

ON THE MANIN–STEVENS 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 idea of the proof	3
1.3. Previous work	5
1.4. Contribution of this paper	5
1.5. Organization of the paper	6
1.6. Acknowledgements	6
2. Preliminaries	6
2.1. Notation and conventions	6
2.2. Results used	8
3. Integrality of lifts	9
3.1. Normalization at the cusp	10
3.2. Formal logarithms at primes of additive reduction	10
3.3. Integrality of the normalized lift	11
4. Modularity and rational torsion	12
4.1. The pullback cover and monodromy	12
4.2. Congruence and level	13
4.3. Descent and rational translations	14
4.4. Optimal parametrizations	15
5. Applications	16
5.1. Proof of the Manin constant conjecture	16
5.2. Proof of Stevens’ conjectures	20
Declaration of generative AI use	21
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	22
A.3. Agentic AI reviewer	22
A.4. Agentic systems: one-shot reproduction of the proof	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.

A.5. Where the idea came from	23
References	23

1. INTRODUCTION

1.1. Main results. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N , and let $f = \sum_{n \geq 1} a_n q^n$ be the normalized newform of weight two and level N attached to it, where $q = e^{2\pi iz}$ for z in the upper half-plane $\mathfrak{H}$. Put $\omega_f = 2\pi i f(z) dz = f(q) dq/q$. A surjection $\pi_0 : J_0(N) \twoheadrightarrow E$ is *optimal* if its kernel is connected.

For such π_0 let $\varphi_0 : X_0(N) \rightarrow E$ be given by $\varphi_0(P) = \pi_0([P] - [\infty])$, and let ω_E be a Néron differential of E .

By multiplicity one there is $c_E \in \mathbb{Q}^\times$ with $\varphi_0^* \omega_E = c_E \omega_f$. This is the Manin constant of E . Manin conjectured that $c_E = \pm 1$ [Man71, §10.3]; see [Čes18, Conj. 1.1] for the formulation used here.

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

Parametrizations by $X_1(N)$ were studied by Stevens [Ste89], where $X_1(N)$ is the Shimura's canonical model over $\mathbb{Q}$ in which the 0-cusp is a rational point [Ste89, §1].

For an isogeny class $\mathcal{C}$ of elliptic curves of conductor N there is a unique curve $E_1 \in \mathcal{C}$ with a parametrization $\varphi_1 : X_1(N) \rightarrow E_1$, sending the 0-cusp to the origin, whose Jacobian map $\pi_1 : J_1(N) \twoheadrightarrow E_1$ has connected kernel; φ_1 is unique up to sign [Ste89, Prop. 1.4].

Its Manin constant c_1 is defined by $\varphi_1^* \omega_{E_1} = c_1 \omega_f^{\text{St}}$, where ω_f^{St} is the differential attached to f in Stevens' coordinate [Ste89, Def. 1.1] (see §2.1), and $c_1 \in \mathbb{Z}$ [Ste89, Thm. 1.6].

Let $E_{\min} \in \mathcal{C}$ be the curve of minimal Faltings height. By [Ste89, Thm. 2.3] it is the unique curve of $\mathcal{C}$ that admits an étale isogeny to every member of $\mathcal{C}$.

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

The two assertions are Stevens' Conjecture I'(a) and Conjecture II, respectively; together they imply Conjecture I [Ste89, (1.7), Thms. 1.8 and 2.3, (2.4)]. The assertion $c_1 = \pm 1$ follows from Theorem 1.1 by [Čes18, Lemma 2.12]; the additional result proved here is $E_1 \simeq E_{\min}$.

Both proofs lift a modular parametrization through an isogeny: through $[c] : E \rightarrow E$, with $c = |c_E|$, for Theorem 1.1, and through $\alpha : E_{\min} \rightarrow E_1$ for the second assertion of Theorem 1.2. The lift exists analytically on the upper half-plane; the essential step is to prove modularity and then to descend to an algebraic map over $\mathbb{Q}$ on a modular curve of the required level.

Theorem 1.3 provides this modularity and descent under a bounded denominators hypothesis, with an isogeny variant used for α . We verify the hypothesis by proving integrality of the lifts.

We formulate the lifting result first for multiplication maps. Write $\pm G = \langle G, -I \rangle$ for a subgroup $G \subseteq \text{SL}_2(\mathbb{Z})$ and $\Gamma_1^\pm(N) = \pm \Gamma_1(N)$.

Let Γ be a group with $\Gamma_1^\pm(N) \subseteq \Gamma \subseteq \Gamma_0(N)$ and let X_Γ be the corresponding curve over $\mathbb{Q}$ in the μ_N -model, with its rational cusp ∞ and parameter q there (§2.1).

Let $E/\mathbb{Q}$ be an elliptic curve. Fix a global minimal integral Weierstrass equation for E , and let $x, y \in \mathbb{Q}(E)$ be its coordinate functions. Let $\varphi : X_\Gamma \rightarrow E$ be a non-constant morphism over $\mathbb{Q}$ with $\varphi(\infty) = 0$, and let $m \geq 1$.

There is a unique holomorphic map $\psi : \mathfrak{H} \rightarrow E(\mathbb{C})$ with

$$[m] \circ \psi = \varphi \quad \text{on } \mathfrak{H}, \quad \psi(z) \rightarrow 0 \text{ as } z \rightarrow i\infty.$$

We call ψ the *normalized lift of φ through $[m]$* . Its existence, uniqueness and rational q -expansions are established in Lemma 3.1. We denote the stabilizer of ψ by

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

Theorem 1.3 (Congruence, modularity and descent of lifts). *Assume that the coordinate q -expansions of the normalized lift ψ have **bounded denominators**: there is an integer $k \geq 1$ such that*

$$(1.1) \quad k \cdot x(\psi(q)), \quad k \cdot y(\psi(q)) \in \mathbb{Z}((q)).$$

Then:

- (i) 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 $X_\Gamma(\mathbb{C}) \times_{\varphi, E, [m]} E(\mathbb{C})$.
- (ii) $\Gamma_1^\pm(N) \subseteq G_\psi \subseteq \Gamma$, and G_ψ contains every parabolic and elliptic element of Γ .
- (iii) There is a unique morphism $\psi_\mu : X_\mu(N) \rightarrow E$ over $\mathbb{Q}$ with $\psi_\mu(\infty) = 0$ that is analytically equal to ψ ; it satisfies $[m]\psi_\mu = \varphi \circ \varpi_\Gamma$, where $\varpi_\Gamma : X_\mu(N) \rightarrow X_\Gamma$ is the quotient map.

The monodromy group

$$H = \{\psi(\gamma z) - \psi(z) : \gamma \in \Gamma\} \subseteq E[m]$$

consists of the points $\tau_\delta = \psi_\mu(\langle \delta \rangle \infty)$, where $\langle \delta \rangle$ runs through the diamond operators in $\Gamma/\Gamma_1^\pm(N)$; these points are rational: $H \subseteq E(\mathbb{Q})$.

The component in (i) descends to $\mathbb{Q}$, and its deck group is the constant group H , 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 .

- (iv) If $\Gamma = \Gamma_0(N)$ and $\varphi = \varphi_0$ comes from an optimal quotient $\pi_0 : J_0(N) \rightarrow E$, then $H = E[m]$. In particular $E[m] \subseteq E(\mathbb{Q})$.

Remark 1.4. In the proof of Theorem 1.1, we will use the case where $k = 1$, and the assumption (1.1) is proved in Proposition 3.6. The proofs of (i)–(iii) do not use that $[m]$ is multiplication: the same statements hold for the normalized lift of φ through any isogeny $\nu : E' \rightarrow E$ over $\mathbb{Q}$ (Remark 4.7). This is the variant used in the proof of Theorem 1.2 in §5.2.

1.2. The idea of the proof. The key step, which also motivates Theorem 1.3, is to show that $E[[c_E]]$ equals the set $\{\psi_\mu(\langle \delta \rangle \infty)\}_\delta$ of images of cusps. By Theorem 1.3, ψ_μ is defined over $\mathbb{Q}$, and the cusps $\langle \delta \rangle \infty$ are rational. Hence $E[[c_E]] \subseteq E(\mathbb{Q})$.

It therefore remains to prove that ψ has bounded denominators and to prove Theorem 1.3.

Put $c = |c_E|$, and choose the sign of φ_0 so that $c_E = c$. In the notation of Theorem 1.3, we take $\Gamma = \Gamma_0(N)$, $\varphi = \varphi_0$ and $m = c$, and let ψ be the normalized lift of φ_0 through $[c]$, with stabilizer $G_\psi \subseteq \Gamma_0(N)$. Since $[c] \circ \psi = \varphi_0$, the lift ψ can be viewed as a c -th root of φ_0 . As in §2.1, $t = -x/y$ is the parameter at the origin of the chosen minimal equation, $t_\psi = t \circ \psi$, and L_E is the normalized formal logarithm in this parameter.

The proof of Theorem 1.1 consists of four steps.

Step 1: ψ is integral. We recall Honda's formal-group comparison [Hon70, Thm. 9]; see also [Hon73, §3, p. 328]. The formal parameter of ψ is

$$t_\psi(q) = L_E^{-1} \left(\sum_{n \geq 1} \frac{a_n}{n} q^n \right).$$

At primes $p \nmid c$, integrality follows from the integral cusp and the integral formal inverse of $[c]$. At primes $p \mid c$, the support theorem [Čes18, Thm. 2.11] gives additive reduction. The formal logarithm and its inverse are then integral, and $a_n = 0$ whenever $p \mid n$. Together these give $t_\psi \in q + q^2 \mathbb{Z}[[q]]$ and $x \circ \psi, y \circ \psi \in \mathbb{Z}((q))$ (Proposition 3.6), establishing the bounded denominators hypothesis.

The next two steps prove Theorem 1.3.

Step 2: ψ is modular. After clearing the poles of the coordinate functions, the unbounded denominators theorem [CDT25, Thm. 1.0.1] implies that G_ψ is a congruence subgroup. The pullback cover is unramified at the cusps, so their widths are unchanged. Wohlfahrt's theorem [Woh64, Thm. 2], together with $T \in G_\psi$, then gives $\Gamma_1^\pm(N) \subseteq G_\psi$.

Thus the lift defines an algebraic map on $X_\mu(N)_\mathbb{C}$ (Theorem 1.3(i),(ii)).

Step 3: $E[c]$ is rational. The graph of the map from Step 2 is the connected component through $(\infty, 0)$ of $(X_\mu(N) \times_{\varphi_0 \circ \varpi, E, [c]} E)_\mathbb{C}$.

The pullback is defined over $\mathbb{Q}$, its geometric components are disjoint, and $(\infty, 0)$ is rational. Hence the graph is Galois-stable and the lift descends to a morphism

$$\psi_\mu : X_\mu(N) \longrightarrow E \quad \text{over } \mathbb{Q}, \quad [c] \circ \psi_\mu = \varphi_0 \circ \varpi.$$

This field of definition supplies the rationality needed in the local argument. Since the diamond operators and the cusp ∞ are also defined over $\mathbb{Q}$, the monodromy translations satisfy $\tau_\delta = \psi_\mu(\langle \delta \rangle \infty) \in E(\mathbb{Q})$. Thus the monodromy group H consists of rational torsion points (Theorem 1.3(iii)).

Optimality now identifies H with $E[c]$ (Theorem 1.3(iv)), so $E[c] \subseteq E(\mathbb{Q})$. One can then deduce directly from the Weil pairing that $c \mid 2$; see Remark 5.1.

It remains to exclude the case $c = 2$.

Step 4: Igusa schemes and local torsion. We use an argument valid for any prime $p \mid c$. The rational translations τ_δ lie in $E(\mathbb{Q}_p)$. The Igusa scheme is smooth over an unramified extension of $\mathbb{Z}_p$ and has connected special fibre. Its geometry forces the diamond translations into the identity component of the Néron model, giving $E[p] \subseteq E^0(\mathbb{Q}_p)$. The local torsion bound then gives

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

a contradiction. Thus $c = 1$, proving Theorem 1.1.

Proof of Theorem 1.2: lifting the parametrization to $E_{\min}$. Theorem 1.1 and [Čes18, Lemma 2.12] first give $c_1 = \pm 1$. Stevens' theorem supplies an isogeny $\alpha : E_{\min} \rightarrow E_1$ that is étale on Néron models. After choosing its sign, its formal expansion has linear coefficient 1 and an integral inverse. The normalized lift of φ_1 through α therefore has integral coordinate expansions.

We apply the same congruence, level and descent argument to this lift, using the isogeny variant in Remark 4.7. It gives

$$h' : X_\mu(N) \longrightarrow E_{\min} \quad \text{over } \mathbb{Q}, \quad \alpha \circ h' = \varphi_1.$$

On Jacobians, this factorization and the connected kernel of the optimal quotient force α to be an isomorphism. Hence $E_1 \simeq E_{\min}$; together with $c_1 = \pm 1$, this proves Theorem 1.2.

1.3. Previous work. Using reduction modulo p and stable models [Edi91, §1], Edixhoven proved that c_E is an integer [Edi91, Prop. 2], and that $\text{ord}_p(c_E) = 0$ for $p \geq 11$ unless $E_{\mathbb{Q}_p}$ has potentially ordinary reduction of Kodaira type II, III or IV [Edi91, Thm. 3].

Česnavičius proved that $\text{ord}_p(c_E) = 0$ whenever $p^2 \nmid N$, so that the Manin constant conjecture holds for semistable E [Čes18, Thm. 2.11]; the same holds for the curves between $X_1(N)$ and $X_0(N)$ [Čes18, Thm. 2.13]. His approach uses multiplicity one for the Hecke action on the Lie algebra of the Néron model of $J_0(N)$ and compares congruences with the modular degree [Čes18, §2].

Many special cases of these statements, in particular at odd primes, were known before [Maz78, Cor. 4.1], [AU96], [ARS06, Thm. 2.7]; see [Čes18, §1].

Česnavičius, Neururer and Saha prove $c_\varphi \mid \deg \varphi$ for $X_1(N)$ and $c_\varphi \mid 6 \deg \varphi$ for intermediate modular curves [ČNS24, Thms. 1.1, 1.2]. They use local Whittaker newforms to bound the denominators of f at all cusps and prove integrality of the newform differential [ČNS24, §§4–5]. Generalizations of the Manin constant conjecture to optimal quotients of higher dimension fail [Čes18, Thm. 5.10].

For $X_1(N)$, Stevens formulated Conjectures I, I' and II, proved the existence of $E_{\min}$ [Ste89, Thm. 2.3], and verified Conjecture I for conductors at most 200 [Ste89, Thm. 7.1]. Vatsal proved that the étale isogeny $E_{\min} \rightarrow E_1$ has 2-power degree for semistable isogeny classes, and that $E_{\min} \simeq E_1$ when E has a rational ℓ -isogeny for some $\ell \geq 7$ at which it is ordinary [Vat05, Thms. 1.10, 1.11].

Honda proved that the formal group of a global minimal Weierstrass model of an elliptic curve over $\mathbb{Q}$ and the formal group attached to its L -series are strongly isomorphic over $\mathbb{Z}$ [Hon70, Thm. 9]; see also [Hon73, §3, p. 328]. Babei, Fiori and Franc [BFF23, §3.2.2] study lifts through multiplication maps on the elliptic modular curve $y^2 = x^3 - 1728$, including coordinate q -expansions and their denominators.

Optimality cannot be dropped in Theorem 1.1: in the isogeny class of conductor 11, a non-optimal curve receives a map from $X_0(11)$ with Manin constant 5 [Ste89, Example 1.11].

1.4. Contribution of this paper. In this paper, we adapt the results above and combine Honda's classical computation [Hon70, Thm. 9], [Hon73, §3, p. 328] with the unbounded denominators theorem [CDT25] to prove the modularity of the normalized lift.

This application adapts Yin's argument for certain cubic roots of modular functions attached to CM curves [Yin26, Prop. 8.1]. The subsequent use of parabolic

elements and Wohlfahrt's theorem also occurs in Stevens' universal factorization theorem [Ste89, Thm. 1.9]. The order of the integrality argument is different: Yin first proves that the relevant Manin–Stevens constants are units [Yin26, Thm. 6.1] and uses this to obtain integral expansions [Yin26, §7 and proof of Prop. 8.1]; here the lift is integral before c is determined.

1.5. Organization of the paper. Section 2 fixes notation and records the results used. Section 3 constructs the normalized lift and proves its integrality through Proposition 3.6 (Step 1). Section 4 proves Theorem 1.3: congruence and level give modularity (Step 2), while descent and optimality give rational torsion (Step 3). Section 5 contains the two applications in sequence. In §5.1, Igusa geometry and the local torsion bound complete Step 4 and prove Theorem 1.1. In §5.2, this result and the isogeny variant then yield Theorem 1.2.

1.6. Acknowledgements. Z. Chi would like to thank Hongbo Yin for sharing the motivation behind the beautiful theory 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. PRELIMINARIES

2.1. Notation and conventions.

2.1.1. Groups and cusp widths. We use $\pm G$ and $\Gamma_1^\pm(N)$ as in §1.1, and write

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

An element $\gamma \neq \pm I$ of $\mathrm{SL}_2(\mathbb{Z})$ is *parabolic* if $|\mathrm{tr} \gamma| = 2$, and *elliptic* if $|\mathrm{tr} \gamma| < 2$.

Let $G \subseteq \mathrm{SL}_2(\mathbb{Z})$ have finite index and contain $-I$. If $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ maps ∞ to a cusp κ , the *width* of κ for G is

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

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

2.1.2. The modular curve $X_\mu(N)$. 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]. The rational cusp ∞ is the Tate curve $\mathrm{Tate}(q)$ with $\mu_N \subseteq \mathbf{G}_m$, and q is a parameter at ∞ .

Analytically, we use the identification

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

Under this identification, ∞ maps to ∞ and $q = e^{2\pi iz}$.

2.1.3. *Diamond operators and quotient curves.* 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 over $\mathbb{Q}$. A matrix $\gamma = \begin{pmatrix} a & b \\ Nr & d \end{pmatrix} \in \Gamma_0(N)$ acts on $X_\mu(N)(\mathbb{C})$ as $\langle d \rangle$. Indeed, multiplication by $Nrz + d$ gives

$$\mathbb{C}/(\mathbb{Z}\gamma z + \mathbb{Z}) \longrightarrow \mathbb{C}/(\mathbb{Z}z + \mathbb{Z}), \quad w \mapsto (Nrz + d)w,$$

and sends $1/N$ to d/N modulo the lattice.

For $\Gamma_1^\pm(N) \subseteq \Gamma \subseteq \Gamma_0(N)$, let Δ_Γ be the image of Γ in $(\mathbb{Z}/N\mathbb{Z})^\times / \{\pm 1\}$. We put

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

Here ϖ_Γ is the quotient map. All points $\langle \delta \rangle_\infty$ are rational, and $X_\Gamma(\mathbb{C}) = \Gamma \backslash \mathfrak{H}^*$.

For $\Gamma = \Gamma_0(N)$, this is the usual model of $X_0(N)$ with its cusp ∞ and parameter q . In this case we write $\varpi = \varpi_{\Gamma_0(N)}$ for the forgetful map $\varpi : (A, \iota) \mapsto (A, \iota(\mu_N))$.

2.1.4. *Comparison with Stevens' conventions.* The μ_N -model 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 Stevens' rational 0-cusp is identified with the Tate cusp; see also [CES03, proof of Lemma 6.1.6]. His uniformizing variable τ and ours are related by $z = -1/(N\tau)$ and $q_0 = e^{-2\pi i/(N\tau)} = e^{2\pi iz} = q$.

Stevens' differential ω_f^{St} is $2\pi i f(\tau) d\tau$ in his coordinate. In ours it is

$$\omega_f^{\text{St}} = \varepsilon_N \cdot 2\pi i f(z) dz,$$

where $\varepsilon_N = \pm 1$ is the eigenvalue of the Fricke involution on f . Consequently, in our coordinate,

$$(2.1) \quad \varphi_1^* \omega_{E_1} = \varepsilon_N c_1 f(q) \frac{dq}{q} \quad \text{on } X_\mu(N).$$

2.1.5. *Cartier duality.* For a finite locally free commutative group scheme G , we write G^D for its Cartier dual.

2.1.6. *Néron models and formal groups.* For an elliptic curve E over $\mathbb{Q}_p$, let $\mathcal{E}$ be its Néron model over $\mathbb{Z}_p$, and let $\mathcal{E}^0$ be its identity component. We write

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

Thus $E^0(\mathbb{Q}_p)$ is the subgroup of points whose reduction lies in $\mathcal{E}_{\mathbb{F}_p}^0$.

For a minimal Weierstrass equation, we use the parameter $t = -x/y$ at the origin. We denote the formal group in this parameter by $\widehat{E}$ and its normalized logarithm by

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

From now on, ω_E denotes the invariant differential of the chosen minimal equation. It is a Néron differential, and its expansion in t is $dL_E(t)$.

Replacing a parametrization by its negative changes the sign of its Manin constant. For instance, replacing π_0 by $-\pi_0$ preserves optimality. For a based map g to E , we write $t_g = t \circ g$.

2.1.7. *Maps on Jacobians.* We use the following elementary fact.

Lemma 2.1. *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 $g : V \rightarrow D_2$ be a morphism to an elliptic curve with $g(o) = 0$. If $g_*(\ker \pi)$ is finite, where $g_* : J_V \rightarrow D_2$ is the induced homomorphism, then $g_* = u \circ \pi$ for a unique homomorphism $u : D_1 \rightarrow D_2$. If moreover $\lambda \circ g_* = \pi$ for an isogeny $\lambda : D_2 \rightarrow D_1$, then $\lambda \circ u = \text{id}_{D_1}$, and λ and u are isomorphisms.*

Proof. The image $g_*(\ker \pi)$ is connected and finite, hence zero, and g_* factors through the quotient $J_V/\ker \pi = D_1$. If $\lambda g_* = \pi$, then $\lambda u \pi = \pi$, and surjectivity of π gives $\lambda u = \text{id}$; since degrees of nonzero homomorphisms of elliptic curves multiply, $\deg \lambda = \deg u = 1$. $\square$

2.2. **Results used.** We use the following published results in the stated forms.

- (R1) *Integrality and support of Manin constants.* For an optimal quotient $\pi_0 : J_0(N) \twoheadrightarrow E$ with N the conductor of E , the constant c_E is an integer [Edi91, Prop. 2], and $\text{ord}_p(c_E) = 0$ for every prime p with $p^2 \nmid N$ [Čes18, Thm. 2.11]. For a group Λ with $\Gamma_1(N) \subseteq \Lambda \subseteq \Gamma_0(N)$ and an optimal quotient $J_\Lambda \twoheadrightarrow E$, the Manin constant has $\text{ord}_p = 0$ whenever $p^2 \nmid N$ [Čes18, Thm. 2.13]. The constant c_1 is an integer [Ste89, Thm. 1.6].
- (R2) *Integral cusps.* The completion of $X_0(N)_\mathbb{Z}$ along the cusp ∞ is $\text{Spf } \mathbb{Z}[[q]]$, and ∞ lies in the smooth locus [Edi91, proof of Prop. 2]. 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, is smooth, and the Tate curve with $\mu_N \subseteq \mathbf{G}_m$ defines a morphism from $\text{Spec } \mathbb{Z}[[q]]$ to it which is the formal neighbourhood of the cusp ∞ [Ste89, proof of Thm. 1.6]; the smooth model, its integral cusp, and the formal parameter are also recorded in [CES03, proof of Lemma 6.1.6].
A morphism from the generic fibre of a smooth scheme over a discrete valuation ring to an abelian variety extends to the Néron model, and Néron models commute with étale base change [BLR90, §1.2].
- (R3) *Unbounded denominators* [CDT25, Thm. 1.0.1]. Let $F : \mathfrak{H} \rightarrow \mathbb{C}$ be holomorphic, with Fourier expansion at ∞ in $\mathbb{Z}[[q]]$, and suppose that F is a modular form of some integral weight for a finite-index subgroup of $\text{SL}_2(\mathbb{Z})$ that is meromorphic at the cusps. Then F is a modular form for a congruence subgroup. (The full theorem allows expansions in fractional powers of $e^{\pi iz}$; we only need $\mathbb{Z}[[q]]$.) This theorem is applied in Proposition 4.3, after clearing the poles of the coordinate functions of the normalized lift, to prove that G_ψ is a congruence subgroup.
- (R4) *Wohlfahrt's theorem* [Woh64, Thm. 2], in the form quoted from the end of the proof of [CDT25, Lemma 4.4.1] where they denote $\{\pm I\}$ by E : if a congruence subgroup G contains $-I$, then

$$\langle -I, \Gamma(L(G)) \rangle = \pm \Gamma(L(G)) \subseteq G.$$

For an integer $m \geq 1$, we write

$$\Gamma(m) = \ker(\text{SL}_2(\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/m\mathbb{Z})), \pm \Gamma(m) = \langle -I, \Gamma(m) \rangle.$$

- (R5) *Igusa's theorem* [Kat73, Thm. 4.3 and its proof]. Let $n \geq 3$ with $p \nmid n$, put $q = p^{f_0}$ with $q \equiv 1 \pmod{n}$, and fix a primitive n -th root of unity $\zeta \in \mathbb{F}_q$. Let $B_{n, \mathbb{F}_q}$ be the fine moduli scheme of elliptic curves equipped with an ordered basis (P_1, P_2) of their n -torsion satisfying $e_n(P_1, P_2) = \zeta$, and let $\mathcal{A} \rightarrow B_{n, \mathbb{F}_q}$ be the universal elliptic curve. Denote by $B_{n, \mathbb{F}_q}^{\text{ord}}$ the complement of the supersingular locus. This ordinary locus is smooth, affine, and geometrically connected.

For every $a \geq 1$, the geometric monodromy representation on the kernel of the iterated Verschiebung $V^a : \mathcal{A}^{(p^a)} \rightarrow \mathcal{A}$ is surjective:

$$\pi_1\left(B_{n, \mathbb{F}_p}^{\text{ord}}, \bar{\eta}\right) \longrightarrow \text{Aut}((\ker V^a)_{\bar{\eta}}) \cong (\mathbb{Z}/p^a\mathbb{Z})^\times,$$

where $\bar{\eta}$ is a geometric generic point. The representation remains surjective after restriction to every nonempty open subset.

Remark 2.2 (Comparison with Katz's notation). The scheme $B_{n, \mathbb{F}_q}$ is the open-and-closed component, on which the Weil pairing has value ζ , of Katz's noncompactified modular scheme $M_n \otimes_{\mathbb{Z}[1/n]} \mathbb{F}_q$ [Kat73, §1.4, pp. 81–82]. Our ordered basis (P_1, P_2) corresponds to Katz's level structure $\alpha_n : \mathcal{A}[n] \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^2$ via $\alpha_n(P_1) = (1, 0)$ and $\alpha_n(P_2) = (0, 1)$ [Kat73, §1.2, p. 79]. In the notation of [Kat73, §4.2.0, p. 146], we therefore have

$$B_{n, \mathbb{F}_q}^{\text{ord}} \simeq S_1^\zeta, \quad B_{n, \mathbb{F}_p}^{\text{ord}} \simeq S_1^\zeta \times_{\mathbb{F}_q} \overline{\mathbb{F}_p}.$$

Here S_1^ζ is the ordinary locus in $M_n \otimes \mathbb{F}_q$; Katz's $\overline{S}_1^\zeta$ also includes the cusps.

Katz's Theorem 4.3 is stated for $\overline{S}_m^\zeta$ over $W_m(\mathbb{F}_q) = W(\mathbb{F}_q)/p^m$, and its assertion for every nonempty open subset applies in particular to S_m^ζ . The group appearing there is $\ker((\tilde{\pi})^m)$, where $(\tilde{\pi})^m$ denotes the composite of the successive dual canonical-quotient isogenies. Its reduction to S_1^ζ is $\ker(V^m)$; the passage between these representations uses invariance of the étale topology under nilpotent thickenings [Kat73, p. 147, proof of Lemma 4.2.1]. With $m = a$, the characteristic- p representation in Katz's proof is precisely the one displayed above. Its geometric surjectivity follows from the full supersingular inertia computed in the proof of Theorem 4.3 and in Theorem 4.3 bis [Kat73, pp. 149–150].

- (R6) *Stevens* [Ste89]. The optimal $X_1(N)$ -parametrization exists and is unique up to sign [Ste89, Prop. 1.4]. The curve $E_{\min}$ exists and admits an isogeny to every curve in its isogeny class which is étale on Néron models [Ste89, Thm. 2.3]. An isogeny over $\mathbb{Q}_p$ induces an étale morphism of Néron models over $\mathbb{Z}_p$ if and only if it pulls back a Néron differential to a Néron differential [Ste89, Lemma 2.2].

3. INTEGRALITY OF LIFTS

We first construct normalized lifts and establish their rational q -expansions. We then prove integrality for the lift through the Manin constant in Proposition 3.6, using formal groups and integral cusp models. The support statement (R1) ensures that primes dividing the constant are primes of additive reduction.

3.1. Normalization at the cusp.

Lemma 3.1 (Normalization at the cusp). *Let $\Gamma_1^\pm(N) \subseteq \Gamma \subseteq \Gamma_0(N)$, let $\varphi : X_\Gamma \rightarrow E$ be a non-constant morphism over $\mathbb{Q}$ with $\varphi(\infty) = 0$, and let $m \geq 1$. Fix a global minimal integral equation of E , with coordinate functions x, y and parameter $t = -x/y$. There is a unique holomorphic map $\psi : \mathfrak{H} \rightarrow E(\mathbb{C})$ with*

$$[m] \circ \psi = \varphi, \quad \psi(z) \rightarrow 0 \quad \text{as } z \rightarrow i\infty.$$

It is invariant under T , and $t_\psi \in q\mathbb{Q}[[q]]$. Consequently $x \circ \psi$ and $y \circ \psi$ are Laurent series in q with rational coefficients.

Proof. The map $[m] : E(\mathbb{C}) \rightarrow E(\mathbb{C})$ is a covering and $\mathfrak{H}$ is simply connected, so lifts of φ exist and any two differ by a constant in $E[m]$. As $z \rightarrow i\infty$, a lift remains in one sheet over a small disc around 0 and tends to a point of $E[m]$. Translating by its inverse gives the unique lift with limit 0.

The function $z \mapsto \psi(z+1) - \psi(z)$ is continuous with values in $E[m]$, hence constant, and its limit at $i\infty$ is zero. Thus the lift is invariant under T and extends as a holomorphic function of q across $q = 0$. Since φ and the cusp parameter are defined over $\mathbb{Q}$, $t_\varphi \in q\mathbb{Q}[[q]]$. The formal multiplication series $[m]_{\widehat{E}}(w) = mw + O(w^2)$ has a compositional inverse over $\mathbb{Q}$, so

$$t_\psi = [m]_{\widehat{E}}^{-1}(t_\varphi) \in q\mathbb{Q}[[q]].$$

The series is nonzero because φ is non-constant. Substitution in $x(t) \in t^{-2}\mathbb{Z}[[t]]$ and $y(t) \in t^{-3}\mathbb{Z}[[t]]$ gives the coordinate Laurent series. $\square$

3.2. Formal logarithms at primes of additive reduction.

Lemma 3.2. *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 . $\square$

Lemma 3.3. *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 $[p]_F(w) = pg(w)$ 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

$$(3.1) \quad (1 - p^{r-1})b_r = g_r + \sum_{\ell=2}^{r-1} p^{\ell-1}b_\ell [w^r]g(w)^\ell,$$

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 3.2. $\square$

Lemma 3.4. *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 smooth locus of the minimal Weierstrass model is $\mathcal{E}^0$, and $\widehat{E}$ is its completion along the zero section. The special fibre $\mathcal{E}_{\mathbb{F}_p}^0$ is a form of $\mathbb{G}_a$ over the perfect field $\mathbb{F}_p$, hence isomorphic to $\mathbb{G}_a$, on which multiplication by p is zero. Therefore $[p]_{\widehat{E}}$ reduces to zero modulo p , and Lemma 3.3 applies. $\square$

3.3. Integrality of the normalized lift. The cusp ∞ of $X_0(N)_{\mathbb{Z}}$ lies in the smooth locus over $\mathbb{Z}$, and the completion of $X_0(N)_{\mathbb{Z}}$ along it is $\mathrm{Spf} \mathbb{Z}[[q]]$ [Edi91, proof of Prop. 2]. Likewise, let $\mathcal{X}_{\mu}(N)$ be 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. This scheme is smooth over $\mathbb{Z}$, and its generic fibre is an open subscheme of $X_{\mu}(N)$ containing ∞ ; the Tate curve with $\mu_N \subseteq \mathbb{G}_m$ defines a $\mathbb{Z}$ -point ∞ of $\mathcal{X}_{\mu}(N)$, and the completion along it is $\mathrm{Spf} \mathbb{Z}[[q]]$ [Ste89, proof of Thm. 1.6], [CES03, proof of Lemma 6.1.6]. In both cases the formal parameter q computes the analytic q -expansion at ∞ . We write $V_{\mathbb{Z}_p}^{\mathrm{sm}}$ for the smooth locus of $X_0(N)_{\mathbb{Z}_p}$, respectively for $\mathcal{X}_{\mu}(N)_{\mathbb{Z}_p}$, and note that ∞ is a $\mathbb{Z}_p$ -point of $V_{\mathbb{Z}_p}^{\mathrm{sm}}$.

These integral cusp models let us apply the Néron mapping property to the original parametrization before lifting it.

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

Proof. If φ is constant, it is the zero map and the assertion is immediate. Assume that φ is non-constant. Fix a prime p . Let $U = V_{\mathbb{Z}_p}^{\mathrm{sm}}$ be the smooth $\mathbb{Z}_p$ -scheme of §3.3, which contains the cusp ∞ as a $\mathbb{Z}_p$ -point with completed local ring $\mathbb{Z}_p[[q]]$. The Néron mapping property extends φ to a morphism $U \rightarrow \mathcal{E}$. The section ∞ of U maps to a section of $\mathcal{E}$ which vanishes on the generic fibre, hence is the zero section, since $\mathcal{E}$ is separated. Therefore the composite $\mathrm{Spf} \mathbb{Z}_p[[q]] \rightarrow U \rightarrow \mathcal{E}$ factors through the formal completion $\mathrm{Spf} \mathbb{Z}_p[[t]]$ of $\mathcal{E}$ along its zero section, and $t \mapsto t_{\varphi}(q) \in q\mathbb{Z}_p[[q]]$. The coefficients of t_{φ} are rational because φ , the cusp, and the parameter q are defined over $\mathbb{Q}$. Since p was arbitrary, we get $t_{\varphi} \in q\mathbb{Z}[[q]]$. $\square$

Proposition 3.6. *Let V be $X_0(N)$ or $X_{\mu}(N)$, with its rational cusp ∞ and parameter q . Let $E/\mathbb{Q}$ be an elliptic curve of conductor N with newform f . Fix a global minimal integral Weierstrass equation for E , with coordinate functions x, y and invariant Néron differential ω_E . Let $\varphi : V \rightarrow E$ 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 $p \mid c$. Let ψ be the normalized lift of φ through $[c]$. Then

$$t_{\psi}(q) = L_E^{-1} \left(\sum_{n \geq 1} \frac{a_n}{n} q^n \right) \in q\mathbb{Z}[[q]], \quad t_{\psi}(q) = q + O(q^2),$$

and $x(\psi(q)), y(\psi(q)) \in \mathbb{Z}((q))$. In particular, the bounded denominators hypothesis (1.1) holds with $k = 1$.

Proof. Step 1: the formula for t_{ψ} . Integrating $\varphi^* \omega_E = c \omega_f$ with vanishing constant term gives

$$L_E(t_{\varphi}(q)) = c \ell_f(q), \quad \ell_f(q) = \sum_{n \geq 1} \frac{a_n}{n} q^n.$$

Since $L_E \circ [c]_{\widehat{E}} = c L_E$, the normalized lift ψ , characterized by $[c]_{\widehat{E}}(t_\psi) = t_\varphi$ and $t_\psi(0) = 0$ (Lemma 3.1), satisfies $L_E(t_\psi) = \ell_f$, that is, $t_\psi = L_E^{-1}(\ell_f)$. Its linear coefficient is $a_1 = 1$.

Step 2: integrality of t_ψ at each prime. Fix a prime p . If $p \nmid c$, then $c^{-1}[c]_{\widehat{E}}(w) = w + O(w^2)$ has coefficients in $\mathbb{Z}_p$, so $[c]_{\widehat{E}}^{-1}$ is p -integral by Lemma 3.2, and $t_\psi = [c]_{\widehat{E}}^{-1}(t_\varphi) \in q\mathbb{Z}_p[[q]]$ by Lemma 3.5. If $p \mid c$, then $p^2 \mid N$, so E has additive reduction at p and the Euler factor of f at p is trivial. Hence $a_n = 0$ whenever $p \mid n$, every nonzero coefficient a_n/n of ℓ_f lies in $\mathbb{Z}_p$, and Lemma 3.4 gives $t_\psi = L_E^{-1}(\ell_f) \in q\mathbb{Z}_p[[q]]$.

Every coefficient of t_ψ is rational and belongs to $\mathbb{Z}_p$ for every prime p , so $t_\psi \in q\mathbb{Z}[[q]]$ with linear coefficient 1. The minimal equation gives $x(t) \in t^{-2}\mathbb{Z}[[t]]$ and $y(t) \in t^{-3}\mathbb{Z}[[t]]$, with leading coefficients 1 and -1 ; substituting $t = t_\psi(q)$ gives the last assertion. $\square$

Remark 3.7. The parameter of φ itself is $t_\varphi(q) = cq + O(q^2)$, whereas $t_\psi(q) = q + O(q^2)$. Thus $x \circ \varphi$ and $y \circ \varphi$ have denominators at the primes dividing c , while $x \circ \psi$ and $y \circ \psi$ do not. The integrality of $t_\psi = L_E^{-1}(\ell_f)$ also follows from Honda's formal-group comparison [Hon70, Thm. 9]; see also [Hon73, §3, p. 328].

4. MODULARITY AND RATIONAL TORSION

We use the notation of Theorem 1.3 and the normalized lift constructed in Lemma 3.1. The pullback cover and its monodromy do not require bounded denominators; we impose (1.1) from §4.2 onwards. Following Yin's congruence strategy [Yin26, Prop. 8.1], bounded denominators and cusp widths give $\Gamma_1^\pm(N)$ -invariance. Descent at the rational cusp then makes the translations rational, and optimality identifies them with $E[m]$. The isogeny variant needed for Stevens' conjectures is recorded in Remark 4.7.

4.1. The pullback cover and monodromy. The normalization singles out one component of the pullback cover. Its monodromy records exactly how the lift changes under Γ .

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

$$(4.1) \quad Y = X \times_{\varphi, E, [m]} E.$$

Since $[m]$ is finite étale, so is $Y \rightarrow X$; in particular Y is a compact complex curve, possibly disconnected, unramified over X at every point, including the cusps and the images of the elliptic points.

Lemma 4.1. *For $\gamma \in \Gamma$, the function $z \mapsto \psi(\gamma z) - \psi(z)$ is constant, with value $\rho(\gamma) \in E[m]$. The map $\rho : \Gamma \rightarrow E[m]$ is a homomorphism with kernel G_ψ ; it 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 from $X_{G_\psi}(\mathbb{C}) = G_\psi \backslash \mathfrak{H}^*$ onto the connected component Y_ψ of Y through $(\infty, 0)$, and the deck group of $Y_\psi \rightarrow X$ is $H = \rho(\Gamma)$, acting by translation on the second factor.*

Proof. The function $z \mapsto \psi(\gamma z) - \psi(z)$ is continuous with values in the discrete group $E[m]$, hence constant. For $\gamma, \gamma' \in \Gamma$,

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

so ρ is a homomorphism, with kernel G_ψ by definition. 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 $\mathrm{Im} z'$ 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 $Y \rightarrow X$ is a covering, its lift $z \mapsto (z, \psi(z))$ is a closed loop, so $\rho(\gamma) = 0$.

The map $z \mapsto (z, \psi(z))$ identifies $G_\psi \backslash \mathfrak{H}$ with an open subset of Y_ψ , and H acts on Y_ψ by translation on the second factor; this is the deck group of $Y_\psi \rightarrow X$. The map extends over every cusp, because $Y \rightarrow X$ is unramified there, so $Y_\psi = X_{G_\psi}(\mathbb{C})$ as compact Riemann surfaces. $\square$

Corollary 4.2. *Every cusp has the same width for G_ψ as for Γ . In particular $L(G_\psi) = L(\Gamma)$.*

Proof. The inclusion $G_\psi \subseteq \Gamma$ shows that the width for Γ divides the width for G_ψ , and the parabolic elements of Γ lie in G_ψ by Lemma 4.1, which gives the other divisibility. $\square$

The finite translation action described by ρ plays the role of the cubic characters used by Yin to describe changes of branches [Yin26, Props. 5.6 and 5.7].

4.2. Congruence and level.

4.2.1. *From bounded denominators to congruence.* We follow the congruence and level argument of [Yin26, Prop. 8.1], applied to the coordinate functions of the lift. To use the holomorphic formulation of the unbounded denominators theorem, we first clear their poles by modular forms of level one.

Let j denote the classical modular invariant, and let

$$\Delta(q) = q \prod_{n \geq 1} (1 - q^n)^{24}$$

be the normalized cusp form of weight 12 for $\mathrm{SL}_2(\mathbb{Z})$. It has no zeros on $\mathfrak{H}$.

Proposition 4.3. *G_ψ is a congruence subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$.*

Proof. The group G_ψ has finite index in Γ by Lemma 4.1, hence in $\mathrm{SL}_2(\mathbb{Z})$. Set $u_x = x \circ \psi$ and $u_y = y \circ \psi$. The bounded denominators assumption (1.1) is proved by Proposition 3.6. Thus we can choose positive integer k so that both ku_x and ku_y lies in $\mathbb{Z}((q))$. Because $\Delta \in q + q^2\mathbb{Z}[[q]]$, we may choose sufficiently large integer s so that $k\Delta^s u_x, k\Delta^s u_y \in \mathbb{Z}[[q]]$.

They are G_ψ -invariant meromorphic functions on $\mathfrak{H}$, meromorphic at the cusps by Lemma 4.1. A pole of u_x or u_y in $\mathfrak{H}$ is a point z with $\psi(z) = 0$, hence $\varphi(z) = 0$, 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, since u_x and u_y are G_ψ -invariant with finitely many poles modulo G_ψ . Choose a nonzero polynomial P with integer coefficients vanishing to sufficiently high order at all these j -values. Then $P(j)u_x$ and $P(j)u_y$ are holomorphic on $\mathfrak{H}$, and for a sufficiently large positive integer s , the functions

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

are holomorphic at every cusp as well, because Δ vanishes at every cusp. They are modular forms of weight $12s$ for G_ψ , and their expansions at ∞ lie in $\mathbb{Z}[[q]]$ by (1.1), since $\Delta \in q\mathbb{Z}[[q]]$ and $j \in q^{-1}\mathbb{Z}[[q]]$.

By the unbounded denominators theorem [CDT25, Thm. 1.0.1], recalled in (R3), F_x and F_y are modular for congruence subgroups C_x and C_y , a priori unrelated to G_ψ . 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 $E(\mathbb{C}) \setminus \{0\}$, so $\psi \circ \gamma = \psi$ for $\gamma \in C_x \cap C_y$ on the complement of a discrete set, hence everywhere. Choose $M_1 \geq 1$ with $\Gamma(M_1) \subseteq C_x \cap C_y$. Then

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

so G_ψ is a congruence subgroup. $\square$

4.2.2. From cusp widths to the level.

Proposition 4.4. $\Gamma_1^\pm(N) \subseteq G_\psi \subseteq \Gamma$.

Proof. Every group between $\Gamma_1^\pm(N)$ and $\Gamma_0(N)$ contains $\Gamma(N)$, so all its cusp widths divide N ; the cusp 0 has width exactly N for $\Gamma_0(N)$ and for $\Gamma_1^\pm(N)$, since $\begin{pmatrix} 1 & 0 \\ -w & 1 \end{pmatrix} \in \Gamma_0(N)$ if and only if $N \mid w$. Thus $L(\Gamma) = N$, and $L(G_\psi) = N$ by Corollary 4.2. Since G_ψ is a congruence subgroup containing $-I$ (Lemma 4.1 and Proposition 4.3), Wohlfahrt's theorem (R4) 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 $\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}/N\mathbb{Z}\}$, which is generated by the image of T . Hence

$$\Gamma_1^\pm(N) = \langle \pm\Gamma(N), T \rangle \subseteq G_\psi \subseteq \Gamma. \quad \square$$

Lemma 4.1 and Propositions 4.3 and 4.4 prove parts (i) and (ii) of Theorem 1.3.

4.3. Descent and rational translations. The level calculation gives an algebraic lift over $\mathbb{C}$. Its normalization at the rational cusp determines a Galois-stable graph, which is the reason the lift descends to $\mathbb{Q}$. We then evaluate diamond translations at that same cusp to see that they are rational.

Proposition 4.5. *There is a unique morphism $\psi_\mu : X_\mu(N) \rightarrow E$ over $\mathbb{Q}$ with $\psi_\mu(\infty) = 0$ and $[m] \circ \psi_\mu = \varphi \circ \varpi_\Gamma$. Its analytification is induced by ψ through the uniformization of §2.1.*

Proof. Since $\Gamma_1^\pm(N) \subseteq G_\psi$, the function ψ is invariant under $\Gamma_1^\pm(N)$ and defines a holomorphic map $X_\mu(N)(\mathbb{C}) \rightarrow E(\mathbb{C})$, which extends over the cusps by §4.1. By GAGA it is algebraic; call it ψ_μ . It satisfies

$$[m]\psi_\mu = \varphi \circ \varpi_\Gamma$$

and $\psi_\mu(\infty) = 0$.

The cover

$$\mathcal{Z} = X_\mu(N) \times_{\varphi \circ \varpi_\Gamma, E, [m]} E$$

is finite étale over $X_\mu(N)$ and defined over $\mathbb{Q}$, and $(\infty, 0) \in \mathcal{Z}(\mathbb{Q})$. The graph of ψ_μ is a connected component of $\mathcal{Z}_{\overline{\mathbb{Q}}}$: it is closed, and open because $\mathcal{Z} \rightarrow X_\mu(N)$ is étale and the graph maps isomorphically to $X_\mu(N)$. It contains $(\infty, 0)$.

Distinct geometric components are disjoint and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ fixes $(\infty, 0)$, so the graph is Galois-stable and descends to a closed subscheme of $\mathcal{Z}$ mapping isomorphically to $X_\mu(N)$. Hence ψ_μ is defined over $\mathbb{Q}$.

It is unique: two morphisms with these properties differ by a morphism from the geometrically connected curve $X_\mu(N)$ to $E[m]$ vanishing at ∞ . $\square$

Proposition 4.6. *For $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$ whose class lies in Δ_Γ , there is a point $\tau_\delta \in E(\mathbb{Q})$, depending only on the class of δ in Δ_Γ because $\langle -1 \rangle$ is the identity, with*

$$(4.2) \quad \psi_\mu \circ \langle \delta \rangle = \psi_\mu + \tau_\delta, \quad \tau_\delta = \psi_\mu(\langle \delta \rangle \infty).$$

If $\gamma = \begin{pmatrix} a & b \\ Nr & d \end{pmatrix} \in \Gamma$, then $\rho(\gamma) = \tau_d$. Hence $H = \{\tau_\delta : \delta \in \Delta_\Gamma\} \subseteq E(\mathbb{Q})$.

Proof. Since $\langle \delta \rangle$ lies in Δ_Γ , we have $\varpi_\Gamma \circ \langle \delta \rangle = \varpi_\Gamma$, so $\psi_\mu \circ \langle \delta \rangle - \psi_\mu$ takes values in $E[m]$. As $X_\mu(N)$ is geometrically connected, this difference is constant, equal to its value $\psi_\mu(\langle \delta \rangle \infty)$ at ∞ , which is a rational point because ψ_μ , $\langle \delta \rangle$ and ∞ are defined over $\mathbb{Q}$. The matrix γ acts on $X_\mu(N)(\mathbb{C})$ as $\langle d \rangle$ (§2.1), so $\rho(\gamma) = \psi(\gamma z) - \psi(z) = \tau_d$. $\square$

Proof of Theorem 1.3(iii). The first assertions are Lemma 4.1 and Propositions 4.5 and 4.6. The component Y_ψ of Lemma 4.1 is the image of $X_\mu(N)$ 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 $X_\Gamma \times_{\varphi, E, [m]} E$. The automorphisms of $Y_\psi^\mathbb{Q}$ over X_Γ are the translations by elements of $E[m]$ preserving it, and over $\mathbb{C}$ these are the translations by the points of H , which are rational; so the automorphism group scheme is the constant group H . Finally, ρ kills $\Gamma_1^\pm(N)$ and the parabolic and elliptic elements of Γ by Lemma 4.1 and Proposition 4.4, so $H = \rho(\Gamma)$ is a quotient of Γ/Γ' . $\square$

4.4. Optimal parametrizations. Descent has identified the monodromy as rational torsion. Optimality now ensures that this monodromy is the entire group $E[m]$.

Proof of Theorem 1.3(iv). Let $\Gamma = \Gamma_0(N)$ and let $\varphi = \varphi_0$ come from an optimal quotient π_0 . Because $\ker \pi_0$ is connected, the homotopy sequence of $0 \rightarrow \ker \pi_0 \rightarrow J_0(N) \rightarrow E \rightarrow 0$ shows that $H_1(J_0(N)(\mathbb{C}), \mathbb{Z}) \rightarrow H_1(E(\mathbb{C}), \mathbb{Z})$ is surjective; through the Abel–Jacobi map, so is

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

The covering $Y \rightarrow X$ is the pullback along φ_0 of the covering $[m] : E(\mathbb{C}) \rightarrow E(\mathbb{C})$, whose deck group is $E[m] \cong H_1(E(\mathbb{C}), \mathbb{Z})/mH_1(E(\mathbb{C}), \mathbb{Z})$. Hence the monodromy of $Y \rightarrow X$ along a loop ℓ in X avoiding the cusps and elliptic points is translation by the class of $\varphi_{0*}[\ell]$ in $E[m]$. Every such loop is the image of a path from z_0 to γz_0 in $\mathfrak{H}$ for some $\gamma \in \Gamma_0(N)$, with monodromy $\rho(\gamma)$, and such loops generate $H_1(X_0(N)(\mathbb{C}), \mathbb{Z})$. Therefore $H = \rho(\Gamma_0(N))$ is the image of $H_1(X_0(N)(\mathbb{C}), \mathbb{Z})$ in $E[m]$, which is all of $E[m]$ by surjectivity of φ_{0*} . Together with Proposition 4.6 this gives $E[m] = H \subseteq E(\mathbb{Q})$. $\square$

Remark 4.7 (Lifts through isogenies). The same proof applies to a normalized lift through an isogeny $\nu : E' \rightarrow E$ over $\mathbb{Q}$. Use the coordinate functions of a global minimal integral equation of E' and replace $E[m]$ by $\ker \nu$. The formal expansion of ν has a nonzero rational linear coefficient, so the normalization and rational expansions are obtained just as in Lemma 3.1. The pullback is again finite étale, and the congruence and level arguments are unchanged.

In particular, if the coordinate expansions of the normalized lift have bounded denominators, Proposition 4.5 gives a unique morphism $\psi_\mu : X_\mu(N) \rightarrow E'$ over $\mathbb{Q}$ with

$$\psi_\mu(\infty) = 0, \quad \nu \circ \psi_\mu = \varphi \circ \varpi_\Gamma.$$

This is the form used for the étale isogeny in §5.2. The graph argument and rational-translation argument prove all of Theorem 1.3(i)–(iii) in this setting. For an optimal φ_0 , the last step uses the quotient $H_1(E(\mathbb{C}), \mathbb{Z})/\nu_* H_1(E'(\mathbb{C}), \mathbb{Z}) \simeq \ker \nu$ in place of $H_1(E(\mathbb{C}), \mathbb{Z})/mH_1(E(\mathbb{C}), \mathbb{Z})$, and gives $H = \ker \nu$ as well.

Remark 4.8 (The Shimura subgroup). Part (iv) can be refined; this is not used below. Let $\pi_1 : J_1(N) \twoheadrightarrow E_1$ and $\varphi_1 : X_\mu(N) \rightarrow E_1$ be the optimal $X_1(N)$ -quotient and parametrization for the newform of E , based at ∞ . Let $e : E_1 \rightarrow E$ be the isogeny with $\pi_0 \circ \varpi_* = e \circ \pi_1$ [Čes18, Lemma 2.12], so that $\varphi_0 \circ \varpi = e \circ \varphi_1$. The diamond translations of φ_1 form $\ker e$.

Indeed, let Θ be the group they form. It lies in $\ker e$ because $e\varphi_1$ is diamond invariant. The composite of φ_1 with $E_1 \rightarrow E_1/\Theta$ descends to a based map $h_0 : X_0(N) \rightarrow E_1/\Theta$, and the isogeny $\lambda : E_1/\Theta \rightarrow E$ induced by e satisfies $\lambda h_0 = \varphi_0$. On Jacobians $\lambda h_{0*} = \pi_0$, and Lemma 2.1 gives $h_{0*} = u\pi_0$ with $\lambda u = \text{id}_E$; hence λ is an isomorphism and $\Theta = \ker e$.

Moreover $(\ker e)^D$ is a subgroup of the Shimura subgroup $\Sigma(N) = \ker(J_0(N) \rightarrow J_1(N))$ [Čes18, proof of Lemma 2.12].

In the situation of (iv), the Jacobian map of ψ_μ kills $\ker \pi_1$, because $\ker \pi_1$ has no quotient isogenous to E by multiplicity one, so $\psi_\mu = \beta \circ \varphi_1$ for an isogeny $\beta : E_1 \rightarrow E$ with $[m]\beta = e$. Then $H = \beta(\ker e)$ and $H^D \hookrightarrow (\ker e)^D \subseteq \Sigma(N)$.

5. APPLICATIONS

We apply the lifting principle twice. For the Manin constant conjecture, integrality gives rational torsion, and the Igusa argument places that torsion in the identity component of the local Néron model. For Stevens' conjectures, the étale isogeny and $c_1 = \pm 1$ give integral coordinate expansions for the normalized lift; descent and optimality then yield $E_1 \simeq E_{\min}$.

5.1. Proof of the Manin constant conjecture. Let E , π_0 and φ_0 be as in Theorem 1.1, with ω_E as in §2.1, and replace π_0 by $-\pi_0$ if necessary so that $c := c_E > 0$. By the support statement (R1), $c \in \mathbb{Z}$ and $p^2 \mid N$ for every prime $p \mid c$.

5.1.1. Reduction to rational torsion. Proposition 3.6, applied to $V = X_0(N)$, shows that the normalized lift of φ_0 through $[c]$ has integral coordinate q -expansions. By Theorem 1.3(iii),(iv) with $\Gamma = \Gamma_0(N)$ and $m = c$, we obtain a morphism $\psi_\mu : X_\mu(N) \rightarrow E$ over $\mathbb{Q}$ with

$$(5.1) \quad \begin{aligned} [c] \circ \psi_\mu &= \varphi_0 \circ \varpi, & \psi_\mu \circ \langle \delta \rangle &= \psi_\mu + \tau_\delta, \\ \{\tau_\delta : \delta \in (\mathbb{Z}/N\mathbb{Z})^\times\} &= E[c] \subseteq E(\mathbb{Q}). \end{aligned}$$

Remark 5.1. Since $E[c] \subseteq E(\mathbb{Q})$, the Weil pairing shows $\mu_c \subseteq \mathbb{Q}$, so already $c \mid 2$. Thus Proposition 3.6 and Theorem 1.3 prove Theorem 1.1 at all odd primes, and the Igusa argument below is needed only to exclude $c = 2$, that is, an optimal curve with additive reduction at 2 whose full 2-torsion is rational. The argument is nevertheless uniform in p and does not use this observation.

Remark 5.2. The exclusion of the case $c = 2$ also admits an argument using the Shimura subgroup, quadratic twists, rational 2-isogenies, and arithmetic cusp fibres. The local analysis reduces to $N = 32M$, with M odd and squarefree, and reduction of type III at 2. In this case E has no point of order 4 over an unramified extension of $\mathbb{Q}_2$. The division fibres above $w_p(\infty)$, for odd $p \mid M$, then force all odd diamond factors to vanish. Consequently $E[2]$ would be a quotient of the cyclic group $(\mathbb{Z}/32\mathbb{Z})^\times / \langle -1 \rangle$, a contradiction.

5.1.2. The Igusa scheme. To control these rational translations at primes of bad reduction, we construct a smooth scheme with connected special fibre on which the diamond operators act. Fix a prime $p \mid N$ and write $N = p^a M$ with $p \nmid M$. Choose an integer $n \geq 3$ with $p \nmid n$ and $M \mid n$, an integer $f_0 \geq 1$ with $p^{f_0} \equiv 1 \pmod{n}$, and put $R = W(\mathbb{F}_{p^{f_0}})$, a finite étale extension of $\mathbb{Z}_p$ with fraction field $K = R[1/p]$. Fix a primitive n -th root of unity $\zeta \in R$.

Let $B = B_n$ be the moduli scheme over R of elliptic curves $\mathcal{A}$ with a basis (P_1, P_2) of $\mathcal{A}[n]$ such that $e_n(P_1, P_2) = \zeta$, let $\mathcal{A} \rightarrow B$ be the universal curve, and let $B^{\text{ord}} \subseteq B$ be the complement of the supersingular points of the special fibre. Thus B is the component of $M_n \otimes_{\mathbb{Z}[1/n]} R$ on which the Weil pairing has value ζ ; in particular, it is smooth affine over R [Kat73, §1.4, pp. 81–82]. Writing $q = p^{f_0}$, its special fibre is the curve $B_{n, \mathbb{F}_q}$ of (R5), with the root of unity there taken to be the reduction of ζ . Moreover, for every $m \geq 1$,

$$B^{\text{ord}} \times_R W_m(\mathbb{F}_q) \simeq S_m^\zeta$$

in Katz's notation [Kat73, §4.2.0, p. 146]. Consequently, we have

$$B_{\mathbb{F}_p}^{\text{ord}} \simeq B_{n, \mathbb{F}_p}^{\text{ord}} \simeq S_1^\zeta \times_{\mathbb{F}_q} \overline{\mathbb{F}_p}.$$

This geometric special fibre is nonempty and connected by (R5).

The following elementary fact supplies the étaleness needed in this construction.

Lemma 5.3. *Let Z be a finite locally free commutative group scheme over a scheme T , and let Σ be a finite abelian group. The functor $T' \mapsto \text{Hom}_{T'}(Z_{T'}, \Sigma_{T'})$ of homomorphisms to the constant group scheme is represented by a scheme $\underline{\text{Hom}}(Z, \Sigma)$ which is étale over T .*

Proof. A morphism of T' -schemes $u : Z_{T'} \rightarrow \Sigma_{T'}$ is a decomposition of $Z_{T'}$ into open and closed subschemes indexed by Σ , that is, a complete system $(e_s)_{s \in \Sigma}$ of orthogonal idempotents in $\mathcal{O}(Z_{T'}) = \mathcal{O}(Z) \otimes_{\mathcal{O}_T} \mathcal{O}_{T'}$. Since $\mathcal{O}(Z)$ is a finite locally free $\mathcal{O}_T$ -module, this functor is represented by the closed subscheme of the vector bundle $\mathbb{V}(\mathcal{O}(Z))^\Sigma$ defined by $e_s^2 = e_s$, $e_s e_{s'} = 0$ for $s \neq s'$, and $\sum_s e_s = 1$; it is of finite presentation over T . It is formally étale, because a complete system of orthogonal idempotents lifts uniquely along a nilpotent thickening of rings: existence is standard, and for uniqueness note that two commuting idempotents e, e' satisfy $(e - e')^3 = e - e'$, so if $e - e'$ is nilpotent then $e = e'$. A morphism locally of finite presentation which is formally étale is étale [BLR90, §2.2, Prop. 6].

Let M be the étale T -scheme just constructed, with universal morphism $u : Z_M \rightarrow \Sigma_M$. The subfunctor of homomorphisms is represented by the locus in M over which the two morphisms $Z_M \times_M Z_M \rightarrow \Sigma_M$ given by $(g, h) \mapsto u(g + h)$ and $(g, h) \mapsto u(g) + u(h)$ agree. Two morphisms from a scheme to an étale separated scheme agree on an open and closed subscheme, and since $Z_M \times_M Z_M \rightarrow M$ is finite locally free, hence open and closed, the locus of points of M over which they

agree on the whole fibre is open and closed. Thus $\underline{\mathrm{Hom}}(Z, \Sigma)$ is an open and closed subscheme of the étale T -scheme M . $\square$

A homomorphism $\mu_{p^a} \rightarrow \mathcal{A}[p^a]$ over a B^{ord} -scheme corresponds by Cartier duality to a homomorphism $\mathcal{A}[p^a]^D \rightarrow (\mu_{p^a})^D = \mathbb{Z}/p^a\mathbb{Z}$. By Lemma 5.3, these homomorphisms are represented by a scheme

$$\mathcal{H} = \underline{\mathrm{Hom}}(\mathcal{A}[p^a]^D, \mathbb{Z}/p^a\mathbb{Z})$$

which is étale over B^{ord} . A homomorphism $\mu_{p^a} \rightarrow \mathcal{A}[p^a]$ is a closed immersion exactly when the corresponding map of finite locally free algebras is surjective; since the cokernel is a finitely generated module, this is an open condition. Let $S \subseteq \mathcal{H}$ be the open subscheme of closed immersions.

Lemma 5.4. (a) *The morphism $S \rightarrow B^{\mathrm{ord}}$ is étale. In particular S is smooth over R , and its generic fibre is schematically dense.*

(b) *Over the ordinary locus of the special fibre, every closed immersion $\mu_{p^a} \hookrightarrow \mathcal{A}[p^a]$ is an isomorphism onto the connected part $\mathcal{A}[p^a]^0 = \ker(F^a)$, and*

$$S_{\mathbb{F}_p} \simeq \mathrm{Isom}(\mathbb{Z}/p^a\mathbb{Z}, \mathcal{A}[p^a]^{\mathrm{ét}}),$$

the scheme of generators of the étale quotient of $\mathcal{A}[p^a]$ over $B_{\mathbb{F}_p}^{\mathrm{ord}}$. It is nonempty and connected.

Proof. **Proof of (a).** The morphism $S \rightarrow B^{\mathrm{ord}}$ is an open subscheme of the étale morphism $\mathcal{H} \rightarrow B^{\mathrm{ord}}$, hence étale. Since B^{ord} is smooth over R , so is S ; in particular S is flat over the discrete valuation ring R , so $\mathcal{O}_S$ has no p -torsion and the generic fibre is schematically dense.

Proof of (b). Let T be a scheme over $B_{\mathbb{F}_p}^{\mathrm{ord}}$. Over T the group $\mathcal{A}[p^a]$ is an extension

$$0 \rightarrow \mathcal{A}[p^a]^0 \rightarrow \mathcal{A}[p^a] \rightarrow \mathcal{A}[p^a]^{\mathrm{ét}} \rightarrow 0$$

of an étale group of rank p^a by the connected group $\mathcal{A}[p^a]^0 = \ker(F^a)$ of rank p^a , where $F : \mathcal{A} \rightarrow \mathcal{A}^{(p)}$ is the relative Frobenius. The scheme $\mu_{p^a, T}$ is a nilpotent thickening of T along its identity section, so every homomorphism $\mu_{p^a, T} \rightarrow \mathcal{A}[p^a]^{\mathrm{ét}}_T$ is determined by its restriction to the identity section and is therefore trivial. Hence every homomorphism $\mu_{p^a, T} \rightarrow \mathcal{A}[p^a]_T$ factors through $\mathcal{A}[p^a]^0$, and a closed immersion between finite locally free group schemes of the same rank is an isomorphism. By Cartier duality,

$$S_{\mathbb{F}_p} = \mathrm{Isom}(\mu_{p^a}, \mathcal{A}[p^a]^0) = \mathrm{Isom}((\mathcal{A}[p^a]^0)^D, \mathbb{Z}/p^a\mathbb{Z}).$$

Cartier duality interchanges Frobenius and Verschiebung, so $(\mathcal{A}[p^a]^0)^D = (\ker F^a)^D$ is isomorphic to $\ker(V^a : \mathcal{A}^{(p^a)} \rightarrow \mathcal{A})$, which is étale because V is étale on the ordinary locus. The Weil pairing $\mathcal{A}[p^a] \times \mathcal{A}[p^a] \rightarrow \mu_{p^a}$ is perfect, and its restriction to $\mathcal{A}[p^a]^0 \times \mathcal{A}[p^a]^0$ vanishes, being a homomorphism from the connected group $\mathcal{A}[p^a]^0$ to the étale group $(\mathcal{A}[p^a]^0)^D$. Hence it identifies $(\mathcal{A}[p^a]^0)^D$ with $\mathcal{A}[p^a]^{\mathrm{ét}}$, and $S_{\mathbb{F}_p}$ with the scheme of isomorphisms $\mathbb{Z}/p^a\mathbb{Z} \simeq \mathcal{A}[p^a]^{\mathrm{ét}}$, that is, of generators of $\mathcal{A}[p^a]^{\mathrm{ét}}$.

The a -th power of Frobenius identifies $\mathcal{A}[p^a]^{\mathrm{ét}} = \mathcal{A}[p^a]/\ker(F^a)$ with $\ker(V^a : \mathcal{A}^{(p^a)} \rightarrow \mathcal{A})$, since $V^a F^a = p^a$. By Igusa's theorem (R5), the fundamental group of $B_{\mathbb{F}_p}^{\mathrm{ord}}$ acts on the generators of this kernel through a surjection onto $(\mathbb{Z}/p^a\mathbb{Z})^\times$. The

scheme of generators is finite étale over the connected scheme $B_{\mathbb{F}_p}^{\text{ord}}$ with transitive monodromy on each fibre, hence connected. It is nonempty because $B_{\mathbb{F}_p}^{\text{ord}}$ is. $\square$

Remark 5.5. The special fibre of S is the Igusa curve of level p^a over the ordinary locus, and Lemma 5.4(b) is Igusa's irreducibility theorem; see [KM85, Ch. 12].

5.1.3. *Diamond operators and the identity component.* Each diamond operator lifts to an automorphism of S . Compatibility with translation by τ_δ and connectedness of the special fibre then imply that τ_δ reduces to the identity component of the Néron model.

For a point (A, P_1, P_2, ι) of S over a K -scheme, let $\iota_M : \mu_M \hookrightarrow A[M]$ send $\zeta^{n/M}$ to $(n/M)P_1$, and let $\iota_M \times \iota : \mu_N = \mu_M \times \mu_{p^a} \hookrightarrow A[N]$. Since $(n/M)P_1$ has exact order M and μ_M is constant over R , this is a closed immersion, and we obtain a morphism

$$j : S_K \longrightarrow X_\mu(N)_K.$$

For $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$ choose any $v \in (\mathbb{Z}/n\mathbb{Z})^\times$ with $v \equiv \delta \pmod{M}$, and let

$$(5.2) \quad \tilde{\delta} : (A, P_1, P_2, \iota) \longmapsto (A, vP_1, v^{-1}P_2, \iota \circ [\delta]).$$

This preserves $e_n(P_1, P_2)$ and closed immersions, so it is an automorphism of S over R , and $j \circ \tilde{\delta} = \langle \delta \rangle \circ j$, since $(n/M)vP_1 = \delta \cdot (n/M)P_1$.

Proposition 5.6. *Let $p \mid N$, with the notation of §5.1.2. For every $\delta \in (\mathbb{Z}/N\mathbb{Z})^\times$, the point τ_δ of (5.1) lies in $E^0(\mathbb{Q}_p)$. Hence $E[c] \subseteq E^0(\mathbb{Q}_p)$.*

Proof. Let $\mathcal{E}_R = \mathcal{E} \otimes_{\mathbb{Z}_p} R$; it is the Néron model of E_K over R because $\mathbb{Z}_p \rightarrow R$ is étale (§2.1). Since S is smooth over R (Lemma 5.4(a)), the Néron mapping property extends

$$\psi_\mu \circ j : S_K \longrightarrow E_K$$

to a morphism $\Phi : S \rightarrow \mathcal{E}_R$. The rational point τ_δ extends to a section $\bar{\tau}_\delta \in \mathcal{E}_R(R)$. By (5.1) and $j \circ \tilde{\delta} = \langle \delta \rangle \circ j$, we have $\Phi \circ \tilde{\delta} = \Phi + \bar{\tau}_\delta$ on the generic fibre of S ; since $\mathcal{E}_R$ is separated and the generic fibre of S is schematically dense, the identity holds on S .

By Lemma 5.4(b) the special fibre $S_{\mathbb{F}_p}$ is nonempty and connected, so $\Phi(S_{\mathbb{F}_p})$ lies in a single connected component $\mathcal{K}$ of $\mathcal{E}_{\mathbb{F}_p}^0$. The automorphism $\tilde{\delta}$ preserves $S_{\mathbb{F}_p}$. For a point $\xi \in S(\mathbb{F}_p)$, both $\Phi(\xi)$ and $\Phi(\tilde{\delta}\xi) = \Phi(\xi) + \bar{\tau}_\delta$ lie in $\mathcal{K}$, so the reduction of τ_δ lies in the identity component $\mathcal{E}_{\mathbb{F}_p}^0$. Since the identity component of a group scheme of finite type over a field is geometrically connected, $\mathcal{E}_{\mathbb{F}_p}^0 = (\mathcal{E}_{\mathbb{F}_p}^0)_{\mathbb{F}_p}$, and as the reduction of τ_δ is an $\mathbb{F}_p$ -point, it lies in $\mathcal{E}^0(\mathbb{F}_p)$, so $\tau_\delta \in E^0(\mathbb{Q}_p)$. The last assertion follows from (5.1). $\square$

5.1.4. *The local torsion bound and conclusion.* It remains to compare the full p -torsion supplied by optimality with the torsion allowed in the identity component at an additive prime.

Lemma 5.7. *If E is an elliptic curve over $\mathbb{Q}_p$ with additive reduction, then*

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

Proof. Reduction gives $E^0(\mathbb{Q}_p)/\widehat{E}(p\mathbb{Z}_p) \simeq \mathbb{G}_a(\mathbb{F}_p)$ [Sil09, Props. VII.2.1, VII.2.2 and VII.5.1(c)]. Since the reduction of $\widehat{E}$ is additive, $[p]_{\widehat{E}}(T) = pT(1 + Th(T))$ for some $h \in \mathbb{Z}_p[[T]]$. For $0 \neq t \in p\mathbb{Z}_p$, the factor $1 + th(t)$ is a unit, so $[p]_{\widehat{E}}(t) \neq 0$, including when $p = 2$. Thus reduction injects $E^0(\mathbb{Q}_p)[p]$ into $\mathbb{G}_a(\mathbb{F}_p)$, which has order p . $\square$

Proof of Theorem 1.1. Suppose that a prime p divides c . Then $p^2 \mid N$, so E has additive reduction at p . By (5.1) and Proposition 5.6,

$$E[p] \subseteq E[c] \subseteq E^0(\mathbb{Q}_p),$$

so $E^0(\mathbb{Q}_p)[p]$ has p^2 elements, contradicting Lemma 5.7. Hence $c = 1$ and $c_E = \pm 1$. $\square$

5.2. Proof of Stevens' conjectures. Let $\mathcal{C}$ be an isogeny class of conductor N with newform f , and let $\pi_1, \varphi_1, E_1, c_1$ and $E_{\min}$ be as in §1.1. By §2.1 we regard φ_1 as a morphism $X_\mu(N) \rightarrow E_1$ over $\mathbb{Q}$ with $\varphi_1(\infty) = 0$ satisfying (2.1).

5.2.1. The constant. The following comparison shows that $c_1 \mid c_E$, so Theorem 1.1 gives $c_1 = \pm 1$.

Lemma 5.8 ([Čes18, Lemma 2.12]). *Let $\pi_0 : J_0(N) \rightarrow E$ be the optimal quotient attached to f . Then c_1 divides c_E .*

Proof. The homomorphism $\pi_0 \circ \varpi_* : J_1(N) \rightarrow E$, where $\varpi_* : J_1(N) \rightarrow J_0(N)$ is induced by ϖ , kills $\ker \pi_1$, because $\ker \pi_1$ has no quotient isogenous to E by multiplicity one; it is nonzero because $\pi_0 \circ \varpi_* \circ \varpi^* = \deg(\varpi) \pi_0$. Hence $\pi_0 \circ \varpi_* = e \circ \pi_1$ for an isogeny $e : E_1 \rightarrow E$, and $\varphi_0 \circ \varpi = e \circ \varphi_1$ as based morphisms $X_\mu(N) \rightarrow E$. The isogeny e extends to a morphism of Néron models over $\mathbb{Z}_p$ for every p , so $e^* \omega_E = d \omega_{E_1}$ with $d \in \mathbb{Z}$. Since $\varpi^* \omega_f = \omega_f$, we get

$$c_E \omega_f = \varpi^* \varphi_0^* \omega_E = \varphi_1^* e^* \omega_E = d \varphi_1^* \omega_{E_1} = d \varepsilon_N c_1 \omega_f$$

by (2.1), so $c_E = \pm d c_1$. $\square$

By Lemma 5.8 and Theorem 1.1, $c_1 = \pm 1$, which is the first assertion of Theorem 1.2. We choose the sign of φ_1 so that, in the coordinate of (2.1),

$$(5.3) \quad \varphi_1^* \omega_{E_1} = f(q) \frac{dq}{q}.$$

5.2.2. The minimal curve.

Proof of Theorem 1.2. It remains to prove $E_1 \simeq E_{\min}$. By Stevens' theorem (R6) there is an étale isogeny $\alpha : E_{\min} \rightarrow E_1$, and $\alpha^* \omega_{E_1} = \pm \omega_{E_{\min}}$ for the differentials of §2.1; replace α by $-\alpha$ if necessary so that $\alpha^* \omega_{E_1} = \omega_{E_{\min}}$.

Step 1: integrality of the normalized lift through α . The isogeny α extends to a morphism of Néron models over $\mathbb{Z}_p$ for every prime p , preserving the zero sections, so its expansion in the formal parameters of minimal equations of $E_{\min}$ and E_1 satisfies

$$\widehat{\alpha}(w) \in w + w^2 \mathbb{Z}[[w]],$$

the linear coefficient being 1 by the normalization of α . Its compositional inverse is integral by Lemma 3.2. Let $\psi' : \mathfrak{H} \rightarrow E_{\min}(\mathbb{C})$ be the normalized lift of φ_1

through α . By Lemma 3.5, $t_{\varphi_1} \in q\mathbb{Z}[[q]]$, with linear coefficient 1 because (5.3) gives $dL_{E_1}(t_{\varphi_1}) = (1 + O(q))dq$. Hence

$$t_{\psi'} = \hat{\alpha}^{-1}(t_{\varphi_1}) \in q\mathbb{Z}[[q]],$$

and the coordinates of a minimal equation of $E_{\min}$ along ψ' lie in $\mathbb{Z}((q))$. Thus the coordinate q -expansions of ψ' satisfy the bounded denominators hypothesis with $k = 1$.

Step 2: descent and optimality. By the isogeny variant in Remark 4.7 and Proposition 4.5, with $\Gamma = \Gamma_1^\pm(N)$, $\varphi = \varphi_1$ and $\nu = \alpha$, the normalized lift ψ' descends to a morphism $h' : X_\mu(N) \rightarrow E_{\min}$ over $\mathbb{Q}$ with $\alpha \circ h' = \varphi_1$. On Jacobians, $\alpha \circ h'_* = \pi_1$, so $h'_*(\ker \pi_1) \subseteq \ker \alpha$ is finite, and Lemma 2.1 with $\pi = \pi_1$, $g = h'$ and $\lambda = \alpha$ shows that α is an isomorphism. Hence $E_{\min} \simeq E_1$. $\square$

Remark 5.9. The assumption that E is an elliptic curve is used in Proposition 4.3, where x, y separate points of $E(\mathbb{C}) \setminus \{0\}$, and in the local arguments of Lemmas 3.4 and 5.7.

For an abelian variety, one could instead impose bounded denominators on the compositions of the lift with finitely many rational functions that separate points on an open subset met by the lift. In Proposition 3.6, the differential identity is combined with the integrality of the formal logarithm at primes of additive reduction.

The natural analogues of the Manin constant conjecture for higher-dimensional optimal quotients fail in general [Čes18, Thm. 5.10].

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 $c_E \mid 2$.

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 conjecture. 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 history, 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 possibility.
- (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.
- [Kat73] N. M. Katz, *p-adic properties of modular schemes and modular forms*, in *Modular functions of one variable III (Antwerp, 1972)*, Lecture Notes in Math. **350**, Springer, Berlin, 1973, 69–190.
- [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.
- [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*, preprint (2026).
- [OSVerify26] F. Nie, H. Ye, S. Liu, Z. Wang, S. Ermon and J. Zou, *One-sided verification under limited expert review*, in submission (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*, preprint (2026).

Email address: znchi@zju.edu.cn

Email address: srlu@stanford.edu

Email address: ping.nie@pku.edu.cn