EXPLICIT ESTIMATES IN INTER-UNIVERSAL TEICHMÜLLER THEORY

SHINICHI MOCHIZUKI, IVAN FESENKO, YUICHIRO HOSHI, ARATA MINAMIDE, AND WOJCIECH POROWSKI

Abstract. In the final paper of a series of papers concerning *inter-universal Teichmüller theory*, Mochizuki verified various *numerically non-effective versions* of the *Vojta, ABC, and Szpiro Conjectures* over number fields. In the present paper, we obtain various *numerically effective versions* of Mochizuki's results. In order to obtain these results, we first establish a version of the theory of *étale theta functions* that functions properly at *arbitrary* bad places, i.e., *even bad places that divide the prime "2"*. We then proceed to discuss how such a modified version of the theory of étale theta functions affects inter-universal Teichmüller theory. Finally, by applying our *slightly modified version* of inter-universal Teichmüller theory, together with various *explicit estimates* concerning *heights*, the *j-invariants* of "*arithmetic*" elliptic curves, and the *prime number theorem*, we verify the *numerically effective versions* of Mochizuki's results referred to above. These numerically effective versions imply *effective diophantine results* such as an *effective version of the ABC inequality over mono-complex number fields* [i.e., the rational number field or an imaginary quadratic field] and *effective versions of conjectures of Szpiro*. We also obtain an *explicit estimate* concerning "*Fermat's Last Theorem*" (FLT) — i.e., to the effect that FLT holds for *prime exponents* $> 1.615 \cdot 10^{14}$ — which is sufficient, in light of a numerical result of Coppersmith, to give an *alternative proof* of the *first case of FLT*. In the *second case of FLT*, if one combines the techniques of the present paper with a recent estimate due to Mihăilescu and Rassias, then the lower bound "$1.615 \cdot 10^{14}$" can be improved to "257". This estimate, combined with a classical result of Vandiver, yields an *alternative proof* of the *second case of FLT*. In particular, the results of the present paper, combined with the results of Vandiver, Coppersmith, and Mihăilescu-Rassias, yield an *unconditional new alternative proof* of *Fermat's Last Theorem*.

Contents

2020 *Mathematics Subject Classification.* Primary 14H25; Secondary 14H30.

Key words and phrases. inter-universal Teichmüller theory, punctured elliptic curve, number field, mono-complex, étale theta function, 6-torsion points, height, explicit estimate, effective version, diophantine inequality, ABC Conjecture, Szpiro Conjecture, Fermat's Last Theorem.

Introduction

In [IUTchIV], Mochizuki applied the theory of [IUTchI-IV] [cf. also [Alien] for a *detailed survey* of this theory] to prove the following result [cf. [IUTchIV], Corollary 2.2, (ii), (iii)]:

Theorem. *Write X for the* **projective line** *over $\mathbb{Q}$; $D \subseteq X$ for the divisor consisting of the* **three points** *"0", "1", and "∞"; $(\mathcal{M}_{\mathrm{ell}})_{\mathbb{Q}}$ for the moduli stack of elliptic curves over $\mathbb{Q}$. We shall regard X as the "λ-**line**" — i.e., we shall regard the standard coordinate on X as the "λ" in the* **Legendre form** *"$y^2 = x(x-1)(x-\lambda)$" of the Weierstrass equation defining an elliptic curve — and hence as being equipped with a natural* **classifying morphism** *$U_X \stackrel{\text{def}}{=} X \setminus D \to (\mathcal{M}_{\mathrm{ell}})_{\mathbb{Q}}$. Write*

$$\log(\mathfrak{q}_{(-)}^{\forall})$$

for the $\mathbb{R}$-valued function on $(\mathcal{M}_{\mathrm{ell}})_{\mathbb{Q}}(\overline{\mathbb{Q}})$, hence also on $U_X(\overline{\mathbb{Q}})$, obtained by forming the normalized degree "$\underline{\deg}(-)$" of the effective arithmetic divisor determined by the ***q*-parameters** *of an elliptic curve over a number field at* **arbitrary** *nonarchimedean places. Let*

$$\mathcal{K}_V \ \subseteq \ U_X(\overline{\mathbb{Q}})$$

be a **compactly bounded subset** *that satisfies the following conditions:*

(CBS1) *The support of $\mathcal{K}_V$ contains the nonarchimedean place "2".*

(CBS2) *The image of the subset "$\mathcal{K}_2 \subseteq U_X(\overline{\mathbb{Q}}_2)$" associated to $\mathcal{K}_V$ via the* ***j*-invariant** *$U_X \to (\mathcal{M}_{\mathrm{ell}})_{\mathbb{Q}} \to \mathbb{A}^1_{\mathbb{Q}}$ is a* **bounded** *subset of $\mathbb{A}^1_{\mathbb{Q}}(\overline{\mathbb{Q}}_2) = \overline{\mathbb{Q}}_2$, i.e., is contained in a subset of the form $2^{N_{j\text{-inv}}} \cdot \mathcal{O}_{\overline{\mathbb{Q}}_2} \subseteq \overline{\mathbb{Q}}_2$, where $N_{j\text{-inv}} \in \mathbb{Z}$, and $\mathcal{O}_{\overline{\mathbb{Q}}_2} \subseteq \overline{\mathbb{Q}}_2$ denotes the ring of integers [cf. the condition $(*_{j\text{-inv}})$ of* [IUTchIV]*, Corollary 2.2, (ii)].*

Then there exist

- *a positive real number H_{unif} which is* **independent** *of $\mathcal{K}_V$ and*
- *positive real numbers $C_{\mathcal{K}}$ and $H_{\mathcal{K}}$ which* **depend only** *on the choice of the* **compactly bounded subset** *$\mathcal{K}_V$*

such that the following property is satisfied: Let d be a positive integer, ϵ_d and ϵ positive real numbers ≤ 1. Then there exists a **finite** *subset*

$$\mathfrak{Exc}_{\epsilon,d} \ \subseteq \ U_X(\overline{\mathbb{Q}})^{\leq d}$$

— where we denote by $U_X(\overline{\mathbb{Q}})^{\leq d} \subseteq U_X(\overline{\mathbb{Q}})$ the subset of $\overline{\mathbb{Q}}$-rational points defined over a finite extension field of $\mathbb{Q}$ of degree $\leq d$ — which depends only on $\mathcal{K}_V$, ϵ, d, and ϵ_d, and satisfies the following properties:

- *The function* $\log(\mathfrak{q}^{\forall}_{(-)})$ *is*

$$\leq\ H_{\mathrm{unif}} \cdot \epsilon^{-3} \cdot \epsilon_d^{-3} \cdot d^{4+\epsilon_d} + H_{\mathcal{K}}$$

on $\mathfrak{Exc}_{\epsilon,d}$.

- *Let* E_F *be an* **elliptic curve** *over a number field* $F \subseteq \overline{\mathbb{Q}}$ *that determines a* $\overline{\mathbb{Q}}$*-valued point of* $(\mathcal{M}_{\mathrm{ell}})_{\mathbb{Q}}$ *which lifts [not necessarily uniquely!] to a point* $x_E \in U_X(F) \cap U_X(\overline{\mathbb{Q}})^{\leq d}$ *such that*

$$x_E\ \in\ \mathcal{K}_V,\quad x_E\ \notin\ \mathfrak{Exc}_{\epsilon,d}.$$

Write F_{mod} *for the* **minimal field of definition** *of the corresponding point* $\in (\mathcal{M}_{\mathrm{ell}})_{\mathbb{Q}}(\overline{\mathbb{Q}})$ *and*

$$F_{\mathrm{mod}}\ \subseteq\ F_{\mathrm{tpd}}\ \stackrel{\mathrm{def}}{=}\ F_{\mathrm{mod}}(E_{F_{\mathrm{mod}}}[2])\ \subseteq\ F$$

for the **"tripodal"** *intermediate field obtained from* F_{mod} *by adjoining the fields of definition of the* 2*-torsion points of any model of* $E_F \times_F \overline{\mathbb{Q}}$ *over* F_{mod} *[cf.* [IUTchIV]*, Proposition 1.8, (ii), (iii)]. Moreover, we assume that the* $(3 \cdot 5)$*-torsion points of* E_F *are defined over* F*, and that*

$$F\ =\ F_{\mathrm{mod}}(\sqrt{-1}, E_{F_{\mathrm{mod}}}[2 \cdot 3 \cdot 5])\ \stackrel{\mathrm{def}}{=}\ F_{\mathrm{tpd}}(\sqrt{-1}, E_{F_{\mathrm{tpd}}}[3 \cdot 5])$$

— i.e., that F *is obtained from* F_{tpd} *by adjoining* $\sqrt{-1}$*, together with the fields of definition of the* $(3 \cdot 5)$*-torsion points of a model* $E_{F_{\mathrm{tpd}}}$ *of the elliptic curve* $E_F \times_F \overline{\mathbb{Q}}$ *over* F_{tpd} *determined by the* **Legendre form** *of the Weierstrass equation discussed above. Then* E_F *and* F_{mod} *arise as the "*E_F*" and "*F_{mod}*" for a collection of* **initial Θ-data** *as in* [IUTchIV]*, Theorem 1.10, that satisfies the following conditions:*

(C1) $(\log(\mathfrak{q}^{\forall}_{x_E}))^{1/2}\ \leq\ l\ \leq\ 10\delta \cdot (\log(\mathfrak{q}^{\forall}_{x_E}))^{1/2} \cdot \log(2\delta \cdot \log(\mathfrak{q}^{\forall}_{x_E}))$*;*

(C2) we have an inequality

$$\tfrac{1}{6} \cdot \log(\mathfrak{q}^{\forall}_{x_E})\ \leq\ (1+\epsilon) \cdot (\text{log-diff}_X(x_E) + \text{log-cond}_D(x_E)) + C_{\mathcal{K}}$$

— where we write $\delta \stackrel{\mathrm{def}}{=} 2^{12} \cdot 3^3 \cdot 5 \cdot d$*;* log-diff_X *for the [normalized] log-different function on* $U_X(\overline{\mathbb{Q}})$ *[cf.* [GenEll]*, Definition 1.5, (iii)];* log-cond_D *for the [normalized] log-conductor function on* $U_X(\overline{\mathbb{Q}})$ *[cf.* [GenEll]*, Definition 1.5, (iv)].*

In the present paper, we prove a *numerically effective version* of this theorem *without* assuming the conditions (CBS1), (CBS2) [cf. the portion of Corollary 5.2 that concerns $\kappa/\kappa^{\log}/\mathcal{K}$]. Moreover, we prove that if one restricts one's attention to the case where the point "x_E" is defined over a *mono-complex* number field [i.e., $\mathbb{Q}$ or an imaginary quadratic field — cf. Definition 1.2], then one may *eliminate* the compactly bounded subset "$\mathcal{K}_V$" from the statement of this theorem [cf. the portion of Corollary 5.2 that does *not* concern $\kappa/\kappa^{\log}/\mathcal{K}$].

In order to obtain Corollary 5.2, we establish a version of the theory of *étale theta functions* that functions properly at *arbitrary* bad places, i.e., *even bad places that divide the prime "*2*"*. Roughly speaking, this is achieved by modifying the notion of *evaluation points* at which the theta function is evaluated [cf. the explanation of §3 below for more details].

We then proceed to apply Corollary 5.2 to verify the following *effective diophantine results* [cf. Theorems 5.3, 5.4; Remarks 5.3.3, 5.3.4, 5.3.5; Corollary 5.8; the notations and conventions of §0]:

Theorem A. (Effective versions of ABC/Szpiro inequalities over mono-complex number fields) *Let L be a* **mono-complex** *number field [i.e., $\mathbb{Q}$ or an imaginary quadratic field — cf. Definition 1.2]; a, b, $c \in L^{\times}$ nonzero elements of L such that*

$$a + b + c \;=\; 0;$$

ϵ a positive real number ≤ 1. Write $E_{a,b,c}$ for the elliptic curve over L defined by the equation $y^2 = x(x-1)(x+\frac{a}{c})$; $j(E_{a,b,c})$ for the j-invariant of $E_{a,b,c}$; Δ_L for the absolute value of the discriminant of L; $d \stackrel{\text{def}}{=} [L : \mathbb{Q}]$;

$$H_L(a,b,c) \;\stackrel{\text{def}}{=}\; \prod_{v \in \mathbb{V}(L)} \max\{|a|_v, |b|_v, |c|_v\};$$

$$I_L(a,b,c) \;\stackrel{\text{def}}{=}\; \{v \in \mathbb{V}(L)^{\text{non}} \mid \sharp\{|a|_v, |b|_v, |c|_v\} \geq 2\} \;\subseteq\; \mathbb{V}(L)^{\text{non}};$$

$$\text{rad}_L(a,b,c) \;\stackrel{\text{def}}{=}\; \prod_{v \in I_L(a,b,c)} \sharp(\mathcal{O}_L/\mathfrak{p}_v);$$

$$h_d(\epsilon) \;\stackrel{\text{def}}{=}\; \begin{cases} 3.4 \cdot 10^{30} \cdot \epsilon^{-166/81} & (d = 1) \\ 6 \cdot 10^{31} \cdot \epsilon^{-174/85} & (d = 2). \end{cases}$$

Then the following hold:

(i) *We have [cf. Definition 1.1, (i)]*

$$\begin{aligned} \tfrac{1}{6} \cdot h_{\text{non}}(j(E_{a,b,c})) &\leq \max\{\tfrac{1}{d} \cdot (1+\epsilon) \cdot \log(\Delta_L \cdot \text{rad}_L(a,b,c)), \tfrac{1}{6} \cdot h_d(\epsilon)\} \\ &\leq \tfrac{1}{d} \cdot (1+\epsilon) \cdot \log(\Delta_L \cdot \text{rad}_L(a,b,c)) + \tfrac{1}{6} \cdot h_d(\epsilon). \end{aligned}$$

(ii) *We have*

$$\begin{aligned} H_L(a,b,c) &\leq 2^{5d/2} \cdot \max\{\exp(\tfrac{d}{4} \cdot h_d(\epsilon)), (\Delta_L \cdot \text{rad}_L(a,b,c))^{3(1+\epsilon)/2}\} \\ &\leq 2^{5d/2} \cdot \exp(\tfrac{d}{4} \cdot h_d(\epsilon)) \cdot (\Delta_L \cdot \text{rad}_L(a,b,c))^{3(1+\epsilon)/2}. \end{aligned}$$

Theorem B. (Effective version of a conjecture of Szpiro) *Let a, b, c be nonzero coprime integers such that*

$$a + b + c \;=\; 0;$$

ϵ a positive real number ≤ 1. Then we have

$$\begin{aligned} |abc| &\leq 2^4 \cdot \max\{\exp(1.7 \cdot 10^{30} \cdot \epsilon^{-166/81}), (\text{rad}(abc))^{3(1+\epsilon)}\} \\ &\leq 2^4 \cdot \exp(1.7 \cdot 10^{30} \cdot \epsilon^{-166/81}) \cdot (\text{rad}(abc))^{3(1+\epsilon)} \end{aligned}$$

— which may be regarded as an explicit version of the inequality

$$\text{“}|abc| \;\leq\; C(\epsilon)\Big(\prod_{p \mid abc} p\Big)^{3+\epsilon}\text{”}$$

conjectured in [Szp], *§2 [i.e., the "forme forte" of loc. cit., where we note that the "p" to the right of the "$\prod$" in the above display was apparently unintentionally omitted in loc. cit.].*

Corollary C. (Application to "Fermat's Last Theorem") *Let*

$$p \ > \ 1.615 \cdot 10^{14}$$

be a prime number. Then there does not exist any triple (x, y, z) *of positive integers that satisfies the Fermat equation*

$$x^p + y^p \ = \ z^p.$$

The proof of Corollary C is obtained by combining

- the slightly modified version of [IUTchI-IV] developed in the present paper with
- various estimates [cf. Lemmas 5.5, 5.6, 5.7] of an *entirely elementary nature*.

In fact, the lower bound of Corollary C may be strengthened roughly by a factor of 2 by applying the results of [Ink1], [Ink2] [cf. Remarks 5.7.1, 5.8.2], which are obtained by means of techniques of classical algebraic number theory that are somewhat more involved than the argument applied in the corresponding portion of the proof of Corollary C. The original estimate of Corollary C is sufficient, in light of a numerical result of Coppersmith, to give an *alternative proof* [i.e., to the proof of [Wls]] of the *first case of Fermat's Last Theorem* [cf. Remark 5.8.1]. In the *second case of Fermat's Last Theorem*, if one combines the techniques of the present paper with a recent estimate due to Mihăilescu and Rassias, then the lower bound "$1.615 \cdot 10^{14}$" of Corollary C can be improved to "257" [cf. Remark 5.8.3, (i)]. This estimate, combined with a classical result of Vandiver, yields an *alternative proof* [i.e., to the proof of [Wls]] of the *second case of Fermat's Last Theorem* [cf. Remark 5.8.3, (ii)]. In particular,

> the results of the present paper, combined with the results of Vandiver, Coppersmith, and Mihăilescu-Rassias, yield an **unconditional new alternative proof** [i.e., to the proof of [Wls]] of **Fermat's Last Theorem**.

[The authors have received informal reports to the effect that one mathematician has obtained some sort of numerical estimate that is formally similar to Corollary C, but with a *substantially weaker* [by many orders of magnitude!] lower bound for p, by combining the techniques of [IUTchIV], §1, §2, with effective computations concerning Belyi maps. On the other hand, the authors have not been able to find any detailed written exposition of this informally advertized numerical estimate and are not in a position to comment on it.]

We also obtain an application of the *ABC inequality* of Theorem B to a *generalized version of Fermat's Last Theorem* [cf. Corollary 5.9], which does *not* appear to be *accessible* via the techniques involving *modularity* of

elliptic curves over $\mathbb{Q}$ and *deformations of Galois representations* that play a central role in [Wls].

In the following, we explain the content of each section of the present paper in greater detail.

In §1, we examine various [elementary and essentially well-known] properties of *heights of elliptic curves over number fields*. Let $F \subseteq \overline{\mathbb{Q}}$ be a number field; E an elliptic curve over F that has *semi-stable reduction* over the ring of integers $\mathcal{O}_F$ of F. Suppose that E is isomorphic over $\overline{\mathbb{Q}}$ to the elliptic curve defined by an equation

$$y^2 \ = \ x(x-1)(x-\lambda)$$

— where $\lambda \in \overline{\mathbb{Q}} \setminus \{0, 1\}$. For simplicity, assume further that

$$\mathbb{Q}(\lambda) \text{ is } \textit{mono-complex}$$

[i.e., $\mathbb{Q}$ or an imaginary quadratic field — cf. Definition 1.2]. Write $j(E) \in \overline{\mathbb{Q}}$ for the j-invariant of E. In Corollary 1.14, (iii), we verify that the [logarithmic] *Weil height*

$$h(j(E))$$

[cf. Definition 1.1, (i)] of $j(E)$ satisfies the following property:

(H1) Let l be a prime number. Suppose that E admits an *l-cyclic* subgroup scheme, and that l is *prime* to the *local heights* of E at each of its places of [bad] multiplicative reduction [i.e., the orders of the q-parameter at such places — cf. [GenEll], Definition 3.3]. Then the *nonarchimedean* portion of $h(j(E))$ is *bounded by an explicit absolute constant* $\in \mathbb{R}$.

To verify (H1), we make use of the following two types of heights:

- the *Faltings height* $h^{\mathrm{Fal}}(E)$ [cf. the discussion entitled "Curves" in §0],
- the *symmetrized toric height* $h^{\mathfrak{S}\text{-tor}}(E)$ [cf. Definition 1.7].

These heights $h^{\mathrm{Fal}}(E)$ and $h^{\mathfrak{S}\text{-tor}}(E)$ may be related to $h(j(E))$ by means of *numerically explicit inequalities* [cf. Propositions 1.8, 1.10, 1.12] and satisfy the following important properties:

(H2) Let E' be an elliptic curve over F; $\phi : E \to E'$ an isogeny of degree d. Then it holds that $h^{\mathrm{Fal}}(E') - h^{\mathrm{Fal}}(E) \leq \frac{1}{2}\log(d)$ [cf. [Falt], Lemma 5].

(H3) The *archimedean* portion of $h^{\mathfrak{S}\text{-tor}}(E)$ is *bounded above* by the *nonarchimedean* portion of $h^{\mathfrak{S}\text{-tor}}(E)$ [cf. Proposition 1.9, (i)].

[Here, we note that (H3) is an immediate consequence of the *product formula*, together with the assumption that the cardinality of the set of archimedean places of the *mono-complex* number field $\mathbb{Q}(\lambda)$ is *one*.] The property (H1) then follows, essentially formally, by applying (H2) and (H3), together with the numerically explicit inequalities [mentioned above], which allow one to compare the different types of heights.

In §2, we review

- a result concerning the *j-invariants* of "*arithmetic*" elliptic curves [cf. Proposition 2.1];
- certain *effective versions* of the *prime number theorem* [cf. Proposition 2.2].

In §3, we establish a version of the theory of *étale theta functions* [cf. [EtTh], [IUTchII]] that functions properly at *arbitrary* bad places, i.e., *even bad places that divide the prime "2"*. Here, we note that the original definition of the notion of an *evaluation point* — i.e., a point at which the theta function is evaluated that is obtained by translating a cusp by a 2-*torsion point* [cf. [EtTh], Definition 1.9; [IUTchI], Example 4.4, (i)] — does not function properly at places over 2 [cf. [IUTchIV], Remark 1.10.6, (ii)]. Thus, it is natural to pose the following question:

> Is it possible to obtain a *new definition* of evaluation points that functions properly at *arbitrary* bad places by replacing the "2-*torsion point*" appearing in the [original] definition of an evaluation point by an "n-*torsion point*", for some integer $n > 2$?

Here, we recall that the definition of an evaluation point obtained by translating a cusp by an n-*torsion point* functions properly at *arbitrary* bad places if the following two conditions are satisfied:

(1) The various *ratios* of theta values at the Galois conjugates of [the point of the Tate uniformization of a Tate curve corresponding to a primitive $2n$-th root of unity] ζ_{2n} are *roots of unity* [cf. [IUTchII], Remark 2.5.1, (ii)].

(2) The theta value at ζ_{2n} is a *unit* at *arbitrary* bad places [cf. [IUTchIV], Remark 1.10.6, (ii)].

One *fundamental observation* — due to *Porowski* — that underlies the theory of the present paper is the following:

$$n \text{ satisfies the conditions (1), (2) if and only if } n = 6$$

[cf. Lemma 3.1; Proposition 3.2; the well-known fact that $1 - \zeta_4$, $1 - \zeta_8$ are *non-units* at places over 2]. Following this observation, in Definition 3.3, we introduce a *new version* of the notion of an "étale theta function of standard type" [cf. [EtTh], Definition 1.9] obtained by normalizing étale theta functions at points arising from 6-*torsion points* of the given elliptic curve. In the remainder of §3, we then proceed to discuss how the adoption of such *"étale theta functions of $\boldsymbol{\mu}_6$-standard type"* affects the theory developed in [EtTh].

Next, in §4, we discuss how the modifications of §3 affect [IUTchI-III]. Roughly speaking, we observe that, once one makes suitable minor technical modifications,

(∗) the theory developed in [IUTchI-III] *remains essentially unaffected* even if, in the notation of [IUTchI], Definition 3.1, (b), one *eliminates*

the assumption "of *odd* residue characteristic" that appears in the discussion of "$\mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}$".

In §5, we begin by proving a "$\boldsymbol{\mu}_6$-version" [cf. Theorem 5.1] of [IUTchIV], Theorem 1.10, i.e., that applies the theory developed in §2, §3, §4. This allows us to obtain a "$\boldsymbol{\mu}_6$-version" [cf. Corollary 5.2] of [IUTchIV], Corollary 2.2, (ii), (iii) [i.e., the "Theorem" reviewed at the beginning of the present Introduction] *without* assuming the conditions (CBS1), (CBS2) that appear in the statement of this Theorem concerning the nonarchimedean place "2". The proof of Corollary 5.2 makes *essential use of the theory of §1, §2* [cf., especially, Corollary 1.14; Propositions 2.1, 2.2]. In the case of *mono-complex* number fields, we then derive

- Theorem 5.3 from Corollary 5.2 by applying the *product formula*, together with the *essential assumption* that the number field under consideration is *mono-complex* [cf. the property (H3) discussed above] and various elementary computations [such as Proposition 1.8, (i)];
- Theorem 5.4 from Theorem 5.3, together with various elementary computations [such as Proposition 1.8, (i)].

Finally, we apply

- Theorem 5.3, together with various elementary considerations, to *"Fermat's Last Theorem"* [cf. Corollary 5.8] and
- Theorem 5.4, again together with various elementary computations, to a *generalized version of "Fermat's Last Theorem"* [cf. Corollary 5.9].

In this context, we note [cf. Remark 5.3.2] that it is quite possible that, in the future, other interesting applications of Theorems 5.3, 5.4 to the study of numerical aspects of diophantine equations can be found.

Acknowledgements

Each of the co-authors of the present paper would like to thank the other co-authors for their valuable contributions to the theory exposed in the present paper. In particular, the co-authors [other than the first author] of the present paper wish to express their deep gratitude to the first author, i.e., the originator of inter-universal Teichmüller theory, for countless hours of valuable discussions related to his work. The authors are grateful to J. Sijsling for responding to our request to provide us with the computations that underlie Proposition 2.1. Moreover, the authors are grateful to P. Mihăilescu for producing a paper, co-authored with M. Rassias, based on his unpublished results on lower bounds for the second case of Fermat's Last Theorem and a new insight on lattices and an "inhomogeneous Siegel box principle". The second and fifth authors were partially supported by the ESPRC Programme Grant "Symmetries and Correspondences". The third author was supported by JSPS KAKENHI Grant Number 18K03239; the fourth author was supported by JSPS KAKENHI Grant Number 20K14285. This

research was supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University, as well as by the Center for Next Generation Geometry [a research center affiliated with the Research Institute for Mathematical Sciences].

0. Notations and Conventions

Numbers:

Let S be a set. Then we shall write $\sharp S$ for the cardinality of S.

Let $E \subseteq \mathbb{R}$ be a subset of the set of real numbers $\mathbb{R}$. Then for $\lambda \in \mathbb{R}$, if $\square$ denotes "$< \lambda$", "$\leq \lambda$", "$> \lambda$", or "$\geq \lambda$", then we shall write $E_{\square} \subseteq E$ for the subset of elements that satisfy the inequality "$\square$". If E is *finite*, then we shall write $\max E$ for the smallest real number λ such that $E_{\leq \lambda} = E$ and $\min E$ for the largest real number λ such that $E_{\geq \lambda} = E$.

For any nonzero integer $n \notin \{1, -1\}$, we shall write $\mathrm{rad}(n)$ for the product of the distinct prime numbers p which divide n. We shall define $\mathrm{rad}(1)$ and $\mathrm{rad}(-1)$ to be 1.

Let F be a field. Then we shall write $F^{\dagger} \stackrel{\text{def}}{=} F \setminus \{0, 1\}$.

Let $\overline{\mathbb{Q}}$ be an algebraic closure of the field of rational numbers $\mathbb{Q}$, $F \subseteq \overline{\mathbb{Q}}$ a subfield. Then we shall write $\mathcal{O}_F \subseteq F$ for the ring of integers of F; $\mathbb{Z} \stackrel{\text{def}}{=} \mathcal{O}_{\mathbb{Q}}$; $\mathfrak{Primes} \subseteq \mathbb{Z}$ for the set of all prime numbers; $\mathbb{V}(F)^{\mathrm{non}}$ (respectively, $\mathbb{V}(F)^{\mathrm{arc}}$) for the set of *nonarchimedean* (respectively, *archimedean*) *places* of F;

$$\mathbb{V}(F) \stackrel{\text{def}}{=} \mathbb{V}(F)^{\mathrm{arc}} \bigcup \mathbb{V}(F)^{\mathrm{non}}.$$

For $v \in \mathbb{V}(F)$, we shall write F_v for the *completion* of F at v.

Now suppose that F is a *number field*, i.e., that $[F : \mathbb{Q}] < \infty$.

Let $v \in \mathbb{V}(F)^{\mathrm{non}}$. Write $\mathfrak{p}_v \subseteq \mathcal{O}_F$ for the *prime ideal* corresponding to v; p_v for the *residue characteristic* of F_v; f_v for the *residue field degree* of F_v over $\mathbb{Q}_{p_v}$; ord_v for the *normalized valuation* on F_v determined by v, where we take the normalization to be such that ord_v restricts to the *standard p_v-adic valuation* on $\mathbb{Q}_{p_v}$. Then for any $x \in F_v$, we shall write

$$||x||_v \stackrel{\text{def}}{=} p_v^{-\mathrm{ord}_v(x)}, \quad |x|_v \stackrel{\text{def}}{=} ||x||_v^{[F_v : \mathbb{Q}_{p_v}]}.$$

Let $v \in \mathbb{V}(F)^{\mathrm{arc}}$. Write $\sigma_v : F \hookrightarrow \mathbb{C}$ for the embedding determined, up to complex conjugation, by v. Then for any $x \in F_v$, we shall write

$$||x||_v \stackrel{\text{def}}{=} ||\sigma_v(x)||_{\mathbb{C}}, \quad |x|_v \stackrel{\text{def}}{=} ||x||_v^{[F_v : \mathbb{R}]}$$

— where we denote by $||\cdot||_{\mathbb{C}}$ the *standard [complex] absolute value* on $\mathbb{C}$.

Note that for any $w \in \mathbb{V}(\overline{\mathbb{Q}})$ that lies over $v \in \mathbb{V}(F)$, the absolute value $||\cdot||_v : F_v \to \mathbb{R}_{\geq 0}$ extends uniquely to an absolute value $||\cdot||_w : \overline{\mathbb{Q}}_w \to \mathbb{R}_{\geq 0}$. We shall refer to this absolute value on $\overline{\mathbb{Q}}_w$ as the *standard absolute value* on $\overline{\mathbb{Q}}_w$.

Curves:

Let E be an elliptic curve over a field. Then we shall write $j(E)$ for the *j-invariant* of E.

Let E be an elliptic curve over a number field F that has semi-stable reduction over $\mathcal{O}_F$. Write $\underline{h}^{\mathrm{Fal}}(E)$ for the *Faltings height* of E [cf. [Falt], §3, the first Definition]. Then we shall write

$$h^{\mathrm{Fal}}(E) \stackrel{\mathrm{def}}{=} \underline{h}^{\mathrm{Fal}}(E) + \tfrac{1}{2}\log \pi$$

[cf. [Lbr], Definition 2.3; [Lbr], Remark 2.1]. Here, we note that the quantity $h^{\mathrm{Fal}}(E)$ is unaffected by passage to a finite extension of the base field F of E [cf., e.g., [Lbr], Proposition 2.1, (i)].

1. Heights

Let E be an elliptic curve over a number field. In the present section, we introduce the notion of the *symmetrized toric height* $h^{\mathfrak{S}\text{-}\mathrm{tor}}(E)$ of E [cf. Definition 1.7]. We then compare $h^{\mathfrak{S}\text{-}\mathrm{tor}}(E)$ with the [logarithmic] *Weil height* $h(j(E))$ of $j(E)$ [cf. Proposition 1.8]. Finally, we prove that if E satisfies certain conditions, then the *nonarchimedean* portion of $h(j(E))$ is *bounded* by an *absolute constant* [cf. Corollary 1.14, (iii)].

Definition 1.1. Let F be a number field.

(i) Let $\alpha \in F$. Then for $\square \in \{\mathrm{non}, \mathrm{arc}\}$, we shall write

$$h_{\square}(\alpha) \stackrel{\mathrm{def}}{=} \tfrac{1}{[F:\mathbb{Q}]} \sum_{v \in \mathbb{V}(F)^{\square}} \log \max\{|\alpha|_v, 1\} \quad (\geq 0),$$

$$h(\alpha) \stackrel{\mathrm{def}}{=} h_{\mathrm{non}}(\alpha) + h_{\mathrm{arc}}(\alpha)$$

and refer to $h(\alpha)$ as the [*logarithmic*] *Weil height* of α. We shall also write $h_{\circledcirc}(\alpha)$ for $h(\alpha)$.

(ii) Let $\alpha \in F^{\times}$. Then for $\square \in \{\mathrm{non}, \mathrm{arc}\}$, we shall write

$$h^{\mathrm{tor}}_{\square}(\alpha) \stackrel{\mathrm{def}}{=} \tfrac{1}{2[F:\mathbb{Q}]} \sum_{v \in \mathbb{V}(F)^{\square}} \log \max\{|\alpha|_v, |\alpha|_v^{-1}\} \quad (\geq 0),$$

$$h^{\mathrm{tor}}(\alpha) \stackrel{\mathrm{def}}{=} h^{\mathrm{tor}}_{\mathrm{non}}(\alpha) + h^{\mathrm{tor}}_{\mathrm{arc}}(\alpha)$$

and refer to $h^{\mathrm{tor}}(\alpha)$ as the [*logarithmic*] *toric height* of α. We shall also write $h^{\mathrm{tor}}_{\circledcirc}(\alpha)$ for $h^{\mathrm{tor}}(\alpha)$.

Remark 1.1.1. One verifies easily that for $\square \in \{\mathrm{non}, \mathrm{arc}, \circledcirc\}$, the quantities $h_{\square}(\alpha)$ and $h^{\mathrm{tor}}_{\square}(\alpha)$ are unaffected by passage to a finite extension of F.

Definition 1.2. Let F be a number field. Then we shall say that F is *mono-complex* if F is either

the *field of rational numbers* $\mathbb{Q}$ or an *imaginary quadratic field*.

One verifies easily that F is mono-complex if and only if the cardinality of $\mathbb{V}(F)^{\mathrm{arc}}$ is one.

Lemma 1.3. (Properties of toric heights) *Let F be a* **number field**, $\alpha \in F^{\times}$. *Then the following hold:*

(i) *It holds that*

$$h^{\mathrm{tor}}_{\square}(\alpha) \;=\; h^{\mathrm{tor}}_{\square}(\alpha^{-1}); \quad h^{\mathrm{tor}}_{\square}(\alpha) \;=\; \tfrac{1}{2} \cdot \{h_{\square}(\alpha) + h_{\square}(\alpha^{-1})\}$$

for $\square \in \{\mathrm{non}, \mathrm{arc}, \circledcirc\}$.

(ii) *It holds that*

$$h(\alpha) \;=\; h^{\mathrm{tor}}(\alpha).$$

In particular, we have $h(\alpha) = h(\alpha^{-1})$ *[cf. (i)].*

(iii) *Suppose that F is* **mono-complex**. *Then we have*

$$h^{\mathrm{tor}}_{\mathrm{arc}}(\alpha) \;\leq\; h^{\mathrm{tor}}_{\mathrm{non}}(\alpha).$$

(iv) *Let x, $y \in F$; x^{tor}, $y^{\mathrm{tor}} \in F^{\times}$. Then we have*

$$h_{\square}(x) + h_{\square}(y) \;\geq\; h_{\square}(x \cdot y);$$
$$h^{\mathrm{tor}}_{\square}(x^{\mathrm{tor}}) + h^{\mathrm{tor}}_{\square}(y^{\mathrm{tor}}) \;\geq\; h^{\mathrm{tor}}_{\square}(x^{\mathrm{tor}} \cdot y^{\mathrm{tor}})$$

for $\square \in \{\mathrm{non}, \mathrm{arc}, \circledcirc\}$.

Proof. First, we consider assertion (i). The first equality follows immediately from the various definitions involved. The second equality follows immediately from the various definitions involved, together with the following [easily verified] *fact*: For any $s \in \mathbb{R}_{>0}$, it holds that

$$\max\{s, s^{-1}\} \;=\; \max\{s, 1\} \cdot \max\{s^{-1}, 1\}.$$

Next, we consider assertion (ii). Write $d \stackrel{\mathrm{def}}{=} [F : \mathbb{Q}]$. Then we compute:

$$\begin{aligned} 2d \cdot h^{\mathrm{tor}}(\alpha) \;&=\; \sum_{v \in \mathbb{V}(F)} \log \max\{|\alpha|_v, |\alpha|_v^{-1}\} \;=\; \sum_{v \in \mathbb{V}(F)} \log(|\alpha|_v^{-1} \cdot \max\{|\alpha|_v^2, 1\}) \\ &=\; 2d \cdot h(\alpha) \;+\; \sum_{v \in \mathbb{V}(F)} \log |\alpha|_v^{-1} \;=\; 2d \cdot h(\alpha) \end{aligned}$$

— where the final equality follows from the *product formula*. This completes the proof of assertion (ii).

Next, we consider assertion (iii). Let w be the *unique* element of $\mathbb{V}(F)^{\mathrm{arc}}$. In light of the first equality of assertion (i), to verify assertion (iii), we may assume without loss of generality that $|\alpha|_w \geq 1$. Then we compute:

$$\begin{aligned} 2d \cdot h^{\mathrm{tor}}_{\mathrm{arc}}(\alpha) \;&=\; \log |\alpha|_w \;=\; \sum_{v \in \mathbb{V}(F)^{\mathrm{non}}} \log |\alpha|_v^{-1} \\ &\leq\; \sum_{v \in \mathbb{V}(F)^{\mathrm{non}}} \log \max\{|\alpha|_v, |\alpha|_v^{-1}\} \;=\; 2d \cdot h^{\mathrm{tor}}_{\mathrm{non}}(\alpha) \end{aligned}$$

— where the second equality follows from the *product formula*. This completes the proof of assertion (iii). Finally, we consider assertion (iv). It follows immediately from the second equality of assertion (i) that to verify the *second inequality* of assertion (iv), it suffices to verify the *first inequality* of assertion (iv). But the first inequality follows immediately from the following [easily verified] fact: For any s, $t \in \mathbb{R}_{\geq 0}$, it holds that

$$\max\{st, 1\} \;\leq\; \max\{s, 1\} \cdot \max\{t, 1\}.$$

This completes the proof of assertion (iv). □

Remark 1.3.1. It may appear to the reader, at first glance, that the notion of the toric height of an element of a number field F is *unnecessary* [cf. Lemma 1.3, (ii)]. In fact, however, the toric height of an element $\alpha \in F^\times$ satisfies the following important property [cf. Lemma 1.3, (iii)]:

> If F is *mono-complex*, then the *archimedean* portion of the toric height of α is *bounded* by the *nonarchimedean* portion of the toric height of α.

This property is an immediate consequence of the *product formula* [cf. the proof of Lemma 1.3, (iii)]. We note that, in general, the notion of the Weil height *does not satisfy* this property. For instance, for any $n \in \mathbb{Z}_{>0}$, we have

$$h_{\mathrm{non}}(n) \;=\; 0; \quad h_{\mathrm{arc}}(n) \;=\; \log(n);$$
$$h^{\mathrm{tor}}_{\mathrm{non}}(n) \;=\; \tfrac{1}{2}\log(n); \quad h^{\mathrm{tor}}_{\mathrm{arc}}(n) \;=\; \tfrac{1}{2}\log(n).$$

Definition 1.4. Let F be a field; $|\cdot| : F \to \mathbb{R}_{\geq 0}$ a map satisfying the following conditions:

(i) The restriction of $|\cdot|$ to $F^\times$ determines a group homomorphism $F^\times \to \mathbb{R}_{>0}$ [relative to the multiplicative group structures on $F^\times$, $\mathbb{R}_{>0}$].

(ii) It holds that $|0| = 0$.

(iii) For any $x \in F$, it holds that $|x+1| \leq |x| + 1$.

Then for $\alpha \in F^\dagger$, we shall write

$$\begin{aligned}
J(\alpha) &\stackrel{\mathrm{def}}{=} |\alpha^2 - \alpha + 1|^3 \cdot |\alpha|^{-2} \cdot |\alpha - 1|^{-2} \\
&= |\alpha(1-\alpha) - 1|^3 \cdot |\alpha|^{-2} \cdot |1-\alpha|^{-2}; \\
J_{0\infty}(\alpha) &\stackrel{\mathrm{def}}{=} \max\left\{|\alpha|, |\alpha|^{-1}\right\}; \\
J_{1\infty}(\alpha) &\stackrel{\mathrm{def}}{=} \max\left\{|\alpha - 1|, |\alpha - 1|^{-1}\right\}; \\
J_{01}(\alpha) &\stackrel{\mathrm{def}}{=} \max\left\{|\alpha - 1| \cdot |\alpha|^{-1}, |\alpha| \cdot |\alpha - 1|^{-1}\right\}.
\end{aligned}$$

Lemma 1.5. (Comparison between $J(\alpha)$ and $|\alpha|^2$) *In the notation of Definition 1.4, suppose that $|\alpha| \geq 2$. Then we have*

$$|\alpha|^2 \;\leq\; 2^8 \cdot J(\alpha).$$

Proof. First, we note that since $|\alpha - 1| \;\leq\; |\alpha| + 1$, we have

$$|\alpha^2 - \alpha + 1| \;=\; |\alpha^2 - (\alpha - 1)| \;\geq\; |\alpha|^2 - |\alpha - 1| \;\geq\; |\alpha|^2 - (|\alpha| + 1).$$

Thus, we conclude that

$$\begin{aligned}
2^8 \cdot |\alpha^2 - \alpha + 1|^3 \cdot |\alpha|^{-2} \cdot |\alpha - 1|^{-2} &\geq\; 2^8 \cdot (|\alpha|^2 - |\alpha| - 1)^3 \cdot |\alpha|^{-2} \cdot (|\alpha| + 1)^{-2} \\
&\geq\; |\alpha|^2
\end{aligned}$$

— where we observe that since $x^2 - x - 1 \geq x(x - \frac{3}{2})$, $-(x+1)^2 \geq -(2x)^2$, and the function $\frac{3}{2x-3}$ is monotonically decreasing for $x \in \mathbb{R}_{\geq 2}$, the final inequality follows from the elementary fact that

$$\begin{aligned} 2^8 \cdot (x^2 - x - 1)^3 - x^4 \cdot (x+1)^2 &\geq x^3 \cdot \left\{2^8 \cdot (x - \tfrac{3}{2})^3 - x \cdot (x+1)^2\right\} \\ &\geq 2^2 \cdot x^3 \cdot \left\{2^6 \cdot (x - \tfrac{3}{2})^3 - x^3\right\} \\ &\geq 2^8 \cdot x^3 \cdot (x - \tfrac{3}{2})^3 \cdot \left\{1 - 2^{-6} \cdot (1 + \tfrac{3}{2x-3})^3\right\} \\ &\geq 0 \end{aligned}$$

for $x \in \mathbb{R}_{\geq 2}$. □

Lemma 1.6. (Comparison between $J(\alpha)$ and $J_{0\infty}(\alpha) \cdot J_{1\infty}(\alpha) \cdot J_{01}(\alpha)$) *In the notation of Definition 1.4, the following hold:*

(i) *Write z for the rational function given by the standard coordinate on $\mathbb{P}^1_{\mathbb{Z}}$ and*

$$\begin{aligned} A &\stackrel{\text{def}}{=} \{z, z^{-1}, 1-z, (1-z)^{-1}, z \cdot (z-1)^{-1}, (z-1) \cdot z^{-1}\}, \\ B &\stackrel{\text{def}}{=} \{\delta \subseteq A \mid \sharp\delta = 2;\ \textit{if we write } \delta = \{a, b\},\ \textit{then} \\ &\qquad \textit{it holds that } A = \{a, a^{-1}, b, b^{-1}, -ab, -(ab)^{-1}\}\}. \end{aligned}$$

Then the set B **coincides** *with the set*

$$\begin{aligned} B' \stackrel{\text{def}}{=} &\{\{z, (1-z)^{-1}\},\ \{z, (z-1) \cdot z^{-1}\},\ \{z^{-1}, 1-z\}, \\ &\{z^{-1}, z \cdot (z-1)^{-1}\},\ \{1-z, z \cdot (z-1)^{-1}\}, \\ &\{(1-z)^{-1}, (z-1) \cdot z^{-1}\}\}. \end{aligned}$$

Moreover, the map

$$\begin{aligned} \phi :\ B &\to A \\ \{a, b\} &\mapsto -ab \end{aligned}$$

is **bijective**. *Here, we recall that the symmetric group on 3 letters $\mathfrak{S}_3$ admits a natural faithful action on the projective line $\mathbb{P}^1_{\mathbb{Z}}$ over $\mathbb{Z}$, hence also on the set of F-rational points $(\mathbb{P}^1_{\mathbb{Z}} \setminus \{0, 1, \infty\})(F) \stackrel{\sim}{\to} F^{\text{⫛}}$, and that the* **orbit** *$\mathfrak{S}_3 \cdot z$ of z* **coincides** *with the set A. In particular, the action of $\mathfrak{S}_3$ on A induces, via ϕ^{-1}, a* **transitive action** *of $\mathfrak{S}_3$ on B.*

(ii) *For every $\delta = \{a, b\} \in B$, write*

$$\mathbb{D}_\delta \stackrel{\text{def}}{=} \{f \in F^{\text{⫛}} \mid |a(f)| \geq 1,\ |b(f)| \geq 1\} \subseteq F^{\text{⫛}}.$$

We note that the action of $\mathfrak{S}_3$ on B [cf. (i)] induces a **transitive action** *on the set [of subsets of $F^{\text{⫛}}$] $\{\mathbb{D}_\delta\}_{\delta \in B}$. Then we have*

$$F^{\text{⫛}} = \bigcup_{\delta \in B} \mathbb{D}_\delta.$$

(iii) *For any* $\epsilon \in \mathbb{R}_{\geq 0}$*, we have*

$$\begin{aligned} 2^{-2} \cdot J_{0\infty}(\alpha) \cdot J_{1\infty}(\alpha) \cdot J_{01}(\alpha) &\leq \max\{2^{6+\epsilon} \cdot J(\alpha),\ 1\} \\ &\leq 2^{9+\epsilon} \cdot J_{0\infty}(\alpha) \cdot J_{1\infty}(\alpha) \cdot J_{01}(\alpha). \end{aligned}$$

(iv) *Suppose that* $|\cdot|$ *is* **nonarchimedean***, i.e., that for any* $x \in F$*, it holds that* $|x+1| \leq \max\{|x|, 1\}$*. [Thus, for any* $x \in F$ *such that* $|x| < 1$*, it holds that* $|x+1| = 1$*.] Then we have*

$$\max\{J(\alpha),\ 1\} \ = \ J_{0\infty}(\alpha) \cdot J_{1\infty}(\alpha) \cdot J_{01}(\alpha).$$

Proof. First, we consider assertion (i). To verify assertion (i), it suffices to show that $B = B'$. [Indeed, it follows from this equality that $\sharp B = 6$. Thus, to verify that ϕ is bijective, it suffices to show that ϕ is *surjective*. But this surjectivity follows immediately from the equality $B = B'$ and the various definitions involved.] The inclusion $B' \subseteq B$ follows immediately from the various definitions involved. Thus, it suffices to verify the inclusion $B \subseteq B'$. First, we observe that A is the [disjoint] union of the following sets:

$$A_{0\infty} \stackrel{\text{def}}{=} \{z, z^{-1}\},\ A_{1\infty} \stackrel{\text{def}}{=} \{1-z, (1-z)^{-1}\},\ A_{01} \stackrel{\text{def}}{=} \{z\cdot(z-1)^{-1}, (z-1)\cdot z^{-1}\}.$$

Let $\delta \in B$. Note that [as is easily verified] $\delta \notin \{A_{0\infty}, A_{1\infty}, A_{01}\}$. Thus, we may write

$$\delta \ = \ \{a, b\}$$

— where the pair (a, b) satisfies *precisely one* of the following three conditions:

(1) $a \in A_{0\infty},\ b \in A_{1\infty}$, (2) $a \in A_{1\infty},\ b \in A_{01}$, (3) $a \in A_{01},\ b \in A_{0\infty}$.

On the other hand, in each of these three cases, one verifies immediately that the condition

$$A \ = \ \{a, a^{-1}, b, b^{-1}, -ab, -(ab)^{-1}\}$$

implies that there are *precisely two* possibilities for δ, and, moreover, that these two possibilities are $\in B'$, as desired. This completes the proof of assertion (i).

Next, we consider assertion (ii). Assertion (ii) follows immediately from the following *claim*:

> *Claim 1.6A:* For $f \in F^{\dagger}$, $\delta \in B$, write $\delta(f) \stackrel{\text{def}}{=} \phi(\delta)(f)$. Suppose that it holds that
>
> $$|\delta(f)| \ = \ \max_{\epsilon \in B}\{|\epsilon(f)|\}.$$
>
> Then we have $f \in \mathbb{D}_{\delta}$.

Let us verify Claim 1.6A. Write $\delta = \{a, b\}$. Suppose that $f \notin \mathbb{D}_{\delta}$. Then we may assume without loss of generality that $|a(f)| < 1$. Thus, we have

$$|\delta(f)| \ = \ |a(f)| \cdot |b(f)| \ < \ |b(f)|.$$

On the other hand, since we have $|b(f)| \in \{\epsilon(f)\}_{\epsilon \in B}$ [cf. the latter portion of assertion (i), i.e., the fact that ϕ is a bijection], we obtain a contradiction. Therefore, we conclude that $f \in \mathbb{D}_{\delta}$. This completes the verification of Claim 1.6A, hence also of assertion (ii).

Next, we consider assertions (iii) and (iv). First, we observe that, in assertion (iii), we may assume without loss of generality, that $\epsilon = 0$. Write

$$\mathbb{D} \stackrel{\text{def}}{=} \mathbb{D}_{\{1-z,z\cdot(z-1)^{-1}\}} = \{f \in F^{\dagger} \mid |f| \geq |f-1| \geq 1\} \subseteq F^{\dagger}.$$

Then we observe that

$$F^{\dagger} = \bigcup_{\sigma \in \mathfrak{S}_3} (\sigma \cdot \mathbb{D})$$

[cf. assertion (ii)], and that for $\alpha \in F^{\dagger}$, $\sigma \in \mathfrak{S}_3$, we have

$$J_{0\infty}(\alpha) \cdot J_{1\infty}(\alpha) \cdot J_{01}(\alpha) = J_{0\infty}(\sigma \cdot \alpha) \cdot J_{1\infty}(\sigma \cdot \alpha) \cdot J_{01}(\sigma \cdot \alpha),$$

$$J(\alpha) = J(\sigma \cdot \alpha)$$

[cf. the *fact* discussed in the proof of Lemma 1.3, (i); Definition 1.4; the equality "$A = \mathfrak{S}_3 \cdot z$" discussed in assertion (i); the manifest invariance of $J(\alpha)$ with respect to the transformations $\alpha \mapsto 1-\alpha$, $\alpha \mapsto \alpha^{-1}$, which correspond to a pair of generators of $\mathfrak{S}_3$]. Thus, to verify assertions (iii) and (iv), we may assume without loss of generality that $\alpha \in \mathbb{D}$. Then observe that $J_{0\infty}(\alpha) = |\alpha| \geq 1$, $J_{1\infty}(\alpha) = |\alpha - 1| \geq 1$, $J_{01}(\alpha) = |\alpha| \cdot |\alpha - 1|^{-1} \geq 1$, hence that

$$J_{0\infty}(\alpha) \cdot J_{1\infty}(\alpha) \cdot J_{01}(\alpha) = |\alpha|^2 \ (\geq 1).$$

Now let us verify assertion (iii). The inequality

$$J_{0\infty}(\alpha) \cdot J_{1\infty}(\alpha) \cdot J_{01}(\alpha) \leq 2^2 \cdot \max\{2^6 \cdot J(\alpha), 1\}$$

follows immediately from Lemma 1.5. On the other hand, the inequality

$$\max\{2^6 \cdot J(\alpha), 1\} \leq 2^9 \cdot J_{0\infty}(\alpha) \cdot J_{1\infty}(\alpha) \cdot J_{01}(\alpha)$$

follows immediately from the following computation:

$$\begin{aligned} J(\alpha) &= |\alpha(\alpha-1)+1|^3 \cdot |\alpha|^{-2} \cdot |\alpha-1|^{-2} \\ &\leq 2^3 \cdot |\alpha|^{-2} \cdot |\alpha-1|^{-2} \cdot \max\{|\alpha|^3 \cdot |\alpha-1|^3, 1\} \\ &= 2^3 \cdot |\alpha| \cdot |\alpha-1| \leq 2^3 \cdot |\alpha|^2 = 2^3 \cdot J_{0\infty}(\alpha) \cdot J_{1\infty}(\alpha) \cdot J_{01}(\alpha). \end{aligned}$$

— where we apply the easily verified fact that $|x+1|^3 \leq 2^3 \cdot \max\{|x|^3, 1\}$ for $x \in F$. This completes the proof of assertion (iii).

Finally, let us verify assertion (iv). First, observe that it follows immediately from our assumption that $|\cdot|$ is *nonarchimedean* that

$$\mathbb{D} = \{f \in F^{\dagger} \mid |f| = |f-1|\}.$$

Suppose that $|\alpha| = |\alpha - 1| = 1$ (respectively, $|\alpha| = |\alpha - 1| > 1$). Then we have

$$J(\alpha) = |\alpha(\alpha-1)+1|^3 \leq (\max\{|\alpha| \cdot |\alpha-1|, 1\})^3 = 1 = |\alpha|^2$$

$$\text{(respectively, } J(\alpha) = |\alpha(\alpha-1)+1|^3 \cdot |\alpha|^{-4} = |\alpha|^6 \cdot |\alpha|^{-4} = |\alpha|^2\text{)}.$$

Thus, we conclude that

$$\max\{J(\alpha),\ 1\} = |\alpha|^2 = J_{0\infty}(\alpha) \cdot J_{1\infty}(\alpha) \cdot J_{01}(\alpha),$$

as desired. This completes the proof of assertion (iv). □

Definition 1.7. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, $F \subseteq \overline{\mathbb{Q}}$ a number field, E an elliptic curve over F. Recall that E is isomorphic over $\overline{\mathbb{Q}}$ to the elliptic curve defined by an equation

$$y^2 \ = \ x(x-1)(x-\lambda)$$

— where $\lambda \in \overline{\mathbb{Q}}^{\dagger}$ [cf. [Silv1], Chapter III, Proposition 1.7, (a)]. Recall further that the j-invariant $j(E)$ of E satisfies

$$j(E) \ = \ 2^8 \tfrac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2} \ \ (\in F)$$

[cf. [Silv1], Chapter III, Proposition 1.7, (b)], and that the symmetric group on 3 letters $\mathfrak{S}_3$ admits a natural faithful action on the projective line $\mathbb{P}^1_{\mathbb{Q}}$ over $\mathbb{Q}$, hence also on the set of $\overline{\mathbb{Q}}$-rational points $(\mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\})(\overline{\mathbb{Q}}) \xrightarrow{\sim} \overline{\mathbb{Q}}^{\dagger}$. For $\square \in \{\mathrm{non}, \mathrm{arc}\}$, we shall write

$$h_{\square}^{\mathfrak{S}\text{-}\mathrm{tor}}(E) \ \stackrel{\mathrm{def}}{=} \ \sum_{\sigma \in \mathfrak{S}_3} h_{\square}^{\mathrm{tor}}(\sigma \cdot \lambda),$$

$$h^{\mathfrak{S}\text{-}\mathrm{tor}}(E) \ \stackrel{\mathrm{def}}{=} \ h_{\mathrm{non}}^{\mathfrak{S}\text{-}\mathrm{tor}}(E) + h_{\mathrm{arc}}^{\mathfrak{S}\text{-}\mathrm{tor}}(E)$$

[cf. Remark 1.1.1] and refer to $h^{\mathfrak{S}\text{-}\mathrm{tor}}(E)$ as the *symmetrized toric height* of E. We shall also write $h_{\circledcirc}^{\mathfrak{S}\text{-}\mathrm{tor}}(E)$ for $h^{\mathfrak{S}\text{-}\mathrm{tor}}(E)$. One verifies easily that $h_{\mathrm{non}}^{\mathfrak{S}\text{-}\mathrm{tor}}(E)$, $h_{\mathrm{arc}}^{\mathfrak{S}\text{-}\mathrm{tor}}(E)$, $h^{\mathfrak{S}\text{-}\mathrm{tor}}(E)$ do not depend on the choice of "λ" [cf. the proof of [Silv1], Chapter III, Proposition 1.7, (c)].

Remark 1.7.1. One verifies easily [cf. Remark 1.1.1] that for $\square \in \{\mathrm{non}, \mathrm{arc}, \circledcirc\}$, the quantity $h_{\square}^{\mathfrak{S}\text{-}\mathrm{tor}}(E)$ is unaffected by passage to a finite extension of the base field F of E.

Remark 1.7.2. It follows immediately from Lemma 1.3, (i), that for $\square \in \{\mathrm{non}, \mathrm{arc}, \circledcirc\}$, we have

$$h_{\square}^{\mathfrak{S}\text{-}\mathrm{tor}}(E) \ = \ \sum_{\sigma \in \mathfrak{S}_3} h_{\square}(\sigma \cdot \lambda).$$

Proposition 1.8. (Comparison between $h_{\square}^{\mathfrak{S}\text{-}\mathrm{tor}}(E)$ and $h_{\square}(j(E))$) *In the notation of Definition 1.7, the following hold:*

(i) $0 \ \leq \ h_{\mathrm{non}}^{\mathfrak{S}\text{-}\mathrm{tor}}(E) - h_{\mathrm{non}}(j(E)) \ \leq \ 8 \log 2.$

(ii) $-11 \log 2 \ \leq \ h_{\mathrm{arc}}^{\mathfrak{S}\text{-}\mathrm{tor}}(E) - h_{\mathrm{arc}}(j(E)) \ \leq \ 2 \log 2.$

Proof. If $v \in \mathbb{V}(F)$, then it is well-known that $|| \cdot ||_v$ satisfies the conditions (i), (ii), and (iii) of Definition 1.4, and, moreover, that, if $v \in \mathbb{V}(F)^{\mathrm{non}}$, then $|| \cdot ||_v$ is *nonarchimedean* in the sense of Lemma 1.6, (iv). Observe that, in the remainder of the proof, we may assume without loss of generality that, in the situation of Definition 1.7, $\lambda \in F^{\dagger}$ [cf. Remark 1.7.1]. In the following, for $v \in \mathbb{V}(F)$, we shall write $J(\lambda)_v$, $J_{0\infty}(\lambda)_v$, $J_{1\infty}(\lambda)_v$, $J_{01}(\lambda)_v$ for the "$J(\alpha)$", "$J_{0\infty}(\alpha)$", "$J_{1\infty}(\alpha)$", "$J_{01}(\alpha)$" of Definition 1.4, where we take

· "F" to be F;
· "α" to be λ;
· "$|\cdot|$" to be $||\cdot||_v$.

Here, we observe that, for $\square \in \{\mathrm{non}, \mathrm{arc}\}$, we have

$$h_{\square}^{\mathfrak{S}\text{-tor}}(E) \;=\; 2 \cdot h_{\square}^{\mathrm{tor}}(\lambda) + 2 \cdot h_{\square}^{\mathrm{tor}}(1-\lambda) + 2 \cdot h_{\square}^{\mathrm{tor}}(\lambda \cdot (\lambda-1)^{-1})$$

[cf. Lemma 1.3, (i); the set "A" of Lemma 1.6, (i)].

First, we consider assertion (i). It follows from Lemma 1.6, (iv), that

$$\begin{aligned}[F:\mathbb{Q}] \cdot h_{\mathrm{non}}^{\mathfrak{S}\text{-tor}}(E) &= \sum_{v \in \mathbb{V}(F)^{\mathrm{non}}} [F_v : \mathbb{Q}_{p_v}] \cdot \log(J_{0\infty}(\lambda)_v \cdot J_{1\infty}(\lambda)_v \cdot J_{01}(\lambda)_v) \\ &= \sum_{v \in \mathbb{V}(F)^{\mathrm{non}}} [F_v : \mathbb{Q}_{p_v}] \cdot \log \max\{J(\lambda)_v, 1\}.\end{aligned}$$

Thus, to verify assertion (i), it suffices to show that, for every $v \in \mathbb{V}(F)^{\mathrm{non}}$ *lying over* 2, it holds that

$$0 \;\leq\; \log \max\{J(\lambda)_v, 1\} \;-\; \log \max\{2^{-8} \cdot J(\lambda)_v, 1\} \;\leq\; 8 \log 2$$

[cf. the equality $2^{-8} \cdot J(\lambda)_v = ||j(E)||_v$]. The first inequality follows immediately from the inequality $J(\lambda)_v \geq 2^{-8} \cdot J(\lambda)_v$. Next, we verify the second inequality. If $J(\lambda)_v \leq 1$, then

$$\log \max\{J(\lambda)_v, 1\} \;-\; \log \max\{2^{-8} \cdot J(\lambda)_v, 1\} \;=\; 0 \;-\; 0 \;\leq\; 8 \log 2$$

Thus, we may assume that $J(\lambda)_v > 1$, hence that $\max\{J(\lambda)_v, 1\} = J(\lambda)_v$. In particular, if $2^{-8} \cdot J(\lambda)_v > 1$ (respectively, $2^{-8} \cdot J(\lambda)_v \leq 1$), then we have

$$\log J(\lambda)_v \;-\; \log \max\{2^{-8} \cdot J(\lambda)_v, 1\} \;=\; -\log(2^{-8}) \;=\; 8 \log 2$$

(respectively,

$$\log J(\lambda)_v \;-\; \log \max\{2^{-8} \cdot J(\lambda)_v, 1\} \;=\; \log J(\lambda)_v \;\leq\; 8 \log 2).$$

This completes the verification of the second inequality, hence also of assertion (i).

Next, we consider assertion (ii). Observe that

$$[F:\mathbb{Q}] \cdot h_{\mathrm{arc}}^{\mathfrak{S}\text{-tor}}(E) \;=\; \sum_{v \in \mathbb{V}(F)^{\mathrm{arc}}} [F_v : \mathbb{R}] \cdot \log(J_{0\infty}(\lambda)_v \cdot J_{1\infty}(\lambda)_v \cdot J_{01}(\lambda)_v).$$

Assertion (ii) then follows immediately from Lemma 1.6, (iii) — where we take the "ϵ" of Lemma 1.6, (iii), to be 2 [cf. the equality $2^8 \cdot J(\lambda)_v = ||j(E)||_v$]. □

Proposition 1.9. (Comparison between $h_{\mathrm{non}}(j(E))$ and $h_{\mathrm{arc}}(j(E))$) *In the notation of Definition 1.7, suppose that $\mathbb{Q}(\lambda)$ is* **mono-complex**. *[Here, note that the fact that $\mathbb{Q}(\lambda)$ is mono-complex does not depend on the choice of "λ" [cf. the set "A" of Lemma 1.6, (i)].] Then the following hold:*

(i) $h_{\mathrm{arc}}^{\mathfrak{S}\text{-tor}}(E) \;\leq\; h_{\mathrm{non}}^{\mathfrak{S}\text{-tor}}(E)$.
(ii) $h_{\mathrm{arc}}(j(E)) \;\leq\; h_{\mathrm{non}}(j(E)) + 19 \log 2$.
(iii) *If $C \in \mathbb{R}$, then the element $j(E) \in \overline{\mathbb{Q}}$ is completely determined up to a* **finite number of possibilities** *by the condition $h_{\mathrm{non}}(-) \leq C$.*

Proof. Assertion (i) follows immediately from Lemma 1.3, (iii), and the various definitions involved. Assertion (ii) follows from assertion (i) and Proposition 1.8, (i), (ii). Finally, we consider assertion (iii). It follows from assertion (ii) [cf. also Definition 1.1, (i)] that

$$h(j(E)) \;=\; h_{\mathrm{non}}(j(E)) \;+\; h_{\mathrm{arc}}(j(E)) \;\leq\; 2h_{\mathrm{non}}(j(E)) \;+\; 19\log 2.$$

Thus, assertion (iii) follows immediately from *Northcott's theorem*, i.e., the well-known fact that the set of algebraic numbers of bounded degree and bounded height is *finite* [cf. [BG], Theorem 1.6.8]. □

Proposition 1.10. (Comparison between $h(j(E))$ and $h^{\mathrm{Fal}}(E)$, I) *Let F be a number field; E an elliptic curve over F that has* **semi-stable reduction** *over $\mathcal{O}_F$. Then, in the notation of Definitions 1.1, (i); 1.7 [cf. also the discussion entitled "Curves" in §0], we have*

$$0 \;\leq\; \tfrac{1}{12}\cdot h(j(E)) - h^{\mathrm{Fal}}(E) \;\leq\; \tfrac{1}{2}\cdot\log(1 + h(j(E))) + 2.071.$$

Proof. This follows immediately from [Lbr], Proposition 3.1 [and the surrounding discussion]. □

Remark 1.10.1. In the notation of Proposition 1.10, we observe that

(a) the normalized degree [cf. [IUTchIV], Definition 1.9, (i)] of the [effective] arithmetic divisor determined by the *q-parameters* of E at the elements of $\mathbb{V}(F)^{\mathrm{non}}$

coincides with

(b) $h_{\mathrm{non}}(j(E))$.

Indeed, this follows immediately from [Silv1], Chapter VII, Proposition 5.5; the discussion at the beginning of [Silv2], Chapter V, §5. Moreover, we observe that both (a) and (b) are *unaffected* by passing to finite extensions of the number field F [cf. [GenEll], Remark 3.3.1]. In particular, the assumption [cf. the statement of Proposition 1.10] that E has *semi-stable reduction* over $\mathcal{O}_F$ is, in fact, *inessential*.

Lemma 1.11. (Linearization of logarithms) *Let $a \in \mathbb{R}_{>0}$ be a positive real number. Then we have*

$$0 \;\leq\; a - \log(a) - 1.$$

In particular, [by taking "a" to be $a\cdot(1+x)$] we have

$$\log(1+x) - a\cdot x \;\leq\; a - \log(a) - 1$$

for all nonnegative real $x \in \mathbb{R}_{\geq 0}$.

Proof. Lemma 1.11 is well-known and entirely elementary. □

Proposition 1.12. (Comparison between $h(j(E))$ and $h^{\mathrm{Fal}}(E)$, II) *Let $\xi \in \mathbb{R}_{>0}$ be a positive real number. Write*

$$C(\xi) \stackrel{\text{def}}{=} \tfrac{1}{2} \cdot \{\tfrac{\xi}{6(1+\xi)} - \log \tfrac{\xi}{6(1+\xi)} - 1\} + 2.071.$$

Then, in the notation of Proposition 1.10, we have

$$\tfrac{1}{12(1+\xi)} \cdot h(j(E)) - h^{\mathrm{Fal}}(E) \leq C(\xi).$$

Proof. Indeed, we have

$$\begin{aligned} & \tfrac{1}{12(1+\xi)} \cdot h(j(E)) - h^{\mathrm{Fal}}(E) \\ = \; & \left\{ \tfrac{1}{12} \cdot h(j(E)) - h^{\mathrm{Fal}}(E) \right\} - \tfrac{\xi}{12(1+\xi)} \cdot h(j(E)) \\ \leq \; & \tfrac{1}{2} \cdot \left\{ \log(1 + h(j(E))) - \tfrac{\xi}{6(1+\xi)} \cdot h(j(E)) \right\} + 2.071 \leq C(\xi) \end{aligned}$$

— where the first (respectively, second) inequality follows from Proposition 1.10 (respectively, Lemma 1.11, where we take "a" to be $\frac{\xi}{6(1+\xi)}$ and "x" to be $h(j(E))$). □

Definition 1.13. Let $\kappa \leq 1$ be a positive real number; Σ a finite subset of $\mathbb{V}(\mathbb{Q})$ such that $\mathbb{V}(\mathbb{Q})^{\mathrm{arc}} \subseteq \Sigma$. Write $\overline{\Sigma} \subseteq \mathbb{V}(\overline{\mathbb{Q}})$ for the inverse image of $\Sigma \subseteq \mathbb{V}(\mathbb{Q})$ via the natural restriction map $\mathbb{V}(\overline{\mathbb{Q}}) \twoheadrightarrow \mathbb{V}(\mathbb{Q})$. Recall the set of rational functions "A" of Lemma 1.6, (i). Then we shall write

$$\mathcal{K}_{\Sigma}(\kappa) \stackrel{\text{def}}{=} \{x \in \overline{\mathbb{Q}}^{\dagger} \mid \min_{w \in \overline{\Sigma}} \min_{a \in A} \{||a(x)||_w\} \geq \kappa\} \subseteq \overline{\mathbb{Q}}^{\dagger}$$

[cf. the discussion entitled "Numbers" in §0] and refer to $\mathcal{K}_{\Sigma}(\kappa)$ as a *compactly bounded subset* of $\overline{\mathbb{Q}}^{\dagger}$. Thus, the subset $\mathcal{K}_{\Sigma}(\kappa) \subseteq \overline{\mathbb{Q}}^{\dagger}$ is stabilized by the natural action of $\mathfrak{S}_3$ on $\overline{\mathbb{Q}}^{\dagger}$ [cf. Lemma 1.6, (i)].

Corollary 1.14. (Upper bounds for $h_{\mathrm{non}}(j(E))$) *In the notation of Proposition 1.12, let l be a prime number. Suppose that E admits an* ***l-cyclic*** *subgroup scheme [cf.* [GenEll]*, Lemma 3.5], and that l is* **prime** *to the* **local heights** *[cf.* [GenEll]*, Definition 3.3] of E at each of its places of [bad] multiplicative reduction [a condition that is satisfied, for instance, if l is $>$ these local heights]. Then the following hold:*

(i) *We have*

$$\tfrac{l}{12(1+\xi)} \cdot h_{\mathrm{non}}(j(E)) \leq h^{\mathrm{Fal}}(E) + \tfrac{1}{2}\log(l) + C(\xi).$$

In particular, by applying the first inequality of Proposition 1.10, we obtain that

$$\tfrac{l-(1+\xi)}{12(1+\xi)} \cdot h_{\mathrm{non}}(j(E)) \leq \tfrac{1}{12} \cdot h_{\mathrm{arc}}(j(E)) + \tfrac{1}{2}\log(l) + C(\xi).$$

(ii) *In the notation of Definitions 1.7, 1.13, suppose that*

$$\lambda \ \in \ \mathcal{K}_{\Sigma}(\kappa).$$

[Note that the issue of whether or not $\lambda \in \mathcal{K}_{\Sigma}(\kappa)$ does not depend on the choice of the particular element "λ" within the $\mathfrak{S}_3$-orbit of "λ" [cf. the final portion of Definition 1.13].] Then we have

$$\tfrac{l-(1+\xi)}{12(1+\xi)} \cdot h_{\mathrm{non}}(j(E)) \ \leq \ \tfrac{1}{2}\log(l) + C(\xi) - \tfrac{1}{4}\log(\kappa) + \tfrac{11}{12}\log(2).$$

Suppose, moreover, that $l \geq 10^{15}$. Then, by taking ξ to be 1, we obtain that

$$\begin{aligned} h_{\mathrm{non}}(j(E)) \ &\leq \ \tfrac{24}{l-2}\{\tfrac{1}{2}\log(l) + C(1) - \tfrac{1}{4}\log(\kappa) + \tfrac{11}{12}\log(2)\} \\ &\leq \ \tfrac{24}{l-2}\{\tfrac{1}{2}\log(l) + 2.86 - \tfrac{1}{4}\log(\kappa) + 0.64\} \\ &\leq \ 5 \cdot 10^{-13} - 6.01 \cdot 10^{-15}\log(\kappa) \end{aligned}$$

— where we apply the estimates $\frac{\log(l)}{l-2} \leq 3.46 \cdot 10^{-14}$, $\frac{6}{l-2} \leq 6.01 \cdot 10^{-15}$, $\frac{11}{12}\log(2) \leq 0.64$, and $C(1) \leq 2.86$.

(iii) *Suppose that $\mathbb{Q}(\lambda)$ is* **mono-complex**. *Then we have*

$$\tfrac{l-2(1+\xi)}{12(1+\xi)} \cdot h_{\mathrm{non}}(j(E)) \ \leq \ \tfrac{1}{2}\log(l) + C(\xi) + \tfrac{19}{12}\log(2).$$

Suppose, moreover, that $l \geq 10^{15}$. Then, by taking ξ to be 1, we obtain that

$$\begin{aligned} h_{\mathrm{non}}(j(E)) \ &\leq \ \tfrac{24}{l-4}\{\tfrac{1}{2}\log(l) + C(1) + \tfrac{19}{12}\log(2)\} \\ &\leq \ \tfrac{24}{l-4}\{\tfrac{1}{2}\log(l) + 2.86 + 1.1\} \\ &\leq \ 4.16 \cdot 10^{-13} + 0.96 \cdot 10^{-13} \ = \ 5.12 \cdot 10^{-13} \end{aligned}$$

— where we apply the estimates $\frac{\log(l)}{l-4} \leq 3.46 \cdot 10^{-14}$, $\frac{24}{l-4} \leq 2.41 \cdot 10^{-14}$, $\frac{19}{12}\log(2) \leq 1.1$, and $C(1) \leq 2.86$.

Proof. First, we consider assertion (i). Let $H \subseteq E$ be an *l-cyclic* subgroup scheme. Write $E_H \stackrel{\mathrm{def}}{=} E/H$. [In particular, E_H is *isogenous* to E, hence has *semi-stable reduction* at all $v \in \mathbb{V}(F)^{\mathrm{non}}$.] Thus, by applying the same arguments as those applied in the proof of [GenEll], Lemma 3.5, we obtain the following *equality*:

$$h_{\mathrm{non}}(j(E_H)) \ = \ l \cdot h_{\mathrm{non}}(j(E))$$

[cf. also Remark 1.10.1]. On the other hand, it follows from the discussion entitled "Curves" in §0; [Falt], Lemma 5, that we have the following *inequality*:

$$h^{\mathrm{Fal}}(E_H) \ \leq \ h^{\mathrm{Fal}}(E) + \tfrac{1}{2}\log(l).$$

In light of the above equality and inequality, assertion (i) follows from Proposition 1.12.

Next, we consider assertion (ii). Note that, since $\lambda \in \mathcal{K}_{\Sigma}(\kappa)$, for each $v \in \mathbb{V}(\mathbb{Q}(\lambda))^{\mathrm{arc}}$, we have:

$$\max\{||\lambda||_v, ||\lambda||_v^{-1}\} \ \leq \ \kappa^{-1}; \qquad \max\{||\lambda - 1||_v, ||\lambda - 1||_v^{-1}\} \ \leq \ \kappa^{-1};$$
$$\max\{||\lambda - 1||_v \cdot ||\lambda||_v^{-1}, ||\lambda||_v \cdot ||\lambda - 1||_v^{-1}\} \ \leq \ \kappa^{-1}.$$

Thus, we conclude from Proposition 1.8, (ii), that

$$\begin{aligned} h_{\mathrm{arc}}(j(E)) - 11\log(2) &\leq h_{\mathrm{arc}}^{\mathfrak{S}\text{-tor}}(E) \\ &\leq \tfrac{1}{[\mathbb{Q}(\lambda):\mathbb{Q}]} \sum_{v \in \mathbb{V}(\mathbb{Q}(\lambda))^{\mathrm{arc}}} [\mathbb{Q}(\lambda)_v : \mathbb{R}] \cdot \log(\kappa^{-3}) \\ &= \log(\kappa^{-3}). \end{aligned}$$

Assertion (ii) then follows immediately from the second inequality of assertion (i). Finally, assertion (iii) follows immediately from the second inequality of assertion (i) and Proposition 1.9, (ii). □

2. Auxiliary Numerical Results

In the present section, we recall

- a *numerical result* concerning the *j-invariants* of certain *special elliptic curves* over fields of characteristic zero;
- certain *effective versions* of the prime number theorem.

These results will be applied in §5.

Proposition 2.1. (j-invariants of arithmetic elliptic curves) *Let F be a field of characteristic zero; E an elliptic curve over F. Suppose that the hyperbolic curve obtained by removing the origin from E is* **"arithmetic"**, *i.e.,* **fails to admit an $\boldsymbol{F}$-core** *[cf.* [CanLift]*, Remark 2.1.1]. Then the j-invariant $j(E)$ of E coincides with one of the following:*

- $\frac{488095744}{125} = 2^{14} \cdot 31^3 \cdot 5^{-3}$,
- $\frac{1556068}{81} = 2^2 \cdot 73^3 \cdot 3^{-4}$,
- $1728 = 2^6 \cdot 3^3$,
- 0.

Proof. Proposition 2.1 follows immediately from [Sijs], Table 4 [cf. also [Sijs], Lemma 1.1.1; [CanLift], Proposition 2.7]. □

Proposition 2.2. (Effective versions of the prime number theorem) *For $x \in \mathbb{R}_{\geq 2}$, write*

$$\pi(x) \stackrel{\text{def}}{=} \sharp\{p \in \mathfrak{Primes} \mid p \leq x\};$$

$$\theta(x) \stackrel{\text{def}}{=} \sum_{p \in \mathfrak{Primes};\ p \leq x} \log(p).$$

Set

$$\eta_{\mathrm{prm}} \stackrel{\text{def}}{=} 5 \cdot 10^{20}; \qquad \xi_{\mathrm{prm}} \stackrel{\text{def}}{=} 10^{15}.$$

Then the following hold:

(i) *For any real number* $x \geq \eta_{\mathrm{prm}}$*, it holds that*

$$\pi(x) \ \leq \ 1.022 \cdot \tfrac{x}{\log(x)}$$

[cf. [IUTchIV]*, Proposition 1.6].*

(ii) *For any real number* $x \geq \xi_{\mathrm{prm}}$*, it holds that*

$$|\theta(x) - x| \ \leq \ 0.00071 \cdot x$$

In particular, if $\mathcal{A}$ *is a finite subset of* $\mathfrak{Primes}$*, and we write*

$$\theta_{\mathcal{A}} \ \stackrel{\text{def}}{=} \ \sum_{p \in \mathcal{A}} \log(p)$$

[where we take the sum to be 0 *if* $\mathcal{A} = \emptyset$*], then there exists a prime number* $p \notin \mathcal{A}$ *such that*

$$p \ \leq \ (1 - 0.00071)^{-1} \cdot (\theta_{\mathcal{A}} + \xi_{\mathrm{prm}}) \ \leq \ 1.00072 \cdot (\theta_{\mathcal{A}} + \xi_{\mathrm{prm}})$$

[cf. [IUTchIV]*, Proposition 2.1, (ii)].*

Proof. First, we consider assertion (i). Observe that $\log(x) \geq \log(\eta_{\mathrm{prm}}) \geq 47.66 \geq \frac{1.17}{0.0246}$. Thus, it holds that

$$\pi(x) \ \leq \ \tfrac{x}{\log(x) - 1 - \frac{1.17}{\log(x)}} \ \leq \ \tfrac{x}{\log(x) - 1.0246}$$

[cf. [Ax1], Corollary 3.4; [Ax2]]. Therefore, we conclude that

$$1.022 \cdot \tfrac{x}{\log(x)} \ \geq \ \tfrac{x}{\log(x) - 1.0246} \ \geq \ \pi(x).$$

Next, we consider assertion (ii). Observe that $\log(x) \geq \log(\xi_{\mathrm{prm}}) \geq 34.53$. Then since $\frac{0.0242269}{\log(x)} \leq 0.00071$, assertion (ii) follows immediately from [RS], Theorem 7. □

3. $\boldsymbol{\mu}_6$-Theory for [EtTh]

In the present section, we introduce a slightly modified version of the notion of an *étale theta function of standard type* [cf. Definitions 3.3, 3.5], a notion which plays a central role in the theory developed in [EtTh]. We then proceed to discuss how the adoption of such a modified version of the notion of an étale theta function of standard type affects the theory developed in [EtTh].

We begin with certain elementary observations concerning *roots of unity* and *theta functions*.

Lemma 3.1. (Group actions on primitive roots of unity) *Let* $n \geq 2$ *be an* **even** *integer;* k *an algebraically closed field of characteristic zero. Write* $\boldsymbol{\mu}_{2n}^{\times} \subseteq k^{\times}$ *for the set of* **primitive $2n$-th roots of unity** *in* k*;* $\mathrm{Aut}(\boldsymbol{\mu}_{2n}^{\times})$ *for the group of automorphisms of the set* $\boldsymbol{\mu}_{2n}^{\times}$*;* $\Gamma_{-} \subseteq \mathrm{Aut}(\boldsymbol{\mu}_{2n}^{\times})$ *(respectively,* $\Gamma^{-} \subseteq \mathrm{Aut}(\boldsymbol{\mu}_{2n}^{\times})$*) for the subgroup of cardinality two generated by the automorphism of* $\boldsymbol{\mu}_{2n}^{\times}$ *defined as follows:* $\forall \zeta \in \boldsymbol{\mu}_{2n}^{\times}$*,*

$$\zeta \ \mapsto \ -\zeta \quad (\textit{respectively,} \ \ \zeta \ \mapsto \ \zeta^{-1}).$$

[Note that since n is even, it follows that $-\zeta \in \boldsymbol{\mu}_{2n}^{\times}$.] Then the following conditions are equivalent:

(1) $n \in \{2, 4, 6\}$.

(2) *The action of* $\Gamma_- \times \Gamma^-$ *on* $\boldsymbol{\mu}_{2n}^{\times}$ *is* **transitive**.

Proof. The fact that (1) $\Rightarrow$ (2) is immediate from the definitions. Thus, it remains to verify that (2) $\Rightarrow$ (1). First, we observe that the *transitivity* of the action of the group $\Gamma_- \times \Gamma^-$ [whose cardinality is four] on $\boldsymbol{\mu}_{2n}^{\times}$ implies that $\sharp(\boldsymbol{\mu}_{2n}^{\times}) \leq 4$. In light of this observation, one verifies easily that

$$n \in \{1, 2, 3, 4, 5, 6\}.$$

Since n is *even*, we thus conclude that $n \in \{2, 4, 6\}$. This completes the proof of Lemma 3.1. □

Proposition 3.2. (Theta values at primitive 12-th roots of unity) *In the notation of* [EtTh]*, Proposition 1.4: Suppose that* $\ddot{K}$ *contains a primitive* 12*-th root of unity* ζ_{12}*. Thus, we note that the set of primitive* 12*-th roots of unity in* $\ddot{K}$ *coincides with the set*

$$\{\zeta_{12},\ \zeta_{12}^5,\ \zeta_{12}^7,\ \zeta_{12}^{11}\} \ \subseteq\ \ddot{K}.$$

Recall the **theta function** $\ddot{\Theta}$ *of* [EtTh]*, Proposition 1.4,*

$$\ddot{\Theta}(U) \ =\ q_X^{-\frac{1}{8}} \cdot \sum_{n \in \mathbb{Z}} (-1)^n \cdot q_X^{\frac{1}{2}(n+\frac{1}{2})^2} \cdot \ddot{U}^{2n+1},$$

which satisfies the relations $\ddot{\Theta}(\ddot{U}) = -\ddot{\Theta}(\ddot{U}^{-1}) = -\ddot{\Theta}(-\ddot{U})$ *[cf.* [EtTh]*, Proposition 1.4, (ii)]. Then the following hold:*

(i) *We have*

$$\ddot{\Theta}(\zeta_{12}),\ \ddot{\Theta}(\zeta_{12}^5),\ \ddot{\Theta}(\zeta_{12}^7),\ \ddot{\Theta}(\zeta_{12}^{11}) \ \in\ \{\ddot{\Theta}(\zeta_{12}),\ -\ddot{\Theta}(\zeta_{12})\}.$$

(ii) *We have* $\ddot{\Theta}(\zeta_{12}) \in \mathcal{O}_{\ddot{K}}^{\times}$.

Proof. Assertion (i) follows immediately from Lemma 3.1 and [EtTh], Proposition 1.4, (ii). Assertion (ii) follows immediately from the fact that $\zeta_{12} - \zeta_{12}^{-1} \in \mathcal{O}_{\ddot{K}}^{\times}$ [cf. the equality $-(\zeta_{12} - \zeta_{12}^{-1})^2 = 1$]. □

Remark 3.2.1. Lemma 3.1 and Proposition 3.2 arose from *observations* due to Porowski. These observations are, in some sense, the *starting point* of the theory developed in the present paper.

In the remainder of the present §3, we consider a slightly modified version of [EtTh] based on *"étale theta functions of* $\boldsymbol{\mu}_6$*-standard type"*.

Definition 3.3. In the notation of [EtTh], Definition 1.9, suppose that K contains a *primitive* 12*-th root of unity*. Note that the primitive 12-th roots of unity in K determine precisely four 12*-torsion points*

$$\{\tau_1,\ \tau_2,\ \tau_3,\ \tau_4\}$$

of [the underlying elliptic curve of] $\dot{X}$ whose restriction to the special fiber lies in the interior of [i.e., avoids the nodes of] the *unique irreducible component* of the special fiber.

(i) We shall refer to either of the following four sets of values [cf. [EtTh], Proposition 1.4, (iii)] of $\ddot{\eta}^{\Theta,\underline{\mathbb{Z}}}$

$$\ddot{\eta}^{\Theta,\underline{\mathbb{Z}}}|_{\tau_1},\ \ \ddot{\eta}^{\Theta,\underline{\mathbb{Z}}}|_{\tau_2},\ \ \ddot{\eta}^{\Theta,\underline{\mathbb{Z}}}|_{\tau_3},\ \ \ddot{\eta}^{\Theta,\underline{\mathbb{Z}}}|_{\tau_4}\ \ \subseteq\ \ K^{\times}$$

as a $\boldsymbol{\mu}_6$*-standard set of values of* $\ddot{\eta}^{\Theta,\underline{\mathbb{Z}}}$.

(ii) If $\ddot{\eta}^{\Theta,\underline{\mathbb{Z}}}$ satisfies the property that the *unique* value $\in K^{\times}$ [cf. Proposition 3.2, (i); Remark 4.2.3, (vi); [IUTchII], Remark 2.5.1, (ii)] of *maximal order* [i.e., relative to the valuation on K] of some $\boldsymbol{\mu}_6$-standard set of values of $\ddot{\eta}^{\Theta,\underline{\mathbb{Z}}}$ is equal to ± 1, then we shall say that $\ddot{\eta}^{\Theta,\underline{\mathbb{Z}}}$ is *of* $\boldsymbol{\mu}_6$*-standard type*.

Remark 3.3.1. By applying Definition 4.3, together with a similar argument to the argument applied in the proof of [EtTh], Theorem 1.10, one may prove a "$\boldsymbol{\mu}_6$-version" of [EtTh], Theorem 1.10, i.e., the assertion obtained by replacing, in [EtTh], Theorem 1.10, (iii),

$$\text{"odd"}\ \longrightarrow\ \text{"arbitrary"}$$

[cf. Proposition 3.2, (ii); [IUTchIV], Remark 1.10.6, (ii)]. Note that, in the notation of [EtTh], Theorem 1.10,

> *the dual graphs of the special fibers of the various coverings of* C_α, C_β *are somewhat more complicated in the case where* $p \in \{2, 3\}$.

On the other hand, since one may still reconstruct the dual graphs group-theoretically, this will not affect the proof of the $\boldsymbol{\mu}_6$-version of [EtTh], Theorem 1.10, in any significant way.

Definition 3.4. Let $l \geq 1$ be an integer *coprime to* 6. In the notation of [EtTh], §1, suppose that

- the *residue characteristic* of K is *arbitrary*;
- $K = \ddot{K}$;
- K contains a *primitive* 12*-th root of unity* ζ_{12}

[cf. [EtTh], Definition 1.7, and the preceding discussion; [EtTh], Definition 2.5].

(i) Suppose, in the situation of [EtTh], Definitions 2.1, 2.3, that the quotient $\overline{\Pi}_X^{\mathrm{ell}} \twoheadrightarrow Q$ *factors* through the natural quotient $\underline{\Pi}_X \twoheadrightarrow \overline{\mathbb{Z}}$ determined by the quotient $\underline{\Pi}_X^{\mathrm{tp}} \twoheadrightarrow \mathbb{Z}$ discussed at the beginning of [EtTh], §1, and that the *choice of a splitting* of $\overline{D}_x \to G_K$ [cf. [EtTh], Proposition 2.2, (ii)] that determined the covering $\underline{\underline{X}}^{\log} \to \underline{X}^{\log}$ is *compatible* with the "$\{\pm 1\}$-*structure*" of the $\boldsymbol{\mu}_6$-version of Theorem 1.10, (iii), of Remark 3.3.1. Then we shall say that the orbicurve of type $(1, l\text{-tors})$ (respectively, $(1, l\text{-tors}^{\Theta})$; $(1, l\text{-tors})_{\pm}$; $(1, l\text{-tors}^{\Theta})_{\pm}$) under consideration is *of type* $(1, \mathbb{Z}/l\mathbb{Z})$ (respectively, $(1, (\mathbb{Z}/l\mathbb{Z})^{\Theta})$; $(1, \mathbb{Z}/l\mathbb{Z})_{\pm}$; $(1, (\mathbb{Z}/l\mathbb{Z})^{\Theta})_{\pm}$).

(ii) In the notation of the above discussion and the discussion at the end of [EtTh], §1, we shall refer to a smooth log orbicurve isomorphic to the smooth log orbicurve

$$\underline{\dot{X}}^{\log}(\text{respectively}, \underline{\underline{\dot{X}}}^{\log}; \underline{\dot{C}}^{\log}; \underline{\underline{\dot{C}}}^{\log})$$

obtained by taking the composite of the covering

$$\underline{X}^{\log} \text{ (respectively}, \underline{\underline{X}}^{\log}; \underline{C}^{\log}; \underline{\underline{C}}^{\log})$$

of $C^{\log}$ with the covering $\dot{C}^{\log} \to C^{\log}$, as being *of type* $(1, \boldsymbol{\mu}_2 \times \mathbb{Z}/l\mathbb{Z})$ (respectively, $(1, \boldsymbol{\mu}_2 \times (\mathbb{Z}/l\mathbb{Z})^{\Theta})$; $(1, \boldsymbol{\mu}_2 \times \mathbb{Z}/l\mathbb{Z})_{\pm}$; $(1, \boldsymbol{\mu}_2 \times (\mathbb{Z}/l\mathbb{Z})^{\Theta})_{\pm}$).

Remark 3.4.1. In the "$\boldsymbol{\mu}_6$-version" of [EtTh], Remark 2.5.1, the portion concerning "$\underline{\dot{C}}$" should be *eliminated*.

Definition 3.5. In the notation of Definition 3.3 and the discussion preceding of [EtTh], Definition 2.7, if $\ddot{\eta}^{\Theta,\mathbb{Z}}$ is of $\boldsymbol{\mu}_6$-standard type, then we shall also refer to $\ddot{\eta}^{\Theta,l\cdot\mathbb{Z}}$, $\underline{\ddot{\eta}}^{\Theta,l\cdot\mathbb{Z}}$, $\ddot{\eta}^{\Theta,l\cdot\mathbb{Z}\times\boldsymbol{\mu}_2}$, $\underline{\ddot{\eta}}^{\Theta,l\cdot\mathbb{Z}\times\boldsymbol{\mu}_2}$, $\ddot{\eta}^{\Theta,\mathbb{Z}\times\boldsymbol{\mu}_2}$ as being of $\boldsymbol{\mu}_6$-*standard type*.

Remark 3.5.1. By applying Definitions 3.3, 3.4, 3.5 [cf. also Remarks 3.3.1, 3.4.1], the exposition of [EtTh], §1, §2, goes through without essential change under the *assumptions stated in the first paragraph of Definition 3.4*, with the following *exception*: In the "$\boldsymbol{\mu}_6$-versions" of [EtTh], Proposition 2.12; [EtTh], Remark 2.12.1, the portions concerning the hyperbolic orbicurves whose notation contains a "$\dot{}$" [i.e., a single "overline dot"] should be *eliminated*.

Remark 3.5.2. By applying Definitions 3.3, 3.4, 3.5 [cf. also Remarks 3.3.1, 3.4.1, 3.5.1], the exposition of [EtTh], §3, §4, goes through without essential change under the *assumptions stated in the first paragraph of Definition 3.4*, with the following *exception*: In the "$\boldsymbol{\mu}_6$-version" of [EtTh], Example 3.9, the portions concerning the hyperbolic orbicurves whose notation contains a "$\dot{}$" [i.e., a single "overline dot"] should be *eliminated*.

Remark 3.5.3. By applying Definitions 3.3, 3.4, 3.5 [cf. also Remarks 3.3.1, 3.4.1, 3.5.1, 3.5.2], the exposition of [EtTh], §5, goes through without essential change under the *assumptions stated in the first paragraph of Definition 3.4*, with the following *exceptions*:

(i) Throughout the "$\boldsymbol{\mu}_6$-version" of [EtTh], §5, the portions concerning the hyperbolic orbicurves whose notation contains a "$\dot{}$" [i.e., a single "overline dot"] should be *eliminated*.

(ii) In the "$\boldsymbol{\mu}_6$-version" of the statement and proof of [EtTh], Proposition 5.3, as well as the preceding discussion, the notation "$\ddot{\mathcal{Y}}$" should be replaced by "$\mathcal{Y}$".

(iii) In the "$\boldsymbol{\mu}_6$-version" of [EtTh], Theorem 5.7, as well as the "$\boldsymbol{\mu}_6$-version" of the remainder of [EtTh], §5, the following modification should be made:

$$\text{“}\ddot{\Theta}(\sqrt{-1})^{-1} \cdot \ddot{\Theta}\text{”} \longrightarrow \text{“}\ddot{\Theta}(\zeta_{12})^{-1} \cdot \ddot{\Theta}\text{”}.$$

4. $\boldsymbol{\mu}_6$-Theory for [IUTchI-III]

In the present section, we introduce a slightly modified version of the notion of *initial* Θ*-data* [cf. Definitions 4.1], a notion which plays a central role in the theory developed in [IUTchI-IV]. We then proceed to discuss how the adoption of such a modified version of the notion of initial Θ-data affects the theory developed in [IUTchI-III].

Definition 4.1. We shall refer to as $\boldsymbol{\mu}_6$*-initial* Θ*-data* any collection of data

$$(\overline{F}/F,\ X_F,\ l,\ \underline{C}_K,\ \underline{\mathbb{V}},\ \mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}},\ \underline{\epsilon})$$

satisfying the following conditions:

- [IUTchI], Definition 3.1, (a), (c), (d);
- The "$\boldsymbol{\mu}_6$-version" of [IUTchI], Definition 3.1, (b), i.e., the condition obtained by replacing, in [IUTchI], Definition 3.1, (b),

  $$\text{“}\textit{odd}\text{”} \longrightarrow \text{“}\textit{arbitrary}\text{”};$$

- The "$\boldsymbol{\mu}_6$-versions" of [IUTchI], Definition 3.1, (e), (f), i.e., the conditions obtained by replacing, in [IUTchI], Definition 3.1, (e), (f),

  $$\text{“[EtTh], Definition 2.5, (i)”} \longrightarrow \text{“Definition 3.4, (i)”}$$

  [cf. Remark 4.1.1 below].

Remark 4.1.1. In the notation of Definition 4.1, write E_F for the elliptic curve over F determined by X_F [so $X_F \subseteq E_F$]. Then since $\sqrt{-1} \in F$ [cf. [IUTchI], Definition 3.1, (a)], and, moreover, the *3-torsion points* of E_F are *rational* over F [cf. [IUTchI], Definition 3.1, (b)], we conclude that F contains a *primitive* 12*-th root of unity* ζ_{12} [cf. the conditions in the first display of Definition 3.4].

Remark 4.1.2. By applying Definitions 3.3, 3.4, 3.5, 4.1 [cf. also Remarks 3.3.1, 3.4.1, 3.5.1, 3.5.2, 3.5.3, 4.1.1], the exposition of [IUTchI], §3, goes through without essential change, with the following *exceptions*: In the "$\boldsymbol{\mu}_6$-version" of [IUTchI], Example 3.2, the following modifications should be made:

- In [IUTchI], Example 3.2, (ii),
$$\text{“}\sqrt{-1}\text{”} \longrightarrow \text{“}\zeta_{12}\text{”};$$
- In [IUTchI], Example 3.2, (iv),
$$\begin{aligned} \text{“}\sqrt{-q_{\underline{v}}}\text{”} &\longrightarrow \text{“}\zeta_{12}\sqrt{q_{\underline{v}}}\text{”};\\ \text{“}\boldsymbol{\mu}_{2l}(\mathbb{T}_{\underline{\underline{X}}_{\underline{v}}})\text{-multiple”} &\longrightarrow \text{“}\boldsymbol{\mu}_{6l}(\mathbb{T}_{\underline{\underline{X}}_{\underline{v}}})\text{-multiple”};\\ \text{“}\boldsymbol{\mu}_{2l}(-)\textit{-orbit}\text{”} &\longrightarrow \text{“}\boldsymbol{\mu}_{6l}(-)\textit{-orbit}\text{”}. \end{aligned}$$
- In [IUTchI], Example 3.2, (v),
$$\text{“}\boldsymbol{\mu}_{2l}(-)\textit{-orbit}\text{”} \longrightarrow \text{“}\boldsymbol{\mu}_{6l}(-)\textit{-orbit}\text{”}.$$

Remark 4.1.3. By applying Definitions 3.3, 3.4, 3.5, 4.1 [cf. also Remarks 3.3.1, 3.4.1, 3.5.1, 3.5.2, 3.5.3, 4.1.1, 4.1.2], the exposition of [IUTchI], §4, §5, §6, goes through without essential change, with the following *exceptions*: In the "$\boldsymbol{\mu}_6$-version" of [IUTchI], Example 4.4, the following modifications should be made:

- In [IUTchI], Example 4.4, (i),
$$\text{“the } \textit{unique torsion point of order } 2\text{”} \longrightarrow \text{“a } \textit{torsion point of order } 6\text{”}.$$
Thus, throughout the $\boldsymbol{\mu}_6$-version of [IUTchI], Example 4.4, (i) — and indeed throughout the remainder of the "$\boldsymbol{\mu}_6$-version" of [IUTchI-IV] — "μ_-" is to be regarded as being allowed to *vary* among the *torsion points of order* 6 that satisfy the condition stated in the initial definition of "μ_-", with the following *exception*: In [IUTchI], Remark 5.2.3, the notation "μ_-" is to be understood in the original "non-$\boldsymbol{\mu}_6$" sense, i.e., as the *unique torsion point of order* 2 discussed in the original "non-$\boldsymbol{\mu}_6$" version of [IUTchI], Example 4.4, (i).
- In [IUTchI], Example 4.4, (i),
$$\begin{aligned} \text{“}\textbf{evaluation points}\text{”} &\longrightarrow \text{“}\boldsymbol{\mu}_{6l}\textbf{-evaluation points}\text{”};\\ \text{“}\textbf{evaluation sections}\text{”} &\longrightarrow \text{“}\boldsymbol{\mu}_{6l}\textbf{-evaluation sections}\text{”};\\ \text{“}\boldsymbol{\mu}_{2l}\text{-orbit”} &\longrightarrow \text{“}\boldsymbol{\mu}_{6l}\text{-orbit”}. \end{aligned}$$

Definition 4.2. Suppose that we are in the situation of [IUTchII], Remark 1.4.1 [cf. also Remark 4.2.2 below]. Write

$$\underline{\tau} \in \underline{X}_k(k)$$

for a *torsion point of order* 6 whose closure in any stable model of $\underline{X}_k$ over $\mathcal{O}_k$ intersects the same irreducible component of the special fiber of the stable model as the zero cusp [cf. Remark 4.1.3]. Since k contains a *primitive* $12l$*-th root of unity* [cf. Remark 4.2.2 below], it follows from the definition of an "étale theta function of $\boldsymbol{\mu}_6$-standard type" [cf. Definitions 3.3, (ii); 3.5] that *there exists a rational point*

$$\underline{\tau}_{\underline{\underline{\ddot{Y}}}} \in \underline{\underline{\ddot{Y}}}_k(k)$$

such that $\underline{\tau}_{\underline{\underline{\ddot{Y}}}} \mapsto \underline{\tau}$. Write

$$D_{\underline{\tau}} \subseteq \Pi^{\mathrm{tp}}_{\underline{\underline{\ddot{Y}}}_k}$$

for the *decomposition group* of $\underline{\tau}_{\underline{\underline{\ddot{Y}}}}$ [which is well-defined up to $\Delta^{\mathrm{tp}}_{\underline{\underline{\ddot{Y}}}_k}$-conjugacy]. We shall refer to either of the pairs

$$(\iota_{\underline{\underline{\ddot{Y}}}} \in \mathrm{Aut}(\underline{\underline{\ddot{Y}}}_k), \underline{\tau}_{\underline{\underline{\ddot{Y}}}}); \quad (\iota_{\underline{\underline{\ddot{Y}}}} \in \mathrm{Aut}(\Pi^{\mathrm{tp}}_{\underline{\underline{\ddot{Y}}}_k})/\mathrm{Inn}(\Delta^{\mathrm{tp}}_{\underline{\underline{\ddot{Y}}}_k}), D_{\underline{\tau}})$$

as a $\boldsymbol{\mu}_6$*-pointed inversion automorphism*. Again, we recall from Definitions 3.3, (ii); 3.5, that

> *an "étale theta function of $\boldsymbol{\mu}_6$-standard type" is defined precisely by the condition that its restriction to $D_{\underline{\tau}}$ be a $2l$-th root of unity.*

Remark 4.2.1. By applying Definitions 3.3, 3.4, 3.5, 4.1, 4.2 [cf. also Remarks 3.3.1, 3.4.1, 3.5.1, 3.5.2, 3.5.3, 4.1.1, 4.1.2, 4.1.3], the exposition of the Abstract and Introduction of [IUTchII] goes through without essential change, with the following *exceptions*:

(i) In the "$\boldsymbol{\mu}_6$-version" of the Abstract of [IUTchII], the following modification should be made:

$$\text{"2-torsion point"} \longrightarrow \text{"6-torsion point"}.$$

(ii) In the "$\boldsymbol{\mu}_6$-version" of the first display and the discussion immediately following the first display of the Introduction of [IUTchII], the following modifications should be made:

$$\text{"}\Big(\sqrt{-1}\cdot\sum_{m\in\mathbb{Z}} q_{\underline{v}}^{\frac{1}{2}(m+\frac{1}{2})^2}\Big)\text{"} \longrightarrow \text{"}\Big(\sqrt{-1}\cdot\sum_{m\in\mathbb{Z}} \zeta_3^{m+2} q_{\underline{v}}^{\frac{1}{2}(m+\frac{1}{2})^2}\Big)\text{"};$$

$$\text{"2-torsion point"} \longrightarrow \text{"6-torsion point } -\zeta_3\text{"};$$

$$\text{"}2l\text{-}th \textit{ root of unity"} \longrightarrow \text{"}6l\text{-}th \textit{ root of unity"}.$$

(iii) In the "$\boldsymbol{\mu}_6$-version" of the paragraph of the Introduction of [IUTchII] that begins "**Constant multiple rigidity**", the following modifications should be made:

"*[2-]torsion point*" $\longrightarrow$ "*[6-]torsion point*";
"$2l$-th roots of unity" $\longrightarrow$ "$6l$-th roots of unity".

Remark 4.2.2. By applying Definitions 3.3, 3.4, 3.5, 4.1, 4.2 [cf. also Remarks 3.3.1, 3.4.1, 3.5.1, 3.5.2, 3.5.3, 4.1.1, 4.1.2, 4.1.3], the exposition of [IUTchII], §1, goes through without essential change, with the following *exceptions*:

(i) In the "$\boldsymbol{\mu}_6$-version" of the discussion preceding [IUTchII], Definition 1.1, the following modifications should be made:

"*odd* prime number" $\longrightarrow$ "prime number ≥ 5";
"of *odd residue*" $\longrightarrow$ "of *arbitrary residue*";
"$4l$*-th root*" $\longrightarrow$ "$12l$*-th root*".

(ii) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Remark 1.12.2, (ii), the following modifications should be made:

"the 2-torsion point "μ_-" of [IUTchI], Example 4.4, (i)"
$\longrightarrow$ "a 6-torsion point "$\underline{\tau}$" as in Definition 4.2";

"the 2-torsion point "μ_-" are reconstructed"
$\longrightarrow$ "6-torsion points "$\underline{\tau}$" are reconstructed".

(iii) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Remark 1.12.2, (iii), the following modification should be made:

"where we recall that ... is assumed to be"
$\longrightarrow$ "where we assume, for simplicity, that ... is".

(iv) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Remark 1.12.4, the following modification should be made:

" *the point "μ_-"* " $\longrightarrow$ " 6*-torsion points "$\underline{\tau}$"* ".

Remark 4.2.3. By applying Definitions 3.3, 3.4, 3.5, 4.1, 4.2 [cf. also Remarks 3.3.1, 3.4.1, 3.5.1, 3.5.2, 3.5.3, 4.1.1, 4.1.2, 4.1.3, 4.2.2], the exposition of [IUTchII], §2, goes through without essential change, with the following *exceptions*:

(i) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Corollary 2.4, (ii), (b), the following modifications should be made:

"$D^{\delta}_{\mu_-}$" $\longrightarrow$ "$D^{\delta}_{\underline{\tau}}$";

"the torsion point "μ_-" of Remark 1.4.1, (i), (ii)"

$\longrightarrow$ "some torsion point "$\underline{\tau}$" as in Definition 4.2".

(ii) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Corollary 2.4, (ii), (c), the following modifications should be made:

$$\text{"}D^{\delta}_{t,\mu_-}\text{"} \longrightarrow \text{"}D^{\delta}_{t,\underline{\tau}}\text{"};$$
$$\text{"[IUTchI], Example 4.4, (i)"} \longrightarrow \text{"Remark 4.1.3"};$$
$$\text{"}\mu_-\text{-translate"} \longrightarrow \text{"}\underline{\tau}\text{-translate"}.$$

(iii) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Corollary 2.5, (ii), the following modifications should be made:

$$\text{"}D^{\delta}_{t,\mu_-}\text{"} \longrightarrow \text{"}D^{\delta}_{t,\underline{\tau}}\text{"};$$
$$\text{"yield } \boldsymbol{\mu}_{2l}\text{-,"} \longrightarrow \text{"yield } \boldsymbol{\mu}_{6l}\text{-,"}.$$

(iv) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Corollary 2.5, (iii), the following modification should be made:

$$\text{"}\boldsymbol{\mu}_{2l}\text{"} \longrightarrow \text{"}\boldsymbol{\mu}_{6l}\text{"}.$$

(v) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Remark 2.5.1, (i), the following modification should be made:

$$\text{"}\boldsymbol{\mu}_{2l}\text{"} \longrightarrow \text{"}\boldsymbol{\mu}_{6l}\text{"}.$$

(vi) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Remark 2.5.1, (ii), the following modification should be made:

$$\text{"}\pm\sqrt{-1}\text{"} \longrightarrow \text{"}\pm\zeta_{12}^{\pm 1}\text{"}.$$

(vii) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Remark 2.5.1, (iii), the following modification should be made:

$$\text{"}\boldsymbol{\mu}_{2l}\text{-orbit"} \longrightarrow \text{"}\boldsymbol{\mu}_{6l}\text{-orbit"}.$$

(viii) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Remark 2.5.2, (i), the following modification should be made:

$$\text{"}D^{\gamma_1}_{t,\mu_-}\text{"} \longrightarrow \text{"}D^{\gamma_1}_{t,\underline{\tau}}\text{"}.$$

(ix) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Corollary 2.6, (ii), the following modifications should be made:

$$\text{"}\boldsymbol{\mu}_{2l}\text{"} \longrightarrow \text{"}\boldsymbol{\mu}_{6l}\text{"};$$
$$\text{"}D^{\delta}_{t,\mu_-}\text{"} \longrightarrow \text{"}D^{\delta}_{t,\underline{\tau}}\text{"}.$$

(x) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Remark 2.6.3, (i), the following modification should be made:

$$\text{"}\mu_-\text{-translates"} \longrightarrow \text{"}\underline{\tau}\text{-translates"}.$$

(xi) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Corollary 2.8, (i), the following modifications should be made:

$$\begin{array}{rcl} \text{“}D^{\delta}_{t,\mu_-}\text{”} & \longrightarrow & \text{“}D^{\delta}_{t,\underline{\tau}}\text{”}; \\ \text{“yield } \boldsymbol{\mu}_{2l}\text{-,”} & \longrightarrow & \text{“yield } \boldsymbol{\mu}_{6l}\text{-,”}. \end{array}$$

(xii) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Corollary 2.8, (ii), the following modification should be made:

$$\text{“}\boldsymbol{\mu}_{2l}\text{”} \longrightarrow \text{“}\boldsymbol{\mu}_{6l}\text{”}.$$

(xiii) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Corollary 2.9, (i), the following modifications should be made:

$$\begin{array}{rcl} \text{“}D^{\delta}_{t,\mu_-}\text{”} & \longrightarrow & \text{“}D^{\delta}_{t,\underline{\tau}}\text{”}; \\ \text{“yield } \boldsymbol{\mu}_{2l}\text{-,”} & \longrightarrow & \text{“yield } \boldsymbol{\mu}_{6l}\text{-,”}. \end{array}$$

(xiv) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Corollary 2.9, (ii), the following modification should be made:

$$\text{“}\boldsymbol{\mu}_{2l}\text{”} \longrightarrow \text{“}\boldsymbol{\mu}_{6l}\text{”}.$$

Remark 4.2.4. By applying Definitions 3.3, 3.4, 3.5, 4.1, 4.2 [cf. also Remarks 3.3.1, 3.4.1, 3.5.1, 3.5.2, 3.5.3, 4.1.1, 4.1.2, 4.1.3, 4.2.2, 4.2.3], the exposition of [IUTchII], §3, goes through without essential change, with the following *exceptions*:

(i) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Corollary 3.5, (i), the following modification should be made:

$$\text{“}D^{\delta}_{t,\mu_-}\text{”} \longrightarrow \text{“}D^{\delta}_{t,\underline{\tau}}\text{”}.$$

(ii) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Corollary 3.5, (ii), the following modifications should be made:

$$\begin{array}{rcl} \text{“}(2l)^{l^*}\text{”} & \longrightarrow & \text{“}(6l)^{l^*}\text{”}; \\ \text{“}\Psi_{2l\cdot\xi}(\mathbb{M}^{\Theta}_*)\text{”} & \longrightarrow & \text{“}\Psi_{6l\cdot\xi}(\mathbb{M}^{\Theta}_*)\text{”}; \\ \text{“}\xi^{2l\cdot\mathbb{N}}\text{”} & \longrightarrow & \text{“}\xi^{6l\cdot\mathbb{N}}\text{”}; \\ \text{“}D^{\delta}_{t,\mu_-}\text{”} & \longrightarrow & \text{“}D^{\delta}_{t,\underline{\tau}}\text{”}; \\ \text{“}\Psi_{2l\cdot\xi_1}(\mathbb{M}^{\Theta}_*) = \Psi_{2l\cdot\xi_2}(\mathbb{M}^{\Theta}_*)\text{”} & \longrightarrow & \text{“}\Psi_{6l\cdot\xi_1}(\mathbb{M}^{\Theta}_*) = \Psi_{6l\cdot\xi_2}(\mathbb{M}^{\Theta}_*)\text{”}. \end{array}$$

(iii) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Remark 3.5.1, (i), the following modification should be made:

$$\text{“}D^{\delta}_{t,\mu_-}\text{”} \longrightarrow \text{“}D^{\delta}_{t,\underline{\tau}}\text{”}.$$

(iv) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Corollary 3.6, (ii), the following modification should be made:

$$\text{“}\Psi_{2l\cdot\xi}(-)\text{”} \longrightarrow \text{“}\Psi_{6l\cdot\xi}(-)\text{”}.$$

(v) In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Definition 3.8, (ii), (iii), the following modifications should be made:

$$\begin{array}{rcl} \text{“}\mathcal{F}_{2l\cdot\xi}(\mathbb{M}_*^{\Theta})\text{”} & \longrightarrow & \text{“}\mathcal{F}_{6l\cdot\xi}(\mathbb{M}_*^{\Theta})\text{”}; \\ \text{“}\mathcal{F}_{\mathcal{F}_{2l\cdot\xi}}({}^{\dagger}\underline{\underline{\mathcal{F}}}_{\underline{v}})\text{”} & \longrightarrow & \text{“}\mathcal{F}_{\mathcal{F}_{6l\cdot\xi}}({}^{\dagger}\underline{\underline{\mathcal{F}}}_{\underline{v}})\text{”}; \\ \text{“}\Psi_{2l\cdot\xi}(-)\text{”} & \longrightarrow & \text{“}\Psi_{6l\cdot\xi}(-)\text{”}. \end{array}$$

Remark 4.2.5. By applying Definitions 3.3, 3.4, 3.5, 4.1, 4.2 [cf. also Remarks 3.3.1, 3.4.1, 3.5.1, 3.5.2, 3.5.3, 4.1.1, 4.1.2, 4.1.3, 4.2.2, 4.2.3, 4.2.4], the exposition of [IUTchII], §4, goes through without essential change, with the following *exceptions*: In the "$\boldsymbol{\mu}_6$-version" of [IUTchII], Definition 4.9, (ii), the following modifications should be made:

$$\begin{array}{rcl} \text{“}2l\textit{-torsion subgroup}\text{”} & \longrightarrow & \text{“}6l\textit{-torsion subgroup}\text{”}; \\ \text{“}\boldsymbol{\mu}_{2l}({}^{\ddagger}A)\text{”} & \longrightarrow & \text{“}\boldsymbol{\mu}_{6l}({}^{\ddagger}A)\text{”}. \end{array}$$

Remark 4.2.6. By applying Definitions 3.3, 3.4, 3.5, 4.1, 4.2 [cf. also Remarks 3.3.1, 3.4.1, 3.5.1, 3.5.2, 3.5.3, 4.1.1, 4.1.2, 4.1.3, 4.2.2, 4.2.3, 4.2.4, 4.2.5], the exposition of [IUTchIII], §1, §2, §3, goes through without essential change, with the following *exceptions*:

(i) In the "$\boldsymbol{\mu}_6$-version" of [IUTchIII], Proposition 3.5, (ii), (c), the following modification should be made:

$$\text{“}2l\text{-torsion subgroup”} \longrightarrow \text{“}6l\text{-torsion subgroup”}.$$

(ii) In the "$\boldsymbol{\mu}_6$-version" of [IUTchIII], Remark 3.11.4, (i), the following modification should be made:

$$\text{“}2l\text{-th roots of unity”} \longrightarrow \text{“}6l\text{-th roots of unity”}.$$

(iii) In the "$\boldsymbol{\mu}_6$-version" of [IUTchIII], Fig. 3.4, the following modification should be made:

$$\text{“}\boldsymbol{\mu}_{2l}\text{”} \longrightarrow \text{“}\boldsymbol{\mu}_{6l}\text{”}.$$

5. $\boldsymbol{\mu}_6$-Theory for [IUTchIV]

In the present section, we first give explicit log-volume estimates for the "$\boldsymbol{\mu}_6$-version" of Θ-pilot objects [cf. Theorem 5.1; Corollary 5.2]. [We refer to [IUTchIV], Theorem 1.10; [IUTchIV], Corollary 2.2, (ii), (iii), for the original "non-$\boldsymbol{\mu}_6$" versions of these results.] Theorem 5.1 follows directly from the modified version of [IUTchI-III] discussed in §4 [cf. also §3], together with certain estimates from §2, while Corollary 5.2 is obtained by combining Theorem 5.1 with the theory of §1, §2. We then examine Corollary 5.2 in more detail in the case of *mono-complex number fields*; this yields an *effective version* of the *ABC inequality* over *mono-complex number fields* [cf. Theorem 5.3], as well as an *effective version* of a *conjecture of Szpiro* over the *field of rational numbers* [cf. Theorem 5.4]. As an application, we compute

an *explicit* integer $n_0 > 0$ such that for any prime number $p \geq n_0$, the *Fermat equation* $x^p + y^p = z^p$ does not have any positive integer solutions [cf. Corollary 5.8], i.e., we give an alternative approach, via fundamentally different techniques, to verifying an *effective asymptotic* version of *"Fermat's Last Theorem"*, as proven in [Wls]. We also apply the effective version of the ABC inequality that we obtain to a generalized version of the Fermat equation [cf. Corollary 5.9].

Theorem 5.1. (Log-volume estimates for the "μ_6-version" of Θ-pilot objects) *Fix a collection of* **μ_6-initial Θ-data** *[cf. Definition 4.1]. Suppose that we are in the situation of the "μ_6-version" of* [IUTchIII]*, Corollary 3.12 [cf. Remark 4.2.6], and that the elliptic curve E_F has* **good reduction** *at every place $\in \mathbb{V}(F)^{\mathrm{good}} \cap \mathbb{V}(F)^{\mathrm{non}}$ that does not divide $2 \cdot 3 \cdot 5 \cdot l$. In the notation of Definition 4.1, let us write $d_{\mathrm{mod}} \stackrel{\mathrm{def}}{=} [F_{\mathrm{mod}} : \mathbb{Q}]$, $(1 \leq)$ e_{mod} $(\leq d_{\mathrm{mod}})$ for the* **maximal ramification index** *of F_{mod} [i.e., of places $\in \mathbb{V}^{\mathrm{non}}_{\mathrm{mod}}$] over $\mathbb{Q}$, $d^*_{\mathrm{mod}} \stackrel{\mathrm{def}}{=} 2^{12} \cdot 3^3 \cdot 5 \cdot d_{\mathrm{mod}}$, $e^*_{\mathrm{mod}} \stackrel{\mathrm{def}}{=} 2^{12} \cdot 3^3 \cdot 5 \cdot e_{\mathrm{mod}}$ $(\leq d^*_{\mathrm{mod}})$, and*

$$F_{\mathrm{mod}} \subseteq F_{\mathrm{tpd}} \stackrel{\mathrm{def}}{=} F_{\mathrm{mod}}(E_{F_{\mathrm{mod}}}[2]) \subseteq F$$

*for the "***tripodal***" intermediate field obtained from F_{mod} by adjoining the fields of definition of the 2-torsion points of any model of $E_F \times_F \overline{F}$ over F_{mod} [cf.* [IUTchIV]*, Proposition 1.8, (ii), (iii)]. Moreover, we assume that the $(3 \cdot 5)$-torsion points of E_F are defined over F, and that*

$$F = F_{\mathrm{mod}}(\sqrt{-1},\ E_{F_{\mathrm{mod}}}[2 \cdot 3 \cdot 5]) \stackrel{\mathrm{def}}{=} F_{\mathrm{tpd}}(\sqrt{-1},\ E_{F_{\mathrm{tpd}}}[3 \cdot 5])$$

— i.e., that F is obtained from F_{tpd} by adjoining $\sqrt{-1}$, together with the fields of definition of the $(3 \cdot 5)$-torsion points of a model $E_{F_{\mathrm{tpd}}}$ of the elliptic curve $E_F \times_F \overline{F}$ over F_{tpd} determined by the **Legendre form** *of the Weierstrass equation [cf., e.g., the statement of Corollary 5.2, below;* [IUTchIV]*, Proposition 1.8, (vi)]. [Thus, it follows from* [IUTchIV]*, Proposition 1.8, (iv), that $E_F \cong E_{F_{\mathrm{tpd}}} \times_{F_{\mathrm{tpd}}} F$ over F, and from Definition 4.1 that $l \neq 5$.] If $F_{\mathrm{mod}} \subseteq F_\square \subseteq K$ is any intermediate extension which is Galois over F_{mod}, then we shall write*

$$\mathfrak{d}^{F_\square}_{\mathrm{ADiv}} \in \mathrm{ADiv}_{\mathbb{R}}(F_\square)$$

for the effective arithmetic divisor determined by the **different ideal** *of $F_\square$ over $\mathbb{Q}$,*

$$\mathfrak{q}^{F_\square}_{\mathrm{ADiv}} \in \mathrm{ADiv}_{\mathbb{R}}(F_\square)$$

for the effective arithmetic divisor determined by the ***q*-parameters** *of the elliptic curve E_F at the elements of $\mathbb{V}(F_\square)^{\mathrm{bad}} \stackrel{\mathrm{def}}{=} \mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}} \times_{\mathbb{V}_{\mathrm{mod}}} \mathbb{V}(F_\square)$ $(\neq \emptyset)$ [cf.* [GenEll]*, Remark 3.3.1],*

$$\mathfrak{f}^{F_\square}_{\mathrm{ADiv}} \in \mathrm{ADiv}_{\mathbb{R}}(F_\square)$$

for the effective arithmetic divisor whose support coincides with $\mathrm{Supp}(\mathfrak{q}^{F_\square}_{\mathrm{ADiv}})$, but all of whose coefficients are equal to 1 — i.e., the **conductor** *— and*

$$\log(\mathfrak{d}^{F_\square}_v) \stackrel{\mathrm{def}}{=} \underline{\deg}_{\mathbb{V}(F_\square)_v}(\mathfrak{d}^{F_\square}_{\mathrm{ADiv}}) \in \mathbb{R}_{\geq 0};\ \log(\mathfrak{d}^{F_\square}_{v_{\mathbb{Q}}}) \stackrel{\mathrm{def}}{=} \underline{\deg}_{\mathbb{V}(F_\square)_{v_{\mathbb{Q}}}}(\mathfrak{d}^{F_\square}_{\mathrm{ADiv}}) \in \mathbb{R}_{\geq 0}$$

$$\log(\mathfrak{d}^{F_\square}) \stackrel{\mathrm{def}}{=} \underline{\deg}(\mathfrak{d}^{F_\square}_{\mathrm{ADiv}}) \in \mathbb{R}_{\geq 0}$$

$$\log(\mathfrak{q}_v) \stackrel{\text{def}}{=} \underline{\deg}_{\mathbb{V}(F_\square)_v}(\mathfrak{q}^{F_\square}_{\text{ADiv}}) \in \mathbb{R}_{\geq 0};\ \log(\mathfrak{q}_{v_{\mathbb{Q}}}) \stackrel{\text{def}}{=} \underline{\deg}_{\mathbb{V}(F_\square)_{v_{\mathbb{Q}}}}(\mathfrak{q}^{F_\square}_{\text{ADiv}}) \in \mathbb{R}_{\geq 0}$$

$$\log(\mathfrak{q}) \stackrel{\text{def}}{=} \underline{\deg}(\mathfrak{q}^{F_\square}_{\text{ADiv}}) \in \mathbb{R}_{\geq 0}$$

$$\log(\mathfrak{f}^{F_\square}_v) \stackrel{\text{def}}{=} \underline{\deg}_{\mathbb{V}(F_\square)_v}(\mathfrak{f}^{F_\square}_{\text{ADiv}}) \in \mathbb{R}_{\geq 0};\ \log(\mathfrak{f}^{F_\square}_{v_{\mathbb{Q}}}) \stackrel{\text{def}}{=} \underline{\deg}_{\mathbb{V}(F_\square)_{v_{\mathbb{Q}}}}(\mathfrak{f}^{F_\square}_{\text{ADiv}}) \in \mathbb{R}_{\geq 0}$$

$$\log(\mathfrak{f}^{F_\square}) \stackrel{\text{def}}{=} \underline{\deg}(\mathfrak{f}^{F_\square}_{\text{ADiv}}) \in \mathbb{R}_{\geq 0}$$

— *where* $v \in \mathbb{V}_{\text{mod}} \stackrel{\text{def}}{=} \mathbb{V}(F_{\text{mod}})$, $v_{\mathbb{Q}} \in \mathbb{V}_{\mathbb{Q}} = \mathbb{V}(\mathbb{Q})$, $\mathbb{V}(F_\square)_v \stackrel{\text{def}}{=} \mathbb{V}(F_\square) \times_{\mathbb{V}_{\text{mod}}} \{v\}$, $\mathbb{V}(F_\square)_{v_{\mathbb{Q}}} \stackrel{\text{def}}{=} \mathbb{V}(F_\square) \times_{\mathbb{V}_{\mathbb{Q}}} \{v_{\mathbb{Q}}\}$ *[cf. also* [IUTchIV]*, Definition 1.9]. Here, we observe that the various "*$\log(\mathfrak{q}_{(-)})$*'s" are independent of the choice of* $F_\square$*, and that the quantity "*$|\log(\underline{\underline{q}})| \in \mathbb{R}_{>0}$*" defined in the* $\boldsymbol{\mu}_6$*-version of* [IUTchIII]*, Corollary 3.12 [cf. Remark 4.2.6], is equal to* $\frac{1}{2l} \cdot \log(\mathfrak{q}) \in \mathbb{R}$ *[cf. the definition of "*$\underline{\underline{q}}_{\underline{v}}$*" in* [IUTchI]*, Example 3.2, (iv)]. Moreover, suppose that*

$$l \geq 10^{15}.$$

Then one may take the constant "$C_\Theta \in \mathbb{R}$*" of the* $\boldsymbol{\mu}_6$*-version of* [IUTchIII]*, Corollary 3.12 [cf. Remark 4.2.6], to be*

$$\tfrac{l+1}{4 \cdot |\log(\underline{\underline{q}})|} \cdot \Big\{ (1 + \tfrac{12 \cdot d_{\text{mod}}}{l}) \cdot (\log(\mathfrak{d}^{F_{\text{tpd}}}) + \log(\mathfrak{f}^{F_{\text{tpd}}})) + 4.08803 \cdot e^*_{\text{mod}} \cdot l - \tfrac{1}{6} \cdot (1 - \tfrac{12}{l^2}) \cdot \log(\mathfrak{q}) \Big\} - 1$$

and hence, by applying the inequality "$C_\Theta \geq -1$*" of the* $\boldsymbol{\mu}_6$*-version of* [IUTchIII]*, Corollary 3.12 [cf. Remark 4.2.6], conclude that*

$$\begin{aligned} \tfrac{1}{6} \cdot \log(\mathfrak{q}) &\leq (1 + \tfrac{20 \cdot d_{\text{mod}}}{l}) \cdot (\log(\mathfrak{d}^{F_{\text{tpd}}}) + \log(\mathfrak{f}^{F_{\text{tpd}}})) + 4.0881 \cdot e^*_{\text{mod}} \cdot l \\ &\leq (1 + \tfrac{20 \cdot d_{\text{mod}}}{l}) \cdot (\log(\mathfrak{d}^{F}) + \log(\mathfrak{f}^{F})) + 4.0881 \cdot e^*_{\text{mod}} \cdot l. \end{aligned}$$

Proof. Theorem 5.1 follows by applying a similar argument to the argument applied in the proof of [IUTchIV], Theorem 1.10. In the present paper, however, we replace *some of the estimates* applied in the proof of [IUTchIV], Theorem 1.10, as follows:

• We replace the estimate "$\frac{4(l+5)}{l+1} \leq \frac{20}{3}$" appearing in the final portion of *Step (v)* of the proof of [IUTchIV], Theorem 1.10, by the estimate

$$\tfrac{4(l+5)}{l+1} = 4 + \tfrac{16}{l+1} \leq 4 + \tfrac{100}{l} \leq 4 + 10^{-13}$$

— cf. our assumption that $l \geq 10^{15}$.

• We replace the estimate "$l^*_{\text{mod}} \cdot \log(\mathfrak{s}^{\leq}) \leq \frac{4}{3} \cdot (e^*_{\text{mod}} \cdot l + \eta_{\text{prm}})$" appearing in *Step (viii)* of the proof of [IUTchIV], Theorem 1.10, by the estimate

$$l^*_{\text{mod}} \cdot \log(\mathfrak{s}^{\leq}) \leq 1.022 \cdot e^*_{\text{mod}} \cdot l$$

— cf. Proposition 2.2, (i); our assumption that $l \geq 10^{15}$, which implies the estimate $e^*_{\text{mod}} \cdot l \geq 2^{12} \cdot 3^3 \cdot 5 \cdot 10^{15} \geq \eta_{\text{prm}} = 5 \cdot 10^{20}$.

• We replace the estimate

$$"\tfrac{1}{3} \cdot \tfrac{4}{3} \cdot e^*_{\text{mod}} \cdot l \geq 2 \cdot 2 \cdot 2^{12} \cdot 3 \cdot 5 \cdot l \geq 2 \cdot \log(l) + 56"$$

appearing in *Step (viii)* of the proof of [IUTchIV], Theorem 1.10, by the estimate

$$10^{-5} \cdot 1.022 \cdot e^{*}_{\mathrm{mod}} \cdot l \;\geq\; (10^{-5} \cdot 2^{12} \cdot 3^2 \cdot 5) \cdot 3l \;\geq\; 3l \;\geq\; 2 \cdot \log(l) + 56$$

— where the first (respectively, second; third) inequality follows from the estimate $1.022 \geq 1$ (respectively, $2^{12} \cdot 3^2 \cdot 5 \geq 10^5$; $l \geq \max\{56, \log(l)\}$ [which is a consequence of our assumption that $l \geq 10^{15}$]).

In light of these [three] modifications, together with the estimate

$$(4 + 10^{-13} + 10^{-5}) \cdot 1.022 \;\leq\; (4 + 2 \cdot 10^{-5}) \cdot 1.022 \;\leq\; 4.08803,$$

we conclude that one may take the constant "$C_\Theta \in \mathbb{R}$" to be the constant stated in Theorem 5.1.

Finally, by replacing the estimate "$(1 - \frac{12}{l^2})^{-1} \leq 2$" appearing in the final portion of *Step (viii)* of the proof of [IUTchIV], Theorem 1.10, by the estimate

$$(1 - \tfrac{12}{l^2})^{-1} \;=\; 1 + \tfrac{12}{l^2 - 12} \;\leq\; 1 + \tfrac{100}{l} \;\leq\; 1 + 10^{-13}$$

[where we apply the estimates $l \geq 10^{15}$, $l^2 - 12 \geq l$], we obtain [by applying the estimate $4.08803 \cdot (1 + 10^{-13}) \leq 4.0881$] the final inequality of Theorem 5.1. □

Corollary 5.2. (Construction of suitable μ_6-initial Θ-data) *Write X for the* **projective line** *over $\mathbb{Q}$; $D \subseteq X$ for the divisor consisting of the* **three points** *"0", "1", and "∞"; $(\mathcal{M}_{\mathrm{ell}})_{\mathbb{Q}}$ for the moduli stack of elliptic curves over $\mathbb{Q}$. We shall regard X as the "λ-**line**" — i.e., we shall regard the standard coordinate on X as the "λ" in the* **Legendre form** *"$y^2 = x(x-1)(x-\lambda)$" of the Weierstrass equation defining an elliptic curve — and hence as being equipped with a natural* **classifying morphism** *$U_X \stackrel{\mathrm{def}}{=} X \setminus D \to (\mathcal{M}_{\mathrm{ell}})_{\mathbb{Q}}$ [cf. the discussion preceding* [IUTchIV]*, Proposition 1.8]. Let $\kappa \in \mathbb{R}_{>0} \cap \mathbb{R}_{\leq 1}$;*

$$\mathcal{K} \;\stackrel{\mathrm{def}}{=}\; \mathcal{K}_{\mathbb{V}(\mathbb{Q})^{\mathrm{arc}}}(\kappa) \;\subseteq\; U_X(\overline{\mathbb{Q}}) \;\; (\stackrel{\sim}{\to} \overline{\mathbb{Q}}^{\mathbb{h}})$$

a **compactly bounded subset** *[cf. Definition 1.13]; $d \in \mathbb{Z}_{>0}$ [cf.* [IUTchIV]*, Corollary 2.2, (ii), (iii)]; $\epsilon \in \mathbb{R}_{>0} \cap \mathbb{R}_{\leq 1}$ [cf.* [IUTchIV]*, Corollary 2.2, (iii)]. Write*

$$\log(\mathfrak{q}^{\forall}_{(-)})$$

for the $\mathbb{R}$-valued function on $(\mathcal{M}_{\mathrm{ell}})_{\mathbb{Q}}(\overline{\mathbb{Q}})$, hence on $U_X(\overline{\mathbb{Q}})$, obtained by forming the normalized degree "$\underline{\deg}(-)$" of the effective arithmetic divisor determined by the ***q*-parameters** *of an elliptic curve over a number field at* **arbitrary** *nonarchimedean places [cf.* [IUTchIV]*, Corollary 2.2, (i)]; $U_X(\overline{\mathbb{Q}})^{\leq d} \subseteq U_X(\overline{\mathbb{Q}})$ for the subset of $\overline{\mathbb{Q}}$-rational points defined over a finite extension field of $\mathbb{Q}$ of degree $\leq d$; $U_X(\overline{\mathbb{Q}})^{\mathrm{mcx}} \subseteq U_X(\overline{\mathbb{Q}})$ for the subset of $\overline{\mathbb{Q}}$-rational points defined over a* **mono-complex** *number field [cf. Definition 1.2]. Set*

$$\delta \;\stackrel{\mathrm{def}}{=}\; 2^{12} \cdot 3^3 \cdot 5 \cdot d \;=\; 552960 \cdot d;$$

$$\kappa^{\log} \;\stackrel{\mathrm{def}}{=}\; 5 \cdot 10^{-13} - 6.01 \cdot 10^{-15} \log(\kappa)$$

[cf. the term "$H_{\mathcal{K}}$" in the first display of [IUTchIV]*, Corollary 2.2, (iii)];*

$$h_d(\epsilon) \stackrel{\text{def}}{=} \begin{cases} 3.4 \cdot 10^{30} \cdot \epsilon^{-166/81} & (d = 1) \\ 6 \cdot 10^{31} \cdot \epsilon^{-174/85} & (d = 2) \\ 3.4 \cdot 10^{30} \cdot \epsilon^{-166/81} \cdot d^5 & (d \geq 3) \end{cases}$$

[cf. the term "$H_{\text{unif}} \cdot \epsilon^{-3} \cdot \epsilon_d^{-3} \cdot d^{4+\epsilon_d}$" in the first display of [IUTchIV]*, Corollary 2.2, (iii), where we take "ϵ_d" to be* 1*]. Then there exists a* **finite** *subset*

$$\mathfrak{Exc}_{\kappa,d,\epsilon} \subseteq U_X(\overline{\mathbb{Q}})^{\leq d} \qquad (\textit{respectively, } \mathfrak{Exc}^{\text{mcx}}_{d,\epsilon} \subseteq U_X(\overline{\mathbb{Q}})^{\leq d} \cap U_X(\overline{\mathbb{Q}})^{\text{mcx}})$$

— which depends only on κ, d, ϵ (respectively, d, ϵ) and contains all points corresponding to elliptic curves that admit automorphisms of order > 2 — satisfying the following properties:

- *The function* $\log(\mathfrak{q}^{\forall}_{(-)})$ *is*

$$\leq \max\{\kappa^{\log},\ h_d(\epsilon)\} \qquad (\textit{respectively, } \leq h_d(\epsilon))$$

on $\mathfrak{Exc}_{\kappa,d,\epsilon}$ *(respectively,* $\mathfrak{Exc}^{\text{mcx}}_{d,\epsilon}$*).*

- *Let E_F be an elliptic curve over a number field $F \subseteq \overline{\mathbb{Q}}$ that determines a $\overline{\mathbb{Q}}$-valued point of $(\mathcal{M}_{\text{ell}})_{\mathbb{Q}}$ which lifts [not necessarily uniquely!] to a point*

$$x_E \in U_X(F) \cap U_X(\overline{\mathbb{Q}})^{\leq d} \cap \mathcal{K}$$

$$(\textit{respectively, } x_E \in U_X(F) \cap U_X(\overline{\mathbb{Q}})^{\leq d} \cap U_X(\overline{\mathbb{Q}})^{\text{mcx}})$$

such that

$$x_E \notin \mathfrak{Exc}_{\kappa,d,\epsilon} \quad (\textit{respectively, } x_E \notin \mathfrak{Exc}^{\text{mcx}}_{d,\epsilon}).$$

Write F_{mod} for the **minimal field of definition** *of the corresponding point $\in (\mathcal{M}_{\text{ell}})_{\mathbb{Q}}(\overline{\mathbb{Q}})$ and*

$$F_{\text{mod}} \subseteq F_{\text{tpd}} \stackrel{\text{def}}{=} F_{\text{mod}}(E_{F_{\text{mod}}}[2]) \subseteq F$$

for the **"tripodal"** *intermediate field obtained from F_{mod} by adjoining the fields of definition of the 2-torsion points of any model of $E_F \times_F \overline{\mathbb{Q}}$ over F_{mod} [cf.* [IUTchIV]*, Proposition 1.8, (ii), (iii)]. Moreover, we assume that the $(3 \cdot 5)$-torsion points of E_F are defined over F, and that*

$$F = F_{\text{mod}}(\sqrt{-1}, E_{F_{\text{mod}}}[2 \cdot 3 \cdot 5]) \stackrel{\text{def}}{=} F_{\text{tpd}}(\sqrt{-1}, E_{F_{\text{tpd}}}[3 \cdot 5])$$

— i.e., that F is obtained from F_{tpd} by adjoining $\sqrt{-1}$, together with the fields of definition of the $(3 \cdot 5)$-torsion points of a model $E_{F_{\text{tpd}}}$ of the elliptic curve $E_F \times_F \overline{\mathbb{Q}}$ over F_{tpd} determined by the **Legendre form** *of the Weierstrass equation discussed above [cf.* [IUTchIV]*, Proposition 1.8, (vi)]. [Thus, it follows from* [IUTchIV]*, Proposition 1.8, (iv), that $E_F \cong E_{F_{\text{tpd}}} \times_{F_{\text{tpd}}} F$ over F, so $x_E \in U_X(F_{\text{tpd}}) \subseteq U_X(F)$; it follows from* [IUTchIV]*, Proposition 1.8, (v), that E_F has* **stable reduction** *at every element of $\mathbb{V}(F)^{\text{non}}$.] Write*

$$\log(\mathfrak{q}^{\forall})$$

for the result of applying the function "$\log(\mathfrak{q}^{\forall}_{(-)})$" to x_E. Then E_F and F_{mod} arise as the "E_F" and "F_{mod}" for a collection of **$\boldsymbol{\mu_6}$-initial $\boldsymbol{\Theta}$-data** *as in Theorem 5.1 that satisfies the following conditions:*

(C1) $(10^{15}\cdot d \leq)\ (\log(\mathfrak{q}^{\forall}))^{\frac{1}{2}} \leq l \leq 1.464\delta\cdot(\log(\mathfrak{q}^{\forall}))^{\frac{1}{2}}\cdot\log(1.45\delta\cdot\log(\mathfrak{q}^{\forall}))$*;*

(C2) we have an inequality

$$\tfrac{1}{6}\cdot\log(\mathfrak{q}^{\forall}) \leq (1+\epsilon)\cdot(\text{log-diff}_X(x_E)+\text{log-cond}_D(x_E))$$

— where we write log-diff_X *for the [normalized] log-different function on* $U_X(\overline{\mathbb{Q}})$ *[cf.* [GenEll]*, Definition 1.5, (iii)];* log-cond_D *for the [normalized] log-conductor function on* $U_X(\overline{\mathbb{Q}})$ *[cf.* [GenEll]*, Definition 1.5, (iv)].*

Proof. First, let us recall that if the once-punctured elliptic curve associated to E_F *fails to admit an* F*-core*, then it holds that

$$j(E_F) \in \{2^{14}\cdot 31^3\cdot 5^{-3},\ \ 2^2\cdot 73^3\cdot 3^{-4},\ \ 2^6\cdot 3^3,\ \ 0\}$$

[cf. Proposition 2.1]. Thus, if we take the set $\mathfrak{Exc}_{\kappa,d,\epsilon}$ (respectively, $\mathfrak{Exc}^{\text{mcx}}_{d,\epsilon}$) to be the [*finite*!] collection of points corresponding to these four j-invariants, then we may assume that the once-punctured elliptic curve associated to E_F *admits an* F*-core* — hence, in particular, does not have any automorphisms of order > 2 over $\overline{\mathbb{Q}}$ — and that it holds that

$$\log(\mathfrak{q}^{\forall}_{(-)}) \leq \max\{\log(5^3),\ \log(3^4)\} = \log(5^3)$$

on $\mathfrak{Exc}_{\kappa,d,\epsilon}$ (respectively, $\mathfrak{Exc}^{\text{mcx}}_{d,\epsilon}$) [cf. Remark 1.10.1]. [In the discussion to follow, it will in fact be necessary to *enlarge* the finite set $\mathfrak{Exc}_{\kappa,d,\epsilon}$ (respectively, $\mathfrak{Exc}^{\text{mcx}}_{d,\epsilon}$) several times.]

Next, let us write

$$h \stackrel{\text{def}}{=} \log(\mathfrak{q}^{\forall}) = \tfrac{1}{[F:\mathbb{Q}]}\cdot\sum_{v\in\mathbb{V}(F)^{\text{non}}} h_v\cdot f_v\cdot\log(p_v)$$

— that is to say, $h_v = 0$ for those v at which E_F has *good reduction*; $h_v \in \mathbb{N}_{\geq 1}$ is the *local height* of E_F [cf. [GenEll], Definition 3.3] for those v at which E_F has *bad multiplicative reduction*. Now it follows [from [GenEll], Proposition 1.4, (iv) [cf. also the proof of [IUTchIV], Corollary 2.2, (i)] (respectively, from Proposition 1.9, (iii), of the present paper)] that the inequality $h^{1/2} < 10^{15}\cdot d$ implies that there is only a *finite number of possibilities* for the j-invariant of E_F. Thus, by possibly *enlarging* the finite set $\mathfrak{Exc}_{\kappa,d,\epsilon}$ (respectively, $\mathfrak{Exc}^{\text{mcx}}_{d,\epsilon}$), we may assume without loss of generality that

$$h^{1/2} \geq 10^{15}\cdot d\ \ (\geq \xi_{\text{prm}}),$$

[cf. the notation of Proposition 2.2], and that it holds that

$$\log(\mathfrak{q}^{\forall}_{(-)}) \leq \max\{\log(5^3),\ 10^{30}\cdot d^2\} = 10^{30}\cdot d^2$$

on $\mathfrak{Exc}_{\kappa,d,\epsilon}$ (respectively, $\mathfrak{Exc}^{\text{mcx}}_{d,\epsilon}$).

Thus, since $[F : \mathbb{Q}] \leq \delta$ [cf. the properties (E3), (E4), (E5) in the proof of [IUTchIV], Theorem 1.10], it follows that

$$\begin{aligned}\delta \cdot h^{1/2} &\geq [F : \mathbb{Q}] \cdot h^{1/2} = \sum_v h^{-1/2} \cdot h_v \cdot f_v \cdot \log(p_v) \\ &\geq \sum_v h^{-1/2} \cdot h_v \cdot \log(p_v) \geq \sum_{h_v \geq h^{1/2}} h^{-1/2} \cdot h_v \cdot \log(p_v) \\ &\geq \sum_{h_v \geq h^{1/2}} \log(p_v)\end{aligned}$$

and

$$\begin{aligned}1.45\delta \cdot h^{1/2} \cdot \log(1.45\delta \cdot h) &\geq 1.45 \cdot [F : \mathbb{Q}] \cdot h^{1/2} \cdot \log(1.45 \cdot [F : \mathbb{Q}] \cdot h) \\ &\geq \sum_{h_v \neq 0} 1.45 \cdot h^{-1/2} \cdot \log(1.45 \cdot h_v \cdot f_v \cdot \log(p_v)) \cdot h_v \cdot f_v \cdot \log(p_v) \\ &\geq \sum_{h_v \neq 0} h^{-1/2} \cdot \log(h_v) \cdot h_v \geq \sum_{h_v \geq h^{1/2}} h^{-1/2} \cdot \log(h_v) \cdot h_v \\ &\geq \sum_{h_v \geq h^{1/2}} \log(h_v)\end{aligned}$$

— where the sums are all over $v \in \mathbb{V}(F)^{\mathrm{non}}$ [possibly subject to various conditions, as indicated], and we apply the elementary estimate $1.45 \cdot \log(p_v) \geq 1.45 \cdot \log(2) \geq 1$.

Thus, in summary, we conclude from the estimates made above that if we take

$$\mathcal{A}$$

to be the [*finite*!] set of prime numbers p such that p either

(S1) is $\leq h^{1/2}$,
(S2) *divides a nonzero* h_v for some $v \in \mathbb{V}(F)^{\mathrm{non}}$, or
(S3) is *equal to* p_v for some $v \in \mathbb{V}(F)^{\mathrm{non}}$ for which $h_v \geq h^{1/2}$,

then it follows from Proposition 2.2, (ii), together with our assumption that $h^{1/2} \geq \xi_{\mathrm{prm}}$, that, in the notation of Proposition 2.2, (ii),

$$\begin{aligned}\theta_{\mathcal{A}} &\leq 2 \cdot h^{1/2} + \delta \cdot h^{1/2} + 1.45\delta \cdot h^{1/2} \cdot \log(1.45\delta \cdot h) \\ &= (2 + \delta + 1.45\delta \cdot \log(1.45\delta \cdot h)) \cdot h^{1/2} \\ &\leq 1.4621\delta \cdot h^{1/2} \cdot \log(1.45\delta \cdot h)\end{aligned}$$

— where we apply the estimates $1 + 0.00071 \leq 2$;

$$2 \leq 0.0121\delta \cdot \log(1.45\delta \cdot 10^{30}) - \delta \leq 0.0121\delta \cdot \log(1.45\delta \cdot h) - \delta$$

[cf. the fact that the function

$$0.0121x \cdot \log(1.45x \cdot 10^{30}) - x$$

is *monotonically increasing* for $x \in \mathbb{R}_{\geq 552960}$]. On the other hand, since we have

$$\xi_{\mathrm{prm}} \leq h^{1/2} \leq 0.0001\delta \cdot h^{1/2} \cdot \log(1.45\delta \cdot h)$$

[cf. the estimates $1 \leq 0.0001\delta$ and $1 \leq \log(1.45\delta \cdot h)$], we obtain that

$$1.00072 \cdot (\theta_{\mathcal{A}} + \xi_{\mathrm{prm}}) \ \leq \ 1.464\delta \cdot h^{1/2} \cdot \log(1.45\delta \cdot h)$$

[cf. the estimate $1.00072 \cdot (1.4621 + 0.0001) \leq 1.464$]. In particular, it follows from Proposition 2.2, (ii), that there exists a *prime number* l such that

(P1) $(10^{15} \cdot d \leq) \ h^{1/2} \ \leq \ l \ \leq \ 1.464\delta \cdot h^{1/2} \cdot \log(1.45\delta \cdot h)$ [cf. the condition (C1) in the statement of Corollary 5.2];

(P2) l does *not divide* any nonzero h_v for $v \in \mathbb{V}(F)^{\mathrm{non}}$;

(P3) if $l = p_v$ for some $v \in \mathbb{V}(F)^{\mathrm{non}}$, then $h_v \ < \ h^{1/2}$.

Next, let us *observe* that, again by possibly *enlarging* the finite set $\mathfrak{Exc}_{\kappa,d,\epsilon}$ (respectively, $\mathfrak{Exc}^{\mathrm{mcx}}_{d,\epsilon}$), we may assume without loss of generality that, in the terminology of [GenEll], Lemma 3.5,

(P4) E_F does *not* admit an l-*cyclic* subgroup scheme,

and that it holds that

$$\log(\mathfrak{q}^{\forall}_{(-)}) \ \leq \ \max\{10^{30} \cdot d^2, \ \kappa^{\log}\}$$

$$(\text{respectively, } \log(\mathfrak{q}^{\forall}_{(-)}) \ \leq \ \max\{10^{30} \cdot d^2, \ 5.12 \cdot 10^{-13}\} \ = \ 10^{30} \cdot d^2)$$

on $\mathfrak{Exc}_{\kappa,d,\epsilon}$ (respectively, $\mathfrak{Exc}^{\mathrm{mcx}}_{d,\epsilon}$). Indeed, the existence of an l-cyclic subgroup scheme of E_F, together with the fact that $l \geq 10^{15}$ [cf. (P1)], would imply that

$$h \ \leq \ \kappa^{\log} \qquad (\text{respectively, } h \ \leq \ 5.12 \cdot 10^{-13})$$

[cf. (P2); Remark 1.10.1; Corollary 1.14, (ii) (respectively, Corollary 1.14, (iii))]. On the other hand, [by [GenEll], Proposition 1.4, (iv) [cf. also the proof of [IUTchIV], Corollary 2.2, (i)] (respectively, Proposition 1.9, (iii))] this implies that there is only a *finite number of possibilities* for the j-invariant of E_F. This completes the proof of the above *observation*.

Next, we *observe* that

(P5) if we write $\mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}$ for the set of nonarchimedean places $\in \mathbb{V}_{\mathrm{mod}}$ that do *not divide* l and at which E_F has *bad multiplicative reduction*, then $\mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}} \neq \emptyset$.

Indeed, if $\mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}} = \emptyset$, then it follows, in light of the definition of h, from (P3) that

$$h \ \leq \ h^{1/2} \cdot \log(l).$$

In particular, we have

$$\begin{aligned} h^{1/2} \ \leq \ \log(l) \ &\leq \ \log(1.464\delta) \ + \ 0.5 \cdot \log(h) \ + \ \log(\log(1.45\delta \cdot h)) \\ &\leq \ \log(1.464\delta) \ + \ 0.5 \cdot \log(h) \ + \ \log(1.45\delta \cdot h) \\ &= \ 1.5 \cdot \log(h) \ + \ \log(1.464\delta) \ + \ \log(1.45\delta) \\ &\leq \ 1.5 \cdot \log(h) \ + \ 2 \cdot \log(2\delta) \end{aligned}$$

— where the second inequality follows from (P1); the third inequality follows from the fact that $\log(x) \leq x$ for all $x \in \mathbb{R}_{\geq 1}$; the fourth inequality follows from the estimate $1.464 \cdot 1.45 \leq 4$. Thus, if we write $f(x)$ for the function

$$x^{1/2} \ - \ 1.5 \cdot \log(x) \ - \ 2 \cdot \log(2\delta),$$

then it holds that $f(h) \leq 0$. On the other hand, since [as is easily verified] $f(x)$ is *monotonically increasing* for $x \in \mathbb{R}_{\geq 9}$, we obtain that

$$\begin{aligned} f(h) &\geq f(10^{30} \cdot d^2) \\ &= 10^{15} \cdot d \ - \ 3 \cdot \log(10^{15} \cdot d) \ - \ 2 \cdot \log(2^{13} \cdot 3^3 \cdot 5 \cdot d) \\ &\geq 10^{15} \cdot d \ - \ 5 \cdot \log(10^{15} \cdot d) \ > \ 0 \end{aligned}$$

— where we apply the estimate $2^{13} \cdot 3^3 \cdot 5 \leq 10^{15}$; the fact that $5 \cdot \log(x) < x$ for all $x \in \mathbb{R}_{\geq 13}$ — a contradiction. This completes the proof of the above *observation*. This property (P5) implies that

(P6) the image of the outer homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/F) \to GL_2(\mathbb{F}_l)$ determined by the *l-torsion points* of E_F *contains the subgroup* $SL_2(\mathbb{F}_l) \subseteq GL_2(\mathbb{F}_l)$.

Indeed, since, by (P5), E_F has *bad multiplicative reduction* at some place $\in \mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}} \neq \emptyset$, (P6) follows formally from (P2), (P4), and [GenEll], Lemma 3.1, (iii) [cf. the proof of the final portion of [GenEll], Theorem 3.8].

Now it follows formally from (P1), (P2), (P5), and (P6) that, if one takes "$\overline{F}$" to be $\overline{\mathbb{Q}}$, "F" to be the number field F of the above discussion, "X_F" to be the once-punctured elliptic curve associated to E_F, "l" to be the prime number l of the above discussion, and "$\mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}$"to be the set $\mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}$ of (P5), then there exist data "$\underline{C}_K$", "$\underline{\mathbb{V}}$", and "$\underline{\epsilon}$" such that *all of the conditions of Definition 4.1 are satisfied*, and, moreover, that

(P7) *the resulting* $\boldsymbol{\mu_6}$**-initial Θ-data**

$$(\overline{F}/F, \ X_F, \ l, \ \underline{C}_K, \ \underline{\mathbb{V}}, \ \mathbb{V}^{\mathrm{bad}}_{\mathrm{mod}}, \ \underline{\epsilon})$$

satisfies the various conditions in the statement of Theorem 5.1.

Here, we note in passing that the crucial *existence* of data "$\underline{\mathbb{V}}$" and "$\underline{\epsilon}$" satisfying the requisite conditions follows, in essence, as a consequence of the fact [i.e., (P6)] that the Galois action on l-torsion points contains the *full special linear group* $SL_2(\mathbb{F}_l)$.

In light of (P7), we may apply Theorem 5.1 [cf. also the fact that $e^*_{\mathrm{mod}} \leq d^*_{\mathrm{mod}}$] to conclude that

$$\begin{aligned} \tfrac{1}{6} \cdot \log(\mathfrak{q}) &\leq (1 + \tfrac{20 \cdot d_{\mathrm{mod}}}{l}) \cdot (\log(\mathfrak{d}^{F_{\mathrm{tpd}}}) + \log(\mathfrak{f}^{F_{\mathrm{tpd}}})) \ + \ 4.0881 \cdot d^*_{\mathrm{mod}} \cdot l \\ &\leq (1 + \delta \cdot h^{-1/2}) \cdot (\log(\mathfrak{d}^{F_{\mathrm{tpd}}}) + \log(\mathfrak{f}^{F_{\mathrm{tpd}}})) \\ &\qquad + \ 5.985 \cdot \delta^2 \cdot h^{1/2} \cdot \log(1.45\delta \cdot h) \end{aligned}$$

— where we apply (P1), as well as the estimates $20 \cdot d_{\mathrm{mod}} \leq d^*_{\mathrm{mod}} \leq \delta$ and $4.0881 \cdot 1.464 \leq 5.985$.

Next, let us *observe* that it follows from (P3) that

$$\tfrac{1}{6} \cdot h - \tfrac{1}{6} \cdot \log(\mathfrak{q}) \ \leq \ \tfrac{1}{6} \cdot h^{1/2} \cdot \log(l).$$

Thus, we conclude that

$$\begin{aligned}\tfrac{1}{6}\cdot h \;\leq\; (1+\delta\cdot h^{-1/2})\cdot(\log(\mathfrak{d}^{F_{\mathrm{tpd}}})+\log(\mathfrak{f}^{F_{\mathrm{tpd}}}))\;+\;\tfrac{1}{6}\cdot h^{1/2}\cdot\log(l)\\ +\;5.985\cdot\delta^2\cdot h^{1/2}\cdot\log(1.45\delta\cdot h)\end{aligned}$$

and hence that

(P8) the following equality holds:

$$\begin{aligned}\tfrac{1}{6}\cdot h\;\cdot(1-h^{-1/2}\cdot\log(l)-35.91\cdot\delta^2\cdot h^{-1/2}\cdot\log(1.45\delta\cdot h))\\ \leq\;(1+\delta\cdot h^{-1/2})\cdot(\log(\mathfrak{d}^{F_{\mathrm{tpd}}})+\log(\mathfrak{f}^{F_{\mathrm{tpd}}})).\end{aligned}$$

Now we *claim* that

Claim 5.2A: If $h\geq h_d(\epsilon)$, then it holds that

$$71.82\cdot\delta^2\cdot h^{-1/2}\cdot\log(1.45\delta\cdot h)\;\leq\;\epsilon\cdot(1-10^{-7}).$$

Indeed, since [as is easily verified] the function $x^{-1/2}\cdot\log(1.45\delta\cdot x)$ is *monotonically decreasing* for $x\in\mathbb{R}_{>1}$, to verify Claim 5.2A, it suffices to show that

$$71.82\cdot\delta^2\cdot h_d(\epsilon)^{-1/2}\cdot\log(1.45\delta\cdot h_d(\epsilon))\;\leq\;\epsilon\cdot(1-10^{-7}).$$

Let us prove this inequality. First, suppose that $d\in\{1,2\}$. Write $\delta_1\stackrel{\text{def}}{=}2^{12}\cdot3^3\cdot5$, $\delta_2\stackrel{\text{def}}{=}2^{13}\cdot3^3\cdot5$. Then one verifies easily that

$$71.82\cdot\delta^2\cdot h_d(1)^{-1/2}\cdot\log(1.45\delta\cdot h_d(1))\;\leq\;1-10^{-7}.$$

Thus, if $d=1$, then we have

$$\begin{aligned}&71.82\cdot\delta^2\cdot h_d(\epsilon)^{-1/2}\cdot\log(1.45\delta\cdot h_d(\epsilon))\\ &=\;71.82\cdot\delta^2\cdot h_d(1)^{-1/2}\cdot\log(1.45\delta\cdot h_d(1))\cdot\epsilon^{83/81}\cdot\left\{1-\tfrac{\log(\epsilon^{2/81})\cdot83}{\log(1.45\delta\cdot h_d(1))}\right\}\\ &\leq\;\epsilon\cdot(1-10^{-7})\cdot\epsilon^{2/81}\cdot(1-\log(\epsilon^{2/81}))\;\leq\;\epsilon\cdot(1-10^{-7});\end{aligned}$$

if $d=2$, then we have

$$\begin{aligned}&71.82\cdot\delta^2\cdot h_d(\epsilon)^{-1/2}\cdot\log(1.45\delta\cdot h_d(\epsilon))\\ &=\;71.82\cdot\delta^2\cdot h_d(1)^{-1/2}\cdot\log(1.45\delta\cdot h_d(1))\cdot\epsilon^{87/85}\cdot\left\{1-\tfrac{\log(\epsilon^{2/85})\cdot87}{\log(1.45\delta\cdot h_d(1))}\right\}\\ &\leq\;\epsilon\cdot(1-10^{-7})\cdot\epsilon^{2/85}\cdot(1-\log(\epsilon^{2/85}))\;\leq\;\epsilon\cdot(1-10^{-7}).\end{aligned}$$

Here, we apply the estimate $\log(1.45\delta_1\cdot h_1(1))\geq83$; the estimate $\log(1.45\delta_2\cdot h_2(1))\geq87$; our assumption that $0<\epsilon\leq1$; the fact that $x\cdot(1-\log(x))\leq1$ for all $x\in\mathbb{R}_{>0}$.

Next, suppose that $d\geq3$. Then we have

$$\begin{aligned}&71.82\cdot\delta^2\cdot h_d(\epsilon)^{-1/2}\cdot\log(1.45\delta\cdot h_d(\epsilon))\\ &=\;71.82\cdot\delta_1^2\cdot h_1(\epsilon)^{-1/2}\cdot\log(1.45\delta_1\cdot h_1(\epsilon))\cdot d^{-1/2}\cdot\left\{1+\tfrac{6\cdot\log(d)}{\log(1.45\delta_1\cdot h_1(\epsilon))}\right\}\\ &\leq\;\epsilon\cdot(1-10^{-7})\cdot d^{-1/2}\cdot(1+\tfrac{6}{83}\cdot\log(d))\;\leq\;\epsilon\cdot(1-10^{-7})\end{aligned}$$

— where we apply the estimate $\log(1.45\delta_1\cdot h_1(\epsilon))\geq\log(1.45\delta_1\cdot h_1(1))\geq83$; the fact that $x^{-1/2}\cdot(1+\frac{6}{83}\cdot\log(x))\leq1$ for all $x\in\mathbb{R}_{\geq3}$; the estimate obtained above in the case where $d=1$. This completes the proof of Claim 5.2A.

Next, we *claim* that

Claim 5.2B: If $h \geq h_d(\epsilon)$, then it holds that

$$2 \cdot h^{-1/2} \cdot \log(l) \ + \ 71.82 \cdot \delta^2 \cdot h^{-1/2} \cdot \log(1.45\delta \cdot h) \ + \ \delta \cdot h^{-1/2} \ \leq \ \epsilon.$$

Indeed, since [cf. (P1)] it holds that

$$71.82 \cdot \delta \cdot \log(1.45\delta \cdot h) \ \geq \ 71.82 \cdot 2^{12} \cdot 3^3 \cdot 5 \cdot \log(1.45 \cdot 2^{12} \cdot 3^3 \cdot 5 \cdot 10^{30}) \ \geq \ 10^8,$$

we have

$$71.82 \cdot \delta^2 \cdot h^{-1/2} \cdot \log(1.45\delta \cdot h) \ \geq \ 10^8 \cdot \delta \cdot h^{-1/2}.$$

Moreover, since it holds that

$$71.82 \cdot \delta^2 \ \geq \ 71.82 \cdot (2^{12} \cdot 3^3 \cdot 5)^2 \ \geq \ 4 \cdot 10^{12},$$

we have [cf. (P1)]

$$\begin{aligned} 71.82 \cdot \delta^2 \cdot h^{-1/2} \cdot & \log(1.45\delta \cdot h) \\ & \geq \ 10^{12} \cdot 2 \cdot h^{-1/2} \cdot \log((1.45\delta \cdot h)^2) \\ & \geq \ 10^{12} \cdot 2 \cdot h^{-1/2} \cdot \log(1.464\delta \cdot h^{1/2} \cdot 1.45\delta \cdot h) \\ & \geq \ 10^{12} \cdot 2 \cdot h^{-1/2} \cdot \log(1.464\delta \cdot h^{1/2} \cdot \log(1.45\delta \cdot h)) \\ & \geq \ 10^{12} \cdot 2 \cdot h^{-1/2} \cdot \log(l) \end{aligned}$$

— where the second inequality follows from the estimate $1.45 \cdot h^{1/2} \geq 1.464$; the third inequality follows from the fact that $x \geq \log(x)$ for all $x \in \mathbb{R}_{\geq 1}$. Thus, it follows from Claim 5.2A that

$$\begin{aligned} 2 \cdot h^{-1/2} \cdot \log(l) \ + \ & 71.82 \cdot \delta^2 \cdot h^{-1/2} \cdot \log(1.45\delta \cdot h) \ + \ \delta \cdot h^{-1/2} \\ & \leq \ (10^{-12} + 1 + 10^{-8}) \cdot 71.82 \cdot \delta^2 \cdot h^{-1/2} \cdot \log(1.45\delta \cdot h) \\ & \leq \ (10^{-12} + 1 + 10^{-8}) \cdot \epsilon \cdot (1 - 10^{-7}) \ \leq \ \epsilon \end{aligned}$$

— where we apply the estimate $(10^{-12} + 1 + 10^{-8}) \cdot (1 - 10^{-7}) \leq 1$. This completes the proof of Claim 5.2B.

Here, note that the inequality $h < h_d(\epsilon)$ implies [by [GenEll], Proposition 1.4, (iv) [cf. also the proof of [IUTchIV], Corollary 2.2, (i)] (respectively, Proposition 1.9, (iii))] that there is only a *finite number of possibilities* for the j-invariant of E_F. Thus, by possibly *enlarging* the finite set $\mathfrak{Exc}_{\kappa,d,\epsilon}$ (respectively, $\mathfrak{Exc}^{\mathrm{mcx}}_{d,\epsilon}$), we may assume without loss of generality that

$$h \ \geq \ h_d(\epsilon),$$

and that it holds that

$$\begin{aligned} \log(\mathfrak{q}^{\forall}_{(-)}) \ & \leq \ \max\{10^{30} \cdot d^2, \ \kappa^{\log}, \ h_d(\epsilon)\} \\ & = \ \max\{\kappa^{\log}, \ h_d(\epsilon)\} \end{aligned}$$

(respectively,

$$\begin{aligned} \log(\mathfrak{q}^{\forall}_{(-)}) \ & \leq \ \max\{10^{30} \cdot d^2, \ h_d(\epsilon)\} \\ & = \ h_d(\epsilon)) \end{aligned}$$

[cf. the estimate $h_d(\epsilon) \geq 10^{30} \cdot d^2$] on $\mathfrak{Exc}_{\kappa,d,\epsilon}$ (respectively, $\mathfrak{Exc}^{\mathrm{mcx}}_{d,\epsilon}$).

Thus, in light of Claim 5.2B, it follows from (P8) [cf. also (P1)] that

$$\begin{aligned}\tfrac{1}{6}\cdot h &\leq (1+\epsilon)\cdot(\log(\mathfrak{d}^{F_{\mathrm{tpd}}})+\log(\mathfrak{f}^{F_{\mathrm{tpd}}}))\\ &\leq (1+\epsilon)\cdot(\text{log-diff}_X(x_E)+\text{log-cond}_D(x_E))\end{aligned}$$

— where we apply the fact that for any x, $y\in\mathbb{R}_{>0}$ such that $2x+y\leq\epsilon$, it holds that

$$(1-x)^{-1}\cdot(1+y)\ \leq\ 1+\epsilon$$

[which is a consequence of the fact that $0<\epsilon\leq 1$]. This completes the proof of (C2), hence [cf. (P1), (P7)] of Corollary 5.2. □

Theorem 5.3. (Effective versions of ABC/Szpiro inequalities over mono-complex number fields) *Let L be a* **mono-complex** *number field [cf. Definition 1.2]; a, b, $c\in L^{\times}$ nonzero elements of L such that*

$$a+b+c\ =\ 0;$$

ϵ a positive real number ≤ 1. Write $E_{a,b,c}$ for the elliptic curve over L defined by the equation $y^2=x(x-1)(x+\frac{a}{c})$; $j(E_{a,b,c})$ for the j-invariant of $E_{a,b,c}$; Δ_L for the absolute value of the discriminant of L; $d\stackrel{\text{def}}{=}[L:\mathbb{Q}]$;

$$H_L(a,b,c)\ \stackrel{\text{def}}{=}\ \prod_{v\in\mathbb{V}(L)}\max\{|a|_v,|b|_v,|c|_v\};$$

$$I_L(a,b,c)\ \stackrel{\text{def}}{=}\ \{v\in\mathbb{V}(L)^{\text{non}}\mid \sharp\{|a|_v,|b|_v,|c|_v\}\geq 2\}\ \subseteq\ \mathbb{V}(L)^{\text{non}};$$

$$\text{rad}_L(a,b,c)\ \stackrel{\text{def}}{=}\ \prod_{v\in I_L(a,b,c)}\sharp(\mathcal{O}_L/\mathfrak{p}_v);$$

$$h_d(\epsilon)\ \stackrel{\text{def}}{=}\ \begin{cases}3.4\cdot 10^{30}\cdot\epsilon^{-166/81} & (d=1)\\ 6\cdot 10^{31}\cdot\epsilon^{-174/85} & (d=2).\end{cases}$$

Then the following hold:

(i) *We have [cf. Definition 1.1, (i)]*

$$\begin{aligned}\tfrac{1}{6}\cdot h_{\text{non}}(j(E_{a,b,c})) &\leq \max\{\tfrac{1}{d}\cdot(1+\epsilon)\cdot\log(\Delta_L\cdot\text{rad}_L(a,b,c)),\tfrac{1}{6}\cdot h_d(\epsilon)\}\\ &\leq \tfrac{1}{d}\cdot(1+\epsilon)\cdot\log(\Delta_L\cdot\text{rad}_L(a,b,c))+\tfrac{1}{6}\cdot h_d(\epsilon).\end{aligned}$$

(ii) *We have*

$$\begin{aligned}H_L(a,b,c) &\leq 2^{5d/2}\cdot\max\{\exp(\tfrac{d}{4}\cdot h_d(\epsilon)),(\Delta_L\cdot\text{rad}_L(a,b,c))^{3(1+\epsilon)/2}\}\\ &\leq 2^{5d/2}\cdot\exp(\tfrac{d}{4}\cdot h_d(\epsilon))\cdot(\Delta_L\cdot\text{rad}_L(a,b,c))^{3(1+\epsilon)/2}.\end{aligned}$$

Proof. Assertion (i) follows immediately from Corollary 5.2 [cf. the bound on the restriction of the function "$\log(\mathfrak{q}^{\forall}_{(-)})$" to "$\mathfrak{Exc}^{\text{mcx}}_{d,\epsilon}$"; the displayed inequality of (C2)], Remark 1.10.1, and the various definitions involved. Next, we consider assertion (ii). Write $w\in\mathbb{V}(L)^{\text{arc}}$ for the *unique* element of $\mathbb{V}(L)^{\text{arc}}$ [cf. Definition 1.2]. First, we *claim* the following:

Claim 5.3A: It holds that

$$d \cdot h^{\mathrm{tor}}_{\mathrm{non}}(\tfrac{b}{c}) \;=\; \tfrac{1}{2}\log|bc|_w + \sum_{v \in \mathbb{V}(L)^{\mathrm{non}}} \log\max\{|a|_v, |b|_v, |c|_v\}.$$

Indeed, we compute:

$$\begin{aligned} d \cdot h^{\mathrm{tor}}_{\mathrm{non}}(\tfrac{b}{c}) &= \tfrac{1}{2} \sum_{v \in \mathbb{V}(L)^{\mathrm{non}}} \log\max\{|\tfrac{b}{c}|_v, |\tfrac{c}{b}|_v\} \\ &= \tfrac{1}{2} \sum_{v \in \mathbb{V}(L)^{\mathrm{non}}} \log(\tfrac{1}{|bc|_v} \cdot \max\{|b|_v^2, |c|_v^2\}) \\ &= \tfrac{1}{2}\log|bc|_w + \sum_{v \in \mathbb{V}(L)^{\mathrm{non}}} \log\max\{|b|_v, |c|_v\} \\ &= \tfrac{1}{2}\log|bc|_w + \sum_{v \in \mathbb{V}(L)^{\mathrm{non}}} \log\max\{|a|_v, |b|_v, |c|_v\} \end{aligned}$$

— where the third equality (respectively, the fourth equality) follows from the *product formula* (respectively, the fact that for $v \in \mathbb{V}(L)^{\mathrm{non}}$,

$$|a|_v \;=\; |b+c|_v \;\leq\; \max\{|b|_v, |c|_v\}).$$

This completes the proof of Claim 5.3A.

Next, we observe that, to verify assertion (ii), we may assume without loss of generality that

$$||a||_w \;\leq\; ||b||_w \;\leq\; ||c||_w.$$

Then we observe the following:

Claim 5.3B: It holds that $||\frac{b}{c}||_w \geq \frac{1}{2}$, hence that $|\frac{b}{c}|_w \geq (\frac{1}{2})^d$.

Indeed, since $a + b + c = 0$, we have

$$||c||_w \;=\; ||a+b||_w \;\leq\; ||a||_w + ||b||_w \;\leq\; 2 \cdot ||b||_w.$$

This completes the proof of Claim 5.3B.

Now we *claim* the following:

Claim 5.3C: It holds that

$$\tfrac{1}{6} \cdot h_{\mathrm{non}}(j(E_{a,b,c})) \;\geq\; \tfrac{2}{3d} \cdot \log(H_L(a,b,c)) - \tfrac{5}{3}\log 2.$$

Indeed, it follows from Lemma 1.3, (i), (iv); Proposition 1.8, (i); Remark 1.10.1, that

$$\begin{aligned} (*_1) \qquad \tfrac{1}{6} \cdot h_{\mathrm{non}}(j(E_{a,b,c})) + \tfrac{4}{3}\log 2 &\geq \tfrac{1}{3} \cdot (h^{\mathrm{tor}}_{\mathrm{non}}(\tfrac{a}{c}) + h^{\mathrm{tor}}_{\mathrm{non}}(\tfrac{b}{c}) + h^{\mathrm{tor}}_{\mathrm{non}}(\tfrac{b}{a})) \\ &\geq \tfrac{2}{3} \cdot h^{\mathrm{tor}}_{\mathrm{non}}(\tfrac{b}{c}). \end{aligned}$$

On the other hand, we have

$$\begin{aligned} (*_2) \qquad d \cdot h^{\mathrm{tor}}_{\mathrm{non}}(\tfrac{b}{c}) &= \tfrac{1}{2}\log|bc|_w + \sum_{v \in \mathbb{V}(L)^{\mathrm{non}}} \log\max\{|a|_v, |b|_v, |c|_v\} \\ &= \tfrac{1}{2}\log|\tfrac{b}{c}|_w + \log(H_L(a,b,c)) \\ &\geq \tfrac{d}{2}\log\tfrac{1}{2} + \log(H_L(a,b,c)) \end{aligned}$$

— where the first equality (respectively, the second equality; the final inequality) follows from Claim 5.3A (respectively, the fact that $|c|_w \geq |b|_w \geq$

$|a|_w$; Claim 5.3B). The inequality of Claim 5.3C follows immediately from $(*_1)$ and $(*_2)$.

Finally, in light of assertion (i) and Claim 5.3C, we obtain that

$$\log(H_L(a,b,c)) \;\leq\; \max\{\tfrac{d}{4}\cdot h_d(\epsilon), \tfrac{3}{2}(1+\epsilon)\cdot\log(\Delta_L\cdot \mathrm{rad}_L(a,b,c))\} + \tfrac{5d}{2}\log 2.$$

This completes the proof of assertion (ii). □

Remark 5.3.1. The astronomically large constants in the inequalities established in Theorem 5.3 reflect the explicit [i.e., *"non-conjectural"*] nature of inter-universal Teichmüller theory. Their size may seem quite unexpected, especially from the point of view of the classical [*"conjectural"*] literature on such inequalities, where sometimes it is even naively assumed that these constants may be taken to be as small as 1.

Remark 5.3.2. The approach to applying the version of the ABC inequality established in Theorem 5.3, (ii), to "Fermat's Last Theorem" in the present paper [cf. Corollary 5.8 below] extends to other diophantine equations [cf. Corollary 5.9 below]. Namely, in view of the very large constants [cf. Remark 5.3.1] that appear, in order to apply such an inequality to a concrete diophantine equation of the form $u + v = w$ with polynomial functions u, v, w which involve, respectively, positive integers l, m, n as exponents, one needs first to establish a lower bound on potential solutions of this equation [cf. Lemma 5.7 below; the second to last display of the proof of Corollary 5.9]. One then applies a suitable version of the ABC inequality to obtain an upper bound on l, m, n, under the condition that the diophantine equation admits a solution of the desired type [cf. the portion of the proof of Corollary 5.8 subsequent to the application of Lemma 5.7; the final display of the proof of Corollary 5.9]. Finally, the existence of solutions to the diophantine equation for l, m, n satisfying the upper bound may be investigated by means of computer calculations.

Remark 5.3.3. In the notation of Theorem 5.3, let $\lambda \in L^{\dagger}$. Write E_λ for the elliptic curve over L defined by the equation $y^2 = x(x-1)(x-\lambda)$; $\mathfrak{D}_{E_\lambda}$ (respectively, $\mathfrak{f}_{E_\lambda}$) for the *minimal discriminant ideal* [cf. [Silv1], Chapter VIII, §8, the first Definition] (respectively, *conductor ideal* [cf. [Silv2], Chapter IV, §10, the Definition preceding Example 10.5]) of E_λ over L. Let us first observe that E_λ has *semi-stable reduction* at every place $v \in \mathbb{V}(L)^{\mathrm{non}}$ such that λ is *integral* at v, and v does *not divide* 2. If $v \in \mathbb{V}(L)^{\mathrm{non}}$ is such that λ is *not integral* at v, then observe the following:

> There exists an element $u \in L^\times$ such that $u = \lambda w^2$ for some $w \in L^\times$, and, moreover, u is a *unit* or a *uniformizer* at v. Thus, E_λ is defined by the equation
>
> $$(y')^2 = x'(x'-u)(x'-u\lambda'),$$
>
> where we write $\lambda' \stackrel{\mathrm{def}}{=} \lambda^{-1} \in L^\times$ [so u and $u\lambda'$ are *integral* at v], $x' \stackrel{\mathrm{def}}{=} u\lambda' x$, and $y' \stackrel{\mathrm{def}}{=} w^3 y$.

In particular, by applying a similar argument to the argument applied in [Silv1], Chapter VII, §5, the proof of Proposition 5.4, we obtain that

$$\begin{aligned}\log(N_{L/\mathbb{Q}}(\mathfrak{D}_{E_\lambda})) &\leq d \cdot h_{\mathrm{non}}(j(E_\lambda)) + 6(\log(N_{L/\mathbb{Q}}(\mathfrak{f}_{E_\lambda})) - \log(\mathrm{rad}_L(a,b,c))) \\ &\quad + d \cdot (8-(-4))\log 2\end{aligned}$$

— where we take "a" (respectively, "b"; "c") to be λ (respectively, $1-\lambda$; -1); we write "$N_{L/\mathbb{Q}}(-)$" for the absolute norm of the ideal $(-)$ of $\mathcal{O}_L$; we recall that $N_{L/\mathbb{Q}}(\mathfrak{f}_{E_\lambda}) \geq \mathrm{rad}_L(a,b,c)$ [cf. Remark 1.10.1; [Silv1], Chapter III, §1, Proposition 1.7, (b), and its proof; [Silv2], Chapter IV, §10, Theorem 10.2, (a); [Silv2], Chapter IV, §10, Example 10.5; [Silv2], Chapter IV, §11, Ogg's Formula 11.1 and its proof]. Then it follows immediately from Theorem 5.3, (i), that we have

$$\begin{aligned}N_{L/\mathbb{Q}}(\mathfrak{D}_{E_\lambda}) &\leq 2^{12d} \cdot \max\{\Delta_L^{6(1+\epsilon)} \cdot N_{L/\mathbb{Q}}(\mathfrak{f}_{E_\lambda})^{6(1+\epsilon)}, \exp(d \cdot h_d(\epsilon))\} \\ &\leq 2^{12d} \cdot \Delta_L^{6(1+\epsilon)} \cdot \exp(d \cdot h_d(\epsilon)) \cdot N_{L/\mathbb{Q}}(\mathfrak{f}_{E_\lambda})^{6(1+\epsilon)}.\end{aligned}$$

This may be regarded as an *explicit* version of the inequality

$$\text{"}\mathrm{Norme}_{K/\mathbb{Q}}(\Delta_E) \leq C(K,\epsilon)(\mathrm{Norme}_{K/\mathbb{Q}}(N_E))^{6+\epsilon}\text{"}$$

conjectured in [Szp], §1, CONJECTURE 1 forme forte, in the case of L and E_λ as above.

Remark 5.3.4. Let K be a field such that 2 is *invertible* in K, E an elliptic curve over K whose 2-*torsion points* are K-*rational*. Then, by considering global sections, with suitable *leading terms*, of tensor powers of the line bundle on E determined by the origin [cf., e.g., [Hts], Chapter IV, the proof of Proposition 4.6], one concludes immediately that there exists $\lambda \in K^{\dagger}$ such that E is isomorphic over K to the elliptic curve over K defined by the equation $y^2 = x(x-1)(x-\lambda)$. Conversely, one verifies immediately that the 2-torsion points of any elliptic curve E_λ over K defined by an equation of the form $y^2 = x(x-1)(x-\lambda)$ for some $\lambda \in K^{\dagger}$ are *rational* over K.

Remark 5.3.5. By combining the inequalities in the second to last display of Remark 5.3.3 with [HS], Theorem 0.3, one obtains a *numerically explicit version* of the inequality that appears in a *conjecture of Lang* [cf. [HS], Conjecture 0.1] concerning a lower bound on the canonical height of non-torsion points, for elliptic curves "E_λ" over "L" as in Remarks 5.3.3, 5.3.4. One may also apply the inequalities in the second to last display of Remark 5.3.3 to obtain a "partially numerically explicit" version of the displayed inequality of [HS], Theorem 0.7, for elliptic curves "E_λ" over "L" as in Remarks 5.3.3, 5.3.4.

Theorem 5.4. (Effective version of a conjecture of Szpiro) *Let a, b, c be nonzero coprime integers such that*

$$a + b + c = 0;$$

ϵ a positive real number ≤ 1. Then we have

$$\begin{aligned} |abc| \;=\; ||abc||_{\mathbb{C}} \;&\leq\; 2^4 \cdot \max\{\exp(1.7 \cdot 10^{30} \cdot \epsilon^{-166/81}), (\mathrm{rad}(abc))^{3(1+\epsilon)}\} \\ &\leq\; 2^4 \cdot \exp(1.7 \cdot 10^{30} \cdot \epsilon^{-166/81}) \cdot (\mathrm{rad}(abc))^{3(1+\epsilon)} \end{aligned}$$

— which may be regarded as an explicit version of the inequality

$$\text{“}|abc| \;\leq\; C(\epsilon)\Big(\prod_{p|abc} p\Big)^{3+\epsilon}\text{”}$$

conjectured in [Szp]*, §2 [i.e., the “forme forte” of loc. cit., where we note that the “p” to the right of the “$\prod$” in the above display was apparently unintentionally omitted in loc. cit.].*

Proof. First, we *claim* the following:

Claim 5.4A: In the notation of Theorem 5.3, suppose that

$$||a||_w \;\leq\; ||b||_w \;\leq\; ||c||_w$$

— where $w \in \mathbb{V}(L)^{\mathrm{arc}}$ denotes the unique element of $\mathbb{V}(L)^{\mathrm{arc}}$ [cf. Definition 1.2]. Then it holds that

$$H_L(a,b,c) \;\leq\; 2^{4d/3} \cdot \max\{\exp(\tfrac{d}{6} \cdot h_d(\epsilon)), (\Delta_L \cdot \mathrm{rad}_L(a,b,c))^{1+\epsilon}\} \cdot |abc^{-2}|_w^{-1/3}.$$

Indeed, it follows from Theorem 5.3, (i), that we have

Claim 5.4B: It holds that

$$\tfrac{1}{6} \cdot h_{\mathrm{non}}(j(E_{a,b,c})) \;\leq\; \max\{\tfrac{1}{d} \cdot (1+\epsilon) \cdot \log(\Delta_L \cdot \mathrm{rad}_L(a,b,c)), \tfrac{1}{6} \cdot h_d(\epsilon)\}.$$

Now we *claim* the following:

Claim 5.4C: It holds that

$$\tfrac{1}{6} \cdot h_{\mathrm{non}}(j(E_{a,b,c})) \;\geq\; \tfrac{1}{d} \cdot \log(H_L(a,b,c)) + \tfrac{1}{3d} \cdot \log|abc^{-2}|_w - \tfrac{4}{3}\log 2.$$

Let us verify Claim 5.4C. First, let us recall the inequality $(*_1)$ in the proof of Theorem 5.3

$$(\dagger_1) \qquad \tfrac{1}{6} \cdot h_{\mathrm{non}}(j(E_{a,b,c})) + \tfrac{4}{3}\log 2 \;\geq\; \tfrac{1}{3} \cdot (h^{\mathrm{tor}}_{\mathrm{non}}(\tfrac{a}{c}) + h^{\mathrm{tor}}_{\mathrm{non}}(\tfrac{b}{c}) + h^{\mathrm{tor}}_{\mathrm{non}}(\tfrac{b}{a})).$$

On the other hand, we compute:

$$\begin{aligned} (\dagger_2) \qquad & d \cdot (h^{\mathrm{tor}}_{\mathrm{non}}(\tfrac{a}{c}) + h^{\mathrm{tor}}_{\mathrm{non}}(\tfrac{b}{c}) + h^{\mathrm{tor}}_{\mathrm{non}}(\tfrac{b}{a})) \\ &= \tfrac{1}{2} \cdot (\log|ac|_w + \log|bc|_w + \log|ba|_w) + 3 \sum_{v \in \mathbb{V}(L)^{\mathrm{non}}} \log\max\{|a|_v, |b|_v, |c|_v\} \\ &= \log|abc|_w + 3 \sum_{v \in \mathbb{V}(L)^{\mathrm{non}}} \log\max\{|a|_v, |b|_v, |c|_v\} \\ &= \log|abc^{-2}|_w + 3 \cdot \log(H_L(a,b,c)) \end{aligned}$$

— where the first equality (respectively, the third equality) follows from Claim 5.3A (respectively, the fact that $|c|_w \geq |b|_w \geq |a|_w$). The inequality of Claim 5.4C follows immediately from $(\dagger_1)$ and $(\dagger_2)$. The inequality of Claim 5.4A then follows immediately from the inequalities of Claims 5.4B, 5.4C.

Next, we observe that, to verify Theorem 5.4, we may assume without loss of generality that

$$||a||_{\mathbb{C}} \ \leq \ ||b||_{\mathbb{C}} \ \leq \ ||c||_{\mathbb{C}}.$$

Now we apply the inequality in Claim 5.4A to the present situation, by taking "L" to be $\mathbb{Q}$. Then we have

$$||c||_{\mathbb{C}} \ \leq \ 2^{4/3} \cdot \max\{\exp(\tfrac{1}{6} \cdot 3.4 \cdot 10^{30} \cdot \epsilon^{-166/81}), (\mathrm{rad}(abc))^{1+\epsilon}\} \cdot ||abc^{-2}||_{\mathbb{C}}^{-1/3}.$$

Therefore, by raising this inequality to the 3-rd power, we conclude that

$$||abc||_{\mathbb{C}} \ \leq \ 2^4 \cdot \max\{\exp(1.7 \cdot 10^{30} \cdot \epsilon^{-166/81}), (\mathrm{rad}(abc))^{3(1+\epsilon)}\}.$$

This completes the proof of Theorem 5.4. □

In the following, we give an alternative approach to proving an *effective asymptotic* version of *"Fermat's Last Theorem"*, as proven in [Wls]. The following Lemmas 5.5, 5.6, 5.7 are *entirely elementary*, but their statements and proofs are given in full detail for lack of a suitable reference.

Lemma 5.5. (Elementary identity) *Let $p \geq 3$ be an odd integer; r, s integers such that $r + s \neq 0$. Then we have*

$$(r^p + s^p)(r+s)^{-1} \ = \ ps^{p-1} - (r+s)\sum_{i=0}^{p-2}(-1)^{i+1}(i+1)r^{p-2-i}s^i.$$

Proof. One verifies immediately that we may assume without loss of generality that $r \neq 0$. Then, to verify Lemma 5.5, it suffices to show [by dividing by r^{p-1}] the following equality of elements $\in \mathbb{Q}(x)$:

$$(1+x^p)(1+x)^{-1} \ = \ px^{p-1} - (1+x)\sum_{i=0}^{p-2}(-1)^{i+1}(i+1)x^i.$$

Write ∂ for the derivation d/dx on $\mathbb{Q}(x)$. Then:

$$\begin{aligned} px^{p-1} \ = \ \partial(1+x^p) \ &= \ \partial\{(1+x^p)(1+x)^{-1} \cdot (1+x)\} \\ &= \ (1+x^p)(1+x)^{-1} + (1+x)\partial\{(1+x^p)(1+x)^{-1}\} \\ &= \ (1+x^p)(1+x)^{-1} + (1+x)\partial\Big(\sum_{i=-1}^{p-2}(-1)^{i+1}x^{i+1}\Big) \\ &= \ (1+x^p)(1+x)^{-1} + (1+x)\sum_{i=0}^{p-2}(-1)^{i+1}(i+1)x^i. \end{aligned}$$

This completes the verification of Lemma 5.5. □

Lemma 5.6. (Elementary properties of possible solutions of the Fermat equation) *Let $p \geq 3$ be a prime number; r, s, t nonzero coprime integers such that*

$$r^p + s^p + t^p \;=\; 0.$$

Then the following hold:

(i) *Let l be a prime number which divides $r+s, (r^p+s^p)(r+s)^{-1} \in \mathbb{Z}$. Then it holds that $l = p$.*

(ii) *Suppose that p does* **not divide** *t. Then $r+s$ and $(r^p+s^p)(r+s)^{-1}$ are* **coprime**. *In particular, [since $(r+s)\cdot(r^p+s^p)(r+s)^{-1} = (-t)^p$] there exist integers u and $\tilde{u}$ such that*

$$r+s \;=\; u^p, \qquad (r^p+s^p)(r+s)^{-1} \;=\; \tilde{u}^p \qquad t \;=\; -u\tilde{u}.$$

(iii) *Suppose that p* **divides** *t. Then it holds that*

$$r+s \;\in\; p\mathbb{Z}, \qquad (r^p+s^p)(r+s)^{-1} \;\in\; p\mathbb{Z} \setminus p^2\mathbb{Z}.$$

In particular, if we write $t = p^k v$, where $k \in \mathbb{Z}_{>0}$, $v \in \mathbb{Z} \setminus p\mathbb{Z}$, then [since $(r+s)\cdot(r^p+s^p)(r+s)^{-1} = (-t)^p$] there exist integers $w \notin p\mathbb{Z}$ and $\tilde{w} \notin p\mathbb{Z}$ such that

$$r+s \;=\; p^{kp-1}w^p, \qquad (r^p+s^p)(r+s)^{-1} \;=\; p\tilde{w}^p, \qquad v \;=\; -w\tilde{w}$$

[cf. (i)].

Proof. First, we consider assertion (i). Let l be a prime number which divides $r+s$ and $(r^p+s^p)(r+s)^{-1}$. In particular, it follows from Lemma 5.5 that l divides ps^{p-1}. Thus, if $l \neq p$, then we conclude that l divides s, hence that l divides $r = (r+s) - s$ — a contradiction. This completes the proof of assertion (i).

Next, we consider assertion (ii). Suppose that $r+s$ and $(r^p+s^p)(r+s)^{-1}$ are *not coprime*. Then it follows from assertion (i) that p divides $r+s$ and $(r^p+s^p)(r+s)^{-1}$, hence that p divides $r^p+s^p = (-t)^p$ — a contradiction. Therefore, we conclude that $r+s$ and $(r^p+s^p)(r+s)^{-1}$ are *coprime*. This completes the proof of assertion (ii).

Finally, we consider assertion (iii). We begin by observing that

$$(r+s)^p \;\equiv\; r^p+s^p \;\equiv\; -t^p \;\equiv\; 0 \pmod{p},$$

hence that $r+s \equiv 0 \pmod{p}$. In particular, it follows from Lemma 5.5 that $(r^p+s^p)(r+s)^{-1} \equiv 0 \pmod{p}$. Thus, to verify assertion (iii), it suffices to prove the following *claim*:

Claim 5.6A: It holds that $(r^p+s^p)(r+s)^{-1} \notin p^2\mathbb{Z}$.

Indeed, suppose that $(r^p + s^p)(r+s)^{-1} \in p^2\mathbb{Z}$. Write $r + s = pm$, where $m \in \mathbb{Z}$. Then since we have

$$\begin{aligned}(r^p + s^p)(r+s)^{-1} &= \{r^p + (pm - r)^p\}(pm)^{-1} \\ &= \Big\{r^p + \sum_{i=0}^{p} \binom{p}{i}(pm)^{p-i}(-r)^i\Big\}(pm)^{-1} \\ &= \sum_{i=0}^{p-1} \binom{p}{i}(pm)^{p-i-1}(-r)^i,\end{aligned}$$

our assumption that $(r^p + s^p)(r+s)^{-1} \in p^2\mathbb{Z}$ implies that $pr^{p-1} \in p^2\mathbb{Z}$. Thus, we conclude that $r \in p\mathbb{Z}$, hence that $s = (r+s) - r \in p\mathbb{Z}$ — a contradiction. Therefore, we conclude that $(r^p + s^p)(r+s)^{-1} \notin p^2\mathbb{Z}$. This completes the proof of Claim 5.6A, hence also of assertion (iii). □

Lemma 5.7. (Elementary estimate for possible solutions of the Fermat equation) *Let $p \geq 3$ be a prime number; x, y, z coprime positive integers such that*

$$x^p + y^p = z^p.$$

Then it holds that

$$z > \tfrac{(p+1)^p}{2}.$$

Proof. First, we consider the case where p *divides* xy. [In particular, p does *not divide* z.] In this case, to verify Lemma 5.7, we may assume without loss of generality that p *divides* x. [In particular, p does *not divide* y.] Then it follows by applying Lemma 5.6, (ii), first in the case where we take "(r, s, t)" to be $(x, y, -z)$, then in the case where we take "(r, s, t)" to be $(z, -x, -y)$, that there exist *positive* integers a and b such that

$$x + y = a^p, \qquad z - x = b^p.$$

Here, observe that

$$(z-y)^p \equiv z^p - y^p \equiv x^p \equiv 0 \pmod{p},$$

hence that $z - y \equiv 0 \pmod{p}$. Thus, we obtain that

$$(b-a)^p \equiv b^p - a^p \equiv (z-y) - 2x \equiv 0 \pmod{p},$$

hence that $b - a \equiv 0 \pmod{p}$. Now we *claim* the following:

Claim 5.7A: It holds that $\max\{a, b\} \geq p + 1$.

Indeed, suppose that $\max\{a, b\} \leq p$. Then it follows from the fact that $b - a \equiv 0 \pmod{p}$ that $a = b$, hence that $z = 2x + y$. In particular, we conclude that $z^p = (2x+y)^p > x^p + y^p$ — a contradiction.

In light of Claim 5.7A, we have

$$2z > z + y = a^p + b^p > (p+1)^p.$$

This completes the proof of Lemma 5.7 in the case where p *divides* xy.

Next, we consider the case where p does *not divide* xyz. Then it follows by applying Lemma 5.6, (ii), first in the case where we take "(r, s, t)" to be $(x, y, -z)$, then in the case where we take "(r, s, t)" to be $(z, -x, -y)$, and

finally in the case where we take "(r, s, t)" to be $(z, -y, -x)$, that there exist *positive* integers a, b, and c such that

$$x + y \;=\; a^p, \qquad z - x \;=\; b^p, \qquad z - y \;=\; c^p.$$

Here, observe that

$$(z - x - y)^p \;\equiv\; z^p - x^p - y^p \;\equiv\; 0 \pmod{p},$$

hence that $z - x - y \equiv 0 \pmod{p}$. Thus, we obtain that

$$(b + c - a)^p \;\equiv\; b^p + c^p - a^p \;\equiv\; 2(z - x - y) \;\equiv\; 0 \pmod{p},$$

hence that $b + c - a \equiv 0 \pmod{p}$. Now we *claim* the following:

Claim 5.7B: It holds that $a \geq p + 1$.

Indeed, suppose that $a \leq p$. Observe that since $(2x + y)^p > x^p + y^p = z^p$, $(x + 2y)^p > x^p + y^p = z^p$, it holds that $x + y > z - x$, $x + y > z - y$, hence that $a > b$, $a > c$. Thus, we conclude that

$$-p \;\leq\; -a \;<\; b + c - a \;<\; a + a - a \;\leq\; p,$$

hence that $b + c - a = 0$. Next, we *claim* that

Claim 5.7C: Write $E \stackrel{\text{def}}{=} \{\square \in \{a, b, c\} \mid \square \text{ is even}\}$. Then it holds that $\sharp E = 1$.

Indeed, it follows immediately from the equality $b + c - a = 0$ that $\sharp E \geq 1$. Suppose that $\sharp E \geq 2$. Then it follows from the equality $b + c - a = 0$ that a, b, and c are *even*. In particular, since a^p $(= x + y)$ divides z^p $(= x^p + y^p)$, we conclude that z is *even*. On the other hand, this implies that x and y are *even* [cf. the equalities $z - x = b^p$ and $z - y = c^p$] — a contradiction. This completes the proof of Claim 5.7C.

Now suppose that $E = \{a\}$ [cf. Claim 5.7C]. Here, note that it follows by applying Lemma 5.6, (ii), in the case where we take "(r, s, t)" to be $(x, y, -z)$, that there exists a *positive* integer $\tilde{a}$ such that $(x^p + y^p)(x + y)^{-1} = \tilde{a}^p$. [In particular, we have $z = a\tilde{a}$.] Then since

$$(b^p + c^p)(b + c)^{-1} \;=\; (b^p + c^p)a^{-1} \;=\; (2z - x - y)a^{-1} \;=\; 2\tilde{a} - a^{p-1},$$

we conclude that $(b^p + c^p)(b + c)^{-1}$ is an *even integer*. On the other hand, since

$$(b^p + c^p)(b + c)^{-1} \;=\; \sum_{i=0}^{p-1} (-1)^i b^{p-i-1} c^i,$$

and, moreover, each term "$b^{p-i-1}c^i$" is *odd*, we conclude that $(b^p + c^p)(b + c)^{-1}$ is *odd* — a contradiction.

Thus, it follows from Claim 5.7C that $E \in \{\{b\}, \{c\}\}$. Moreover, to verify Claim 5.7B, we may assume without loss of generality that $E = \{b\}$. Next, observe that it follows by applying Lemma 5.6, (ii), in the case where we take "(r, s, t)" to be $(z, -x, -y)$, that there exists a *positive* integer $\tilde{b}$ such that $(z^p - x^p)(z - x)^{-1} = \tilde{b}^p$. [In particular, we have $y = b\tilde{b}$.] Then since

$$(a^p - c^p)(a - c)^{-1} \;=\; (a^p - c^p)b^{-1} \;=\; (2y + x - z)b^{-1} \;=\; 2\tilde{b} - b^{p-1},$$

we conclude that $(a^p - c^p)(a-c)^{-1}$ is an *even integer*. On the other hand, since

$$(a^p - c^p)(a-c)^{-1} \;=\; \sum_{i=0}^{p-1} a^{p-i-1}c^i,$$

and, moreover, each term "$a^{p-i-1}c^i$" is *odd*, we conclude that $(a^p - c^p)(a-c)^{-1}$ is *odd* — a contradiction. This completes the proof of Claim 5.7B.

In light of Claim 5.7B, we have

$$2z \;>\; x + y \;=\; a^p \;\geq\; (p+1)^p.$$

This completes the proof of Lemma 5.7 in the case where p does *not divide* xyz.

Finally, we consider the case where p *divides* z. [In particular, p does *not divide* xy.] Then it follows by applying Lemma 5.6, (ii), first in the case where we take "(r, s, t)" to be $(z, -x, -y)$, then in the case where we take "(r, s, t)" to be $(z, -y, -x)$, that there exist *positive* integers b and c such that

$$z - x \;=\; b^p, \qquad z - y \;=\; c^p.$$

Moreover, it follows by applying Lemma 5.6, (iii), in the case where we take "(r, s, t)" to be $(x, y, -z)$, that there exist *positive* integers $w \notin p\mathbb{Z}$ and k, together with a *negative* integer $v \notin p\mathbb{Z}$, such that

$$x + y \;=\; p^{kp-1}w^p, \qquad z \;=\; -p^k v.$$

Next, observe that

$$(b+c)^p \;\equiv\; b^p + c^p \;\equiv\; 2z - x - y \;\equiv\; 0 \pmod{p},$$

hence that $b + c \equiv 0 \pmod{p}$. In particular, it follows from the equality

$$b^p + c^p \;=\; pc^{p-1}(b+c) - (b+c)^2 \sum_{i=0}^{p-2} (-1)^{i+1}(i+1)b^{p-2-i}c^i$$

[cf. Lemma 5.5] that $b^p + c^p \in p^2\mathbb{Z}$. Thus, since we have

$$-2p^k v \;=\; 2z \;=\; (z-x) + (z-y) + (x+y) \;=\; b^p + c^p + p^{kp-1}w^p \;\in\; p^2\mathbb{Z}$$

[cf. the fact that $kp - 1 \geq 2$], we conclude that $k \geq 2$. Therefore, we conclude that

$$2z \;>\; x + y \;\geq\; p^{2p-1}w^p \;>\; (p+1)^p$$

[cf. the fact that $\gamma^{2\gamma-1} > (\gamma+1)^\gamma$ for all $\gamma \in \mathbb{R}_{\geq 3}$]. This completes the proof of Lemma 5.7 in the case where p *divides* z. □

Remark 5.7.1.

(i) In the notation of Lemma 5.7, we observe that a stronger estimate

$$z \;>\; z - x \;>\; (2p^{20/7})^p$$

may be obtained by means of techniques of classical algebraic number theory that are somewhat more involved than the argument given above in the proof of Lemma 5.7 [cf. [Ink1]; [Ink2], Theorem 2].

(ii) In fact, it follows from [Ink1], (4), that, in the situation of (i), if we assume further that p divides xyz, then a stronger estimate

$$z \ > \ \tfrac{p^{3p-1}}{2}$$

may be obtained.

Remark 5.7.2. In the notation of Lemma 5.7, suppose that p divides xyz, and that $p \geq 257$. Then we observe that an even stronger estimate [i.e., than the estimate of Remark 5.7.1, (ii)]

$$z \ \geq \ p^{(5/2)^{p-1}}$$

may be obtained by means of techniques that are somewhat more involved than the argument given above in the proof of Lemma 5.7 [cf. [MR], Theorem 1]. [A similar, but weaker estimate may be found in [Mls], Lemma 2.] These techniques of Mihăilescu [and Rassias] use Mihăilescu's technique of working with a map of the Stickelberger ideal into the algebraic integers and related power series developments associated to the image of this map, as well as a new insight on lattices and an "inhomogeneous Siegel box principle".

Corollary 5.8. (Application to "Fermat's Last Theorem") *Let*

$$p \ > \ 1.615 \cdot 10^{14}$$

be a prime number. Then there does not exist any triple (x, y, z) *of positive integers that satisfies the Fermat equation*

$$x^p + y^p \ = \ z^p.$$

Proof. Suppose that there exists a triple (x, y, z) of positive integers such that $x^p + y^p = z^p$. Here, we may assume without loss of generality that x, y, z are *coprime*. Then it follows from Lemma 5.7 that

$$z \ > \ \tfrac{(p+1)^p}{2}.$$

Now we apply Theorem 5.3, (ii), to the present situation, by taking

- "L" to be $\mathbb{Q}$;
- "(a, b, c)" to be $(x^p, y^p, -z^p)$;
- "ϵ" to be 1.

Then, in the notation of Theorem 5.3, we have

$$\begin{aligned} z^p \ &\leq \ 2^{5/2} \cdot \exp(\tfrac{1}{4} \cdot h_1(1)) \cdot (\mathrm{rad}_{\mathbb{Q}}(x^p, y^p, -z^p))^3 \\ &\leq \ 2^{5/2} \cdot \exp(\tfrac{1}{4} \cdot h_1(1)) \cdot (xyz)^3 \\ &\leq \ 2^{5/2} \cdot \exp(\tfrac{1}{4} \cdot h_1(1)) \cdot (z^3)^3 \end{aligned}$$

— where we apply the fact that $z \geq \max\{x, y\}$. Thus, we obtain that

$$\left\{\tfrac{(p+1)^p}{2}\right\}^{p-9} \ < \ z^{p-9} \ \leq \ 2^{5/2} \cdot \exp(\tfrac{1}{4} \cdot h_1(1)).$$

In particular, we conclude that

$$(p-9)(-1+p\cdot\log_2(p+1)) \ < \ \tfrac{5}{2}+\log_2(e)\cdot\tfrac{1}{4}\cdot h_1(1) \ < \ 1.227\cdot 10^{30}.$$

On the other hand, since [as is easily verified] the function

$$(x-9)(-1+1.44x\cdot\log(x+1))$$

is *monotonically increasing* for $x \in \mathbb{R}_{\geq 9}$, we have

$$\begin{aligned}(p-9)(-1+p\cdot\log_2(p+1)) &= (p-9)(-1+\tfrac{1}{\log(2)}\cdot p\cdot\log(p+1))\\ &> (p-9)(-1+1.44\cdot p\cdot\log(p+1))\\ &> 1.227\cdot 10^{30}\end{aligned}$$

— where the first (respectively, second) inequality follows from the estimate $\frac{1}{\log(2)} > 1.44$ (respectively, our assumption that $p > 1.615\cdot 10^{14}$) — a contradiction. This completes the proof of Corollary 5.8. □

Remark 5.8.1. By combining Corollary 5.8 with the numerical estimate of [Cop] [cf. [Cop], Abstract; the discussion following the first display of [Cop], §3], we obtain [by applying the estimate $7.568\cdot 10^{17} > 1.615\cdot 10^{14}$] the following result:

> Let p be an odd prime number. Then there does not exist any triple (x, y, z) of positive integers such that p does not divide xyz, and, moreover, the Fermat equation
>
> $$x^p + y^p \ = \ z^p$$
>
> is satisfied.

This assertion is often called the *first case of Fermat's Last Theorem*.

Remark 5.8.2.

(i) If we apply the estimate

$$z \ > \ (2p^{20/7})^p$$

of Remark 5.7.1, (i), instead of Lemma 5.7 in the proof of Corollary 5.8, then the quantity "$1.615\cdot 10^{14}$" in Corollary 5.8 may be replaced by $9.58\cdot 10^{13}$. Indeed, by applying this estimate of Remark 5.7.1, (i), we obtain the estimate

$$(2p^{20/7})^{p(p-9)} \ < \ z^{p-9} \ \leq \ 2^{5/2}\cdot\exp(\tfrac{1}{4}\cdot h_1(1)).$$

In particular, we conclude that

$$p(p-9)(1+\tfrac{20}{7}\cdot\log_2(p)) \ < \ \tfrac{5}{2}+\log_2(e)\cdot\tfrac{1}{4}\cdot h_1(1) \ < \ 1.227\cdot 10^{30}.$$

Thus, it suffices to observe that the manifestly *monotonically increasing* function

$$x(x-9)(1+\tfrac{20}{7}\cdot\log_2(x))$$

satisfies the inequality $> 1.227\cdot 10^{30}$ for $x > 9.58\cdot 10^{13}$.

(ii) Suppose that p divides xyz. That is to say, we suppose that we are in the situation of what is often called the *second case of Fermat's Last Theorem*. Then if we apply the estimate

$$z \ > \ \frac{p^{3p-1}}{2}$$

of Remark 5.7.1, (ii), instead of Lemma 5.7 in the proof of Corollary 5.8, then the quantity "$1.615 \cdot 10^{14}$" in Corollary 5.8 may be replaced by $9.39 \cdot 10^{13}$. Indeed, by applying this estimate of Remark 5.7.1, (ii), we obtain the estimate

$$(\frac{p^{3p-1}}{2})^{(p-9)} \ < \ z^{p-9} \ \leq \ 2^{5/2} \cdot \exp(\tfrac{1}{4} \cdot h_1(1)).$$

In particular, we conclude that

$$(p-9)((3p-1)\log_2(p) - 1) \ < \ \tfrac{5}{2} + \log_2(e) \cdot \tfrac{1}{4} \cdot h_1(1) \ < \ 1.227 \cdot 10^{30}.$$

Thus, it suffices to observe that the manifestly *monotonically increasing* function

$$(x-9)((3x-1)\log_2(x) - 1)$$

satisfies the inequality $> 1.227 \cdot 10^{30}$ for $x > 9.39 \cdot 10^{13}$.

Remark 5.8.3.

(i) Observe that the estimate of Remark 5.7.2 due to [MR] implies the following consequence:

> Let
>
> $$p \ \geq \ 257$$
>
> be a prime number. Then there does not exist any triple (x, y, z) of positive integers such that p divides xyz, and the Fermat equation
>
> $$x^p + y^p \ = \ z^p$$
>
> is satisfied.

[A similar, but weaker lower bound for p follows, by a similar argument, from [Mls], Lemma 2.] Indeed, by applying the estimate of Remark 5.7.2 [instead of Lemma 5.7] in the proof of Corollary 5.8, we obtain the estimate

$$p^{(5/2)^{p-1}(p-9)} \ \leq \ z^{p-9} \ \leq \ 2^{5/2} \cdot \exp(\tfrac{1}{4} \cdot h_1(1)).$$

In particular, we conclude that

$$(\tfrac{5}{2})^{p-1}(p-9)\log_2(p) \ \leq \ \tfrac{5}{2} + \log_2(e) \cdot \tfrac{1}{4} \cdot h_1(1) \ < \ 1.227 \cdot 10^{30}.$$

Thus, it suffices to observe that the manifestly *monotonically increasing* function

$$(\tfrac{5}{2})^{x-1}(x-9)\log_2(x)$$

satisfies the inequality $\geq 1.227 \cdot 10^{30}$ for $x \geq 257$.

(ii) By combining (i) with the classical result of [Van] [cf. [Van], Theorem VIIa, as well as [Rbm], pp. 200-202], we obtain [by applying the estimate $269 > 257$] an *alternative proof* [i.e., to the proof of [Wls]] of the *second case of Fermat's Last Theorem* [cf. Remark 5.8.2, (ii)]. In particular, in light of Remark 5.8.1, we conclude that the results of the present paper, combined

with the results of [Van], [Cop], and [MR], yield an **unconditional new alternative proof** [i.e., to the proof of [Wls]] of **Fermat's Last Theorem**.

Finally, we give an application of the *ABC inequality* of Theorem 5.4 to a *generalized version of Fermat's Last Theorem*, which does *not* appear to be *accessible* via the techniques involving *modularity* of elliptic curves over $\mathbb{Q}$ and *deformations of Galois representations* that play a central role in [Wls].

Corollary 5.9. (Application to a generalized version of "Fermat's Last Theorem") *Let r, s, t be nonzero integers every two of which are coprime. Write*

$$S \stackrel{\text{def}}{=} \{(X, Y, Z) \in \mathbb{Z}^3 \mid ||XYZ||_{\mathbb{C}} \geq 2\}.$$

Let l, m, n be positive integers such that

$$\min\{l, m, n\} \ > \ \max\{2.453 \cdot 10^{30},\ \log_2 ||rst||_{\mathbb{C}},\ 10 + 5\log_2(\mathrm{rad}(rst))\}.$$

Then there does not exist any triple $(x, y, z) \in S$ of coprime [i.e., the set of prime numbers which divide x, y, and z is empty] integers that satisfies the equation

$$rx^l + sy^m + tz^n \ = \ 0.$$

Proof. Write $k \stackrel{\text{def}}{=} \min\{l, m, n\}$. Suppose that there exists a triple $(x, y, z) \in S$ of coprime integers such that $rx^l + sy^m + tz^n = 0$. Then we *claim* the following:

Claim 5.9A: rx^l, sy^m, and tz^n are *coprime*.

Indeed, suppose that a prime number p divides rx^l, sy^m, and tz^n. Let us consider the set

$$E \stackrel{\text{def}}{=} \{\square \in \{x, y, z\} \mid p \text{ divides } \square\}.$$

Then, by applying our assumption that (x, y, z) are coprime (respectively, every two of (r, s, t) are coprime), we conclude that $\sharp E \leq 2$ (respectively, $\sharp E \geq 2$), hence that $\sharp E = 2$. Thus, to verify Claim 5.9A, we may assume without loss of generality that p *divides* x and y. [In particular, p does *not divide* z.] Then observe that p^k divides rx^l and sy^m, hence also tz^n. In particular, since p does not divide z, we conclude that p^k *divides* t. Thus, we have

$$\log_2 ||rst||_{\mathbb{C}} \ \geq \ \log_2 ||t||_{\mathbb{C}} \ \geq \ \log_2 p^k \ \geq \ k$$

— a contradiction. This completes the proof of Claim 5.9A.

Now we apply Theorem 5.4 to the present situation, by taking

- "(a, b, c)" to be (rx^l, sy^m, tz^n) [cf. Claim 5.9A];
- "ϵ" to be 1.

Then we have

$$\begin{aligned} ||rst||_{\mathbb{C}} \cdot ||xyz||_{\mathbb{C}}^k &\leq ||rstx^l y^m z^n||_{\mathbb{C}} \\ &\leq 2^4 \cdot \max\{\exp(1.7 \cdot 10^{30}), (\mathrm{rad}(rstx^l y^m z^n))^6\} \\ &= 2^4 \cdot \max\{\exp(1.7 \cdot 10^{30}), (\mathrm{rad}(rstxyz))^6\}. \end{aligned}$$

On the other hand, since

$$\begin{aligned} ||rst||_{\mathbb{C}} \cdot ||xyz||_{\mathbb{C}}^k &\geq \mathrm{rad}(rst) \cdot ||xyz||_{\mathbb{C}}^k \\ &> 2^4 \cdot (\mathrm{rad}(rst))^6 \cdot ||xyz||_{\mathbb{C}}^6 \\ &\geq 2^4 \cdot (\mathrm{rad}(rstxyz))^6 \end{aligned}$$

[cf. our assumptions that $k > 4+(6-1)\cdot\log_2(\mathrm{rad}(rst))+6$ and $||xyz||_{\mathbb{C}} \geq 2$], we obtain that

$$2^k \leq ||rst||_{\mathbb{C}} \cdot ||xyz||_{\mathbb{C}}^k \leq 2^4 \cdot \exp(1.7 \cdot 10^{30}),$$

hence that $k \leq 2.453 \cdot 10^{30}$ — a contradiction. This completes the proof of Corollary 5.9. □

References

[Ax1] C. Axler, New bounds for the prime counting function, *Integers* **16** (2016), A22.

[Ax2] C. Axler, Corrigendum to "New bounds for the prime counting function", available at the following URL: `http://math.colgate.edu/~integers/vol16.html`

[BG] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, *Cambridge New Mathematical Monographs* **4**, Cambridge University Press (2006).

[Cop] D. Coppersmith, Fermat's Last Theorem (Case 1) and the Wieferich Criterion, Math. Comp. **54** (1990), pp. 895-902.

[Falt] G. Faltings, Finiteness Theorems for Abelian Varieties over Number Fields, in *Arithmetic Geometry*, ed. by G. Cornell and J.H. Silverman, Springer (1986).

[Hts] R. Hartshorne, *Algebraic Geometry*, *Graduate Texts in Mathematics* **52**, Springer-Verlag (1977).

[HS] M. Hindry and J. H. Silverman, The canonical height and integral points on elliptic curves, *Invent. math.* **93** (1988), pp. 419-450.

[Ink1] K. Inkeri, Abschätzungen für eventuelle Lösungen der Gleichung im Fermatschen Problem, *Ann. Univ. Turkuensis. Ser. A.* **16** (1953), pp. 3-9.

[Ink2] K. Inkeri, Remarks on Fermat's equation in *The very knowledge of coding*, Univ. of Turku (1987), pp. 82-87.

[Lbr] S. Löbrich, A Gap in the Spectrum of the Faltings Height, *Journal de Théorie des Nombres de Bordeaux* **29** (2017), pp. 289-305.

[Mls] P. Mihăilescu, Improved lower bounds for possible solutions in the Second Case of the Fermat Last Theorem and in the Catalan Equation, *J. Number Theory* **225** (2021), pp. 151-173.

[MR] P. Mihăilescu and M. Rassias, Double exponential lower bounds for possible solutions in the Second Case of the Fermat Last Theorem, *J. Number Theory* (2022), available at the following URL: `https://doi.org/10.1016/j.jnt.2021.10.014`

[CanLift] S. Mochizuki, The Absolute Anabelian Geometry of Canonical Curves, *Kazuya Kato's fiftieth birthday*, *Doc. Math. 2003, Extra Vol.*, pp. 609-640.

[EtTh] S. Mochizuki, The Étale Theta Function and its Frobenioid-theoretic Manifestations, *Publ. Res. Inst. Math. Sci.* **45** (2009), pp. 227-349.

[GenEll] S. Mochizuki, Arithmetic Elliptic Curves in General Position, *Math. J. Okayama Univ.* **52** (2010), pp. 1-28.

[IUTchI] S. Mochizuki, Inter-universal Teichmüller Theory I: Construction of Hodge Theaters, *Publ. Res. Inst. Math. Sci.* **57** (2021), pp. 3-207.

[IUTchII] S. Mochizuki, Inter-universal Teichmüller Theory II: Hodge-Arakelov-theoretic Evaluation, *Publ. Res. Inst. Math. Sci.* **57** (2021), pp. 209-401.

[IUTchIII] S. Mochizuki, Inter-universal Teichmüller Theory III: Canonical Splittings of the Log-theta-lattice, *Publ. Res. Inst. Math. Sci.* **57** (2021), pp. 403-626.

[IUTchIV] S. Mochizuki, Inter-universal Teichmüller Theory IV: Log-volume Computations and Set-theoretic Foundations, *Publ. Res. Inst. Math. Sci.* **57** (2021), pp. 627-723.

[Alien] S. Mochizuki, The Mathematics of Mutually Alien Copies: from Gaussian Integrals to Inter-universal Teichmüller Theory, *Inter-universal Teichmüller Theory Summit 2016*, *RIMS Kōkyūroku Bessatsu* **B84**, Res. Inst. Math. Sci. (RIMS), Kyoto (2021), pp. 23-192.

[Rbm] P. Ribenboim, *13 lectures on Fermat's last theorem*, Springer-Verlag, New York-Heidelberg, (1979).

[RS] J. B. Rosser and L. Schoenfeld, Sharper Bounds for the Chebyshev Functions $\theta(x)$ and $\psi(x)$, *Math. Comp.* **29** (1975), pp. 243-269.

[Sijs] J. Sijsling, Canonical models of arithmetic $(1, \infty)$ curves, *Arithmetic geometry: computation and applications*, Contemp. Math., **722**, *Amer. Math. Soc., Providence, RI*, (2019), pp. 149-165.

[Silv1] J. H. Silverman, *The Arithmetic of Elliptic Curves, Second Edition*, *Graduate Texts in Mathematics* **106**, Springer-Verlag (2009).

[Silv2] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, *Graduate Texts in Mathematics* **151**, Springer-Verlag (1994).

[Szp] L. Szpiro, *Discriminant et conducteur des courbes elliptiques* in *Astérisque* **183** (1990), pp. 7-18.

[Van] H. S. Vandiver, Summary of Results and Proofs on Fermat's Last Theorem (Fifth Paper), *Proc. Nat. Acad. Sci. U.S.A.* **16** (1930), pp. 298-304.

[Wls] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* **141** (1995), pp. 443-551.

(Shinichi Mochizuki) Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan
E-mail address: motizuki@kurims.kyoto-u.ac.jp

(Ivan Fesenko) Mathematics Institute, Zeeman Building, University of Warwick, Coventry CV4 7AL, United Kingdom
E-mail address: ivan.b.fesenko@gmail.com

(Yuichiro Hoshi) Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan
E-mail address: yuichiro@kurims.kyoto-u.ac.jp

(Arata Minamide) Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan
E-mail address: minamide@kurims.kyoto-u.ac.jp

(Wojciech Porowski) Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan
E-mail address: wo.porowski@gmail.com