2 is not a square, and the quaternion algebra is definite, so its discriminant $4x(\varphi)^2 - 4n_0^2 D$ is negative.

(d) We compute the determinant of $\langle\, , \rangle$ on $\mathbf{H}$ twice. For each prime q there is an isogeny φ_q of degree prime to q, so $\mathbf{H} \otimes \mathbb{Z}_q = (\mathrm{End}\, \bar{A}_1 \otimes \mathbb{Z}_q)\varphi_q$ and the form is a unit times the reduced trace form of a maximal order, which is unimodular for $q \neq v$ and has determinant

v^2 times a unit for $q = v$. So the determinant is $\pm v^2$. On the other hand, write $\mathbf{H} = \mathfrak{A}\varphi_1$ with $\mathfrak{A}$ a fractional ideal of L, and put $\nu_1 := \nu(\varphi_1)$. Then $\langle \lambda\varphi_1, \mu\varphi_1\rangle = \mathrm{Tr}_{L/\mathbb{Q}}(\lambda\sigma(\mu)\nu_1/\sqrt{D})$, with determinant $\pm d_L \mathrm{N}_{L/\mathbb{Q}}(\nu_1/\sqrt{D})\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{A})^2 = \pm \mathrm{N}_{F/\mathbb{Q}}(\mathrm{N}(\mathfrak{A})\nu_1)^2$. Locally at primes of F the values of N on $\mathcal{O}_L$ generate $\mathcal{O}_F$, so $\mathfrak{c}(\mathbf{H}) = \mathrm{N}(\mathfrak{A})\nu_1$, which is integral by (c). Its norm is v. □

So $\deg\varphi = n$ and $x(\varphi) = x$ if and only if $\nu(\varphi) = \nu_x$.

Howard and Yang count these homomorphisms [36, §2]. With the indices 1 and 2 exchanged, their action [36, (2.1)] on $\mathbf{H}$ is ours composed with complex conjugation on $\mathcal{O}_2$, which acts on F as the conjugation $f \mapsto f'$. So their $\deg_{\mathrm{CM}}$ [36, Proposition 2.2] is, on $\mathbf{H}$, $\mathbf{h}(\varphi,\varphi)' = (\nu(\varphi)/\sqrt{D})'$, and the different of F is $\sqrt{D}\,\mathcal{O}_F$. Let $\mathfrak{v}_0$ be the conjugate of their reflex prime [36, Definition 2.8], that is, the prime of F below the kernel of the map $\mathcal{O}_L \to \bar{\mathbb{F}}_v$ sending $a \otimes b$ to the scalar by which $[a] \otimes [\bar{b}]$ acts on $\mathrm{Lie}\,\bar{A}_1 \otimes \mathrm{Lie}\,\bar{A}_2$. It depends only on the place over v, not on (A_1, A_2).

Lemma 4.2. *Put $e_v := 1$ if v splits in F and $e_v := 2$ if v ramifies in F. For every function f of $|x|$,*

$$\sum_{(A_1,A_2)} \sum_{\substack{\varphi \in \mathbf{H}(A_1,A_2) \\ \deg\varphi = n}} f(|x(\varphi)|) = \frac{w_1 w_2 e_v}{4} \sum_{v(x)=v} R(x) f(|x|),$$

and a φ of degree n with $x(\varphi) = x$ has $v(x) = v$ and $\mathrm{ord}_{\mathfrak{v}_0}\nu(\varphi) = b(x)$.

Proof. Let $\nu_0 \in \mathcal{O}_F$ have the signs of ν, so that $\alpha := \nu_0/\sqrt{D}$ is totally positive. The pairs (A_1, A_2) form one orbit of $\mathrm{Pic}\,\mathcal{O}_1 \times \mathrm{Pic}\,\mathcal{O}_2$, with trivial stabilizers [36, Remark 2.15, Lemma 2.16]. So by [36, Proposition 2.18, Theorem 2.21], as the number of ideals of $\mathcal{O}_L$ of given norm is invariant under $'$, the number of triples (A_1, A_2, φ) with $\nu(\varphi) = \nu_0$ is $\frac{1}{2}w_1w_2$ times the number of integral ideals $\mathfrak{B}$ of $\mathcal{O}_L$ with $\mathrm{N}(\mathfrak{B}) = \alpha\sqrt{D}\,\mathfrak{v}_0^{-1} = (\nu_0)\mathfrak{v}_0^{-1}$. In particular every value of ν on $\mathbf{H}(A_1, A_2)$ lies in $\mathfrak{v}_0$, and $\mathfrak{c}(\mathbf{H}(A_1, A_2)) = \mathfrak{v}_0$ by Lemma 4.1(d).

The prime $\mathfrak{v}_0$ is inert in L: the decomposition group of v in $\mathrm{Gal}(L/\mathbb{Q})$ maps onto those of K_1 and K_2. So the number of ideals $\mathfrak{B}$ for $\nu_0 = \nu_x$ is non-zero exactly when $\mathfrak{v}_0$ is the unique prime with $r_{\mathfrak{v}_0}(x) = 0$, and it is then $R(x)$. This proves the last sentence. We have $(\nu_{-x}) = (\nu_x)'$, and conjugation preserves the splitting in L, so R, v and b are even in x. If v splits in F, then for $v(x) = v$ exactly one of $x, -x$ has its prime equal to $\mathfrak{v}_0$, and $x = 0$ does not occur. If v ramifies, both do. Summing over x gives the formula. □

Lifting homomorphisms. Let $k := \bar{\mathbb{F}}_v$ and $W_0 := W(k)$. A *lifting ring* is the ring of integers W' of a finite extension of $\mathrm{Frac}\,W_0$, with uniformizer π. By Serre–Tate [42, Theorem 1.2.1], deforming a supersingular elliptic curve, or a homomorphism of two, is the same as deforming its formal group. Two homomorphisms of formal groups of finite height which agree modulo a nilpotent ideal are equal (*rigidity*).

Let $\bar{A}_1, \bar{A}_2$ be supersingular over k, let A_2 lift $\bar{A}_2$ to W', and let $\mathcal{E}$ over $R := W'[[t]]$ be the universal deformation of $\bar{A}_1$. For $\bar{\varphi}\colon \bar{A}_2 \to \bar{A}_1$ non-zero and a W'-point t_1, let $r(\bar{\varphi}) = r(\bar{\varphi}; A_2, t_1)$ be the largest r such that $\bar{\varphi}$ lifts to a homomorphism $A_2 \to \mathcal{E}_{t_1}$ over W'/π^r.

Lemma 4.3. *Let $\bar{\varphi}\colon \bar{A}_2 \to \bar{A}_1$ be non-zero.*

(a) *There is a smallest ideal I of R over whose quotient $\bar{\varphi}$ lifts to $A_2 \to \mathcal{E}$. It is principal, $I = (f)$ with $\pi \nmid f$, and $r(\bar{\varphi}; A_2, t_1) = \mathrm{ord}_\pi f(t_1)$.*

(b) *For a finite extension $W'' \supset W'$, f also generates the ideal of $\bar{\varphi}$ over $W''[[t]]$.*

(c) *The zeros of f in the maximal ideal of $\mathcal{O}_{\mathbb{C}_v}$ are simple. They are the points $t(A_2/C,\iota)$ attached to pairs (C,ι), where $C\subset A_2$ is a subgroup of order $\deg\bar\varphi$ and $\iota\colon \overline{A_2/C}\to\bar A_1$ is an isomorphism such that ι composed with the reduction of $A_2\to A_2/C$ is $\bar\varphi$.*

(d) *For a W'-point t_1, summing over the $\bar\varphi$ of degree n and over all subgroups C of order n, cyclic or not, and all ι,*

$$\sum_{\bar\varphi} r(\bar\varphi;A_2,t_1)=\sum_{(C,\iota)}\operatorname{ord}_\pi\bigl(t_1-t(A_2/C,\iota)\bigr).$$

Proof. (a), (b) By [56, Proposition 1.4], the locus in the deformation space $\operatorname{Spf} W_0[[t,t']]$ of the pair $(\bar A_1,\bar A_2)$ over which $\bar\varphi$ lifts is a divisor, with an equation g. This locus represents a functor, so it is compatible with base change. Its pull-back along $t'\mapsto t'(A_2)$ is the smallest ideal I of R over whose quotient $\bar\varphi$ lifts, so $I=(f)$ with f the image of g, and the same holds over $W''[[t]]$, which is (b). If $\pi\mid f$, then $\bar\varphi$ lifts over $k[[t]]$, which gives a non-zero homomorphism from a constant supersingular curve to an ordinary one, and this is impossible. Finally $R\to W'/\pi^r$, $t\mapsto t_1$, is onto, so a lift exists over W'/π^r if and only if $f(t_1)\equiv 0 \bmod \pi^r$.

(c) By (b), at a zero t_0 of f the homomorphism $\bar\varphi$ lifts to $\varphi\colon A_2\to\mathcal{E}_{t_0}$ over the integers of $W'(t_0)$. Then $C:=\ker\varphi$ on the generic fiber and the reduction ι of the induced isomorphism $A_2/C\cong\mathcal{E}_{t_0}$ give a pair. Conversely a pair gives a lift to the deformation $(A_2/C,\iota)$, and the two constructions are inverse by rigidity. At a double zero, φ would lift over $\mathcal{O}[\varepsilon]/\varepsilon^2$; inverting π, an isogeny in characteristic 0 from a constant curve has étale kernel, so $\mathcal{E}$ at $t_0+\varepsilon$ would be the constant deformation of A_2/C, against Kodaira–Spencer.

(d) By Weierstrass preparation, f is a unit times $\prod(t-t_0)$ over its simple zeros, and each pair belongs to exactly one $\bar\varphi$. □

Gross and Keating use the same ideals for triples of isogenies over the two-parameter ring [28, (3.13)–(3.16)].

Lemma 4.4. *Let $\mathcal{F}_1,\mathcal{F}_2$ be one-dimensional formal groups of finite height over a lifting ring W', and let $\varpi\in\operatorname{End}_{W'}(\mathcal{F}_1)$ have $\varpi'(0)=\pi$ a uniformizer. For $\bar\psi\colon\bar{\mathcal{F}}_2\to\bar{\mathcal{F}}_1$ non-zero, $r(\bar\varpi\bar\psi)=r(\bar\psi)+1$.*

Proof. Let val be the least valuation of the coefficients of a series, and $u(T)dT$ the invariant differential of $\mathcal{F}_1$. From $\varpi^*\omega=\pi\omega$ we get $\varpi'\in\pi W'[[T]]^\times$. So $\varpi(T)=\sum c_jT^j$ with $c_1=\pi$ and $\pi\mid c_j$ for $v\nmid j$. For $a\ge 1$ the series $\varpi(\pi^a d)/\pi^{a+1}$ is integral with linear coefficient 1, so it is invertible under composition. Hence for series with zero constant term: if $\operatorname{val}\varepsilon\ge 1$ then $\operatorname{val}\varpi(\varepsilon)=\operatorname{val}\varepsilon+1$, and if $\operatorname{val}\eta\ge a+1$ then $\eta=\varpi(\delta)$ with $\operatorname{val}\delta\ge a$.

For a series Y with zero constant term put $\Lambda_Y(T,T'):=Y(T+_{\mathcal{F}_2}T')-_{\mathcal{F}_1}(Y(T)+_{\mathcal{F}_1}Y(T'))$; then Y is a homomorphism modulo π^s if and only if $\operatorname{val}\Lambda_Y\ge s$, and $\Lambda_{\varpi\circ Y}=\varpi(\Lambda_Y)$. This gives $\ge$. Conversely, let $s\ge 2$ and let χ lift $\bar\varpi\bar\psi$ with $\operatorname{val}\Lambda_\chi\ge s$, and let Y_0 lift $\bar\psi$. Both χ and $\varpi\circ Y_0$ are homomorphisms modulo π^2 and they agree modulo π, so by rigidity $\eta:=\chi-_{\mathcal{F}_1}\varpi\circ Y_0$ has $\operatorname{val}\eta\ge 2$. Write $\eta=\varpi(\delta)$ with $\operatorname{val}\delta\ge 1$ and put $Y:=Y_0+_{\mathcal{F}_1}\delta$. Then Y lifts $\bar\psi$, $\varpi\circ Y=\chi$, and $\operatorname{val}\Lambda_Y\ge s-1$. □

This extends [65, Lemma 1.3] to two formal groups; the same step, for an isogeny of degree v between quasi-canonical liftings, is in the proof of [28, Lemma 5.11].

Now let $A_i\in\mathrm{CM}(D_i)$. The formal group $\mathcal{F}_i$ of A_i, with $\mathcal{O}_{i,v}:=\mathcal{O}_i\otimes\mathbb{Z}_v$, is a formal $\mathcal{O}_{i,v}$-module of height one, defined over the integers W_i of the completion of the maximal unramified extension of $K_{i,v}$. It is the canonical lifting of [27, Proposition 2.1]. Let W' be the compositum of W_1,W_2. It is W_0 if $v\nmid D$, and it has ramification index 2 over W_0 if

$v \mid D$. For $\varphi \in \mathbf{H}$ non-zero put $\rho_v(\varphi) := r(\varphi)/e_v$, with $r(\varphi)$ defined by A_2 and the point of A_1, and $b := \operatorname{ord}_{\mathfrak{v}_0} \nu(\varphi)$.

Lemma 4.5. *If $v \nmid D$, then $\rho_v(\varphi) = (b+1)/2$. If $v \mid D$, then $b = 1 + 2\operatorname{ord}_v(\deg\varphi)$ and $\rho_v(\varphi) = (b+1)/4$.*

Proof. We use [27, Proposition 3.3]: if $\mathcal{F}$ is the canonical lifting of height two for a quadratic $\mathcal{O} \supset \mathbb{Z}_v$ with uniformizer $\varpi_{\mathcal{O}}$, and $\mathcal{R} := \operatorname{End}(\bar{\mathcal{F}})$ is the maximal order, then $\operatorname{End}_{W'/\varpi_{\mathcal{O}}^r}(\mathcal{F}) = \mathcal{O} + \varpi_{\mathcal{O}}^{r-1}\mathcal{R}$.

Let $v \nmid D$. Then $\mathcal{O}_{1,v} \cong \mathcal{O}_{2,v} \cong \mathbb{Z}_{v^2} \subset W_0$ by the normalized actions, and uniqueness of the canonical lifting gives an isomorphism $\iota\colon \mathcal{F}_2 \to \mathcal{F}_1$ of formal $\mathbb{Z}_{v^2}$-modules over W_0. Then $\varphi' := \varphi\bar{\iota}^{-1}$ lies in $\mathcal{R} = \operatorname{End}(\bar{A}_1) \otimes \mathbb{Z}_v = \mathbb{Z}_{v^2} \oplus \mathbb{Z}_{v^2}\Pi$, where $\Pi a = \bar{a}\Pi$ and $\Pi^2 = v$, and $\deg\varphi = c\operatorname{Nrd}(\varphi')$ for a constant $c \in \mathbb{Z}_v^\times$. Write $\varphi' = \alpha + \beta\Pi$. By Gross's proposition, φ lifts modulo v^r if and only if $\operatorname{ord}_v\beta \geq r-1$, so $r(\varphi) = 1 + \operatorname{ord}_v\beta$. Let $s_i \in \mathbb{Z}_{v^2}$ be the image of $\sqrt{D_i}$ and $s := s_1 s_2 \in \mathbb{Z}_v$, a unit with $s^2 = D$. Since ι is $\mathbb{Z}_{v^2}$-linear and $\hat{\varphi} = c\bar{\iota}^{-1}\overline{\varphi'}$, with $\overline{\varphi'} = \bar{\alpha} - \beta\Pi$ the conjugate,

$$[\sqrt{D_1}]\varphi[\sqrt{D_2}]\hat{\varphi} = c\,s_1(\alpha+\beta\Pi)s_2(\bar{\alpha}-\beta\Pi) = c\,s(\alpha\bar{\alpha} + v\beta\bar{\beta} - 2\alpha\beta\Pi).$$

So $x(\varphi) = cs(\alpha\bar{\alpha}+v\beta\bar{\beta})$ and $\deg\varphi = c(\alpha\bar{\alpha}-v\beta\bar{\beta})$. In $F\otimes\mathbb{Q}_v = \mathbb{Q}_v\times\mathbb{Q}_v$, with $\sqrt{D} \mapsto (s,-s)$, this reads $\nu(\varphi) = c(s\alpha\bar{\alpha}, sv\beta\bar{\beta})$. Its order at the first prime is even and at the second it is $1+2\operatorname{ord}_v\beta$, and as α,β range over $\mathbb{Z}_{v^2}$ the second prime is $\mathfrak{v}_0$. Hence $b = 1+2\operatorname{ord}_v\beta$. This holds at $v=2$ too.

Let $v \mid D$. By duality, which preserves deg, x and the lifting length, v ramifies in K_1 and is inert in K_2, so $W' = W_1$. Let $\pi_1 \in \mathcal{O}_{1,v}$ be a uniformizer. It generates the maximal ideal of $\mathcal{R}$ and of $\mathcal{O}_{L,v} := \mathcal{O}_L \otimes \mathbb{Z}_v$, which is a discrete valuation ring. Hence $\operatorname{ord}_v(\deg\psi) = i$ if and only if $\psi \in \pi_1^i\mathbf{H}_v \setminus \pi_1^{i+1}\mathbf{H}_v$, with $\mathbf{H}_v := \mathbf{H}\otimes\mathbb{Z}_v$. Let $k' := \operatorname{ord}_v(\deg\varphi)$ and $\varphi = \pi_1^{k'}\varphi'$ with φ' an isomorphism $\bar{\mathcal{F}}_2 \to \bar{\mathcal{F}}_1$. As $\mathfrak{v}_0$ is inert in L and $\mathfrak{c}(\mathbf{H}) = \mathfrak{v}_0$, we get $b = 2k'+1$. By Lemma 4.4, $r(\varphi) = r(\varphi') + k'$. If φ' lifted modulo π_1^2, then $\gamma := \varphi'[(D_2+\sqrt{D_2})/2]\varphi'^{-1}$ would lie in $\mathcal{O}_{1,v} + \pi_1\mathcal{R}$ by the input. That ring acts on $\operatorname{Lie}\bar{\mathcal{F}}_1$ through $\mathbb{F}_v$, while γ acts by a generator of $\mathbb{F}_{v^2}$. Therefore $r(\varphi') = 1$ and $r(\varphi) = (b+1)/2$. □

Howard and Yang compute the same lengths from the same input [36, Lemmas 2.23 and 2.24].

The Cartan condition, and the proof of (a). Let ℓ be an odd prime, $\ell \nmid n$, $(D_i/\ell) = -1$, $e \geq 1$, $v \neq \ell$, and let $\mathfrak{c}_i$ be the action of $\mathcal{O}_i/\ell^e$ on $A_i[\ell^e] \cong \bar{A}_i[\ell^e]$.

Lemma 4.6. *For $\varphi \in \mathbf{H}(A_1,A_2)$ of degree n, we have $\varphi\mathfrak{c}_2\varphi^{-1} = \mathfrak{c}_1$ if and only if $\ell^{2e} \mid m_{x(\varphi)}$.*

Proof. We have $\operatorname{End}(\bar{A}_1)\otimes\mathbb{Z}_\ell = \operatorname{End}_{\mathbb{Z}_\ell}(\mathbb{Z}_{\ell^2}) = \mathbb{Z}_{\ell^2} \oplus \mathbb{Z}_{\ell^2}j$ with $\mathbb{Z}_{\ell^2}$ generated by $\alpha := [\sqrt{D_1}]$ and j its Frobenius, so $j^2 = 1$ and $ja = \bar{a}j$. The element $\beta := \varphi[\sqrt{D_2}]\hat{\varphi}$ has reduced trace 0, so $\beta = a_0\alpha + cj$ with $a_0 \in \mathbb{Z}_\ell$, $c \in \mathbb{Z}_{\ell^2}$. Then $\alpha\beta = x + t$, with $x = x(\varphi) = a_0D_1$ and $t := \alpha cj$ of reduced trace 0, and the reduced norm gives $t^2 = x^2 - n^2D = -4m_x$. As $t^2 = \alpha\bar{\alpha}c\bar{c} = -D_1c\bar{c}$, we get $c\bar{c} = 4m_x/D_1$, so $v_\ell(m_x) = 2v_\ell(c)$. Now $\varphi\mathfrak{c}_2\varphi^{-1}$ is generated by the image of β/n, and $\mathfrak{c}_1 \supseteq \varphi\mathfrak{c}_2\varphi^{-1}$ if and only if $\ell^e \mid c$, which is $\ell^{2e} \mid m_x$. In that case $a_0^2D_1 \equiv n^2D_2 \bmod \ell^e$, so a_0 is a unit and the inclusion is an equality. □

Proof of Theorem 1.3(a). The curve $X_{\mathrm{ns}}^+(\ell^e)$ has a smooth proper model over $\mathbb{Z}[1/\ell]$ [19, VI, Proposition 6.7], whose completed local ring at a geometric point $(\bar{A},\bar{\mathfrak{c}})$ of characteristic v is $W_0[[t]]^\Gamma$, with $\Gamma := \operatorname{Aut}(\bar{A},\bar{\mathfrak{c}})/\{\pm1\}$ [19, I, (8.2.1)]. So, by Weierstrass, two points meet over W'' with multiplicity $\sum_{\gamma\in\Gamma}\operatorname{ord}_\pi(t_1-\gamma t_2)/e(W'')$. As $T_n[A_2,\mathfrak{c}_2]$ is the sum of $[A_2/C,\mathfrak{c}_C]$

over all subgroups of order n, with $\mathfrak{c}_C$ the transport of $\mathfrak{c}_2$, the isomorphisms in this sum are the ι with $\iota\mathfrak{c}_C\iota^{-1} = \mathfrak{c}_1$, up to sign. With $\bar{\varphi} := \iota \circ \bar{\pi}_C$ this is a condition on $\bar{\varphi}$ alone, and Lemma 4.3(d) and Lemma 4.6 give

$$i_v(y(D_1), T_n y(D_2)) = \frac{1}{2} \sum_{(A_1,A_2)} \sum_{\substack{\deg \varphi = n \\ \ell^{2e} \mid m_{x(\varphi)}}} \rho_v(\varphi).$$

By Lemmas 4.5 and 4.2 this is $\frac{1}{2} \cdot \frac{1}{4} w_1 w_2 e_v \sum R(x)(b(x)+1)/(2e_v)$ over x with $v(x) = v$ and $\ell^{2e} \mid m_x$, which is (a). The same argument on the j-line, with no condition on φ, gives the formula on the j-line stated below under "Comparison with earlier formulas", since $\mathrm{ord}_v(j_1 - j_2)$ is the multiplicity of the two points there. □

The prime ℓ. Let $\ell \geq 7$ be a prime with $\ell \equiv 3 \bmod 4$. We work over $\mathbb{C}_\ell$, with $v(\ell) = 1$, and write $X_e := X_{\mathrm{ns}}^+(\ell^e)$ for $e \in \{1, 2\}$, and $d_e := \ell^{2e-1}(\ell-1)/2$ for its degree over the j-line.

Potentially good reduction. As $\ell \equiv 3 \bmod 4$, the dual graph of the semistable model of X_1 in [24, Theorem 3.5] has trivial homology, so $J(X_1)$ has potentially good reduction. By [13, Theorem 1.4], $J(X_1)$ is isogenous to the new part of $J_0(\ell^2)$ fixed by the Fricke involution, and $J(X_2)$ to $J(X_1)$ times the analogous new part at level ℓ^4, attached to newforms of level ℓ^4 with trivial character. A newform with trivial character whose local component at ℓ is a twist $\mathrm{St} \otimes \chi$ has $\chi^2 = 1$, so its level has valuation at most 2 at ℓ. So the ℓ'-adic representations of the newforms of level ℓ^4, for $\ell' \neq \ell$, have no monodromy at ℓ [11, Théorème (A)], and inertia at ℓ acts on them through a finite quotient. Hence $J(X_2)$ also has potentially good reduction [61, §2, Theorem 2(i)], and X_e^{an} is contractible. In particular, any two of its points are joined by exactly one arc.

The root. At the Gauss point of the j-line the universal curve is ordinary, so the decomposition group of a point of full level ℓ^e over it lies in the Borel subgroup of $\mathrm{SL}_2(\mathbb{Z}/\ell^e)$. It is the whole Borel. The diagonal part comes from the irreducibility of the Igusa curve [37, §3]. For the unipotent part, let H' be the unramified extension of the completed field at the Gauss point whose residue field κ' is the function field of the Igusa curve of level ℓ^e. Over H' the ℓ^e-torsion is an extension of $\mathbb{Z}/\ell^e$ by μ_{ℓ^e}, its étale quotient trivialized by the Igusa structure and its connected part identified with μ_{ℓ^e} by the Weil pairing with that structure, and so it is given by a unit q modulo ℓ^eth powers. At each ordinary point of the Igusa curve, q is then, modulo ℓ^eth powers, the Serre–Tate parameter $q(\alpha, \alpha)$ for α in the Tate module lifting the Igusa point, since Katz identifies the connected part with $\hat{\mathbb{G}}_m$ by the same Weil pairings and obtains $q(\alpha, \alpha)$ as the class of the extension of the étale part by the connected part [42, pp. 149–152, proof of Theorem 2.1]. Also $d \log q$ is the Kodaira–Spencer image of $\omega^{\otimes 2}$ for a suitable invariant differential ω [42, Main Theorem 3.7.1]. So $d \log \bar{q} \neq 0$, and $\bar{q}$ is not an ℓth power in κ', nor q in H', since an ℓth root of a unit is a unit; as $\mu_{\ell^e} \subset H'$, the Kummer extension $H'(q^{1/\ell^e})$ has degree ℓ^e, which is the whole unipotent part. Modulo ± 1 the Borel subgroup has order d_e and acts simply transitively on the non-split Cartan subgroups of $\mathrm{SL}_2(\mathbb{Z}/\ell^e)$, because the normalizer of such a subgroup in SL_2 is transitive on $\mathbb{P}^1(\mathbb{Z}/\ell^e)$, as -1 is not a square modulo ℓ. So there is a unique point of X_e^{an} over the Gauss point; this is the root of Theorem 1.3(b). Both steps use $\ell \equiv 3 \bmod 4$: for $\ell \equiv 1 \bmod 4$ two points lie over the Gauss point, and from $\ell = 17$ on $J(X_1)$ has positive toric rank [24, Theorem 3.5].

On divisors of degree 0. On a semistable model with dual graph a tree, the function $\sum n_P(\cdot|P)$ on the vertices is piecewise linear with Laplacian the reduction of $\sum n_P P$, whatever

the root, so it is the vertical correction in Néron's construction. Thus $\sum n_P n'_Q(P|Q)$ is the Néron symbol of two divisors of degree 0.

The tube. Let s be a supersingular j-invariant modulo ℓ, with curve $\bar{A}_s$ over $\bar{\mathbb{F}}_\ell$, and $\Gamma := \mathrm{Aut}(\bar{A}_s)/\{\pm 1\}$. It has order 1, or 2 if $s = 1728$, or 3 if $s = 0$, which is supersingular only for $\ell \equiv 2 \bmod 3$. So $\#\Gamma$ is 1 or a prime, and it is prime to ℓ and to d_e, as $(\ell-1)/2$ is odd. Let $\mathcal{D}$ be the open disc of deformations of the formal group of $\bar{A}_s$, over $W := W(\bar{\mathbb{F}}_\ell)$, and let $\xi_{a,r}$ be the Gauss point of $\{v(t-a) \geq r\}$. Every W-automorphism of $\mathcal{D}$ preserves the radius r, and for $r \leq 1$ the point $\xi_{a,r}$ for $a \in \ell W$ does not depend on a; we write ξ_r for it. Let Y be the rigid space of pairs $(t, \mathfrak{c})$ with $t \in \mathcal{D}$ and $\mathfrak{c}$ a Cartan subalgebra of $\mathrm{End}\,\mathcal{F}_t[\ell^2]$ with $\mathfrak{c} \cong \mathbb{Z}_{\ell^2}/\ell^2$, and $\mathrm{pr}\colon Y \to \mathcal{D}$ the projection, of degree d_2. The tube of s in X_2^{an} is Y/Γ. Let $t_0 \in \ell W$ be a canonical point, that is, one with an action of $\mathcal{O} := \mathbb{Z}_{\ell^2}$ on $\mathcal{F}_0 := \mathcal{F}_{t_0}$, and let $z_0 \in Y$ lie over t_0 with $\mathfrak{c} = \mathcal{O}/\ell^2$. Put

$$r_1 := \frac{\ell}{\ell+1}, \qquad r_2 := 1 + \frac{\ell}{\ell+1}.$$

The Hasse invariant has valuation $v(t-t_0)$ where this is less than 1 (see the proof below), so r_1 is the radius of the too-supersingular disc. For $s = 0$, resp. 1728, and t_0 the point with $j = s$, we have $v(t-t_0) = v(j)/3$, resp. $v(j-1728)/2$; when this is an integer it is the n_0 of Bisatt, Furio and Lombardo [10, Theorem 1.3(ii)]. They show, for $\ell > 7$ and $\ell > \sqrt{n_0+1}$, that a curve over $\mathbb{Q}_\ell$ with semistability defect at least 3 and image modulo ℓ in $N_{\mathrm{ns}}(\ell)$ has image modulo ℓ^{n_0} in $N_{\mathrm{ns}}(\ell^{n_0})$, and the full preimage above. That matches the multiplicities below at $n_0 = 1, 2$, as $r_1 < 1 < r_2 < 2$.

Lemma 4.7. *Along the path in Y from the end of Y to z_0, the map* pr *has multiplicity d_2 for $v(t-t_0) \in (0, r_1)$, multiplicity ℓ^2 on (r_1, r_2), and multiplicity* 1 *on (r_2, ∞) (see Figure 1).*

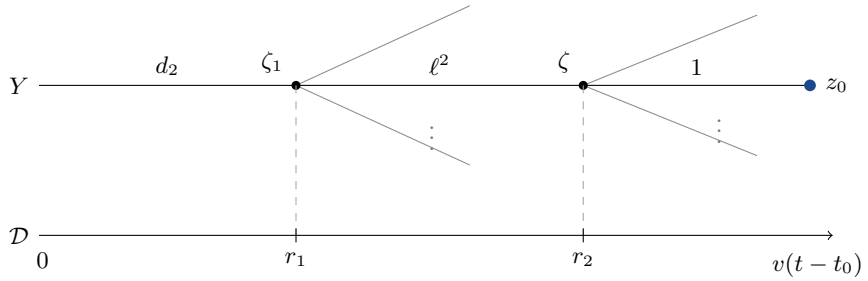


FIGURE 1. The map pr along the path from the end of Y to z_0. Each edge carries the multiplicity of pr. At ζ_1, over ξ_{r_1}, the path enters one of the d_1 pieces over $\{v(t-t_0) > r_1\}$; at ζ, over ξ_{t_0,r_2}, one of ℓ^2 branches. Lengths in Y are lengths in $\mathcal{D}$ divided by the multiplicity.

Proof. Take t centered at t_0 and write $[\ell]_t(x) = \sum_i a_i(t)x^i$. Modulo ℓ this is a series in x^ℓ whose coefficient of x^ℓ is the Hasse invariant, a uniformizer of $k[[t]]$. At $t = 0$ modulo ℓ it is a series in x^{ℓ^2} with non-zero first term. So $\ell \mid a_i$ for $\ell \nmid i$, $a_1 = \ell$, a_{ℓ^2} is a unit, $\ell \mid a_{\ell i}(0)$ for $i < \ell$, and $a_\ell(t) - a_\ell(0) = t\kappa(t)$ with κ a unit; in particular $v(a_\ell(t)) = v(t)$ if $v(t) < 1$. Fix ϖ with $a_{\ell^2}(0)\varpi^{\ell^2-1} = -\ell$, so $v(\varpi) = 1/(\ell^2-1)$. In $[\ell]_t(\varpi\varepsilon)/(a_{\ell^2}(0)\varpi^{\ell^2})$ the terms of degree 1 and ℓ^2 are $-\varepsilon$ and $(1 + O(t))\varepsilon^{\ell^2}$. The term of degree ℓ has valuation $v(a_\ell(t)) - r_1$, which is positive exactly when $v(t) > r_1$. For $1 < i < \ell$ the term of degree ℓi has valuation at least $\min(1, v(t)) + \ell(i-1)/(\ell^2-1) - r_1$, positive when $v(t) > r_1$, and the other terms have

positive valuation. So for $v(t) > r_1$ the series reduces to $\varepsilon^{\ell^2} - \varepsilon$, and $\mathcal{F}_t[\ell]$ has ℓ^2 distinct residues of x/ϖ. At $t = 0$ the map $x \mapsto \bar{u} := \overline{x/\varpi}$ is an $\mathcal{O}$-linear isomorphism $\mathcal{F}_0[\ell] \to \mathbb{F}_{\ell^2}$.

Level ℓ. Let $x_1 \in \mathcal{F}_0[\ell]$ be non-zero, and $v(t) = r > r_1$. The term $i = \ell$ dominates in $[\ell]_t(x_1) = \sum_i (a_i(t) - a_i(0))x_1^i$, which so has valuation $r + \ell/(\ell^2 - 1)$. Newton's polygon then gives a unique torsion point $x_1(t)$ with $\eta := x_1(t) -_{\mathcal{F}_t} x_1$ of valuation $r + \ell/(\ell^2 - 1) - 1 > 1/(\ell^2 - 1)$, namely $\eta = -t\kappa(0)x_1^\ell(1 + \cdots)/\ell$. The same estimates hold for the supremum norm on each closed disc $\{v(t) \geq r'\}$, $r' > r_1$: in its affinoid algebra, $\beta := -_{\mathcal{F}_t}[\ell]_t(x_1)$ has $v(\beta) \geq r' + \ell/(\ell^2 - 1)$, and $\eta \mapsto \ell^{-1}(\beta - \sum_{i \geq 2} a_i \eta^i)$ is a contraction of the ball $v(\eta) \geq r_\eta := r' + \ell/(\ell^2 - 1) - 1$, as $v(a_i) + (i-1)r_\eta > 1$ for all $i \geq 2$ (for $i = \ell$ this is $r' > r_1$). Its fixed point gives $x_1(t) = x_1 +_{\mathcal{F}_t} \eta$ as an analytic function of t, so $\mathcal{F}_t[\ell]$ splits over the disc $B := \{v(t) > r_1\}$. Thus $\mathrm{pr}^{-1}(B)$ is a disjoint union of d_1 pieces $Y^{(\bar{\mathfrak{c}})}$, one for each Cartan subalgebra $\bar{\mathfrak{c}} \cong \mathbb{F}_{\ell^2}$ modulo ℓ, each of degree ℓ^2 over B. We consider $Y^{(\bar{\mathfrak{c}}_0)}$ for $\bar{\mathfrak{c}}_0 := \mathcal{O}/\ell$, which contains z_0.

Level ℓ^2. Let $x_2 \in \mathcal{F}_0[\ell^2]$ with $[\ell]_0(x_2) = x_1$. A point of $\mathcal{F}_t[\ell^2]$ over $x_1(t)$ is $x_2 +_{\mathcal{F}_t} y$ with $[\ell]_t(y) = \delta := x_1(t) -_{\mathcal{F}_t} [\ell]_t(x_2)$, and $\delta = \eta(1 + \cdots)$ since $v([\ell]_t(x_2) - x_1) \geq r > v(\eta)$. Dividing by $a_{\ell^2}(0)\varpi^{\ell^2}$, of valuation $\ell^2/(\ell^2 - 1)$, with $y = \varpi\varepsilon$, the equation reduces to $\varepsilon^{\ell^2} - \varepsilon = \overline{\delta/(a_{\ell^2}(0)\varpi^{\ell^2})}$. If $v(t) > r_2$ then $v(\delta) > \ell^2/(\ell^2 - 1)$, the right side is 0, and by Hensel's lemma all of $\mathcal{F}_t[\ell^2]$ splits over $\{v(t) > r_2\}$. So pr has multiplicity 1 there. If $v(t) = r_2$, the equation reads

$$\varepsilon^{\ell^2} - \varepsilon = \varsigma\, \bar{u}_1^\ell,$$

with ς a coordinate on the residue line of ξ_{t_0,r_2} that does not depend on x_1. If $\varepsilon_0^{\ell^2} - \varepsilon_0 = \varsigma$, its solutions are $\bar{u}_1^\ell \varepsilon_0$ plus elements of $\mathbb{F}_{\ell^2}$, as $\bar{u}_1 \in \mathbb{F}_{\ell^2}$. Distinct torsion points have distinct residues, so the decomposition group of a point over ξ_{t_0,r_2}, in the cover of level ℓ^2 over B, consists of $1 + \ell A_w$ with $A_w(\bar{u}) = w\bar{u}^\ell$, $w \in \mathbb{F}_{\ell^2}$. The A_w are the conjugate-linear part $\mathfrak{p}$ of $\mathfrak{sl}_2(\mathbb{F}_\ell) = \bar{\mathfrak{c}}_0^0 \oplus \mathfrak{p}$, where $\bar{\mathfrak{c}}_0^0$ is the trace-zero part of $\bar{\mathfrak{c}}_0$. The Cartan subalgebras over $\bar{\mathfrak{c}}_0$ form a torsor under $\mathfrak{sl}_2(\mathbb{F}_\ell)/\bar{\mathfrak{c}}_0^0 \cong \mathfrak{p}$. So ξ_{t_0,r_2} has one preimage ζ in $Y^{(\bar{\mathfrak{c}}_0)}$.

At r_1. For $v(t) = r_1$ the same scaling gives $\varepsilon^{\ell^2} + c'\varepsilon^\ell - \varepsilon = 0$ with c' a coordinate on the residue line of ξ_{r_1}. The Moore determinant $\varepsilon_1\varepsilon_2^\ell - \varepsilon_1^\ell\varepsilon_2$ of a basis of solutions is a constant, since its $(\ell - 1)$st power is, up to sign, the product of the non-zero solutions. Ordered bases with a given value are the points of an irreducible plane curve, with free action of $\mathrm{SL}_2(\mathbb{F}_\ell)$ and quotient the c'-line. So the decomposition group G of a point of full level ℓ^2 over ξ_{r_1} maps onto $\mathrm{SL}_2(\mathbb{F}_\ell)$. Its kernel is a stable subspace of the irreducible module $\mathfrak{sl}_2(\mathbb{F}_\ell)$. It is not 0: a lift $g = u(1 + \ell A)$ of $u := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ to $\mathrm{SL}_2(\mathbb{Z}/\ell^2)$ has $g^\ell = u^\ell(1 + \ell \sum_{i<\ell} u^{-i} A u^i) = \left(\begin{smallmatrix} 1 & \ell \\ 0 & 1 \end{smallmatrix}\right)$, since the entries of $u^{-i}Au^i$ are polynomials of degree at most 2 in i and $\sum_{i<\ell} i^m \equiv 0 \bmod \ell$ for $m \leq 2 < \ell - 1$. So $G = \mathrm{SL}_2(\mathbb{Z}/\ell^2)$, which is transitive on the Cartan subalgebras, and ξ_{r_1} has one preimage ζ_1 in Y. In particular Y is connected, so by the uniqueness of the root Y/Γ is one direction at the root, and we may speak of the end of Y.

No branching between. We lift paths through the finite map pr, and use unique arcs in the tree X_2^{an}. Let $a, b \in Y$ lie over ξ_r, $0 < r < r_1$. Lifting $[\xi_r, \xi_{r_1}]$ from each ends at ζ_1, and lifting $[\xi_r, \xi_{r'}]$ with $r' \to 0$ tends to the root in X_2^{an}. Radii are preserved by Γ, so these give two arcs from the root to the image of ζ_1 in Y/Γ, mapped injectively to the j-line. They coincide, so a, b have one image in Y/Γ. Thus Γ is transitive on $\mathrm{pr}^{-1}(\xi_r)$, which has at most $\#\Gamma$ points of equal multiplicity with sum d_2. As $\#\Gamma$ is prime to d_2, there is one point, of multiplicity d_2. Now let $a, b \in Y^{(\bar{\mathfrak{c}}_0)}$ lie over $\xi_{t_0,r}$, $r_1 < r < r_2$. Lifting inside B from each ends at ζ, and lifting outward ends at ζ_1. The same argument gives $b = \gamma a$ with $\gamma \in \Gamma$. If $a \neq b$, then γ generates Γ, it preserves B as $r_1 < 1$, it preserves $Y^{(\bar{\mathfrak{c}}_0)}$ and it fixes $\xi_{t_0,r}$. So

the fiber is a Γ-orbit of points of equal multiplicity with sum ℓ^2, prime to $\#\Gamma$, and it has one point after all. □

For $e = 1$ the same argument, with Cartan subalgebras modulo ℓ, gives multiplicity d_1 on $(0, r_1)$ and 1 on (r_1, ∞). Lengths on Y are lengths on $\mathcal{D}$ divided by the multiplicity of pr: over a closed annulus in $\mathcal{D}$, pr is a finite étale morphism of nice compact curves, so it has a skeleton lying over that of the annulus, and along its edges the multiplicity is the absolute value of the slope of pr [16, 3.3.1, 3.5.11, Lemma 3.5.8(ii) and the proof of Lemma 3.6.10]. So the length in Y of the path to z_0 up to radius r is the function g_e of Theorem 1.3. For $e = 2$ it is $r_1/d_2 + (1 - r_1)/\ell^2 = 1/(\ell^2(\ell - 1))$ up to radius 1, plus $(r_2 - 1)/\ell^2 + (2 - r_2) = 1/\ell$ up to radius 2, plus $r - 2$; for $e = 1$ it is $r_1/d_1 + (1 - r_1) = 1/(\ell - 1)$ up to radius 1, plus $r - 1$.

Lemma 4.8. *Let $z, z' \in Y$ be points with complex multiplication by orders of conductor prime to ℓ in quadratic fields in which ℓ is inert, with their CM Cartan structures, and let $\rho := v(t_z - t_{z'}) \geq 1$. Then the Gromov product of z, z' from the end of Y is $g_2(\rho)$.*

Proof. The points $t_z, t_{z'}$ lie in W, and z, z' are fixed by $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell / \operatorname{Frac} W)$. On the fiber over t_z this group acts through all of $(\mathcal{O}/\ell^2)^\times$, by Lubin–Tate theory, with $\mathcal{O}$ the local ring of the field at z, and by conjugation on Cartan subalgebras. On $\mathfrak{sl}_2(\mathbb{F}_\ell) = \bar{\mathfrak{c}}_0^0 \oplus \mathfrak{p}$ it acts trivially on the first term and on $\mathfrak{p} \cong \mathbb{F}_{\ell^2}$ by multiplication by the norm-one group of order $\ell + 1$. As $(\ell + 1) \nmid (\ell - 1)$, this group has no stable $\mathbb{F}_\ell$-line and no non-zero fixed vector in $\mathfrak{p}$. So $\mathcal{O}/\ell$ is the only fixed Cartan subalgebra modulo ℓ, and $\mathcal{O}/\ell^2$ the only one over it. The same holds over t_0, with $\bar{\mathfrak{c}}_0$. Now $t_z, t_{z'} \in \ell W$ lie in B, and for $t \in B \cap W$ and σ in this group we have $\sigma(x_1(t)) = (\sigma x_1)(t)$, by the uniqueness of the fixed point in the proof of Lemma 4.7, since for $t \in W$ the series $\mathcal{F}_t$ and $[\ell]_t$ have coefficients in W. So the identification of $\mathcal{F}_t[\ell]$ with $\mathcal{F}_0[\ell]$ over B commutes with the group, and it carries the fixed Cartan subalgebra over t_z, and the one over $t_{z'}$, to $\bar{\mathfrak{c}}_0$. Hence z and z' both lie in $Y^{(\bar{\mathfrak{c}}_0)}$. If $\rho > r_2$, the same argument over $\{v(t - t_z) > r_2\}$, where all of $\mathcal{F}_t[\ell^2]$ splits by Hensel's lemma, with t_z as the canonical point, shows that z and z' lie in the same piece of its preimage. By Lemma 4.7 the paths to z and z' agree up to radius ρ. Past ρ their images differ. The argument for $e = 1$ is the same, with g_1. □

Proof of Theorem 1.3(b). Points in different tubes have Gromov product 0. For $P, Q \in Y$ with images $\bar{P}, \bar{Q}$ in Y/Γ, the map $Y \to Y/\Gamma$ expands a segment by the order of its stabilizer, and exactly that many translates of the path to Q pass through a given point of the path to P. So $(\bar{P}|\bar{Q}) = \sum_{\gamma \in \Gamma} (P|\gamma Q)_Y$. For $Q = (A_2/C, \mathfrak{c}_C)$ the structure $\mathfrak{c}_C$ is the CM one, as $\ell \nmid n$, and C is determined by $\bar{\pi}_C$. By Lemmas 4.8 and 4.3, with $\rho(\varphi) := r(\varphi)$,

$$i_\ell(y(D_1), T_n y(D_2)) = \frac{1}{2} \sum_{(A_1, A_2)} \sum_{\deg \varphi = n} g_e(\rho(\varphi)).$$

Here $\ell \nmid D$ and ℓ splits in F, so Lemmas 4.5 and 4.2 give

$$\tfrac{1}{2} \cdot \tfrac{1}{4} w_1 w_2 \sum_{v(x) = \ell} R(x)\, g_e\big((b(x) + 1)/2\big). \qquad \square$$

For $e \geq 3$, potentially good reduction and the root are proved in the same way, since no newform of level ℓ^{2k}, $k \geq 2$, with trivial character has a twist of Steinberg as local component at ℓ; what is missing for g_e is the analogue of Lemma 4.7 at the further radii $r_k := k - 1 + \ell/(\ell + 1)$, $3 \leq k \leq e$, namely that ξ_{t_0, r_k} has a single preimage in the cover of level ℓ^k.

Comparison with earlier formulas. On the j-line the proof of (a) gives, for every prime v,

$$\operatorname{ord}_v \operatorname{Res}(H_{D_1}, T_n H_{D_2}) = \frac{w_1 w_2}{8} \sum_{v(x)=v} R(x)\, \frac{b(x)+1}{2},$$

where $\operatorname{Res}(H_{D_1}, T_n H_{D_2})$ is the product of $j(A_1) - j(A_2/C)$ over A_i with $\operatorname{End} A_i = \mathcal{O}_{D_i}$ and subgroups $C \subset A_2$ of order n; this is the finite part of [29, Ch. V, §1, (1), p. 552], and [30, Theorem 1.3] at $n = 1$. For example, for $(D_1, D_2) = (-3, -67)$ and $n = 1$ the only x with $v(x) = 11$ are ± 5, with $m_x = 44$, and $i_{11} = 3/1210$ at $\ell = 11$, $e = 2$; on the j-line $\operatorname{ord}_{11}(5280^3) = 3$.

Part (a) at $n = 1$ is the local form of [52, Theorem C]. At $n = 1$ no two primes of F over one rational prime divide ν_x, so $b(x) = \operatorname{ord}_v m_x$; $R(x)$ is the number of maximal orders containing the Clifford order S_x of [52, (18)], by [52, Proposition 3.9]; and $R(x)(b(x)+1)/2$ is the coefficient of $\log v$ in the sum over $dd' = m_x/\ell^{2e}$ in their proof of Theorem C [52, pp. 21–22]. For $v \mid n$ both primes of F over a split v can divide ν_x, and then $b(x) < \operatorname{ord}_v m_x$: for $(D_1, D_2, n) = (-3, -4, 22)$ the resultant has valuation 6 at 11, and $\operatorname{ord}_{11} m_x$ in place of $b(x)$ would give 12. Their extension to non-maximal orders [52, Proposition 3.15] excludes primes dividing the conductor, so it does not reach $v \mid n$. At level one, Lauter and Viray [49, Theorems 1.1 and 1.5] treat such primes for singular moduli of arbitrary discriminants, which include the $H_{D_2 f^2}$, $f \mid n$, that make up $T_n H_{D_2}$.

At $v = \ell$ part (b) and [52, Theorem C] compute different quantities. At $n = 1$ theirs is the intersection number on their smooth model [52, Theorem A]; at $e = 2$ its coefficient of $R(x) \log \ell$ is $(b(x) - 3)/2$, from their level $N = \ell^2$, and only x with $\ell^4 \mid m_x$, so with $b(x) \geq 5$, occur. Part (b) is the Néron symbol, which also has the vertical part: for $b(x) \geq 5$ its coefficient is $g_2((b(x)+1)/2) = (b(x) - 3)/2 + 1/\ell + 1/(\ell^2(\ell - 1))$, and x with $b(x) = 1, 3$ contribute $g_2(1)$ and $g_2(2)$. The height needs these terms. At $\ell = 11$, $e = 1$ and $n = 1$, part (b) also follows from [52, Theorem B], through [52, Propositions 2.31, 2.32], together with the vertical correction, which the semistable model of [24, Theorem 3.5] determines: that of a fiber of type III [52, Example 1.1].

The height at CM divisors. The proof of (b) shows that T_n is self-adjoint for i_ℓ on CM divisors in every degree: $\sum_C (P/C|Q)$ and $\sum_{C'} (P|Q/C')$ are both half the sum of g_e over the isogenies $\bar{Q} \to \bar{P}$ of degree n. For $v \neq \ell$ this is the projection formula. For $v \neq p$ we have $\log_p v \equiv -p\, q_p(v) \bmod p^2$, with $q_p(v) := (v^{p-1} - 1)/p$.

Proposition 4.9. *Let $X = X_{\mathrm{ns}}^+(121)$ and $p \nmid 2 \cdot 3 \cdot 5 \cdot 11$ a prime satisfying* (B) *and* (Φ). *Let D_1, D_2 be as above with $(D_i/11) = -1$ and D_1 split at p. For $n \geq 1$ prime to 11 put*

$$\mathcal{A}(n) := \frac{w_1 w_2}{8} \left(\sum_{\substack{v(x) \neq 11, p \\ 11^4 \mid m_x}} R(x)\, \frac{b(x)+1}{2}\, q_p(v(x)) + q_p(11) \sum_{v(x)=11} R(x)\, g\Big(\frac{b(x)+1}{2}\Big) \right),$$

the sum over the x of n, with $g := g_2$ of Theorem 1.3(b) *at $\ell = 11$, that is, $g(1) = \frac{1}{1210}$ and $g(r) = r - 2 + \frac{1}{11} + \frac{1}{1210}$ for $r \geq 2$. Then for m prime to $11p$,*

$$p^{-1} h(By(D_1), T_m By(D_2)) \equiv \mathcal{A}(m) - 2\mathcal{A}(mp) + \mathcal{A}(mp^2) \pmod{p}.$$

Proof. The reductions of points of $y(D_1)$ are ordinary with endomorphism algebra K_1, and those of points of $T_m By(D_2)$ are isogenous to reductions of curves with K_2 in their endomorphism algebra, so they are different points. So (1.3) applies. By self-adjointness, $i_v(By(D_1), T_m By(D_2)) = i_v(y(D_1), B^2 T_m y(D_2))$ for $v \neq p$, and $T_p^2 = T_{p^2} + p$ gives $B^2 T_m \equiv$

$T_m - 2T_{mp} + T_{mp^2}$ modulo p. The denominators of g and of $w_1w_2/8$ are prime to p, and Theorem 1.3 gives the sum over $v \neq p$. □

5. Correspondences that change only the Cartan subgroup

Let $X = X_{\mathrm{ns}}^+(121)$ and $H := N_{\mathrm{ns}}(121)$. The correspondences we use replace the Cartan subgroup and fix the elliptic curve. So they preserve j, which Section 9 uses to make the term at 11 vanish, and their fixed points can be counted by hand.

As -1 is a non-residue modulo 11, a non-split Cartan subring of $\operatorname{End} A[121]$ is $(\mathbb{Z}/121)[x]$ for exactly one pair $\pm x$ with $x^2 = -1$, and every such pair arises. So a point of X off the cusps is a class $[A, \pm x]$ modulo $\operatorname{Aut} A$, with 6655 pairs $\pm x$ on each A. A double coset of H is an orbit of the stabilizer of $\pm x$ on these pairs, and its correspondence sends $[A, \pm x]$ to the sum of $[A, \pm x']$ over the orbit.

To name the orbits, write $x' = Cx + w$ with $C := -\frac{1}{2}\operatorname{tr}(xx')$ and w anticommuting with x, so that $w^2 = C^2 - 1$. Let $\mathfrak{c} := (\mathbb{Z}/121)[x]$. The elements anticommuting with x form a free $\mathfrak{c}$-module on a generator w_0 with w_0^2 a unit, and $(rw_0)^2 = \mathrm{N}(r)w_0^2$. Conjugation by $r \in \mathfrak{c}^\times$ fixes x and multiplies w by $r/\bar{r}$, which runs over the norm-one group of $\mathfrak{c}$, of order 132.

If $C \not\equiv \pm 1 \bmod 11$, then w is a unit, so the pairs $\pm x'$ with $\pm\frac{1}{2}\operatorname{tr}(xx') = \pm C$ form one orbit. We write R_C for it, with $C \in (\mathbb{Z}/121)/\pm$. It has 132 elements, or 66 if $C = 0$, where w and $-w$ give one pair. If $C \equiv \pm 1 \bmod 11$, then $w \equiv 0 \bmod 11$, since the norm is anisotropic modulo 11. So $C = \pm 1$ and $x' = \pm(x + 11w)$ with w anticommuting with x modulo 11, and $\nu := w^2 \in \mathbb{F}_{11}$ names the orbit: $\nu = 0$ is $x' = \pm x$, and for $\nu \neq 0$ we write S_ν, with 12 elements. These are the 61 orbits: the identity, 50 values of C and 10 of ν.

Let T be one of the R_C, S_ν. It preserves the j-invariant. It is defined over $\mathbb{Q}$, because Galois acts on $A[121]$ by group automorphisms, which preserve C and ν. It is symmetric, because $\operatorname{tr}(xx') = \operatorname{tr}(x'x)$ and $x = \pm(x' - 11w)$. By Section 3 it lies in $\mathbb{T}_p$ when (M) holds. Let $\mathbf{C}$ be the sum of the 55 cusps of X. The pull-back of ∞ from the j-line is $121\mathbf{C}$, and $T_p\infty = (p+1)\infty$, so $T_p\mathbf{C} = (p+1)\mathbf{C}$, that is,

$$B\mathbf{C} = 0. \tag{5.1}$$

On the curve at $j = 1728$ and at $j = 0$ let x_0 be the CM generator, namely i and $(2\omega + 1)/\sqrt{3}$ with $\sqrt{3} \in \mathbb{Z}/121$; the points $y(-4)$ and $y(-3)$ are the classes of $\pm x_0$. For $x = Cx_0 + w$ we have $ixi^{-1} = Cx_0 - w$ and, as $w\omega = \bar{\omega}w$, $\omega x\omega^{-1} = Cx_0 + \omega^2 w$. Taking traces,

$$\pm\tfrac{1}{2}\operatorname{tr}(x \cdot ixi^{-1}) = \pm(2C^2 - 1), \qquad \pm\tfrac{1}{2}\operatorname{tr}(x \cdot \omega x\omega^{-1}) = \pm\tfrac{1}{2}(3C^2 - 1).$$

So the orbit of $\pm ixi^{-1}$ relative to x depends only on the orbit U of x relative to x_0. Call it $F_4(U)$, and define $F_3(U)$ in the same way from ω. For $x = x_0 + 11w$ we get $ixi^{-1} = x - 22w$ and $\omega x\omega^{-1} = x + 11(\omega^2 - 1)w$, with $\mathrm{N}(\omega^2 - 1) = 3$, and for $C = 11c \neq 0$ we get $-ixi^{-1} = x - 22cx_0$. Therefore

$$F_4(R_C) = R_{2C^2-1} \ \ (11 \nmid C), \qquad F_4(R_{11c}) = S_{-4c^2}, \qquad F_4(S_\nu) = S_{4\nu},$$
$$F_3(R_C) = R_{(3C^2-1)/2}, \qquad F_3(S_\nu) = S_{3\nu};$$

here $(3C^2 - 1)/2 \not\equiv \pm 1 \bmod 11$ as -4 is a non-residue. Let F_4^*T be the sum of the orbits U with $F_4(U) = T$, and F_3^*T likewise for the second (the identity and R_0 have no image under the first map, since there $ixi^{-1} = \pm x$; the identity has none under the second). Put $n(R_C) := \#\{m \neq 0 \bmod 121 : 1 + m^2/2 = \pm C\}$, and $n(S_\nu) := 2$ if ν is a square and 0 if not.

Proposition 5.1. *For $T = R_C$ or S_ν, the fixed points of T lie over $j = 0, 1728, \infty$, and*

$$\operatorname{Fix} T = \tfrac{1}{2}(F_4^* T)\, y(-4) + \tfrac{2}{3}(F_3^* T)\, y(-3) + n(T)\mathbf{C}, \qquad \operatorname{Tr}(T \mid \mathcal{L}) = \deg T - \tfrac{1}{2}\deg \operatorname{Fix} T.$$

Proof. Off the cusps, a branch of the curve of T at (P, P), $P = [A, \pm x]$, is an x' in the orbit with $x' = \pm\alpha x \alpha^{-1}$, $\alpha \in \operatorname{Aut} A$. As $x' \neq \pm x$, we have $\alpha \neq \pm 1$, so $j(A) \in \{0, 1728\}$. Then P has the deformation disc of A as a neighborhood, with a parameter s on which $\operatorname{Aut} A$ acts linearly, and the branch is the graph of α^{-1}.

At $j = 1728$, a point with $ixi^{-1} \neq \pm x$ has one branch, $s \mapsto -s$, transversal to the diagonal. It occurs once in $\operatorname{Fix} T$ if $T = F_4(U)$ for its orbit U, and twice in $Uy(-4)$, since i fixes x_0. This gives the factor $\frac{1}{2}$. No T fixes a point with $ixi^{-1} = \pm x$.

At $j = 0$, a point with $x \neq \pm x_0$ has two branches, $s \mapsto \zeta_3^{\pm 1} s$, in one orbit, because conjugating by ω gives $\operatorname{tr}(x \cdot \omega^2 x \omega^{-2}) = \operatorname{tr}(\omega x \omega^{-1} \cdot x)$. It occurs twice in $\operatorname{Fix} T$ if $T = F_3(U)$, and three times in $Uy(-3)$. This gives the factor $\frac{2}{3}$. The pair $\pm x_0$ is the only one fixed by ω, and no T fixes it.

At a cusp, take $u = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $x = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$; here c is a unit, since $a^2 + bc = -1$ has no solution with $11 \mid c$. The branches are $x' = u^m x u^{-m}$, $m \neq 0 \bmod 121$, and in the parameter $q^{1/121}$ they are multiplications by ζ_{121}^m, so transversal. We have $\operatorname{tr}(xx') = -2 - m^2 c^2$, so $C = \pm(1 + (mc)^2/2)$. For $m = 11m'$ we have $x' = x + 11m'(ux - xu)$ and $\nu = (m'c)^2$. As $m \mapsto mc$ is a bijection, T has $n(T)$ branches at each cusp.

Finally $\deg \operatorname{Fix} T = 2 \deg T - \operatorname{Tr}(T \mid H^1_{\mathrm{dR}})$, and the trace on H^1_{dR} is $2 \operatorname{Tr}(T \mid \mathcal{L})$, as T is symmetric. □

Solving the equations above gives Table 1, the correspondences of Section 11.

T	$\deg T$	$F_4^* T$	$F_3^* T$	$n(T)$	$\operatorname{Tr}(T \mid \mathcal{L})$
S_{-1}	12	$S_8 + R_{55}$	S_7	0	-28
S_1	12	S_3	S_4	2	-50
R_{50}	132	$R_6 + R_{36}$	0	0	66
R_{18}	132	R_{42}	$R_{39} + R_{59}$	2	-44
R_2	132	R_{51}	R_{52}	2	0

TABLE 1. Five correspondences on $X_{\mathrm{ns}}^+(121)$.

6. Differentials without an equation

We now make S, the T_q and the functionals λ_u explicit on $X = X_{\mathrm{ns}}^+(121)$, with no equation for X. Throughout, $p \geq 5$ and $p \neq 11$. The differentials are products of two Eisenstein series of weight one, and their jets at a CM point come from a differential system satisfied by those series.

The forms. Let $O := (\mathbb{Z}/121)[i]$ with $i^2 = -1$, a local ring with residue field $\mathbb{F}_{121}$. Identify $x = d + ci \in O$ with the row vector $\underline{x} := (c, d)$ and put $\mathrm{N}(x) := c^2 + d^2$. Multiplication by units gives the Cartan subgroup, and with $\operatorname{diag}(1, -1)$ its normalizer H. Put $\zeta := e^{2\pi i/121}$, $t := e^{2\pi i\tau/121}$ and $\xi_s := \zeta^s + \zeta^{-s}$. For $v = (c, d) \neq 0$ in $(\mathbb{Z}/121)^2$ put $z_v := (c\tau + d)/121$ and

$$\mathbf{e}_v(\tau) := \frac{1}{2\pi i}\Big(\zeta_{\mathrm{W}}(z_v) - \frac{c\eta_2 + d\eta_1}{121}\Big),$$

where ζ_{W} is the Weierstrass function of $\mathbb{Z}+\mathbb{Z}\tau$ and η_1,η_2 are its quasi-periods. This is Hecke's Eisenstein series of weight one. It has the expansion

$$\mathbf{e}_{(c,d)} = C(c,d) + \sum_{n\geq 1}\Big(-\sum_{\substack{kr=n\\ r\equiv c}}\zeta^{dk} + \sum_{\substack{kr=n\\ r\equiv -c}}\zeta^{-dk}\Big)t^n,$$

with $C = c/121 - \frac{1}{2}$ for $0<c<121$ and $C=(\zeta^d+1)/(2(\zeta^d-1))$ for $c=0$. It satisfies $\mathbf{e}_{-v}=-\mathbf{e}_v$ and $\mathbf{e}_v|\gamma = \mathbf{e}_{v\gamma}$ for $\gamma\in\mathrm{SL}_2(\mathbb{Z})$. For $a\in\mathbb{Z}$ and $\rho\in O^\times$ put $\mathbf{e}_x := \mathbf{e}_{\underline{x}}$ and

$$F_{a,\rho} := \sum_{x\in O^\times} \xi_{a\mathrm{N}(x)}\,\mathbf{e}_x(\mathbf{e}_{\rho x}+\mathbf{e}_{\bar\rho x}), \qquad \omega_F := F\,\frac{dq}{q} = 121F\,\frac{dt}{t}.$$

We use the 780 forms with $a=1,\dots,60$ and $\rho = 1+i,\ 2+3i,\ 5+i,\ 3+2i,\ i,\ 1+2i,\ 4+i,\ 7+3i,\ 10+i,\ 1+5i,\ 6+7i,\ 2+9i,\ 12+5i$; those with $\rho=i$ are 0, as $\mathbf{e}_{-v}=-\mathbf{e}_v$. Over $\mathbb{C}$, generation by weight-one forms goes back to Khuri-Makdisi [45, Theorem 5.1]; here the span comes from a rank test.

Let $\mathcal{X}/\mathbb{Z}_{(p)}$ be the smooth model [19, VI, Proposition 6.7], and $\mathcal{L}^c := H^0(\mathcal{X},\Omega^1(\mathrm{cusps}))$, free of rank $g+54=565$ since there are 55 cusps. For $\omega\in\mathcal{L}^c\otimes\mathbb{Z}_{(p)}[\zeta]$ write $\omega = 121\sum_n c_n(\omega)t^n dt/t$, and let σ_a be the automorphism $\zeta\mapsto\zeta^a$.

Proposition 6.1. (a) *Each ω_F lies in $\mathcal{L}^c$.*

(b) *If the expansions of the 780 forms have rank 565 modulo p, then they span $\mathcal{L}^c$ over $\mathbb{Z}_{(p)}$.*

(c) *In that case $S=\{\omega\in\mathcal{L}^c/p : c_0(\omega)=0\}$, and each element of S lifts to a combination of the ω_F lying in $\mathcal{L}$.*

(d) *For a prime $q\neq 11$, $c_n(T_qF) = \sigma_q^{-1}(c_{qn}(F)) + q\sigma_q(c_{n/q}(F))$.*

Proof. (a) With the action $F^{\mathrm{diag}(1,b)}=\sigma_b F$ on forms with coefficients in $\mathbb{Q}(\zeta)$ we have $\mathbf{e}_v^g = \mathbf{e}_{vg}$ for all $g\in\mathrm{GL}_2(\mathbb{Z}/121)$. For $u\in O^\times$, the matrix of multiplication by u has determinant $\mathrm{N}(u)$, and the substitution $x'=xu$ shows that $F_{a,\rho}$ is invariant; $\mathrm{diag}(1,-1)$ sends $\underline{x}$ to $\underline{-\bar x}$, and $x'=\bar x$ shows the same. So ω_F is defined over $\mathbb{Q}$ on X, with at most simple poles at the cusps. The stabilizer of the cusp ∞ in $H\cap\mathrm{SL}_2(\mathbb{Z}/121)$ is $\{\pm1\}$, so t is a formal parameter along ∞ [44, Theorem 10.9.1]. The coefficients of $\mathbf{e}_v$ lie in $\mathbb{Z}_{(p)}[\zeta]$, and a form with integral expansion at a cusp on each component is integral.

(b) We have $\mathcal{L}^c/p = H^0(\bar X,\Omega^1(\mathrm{cusps}))$, on which the expansion is injective. So the reductions span and Nakayama applies.

(c) The group $\mathrm{Gal}(\mathbb{Q}(\zeta)^+/\mathbb{Q})$ acts simply transitively on the 55 cusps, through $\mathrm{N}(x)$. So if ω is rational and $c_0(\omega)\equiv 0$, all residues of ω vanish modulo p, and ω is regular modulo p. By base change on the smooth proper curve, $\mathcal{L}/p = H^0(\bar X,\Omega^1)$.

(d) Regard F as a function of the lattice $\Lambda=\mathbb{Z}\tau+\mathbb{Z}$ and the O-linear level structure $x\mapsto z_{\underline{x}}$, of degree -2, and T_qF as $q^{-1}\sum F(\Lambda',\psi')$ over $\Lambda'\supset\Lambda$ of index q. For $\Lambda'=\mathbb{Z}(\tau+b)/q+\mathbb{Z}$ with $b\equiv 0 \bmod 121$ the Weil pairing is multiplied by q, so the term is $F^{\mathrm{diag}(q,1)}((\tau+b)/q)$ with $F^{\mathrm{diag}(q,1)}=\sigma_q^{-1}F$, as $qI\in H$. Summing over b gives the first term. For $\Lambda'=\mathbb{Z}\tau+\mathbb{Z}/q$ the term is $q^2(\sigma_qF)(q\tau)$, which gives the second. □

A computation in C and python-flint (Appendix A) gives the rank 565 on $c_0,\dots,c_{19}$ at $p=17,43$; the rank of c_0 alone is 54, so S has dimension 511, the genus. By (d) the T_q are then matrices on S computed from coefficients of the 780 products. As $B\equiv 1-T_p$ modulo p, the condition (B) is $\mathrm{rank}(1-T_p \mid S)=511$, and the computation gives this at both primes. The joint primary components of S under the T_q are the blocks. There are 24 at $p=17$, already for $q\in\{2,3,7,13,19,23\}$, and 87 at $p=43$, for the primes

$q \le 41$, $q \ne 11$, and each has dimension equal to its residue degree. With exponents for multiplicities, the dimensions are $1, 5^9, 10^3, 15, 20^3, 25^2, 35^2, 40^2, 160$ at $p = 17$ and $1^{22}, 2^{17}, 3^6, 4^9, 5^6, 6^3, 7^3, 8^4, 10^4, 12^3, 14^2, 18^4, 24, 28, 36^2$ at $p = 43$. So every block is étale, $\mathbb{T}_p = \prod_{\mathfrak{n}} W(\mathbb{T}_p/\mathfrak{n})$ and (M) holds.

Lemma 6.2. (Φ) *holds for X at all $p \notin \{2, 3, 5, 11\}$.*

Proof. Let $\mathcal{K}$ be the completion of $\mathbb{Q}_{11}^{\mathrm{nr}}$. By Section 4 the local components at 11 of the newforms in J are not twists of Steinberg. As 11 is odd they are principal series or dihedral. With trivial character and level dividing 11^4, inertia acts on the first through a group of order dividing 110, on those induced from the unramified quadratic extension through a group of order dividing $120 \cdot 121$, and on those from a ramified one through a group of order dividing $2 \cdot 10 \cdot 121$. Hence J has good reduction over a Galois extension $\mathcal{L}/\mathcal{K}$ of degree m prime to p. The Weil restriction from $\mathcal{O}_{\mathcal{L}}$ to $\mathcal{O}_{\mathcal{K}}$ of the abelian scheme is smooth with connected special fiber, so by the Néron property the norm sends $J(\mathcal{L})$ into the identity component of the Néron model. On $J(\mathcal{K})$ the norm is multiplication by m, so m kills the component group. □

The Hecke algebra modulo p acts faithfully on S. As every block is étale, $\mathrm{End}_{\mathbb{T}_p}(\mathcal{L} \otimes \mathbb{Z}_p) = \mathbb{T}_p$, so a combination of Hecke operators is 0 in $\mathbb{T}_p/p$ if and only if it acts as 0 on S. At $p = 43$ the T_q for the 126 primes $q \le 719$, $q \ne 11, 43$, computed from (d), and the recurrences $T_{ab} = T_a T_b$ for coprime a, b and $T_{q^{k+1}} = T_q T_{q^k} - q T_{q^{k-1}}$ give the T_m for the 616 non-square $m \le 720$ prime to 11 and 43. A computation shows that they span a space of dimension 511 in $\mathrm{End}\, S$, so they span $\mathbb{T}_{43}/43$. As a computation shows that a form in S is determined by $c_1, \dots, c_{11}$, the exponents needed are qn with $n \le 11$.

The derivative at a CM point. Let $y \in X(\mathbb{Q})$ be the CM point of a discriminant $D \ne -3, -4$, so that $\mathcal{O}_D$ has class number one, and let $\tau' \in \mathbb{H}$ lie over y; thus $j(\tau') = j_0$ and $x \mapsto z_{\underline{x}}$ is O-linear for a ring isomorphism $\mathcal{O}_D/121 \cong O$. Let $w := (\tau - \tau')/(\tau - \bar{\tau}')$ be the disc coordinate. If $j_0 \ne 0, 1728$ put $\kappa_1 := (dj/dw)(0)$ and $w' := \kappa_1 w$, and for a differential ω define its *jets* by

$$\omega = \sum_{m \ge 0} A_m(\omega; y)\, w'^m\, dw'.$$

Let φ be the inverse of the series $j - j_0 = \sum_{m \ge 1} J_m w'^m$. The J_m are rational. Indeed, let A_D be a model over $\mathbb{Q}$ of the curve at y, ω_{alg} a non-zero invariant differential on it over $\mathbb{Q}$, and $b_m := (\partial^m j)(A_D, \omega_{\mathrm{alg}})$, where ∂ is the Shimura–Maass operator, $\partial f := (2\pi i)^{-1} df/d\tau - (k/(4\pi \operatorname{Im}\tau)) f$ for f of weight k; then $J_m = b_m/(m!\, b_1^m)$ for any such pair, by the proof of Lemma 6.3. As ∂ is a derivation, $\partial^m j$ is a polynomial over $\mathbb{Q}$ in the $\partial^a E_4$ and $\partial^a \Delta$, $a \le m$, divided by Δ^{m+1}. Katz's operator W [41, §1.5] becomes ∂ under $f(\tau) = F(2\pi i, 2\pi i \tau)$, so by Damerell's theorem in Katz's form [41, Theorem 4.0.4], applied to A_D over $\mathbb{Q}(\sqrt{D})$, the values of the $\partial^a E_4$ and $\partial^a \Delta$ at $(A_D, \omega_{\mathrm{alg}})$ lie in $\mathbb{Q}(\sqrt{D})$ and do not depend on the embedding $\mathbb{Q}(\sqrt{D}) \hookrightarrow \mathbb{C}$. As $(A_D, \omega_{\mathrm{alg}})$ is defined over $\mathbb{Q}$, both embeddings give the same complex numbers, so these values lie in $\mathbb{Q}$, and so do the b_m and the J_m. As $j - j_0$ is a parameter of X at y, the $A_m(\omega; y)$ are the coefficients of ω in the rational coordinate $\varphi(j - j_0)$, so they are rational when ω is.

Lemma 6.3. *Let p split in $\mathbb{Q}(\sqrt{D})$, with p prime to the conductor of $\mathcal{O}_D$ and $j_0 \not\equiv 0, 1728 \bmod p$. Then $A_{p-2}(\omega; y)$ is p-integral for $\omega \in \mathcal{L}$, and there is $c \in \mathbb{F}_p^\times$, not depending on ω, with $\lambda_y(\omega) = cA_{p-2}(\omega; y)$ for all $\omega \in S$.*

Proof. Let $\hat{W} := W(\bar{\mathbb{F}}_p)$ and let $\hat{W}'$ be the integers of a finite extension containing ζ. The reduction $\bar{A}$ of the curve at y is ordinary with $\operatorname{End} \bar{A} = \mathcal{O}_D$, so $\operatorname{Aut} \bar{A} = \{\pm 1\}$, and the disc of y is the formal deformation space $\operatorname{Spf} \hat{W}'[[q-1]]$ with Serre–Tate parameter q [42, Theorem 2.1]. Level prime to p deforms uniquely. The curve at y is the point $q = 1$. On the disc write $\omega = f(q)\, dq/q$ with $f \in \hat{W}'[[q-1]]$, and, as power series in $q-1$, $\omega = g(\mathrm{t})\, d\mathrm{t}$ with $\mathrm{t} := \log q$ and $g(T) := f(\exp T)$.

The divisor. Let A_1 be the curve at $q = 1$, so $A_1[p^\infty] = \mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p$ over $\hat{W}$. Its subgroups of order p are μ_p and $C_i := \{(\varsigma^{ia}, a/p)\}$ for $i \in \mathbb{Z}/p$, with ς a primitive pth root of 1. All quotients reduce to $\bar{A}$, the isogenies being given by $\mathcal{O}_D$, which commutes with the Cartan structure. The extension class of A_1/C_i is computed by $(1, p^{-n-1})$, whose image p^n times is that of $(1, 1/p)$, which is that of $(\varsigma^{-i}, 0)$. So A_1/C_i has parameter ς^{-ei} with $e \in \mathbb{Z}_p^\times$ fixed, and A_1/μ_p has parameter 1. Hence $By = (p-1)[1] - \sum_{i \neq 0} [\varsigma^i]$ on the disc.

The measure. By Amice, $f(q) = \int_{\mathbb{Z}_p} q^x d\mu(x)$ for a $\hat{W}'$-valued measure μ. Split $\mu = \mu_1 + \mu_2$ on $p\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$. A primitive of the part $f_2 dq/q$ is $\int_{\mathbb{Z}_p^\times} x^{-1} q^x d\mu$. The part f_1 is a series in q^p, so it has a primitive F_1 which is p^{-1} times a function of q^p, and F_1 takes one value at all pth roots of 1. So $\int_{By} \omega = pF(1) - \sum_i F(\varsigma^i)$ gets nothing from F_1, and from the other part, as $\sum_i \varsigma^{ix} = 0$ for $x \in \mathbb{Z}_p^\times$,

$$\int_{By} \omega = p \int_{\mathbb{Z}_p^\times} x^{-1} d\mu \equiv p \int_{\mathbb{Z}_p} x^{p-2} d\mu = p(q\tfrac{d}{dq})^{p-2} f(1) \pmod{p^2}.$$

As $(q\frac{d}{dq})^{p-2} f(1) = (p-2)!\, [\mathrm{t}^{p-2}]g$ and $(p-2)! \equiv 1$, this says $\lambda_y(\omega) \equiv [\mathrm{t}^{p-2}]g \bmod p$.

The coordinate. Take A_D as above with good reduction at p and ω_{alg} its Néron differential, and put $\omega_{\mathrm{can}} = \Omega \omega_{\mathrm{alg}}$ with $\Omega \in \hat{W}^\times$, where ω_{can} corresponds to $dT/(1+T)$ on $\hat{\mathbb{G}}_m$. Let θ be Katz's p-adic operator. By Katz's comparison [41, Theorem 8.0.9], $b_n = (\theta^n j)(A_D, \omega_{\mathrm{alg}})$. Along $\partial_q := q\, d/dq$ we have $\nabla(\partial_q)\omega_{\mathrm{can}} = \eta$ and $\nabla(\partial_q)\eta = 0$, with η spanning the unit-root line [42, Main Theorem 4.3.1, Lemma 4.2.1]. Hence $\nabla(\partial_q)(f\omega_{\mathrm{can}}^k) = (\partial_q f)\omega_{\mathrm{can}}^k + kf\omega_{\mathrm{can}}^{k-1}\eta$, and the projection along η leaves $(\partial_q f)\omega_{\mathrm{can}}^k$. As $\omega_{\mathrm{can}}^{\otimes 2}$ goes to dq/q under Kodaira–Spencer [42, Main Theorem 3.7.1], this is $\partial_q[f(A_q, \omega_{\mathrm{can}})] = (\theta f)(A_q, \omega_{\mathrm{can}})$ [41, Lemma 5.8.1, (5.8.4)]. Hence $[\mathrm{t}^n]j = \Omega^{-2n} b_n/n!$ for $n \geq 1$. On the complex side, $j = \sum_n (\partial^n j)(\tau')(-4\pi(\operatorname{Im}\tau')w)^n/n!$ by [66, Proposition 17], with the sign of (58) corrected, and $\partial^n j$ has weight $2n$, so $J_m = b_m/(m!\, b_1^m)$. Therefore $j - j_0$ has the coefficients J_m in $\mathrm{t}_j := \Omega^{-2} b_1 \mathrm{t}$ as well as in w', and $b_1 = -(E_4^2 E_6/\Delta)(A_D, \omega_{\mathrm{alg}})$ is a p-unit since $j_0 \not\equiv 0, 1728$. Thus $\mathrm{t}_j = \varphi(j - j_0)$ as power series in $q-1$, and $\omega = \sum_m A_m \mathrm{t}_j^m d\mathrm{t}_j$. So $g(\mathrm{t}) = \sum_m A_m (\Omega^{-2} b_1)^{m+1} \mathrm{t}^m$. Since f is integral, $[\mathrm{t}^m]g$ is integral for $m < p$, so the A_m are, and $\lambda_y(\omega) = (\Omega^{-2} b_1)^{p-1} A_{p-2}(\omega; y)$. Here $c := (\Omega^{-2} b_1)^{p-1} \bmod p$ lies in $\mathbb{F}_p^\times$: $b_1 \in \mathbb{Z}_{(p)}^\times$, and the isomorphisms of the formal group of A_D with $\hat{\mathbb{G}}_m$ over $\hat{W}$ differ by $\mathbb{Z}_p^\times$ and are permuted by Frobenius σ, both formal groups being defined over $\mathbb{Z}_p$, so $\Omega^\sigma/\Omega \in \mathbb{Z}_p^\times$ and $\bar{\Omega}^{p-1} \in \mathbb{F}_p^\times$. □

The identity $p^{-1} \int_{By} \omega = \int_{\mathbb{Z}_p^\times} x^{-1} d\mu$ is the value at y of the Coleman primitive of the p-depletion, so the lemma is a shadow modulo p of [8, Proposition 3.24].

Jets from a differential system. Let $E_2^* := E_2 - 3/(\pi \operatorname{Im}\tau)$. Put $\wp_v := \wp(z_v)/(2\pi i)^2$ and $\wp_v' := \wp'(z_v)/(2\pi i)^3$, of weights $2, 3$. The next proposition extends Ramanujan's equations to these functions; it holds for $z_v = (c\tau + d)/N$ at any level $N \geq 2$.

Proposition 6.4. *We have* $\partial E_2^* = (E_2^{*2} - E_4)/12$, $\partial E_4 = (E_2^* E_4 - E_6)/3$, $\partial E_6 = (E_2^* E_6 - E_4^2)/2$, *and*

$$\begin{aligned}
\partial \mathbf{e}_v &= \tfrac{1}{12} E_2^* \mathbf{e}_v - \wp_v \mathbf{e}_v - \tfrac{1}{2}\wp_v', \\
\partial \wp_v &= \tfrac{1}{6} E_2^* \wp_v + \mathbf{e}_v \wp_v' + 2\wp_v^2 - \tfrac{1}{36} E_4, \\
\partial \wp_v' &= \tfrac{1}{4} E_2^* \wp_v' + 3\wp_v \wp_v' + \mathbf{e}_v (6\wp_v^2 - \tfrac{1}{24} E_4).
\end{aligned}$$

Proof. The first line is Ramanujan's identities, since $\partial_k f = (D_\tau - \frac{k}{12} E_2) f + \frac{k}{12} E_2^* f$ with $D_\tau := (2\pi i)^{-1} d/d\tau$. For the rest, let $\partial_x := (2\pi i)^{-1}\partial_z$ and $J(z) := (2\pi i)^{-1}(\zeta_{\mathrm{W}}(z) - z\eta_1) = \partial_x \log \theta_1$, with θ_1 the odd Jacobi theta function. Legendre's relation gives $\mathbf{e}_v = J(z_v) + a$ with $a := c/N$. We have $J_x = E_2/12 - \wp_v$, $J_{xx} = -\wp_v'$ and $(\wp_v')_x = 6\wp_v^2 - E_4/24$ at $z = z_v$. The heat equation for θ_1 gives $q\frac{\partial}{\partial q} J = \frac{1}{2} J_{xx} + J J_x$. Since $z_v = a\tau + d/N$, on functions of (z, τ) we have $D_\tau = q\frac{\partial}{\partial q} + a\partial_x$, so

$$D_\tau \mathbf{e}_v = \tfrac{1}{2} J_{xx} + (J + a) J_x = -\tfrac{1}{2}\wp_v' + \mathbf{e}_v(\tfrac{1}{12} E_2 - \wp_v).$$

Applying ∂_x to $D_\tau J = \frac{1}{2} J_{xx} + J J_x + a J_x$ and using $\wp_v = E_2/12 - J_x$ gives $D_\tau \wp_v$, and one more ∂_x gives $D_\tau \wp_v'$. In each identity the E_2-term is $k/12$ times E_2 times the function, so passing from D_τ to ∂ replaces E_2 by E_2^*. □

Fix τ_0, let w be the disc coordinate at τ_0 and $u := -4\pi(\operatorname{Im}\tau_0) w$, and for f of weight k put $\tilde{f}(u) := \sum_n (\partial^n f)(\tau_0) u^n/n!$. For holomorphic f this is $(1-w)^{-k} f(\tau)$, by [66, Proposition 17], corrected as above. Then $d\tilde{f}/du = \widetilde{\partial f}$, and $\widetilde{fg} = \tilde{f}\tilde{g}$ as ∂ is a derivation, so the series $\tilde{E}_2^*, \tilde{E}_4, \tilde{E}_6, \tilde{\mathbf{e}}_v, \tilde{\wp}_v, \tilde{\wp}_v'$ solve the polynomial system of Proposition 6.4, with ∂ replaced by d/du. For weight 2 we get $\omega_F = \tilde{F}(u)du$, and j has $d\tilde{j}/du(0) = \theta_0 := -(E_4^2 E_6/\Delta)(\tau_0)$, so

$$A_m(\omega_F; y) = \frac{[u^m]\tilde{F}}{\theta_0^{m+1}}. \tag{6.1}$$

This recursion at a CM point is that of Rodriguez Villegas and Zagier [57, §§6–7] for a modular form, now on level-structure coordinates. The system is homogeneous for the weights, with u of weight -2. So (6.1) is unchanged if we replace $(\mathbb{C}/\Lambda_{\tau_0}, 2\pi i\, dz)$ by any (A, ω) with the same j, and start from its values. It remains to give the initial values algebraically.

Let A be $Y^2 = 4X^3 - (c_4/12)X + c_6/216$ with $\omega = dX/Y$, over a field of characteristic 0 or ≥ 5, so that c_4, c_6 are the values of E_4, E_6 at (A, ω); the usual c_6 of this equation is $-c_6$. Let N be odd and invertible, and let $\lambda(R_1, R_2)$ be the slope of the line through R_1, R_2. There is at most one odd function $\mathbf{e}$ on $A[N] \setminus 0$ with

$$\mathbf{e}(R_1 + R_2) = \mathbf{e}(R_1) + \mathbf{e}(R_2) + \tfrac{1}{2}\lambda(R_1, R_2) \quad \text{whenever } R_1, R_2, R_1 + R_2 \neq 0, \tag{6.2}$$

since a difference of two would be a homomorphism $A[N] \to \mathbb{G}_a$. On multiples of R of exact order N, summing gives $\mathbf{e}(R) = -(2N)^{-1} \sum_{k=1}^{N-2} \lambda(R, kR)$, so $\mathbf{e}$ exists whenever it does over $\mathbb{C}$ and has good reduction when A does, at primes not dividing $2N$. Over $\mathbb{C}$ the addition law of ζ_{W} gives (6.2) for $R_v \mapsto \mathbf{e}_v(\tau)$.

Lemma 6.5. *Let τ_0 be a CM point with $j_0 \neq 0, 1728$ and $s_2 := (E_2^* E_4/E_6)(\tau_0)$. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ be primitive of determinant $n \geq 2$ with $\gamma\tau_0 = \tau_0$, and $\epsilon := n/(c\tau_0 + d)^2$. Near (j_0, j_0) the curve $\Phi_n = 0$ has the branch $Y - j_0 = \epsilon(X - j_0) + \frac{1}{2}\kappa(X - j_0)^2 + \cdots$. Then*

$$s_2 = 4 + \frac{3j_0}{j_0 - 1728} - \frac{6j_0\kappa}{\epsilon^2 - \epsilon}.$$

Proof. Take the branch $(j(\tau), j(\gamma\tau))$, put $\mu := c\tau_0 + d$, and evaluate at τ_0 throughout. Differentiating twice gives $\kappa\, D_\tau j = (\epsilon^2 - \epsilon) D_\tau \log(D_\tau j) + D_\tau \gamma'$. Ramanujan's identities give $D_\tau \log(D_\tau j) = E_2/6 - E_4^2/(2E_6) - (2/3)E_6/E_4$. Write $E_2 = E_2^* + 3/(\pi \operatorname{Im}\tau_0)$. Since μ and $\bar\mu$ are the eigenvalues of γ, $\epsilon = \bar\mu/\mu$ and $\epsilon - 1 = -2ic(\operatorname{Im}\tau_0)/\mu$, and so the non-holomorphic term cancels against $D_\tau\gamma' = (2\pi i)^{-1}\epsilon(-2c/\mu)$. So $\kappa\, D_\tau j = (\epsilon^2 - \epsilon)(E_2^*/6 - E_4^2/(2E_6) - (2/3)E_6/E_4)$. Multiply by $6E_4/((\epsilon^2 - \epsilon)E_6)$ and use $D_\tau j\, E_4/E_6 = -j_0$ and $E_4^3/E_6^2 = j_0/(j_0 - 1728)$. □

Exact arithmetic on Φ_n, at $n = 17$ for $D = -67$ and $n = 41$ for $D = -163$, the smallest $n \geq 2$ that are norms of primitive elements of $\mathcal{O}_D$, gives

$$s_2(-67) = \frac{33440}{43617}, \qquad s_2(-163) = \frac{77265280}{90856689}.$$

That $s_2 \in \mathbb{Q}(j_0)$ is due to Masser [53, Appendix 1, Theorem A1]. These two numbers are $1 - 6 \cdot 10177/261702$ and $1 - 6 \cdot 13591409/545140134$, from the constants of the Chudnovsky series for $1/\pi$ [15, (1.4)], [14, Theorem 4.3, §4.1].

Proposition 6.6. *Let D, y, τ' be as above, $D \neq -3, -4$, with $s_2(D)$ integral at p, and p as in* Lemma 6.3. *Let $(\bar A, \bar\omega)$ be a curve over $\mathbb{F}_p$ with $j = j_0 \bmod p$, $\varpi \in \mathcal{O}_D$ its Frobenius, f the order of ϖ in $(\mathcal{O}_D/121)^\times \cong O^\times$, $\mathbb{F}_{p^f}$ the field it defines, $\psi\colon O \to \bar A[121]$ an O-linear isomorphism, and $\bar\zeta := e_{121}(\psi(i), \psi(1))$. Solve the system of* Proposition 6.4 *in $\mathbb{F}_{p^f}[[u]]/(u^{p-1})$, starting from $s_2 c_6/c_4, c_4, c_6$ and the values $\mathbf{e}, X, Y$ at $\psi(x)$. Then for $m \leq p - 2$,*

$$A_m(\omega_{F_{a,\rho}}; y) \equiv \frac{1}{\bar\theta^{m+1}}[u^m] \sum_{r \in O^\times/\langle\varpi\rangle} \operatorname{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p}\left[\bar\xi_{a\mathrm{N}(r)} \tilde{\mathbf{e}}_r (\tilde{\mathbf{e}}_{\rho r} + \tilde{\mathbf{e}}_{\bar\rho r})\right] \pmod p,$$

with $\bar\xi_s := \bar\zeta^s + \bar\zeta^{-s}$ and $\bar\theta := -c_4^2 c_6/\Delta$.

Proof. Take a model of good reduction over $\mathbb{Q}$ with c_4, c_6 and Δ units at p, which exists as $j_0 \not\equiv 0, 1728$. Its $\mathbf{e}, X, Y$ are integral above p and reduce to those of $\bar A$. The recursion of the system for $[u^{n+1}]$ divides only by $n + 1$ and by divisors of $2^3 3^3$, which are units for $n + 1 \leq p - 2$. So (6.1) reduces. Frobenius acts on $\bar A[121]$ through ϖ, so $\tilde{\mathbf{e}}_{\varpi x} = \mathrm{Frob}(\tilde{\mathbf{e}}_x)$, with $\bar\zeta^p = \bar\zeta^{\mathrm{N}(\varpi)}$, and the sum over each orbit is a trace. □

Two more values are used. A value $A_0 = \tilde F(0)/\bar\theta$ needs only the initial values, so no s_2. At $D = -3$ we have $c_4 = 0$ and $E_2^*(\tau') = 0$. The system runs with these initial values, and only the $[u^m]\tilde F$ with $m \equiv 2 \bmod 3$ survive, since ζ_3 lies in the Cartan subgroup. Here $j = 64c_6u^3 + \cdots$, and j is a parameter of X at $y(-3)$. So for $\omega = \omega_F$,

$$\frac{\omega}{dj}(y(-3)) = \frac{[u^2]\tilde F}{192\, c_6}. \tag{6.3}$$

7. The seven classes

A rational point of X lies over a point of $E(\mathbb{Q})$ whose j-invariant has a 121st power as denominator. We turn this into an 11th-power condition on a modular unit over $K := \mathbb{Q}(\zeta_{11})^+$, and test that condition modulo a few primes with residue symbols. At level 49, over a base of genus 0, this is the descent of [26, Proposition 3.1] and [1, §3]. In this section we use the translate of Schoof and Tzanakis [59, §4]: with $x' := x - 4$ and $y' := y - 5$,

$$E\colon\ y'^2 + 11y' = x'^3 + 11x'^2 + 33x', \qquad P_0 = (0, 0).$$

The CM points. By Ligozat [51, Proposition 4.3.8.1] and Halberstadt [32, (2–1)], as written in [59, §4], $X_{\mathrm{ns}}^+(11)$ is isomorphic to E over $\mathbb{Q}$ so that the j-map is $\mathrm{j} := f/(x'y' - 11)^{11}$, where

$$f = (x'^2+11x'+22)^3((11x'^2+88x'+121)y'+2x'^4+55x'^3+451x'^2+1452x'+1452)^3 g(x', y'),$$

with $g \in \mathbb{Z}[x', y']$ printed in [59, §4]; f has degree 55 for the weights 2 of x' and 3 of y'. The rational points of E with $\mathrm{j} \in \mathbb{Z}$ are the seven points of Table 2 [59, Theorems 1.1 and 4.1], and their j-invariants are those of the seven orders in the table [59, §4]. An automorphism of E over $\mathbb{Q}$ has the form $P \mapsto \pm P + Q$, so it is fixed by the images of O and P_0, and this is the identification of Theorem 1.1.

k	D_k	kP_0 on $y^2 + y = x^3 - x^2 - 7x + 10$	$\mathrm{j}(D_k)$	exponents of ε_k
-2	-27	$(2, -1)$	$-3 \cdot 160^3$	$(3, 0, 0, 2)$
-1	-16	$(4, -6)$	66^3	$(2, 0, 0, 2)$
0	-12	O	$2 \cdot 30^3$	$(0, 0, 0, 0)$
1	-67	$(4, 5)$	-5280^3	$(0, 0, 1, -2)$
2	-4	$(2, 0)$	12^3	$(2, 2, -1, 2)$
3	-3	$(5/4, 7/8)$	0	$(4, 3, 1, 6)$
4	-163	$(-2, 3)$	-640320^3	$(-7, -2, -4, -2)$

Table 2. The seven points. The last column is defined in (7.1).

For each k the prime 11 is inert in $\mathbb{Q}(\sqrt{D_k})$ and prime to the conductor of $\mathcal{O}_{D_k}$. Let $y_k := y(D_k)$ be the point of X whose Cartan structure on $A[121]$ is the action of $\mathcal{O}_{D_k}/121$, with $\mathrm{End}\, A = \mathcal{O}_{D_k}$.

Lemma 7.1. *Each y_k lies in $X(\mathbb{Q})$, and $\pi(y_k) = kP_0$.*

Proof. Take A over $\mathbb{Q}$ with an invariant differential ω over $\mathbb{Q}$, and normalize the action by $[a]^*\omega = a\omega$. For $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, the endomorphism $\tau[a]\tau^{-1}$ acts on ω by $\tau(a)$, so it is $[\tau(a)]$. Hence τ preserves the image $\mathfrak{c}$ of $\mathcal{O}_{D_k}/121$ in $\mathrm{End}\, A[121]$, and $\tau(A, \mathfrak{c}) = (A, \tau\mathfrak{c}\tau^{-1}) = (A, \mathfrak{c})$. Thus $\pi(y_k) \in E(\mathbb{Q})$ has integral j-invariant $\mathrm{j}(D_k)$, and the seven values in Table 2 are distinct. □

The modular unit. Put $\eta := \zeta_{11} + \zeta_{11}^{-1}$, a root of $t^5 + t^4 - 4t^3 - 3t^2 + 3t + 1$. Then $\mathcal{O}_K = \mathbb{Z}[\eta]$, and K has class number one, since its Minkowski bound is below 5 and 2, 3 are inert. Let $\sigma(\eta) = \eta^2 - 2$ generate $\mathrm{Gal}(K/\mathbb{Q})$; the only prime over 11 is $(2 - \eta)$, of degree one.

The five cusps of E are the zeros of $x'y' - 11$ [59, §4]. They are $C(s) := sC_0$ for $s \in \{1, 3, 9, 5, 4\}$, where $C_0 := (t_0, 11/t_0)$ with

$$t_0 := -\eta^4 - \eta^3 + 2\eta^2 + 3\eta - 1,$$

a root of $t^5+11t^4+33t^3-121t-121$; the point C_0 has order 11, and $\sigma(C_0)=3C_0$. None of them is rational, so neither E nor X has a rational cusp.

Let $g_s := y' - \alpha_s x' - \beta_s$ be the tangent line at $C(s)$. As $-2 \equiv 9 \bmod 11$, its divisor is $2(C(s))+(C(9s))-3(O)$, and $\sigma(g_s)=g_{3s}$. We use

$$\alpha_1 = -\eta^4-2\eta^3+3\eta^2+5\eta-1, \qquad \beta_1 = -\eta^4-4\eta^3+4\eta^2+9\eta-8,$$
$$\alpha_3 = \eta^4+\eta^3-3\eta^2-\eta+1, \qquad \beta_3 = 4\eta^4+3\eta^3-15\eta^2-5\eta+4,$$

all in $\mathcal{O}_K$, and we put

$$U := g_1/g_3, \qquad \operatorname{div} U = 2(C_0)+(9C_0)-2(3C_0)-(5C_0), \qquad U(O)=1.$$

The product $\prod_{i=0}^4 \sigma^i(U)$ telescopes to 1, so $\mathrm{N}_{K/\mathbb{Q}}U(P)=1$ for $P\in E(\mathbb{Q})$.

Lemma 7.2. *Let $z\in X(\mathbb{Q})$ and $P:=\pi(z)$. Then $U(P)=\varepsilon\alpha^{11}$ with $\varepsilon\in\mathcal{O}_K^\times$ and $\alpha\in K^\times$, and the class $\varepsilon(P)$ of ε in $\mathcal{O}_K^\times/\mathcal{O}_K^{\times 11}$ is well defined. If $\mathfrak{q}\nmid 11$ is a prime of K and $\bar P$ is not a zero of $\bar g_1\bar g_3$ modulo $\mathfrak{q}$, then $U(P)$ is a $\mathfrak{q}$-unit with reduction $\bar g_1(\bar P)/\bar g_3(\bar P)$, taken as 1 at $\bar P=\bar O$.*

Proof. Let $\mathfrak{q}$ lie over a prime $q\neq 11$, and let i_s be the intersection number of P and $C(s)$ on the smooth model of E over $\mathcal{O}_{K,\mathfrak{q}}$. At most one i_s is non-zero, since the $C(s)$ differ by points of order 11 and so have distinct reductions.

We claim $11\mid i_s$. Write $P=(a/e^2,b/e^3)$ in lowest terms, so that $\mathrm{j}(P)=f^*/D^{11}$ with $D:=ab-11e^5$ and $f^*:=e^{55}f(a/e^2,b/e^3)\in\mathbb{Z}$. If $q\mid e$, then $q\nmid ab$, so $q\nmid D$ and every i_s is 0. If $q\nmid e$, then $v_q(D)=v_{\mathfrak{q}}((x'y'-11)(P))=\sum_s i_s$, because the divisor $\sum_s(C(s))-5(O)$ of $x'y'-11$ persists modulo $\mathfrak{q}$. If $i_s>0$, then $f(P)\equiv f(C(s)) \bmod \mathfrak{q}$, which is a unit because a computation in PARI/GP gives $\mathrm{N}_{K/\mathbb{Q}}f(C_0)=11^{55}$; so $v_q\mathrm{j}(P)=-11i_s$. As X has no rational cusps, z is the class of a curve over $\mathbb{Q}$ with image in $N_{\mathrm{ns}}(121)$ unless $\mathrm{j}(P)\in\{0,1728\}$, and then $\mathrm{j}(P)$ is integral. Hence the denominator of $\mathrm{j}(P)$ is a 121st power [26, Proposition 2.9], from [25, Proposition 5.14], and $11\mid i_s$.

Since g_s has coefficients in $\mathcal{O}_K$, its reduction is a non-zero function with the same divisor modulo $\mathfrak{q}$. If $\bar P\neq\bar O$, then $v_{\mathfrak{q}}g_s(P)=2i_s+i_{9s}$. If $\bar P=\bar O$, then $g_s(P)=y'(P)(1-\alpha_s x'(P)/y'(P)-\beta_s/y'(P))$, where the bracket is $\equiv 1 \bmod \mathfrak{q}$, so $U(P)\equiv 1 \bmod \mathfrak{q}$. Hence

$$v_{\mathfrak{q}}U(P)=2i_1+i_9-2i_3-i_5\equiv 0 \pmod{11},$$

and the last assertion of the lemma follows. At the prime over 11 the valuation of $U(P)$ is $v_{11}(\mathrm{N}_{K/\mathbb{Q}}U(P))=0$. So the ideal $(U(P))$ is an 11th power, and it is principal because K has class number one. A unit that is an 11th power in K is the 11th power of a unit, so $\varepsilon(P)$ is well defined. □

The sieve. Up to sign, the units of K are the products of $\eta,\sigma\eta,\sigma^2\eta,\sigma^3\eta$, as K has class number one [64, Theorem 8.2] and 2 generates $(\mathbb{Z}/11)^\times/\pm 1$, so that the conjugates of η give the cyclotomic units. So exponents identify $\mathcal{O}_K^\times/\mathcal{O}_K^{\times 11}$ with $\mathbb{F}_{11}^4$; the sign does not matter, since -1 is an 11th power. A computation in PARI/GP shows that the values $\varepsilon_k := U(kP_0)$ are units with

$$\varepsilon_k = \pm\prod_{i=0}^{3}(\sigma^i\eta)^{e_i}, \qquad (e_0,e_1,e_2,e_3) \text{ as in Table 2.} \tag{7.1}$$

Let $r\neq 11$ be a prime with $r\equiv 1,3,4,5,9 \bmod 11$, so that $\mathrm{N}\mathfrak{r}\equiv 1 \bmod 11$ for a prime $\mathfrak{r}\mid r$ of K, and put $\chi_{\mathfrak{r}}(x) := x^{(\mathrm{N}\mathfrak{r}-1)/11}$ in $\mu_{11}(\mathcal{O}_K/\mathfrak{r})$. Let n_r be the order of $\bar P_0$ in $E(\mathbb{F}_r)$,

and write $\bar{U} := \bar{g}_1/\bar{g}_3$. By Lemma 7.2, if $P = \pi(z) = mP_0$ and $m\bar{P}_0$ is not a zero of $\bar{g}_1\bar{g}_3$ modulo $\mathfrak{r}$, then

$$\chi_{\mathfrak{r}}(\bar{U}(m\bar{P}_0)) = \chi_{\mathfrak{r}}(\varepsilon(P)), \tag{7.2}$$

and the left side depends only on $m \bmod n_r$.

Proposition 7.3. *Let $z \in X(\mathbb{Q})$. Then $\pi(z) = mP_0$ with $\varepsilon(\pi(z)) = \varepsilon_k$ for exactly one $k \in \{-2, \dots, 4\}$, and*

$$m \equiv k \pmod{239580}, \qquad 239580 = 2^2 \cdot 3^2 \cdot 5 \cdot 11^3.$$

We call k the *class* of z.

Proof. We have $E(\mathbb{Q}) = \mathbb{Z}P_0$. For a prime r as above, let $A_r \subset \mathbb{F}_{11}^4$ be the set of exponent vectors e such that, for some $c \bmod n_r$, $\chi_{\mathfrak{r}}(\bar{U}(c\bar{P}_0)) = \chi_{\mathfrak{r}}(\prod_i (\sigma^i\eta)^{e_i})$ for all $\mathfrak{r} \mid r$. A computation in PARI/GP gives the following at $r = 2069, 3301, 3631$, each with five primes $\mathfrak{r}$ of degree one and with $n_r = 90, 33, 54$. No multiple of $\bar{P}_0$ is a zero of $\bar{g}_1\bar{g}_3$ modulo any $\mathfrak{r}$, so by (7.2) the exponent vector of $\varepsilon(\pi(z))$ lies in A_r. Further $\#A_r = 979, 110, 594$, and $A_{2069} \cap A_{3301} \cap A_{3631}$ consists of exactly the seven distinct vectors of Table 2.

Now fix k with $\varepsilon(\pi(z)) = \varepsilon_k$. Let $R_r(k) \subset \mathbb{Z}/n_r$ be the set of c such that $c\bar{P}_0$ is a zero of $\bar{g}_1\bar{g}_3$ modulo some $\mathfrak{r} \mid r$, or $\chi_{\mathfrak{r}}(\bar{U}(c\bar{P}_0)) = \chi_{\mathfrak{r}}(\varepsilon_k)$ for all $\mathfrak{r} \mid r$. By (7.2), $m \bmod n_r$ lies in $R_r(k)$. The same computation at $r = 53, 2069, 12101, 5313353$, with $n_r = 12, 90, 1089, 3993$, shows for each k that these four conditions leave only $m \equiv k$ modulo $\operatorname{lcm}(12, 90, 1089, 3993) = 239580$. □

Remark 7.4. Inert primes alone do not suffice, nor do primes with $11 \nmid n_r$. At a prime r inert in K, σ acts on $\mathcal{O}_K/\mathfrak{r}$ by a power of Frobenius, so $\chi_{\mathfrak{r}}(\sigma u) = \chi_{\mathfrak{r}}(u)^9$, and $\chi_{\mathfrak{r}}$ sees only the linear form $\sum_i 9^i e_i$ of the class, the same at every inert prime. At a split prime with $11 \nmid n_r$, such as 2069, the left side of (7.2) depends on m only modulo a number prime to 11, so it says nothing about m modulo 11. For that one needs primes with $11 \mid n_r$, such as 3301.

8. One residue disc

Over $k\bar{P}_0$ the geometric points of X are the 121 Cartan structures lifting the one at $k\bar{P}_0$, taken up to automorphisms of the elliptic curve there. When p splits in the CM field of y_k, Frobenius acts on them linearly through its class modulo 11, and we show that it fixes only $\bar{y}_k$.

Proposition 8.1. *Let $k \in \{-2, \dots, 4\}$, $D := D_k$, let d be the discriminant of $K_D := \mathbb{Q}(\sqrt{D})$, and let $p \geq 5$ be a prime split in K_D such that $p < 121|d|/4$, the exponent of $\bar{E}(\mathbb{F}_p)$ divides 239580, and $\mathrm{j}(D) \not\equiv 0, 1728 \bmod p$ if $D \neq -3, -4$. Then every $z \in X(\mathbb{Q})$ of class k has $\bar{z} = \bar{y}_k$ in $\mathcal{X}(\mathbb{F}_p)$.*

Proof. Let $\mathcal{X}/\mathbb{Z}_{(p)}$ be the smooth model [19, VI, Proposition 6.7]. The forgetful map extends to the smooth models, and so does the isomorphism of $X_{\mathrm{ns}}^+(11)$ with E, as a smooth proper curve of genus one over $\mathbb{Z}_{(p)}$ is the minimal regular model of its generic fiber. This gives $\bar{\pi}\colon \mathcal{X}_{\mathbb{F}_p} \to \bar{E}$. By Proposition 7.3 and Lemma 7.1, $\bar{\pi}(\bar{z}) = m\bar{P}_0 = k\bar{P}_0 = \bar{\pi}(\bar{y}_k)$, so $\bar{z}$ and $\bar{y}_k$ are $\mathbb{F}_p$-points of the fiber $\mathfrak{F} := \bar{\pi}^{-1}(k\bar{P}_0)$.

Let $A/\mathbb{Q}$ have $\operatorname{End} A = \mathcal{O}_D$ and good reduction at p; this is possible because $p \geq 5$ and $\mathrm{j}(D) \not\equiv 0, 1728$, or $D = -3, -4$, where one takes $y^2 = x^3 + 1$ and $y^2 = x^3 + x$. By the proof of Lemma 7.1, $[a]$ is defined over $K_D \subset \mathbb{Q}_p$, so it reduces to an endomorphism of $\bar{A}$ over $\mathbb{F}_p$. So $\bar{y}_k = (\bar{A}, \mathfrak{c}_0)$, with $\mathfrak{c}_0$ the image of $\mathcal{O}_D/121$. The Frobenius endomorphism Φ of $\bar{A}$

commutes with $\mathcal{O}_D$, so it lies in the centralizer of K_D in $\mathrm{End}(\bar{A}) \otimes \mathbb{Q}$, which is K_D. So $\Phi \in \mathcal{O}_{K_D}$ has norm p, and it acts on $\bar{A}[121]$ through $\mathfrak{c}_0$, as $\mathcal{O}_{K_D}/121 = \mathcal{O}_D/121$. Also $\mathrm{Aut}\,\bar{A}$ is the image of $\mathcal{O}_D^\times$: it is $\{\pm 1\}$ if $\mathrm{j}(D) \not\equiv 0, 1728$, and it has order 4, 6 at $D = -4, -3$.

The geometric points of $\mathcal{X}$ off the cusps are the classes $(A', \mathfrak{c}')$ [19, I, Définition 8.1(ii)]. The j-invariant is finite on $\mathfrak{F}$, so a point of $\mathfrak{F}(\bar{\mathbb{F}}_p)$ is $(\bar{A}, \mathfrak{c}')$ with $(\bar{A}, \mathfrak{c}' \bmod 11)$ isomorphic to $(\bar{A}, \mathfrak{c}_0 \bmod 11)$. Applying an automorphism of $\bar{A}$, we may take $\mathfrak{c}' \equiv \mathfrak{c}_0 \bmod 11$. So $\mathfrak{F}(\bar{\mathbb{F}}_p)$ is the set of $\mathrm{Aut}\,\bar{A}$-orbits on the set $\mathcal{C}$ of Cartan subalgebras of $\mathrm{End}\,\bar{A}[121]$ that lift $\bar{\mathfrak{c}} := \mathfrak{c}_0 \bmod 11$.

Let $\mathfrak{p} \subset \mathrm{End}\,\bar{A}[11]$ be the conjugate-linear part: the Ξ with $\Xi a = \bar{a}\Xi$ for $a \in \bar{\mathfrak{c}} \cong \mathbb{F}_{121}$, where $\bar{a} = a^{11}$. Then $\mathrm{End}\,\bar{A}[11] = \bar{\mathfrak{c}} \oplus \mathfrak{p}$. Non-split Cartan subalgebras of $\mathrm{End}\,\bar{A}[121]$ are conjugate, and the normalizer of $\mathfrak{c}_0$ surjects onto that of $\bar{\mathfrak{c}}$, so $\mathcal{C}$ is the orbit of $\mathfrak{c}_0$ under $1 + 11\,\mathrm{End}\,\bar{A}[11]$. An element of the stabilizer acts trivially on $\mathfrak{c}_0$ modulo 11, hence on $\mathfrak{c}_0$, so it lies in $1 + 11\bar{\mathfrak{c}}$. Thus $\Xi \mapsto (1 + 11\Xi)\mathfrak{c}_0(1 + 11\Xi)^{-1}$ is a bijection $\mathfrak{p} \to \mathcal{C}$. If $c \in \mathfrak{c}_0^\times$ reduces to a, conjugation by c carries the point for Ξ to the point for $a\Xi a^{-1} = (a/\bar{a})\Xi$.

Arithmetic Frobenius sends $(\bar{A}, \mathfrak{c}')$ to $(\bar{A}, \Phi\mathfrak{c}'\Phi^{-1})$. Let $g \in \bar{\mathfrak{c}}$ be the class of Φ. Suppose an orbit with $\Xi \neq 0$ is fixed. Then for some $u \in \mathcal{O}_D^\times$ we have $(g/\bar{g})\Xi = (u/\bar{u})\Xi$, so $g\bar{u} = \bar{g}u$, that is, $g\bar{u} \in \mathbb{F}_{11}$. So $\Phi\bar{u} \in \mathbb{Z} + 11\mathcal{O}_{K_D}$, and it is not in $\mathbb{Z}$ because its norm is the prime p. An element of $\mathbb{Z} + 11\mathcal{O}_{K_D}$ outside $\mathbb{Z}$ has norm at least $121|d|/4$, which contradicts the bound on p. Hence $\mathfrak{F}(\mathbb{F}_p) = \{\bar{y}_k\}$. □

Remark 8.2. Without the bound on p the fiber can have more than one $\mathbb{F}_p$-point. For $D = -3$ and $p = 97 = \mathrm{N}(3 + 11\zeta_3)$, some unit multiple of Φ lies in $\mathbb{Z} + 11\mathcal{O}_{K_D}$, so Frobenius fixes all 41 orbits of the fiber, and the class does not pick out $\bar{y}_3$. The same happens at $D = -4$, $p = 137 = \mathrm{N}(11 + 4i)$ and at $D = -12$, $p = 367 = \mathrm{N}(2 + 11\sqrt{-3})$.

Corollary 8.3. *If $z \in X(\mathbb{Q})$ has class k, then $\bar{z} = \bar{y}_k$ modulo 17 for $k = -1, 1, 2$ and modulo 43 for $k = -2, 0, 3, 4$.*

Proof. We have $\#E(\mathbb{F}_{17}) = 18$ and $\#E(\mathbb{F}_{43}) = 44$, both dividing 239580. The prime 17 splits in $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-67})$, and 43 splits in $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-163})$; also $17 < 121$ and $43 < 121 \cdot 3/4$. At $p = 17$, where $1728 \equiv 11$, we have $\mathrm{j}(-16) \equiv 9$ and $\mathrm{j}(-67) \equiv 3$. At $p = 43$, where $1728 \equiv 8$, we have $\mathrm{j}(-27) \equiv 24$, $\mathrm{j}(-12) \equiv 35$ and $\mathrm{j}(-163) \equiv 1$. □

9. The term at 11

The only bad prime of X is 11. Let $z \in X(\mathbb{Q})$ have class k, and put $y := y_k$ and $D := D_k$. We show that y and z lie in one closed disc of X^{an} over $\mathbb{C}_{11}$, so that the Néron symbol of $z - y$ with a divisor off that disc vanishes, and that $D(y, z)$ is off it because our correspondences preserve the j-invariant. The conclusion has the shape of [6, Proposition 3.3 and Lemma 3.6] at level 27, where a stable model is available; here the disc comes from the formal group.

We keep the coordinates x', y' of Section 7, the j-map j, the formal parameter $w := -x'/y'$ at O, and we write $E_r := \{O\} \cup \{P \in E(\mathbb{Q}_{11}) : v(x'(P)) \leq -2r\}$ for $r \geq 1$, the points of the kernel of reduction with $v(w(P)) \geq r$.

The class at 11.

Lemma 9.1. *For $n \in \mathbb{Z}$ and $r \geq 1$, we have $nP_0 \in E_r$ if and only if $22 \cdot 11^{r-1} \mid n$. In particular $\pi(z) - kP_0 \in E_3$.*

Proof. The model reduces to $y'^2 = x'^3$ modulo 11. Let E_0 be the group of points with non-singular reduction, so that $E_0/E_1 \cong \mathbb{F}_{11}$. The point P_0 reduces to the singular point,

and $2P_0 = (-2, -5)$ reduces to $(9, 6)$, which is neither singular nor $\bar{O}$. So $nP_0 \in E_1$ if and only if $22 \mid n$. A computation in PARI/GP gives $v_{11}(x'(22P_0)) = -2$, so $22P_0 \in E_1 \smallsetminus E_2$. As $a_1 = 0$ on this model, $[11](w) = 11w + \sum_{i \geq 3} b_i w^i$ with $b_i \in \mathbb{Z}$, so multiplication by 11 maps $E_r \smallsetminus E_{r+1}$ into $E_{r+1} \smallsetminus E_{r+2}$. Since $E_r/E_{r+1} \cong \mathbb{F}_{11}$, this proves the equivalence. The last assertion follows from Proposition 7.3, as $2 \cdot 11^3 \mid 239580$. □

Let $P(w)$ be the formal point with parameter w, and expand

$$S_k(w) := \mathrm{j}(kP_0 + P(w)) - \mathrm{j}(D) = \sum_{i \geq 1} c_i w^i.$$

Lemma 9.2. *We have $c_1 \in \mathbb{Z}$, with $v_{11}(c_1) = 2$ for k even and $v_{11}(c_1) = 3$ for k odd. For $w \in \mathbb{C}_{11}$ with $v(w) \geq 3$, we have $v(S_k(w)) = v(c_1) + v(w)$.*

Proof. We have $x'(w) \in w^{-2}(1 + w\mathbb{Z}[[w]])$ and $y'(w) \in -w^{-3}(1 + w\mathbb{Z}[[w]])$. For $k = 0$ this gives $x'y' - 11 \in -w^{-5}(1 + w\mathbb{Z}[[w]])$ and $f(x'(w), y'(w)) \in w^{-55}\mathbb{Z}[[w]]$, so $S_0 \in \mathbb{Z}[[w]]$. For $k \neq 0$, the point kP_0 is 11-integral; the chord formula shows that the coordinates of $kP_0 + P(w)$ lie in $\mathbb{Z}_{(11)}[[w]]$, and $x'y' - 11 \in d_k + w\mathbb{Z}_{(11)}[[w]]$ with $d_k := (x'y' - 11)(kP_0)$. Here $d_k = \pm 1$ for k even and $v_{11}(d_k) = 1$ for k odd. So $v_{11}(c_i) \geq 0$ for k even and $v_{11}(c_i) \geq -11 - i$ for k odd.

A computation in PARI/GP of the exact series gives $c_0 = 0$, $c_1 \in \mathbb{Z}$ with the valuations stated, and $v_{11}(c_i) + 3i > v_{11}(c_1) + 3$ for $2 \leq i \leq 8$ when k is odd. Let $s := v(w) \geq 3$. For k even and $i \geq 2$, $v(c_i w^i) \geq 2s > 2 + s$. For k odd and $2 \leq i \leq 8$, $v(c_i w^i) \geq v(c_i) + 3i + (s-3)i > v(c_1) + s$. For k odd and $i \geq 9$, $v(c_i w^i) \geq -11 + 9(s-1) > 3 + s$. So $c_1 w$ is the unique term of least valuation. □

The deformation disc. We use the notation of Section 4 with $\ell = 11$ and $e = 2$, for the tube of the supersingular j-invariant s of $\mathrm{j}(D)$ modulo 11. Thus $s = 1728$ and $\#\Gamma = 2$ for k even, and $s = 0$ and $\#\Gamma = 3$ for k odd; so $v_{11}(c_1) = \#\Gamma$. Let $D_s := -4, -3$ respectively, let t be a coordinate on $\mathcal{D}$ vanishing at the canonical point of D_s on which Γ acts linearly, which exists as $\#\Gamma$ is prime to 11, and let t_D be the canonical point of D. The completed local ring of the j-line at s is $W[[t]]^\Gamma$ [19, I, (8.2.1)], so on $\mathcal{D}$

$$\mathrm{j} - \mathrm{j}(D) = u(t) \prod_{\gamma \in \Gamma} (t - \gamma t_D), \qquad u \in W[[t]]^\times. \tag{9.1}$$

If $D \neq D_s$, then at $t = t_D$ with D_s in place of D this gives $\#\Gamma \cdot v(t_D) = v_{11}(\mathrm{j}(D) - \mathrm{j}(D_s))$. This is 2 for $D = -27, -12, -163$ and 3 for $D = -16, -67$. So $v(t_D) = 1$, and $v(t_D - \gamma t_D) = 1$ for $\gamma \neq 1$. Put

$$\rho_D := 2 \text{ if } D = -3, \qquad \rho_D := \tfrac{5}{2} \text{ if } D = -4, \qquad \rho_D := 4 \text{ otherwise.}$$

Lemma 9.3. *Let $t \in \mathcal{D}$ have $\mathrm{j}(t) = \mathrm{j}(\pi(z))$. After applying an element of Γ to t, we have $v(t - t_D) \geq \rho_D$.*

Proof. Let $s' := v(w(\pi(z) - kP_0))$, which is at least 3 by Lemma 9.1. By Lemma 9.2 and (9.1), $\sum_\gamma v(t - \gamma t_D) = \#\Gamma + s'$, so some term exceeds 1. Applying an element of Γ, we get $\delta := v(t - t_D) > 1$. If $D = D_s$, then $t_D = 0$ and $\delta = 1 + s'/\#\Gamma$. Otherwise the other terms are 1, and $\delta = 1 + s'$. □

Remark 9.4. The argument uses the factor 11^3 in the modulus of Proposition 7.3, because Lemma 9.2 needs $v(w) \geq 3$. With 11^2 in its place, Lemma 9.1 gives only $s' \geq 2$, and at $D = -3$ even the conclusion of Lemma 9.2 at $v(w) = 2$ would give only $\delta = 5/3$, below the radius $r_2 = 23/12$ at which the level structure splits.

One disc. Let $B_D := \{t \in \mathcal{D} : v(t - t_D) \geq \rho_D\}$. As $\rho_D > r_2 = 23/12$, the proof of Lemma 4.7 shows that each point of $\mathcal{F}_{t_D}[121]$ extends uniquely to an analytic section over B_D. Thus $\mathrm{pr}^{-1}(B_D)$ in Y is a disjoint union of discs $B_{\mathfrak{c}}$, indexed by the Cartan subalgebras $\mathfrak{c}$ of $\operatorname{End}\mathcal{F}_{t_D}[121]$, each mapped isomorphically to B_D. Let $\mathfrak{c}_0 := \mathcal{O}/121$ and let V be the image of $B_{\mathfrak{c}_0}$ in $Y/\Gamma \subset X^{\mathrm{an}}$. It is a closed disc: if $D \neq D_s$, the translates of B_D under Γ are disjoint, and if $D = D_s$, then $V = B_{\mathfrak{c}_0}/\Gamma$ has coordinate $t^{\#\Gamma}$.

Proposition 9.5. *The points y and z lie in V.*

Proof. The point y is the image of $(t_D, \mathfrak{c}_0)$. By Lemma 9.3, z has a lift $\tilde{z} = (t, \mathfrak{c}') \in Y$ with $t \in B_D$, say $\tilde{z} \in B_{\mathfrak{c}}$. Let $L := \operatorname{Frac} W$ and $\tau \in \mathrm{Gal}(\bar{L}/L)$. Then τ fixes t_D and acts on $\mathcal{F}_{t_D}[121]$ through an element $c_\tau \in (\mathcal{O}/121)^\times$, and every element arises, by Lubin–Tate theory. By uniqueness of the sections, τ maps $B_{\mathfrak{c}}$ to $B_{c_\tau \mathfrak{c} c_\tau^{-1}}$. As z is rational over $\mathbb{Q}_{11}$, we have $\tau\tilde{z} = \gamma\tilde{z}$ for some $\gamma \in \Gamma$, so $\gamma t \in B_D$. If $D \neq D_s$, this forces $\gamma = 1$. If $D = D_s$, then γ acts on $\mathcal{F}_{t_D}[121]$ by a unit of $\mathcal{O}_D$. In both cases $c_\tau \mathfrak{c} c_\tau^{-1} = \gamma \mathfrak{c} \gamma^{-1}$, so the orbit of $\mathfrak{c}$ under $(\mathcal{O}/121)^\times$ has at most $\#\Gamma \leq 3$ elements.

Now $(\mathcal{O}/121)^\times$ acts on $\mathfrak{sl}_2(\mathbb{F}_{11}) = \bar{\mathfrak{c}}_0^0 \oplus \mathfrak{p}$ trivially on the first term and on $\mathfrak{p} \cong \mathbb{F}_{121}$ through the norm-one group, of order 12. A Cartan subalgebra modulo 11 other than $\bar{\mathfrak{c}}_0$ is a line spanned by $a + \Xi$ with $\Xi \in \mathfrak{p}$ non-zero, and its orbit has at least 6 elements. A Cartan subalgebra over $\bar{\mathfrak{c}}_0$ other than $\mathfrak{c}_0$ is given by a non-zero $\Xi \in \mathfrak{p}$, as in the proof of Proposition 8.1, and its orbit has 12 elements. So $\mathfrak{c} = \mathfrak{c}_0$. □

Corollary 9.6. *If b is a divisor of degree 0 on X whose support misses V, then $i_{11}(z - y, b) = 0$, and so $h_{11}(z - y, b) = 0$.*

Proof. The disc V has one boundary point ξ, and the root of X^{an} lies outside V. So the paths from the root to y and to z both pass through ξ, and the path to a point $Q \notin V$ meets V at most at ξ. This gives $(y|Q) = (\xi|Q) = (z|Q)$. □

Proposition 9.7. *Let Z be an integer combination of the R_C, S_ν of Section 5 with $\mathrm{Tr}(Z \mid \mathcal{L}) = 0$. Then the support of $D(y, z) = \operatorname{Fix} Z - Z(y) - Z(z)$ misses V, and so $h_{11}(z - y, D(y, z)) = 0$.*

Proof. The tube of s in the j-line is $\mathcal{D}/\Gamma$, and $B_{\mathfrak{c}_0} \to B_D$ is an isomorphism. So, by the construction of V in its two cases, $\mathrm{j} \circ \pi$ is injective on V, on $\mathbb{C}_{11}$-points. By (9.1), on V we have $v(\mathrm{j} - \mathrm{j}(D)) > 0$, and if $D \neq D_s$ we have $v(\mathrm{j} - \mathrm{j}(D)) \geq \#\Gamma + 3$, that is, at least 5 at $D = -27, -12, -163$ and at least 6 at $D = -16, -67$. For these D, $v_{11}(\mathrm{j}(D) - \mathrm{j}(D_s))$ is 2 and 3, so $\mathrm{j}(D_s)$ is not a value on V. All values on V are integral and lie in one residue class modulo 11, and $0 \not\equiv 1728 \bmod 11$. So V has no point over $j = 0, 1728, \infty$ if $D \neq D_s$, and if $D = D_s$ the only such point is y.

Let T be a term of Z. The point $y = [A, \pm x]$ is not fixed by T, because $\operatorname{Aut} A$ lies in the Cartan subring $(\mathbb{Z}/121)[x]$ and so fixes $\pm x$. By Proposition 5.1, V therefore holds no fixed point of T. A point of $T(y)$ in V has the j-invariant of y, so it is y by injectivity, and then y is fixed by T. A point of $T(z)$ in V is likewise z, and then z is a fixed point of T in V. So $T(y)$, $T(z)$ and $\operatorname{Fix} T$ all miss V. By Corollary 9.6 the symbol vanishes, as $D(y, z)$ has degree 0. □

10. The rank

Proposition 10.1. $\operatorname{rank} J(\mathbb{Q}) = 511$.

Proof. Rouse, Sutherland and Zureick-Brown state that every isogeny factor of J has analytic rank equal to its dimension [58, §1.1]. By [13, Theorem 1.4], J is isogenous over $\mathbb{Q}$ to the product of the new quotients of the Jacobians of $X_0^+(121)$ and $X_0^+(14641)$. So J is isogenous to $\prod_f A_f$, over the Galois orbits of newforms f of weight 2 and level $M \in \{121, 14641\}$ with Fricke eigenvalue $+1$, where A_f is the quotient of $J_0(M)$ attached to f. There are nine orbits [58, Table 14]: 121.2.a.b, which is E, and 14641.2.a.{a, b, c, d, e, g, i, j}, of dimensions 1 and $5, 5, 35, 35, 50, 90, 90, 200$, with sum 511.

If $L'(f,1) \neq 0$, then $\operatorname{rank} A_f(\mathbb{Q}) = \dim A_f$ [21, Proposition 7.1]. This is the analogue at rank one of [48, Theorem 0.3], and it rests on Gross–Zagier [31]; see [21, Remark 7.3] for its history. As A_f depends only on the orbit of f, it is enough to find one f in each orbit with $L'(f,1) \neq 0$. The root number of f is -1, so

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

From $|a_n| \leq 2n$ and $E_1(x) \leq e^{-x}/x$, the terms with $n > 1154$ contribute less than $1.2 \cdot 10^{-26}$ at $M = 14641$.

Let $\mathcal{T} := 2T_2 + 2T_3 + T_7 + T_{13} + T_{17} + 2T_{19} + T_{31}$. A computation in python-flint on the modular symbols of level 14641 finds the exact characteristic polynomial of $\mathcal{T}$. A form from a lower level occurs in it at least twice, and Eisenstein eigenvalues exceed the Weil bound at some prime, so an irreducible factor of multiplicity one with real roots, on which the coefficients below satisfy $|a_r| \leq 2\sqrt{r}$, is one orbit of newforms. Eight such factors have Fricke sign $+1$; their degrees are $5, 5, 35, 35, 50, 90, 90, 200$, and they are the eight orbits of level 14641 above. For each, let f be the conjugate at the largest real root μ of that factor. In ball arithmetic, $a_r = \psi(T_r\gamma_q)/\psi(\gamma_q)$ for the eigenfunctional ψ and primes $r \leq 1154$, $r \neq 11$, and the three paths $\gamma_q = \{1/q, \infty\}$, $q = 29, 37, 43$, give overlapping balls. With the bound on the tail added to the radius, the series gives balls of radius less than 10^{-10} about the following values, truncated:

$\dim A_f$	5	5	35	35	50	90	90	200
μ	14.343	10.998	15.381	21.084	19.787	28.371	29.153	22.522
$L'(f,1)$	1.9392	3.8038	11.339	7.8327	4.5795	7.1212	9.0620	5.9315

The two orbits of dimension 5 are 14641.2.a.a and 14641.2.a.b, in this order. So $|L'(f,1)| > 1.93$ for one f in each of the eight orbits. At level 121 the same series gives $L'(E,1) = 0.86237\ldots$. □

11. The primes 17 and 43

We finish by applying Theorem 1.2 and Proposition 3.3 at $p = 17$ and $p = 43$. At both primes Section 6 gives (B) and étale blocks, 24 at 17 and 87 at 43, hence (M); (Φ) is Lemma 6.2; and $\operatorname{rank} J(\mathbb{Q}) \leq 511$ is Proposition 10.1. By Table 2, $y_1 = y(-67)$, $y_2 = y(-4)$, $y_3 = y(-3)$ and $y_4 = y(-163)$.

Let k and p be as in Corollary 8.3, with $\bar{A}$ the curve at $\bar{y}_k$. By the proof of Proposition 8.1, $\operatorname{Aut}\bar{A}$ lies in the Cartan subring, so the j-line at $\mathrm{j}(D_k)$, the curve $\bar{E}$ at $k\bar{P}_0$ and the curve $\mathcal{X}_{\mathbb{F}_p}$ at $\bar{y}_k$ have the same completed local ring, $W[[t]]^{\operatorname{Aut}(\bar{A})/\{\pm 1\}}$ [19, I, (8.2.1)]. Hence j is a parameter of $\mathcal{X}$ at $\bar{y}_k$, up to the constant $\mathrm{j}(D_k)$, and $\bar{\pi}$ is unramified there. As $\operatorname{Aut}\bar{A}$ fixes

the Cartan subring of $\bar{y}_k$, no R_C or S_ν has a branch through $(\bar{y}_k, \bar{y}_k)$. The condition on $(\bar{y}_k, \bar{y}_k)$ in Theorem 1.2(c) therefore holds for every integer combination Z of them. At each prime it remains to check Theorem 1.2(b) and to choose $\mathfrak{m}$, u and Z as in Proposition 3.3. The conditions $\mathrm{Tr}(Z \mid \mathcal{L}) = 0$ and $\theta(Z) = 0$ are linear in the coefficients of Z; among their solutions we need one with $c_{\mathfrak{m}}(u, \mathrm{Fix}\, Z) \neq 0$.

The prime 17. Let $\mathfrak{m}$ be the block of E, with character $\theta(T_q) = a_q(E) \bmod 17$, so that $\mathbb{T}_{\mathfrak{m}} = \mathbb{Z}_{17}$ and $e_{\mathfrak{m}} = 121^{-1}\pi^*\pi_*$, as $\deg \pi = 121$. The form $\pi^*\omega_E$, for ω_E the Néron differential, spans $S[\mathfrak{m}]$.

For n prime to 11 and $P \in E$, the sum of T_nP in the group of E is $a_n(E)P + \tau_n$, with $\tau_n \in E(\mathbb{Q})$. As divisors, T_n carries the sum of the five cusps to $\sigma(n)$ times itself, so adding over the cusps gives $5\tau_n = (\sigma(n) - a_n(E)) \sum_s C(s)$. By Section 7, $\sum_s C(s) = 22C_0 = O$. Since $E(\mathbb{Q})$ has no torsion, $\tau_n = O$. For a rational divisor v on X, define $\kappa(v) \in \mathbb{Z}$ by requiring that the sum of $\pi_* v$ on E be $\kappa(v)P_0$. As $a_{17}(E) = 0$, $\tau_{17} = O$ and $\#E(\mathbb{F}_{17}) = 18$, the sum of $\pi_* Bv$ is $18\kappa(v)P_0$. A computation in Python and PARI/GP gives

$$v_{17} \log_E(18P_0) = 2.$$

So for every rational u, $\lambda_u(\pi^*\omega_E) = 17^{-1} \log_E(18\kappa(u)P_0) \equiv 0$ modulo 17: the functional λ_u vanishes on $S[\mathfrak{m}]$. In particular $A_{15}(\cdot\,; y(-16))$ vanishes on this block, by Lemma 6.3.

Let h_E be the Coleman–Gross height on E for the complement $W_E := (\pi^*)^{-1}(e_{\mathfrak{m}} W)$. By the projection formula,

$$c_{\mathfrak{m}}(u, v) \equiv \frac{18^2}{121 \cdot 17} \kappa(u)\kappa(v)\, h_E(P_0, P_0) \pmod{17}. \tag{11.1}$$

We compute h_E from (1.3) on E itself. Put $R := 18P_0$; it lies in $E_2(\mathbb{Q}_{17})$, and in the identity component at 11 since 18 is even. For $T = tP_0$ with $18 \nmid t$, the divisors $(T + R) - (T)$ and $(R) - (O)$ have degree 0 on every residue disc at 17, and no disc meets both. So, with $d(Q)$ the denominator of Q, that is $x(Q) = a/d(Q)^2$ in lowest terms,

$$h_E(R, R) \equiv -\log_{17} \frac{d(T)^2}{d(T + R)\, d(T - R)} \pmod{17^2}.$$

A computation in Python gives $h_E(R, R) \equiv 6 \cdot 17 \bmod 17^2$. As $18^2 \equiv 1$ modulo 17, also $h_E(P_0, P_0) \equiv 6 \cdot 17 \bmod 17^2$, and (11.1) becomes

$$c_{\mathfrak{m}}(u, v) \equiv 3\, \kappa(u)\kappa(v) \pmod{17}. \tag{11.2}$$

Remark 11.1. The curve E is supersingular at 17, so the height here is that of Coleman and Gross [18, §§5–6], for a complement that cannot be the unit root subspace. The value modulo 17^2 does not depend on the complement: changing W_E by $c\,\omega_E$ changes $h_E(P_0, P_0)$ by $c \log_E(P_0)^2$, of valuation at least 4.

Take $u := y(-67)$, so that $\kappa(u) = 1$. By Lemma 6.3, λ_u is a unit times $A_{15}(\cdot\,; y(-67))$, and a computation with Proposition 6.6 shows that this vanishes on exactly one of the 24 blocks, the block of E. So the condition on u in Proposition 3.3 holds.

For $k = -1, 1, 2$, the form $\pi^*\omega_E$ does not vanish at $\bar{y}_k$, since ω_E has no zeros and $\bar{\pi}$ is unramified at $\bar{y}_k$. This is condition (b) of Theorem 1.2.

It remains to choose Z. The eigenvalues of our correspondences on this block are explicit. Reduction modulo 11 sends the orbit of R_C onto an orbit $\bar{R}$ on the Cartan subrings modulo

11, with fibers of size $|R_C|/|\bar{R}|$, and it sends the orbit of S_ν to a point. As $\pi^*\omega_E$ spans $S[\mathfrak{m}]$, this gives

$$\theta(S_\nu) = 12, \qquad \theta(R_C) = \frac{|R_C|}{|\bar{R}|}\,\bar{\chi}(C \bmod 11),$$

where $\bar{\chi}$ is the eigenvalue of $\bar{R}$ on E. As E has genus one, this is the trace, and the proof of Proposition 5.1 at level 11 gives $|\bar{R}| - \frac{1}{2}\deg \operatorname{Fix} \bar{R}$. This gives $\bar{\chi} = -3, 0, 2, -4, 4$ and $|\bar{R}| = 6, 12, 12, 12, 12$ at $\pm C \equiv 0, 2, 3, 4, 5 \bmod 11$.

Take $Z := S_{-1} - S_1 - R_{50} - R_{18}$. Then $\operatorname{Tr}(Z \mid \mathcal{L}) = 0$ by Table 1, and $\theta(Z) = 12 - 12 - 44 + 44 = 0$. As $\kappa(y(-4)) = 2$ and $\kappa(y(-3)) = 3$, Proposition 5.1, (3.3), (5.1) and (11.2) give, for T a term of Z,

$$c_{\mathfrak{m}}(u, \operatorname{Fix} T) = 3\kappa(u)\big(\theta(F_4^* T) + 2\theta(F_3^* T)\big),$$

and the bracket is $-30, 36, 66, 0$ at $T = S_{-1}, S_1, R_{50}, R_{18}$. So

$$c_{\mathfrak{m}}(u, \operatorname{Fix} Z) = 3(-30 - 36 - 66 - 0) = -396 \equiv 12 \pmod{17}.$$

The prime 43. Let $\mathfrak{m}$ be the block of $\mathbb{T}_{43}$ with $a_2, a_3, a_5, a_7, a_{13}, a_{17} \equiv 29, 42, 0, 4, 11, 9$. It has degree one, so $\mathbb{T}_{\mathfrak{m}} = \mathbb{Z}_{43}$, and it lies on the factor A_f of dimension 5 with f in 14641.2.a.b, of coefficient field $\mathbb{Q}(\zeta_{11})^+$. Take $u := y(-163)$. By Lemma 6.3, λ_u is a unit times $A_{41}(\cdot\,; y(-163))$, and a computation with Proposition 6.6 shows that this vanishes on exactly one of the 87 blocks, namely $\mathfrak{m}$. So the condition on u in Proposition 3.3 holds; it gives $a \geq 2$, which suffices.

For condition (b) of Theorem 1.2, a computation shows that $A_0 \neq 0$ on $S[\mathfrak{m}]$ at y_{-2}, y_0, y_4 and that $[u^2]\tilde{F} \neq 0$ on $S[\mathfrak{m}]$ at y_3. As j is a parameter at these points, A_0 and, by (6.3), $[u^2]\tilde{F}$ are units times the value of $\omega/d\mathrm{j}$. Hence the non-zero forms in $S[\mathfrak{m}]$ do not vanish there.

Take $Z := R_2$. Then $\operatorname{Tr}(Z \mid \mathcal{L}) = 0$ and

$$\operatorname{Fix} R_2 = \tfrac{1}{2}R_{51}\, y(-4) + \tfrac{2}{3}R_{52}\, y(-3) + 2\mathbf{C}$$

by Table 1. A correspondence T acts on the forms of Section 6 by $TF = \sum_{Hg \subset T} F^g$, with F^g as in the proof of Proposition 6.1, and a computation in C and Python on $S[\mathfrak{m}]$ gives

$$\theta(R_2) = \theta(R_{51}) = 0, \qquad \theta(R_{52}) = 30.$$

So by (3.3) and (5.1), $c_{\mathfrak{m}}(u, \operatorname{Fix} R_2) = \frac{2}{3} \cdot 30 \cdot c_{\mathfrak{m}}(y(-163), y(-3))$.

The last number comes from Proposition 4.9 with $(D_1, D_2) = (-163, -3)$. For the 616 values of m of Section 6 it gives $p^{-1}h([By(-163)], T_m[By(-3)]) \equiv \mathcal{A}(m) - 2\mathcal{A}(43m) + \mathcal{A}(1849m)$. The 616 right-hand sides satisfy the 105 linear relations among the T_m. The T_m have rank 511 on S, so they span $\mathbb{T}/43$, and the idempotent of $\mathfrak{m}$ is a combination $\sum_m b_m T_m$ read from their table. Then $c_{\mathfrak{m}}(y(-163), y(-3)) = \sum_m b_m(\mathcal{A}(m) - 2\mathcal{A}(43m) + \mathcal{A}(1849m))$, and a computation of the sums over x in C and of this combination in python-flint gives $c_{\mathfrak{m}}(y(-163), y(-3)) \equiv 27 \bmod 43$. Hence

$$c_{\mathfrak{m}}(u, \operatorname{Fix} R_2) = 20 \cdot 27 \equiv 24 \pmod{43}.$$

By Proposition 3.3, $e_{\mathfrak{m}}[Bu'] \in \mathbb{Z}_p\, e_{\mathfrak{m}}[Bu]$ for every rational u', so $\lambda_{u'}$ vanishes on $S[\mathfrak{m}]$; indeed $A_{41}(\cdot\,; y(-27))$ and $A_{41}(\cdot\,; y(-12))$ both vanish on $S[\mathfrak{m}]$.

Remark 11.2. Neither prime suffices alone. The curve E cannot: of the two primes of Remark 3.2, the fields $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-163})$ are inert at 17, and all four CM fields are inert at 32411; a larger prime is out of reach of Proposition 8.1, which needs $p < 121|d|/4 < 4931$. So those two fields need a second block. At 43 there are 22 blocks of residue degree one, so

the heuristic of Remark 3.2 expects about 22/43 non-saturated blocks among them, and we find one.

The end of the proof. By Proposition 7.3, a point $z \in X(\mathbb{Q})$ has a class k. By Corollary 8.3, $\bar{z} = \bar{y}_k$ at $p = 17$ for $k = -1, 1, 2$ and at $p = 43$ for $k = -2, 0, 3, 4$. With the u and Z above, Proposition 3.3 gives condition (a) and the height condition of Theorem 1.2. By Proposition 9.7 the local term at 11 vanishes, and Theorem 1.2 gives $z = y_k$. So $X(\mathbb{Q})$ is the set of the seven points of Lemma 7.1.

Finally let $A/\mathbb{Q}$ have no complex multiplication, with mod 11 image in $N_{\mathrm{ns}}(11)$. By [10, Theorem 1.1], its 11-adic image is the full preimage of $N_{\mathrm{ns}}(11^n)$ for some $n \geq 1$. If $n \geq 2$, then A gives a rational point of X that is not CM, which is impossible. This proves Theorem 1.1.

Appendix A. Computations

The computations the proof uses are listed in Table 3, with where each is used; the last row is used only by Remarks 3.2 and 11.2. All are exact, in integers, rationals, finite fields, number fields or power series over them, except the L-values, which are in ball arithmetic. We used PARI/GP 2.17.3, Python 3.12 with python-flint 0.8.0 and NumPy 2.5.2, and C compiled with gcc 13.3.0. The programs and their outputs are deposited at [38].

Computes	Software	Used in
Exponents of ε_k; A_r at $r = 2069, 3301, 3631$; the congruence modulo 239580 at $r = 53, 2069, 12101, 5313353$; $\mathrm{N}\, f(C_0) = 11^{55}$	PARI/GP	Section 7
$\#E(\mathbb{F}_p)$, splitting and residues of $\mathrm{j}(D)$ at $p = 17, 43$	Python	Corollary 8.3
$x'(22P_0)$; the series S_k	PARI/GP	Lemmas 9.1 and 9.2
One $L'(f, 1)$ for each of the eight orbits at level 14641, and $L'(E, 1)$	python-flint	Proposition 10.1
The 780 products: rank 565, 215 relations, c_0-rank 54, $\dim S = 511$	C, python-flint	Section 6
$\mathrm{rank}(1 - T_p \mid S) = 511$; the blocks	python-flint	Sections 6 and 11
s_2; the jets A_{15}, A_{41}, A_0 and $[u^2]\tilde{F}$ at $y(-3)$ on the blocks	python-flint, PARI/GP	Sections 6 and 11
The table of T_m on S for the 616 values of m	C, python-flint	Section 6
The sums over x of Proposition 4.9 at $(-163, -3)$, for $n = m, 43m, 1849m$	C	Section 11
$c_{\mathfrak{m}}(y(-163), y(-3))$ at 43 from the sums and the table	python-flint	Section 11
The 61 orbits, F_4, F_3, $n(T)$ and the traces, by enumeration of the 6655 pairs	Python	Section 5
TF on the forms: $\theta(R_2)$, $\theta(R_{51})$, $\theta(R_{52})$ at 43; the eigenvalues on E	C, Python	Section 11
$v_{17} \log_E(18P_0)$ and $h_E(P_0, P_0)$	Python, PARI/GP	Section 11
The primes $p \leq 2 \cdot 10^7$ with $\#E(\mathbb{F}_p)P_0 \in E_2(\mathbb{Q}_p)$	C	Remarks 3.2 and 11.2

Table 3. The computations.

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. 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 [38].

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 and Amnon Besser, *Computing local p-adic height pairings on hyperelliptic curves*, Int. Math. Res. Not. IMRN (2012), no. 11, 2405–2444, doi:10.1093/imrn/rnr111, arXiv:1010.6009v1.
5. ———, *Errata for "Computing local p-adic heights on hyperelliptic curves"*, 2021, http://math.bu.edu/people/jbala/cg_heights_errata.pdf.
6. 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.
7. 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.
8. Massimo Bertolini, Henri Darmon, and Kartik Prasanna, *Generalized Heegner cycles and p-adic Rankin L-series*, Duke Math. J. **162** (2013), no. 6, 1033–1148, doi:10.1215/00127094-2142056.
9. Amnon Besser, *Syntomic regulators and p-adic integration. II. K_2 of curves*, Israel J. Math. **120** (2000), 335–359, doi:10.1007/BF02834844.
10. Matthew Bisatt, Lorenzo Furio, and Davide Lombardo, *Explicit p-adic Hodge theory for elliptic curves and non-split Cartan images*, 2026, Preprint, arXiv:2603.04021v2.
11. 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.
12. Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.
13. 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.
14. Imin Chen and Gleb Glebov, *On Chudnovsky–Ramanujan type formulae*, Ramanujan J. **46** (2018), no. 3, 677–712, doi:10.1007/s11139-017-9948-8.
15. David V. Chudnovsky and Gregory V. Chudnovsky, *Approximations and complex multiplication according to Ramanujan*, Ramanujan Revisited, Academic Press, 1988, pp. 375–472.
16. Adina Cohen, Michael Temkin, and Dmitri Trushin, *Morphisms of Berkovich curves and the different function*, Adv. Math. **303** (2016), 800–858, doi:10.1016/j.aim.2016.08.029, arXiv:1408.2949v3.
17. Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770, doi:10.1215/S0012-7094-85-05240-8.
18. 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.
19. 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.

20. Netan Dogra, *The Chabauty–Coleman method and p-adic linear forms in logarithms*, 2020, Preprint, arXiv:2008.09560v1.
21. Netan Dogra and Samuel Le Fourn, *Quadratic Chabauty for modular curves and modular forms of rank one*, Math. Ann. **380** (2021), no. 1–2, 393–448, doi:10.1007/s00208-020-02112-3, arXiv:1906.08751v3.
22. Juanita Duque-Rosero, Sachi Hashimoto, and Pim Spelier, *Geometric quadratic Chabauty and p-adic heights*, Expo. Math. **41** (2023), no. 3, 631–674, doi:10.1016/j.exmath.2023.05.003, arXiv:2207.10389v3.
23. Bas Edixhoven and Guido Lido, *Geometric quadratic Chabauty*, J. Inst. Math. Jussieu **22** (2023), no. 1, 279–333, doi:10.1017/S1474748021000244.
24. Bas Edixhoven and Pierre Parent, *Semistable reduction of modular curves associated with maximal subgroups in prime level*, Doc. Math. **26** (2021), 231–269, doi:10.4171/dm/814, arXiv:1907.02418v2.
25. Lorenzo Furio, *Effective bounds for adelic Galois representations attached to elliptic curves over the rationals*, 2024, Preprint, arXiv:2412.10340v4.
26. 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.
27. Benedict H. Gross, *On canonical and quasi-canonical liftings*, Invent. Math. **84** (1986), no. 2, 321–326, doi:10.1007/BF01388810.
28. Benedict H. Gross and Kevin Keating, *On the intersection of modular correspondences*, Invent. Math. **112** (1993), no. 1, 225–245, doi:10.1007/BF01232433.
29. Benedict H. Gross, Winfried Kohnen, and Don B. Zagier, *Heegner points and derivatives of L-series. II*, Math. Ann. **278** (1987), 497–562, doi:10.1007/BF01458081.
30. Benedict H. Gross and Don B. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220, doi:10.1515/crll.1985.355.191.
31. ———, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320, doi:10.1007/BF01388809.
32. Emmanuel Halberstadt, *Sur la courbe modulaire* $X_{\text{ndép}}(11)$, Experiment. Math. **7** (1998), no. 2, 163–174, doi:10.1080/10586458.1998.10504366.
33. 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.
34. Sachi Hashimoto and Pim Spelier, *A geometric linear Chabauty comparison theorem*, Acta Arith. **202** (2022), no. 1, 67–88, doi:10.4064/aa210616-6-10, arXiv:2102.04967v3.
35. Gustav Herglotz, *Über einen Dirichletschen Satz*, Math. Z. **12** (1922), no. 1, 255–261, doi:10.1007/BF01482079.
36. Benjamin Howard and Tonghai Yang, *Singular moduli refined*, Arithmetic geometry and automorphic forms, Adv. Lect. Math. (ALM), vol. 19, Int. Press, Somerville, MA, 2011, pp. 367–406, arXiv:1202.6410.
37. Jun-ichi Igusa, *On the algebraic theory of elliptic modular functions*, J. Math. Soc. Japan **20** (1968), no. 1–2, 96–106, doi:10.2969/jmsj/02010096.
38. Manvir Jaswal, *Programs and data for "The rational points of the non-split Cartan modular curve of level 121"*, 2026, Zenodo, doi:10.5281/zenodo.24061904.
39. ———, *The rational points of the non-split Cartan modular curve of level 25*, 2026, Preprint, Zenodo, doi:10.5281/zenodo.24061911.
40. 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/.
41. Nicholas M. Katz, *p-adic interpolation of real analytic Eisenstein series*, Ann. of Math. (2) **104** (1976), no. 3, 459–571, doi:10.2307/1970966.
42. ———, *Serre–Tate local moduli*, Surfaces algébriques, Lecture Notes in Math., vol. 868, Springer, 1981, doi:10.1007/BFb0090648, pp. 138–202.
43. ———, *Wieferich past and future*, Topics in Finite Fields, Contemp. Math., vol. 632, Amer. Math. Soc., 2015, doi:10.1090/conm/632/12632, pp. 253–270.
44. Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Ann. of Math. Stud., vol. 108, Princeton University Press, 1985, doi:10.1515/9781400881710.
45. Kamal Khuri-Makdisi, *Moduli interpretation of Eisenstein series*, Int. J. Number Theory **8** (2012), no. 3, 715–748, doi:10.1142/S1793042112500418, arXiv:0903.1439v6.
46. Minhyong Kim, *The motivic fundamental group of* $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ *and the theorem of Siegel*, Invent. Math. **161** (2005), no. 3, 629–656, doi:10.1007/s00222-004-0433-9.
47. ———, *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. **45** (2009), no. 1, 89–133, doi:10.2977/prims/1234361156.

48. Viktor A. Kolyvagin and Dmitrii Yu. Logachev, *Finiteness of the Shafarevich–Tate group and the group of rational points for some modular abelian varieties*, Algebra i Analiz **1** (1989), no. 5, 171–196, In Russian.
49. Kristin Lauter and Bianca Viray, *On singular moduli for arbitrary discriminants*, Int. Math. Res. Not. IMRN (2015), no. 19, 9206–9250, doi:10.1093/imrn/rnu223.
50. Marius Leonhardt and Isabel Rendell, *Aspects of quadratic Chabauty via modular forms*, 2026, Preprint, arXiv:2610.30703v1.
51. Gérard Ligozat, *Courbes modulaires de niveau 11*, Modular functions of one variable, V, Lecture Notes in Math., vol. 601, Springer, Berlin, 1977, doi:10.1007/BFb0063948, pp. 149–237.
52. Jonathan Love, Élie Studnia, and Jan Vonk, *Arithmetic intersections on non-split Cartan modular curves*, 2026, Preprint, arXiv:2604.06963v1.
53. David Masser, *Elliptic functions and transcendence*, Lecture Notes in Math., vol. 437, Springer, 1975.
54. 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.
55. Barry Mazur and John Tate, *Canonical height pairings via biextensions*, Arithmetic and Geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser, 1983, pp. 195–237.
56. Michael Rapoport, *Deformations of isogenies of formal groups*, Astérisque **312** (2007), 139–169.
57. Fernando Rodriguez Villegas and Don Zagier, *Square roots of central values of Hecke L-series*, Advances in Number Theory, Oxford University Press, 1993, doi:10.1093/oso/9780198536680.003.0006, pp. 81–99.
58. 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.
59. René Schoof and Nikos Tzanakis, *Integral points of a modular curve of level 11*, Acta Arith. **152** (2012), no. 1, 39–49, doi:10.4064/aa152-1-4, arXiv:1107.2776v1.
60. 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.
61. 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.
62. Joseph H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237, doi:10.1016/0022-314X(88)90019-4.
63. José Felipe Voloch, *Elliptic Wieferich primes*, J. Number Theory **81** (2000), no. 2, 205–209, doi:10.1006/jnth.1999.2471.
64. 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.
65. Stefan Wewers, *Canonical and quasi-canonical liftings*, Astérisque **312** (2007), 67–86.
66. Don Zagier, *Elliptic modular forms and their applications*, The 1-2-3 of Modular Forms, Springer, 2008, doi:10.1007/978-3-540-74119-0_1, pp. 1–103.

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