ON THE MANIN CONSTANT

ZHUONI CHI

with an appendix by Shurui Liu and Ping Nie

Abstract. We prove the Manin constant conjecture for every optimal elliptic curve over $\mathbb{Q}$ and Stevens' Conjectures I and II. Our method adapts Hongbo Yin's congruence argument for cubic roots of modular functions to lifts of modular parametrizations through isogenies, using the unbounded denominators theorem of Calegari, Dimitrov and Tang.

Contents

1. Introduction 2
1.1. Main results 2
1.2. The normalized lift 3
1.3. Outline of this article 5
1.4. What's new in this article 5
1.5. Acknowledgements 7
2. Deduction of the main theorems 7
2.1. Proof of the Manin constant conjecture 7
2.2. Proof of Stevens' conjectures 8
3. Integrality 9
3.1. Formal logarithms at primes of additive reduction 9
3.2. Integrality of the normalized lift 10
4. Modularity and rationality of normalized lifts 12
4.1. Modularity 12
4.2. Level 13
4.3. Rationality 14
5. Igusa curves and the local torsion 15
5.1. The moduli problems 15
5.2. Connectedness of the special fibre 19
5.3. Proof that $c = 1$ 19
Declaration of generative AI use 20
Appendix A. Details of generative AI usage 21
A.1. Persistent prompting with math guidance: the initial proof 21
A.2. Non-math prompting with feasibility hint: a second proof 21
A.3. Agentic AI reviewer 22
A.4. Agentic systems: one-shot reproduction of the proof 22
A.5. Where the idea came from 22
References 23

2020 *Mathematics Subject Classification.* Primary 11G05; Secondary 11F11, 11G18, 14G35.

Key words and phrases. Manin constant, Manin–Stevens constant, optimal quotient, modular parametrization, unbounded denominators, congruence subgroups, Igusa curves, Néron models.

1. Introduction

1.1. **Main results.** Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, and let $f = \sum_{n\geq 1} a_n q^n$ be the newform of weight two and level N attached to E. Here $q = e^{2\pi i z}$, with z in the upper half-plane $\mathfrak{H}$. We write

$$\omega_f = 2\pi i f(z)\,\mathrm{d}z = f(q)\frac{\mathrm{d}q}{q}$$

for the corresponding differential on the modular curve $X_0(N)$. A surjection $\pi_0 : J_0(N) \twoheadrightarrow E$ is called *optimal* if its kernel is connected. Each isogeny class contains exactly one curve admitting an optimal quotient, and π_0 is then unique up to sign. Let

$$\varphi_0 : X_0(N) \longrightarrow E, \qquad \varphi_0(P) = \pi_0([P] - [\infty])$$

be the corresponding modular parametrization, and let ω_E be a Néron differential of E. By multiplicity one there is a constant $c_E \in \mathbb{Q}^\times$, the *Manin constant*, with

$$\varphi_0^*\omega_E = c_E\,\omega_f.$$

Manin conjectured that $c_E = \pm 1$ [Man71, Section 10.3]; see [Čes18, Conj. 1.1] for the formulation used here.

Theorem 1.1 (Manin constant conjecture)**.** *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, and let $\pi_0 : J_0(N) \twoheadrightarrow E$ be an optimal quotient. Then $c_E = \pm 1$.*

We will prove this conjecture in Section 2 under some assumptions and remove the assumptions in Sections 3 and 4. The case $|c_E| = 2$ will be excluded in Section 5 because the techniques there are heavier.

Stevens studied the analogous question for $X_1(N)$ [Ste89]. Here $X_1(N)$ denotes Shimura's canonical model over $\mathbb{Q}$, in which the cusp 0 is a rational point [Ste89, Section 1]. Let $\mathcal{C}$ be an isogeny class of elliptic curves over $\mathbb{Q}$ of conductor N. There is a unique $E_1 \in \mathcal{C}$ admitting a parametrization $\varphi_1 : X_1(N) \to E_1$ which sends the cusp 0 to 0 and the Jacobian map $\pi_1 : J_1(N) \twoheadrightarrow E_1$ has connected kernel. By [Ste89, Prop. 1.4], φ_1 is unique up to sign. Its Manin constant c_1 is defined by

$$\varphi_1^*\omega_{E_1} = c_1\,\omega_f^{\mathrm{St}},$$

where ω_{E_1} is a Néron differential and ω_f^{St} is the differential attached to f in [Ste89, Def. 1.1] (see Section 2.2). Stevens proved that $c_1 \in \mathbb{Z}$ [Ste89, Thm. 1.6]. In each isogeny class $\mathcal{C}$ there is a unique curve $E_{\min}$ such that, for every $E \in \mathcal{C}$, there is an isogeny $E_{\min} \to E$ over $\mathbb{Q}$ which extends to an étale morphism of Néron models over $\mathbb{Z}_p$ for every prime p [Ste89, Thm. 2.3]. He also conjectured the following:

Theorem 1.2 (Stevens' Conjectures I and II)**.** *For every isogeny class of elliptic curves over $\mathbb{Q}$ we have $c_1 = \pm 1$ and $E_1 \simeq E_{\min}$.*

The two assertions are Stevens' Conjecture I′(a) and Conjecture II, respectively. Together they imply his Conjecture I [Ste89, (1.7), Thms. 1.8 and 2.3, (2.4)]. The first assertion follows from Theorem 1.1 by [Čes18, Lemma 2.12]. The second will be deduced from Theorem 1.1 and Theorem 1.6 below in Section 2.2.

1.2. **The normalized lift.** The central object of this article is the lift of a modular parametrization through an isogeny. Let $\nu : E' \to E$ be an isogeny and let φ be a morphism from a modular curve to E. Since $\mathfrak{H}$ is simply connected, φ lifts through ν to a holomorphic map $\mathfrak{H} \to E'(\mathbb{C})$. We first fix the modular curves on which φ is defined.

For a subgroup $G \subseteq \mathrm{SL}_2(\mathbb{Z})$ we write $\pm G = \langle G, -I\rangle$, and we put $\Gamma_1^{\pm}(N) = \pm\Gamma_1(N)$. Let $X_\mu(N)$ be the compactified moduli space over $\mathbb{Q}$ of pairs (A, ι), where A is an elliptic curve and $\iota : \mu_N \hookrightarrow A$ is a closed immersion [KM85, Section 4.9 and 8.6.3]. Let ∞ be the cusp of $X_\mu(N)$ corresponding to the Tate curve $\mathrm{Tate}(q)$ over $\mathbb{Q}((q))$ with $\mu_N \subseteq \mathbb{G}_{\mathrm{m}}$. It is a rational point, and the completion of $X_\mu(N)$ along it is $\operatorname{Spf}\mathbb{Q}[[q]]$ [KM85, Thm. 8.11.10]. In terms of generalized elliptic curves, ∞ is given by the standard Néron 1-gon with μ_N embedded in its smooth locus $\mathbb{G}_{\mathrm{m}}$ [CES03, proof of Lemma 6.1.6]. Analytically we use the identification

$$\Gamma_1^{\pm}(N)\backslash\mathfrak{H}^* \simeq X_\mu(N)(\mathbb{C}), \qquad z \longmapsto \big(\mathbb{C}/(\mathbb{Z}z+\mathbb{Z}),\ e^{2\pi i/N} \mapsto 1/N\big),$$

under which ∞ corresponds to ∞ and $q = e^{2\pi i z}$.

For $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$ the diamond operator $\langle\delta\rangle : (A, \iota) \mapsto (A, \iota \circ [\delta])$ is an automorphism of $X_\mu(N)$ over $\mathbb{Q}$, and $\langle -1\rangle$ is the identity. A matrix $\gamma = \left(\begin{smallmatrix} a & b \\ Nr & d\end{smallmatrix}\right) \in \Gamma_0(N)$ acts on $X_\mu(N)(\mathbb{C})$ as $\langle d\rangle$: the map $w \mapsto (Nrz + d)w$ is an isomorphism $\mathbb{C}/(\mathbb{Z}\gamma z + \mathbb{Z}) \to \mathbb{C}/(\mathbb{Z}z + \mathbb{Z})$ sending $1/N$ to d/N modulo $\mathbb{Z}z + \mathbb{Z}$.

Let Γ be a group with $\Gamma_1^{\pm}(N) \subseteq \Gamma \subseteq \Gamma_0(N)$, let Δ_Γ be the image of Γ under the homomorphism $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$, $\left(\begin{smallmatrix} a & b \\ Nr & d\end{smallmatrix}\right) \mapsto \pm d$, and put

$$X_\Gamma = X_\mu(N)/\Delta_\Gamma, \qquad \varpi_\Gamma : X_\mu(N) \longrightarrow X_\Gamma.$$

Then $X_\Gamma(\mathbb{C}) = \Gamma\backslash\mathfrak{H}^*$, and X_Γ has the rational cusp ∞ with parameter q. The cusps $\langle\delta\rangle\infty$ of $X_\mu(N)$ are rational. For $\Gamma = \Gamma_0(N)$ this is the usual model of $X_0(N)$, and we write $\varpi = \varpi_{\Gamma_0(N)} : (A, \iota) \mapsto (A, \iota(\mu_N))$. We also write ω_f for the pullbacks of ω_f to X_Γ and to $X_\mu(N)$. Their expansion at ∞ is again $f(q)\,\mathrm{d}q/q$.

Let $\nu : E' \to E$ be an isogeny of elliptic curves over $\mathbb{Q}$, and let $\varphi : X_\Gamma \to E$ be a non-constant morphism over $\mathbb{Q}$ with $\varphi(\infty) = 0$.

Definition 1.3. The *normalized lift* of φ through ν is the holomorphic map $\psi : \mathfrak{H} \to E'(\mathbb{C})$ with

$$\nu \circ \psi = \varphi \quad \text{on } \mathfrak{H}, \qquad \psi(z) \to 0 \text{ as } z \to i\infty.$$

Lemma 1.4. *The normalized lift exists and is unique. It satisfies $\psi(z+1) = \psi(z)$, and as a function of $q = e^{2\pi i z}$ it extends holomorphically to $q = 0$, with value 0 there.*

Proof. The map $\nu : E'(\mathbb{C}) \to E(\mathbb{C})$ is a finite covering and $\mathfrak{H}$ is simply connected, so φ lifts to a holomorphic map $\mathfrak{H} \to E'(\mathbb{C})$. If ψ_1 and ψ_2 are two lifts, then $\psi_1 - \psi_2$ is a continuous map from the connected space $\mathfrak{H}$ to the finite set $\ker\nu$, hence constant.

Choose a disc $D \subseteq E(\mathbb{C})$ around 0 over which ν is a trivial covering, and $y_0 > 0$ with $\varphi(z) \in D$ for $\operatorname{Im} z > y_0$. Let ψ_1 be a lift. Since the half-plane $\{\operatorname{Im} z > y_0\}$ is connected, ψ_1 maps it into a single component of $\nu^{-1}(D)$. This component maps homeomorphically onto D and contains exactly one point $\kappa \in \ker\nu$, so $\psi_1(z) \to \kappa$ as $z \to i\infty$. Then $\psi = \psi_1 - \kappa$ is a lift with $\psi(z) \to 0$. If ψ' is another such lift, the constant $\psi' - \psi \in \ker\nu$ equals the limit of $\psi'(z) - \psi(z)$ as $z \to i\infty$, which is 0. Hence the normalized lift exists and is unique.

The function $z \mapsto \psi(z+1) - \psi(z)$ is continuous with values in $\ker \nu$, hence constant, and its limit as $z \to i\infty$ is zero. Thus $\psi(z+1) = \psi(z)$, and ψ is a holomorphic function of q on a punctured disc which tends to 0 as $q \to 0$. It therefore extends across $q = 0$. □

We will study the geometry and arithmetic of this analytic map ψ. If x, y are the coordinate functions of a global minimal Weierstrass equation for E', then $x(\psi(q))$ and $y(\psi(q))$ lie in $\mathbb{Q}((q))$ (Lemma 3.4).

Lemma 1.5. *For $\gamma \in \Gamma$ the function $z \mapsto \psi(\gamma z) - \psi(z)$ is a constant $\rho(\gamma) \in \ker \nu$. The map $\rho : \Gamma \to \ker \nu$ is a homomorphism, and its kernel*

$$G_\psi = \ker \rho = \{\gamma \in \Gamma : \psi \circ \gamma = \psi\}$$

is a normal subgroup of finite index in Γ.

Proof. Since φ is Γ-invariant, $\psi \circ \gamma$ is also a lift of φ, so the difference is a continuous function with values in the finite group $\ker \nu$, hence constant. For $\gamma, \gamma' \in \Gamma$,

$$\rho(\gamma\gamma') = \big(\psi(\gamma\gamma' z) - \psi(\gamma' z)\big) + \big(\psi(\gamma' z) - \psi(z)\big) = \rho(\gamma) + \rho(\gamma').$$

The last assertion follows because $\ker \nu$ is finite. □

The most important result of this article is the following lifting theorem, which is proved in Section 4:

Theorem 1.6. *Suppose that the* bounded denominators condition (BDC) *holds for ψ: there is an integer $k \geq 1$ with*

$$k\, x(\psi(q)),\ \ k\, y(\psi(q)) \in \mathbb{Z}((q)).$$

Then the following hold.

(i) **(Modularity)** *G_ψ is a congruence subgroup and is normal in Γ. The compact modular curve $X_{G_\psi}(\mathbb{C})$ is the connected component through $(\infty, 0)$ of $X_\Gamma(\mathbb{C}) \times_{\varphi, E, \nu} E'(\mathbb{C})$.*

(ii) **(Level)** *$\Gamma_1^{\pm}(N) \subseteq G_\psi \subseteq \Gamma$, and G_ψ contains every parabolic and elliptic element of Γ.*

(iii) **(Rationality)** *There is a unique morphism $\psi_\mu : X_\mu(N) \to E'$ over $\mathbb{Q}$ with $\psi_\mu(\infty) = 0$ induced from ψ. ψ_μ satisfies $\nu \circ \psi_\mu = \varphi \circ \varpi_\Gamma$, where $\varpi_\Gamma : X_\mu(N) \to X_\Gamma$ is the quotient map.*

The monodromy group

$$H_\psi = \{\psi(\gamma z) - \psi(z) : \gamma \in \Gamma\} \subseteq \ker \nu$$

consists of the points $\tau_\delta = \psi_\mu(\langle\delta\rangle\infty)$, where $\langle\delta\rangle$ runs through the diamond operators in $\Gamma/\Gamma_1^{\pm}(N)$. Moreover, these points are rational, $H_\psi \subseteq E'(\mathbb{Q})$, and $\psi_\mu \circ \langle\delta\rangle = \psi_\mu + \tau_\delta$.

The component in (i) *descends to $\mathbb{Q}$, and its deck group is the constant group H_ψ, which is a quotient of Γ/Γ', where Γ' is the subgroup generated by $\Gamma_1^{\pm}(N)$ and the parabolic and elliptic elements of Γ.*

Theorem 1.1 uses the case $\nu = [c]$ where $c = |c_E|$, and Theorem 1.2 uses the case of the étale isogeny $E_{\min} \to E_1$.

We will prove the following proposition in Section 3 to show that (BDC) holds with $k = 1$ in both cases:

Proposition 1.7. *Let V be $X_0(N)$ or $X_\mu(N)$, let E be an elliptic curve over $\mathbb{Q}$ of conductor N with newform f, and let $\varphi : V \to E$ be a morphism over $\mathbb{Q}$ with $\varphi(\infty) = 0$.*

(i) *If $\varphi^*\omega_E = c\,\omega_f$ for an integer $c \geq 1$ such that $p^2 \mid N$ for every prime $p \mid c$, then the normalized lift of φ through $[c]$ satisfies (BDC) with $k = 1$.*

(ii) *If $\varphi^*\omega_E = \omega_f$ and $\nu : E' \to E$ is an isogeny over $\mathbb{Q}$ with $\nu^*\omega_E = \omega_{E'}$, then the normalized lift of φ through ν satisfies (BDC) with $k = 1$.*

Part (i) also follows from Honda's comparison of formal groups [Hon70, Thm. 9], but we give a direct proof in Section 3.

1.3. **Outline of this article.** In Section 2, we deduce Theorems 1.1 and 1.2 from Theorem 1.6, Proposition 1.7 and Proposition 5.10, whose proofs are postponed to Sections 3–5. Proposition 1.7 gives (BDC) for the two lifts we need, so that Theorem 1.6 applies to them. For the lift of φ_0 through $[c]$, optimality then gives $E[c] \subseteq E(\mathbb{Q})$, and the Weil pairing gives $c \mid 2$. Proposition 5.10 excludes $c = 2$. Stevens' conjectures follow from Theorem 1.1 together with Theorem 1.6 for the lift through $E_{\min} \to E_1$. We put the deduction first so that the reader can see how Theorem 1.6 is used, and why it suffices for the Manin constant conjecture, before the technical details.

In Section 3, we prove that the normalized lift ψ has integral q-expansions and (BDC) holds. The integrality of the modular parametrization (Lemma 3.5) follows [Edi91, proof of Prop. 2] and [Ste89, proof of Thm. 1.6]. The integrality of the lift through $[c]$ can be traced back to Honda's result [Hon70, Thm. 9], and we give a direct proof in Section 3.

In Section 4, we prove Theorem 1.6, which is the heart of this article. Here Proposition 1.7 gives integral expansions of the normalized lift first, so (BDC) holds with $k = 1$. Theorem 1.6 then turns this integrality into modularity and rationality of the lift.

In Section 5, we exclude the case $|c_E| = 2$. For a prime $p \mid N$ we construct a smooth scheme over the ring of integers of an unramified extension of $\mathbb{Q}_p$, with a map from its generic fibre to $X_\mu(N)$ and lifts of the diamond operators, whose geometric special fibre is an open subscheme of an Igusa curve and hence connected. This forces the points τ_δ of Theorem 1.6(iii) into the identity component of the Néron model of E at p. For $p \mid c$ this is impossible: E has additive reduction at p, so the identity component has at most p $\mathbb{Z}_p$-points killed by p, whereas $E[p]$ has p^2 points. Section 5 should be considered as part of Section 2, but we separate it because the techniques are much more complicated. This section works for general p but we only need $p = 2$ for the purpose of this article.

Figure 1 summarizes the logical dependencies among these sections.

1.4. **What's new in this article.** The study of the Manin constant has a long history. Edixhoven proved that c_E is an integer [Edi91, Prop. 2], and Česnavičius proved that $\mathrm{ord}_p(c_E) = 0$ whenever $p^2 \nmid N$ [Čes18, Thm. 2.11]. In particular the conjecture holds for semistable E. For earlier special cases see [Maz78], [AU96], [ARS06], [ČNS24] and the survey in [Čes18, Section 1]. For Stevens' conjectures, Stevens checked conductors up to 200 [Ste89, Thm. 7.1] and Vatsal treated some further cases [Vat05]. These methods are local: they study the Néron model of $J_0(N)$ at p, and they run into difficulty when $p^2 \mid N$, that is, when E has additive reduction at p. The integrality of the coordinate functions of ψ is closely related to

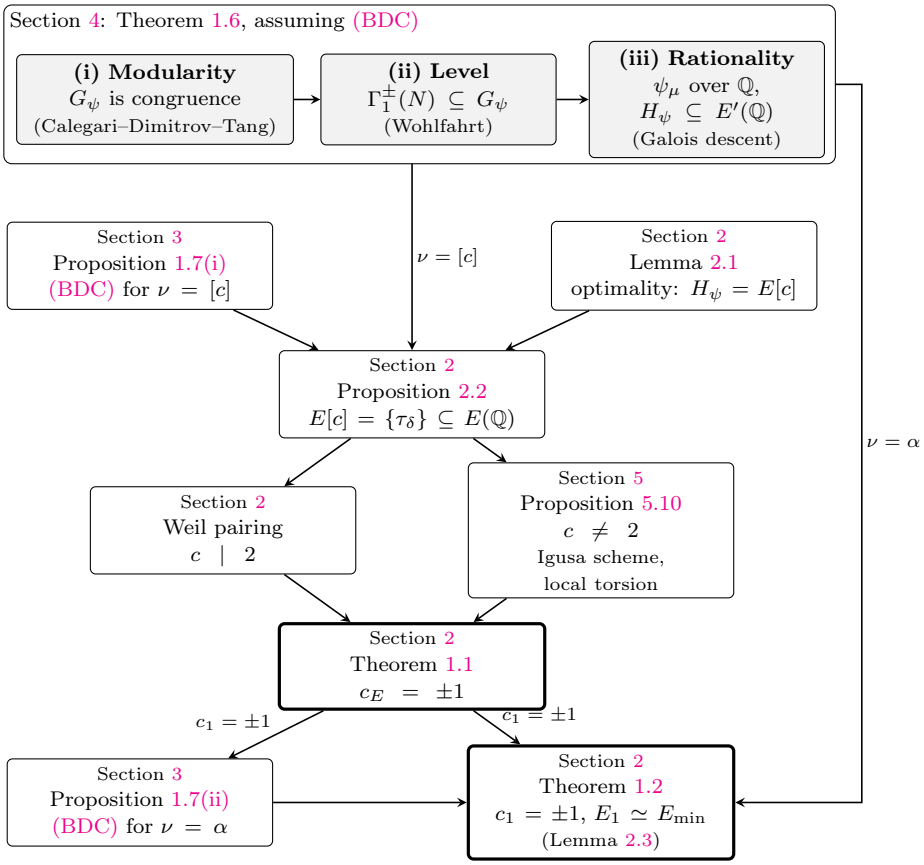

FIGURE 1. Logical structure of Sections 2–5. An arrow means that the target is deduced from the source.

Honda's theorem on formal groups [Hon70, Thm. 9]. Lifts through multiplication maps on a particular modular curve are also studied in [BFF23].

Our starting point is more global. As $\mathfrak{H}$ is simply connected, the parametrization φ_0 should have a "c-th root". So we take the normalized lift ψ of φ_0 through $[c]$. A priori ψ is only a holomorphic map on $\mathfrak{H}$, and there is no reason for it to be invariant under any congruence subgroup.

However, its q-expansion is easily seen to be integral and we may apply the unbounded denominators theorem of Calegari, Dimitrov and Tang [CDT25]. This congruence and argument from [Yin26] forces ψ to be modular, and we use Galois descent to show the induced algebraic map from modular curve to E comes from a morphism $X_\mu(N) \to E$ over $\mathbb{Q}$. Optimality now forces $E[c] \subseteq E(\mathbb{Q})$, and so $c \mid 2$. The case $c = 2$ needs a separate local argument, using the Igusa curve or Shimura subgroups. The same argument, applied to the étale isogeny $E_{\min} \to E_1$ instead of $[c]$, gives Stevens' Conjecture II.

The main innovation of this paper is therefore Theorem 1.6, which lets us treat the normalized lift ψ as an arithmetic object rather than just a holomorphic map. The idea comes from Yin's work on cubic roots of modular functions attached to

CM elliptic curves [Yin26, Prop. 8.1], where the unbounded denominators theorem is used to show that these cubic roots are invariant under a congruence subgroup. There the integral expansions required by [CDT25] are deduced from the fact that the relevant Manin–Stevens constants are units [Yin26, Thm. 6.1]. We go the other way: we prove integrality first, and then use it to show that the lift is modular and to bound c.

1.5. **Acknowledgements.** Z. Chi would like to thank Hongbo Yin for sharing the motivation behind the beautiful result in his paper and for his encouragement of this work. Z. Chi and S. Liu are deeply grateful to Richard Taylor and Brian Conrad for suggestions on improving the manuscript. Z. Chi, S. Liu and P. Nie thank Yiyang Wang for meaningful conversations. Z. Chi would like to thank his advisor Yifeng Liu, and S. Liu would like to thank his advisor Xinwen Zhu, for constant support.

2. Deduction of the main theorems

In this section we deduce Theorems 1.1 and 1.2 from Theorem 1.6 and Proposition 1.7, which are proved in Sections 4 and 3. Together with optimality, they give $E[c] \subseteq E(\mathbb{Q})$ (Proposition 2.2), and the Weil pairing then gives $c \mid 2$. The proof of Theorem 1.1 is completed in Section 5, where Proposition 5.10 uses Proposition 2.2 and the geometry of Igusa curves to show that $c = 1$. Stevens' conjectures are then deduced from Theorem 1.1 in Section 2.2.

2.1. **Proof of the Manin constant conjecture.** Let E, π_0 and φ_0 be as in Theorem 1.1. Replacing π_0 by $-\pi_0$, which changes the sign of c_E and preserves optimality, we may assume that $c = c_E$ is positive. By [Edi91, Prop. 2] c is an integer, and by [Čes18, Thm. 2.11] $\mathrm{ord}_p(c) = 0$ for every prime p with $p^2 \nmid N$. Thus

$$c \in \mathbb{Z}_{\geq 1}, \qquad p^2 \mid N \text{ for every prime } p \mid c. \tag{2.1}$$

We apply the constructions of Section 1.2 with $\Gamma = \Gamma_0(N)$ and $\varphi = \varphi_0$. The input from optimality is the following.

Lemma 2.1. *Let $m \geq 1$, and let ψ be the normalized lift of φ_0 through $[m] : E \to E$. Recall from Theorem 1.6(iii) its monodromy group*

$$H_\psi = \{\psi(\gamma z) - \psi(z) : \gamma \in \Gamma_0(N)\} = \rho(\Gamma_0(N)) \subseteq E[m].$$

Then $H_\psi = E[m]$.

Proof. Since $\ker \pi_0$ is connected, the homotopy sequence of $0 \to \ker \pi_0 \to J_0(N) \to E \to 0$ shows that $\pi_{0*} : H_1(J_0(N)(\mathbb{C}), \mathbb{Z}) \to H_1(E(\mathbb{C}), \mathbb{Z})$ is surjective. The Abel–Jacobi map $\mathrm{AJ} : X_0(N) \to J_0(N)$, $P \mapsto [P] - [\infty]$, induces an isomorphism

$$\mathrm{AJ}_* : H_1(X_0(N)(\mathbb{C}), \mathbb{Z}) \xrightarrow{\sim} H_1(J_0(N)(\mathbb{C}), \mathbb{Z}).$$

Since $\varphi_0 = \pi_0 \circ \mathrm{AJ}$, the map

$$\varphi_{0*} : H_1(X_0(N)(\mathbb{C}), \mathbb{Z}) \longrightarrow H_1(E(\mathbb{C}), \mathbb{Z})$$

is also surjective. Let $X^\circ \subseteq X_0(N)(\mathbb{C})$ be the complement of the cusps and of the images of the elliptic points, and $\mathfrak{H}^\circ \subseteq \mathfrak{H}$ its preimage, so that $\mathfrak{H}^\circ \to X^\circ$ is a covering with group $\Gamma_0(N)/\{\pm I\}$. Let ℓ be a loop in X° based at the image of $z_0 \in \mathfrak{H}^\circ$. It lifts to a path in $\mathfrak{H}^\circ$ from z_0 to γz_0 for some $\gamma \in \Gamma_0(N)$. Along this path, ψ is a continuous lift of $\varphi_0 \circ \ell$ through $[m]$, and its endpoints differ by $\rho(\gamma)$. On the other hand, under the identification $E[m] = \frac{1}{m}\Lambda/\Lambda \simeq \Lambda/m\Lambda$, where $\Lambda = H_1(E(\mathbb{C}), \mathbb{Z})$,

the endpoints of any lift of the loop $\varphi_0 \circ \ell$ through $[m]$ differ by the class of $\varphi_{0*}[\ell]$. Hence this class is $\rho(\gamma) \in H_\psi$. Since loops in X° generate $H_1(X_0(N)(\mathbb{C}), \mathbb{Z})$, and φ_{0*} is surjective, H_ψ contains, and therefore equals, $E[m]$. □

Proposition 2.2. *Let ψ be the normalized lift of φ_0 through $[c]$. There are a morphism $\psi_\mu : X_\mu(N) \to E$ over $\mathbb{Q}$ and points $\tau_\delta \in E(\mathbb{Q})$, $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$, with*

$$[c] \circ \psi_\mu = \varphi_0 \circ \varpi, \qquad \psi_\mu \circ \langle\delta\rangle = \psi_\mu + \tau_\delta, \qquad \tau_\delta = \psi_\mu(\langle\delta\rangle\infty), \tag{2.2}$$

and

$$\{\tau_\delta : \delta \in (\mathbb{Z}/N\mathbb{Z})^\times\} = E[c] \subseteq E(\mathbb{Q}). \tag{2.3}$$

Proof. By (2.1) and Proposition 1.7(i), applied with $V = X_0(N)$, ψ satisfies (BDC) with $k = 1$. Theorem 1.6(iii), with $\Gamma = \Gamma_0(N)$, $\nu = [c]$ and $\varphi = \varphi_0$, gives ψ_μ, and shows that the points $\tau_\delta = \psi_\mu(\langle\delta\rangle\infty)$, $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$, are rational, form H_ψ, and satisfy $\psi_\mu \circ \langle\delta\rangle = \psi_\mu + \tau_\delta$. Finally $H_\psi = E[c]$ by Lemma 2.1. □

Proof of Theorem 1.1. By Proposition 2.2, $E[c] \subseteq E(\mathbb{Q})$. The Weil pairing $E[c] \times E[c] \to \mu_c$ is surjective and Galois equivariant, so $\mu_c \subseteq \mathbb{Q}$, and hence $c \mid 2$. Finally $c \neq 2$ will be proved in Section 5 as Proposition 5.10. Hence $c = 1$, that is, $c_E = \pm 1$. □

Thus the arguments of Sections 3 and 4 prove Theorem 1.1 at every odd prime, and Section 5 is needed only to exclude an optimal curve with additive reduction at 2 whose full 2-torsion is rational.

2.2. **Proof of Stevens' conjectures.** Let $\mathcal{C}$ be an isogeny class of conductor N with newform f, and let π_1, φ_1, E_1, c_1 and $E_{\min}$ be as in Section 1.1. Let $\pi_0 : J_0(N) \twoheadrightarrow E$ be the optimal quotient with $E \in \mathcal{C}$.

The curve $X_\mu(N)$ is Shimura's canonical model of $X_1(N)$ used by Stevens: in the proof of [Ste89, Thm. 1.6], $X_1(N)_\mathbb{Q}$ is identified with the μ_N-moduli space, and his rational cusp 0 with our cusp ∞ (see also [CES03, proof of Lemma 6.1.6]). His variable τ_{St} and ours are related by $z = -1/(N\tau_{\mathrm{St}})$, so that $e^{-2\pi i/(N\tau_{\mathrm{St}})} = q$. His differential $\omega_f^{\mathrm{St}} = 2\pi i f(\tau_{\mathrm{St}})\,\mathrm{d}\tau_{\mathrm{St}}$ is $\varepsilon_N \cdot 2\pi i f(z)\,\mathrm{d}z$ in our coordinate, where $\varepsilon_N = \pm 1$ is the eigenvalue of the Fricke involution on f. Hence, regarding φ_1 as a morphism $X_\mu(N) \to E_1$ with $\varphi_1(\infty) = 0$,

$$\varphi_1^* \omega_{E_1} = \varepsilon_N c_1 f(q) \frac{\mathrm{d}q}{q}. \tag{2.4}$$

Lemma 2.3. *Let V be a smooth projective geometrically connected curve over a field of characteristic zero with a rational point o, let $\pi : J_V \twoheadrightarrow D_1$ be a quotient with connected kernel onto an elliptic curve, and let $g : V \to D_2$ be a morphism to an elliptic curve with $g(o) = 0$. If $g_*(\ker \pi)$ is finite, where $g_* : J_V \to D_2$ is the induced homomorphism, then $g_* = u \circ \pi$ for a unique homomorphism $u : D_1 \to D_2$. If moreover $\lambda \circ g_* = \pi$ for an isogeny $\lambda : D_2 \to D_1$, then $\lambda \circ u = \mathrm{id}_{D_1}$, and λ and u are isomorphisms.*

Proof. The image $g_*(\ker \pi)$ is connected and finite, hence zero, so g_* factors through $J_V / \ker \pi = D_1$. If $\lambda g_* = \pi$, then $\lambda u \pi = \pi$, and the surjectivity of π gives $\lambda u = \mathrm{id}$. Taking degrees yields $\deg \lambda = \deg u = 1$. □

Proof of Theorem 1.2. By [Čes18, Lemma 2.12], applied with $H = \Gamma_1(N)$ and $H' = \Gamma_0(N)$, c_1 divides c_E, so $c_1 = \pm 1$ by Theorem 1.1. Replacing φ_1 by $-\varphi_1$ if necessary, we may assume that

$$\varphi_1^* \omega_{E_1} = f(q)\frac{\mathrm{d}q}{q} = \omega_f. \tag{2.5}$$

It remains to prove that $E_1 \simeq E_{\min}$. By [Ste89, Thm. 2.3] there is an isogeny $\alpha : E_{\min} \to E_1$ which is étale on Néron models over $\mathbb{Z}_p$ for every p. By [Ste89, Lemma 2.2] it pulls back a Néron differential to a Néron differential at every p, so $\alpha^*\omega_{E_1} = \pm\omega_{E_{\min}}$, and replacing α by $-\alpha$ we may assume that $\alpha^*\omega_{E_1} = \omega_{E_{\min}}$. Let ψ' be the normalized lift of φ_1 through α. By (2.5) and Proposition 1.7(ii), applied with $V = X_\mu(N)$, ψ' satisfies (BDC) with $k = 1$.

Theorem 1.6(iii), with $\Gamma = \Gamma_1^{\pm}(N)$, $\varphi = \varphi_1$ and $\nu = \alpha$, now gives a morphism $h' : X_\mu(N) \to E_{\min}$ over $\mathbb{Q}$ with $h'(\infty) = 0$ and $\alpha \circ h' = \varphi_1$. On Jacobians $\alpha \circ h'_* = \pi_1$, so $h'_*(\ker \pi_1) \subseteq \ker \alpha$ is finite, and Lemma 2.3 with $\pi = \pi_1$, $g = h'$ and $\lambda = \alpha$ shows that α is an isomorphism. □

3. Integrality

In this section we prove Proposition 1.7: part (i) is Proposition 3.6 and part (ii) is Proposition 3.8. The desired (BDC) property follows from them.

For an elliptic curve E over $\mathbb{Q}_p$ we write $\mathscr{E}$ for its Néron model over $\mathbb{Z}_p$, $\mathscr{E}^0$ for its identity component, and

$$E(\mathbb{Q}_p) = \mathscr{E}(\mathbb{Z}_p), \qquad E^0(\mathbb{Q}_p) = \mathscr{E}^0(\mathbb{Z}_p).$$

For a minimal Weierstrass equation we use the parameter $t = -x/y$ at the origin, write $\widehat{E}$ for the formal group in this parameter, and

$$L_E(w) = w + \sum_{r\geq 2} b_r w^r \in \mathbb{Q}_p[[w]]$$

for its normalized logarithm. The smooth locus of the minimal Weierstrass model is $\mathscr{E}^0$, and $\widehat{E}$ is its completion along the zero section.

For an elliptic curve E over $\mathbb{Q}$ we always use a global minimal Weierstrass equation, and ω_E denotes its invariant differential which is a Néron differential, and its expansion in t is $\mathrm{d}L_E(t)$. For a morphism g to E with $g(\infty) = 0$ we write $t_g = t \circ g$.

3.1. Formal logarithms at primes of additive reduction.

Lemma 3.1. *Let A be a commutative ring. A power series $w + \sum_{r\geq 2} \beta_r w^r \in A[[w]]$ has a compositional inverse in $A[[w]]$.*

Proof. Write the inverse as $w + \sum_{r\geq 2} \gamma_r w^r$. The coefficient of w^r in the composite is γ_r plus a polynomial with integer coefficients in $\beta_2, \dots, \beta_r, \gamma_2, \dots, \gamma_{r-1}$, so the γ_r are determined recursively in A. □

Lemma 3.2. *Let F be a one-dimensional commutative formal group law over $\mathbb{Z}_p$ with $[p]_F(w) \in p\mathbb{Z}_p[[w]]$. Then the normalized logarithm L_F and its compositional inverse have coefficients in $\mathbb{Z}_p$.*

Proof. Write $[p]_F(w) = p\,g(w)$ with $g(w) = w + \sum_{r\geq 2} g_r w^r \in \mathbb{Z}_p[[w]]$, and $L_F(w) = \sum_{r\geq 1} b_r w^r$ with $b_1 = 1$. Comparing the coefficients of w^r, $r \geq 2$, in $L_F([p]_F(w)) = pL_F(w)$ gives

$$(1 - p^{r-1})\, b_r = g_r + \sum_{\ell=2}^{r-1} p^{\,\ell-1} b_\ell\, [w^r]\, g(w)^\ell,$$

where $[w^r]$ denotes the coefficient of w^r. Since $1 - p^{r-1}$ is a unit in $\mathbb{Z}_p$, induction on r gives $b_r \in \mathbb{Z}_p$. The assertion about L_F^{-1} follows from Lemma 3.1. □

Lemma 3.3. *Let E be an elliptic curve over $\mathbb{Q}_p$ with additive reduction. The formal group of a minimal Weierstrass equation satisfies $[p]_{\widehat{E}}(w) \in p\mathbb{Z}_p[[w]]$. Hence L_E and L_E^{-1} have coefficients in $\mathbb{Z}_p$.*

Proof. The formal group $\widehat{E}$ is the completion of $\mathscr{E}^0$ along the zero section. The special fibre $\mathscr{E}^0_{\mathbb{F}_p}$ is a form of $\mathbb{G}_{\mathrm{a}}$ over the perfect field $\mathbb{F}_p$, hence isomorphic to $\mathbb{G}_{\mathrm{a}}$, on which multiplication by p is zero. Therefore $[p]_{\widehat{E}}$ reduces to zero modulo p, and Lemma 3.2 applies. □

3.2. **Integrality of the normalized lift.** Let Γ, $\nu : E' \to E$ and $\varphi : X_\Gamma \to E$ be as in Section 1.2, and let ψ be the normalized lift of φ through ν. We write x, y for the coordinate functions of a global minimal Weierstrass equation of E', and t for the parameters of E' and of E. Let $\widehat{\nu}(w) \in \mathbb{Q}[[w]]$ be the expansion of ν in these parameters, so that $t \circ \nu = \widehat{\nu}(t)$ near the origin. Its linear coefficient is the constant $d \in \mathbb{Q}^\times$ with $\nu^*\omega_E = d\,\omega_{E'}$, which is nonzero because ν is étale.

Lemma 3.4. *We have $t_\psi = \widehat{\nu}^{-1}(t_\varphi)$, and this series is a nonzero element of $q\,\mathbb{Q}[[q]]$. Consequently $x \circ \psi$ and $y \circ \psi$ are Laurent series in q with rational coefficients.*

Proof. By Lemma 1.4, ψ is a holomorphic function of q near $q = 0$ with value 0 at $q = 0$, so $\widehat{\nu}(t_\psi) = t_\varphi$ near $q = 0$. Since φ, the cusp ∞ and the parameter q are defined over $\mathbb{Q}$, we have $t_\varphi \in q\,\mathbb{Q}[[q]]$, and $t_\varphi \neq 0$ because φ is not constant. As $\widehat{\nu}$ has nonzero linear coefficient, it has a compositional inverse over $\mathbb{Q}$, and $t_\psi = \widehat{\nu}^{-1}(t_\varphi)$. Substituting into $x(t) \in t^{-2}\mathbb{Z}[[t]]$ and $y(t) \in t^{-3}\mathbb{Z}[[t]]$ gives the last assertion. □

The following argument is from [Edi91, proof of Prop. 2] and [Ste89, proof of Thm. 1.6]; see also [Yin26, Thm. 7.2].

Lemma 3.5. *Let V be $X_0(N)$ or $X_\mu(N)$, let E be an elliptic curve over $\mathbb{Q}$, and let $\varphi : V \to E$ be a morphism over $\mathbb{Q}$ with $\varphi(\infty) = 0$. Then $t_\varphi \in q\,\mathbb{Z}[[q]]$.*

Proof. We may assume that φ is not constant. Fix a prime p. If $V = X_0(N)$, let U be the smooth locus of $X_0(N)_{\mathbb{Z}_p}$, where $X_0(N)_{\mathbb{Z}}$ is the modular curve over $\mathbb{Z}$ of [Čes18, Section 1.5]. The cusp ∞ extends to a section of U [Čes18, Rem. 5.3], and the completion of U along it is $\operatorname{Spf}\mathbb{Z}_p[[q]]$, where q is the analytic parameter at ∞ [Edi91, proof of Prop. 2]. If $V = X_\mu(N)$, let $U = \mathcal{X}_\mu(N)_{\mathbb{Z}_p}$, where $\mathcal{X}_\mu(N)$ is the coarse moduli scheme over $\mathbb{Z}$ of generalized elliptic curves with irreducible geometric fibres equipped with a closed immersion of μ_N into the smooth locus. By [CES03, proof of Lemma 6.1.6], $\mathcal{X}_\mu(N)$ is smooth over $\mathbb{Z}$, the cusp ∞ extends to a $\mathbb{Z}$-point of it, and the completion along this point is $\operatorname{Spf}\mathbb{Z}[[q]]$, where q is the analytic parameter at ∞. Its generic fibre is the open subscheme of $X_\mu(N)$ obtained by removing the cusps other than the $\langle\delta\rangle\infty$.

In both cases the Néron mapping property [BLR90, Section 1.2, Def. 1] extends φ to a morphism $U \to \mathscr{E}$. The section ∞ of U maps to a section of $\mathscr{E}$ which is zero on the generic fibre, hence is the zero section, as $\mathscr{E}$ is separated. Therefore the composite $\operatorname{Spf} \mathbb{Z}_p[[q]] \to U \to \mathscr{E}$ factors through the completion $\operatorname{Spf} \mathbb{Z}_p[[t]]$ of $\mathscr{E}$ along its zero section, and $t_\varphi \in q\,\mathbb{Z}_p[[q]]$. The coefficients of t_φ are rational because φ, the cusp and the parameter q are defined over $\mathbb{Q}$. As p was arbitrary, $t_\varphi \in q\,\mathbb{Z}[[q]]$. □

If $t_\psi \in q + q^2\mathbb{Z}[[q]]$ for a morphism ψ to an elliptic curve with global minimal coordinates x, y, then $x \circ \psi$ and $y \circ \psi$ lie in $\mathbb{Z}((q))$, because $x(t) \in t^{-2} + t^{-1}\mathbb{Z}[[t]]$ and $y(t) \in -t^{-3} + t^{-2}\mathbb{Z}[[t]]$. We write $\ell_f(q) = \sum_{n\geq 1}(a_n/n)q^n$, so that $\omega_f = \mathrm{d}\ell_f$.

Proposition 3.6. *Let V be $X_0(N)$ or $X_\mu(N)$, and let $E/\mathbb{Q}$ be an elliptic curve of conductor N with newform f. Let $\varphi : V \to E$ be a morphism over $\mathbb{Q}$ with $\varphi(\infty) = 0$ and*

$$\varphi^*\omega_E = c\,\omega_f$$

for an integer $c \geq 1$ such that $p^2 \mid N$ for every prime $p \mid c$, and let ψ be the normalized lift of φ through $[c]$. Then

$$t_\psi = L_E^{-1}(\ell_f) \in q + q^2\mathbb{Z}[[q]],$$

and $x \circ \psi$, $y \circ \psi$ lie in $\mathbb{Z}((q))$.

Proof. Integrating $\varphi^*\omega_E = c\,\omega_f$ gives $L_E(t_\varphi) = c\,\ell_f$. Since $L_E \circ [c]_{\widehat{E}} = c\,L_E$ and $[c]_{\widehat{E}}(t_\psi) = t_\varphi$ (Lemma 3.4), we get $L_E(t_\psi) = \ell_f$, that is, $t_\psi = L_E^{-1}(\ell_f)$. Its linear coefficient is $a_1 = 1$, and its coefficients are rational. It remains to show that they lie in $\mathbb{Z}_p$ for every prime p.

If $p \nmid c$, then $g(w) = c^{-1}[c]_{\widehat{E}}(w)$ lies in $w + w^2\mathbb{Z}_p[[w]]$, so g^{-1} has coefficients in $\mathbb{Z}_p$ by Lemma 3.1. Since $g(t_\psi) = c^{-1}t_\varphi$, and $t_\varphi \in q\,\mathbb{Z}[[q]]$ by Lemma 3.5, we get $t_\psi = g^{-1}(c^{-1}t_\varphi) \in q\,\mathbb{Z}_p[[q]]$.

If $p \mid c$, then $p^2 \mid N$, so E has additive reduction at p and $a_p = 0$. Hence $a_n = 0$ whenever $p \mid n$, and every coefficient of ℓ_f lies in $\mathbb{Z}_p$. By Lemma 3.3, $t_\psi = L_E^{-1}(\ell_f)$ lies in $q\,\mathbb{Z}_p[[q]]$. □

Remark 3.7. The parameter of φ itself is $t_\varphi = c\,q + O(q^2)$, so $x \circ \varphi$ and $y \circ \varphi$ have denominators at the primes dividing c, while $x \circ \psi$ and $y \circ \psi$ do not. The integrality of $L_E^{-1}(\ell_f)$ also follows from Honda's comparison of formal groups [Hon70, Thm. 9]; see also [Hon73, Section 3].

Proposition 3.8. *Let V be $X_0(N)$ or $X_\mu(N)$, and let $E/\mathbb{Q}$ be an elliptic curve of conductor N with newform f. Let $\varphi : V \to E$ be a morphism over $\mathbb{Q}$ with $\varphi(\infty) = 0$ and $\varphi^*\omega_E = \omega_f$, let $\nu : E' \to E$ be an isogeny over $\mathbb{Q}$ with $\nu^*\omega_E = \omega_{E'}$, and let ψ be the normalized lift of φ through ν.*

Then $t_\psi \in q + q^2\mathbb{Z}[[q]]$, and $x \circ \psi$, $y \circ \psi$ lie in $\mathbb{Z}((q))$, where x, y are the coordinates of a global minimal Weierstrass equation of E'.

Proof. For every prime p, ν extends to a morphism of Néron models over $\mathbb{Z}_p$ preserving the zero sections, hence to a homomorphism of their formal groups. Thus $\widehat{\nu} \in w\,\mathbb{Z}_p[[w]]$ for all p, and its linear coefficient is 1 because $\nu^*\omega_E = \omega_{E'}$. Hence $\widehat{\nu} \in w + w^2\mathbb{Z}[[w]]$, and $\widehat{\nu}^{-1}$ has integral coefficients by Lemma 3.1. By Lemma 3.5, $t_\varphi \in q\,\mathbb{Z}[[q]]$, and $L_E(t_\varphi) = \ell_f$ shows that its linear coefficient is 1. By Lemma 3.4, $t_\psi = \widehat{\nu}^{-1}(t_\varphi) \in q + q^2\mathbb{Z}[[q]]$. □

4. Modularity and rationality of normalized lifts

In this section we prove Theorem 1.6: part (i) (Modularity) is Proposition 4.3 together with Lemma 4.1 (Section 4.1), part (ii) (Level) is Proposition 4.5 (Section 4.2), and part (iii) (Rationality) is Propositions 4.6 and 4.7 (Section 4.3).

We keep the notation of Section 1.2: ψ is the normalized lift of $\varphi : X_\Gamma \to E$ through $\nu : E' \to E$, $\rho : \Gamma \to \ker \nu$ is the homomorphism of Lemma 1.5, and $G_\psi = \ker \rho$. The argument follows Yin's congruence argument for cubic roots of modular functions [Yin26, Prop. 8.1] in an opposite direction.

For a positive integer m we write

$$\Gamma(m) = \ker\big(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})\big),$$

and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

4.1. Modularity.

Let $X = X_\Gamma(\mathbb{C})$, a compact Riemann surface, and let

$$Y = X \times_{\varphi, E(\mathbb{C}), \nu} E'(\mathbb{C}).$$

Since ν is a finite covering, so is $Y \to X$. Thus Y is a compact, possibly disconnected, Riemann surface, unramified over X at every point, including the cusps and the images of the elliptic points. Let Y_ψ be the connected component of Y containing $(\infty, 0)$.

Lemma 4.1. *The homomorphism ρ vanishes on $-I$ and on every parabolic and elliptic element of Γ. The map $z \mapsto (z, \psi(z))$ induces an isomorphism of compact Riemann surfaces $X_{G_\psi}(\mathbb{C}) = G_\psi \backslash \mathfrak{H}^* \simeq Y_\psi$.*

Proof. The element $-I$ acts trivially on $\mathfrak{H}$, so $\rho(-I) = 0$. If γ is elliptic with fixed point $z_0 \in \mathfrak{H}$, then $\rho(\gamma) = \psi(z_0) - \psi(z_0) = 0$. If γ is parabolic, it fixes a cusp $\kappa = \sigma\infty$ with $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, and $\gamma = \pm\sigma T^r \sigma^{-1}$ for some $r \neq 0$. For $\operatorname{Im} z'$ large, the image in X of the path from $\sigma z'$ to $\sigma(z' + r) = \gamma\sigma z'$ is a loop in a small disc around the image of κ, hence null-homotopic in X. Since $Y \to X$ is a covering, its lift $z \mapsto (z, \psi(z))$ is a closed loop, so $\rho(\gamma) = 0$.

If $(z, \psi(z))$ and $(z', \psi(z'))$ have the same image in Y, then $z' = \gamma z$ with $\gamma \in \Gamma$ and $\rho(\gamma) = 0$, so $\gamma \in G_\psi$. Let $Y^\circ \subseteq Y$ be the preimage of $\Gamma\backslash\mathfrak{H}$. Since every elliptic element of Γ lies in G_ψ, the finite map $G_\psi\backslash\mathfrak{H} \to \Gamma\backslash\mathfrak{H}$ is unramified, so $G_\psi\backslash\mathfrak{H} \to Y^\circ$ is an injective local isomorphism which is proper, that is, an isomorphism onto a union of connected components of Y°. Its image is connected and contains the points $(z, \psi(z))$ with $\operatorname{Im} z$ large, which are close to $(\infty, 0)$. Hence it is $Y_\psi \cap Y^\circ$, the complement in Y_ψ of finitely many points over the cusps. Thus $X_{G_\psi}(\mathbb{C})$ and Y_ψ are compact Riemann surfaces, finite over X, containing isomorphic complements of finite sets compatibly with the maps to X, and the isomorphism extends to them. □

From now on we assume (BDC). We use the unbounded denominators theorem in the following form [CDT25, Thm. 1.0.1].

Theorem 4.2 (Calegari–Dimitrov–Tang)**.** *Let $F : \mathfrak{H} \to \mathbb{C}$ be a modular form of some integral weight for a subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$, holomorphic on $\mathfrak{H}$ and at the cusps, whose Fourier expansion at ∞ lies in $\mathbb{Z}[[q]]$. Then F is a modular form for a congruence subgroup.*

The theorem allows expansions in fractional powers of $e^{\pi i z}$ but we only need $\mathbb{Z}[[q]]$.

Let j be the modular invariant and $\Delta = q\prod_{n\geq 1}(1-q^n)^{24}$ the cusp form of weight 12 for $\mathrm{SL}_2(\mathbb{Z})$, which has no zeros on $\mathfrak{H}$.

Proposition 4.3. *G_ψ is a congruence subgroup.*

Proof. By Lemma 1.5, G_ψ has finite index in $\mathrm{SL}_2(\mathbb{Z})$. Put $u_x = x\circ\psi$ and $u_y = y\circ\psi$. By Lemma 4.1 they are meromorphic functions on $X_{G_\psi}(\mathbb{C})$, and in particular meromorphic at the cusps. A pole of u_x or u_y in $\mathfrak{H}$ is a point z with $\psi(z)=0$, hence with $\varphi(z)=0$, so its image in X lies in the finite set $\varphi^{-1}(0)$. These points are algebraic, because φ is defined over $\mathbb{Q}$, and so are their j-invariants. The orders of the poles are bounded, because there are finitely many poles modulo G_ψ. Choose a nonzero polynomial P with integer coefficients vanishing to sufficiently high order at all these j-invariants. Then $P(j)u_x$ and $P(j)u_y$ are holomorphic on $\mathfrak{H}$, and for s sufficiently large the functions

$$F_x = k\,\Delta^s P(j)\,u_x, \qquad F_y = k\,\Delta^s P(j)\,u_y$$

are also holomorphic at every cusp, because Δ vanishes at every cusp. They are modular forms of weight $12s$ for G_ψ, and since $\Delta \in q\,\mathbb{Z}[[q]]$ and $j \in q^{-1}\mathbb{Z}[[q]]$, (BDC) shows that their expansions at ∞ lie in $\mathbb{Z}[[q]]$ once s is large.

By Theorem 4.2, F_x and F_y are modular for congruence subgroups C_x and C_y. The factor $k\Delta^s P(j)$ is modular of weight $12s$ for $\mathrm{SL}_2(\mathbb{Z})$, so u_x and u_y are invariant under $C_x\cap C_y$. The coordinates x, y separate the points of $E'(\mathbb{C})\smallsetminus\{0\}$, so for $\gamma\in C_x\cap C_y$ we have $\psi\circ\gamma=\psi$ outside a discrete set, hence everywhere. Choose $M_1\geq 1$ with $\Gamma(M_1)\subseteq C_x\cap C_y$. Since $\Gamma(N)\subseteq\Gamma$,

$$\Gamma(\mathrm{lcm}(M_1,N)) \subseteq C_x\cap C_y\cap\Gamma \subseteq G_\psi. \qquad \square$$

Proof of Theorem 1.6(i). By Lemma 1.5, G_ψ is normal in Γ. It is a congruence subgroup by Proposition 4.3, and $X_{G_\psi}(\mathbb{C})\simeq Y_\psi$ by Lemma 4.1. $\square$

4.2. **Level.** We first compare cusp widths, using Lemma 4.1. Let $G\subseteq\mathrm{SL}_2(\mathbb{Z})$ be a subgroup of finite index containing $-I$. If $\sigma\in\mathrm{SL}_2(\mathbb{Z})$ maps ∞ to a cusp κ, the *width* of κ for G is

$$w_G(\kappa) = \min\{w\in\mathbb{Z}_{\geq 1} : \sigma T^w\sigma^{-1}\in G\},$$

and the *level* $L(G)$ of G is the least common multiple of its cusp widths [CDT25, Def. 4.1.2].

Corollary 4.4. *Every cusp has the same width for G_ψ as for Γ. In particular $L(G_\psi)=L(\Gamma)$.*

Proof. Let $\kappa=\sigma\infty$ be a cusp, with $\sigma\in\mathrm{SL}_2(\mathbb{Z})$, and let w be the width of κ for Γ, so that $\gamma=\sigma T^w\sigma^{-1}\in\Gamma$. Since $G_\psi\subseteq\Gamma$, the width for Γ divides the width for G_ψ. Conversely, γ is a parabolic element of Γ, so $\rho(\gamma)=0$ by Lemma 4.1, that is, $\gamma\in G_\psi$. Hence the width for G_ψ divides w. $\square$

To determine the level we use Wohlfahrt's theorem [Woh64, Thm. 2], in the form given at the end of the proof of [CDT25, Lemma 4.4.1]: a congruence subgroup G containing $-I$ satisfies

$$\pm\Gamma(L(G))\subseteq G.$$

Proposition 4.5. $\Gamma_1^{\pm}(N)\subseteq G_\psi\subseteq\Gamma$.

Proof. Every group between $\Gamma_1^{\pm}(N)$ and $\Gamma_0(N)$ contains $\Gamma(N)$, so its cusp widths divide N. The cusp 0 has width exactly N for such a group, since $\left(\begin{smallmatrix}1 & 0\\ -w & 1\end{smallmatrix}\right) \in \Gamma_0(N)$ if and only if $N \mid w$. Thus $L(\Gamma) = N$, and $L(G_\psi) = N$ by Corollary 4.4. Since G_ψ is a congruence subgroup containing $-I$ (Lemma 4.1 and Proposition 4.3), Wohlfahrt's theorem gives $\pm\Gamma(N) \subseteq G_\psi$. The parabolic element T lies in Γ, hence in G_ψ. Reduction modulo N identifies $\Gamma_1(N)/\Gamma(N)$ with $\{\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right) : b \in \mathbb{Z}/N\mathbb{Z}\}$, which is generated by the image of T. Hence $\Gamma_1^{\pm}(N) = \langle \pm\Gamma(N), T\rangle \subseteq G_\psi$. □

Proof of Theorem 1.6(ii). This is Proposition 4.5 together with Lemma 4.1. □

4.3. **Rationality.** We will first show that the induced map from ψ is algebraic by GAGA. Because it is normalized at the rational cusp ∞, its graph is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and it descends to $\mathbb{Q}$. Its translations under the diamond operators are then values at rational cusps.

Proposition 4.6. *There is a unique morphism $\psi_\mu : X_\mu(N) \to E'$ over $\mathbb{Q}$ with $\psi_\mu(\infty) = 0$ and $\nu \circ \psi_\mu = \varphi \circ \varpi_\Gamma$. Its analytification is induced by ψ.*

Proof. By Proposition 4.5, ψ is invariant under $\Gamma_1^{\pm}(N)$, and by Lemma 4.1 it defines a holomorphic map $X_\mu(N)(\mathbb{C}) \to X_{G_\psi}(\mathbb{C}) \simeq Y_\psi \to E'(\mathbb{C})$, still denoted by ψ. By GAGA this map is algebraic. It satisfies $\nu \circ \psi = \varphi \circ \varpi_\Gamma$ and $\psi(\infty) = 0$.

The scheme

$$\mathcal{Z} = X_\mu(N) \times_{\varphi\varpi_\Gamma, E, \nu} E'$$

is finite étale over $X_\mu(N)$ and defined over $\mathbb{Q}$, and $(\infty, 0) \in \mathcal{Z}(\mathbb{Q})$. As $\mathcal{Z}_{\overline{\mathbb{Q}}}$ is a smooth curve over an algebraically closed field, its connected components are geometrically connected, so the connected components of $\mathcal{Z}_{\mathbb{C}}$ are the base changes of those of $\mathcal{Z}_{\overline{\mathbb{Q}}}$. The graph of ψ is closed, and open because $\mathcal{Z} \to X_\mu(N)$ is étale and the graph maps isomorphically to $X_\mu(N)$. Thus the graph is a connected component of $\mathcal{Z}_{\mathbb{C}}$, and therefore comes from a connected component of $\mathcal{Z}_{\overline{\mathbb{Q}}}$ containing $(\infty, 0)$. Distinct connected components are disjoint and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ fixes $(\infty, 0)$, so this component is Galois stable. It descends to a closed subscheme of $\mathcal{Z}$ mapping isomorphically to $X_\mu(N)$, and hence ψ descends to a morphism ψ_μ over $\mathbb{Q}$.

Two morphisms with these properties differ by a morphism $X_\mu(N) \to \ker \nu$ which vanishes at ∞. Since $X_\mu(N)$ is geometrically connected and $\ker \nu$ is finite, this morphism is zero. □

Proposition 4.7. *Let $\gamma = \left(\begin{smallmatrix}a & b\\ Nr & d\end{smallmatrix}\right) \in \Gamma$. Then*

$$\psi_\mu \circ \langle d\rangle = \psi_\mu + \rho(\gamma), \qquad \rho(\gamma) = \psi_\mu(\langle d\rangle\infty) \in E'(\mathbb{Q}).$$

Proof. The class of d lies in Δ_Γ, so $\varpi_\Gamma \circ \langle d\rangle = \varpi_\Gamma$, and $\psi_\mu \circ \langle d\rangle - \psi_\mu$ is a morphism from $X_\mu(N)$ to $\ker \nu$. As $X_\mu(N)$ is geometrically connected, it is constant, equal to its value $\psi_\mu(\langle d\rangle\infty)$ at ∞. This value is a rational point because ψ_μ, $\langle d\rangle$ and ∞ are defined over $\mathbb{Q}$. Since γ acts on $X_\mu(N)(\mathbb{C})$ as $\langle d\rangle$ (Section 1.2), this constant is $\psi(\gamma z) - \psi(z) = \rho(\gamma)$. □

Proof of Theorem 1.6(iii). The first assertions are Propositions 4.6 and 4.7. Since $\langle -1\rangle$ is the identity, $\tau_{-d} = \tau_d$, so $H_\psi = \rho(\Gamma) = \{\tau_\delta : \delta \in \Delta_\Gamma\}$. The component Y_ψ is the image of $X_\mu(N)(\mathbb{C})$ under $(\varpi_\Gamma, \psi_\mu)$, a morphism over $\mathbb{Q}$, so it descends to a connected component $Y_\psi^{\mathbb{Q}}$ of the finite étale X_Γ-scheme $X_\Gamma \times_{\varphi, E, \nu} E'$. Over $\mathbb{C}$, the subgroup of $\ker \nu$ preserving Y_ψ is H_ψ, which acts simply transitively on the fibres of $Y_\psi \to X$. Therefore $Y_\psi^{\mathbb{Q}} \to X_\Gamma$ is Galois, and its automorphisms over

X_Γ are the translations by H_ψ. These points are rational, so the automorphism group scheme is the constant group H_ψ. Finally ρ kills $\Gamma_1^{\pm}(N)$ and the parabolic and elliptic elements of Γ by Lemma 4.1 and Proposition 4.5, so $H_\psi = \rho(\Gamma)$ is a quotient of Γ/Γ'. □

Remark 4.8. The assumption that E and E' are elliptic curves is used in Proposition 4.3, where x, y separate the points of $E'(\mathbb{C}) \smallsetminus \{0\}$, and in the local arguments of Lemmas 3.3 and 5.9. For an abelian variety one could instead impose bounded denominators on the compositions of the lift with finitely many rational functions separating the points of an open subset met by the lift. The natural analogues of the Manin constant conjecture for optimal quotients of higher dimension fail in general [Čes18, Thm. 5.10].

5. Igusa curves and the local torsion

Let $E/\mathbb{Q}$, N, and c be as in Section 2. By Proposition 2.2, there are a morphism $\psi_\mu : X_\mu(N) \to E$ over $\mathbb{Q}$ and rational points $\tau_\delta \in E(\mathbb{Q})$ such that

$$\psi_\mu \circ \langle\delta\rangle = \psi_\mu + \tau_\delta, \qquad \{\tau_\delta : \delta \in (\mathbb{Z}/N\mathbb{Z})^\times\} = E[c]. \tag{5.1}$$

Moreover $c \in \mathbb{Z}_{\geq 1}$ and $p^2 \mid N$ for every prime $p \mid c$ by (2.1). In this section we prove Proposition 5.10, which says that no prime divides c. This is stronger than the remaining $c \neq 2$.

Fix a prime $p \mid c$. The main point is that every τ_δ lies in $E^0(\mathbb{Q}_p)$, the group of points reducing into the identity component of the Néron model (Proposition 5.8). Since E has additive reduction at p, the group $E^0(\mathbb{Q}_p)[p]$ has order at most p (Lemma 5.9). On the other hand $E[p] \subseteq E[c]$ consists of p^2 points of $E^0(\mathbb{Q}_p)$, which is a contradiction.

To prove Proposition 5.8, we construct a smooth scheme S over the ring of integers $\mathcal{O}_K$ of an unramified extension $K/\mathbb{Q}_p$ for every prime $p \mid N$, together with a morphism $\jmath : S_K \to Y_\mu(N)_K$ and lifts of the diamond operators to S (Section 5.1). Here $Y_\mu(N) \subset X_\mu(N)$ is the complement of the cusps. The geometric special fibre of S is an open subscheme of an Igusa curve, and it is therefore connected (Theorem 5.7). We extend $\psi_\mu \circ \jmath$ to the Néron model of E over $\mathcal{O}_K$. A point of the special fibre of S and its diamond translate then map to the same component of the special fibre of the Néron model, so τ_δ reduces into the identity component.

The proof in Section 2 that $c \mid 2$ uses only the rationality of the points τ_δ. The argument of this section also uses the geometry of the special fibre of S. We expect this to matter when the method is extended to general number fields, where analogues of the case $c = 2$ occur more often, and when it is applied to other problems related to Theorem 1.6.

5.1. **The moduli problems.** Fix $p \mid N$ and write $N = p^a M$, where $a \geq 1$ and $p \nmid M$. Choose an integer $n \geq 3$, prime to p and divisible by M. Choose a primitive n-th root of unity $\zeta \in \overline{\mathbb{Q}}_p$, and put

$$K = \mathbb{Q}_p(\zeta), \qquad \mathcal{O}_K = \mathbb{Z}_p[\zeta].$$

Write k_0 for the residue field of $\mathcal{O}_K$, and put $k = \bar{k}_0$.

We use the conventions of [KM85, Sections 4.1–4.3 and 4.13]. The objects of $(\mathrm{Ell}/\mathcal{O}_K)$ are elliptic curves A/W over variable $\mathcal{O}_K$-schemes, and its morphisms are cartesian squares over $\mathcal{O}_K$. A moduli problem $\mathcal{F}$ is a contravariant set-valued functor on this category. Thus $\mathcal{F}(A/W)$ is a set of additional structures on the

fixed elliptic curve A/W. When $\mathcal{F}$ is representable, we write $\mathfrak{M}(\mathcal{F})$ for its moduli scheme, following [KM85, (4.3.1)]: its W-points are isomorphism classes of elliptic curves over W equipped with the specified structure. The notation $\mathcal{A}$ will denote a universal elliptic curve, while $E/\mathbb{Q}$ remains the fixed target elliptic curve.

We first recall the inclusion moduli problem of [KM85, Section 4.9], restricted to $\mathbb{Q}$-schemes.

Definition 5.1. Let W be a $\mathbb{Q}$-scheme. A μ_N-level object over W is a pair

$$(A/W,\ \iota),$$

where

- A/W is an elliptic curve;
- $\iota : \mu_{N,W} \hookrightarrow A[N]$ is a closed immersion of W-group schemes.

An isomorphism from $(A/W, \iota)$ to $(A'/W, \iota')$ is an isomorphism $g : A \to A'$ over W such that $g \circ \iota = \iota'$. On $(\mathrm{Ell}/\mathbb{Q})$, the corresponding moduli problem assigns to a fixed A/W the set $\mathrm{Incl}_{W\text{-gp}}(\mu_{N,W}, A[N])$.

As defined in Section 1.2, $X_\mu(N)$ is the compactified moduli space of these pairs. Their coarse moduli scheme is therefore $Y_\mu(N)$, since the cusps are precisely the reduced boundary of the compactification [KM85, (8.6.3.2)]. The diamond operator acts by

$$\langle\delta\rangle(A, \iota) = (A, \iota \circ [\delta]).$$

To obtain a universal elliptic curve, we introduce an auxiliary full level with fixed Weil pairing.

Definition 5.2. Let W be an $\mathcal{O}_K$-scheme. A $\mathcal{P}$-object over W is a triple

$$(A/W,\ P,\ Q),$$

where

- A/W is an elliptic curve;
- $P, Q \in A[n](W)$, and the homomorphism
$$\alpha_{P,Q} : (\mathbb{Z}/n\mathbb{Z})^2_W \longrightarrow A[n], \qquad (r, s) \longmapsto [r]P + [s]Q$$
is an isomorphism;
- $e_n(P, Q) = \zeta$.

An isomorphism of such triples is an isomorphism of elliptic curves over W carrying each basis point to its counterpart. The corresponding moduli problem $\mathcal{P}$ on $(\mathrm{Ell}/\mathcal{O}_K)$ assigns to a fixed A/W the set of pairs (P, Q) with these properties.

Katz–Mazur write $[\Gamma(n)]$ for the moduli problem of Drinfeld n-bases [KM85, Section 3.1]. When n is invertible, these are the ordered bases above without the pairing condition [KM85, Section 4.6]. Their superscript can requires the Weil pairing to equal the primitive root supplied by the $\mathbb{Z}[\zeta_n]$-base structure [KM85, 9.1.5, 9.1.6 and 9.4.3.1]. Thus $\mathcal{P}$ is obtained from $[\Gamma(n)]^{\mathrm{can}}$ by inverting n and making the base change

$$\mathbb{Z}[\zeta_n, 1/n] \longrightarrow \mathcal{O}_K, \qquad \zeta_n \longmapsto \zeta.$$

Put $B = \mathfrak{M}(\mathcal{P})$. Since $n \geq 3$, the moduli problem $[\Gamma(n)]$ over $\mathbb{Z}[1/n]$ is represented by a smooth affine curve $Y(n)$ [KM85, Cor. 4.7.2]. Fixing the pairing selects an

open and closed subscheme of $Y(n)_{\mathcal{O}_K}$, so $B/\mathcal{O}_K$ is a smooth fine moduli scheme. Write $\mathcal{A}/B$ for its universal elliptic curve.

Let $U \subset B$ be the open subscheme obtained by removing the supersingular points of the special fibre [KM85, Lemmas 12.5.2 and 12.5.4]. In particular,

$$U_K = B_K, \qquad U_k = (B_k)^{\mathrm{ord}}.$$

Definition 5.3. Let W be an $\mathcal{O}_K$-scheme. An $\mathcal{S}$-object over W is a quadruple

$$(A/W,\ P,\ Q,\ \iota),$$

where

- $(A/W, P, Q)$ is a $\mathcal{P}$-object whose classifying map $W \to B$ factors through U;
- $\iota : \mu_{p^a,W} \hookrightarrow A[p^a]$ is a closed immersion of W-group schemes.

An isomorphism of $\mathcal{S}$-objects is an isomorphism g of the underlying $\mathcal{P}$-objects satisfying $g \circ \iota = \iota'$. We write $\mathcal{S}$ for the corresponding moduli problem on $(\mathrm{Ell}/\mathcal{O}_K)$, and put $S = \mathfrak{M}(\mathcal{S})$.

Since B represents $\mathcal{P}$, an $\mathcal{S}$-object over W amounts to a morphism $W \to U$ together with a closed immersion $\iota : \mu_{p^a,W} \hookrightarrow \mathcal{A}_W[p^a]$, where $\mathcal{A}_W$ is the pullback of the universal curve. By [KM85, Section 4.9], the functor

$$W \longmapsto \mathrm{Incl}_{W\text{-gp}}(\mu_{p^a,W}, \mathcal{A}_W[p^a])$$

on U-schemes is represented by an affine étale U-scheme. This is S, and the projection $S \to U$ forgets ι. Here fppf injectivity is equivalent to a closed immersion, since the group schemes are finite. As U is noetherian, $S \to U$ is of finite presentation, so $S/\mathcal{O}_K$ is smooth of finite type and relative dimension one.

Construction 5.4. We now explain how the structures defining S determine a point of the given modular curve. Let W be a K-scheme, and let $(A/W, P, Q, \iota_p)$ be an $\mathcal{S}$-object over W. The first basis point defines an inclusion

$$\iota_M : \mu_{M,W} \hookrightarrow A[M], \qquad \iota_M(\zeta^{n/M}) = [n/M]P,$$

with the trivial interpretation when $M = 1$. Since M and p^a are coprime, multiplication gives an isomorphism

$$\mu_{M,W} \times \mu_{p^a,W} \xrightarrow{\sim} \mu_{N,W}, \qquad (x, y) \longmapsto xy.$$

Under this isomorphism, the homomorphism $(x, y) \mapsto \iota_M(x) + \iota_p(y)$ defines $\iota_N : \mu_{N,W} \hookrightarrow A[N]$. It is a closed immersion because the two image subgroups have coprime orders. We define

$$\begin{aligned} \jmath : S_K &\longrightarrow Y_\mu(N)_K \subset X_\mu(N)_K, \\ (A/W, P, Q, \iota_p) &\longmapsto (A/W, \iota_N). \end{aligned} \tag{5.2}$$

The pair on the right denotes its coarse moduli class. The construction commutes with base change and respects isomorphisms, so it gives a morphism of K-schemes. Thus $\jmath$ forgets the auxiliary basis after retaining the μ_M-structure determined by P.

The same data also allow us to lift the diamond operators to S over $\mathcal{O}_K$. For $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$, choose $v \in (\mathbb{Z}/n\mathbb{Z})^\times$ with $v \equiv \delta \pmod{M}$. Such a lift exists because the reduction map $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/M\mathbb{Z})^\times$ is surjective. The formula

$$\begin{aligned} \widetilde{\delta} :\ S &\longrightarrow S, \\ (A, P, Q, \iota_p) &\longmapsto \big(A, [v]P, [v^{-1}]Q, \iota_p \circ [\delta]\big) \end{aligned} \tag{5.3}$$

defines an $\mathcal{O}_K$-automorphism of S: it preserves the pairing and the closed-immersion condition. On the two coprime factors of the level structure one checks $\jmath \circ \widetilde{\delta}_K = \langle \delta \rangle \circ \jmath$. A separate choice for each δ suffices.

To describe the special fibre of S, we use the Igusa moduli problem. For an elliptic curve A/W over a k-scheme, let $A^{(p^a)} = A \times_{W, F_W^a} W$, where F_W is the absolute Frobenius of W, and write

$$F^a : A \longrightarrow A^{(p^a)}, \qquad V^a : A^{(p^a)} \longrightarrow A$$

for the iterated relative Frobenius and its dual Verschiebung [KM85, Sections 12.1–12.2].

Definition 5.5. Let W be a k-scheme and fix an elliptic curve A/W. An Igusa structure of level p^a on A/W, in the sense of [KM85, Def. 12.3.1], is a section

$$Z \in A^{(p^a)}(W)$$

satisfying

- $V^a(Z) = 0$;
- the equality

$$\sum_{i=1}^{p^a} [iZ] = \ker V^a$$

holds as effective Cartier divisors on $A^{(p^a)}/W$, where $[iZ]$ is the divisor of the section iZ.

The divisor condition says that Z generates $\ker V^a$ in the sense of [KM85, 1.4.1]. We write $[\mathrm{Ig}(p^a)]$ for the base change to k of Katz–Mazur's Igusa moduli problem on $(\mathrm{Ell}/\mathbb{F}_p)$ [KM85, (12.3.1.1)]. Its value on A/W is the set of these generators. An isomorphism of Igusa objects $(A/W, Z) \to (A'/W, Z')$ is an isomorphism $g : A \to A'$ over W with $g^{(p^a)}(Z) = Z'$.

The definition applies also at supersingular points. On the ordinary locus it is equivalent to requiring

$$(\mathbb{Z}/p^a\mathbb{Z})_W \longrightarrow \ker V^a, \qquad 1 \longmapsto Z$$

to be an isomorphism [KM85, Prop. 12.3.6 and proof of Thm. 12.6.1]. To retain the auxiliary full level, let $\mathcal{P}_k$ be the base change of $\mathcal{P}$ to k. We equip the same elliptic curve with both structures, taking their product as moduli problems in the sense of [KM85, 4.3.4].

Definition 5.6. Let W be a k-scheme. An object of the simultaneous moduli problem $(\mathcal{P}_k, [\mathrm{Ig}(p^a)])$ over W is a quadruple

$$(A/W,\ P,\ Q,\ Z),$$

where

- $(A/W, P, Q)$ is a $\mathcal{P}_k$-object, with pairing $e_n(P, Q) = \bar{\zeta}$;
- Z is an Igusa structure on A/W as in Definition 5.5.

An isomorphism is an isomorphism $g : A \to A'$ over W satisfying $g(P) = P'$, $g(Q) = Q'$, and $g^{(p^a)}(Z) = Z'$. On a fixed A/W, the simultaneous moduli problem takes the value

$$(\mathcal{P}_k, [\mathrm{Ig}(p^a)])(A/W) = \mathcal{P}_k(A/W) \times [\mathrm{Ig}(p^a)](A/W).$$

Its moduli scheme is

$$C_a = \mathfrak{M}(\mathcal{P}_k, [\mathrm{Ig}(p^a)]).$$

It exists because $\mathcal{P}_k$ is representable and $[\mathrm{Ig}(p^a)]$ is relatively representable [KM85, 4.3.4 and Thm. 12.6.1(1)]. The finite flat map $C_a \to B_k$, of degree $p^{a-1}(p-1)$, forgets Z. This moduli problem is defined over the whole B_k, including its supersingular points.

5.2. **Connectedness of the special fibre.**

Theorem 5.7. *There is an isomorphism of U_k-schemes*

$$S_k \simeq C_a \times_{B_k} U_k. \tag{5.4}$$

The geometric special fibre S_k is nonempty and connected.

Proof. We first prove (5.4). In this comparison, $\mathcal{A}$ denotes the universal elliptic curve restricted to U_k. By [KM85, Lemmas 12.2.1, 12.2.3 and 12.2.5, and Prop. 12.3.6], we have an exact sequence

$$0 \longrightarrow \ker F^a \longrightarrow \mathcal{A}[p^a] \xrightarrow{F^a} \ker V^a \longrightarrow 0,$$

whose kernels have rank p^a, with $\ker V^a$ étale and locally cyclic. For $W \to U_k$, take the kernels after pullback to $\mathcal{A}_W/W$. Any homomorphism $\mu_{p^a,W} \to \ker V^a$ is zero: it vanishes on geometric fibres, and its vanishing locus is open and closed by [KM85, Lemma 4.10.0(3)]. Thus an inclusion ι factors through $\ker F^a$ and is an isomorphism onto it, since both have rank p^a. Cartier duality, using the canonical principal polarizations, identifies $(\ker F^a)^D$ with $\ker V^a$ [KM85, (2.8.2.1)] and gives natural bijections

$$\begin{aligned}\mathrm{Incl}(\mu_{p^a,W}, \mathcal{A}_W[p^a]) &\simeq \mathrm{Isom}(\mu_{p^a,W}, \ker F^a)\\ &\simeq \mathrm{Isom}((\mathbb{Z}/p^a\mathbb{Z})_W, \ker V^a).\end{aligned}$$

The second bijection sends ι to $(\iota^D)^{-1}$, which specifies the Igusa generator $Z = (\iota^D)^{-1}(1)$. The constructions commute with base change and retain (P, Q), proving (5.4).

We now prove that S_k is nonempty and connected. Work over the whole B_k, including its supersingular points. The moduli problem $\mathcal{P}_k$ is representable, finite étale and surjective over (Ell/k): a basis exists étale locally, and rescaling one vector adjusts its pairing to $\bar{\zeta}$. The smooth compactification of B_k is connected, hence irreducible, by [KM85, Cor. 10.13.12]. Therefore B_k is connected. Since $B_k = \mathfrak{M}(\mathcal{P}_k)$ is connected, [KM85, Cor. 12.6.2(2)] shows that C_a is connected. By [KM85, Cor. 12.6.2(1)], C_a is a smooth curve, so it is also irreducible. The ordinary open U_k is nonempty, since the supersingular j-values form a finite set [KM85, Lemma 12.5.4]. As $C_a \to B_k$ is finite flat of positive degree, $C_a \times_{B_k} U_k$ is a nonempty open of this irreducible curve and is therefore connected. Now (5.4) proves that S_k is nonempty and connected. □

5.3. **Proof that $c = 1$.** We now apply the geometric result to the translation relation (5.1). The unramified extension used to construct S will be removed before we apply the local torsion bound.

Proposition 5.8. *For every $p \mid N$ and every $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$, $\tau_\delta \in E^0(\mathbb{Q}_p)$. Thus $E[c] \subseteq E^0(\mathbb{Q}_p)$.*

Proof. Let $\mathscr{E}/\mathbb{Z}_p$ be the Néron model of E. Since $\mathcal{O}_K/\mathbb{Z}_p$ is finite étale, $\mathscr{E}_{\mathcal{O}_K}$ is the Néron model over $\mathcal{O}_K$ [BLR90, Section 1.2, Prop. 2(c)]. Since S is smooth over $\mathcal{O}_K$, the Néron mapping property [BLR90, Section 1.2, Def. 1] extends $\psi_\mu \circ \jmath : S_K \to E_K$ uniquely to a morphism $h : S \to \mathscr{E}_{\mathcal{O}_K}$. The same property extends τ_δ to a section $\tilde{\tau}_\delta \in \mathscr{E}_{\mathcal{O}_K}(\mathcal{O}_K)$. Let $\widetilde{\delta}$ be the automorphism of S from Construction 5.4. Then (5.1) implies, by uniqueness in the Néron mapping property, $h \circ \widetilde{\delta} = h + \tilde{\tau}_\delta$.

The image of the connected scheme S_k (Theorem 5.7) lies in one component of $\mathscr{E}_k$. For $x \in S(k)$, the points $h(x)$ and $h(\widetilde{\delta}x)$ lie in that component. Their difference is $\tilde{\tau}_\delta(k)$, whose component class is therefore zero. Hence the reduction of τ_δ lies in the identity component of $\mathscr{E}_k$. The identity component of $\mathscr{E}_{\mathbb{F}_p}$ is geometrically irreducible [Stacks, Tag 0B7R], so its base change to k is the identity component of $\mathscr{E}_k$. Therefore $\tau_\delta \in \mathscr{E}^0(\mathbb{Z}_p) = E^0(\mathbb{Q}_p)$. The final assertion follows from (5.1). □

Lemma 5.9. *If an elliptic curve $A/\mathbb{Q}_p$ has additive reduction, then $\#A^0(\mathbb{Q}_p)[p] \leq p$.*

Proof. The group $A^0(\mathbb{Q}_p)$ consists of the points whose reduction on a minimal Weierstrass equation is nonsingular [Sil09, App. C, Thm. 15.1(d)]. Such an equation can be chosen with all $a_i \in p\mathbb{Z}_p$ [Pan12, Lemma 9]. By [Pan12, Thm. 1], the group $A^0(\mathbb{Q}_p)$ is then isomorphic to $\mathbb{Z}_p$ or to $p\mathbb{Z}_p \times \mathbb{F}_p$. □

Proposition 5.10. *Let E and c be as in Section 2. Then no prime divides c, that is, $c = 1$. In particular $c \neq 2$.*

Proof. Suppose that a prime p divides c. Since $p^2 \mid N$ and N is the conductor of E, E has additive reduction at p [Sil09, App. C, Section 16]. Equation (5.1) gives $E[p] \subseteq E[c] \subseteq E(\mathbb{Q})$. Proposition 5.8 and Lemma 5.9 then imply

$$p^2 = \#E[p] \leq \#E^0(\mathbb{Q}_p)[p] \leq p,$$

a contradiction. Therefore $c = 1$. □

Remark 5.11 (Another approach to the case $c = 2$). By (5.1), the map $\delta \mapsto \tau_\delta$ is a surjective homomorphism $(\mathbb{Z}/N\mathbb{Z})^\times/\langle -1\rangle \to E[c]$. The case $c = 2$ can also be excluded by showing that this homomorphism factors through a cyclic group. The argument uses the Shimura subgroup $\ker\big(J_0(N) \to J_1(N)\big)$, quadratic twists and rational 2-isogenies to reduce to the case $N = 32M$, with M odd and squarefree and reduction of type III at 2. In this case E has no point of order four over an unramified extension of $\mathbb{Q}_2$. For each odd prime $p \mid M$, let w_p be the Atkin–Lehner involution at p. Comparing the values of ψ_μ at the cusps of $X_\mu(N)$ above $w_p(\infty)$ shows that the factor $(\mathbb{Z}/p\mathbb{Z})^\times$ of $(\mathbb{Z}/N\mathbb{Z})^\times$ maps to zero. Hence $E[2]$ is a quotient of the cyclic group $(\mathbb{Z}/32\mathbb{Z})^\times/\langle -1\rangle$, which is impossible.

Declaration of generative AI use

The proof was initially obtained by ChatGPT-6 Pro. Subsequently, we used Codex 6-Astra, Claude Opus 5.5, and a verification framework OSVerify [OSVerify26] with Codex 5.6-Sol to review the output and improve writing. The authors verified the output and improved the exposition. The details of the use of AI are further disclosed in Appendix A for transparency. The authors are responsible for the correctness of this paper.

Appendix A. Details of generative AI usage

by Shurui Liu and Ping Nie

This appendix records how generative AI tools were used in producing this paper, for transparency and honesty.

A.1. **Persistent prompting with math guidance: the initial proof.** Initially, the result was obtained by heavily prompting ChatGPT-6 Pro, Claude Fable 5.1 and Codex 6-Astra.

A.1.1. *Initial attempt:* $c_\varphi \mid \deg \varphi$. On October 3rd, Ping Nie, who had not previously studied number theory, prompted ChatGPT-6 Pro and Claude Fable 5.1 to solve the classical Manin constant conjecture. The agents claimed to have solved the conjecture, but the authors found that only the weaker statement $c_\varphi \mid \deg \varphi$ had been proved.

A.1.2. *Breakthrough:* $c_E \mid 2$. Chi then continued prompting, building on the initial attempt:

(1) What are the current status and remaining cases? Has the conjecture been reduced to finitely many cases? Is the remaining work "low-hanging fruit"?
(2) Assuming these results and techniques from Nie's GitHub repo are correct. Prove the actual conjecture.

However, the model remained stuck on the "Hecke and lattice" approach, and Chi kept prompting as issues occurred:

(1) Try to find a different tech to solve this conjecture because the old techs were not working by the records from the repo.
(2) Try to prove the two comparisons for all conductors.
(3) Consider global number-theoretic properties, such as torsions and rational points, rather than focusing only on local geometry. If we can prove $c_E \in \{1, 2\}$, that would be substantial progress.

Prompt (3) became the turning point, and the model produced a proof that $c_E|2$.

Chi then asked the agent to write a Markdown file for a new agent to audit. Two independent runs of Codex 6-Astra at `max` reasoning effort reviewed the file and reported that it was correct.

A.1.3. *Finally:* $c_E = 1$. Chi further pushed the agent by prompting

(1) So short? Are you sure the argument is detailed enough?
(2) Try to prove that the constant divides 1.
(3) If you cannot find an example, try to prove that none exists.
(4) If the proof requires finiteness of the Tate–Shafarevich group, abandon that approach. Continue trying to prove the full conjecture.

After these rounds of prompts, ChatGPT-6 Pro finally proved $c_E = 1$.

A.2. **Non-math prompting with feasibility hint: a second proof.** After Nie was informed that Chi had used AI to generate a 22-page proof but did not see the proof, he restarted a fresh Codex 6-Astra session at `max` reasoning effort from the Git state in which only $c_\varphi \mid \deg \varphi$ had been proved, and prompted:

> "It was the wrong route and you only proved a weaker result. You should attack the actual Manin conjecutre. Summarize and learn from the past failures. It is known that there is a 22-page proof with a novel new idea."

The agents then kept working and provided a cleaner argument. Nie asked his agents to proofread the output carefully and also to search for other conjectures that could be resolved using the same method. This search led to the proof of Stevens' conjectures (Theorem 1.2). The combined output became the backbone of the current paper.

A.3. **Agentic AI reviewer.** Subsequently, Chi ran 12 independent checks of the output from Nie's agents using Codex 6-Astra and Claude Opus 5.5. All 12 checks passed and reported no mistakes.

However, Liu checked the output with OSVerify [OSVerify26] running on GPT-5.6-Sol at `xhigh` reasoning effort, which discovered one mistake (the claim that $L_E \in \mathbb{Q}[[w]]$ for every $E/\mathbb{Q}_p$ is wrong) and suggested a fix for the three places affected by it. Liu then used OSVerify with GPT-6-Astra at `max` reasoning effort and found no further issues.

The authors then used Codex-6-Astra and Claude-Opus-5.5 to improve the writing and to find relevant literature and previous work.

A.4. **Agentic systems: one-shot reproduction of the proof.** Liu used the automated mathematical reasoning agent Rethlas [Rethlas26] (running on GPT-6-Astra at `max` reasoning effort), enhanced by the verification framework OSVerify [OSVerify26] (running on GPT-5.6-Sol at `xhigh` reasoning effort), to attack the Manin constant conjecture. Only the statement of the conjecture was provided. The system automatically reproduced essentially the same proof as the one Nie obtained.

A.5. **Where the idea came from.** Probably the most important idea in the proof is to prove modularity of the normalized lift using [CDT25]. When the authors ask Codex-6-Astra to review the literature, list all previous study and check novelty, the agents reported [Yin26, Proposition 8.1] as "the closest earlier use of the method".

However, as Nie and Liu independently investigated the tool calls and websearch histroy, they both found that the agents did not search or read [Yin26] before obtaining the solution. One of the miracle moment was that the agent decided to search "`Manin+unbounded denominators`".

Liu also used the mathematics reasoning agent [Rethlas26] and reproduced the proof. This agent was, by design, required to download everything that it read from the Internet. Liu used Claude Code Fable-5.1 to monitor the process and report every websearch and download attempt. The memory and log files of Rethlas, together with the report by Claude Code, did not mention [Yin26].

This may be indications that AI could come up with this novel idea independently. However,

(1) The models may have learnt [Yin26] before the inference time. There is no solid evidence to exclude this possibilty.

(2) Yiyang Wang independently prompted Codex-6-Astra to ask questions about [Yin26], and then a single prompt "/goal prove manin constant c|2" reproduced the proof quickly. This indicates Yin's method is an extremely strong hint to the model.

References

[AU96] A. Abbes and E. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compos. Math. **103** (1996), no. 3, 269–286.

[ARS06] A. Agashe, K. Ribet and W. A. Stein, *The Manin constant*, Pure Appl. Math. Q. **2** (2006), no. 2, 617–636.

[BFF23] A. Babei, A. Fiori and C. Franc, *Families of ϕ-congruence subgroups of the modular group*, Mathematika **69** (2023), no. 4, 1104–1144.

[BLR90] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **21**, Springer-Verlag, Berlin, 1990.

[CDT25] F. Calegari, V. Dimitrov and Y. Tang, *The unbounded denominators conjecture*, J. Amer. Math. Soc. **38** (2025), no. 3, 627–702.

[Čes18] K. Česnavičius, *The Manin constant in the semistable case*, Compos. Math. **154** (2018), no. 9, 1889–1920.

[ČNS24] K. Česnavičius, M. Neururer and A. Saha, *The Manin constant and the modular degree*, J. Eur. Math. Soc. **26** (2024), no. 2, 573–637.

[CES03] B. Conrad, B. Edixhoven and W. Stein, *$J_1(p)$ has connected fibers*, Doc. Math. **8** (2003), 331–408.

[Edi91] B. Edixhoven, *On the Manin constants of modular elliptic curves*, in *Arithmetic algebraic geometry (Texel, 1989)*, Progr. Math. **89**, Birkhäuser Boston, Boston, MA, 1991, 25–39.

[Hon70] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan **22** (1970), no. 2, 213–246.

[Hon73] T. Honda, *Invariant differentials and L-functions. Reciprocity law for quadratic fields and elliptic curves over $\mathbb{Q}$*, Rend. Sem. Mat. Univ. Padova **49** (1973), 323–335.

[KM85] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies **108**, Princeton University Press, Princeton, NJ, 1985.

[Man71] Ju. I. Manin, *Cyclotomic fields and modular curves*, Uspehi Mat. Nauk **26** (1971), no. 6(162), 7–71 (Russian); English translation in Russian Math. Surveys **26** (1971), no. 6, 7–78.

[Maz78] B. Mazur, *Rational isogenies of prime degree*, with an appendix by D. Goldfeld, Invent. Math. **44** (1978), no. 2, 129–162.

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, second edition, Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009.

[Pan12] R. Pannekoek, *On p-torsion of p-adic elliptic curves with additive reduction*, arXiv: 1211.5833, preprint (2012).

[Stacks] The Stacks project authors, *The Stacks project*, https://stacks.math.columbia.edu, 2026.

[Ste89] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Invent. Math. **98** (1989), no. 1, 75–106.

[Vat05] V. Vatsal, *Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves*, J. Inst. Math. Jussieu **4** (2005), no. 2, 281–316.

[Woh64] K. Wohlfahrt, *An extension of F. Klein's level concept*, Illinois J. Math. **8** (1964), 529–535.

[Yin26] H. Yin, *A proof of the 4, 7 cases of Sylvester's conjecture on cube sums*, arXiv: 2605.25917, preprint (2026).

[OSVerify26] F. Nie, H. Ye, S. Liu, Z. Wang, S. Ermon and J. Zou, *One-sided verification under limited expert review*, arXiv: 2610.18089, preprint (2026).

[Rethlas26] H. Ju, G. Gao, J. Jiang, B. Wu, Z. Sun, S. Liu, L. Chen, Y. Wang, Y. Wang, Z. Wang, W. He, P. Wu, L. Xiao, R. Liu, B. Dai and B. Dong, *Automated conjecture resolution with formal verification*, arXiv: 2604.03789, preprint (2026).

Email address: znchi@zju.edu.cn
Email address: srliu@stanford.edu
Email address: ping.nie@pku.edu.cn