Explicit estimates in inter-universal Teichmüller theory (in progress)

(joint work w/ I. Fesenko, Y. Hoshi, S. Mochizuki, and W. Porowski)

Arata Minamide

RIMS, Kyoto University

November 2, 2018

§0 Notations

F: a number field $\supseteq$ $\mathcal{O}_F$: the ring of integers

Δ_F: the absolute value of the discriminant of F

$\mathbb{V}(F)^{\mathrm{non}}$: the set of nonarchimedean places of F

$\mathbb{V}(F)^{\mathrm{arc}}$: the set of archimedean places of F

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

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

For $v \in \mathbb{V}(F)^{\mathrm{non}}$, write $\mathfrak{p}_v \subseteq \mathcal{O}_F$ for the prime ideal corr. to v

- Let $v \in \mathbb{V}(F)^{\mathrm{non}}$. Write $\mathrm{ord}_v : F^\times \twoheadrightarrow \mathbb{Z}$ for the order def'd by v. Then for any $x \in F$, we shall write

$$|x|_v \stackrel{\mathrm{def}}{=} \sharp(\mathcal{O}_F/\mathfrak{p}_v)^{-\mathrm{ord}_v(x)}.$$

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

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

Note: (Product formula) For $\alpha \in F^\times$, it holds that

$$\prod_{v \in \mathbb{V}(F)} |\alpha|_v = 1.$$

For an elliptic curve E /a field, write $j(E)$ for the j-invariant of E

§1 Introduction

Main theorem of IUTch:

There exist "multiradial representations"— i.e., description up to mild indeterminacies in terms that make sense from the point of view of an alien ring structure — of the following data:

- $G_{\underline{v}} \curvearrowright \mathcal{O}_{\underline{v}}^{\times\boldsymbol{\mu}}$
- $\{q_{\underline{v}}^{j^2/2l}\}_{j=1,\dots,(l-1)/2} \curvearrowright \log(\mathcal{O}_{\underline{v}}^{\times\boldsymbol{\mu}})$ [cf. §2]
- $F_{\mathrm{mod}} \curvearrowright \log(\mathcal{O}_{\underline{v}}^{\times\boldsymbol{\mu}})$

$\Rightarrow$ As an application, we obtain a diophantine inequality.

Write:

For $\lambda \in \overline{\mathbb{Q}} \setminus \{0, 1\}$,

A_λ: the elliptic curve $/\mathbb{Q}(\lambda)$ def'd by "$y^2 = x(x-1)(x-\lambda)$"

$F_\lambda \stackrel{\mathrm{def}}{=} \mathbb{Q}(\lambda, \sqrt{-1}, A_\lambda[3 \cdot 5](\overline{\mathbb{Q}}))$

$\Rightarrow E_\lambda \stackrel{\mathrm{def}}{=} A_\lambda \times_{\mathbb{Q}(\lambda)} F_\lambda$ has at most split multipl. red. at $\forall \in \mathbb{V}(F_\lambda)$

$\mathfrak{q}_\lambda$: the arithmetic divisor det'd by the q-parameter of E_λ/F_λ

$\mathfrak{f}_\lambda$: the "reduced" arithmetic divisor det'd by $\mathfrak{q}_\lambda$

$\mathfrak{d}_\lambda$: the arithmetic divisor det'd by the different of $F_\lambda/\mathbb{Q}$

Theorem (Vojta Conj. — in the case of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ — for "$\mathcal{K}$")

$d \in \mathbb{Z}_{>0} \quad \epsilon \in \mathbb{R}_{>0}$

$\mathcal{K} \subseteq \overline{\mathbb{Q}} \setminus \{0, 1\}$: a compactly bounded subset whose "support" $\ni 2, \infty$

Then ${}^{\exists}B(d, \epsilon, \mathcal{K}) \in \mathbb{R}_{>0}$ — that depends only on d, ϵ, and $\mathcal{K}$ — s.t. the function on $\{\lambda \in \mathcal{K} \mid [\mathbb{Q}(\lambda) : \mathbb{Q}] \leq d\}$ given by

$$\lambda \mapsto \frac{1}{6} \cdot \deg(\mathfrak{q}_\lambda) - (1 + \epsilon) \cdot (\deg(\mathfrak{d}_\lambda) + \deg(\mathfrak{f}_\lambda))$$

is bounded by $B(d, \epsilon, \mathcal{K})$.

Then, by applying the theory of noncritical Belyi maps, we obtain

$(*)$: the "version with $\mathcal{K}$ removed" of this Theorem.

Finally, we conclude:

Theorem (ABC Conjecture for number fields)

$d \in \mathbb{Z}_{>0} \quad \epsilon \in \mathbb{R}_{>0}$

Then $^{\exists}C(d, \epsilon) \in \mathbb{R}_{>0}$ — that depends only on d and ϵ — s.t. for

- F: a number field — where $d = [F : \mathbb{Q}]$
- (a, b, c) : a triple of elements $\in F^{\times}$ — where $a + b + c = 0$

we have

$$H_F(a, b, c) < C(d, \epsilon) \cdot (\Delta_F \cdot \mathrm{rad}_F(a, b, c))^{1+\epsilon}$$

— where

$$H_F(a, b, c) \stackrel{\mathrm{def}}{=} \prod_{v \in \mathbb{V}(F)} \max\{|a|_v, |b|_v, |c|_v\},$$

$$\mathrm{rad}_F(a, b, c) \stackrel{\mathrm{def}}{=} \prod_{\{v \in \mathbb{V}(F)^{\mathrm{non}} \mid \sharp\{|a|_v, |b|_v, |c|_v\} \geq 2\}} \sharp(\mathcal{O}_F / \mathfrak{p}_v).$$

Note: We do not know the constant "$C(d, \epsilon)$" explicitly.

For instance, it is hard to compute noncritical Belyi maps explicitly!

Goal of this joint work: Under certain conditions, we prove $(*)$ directly [i.e., without applying the theory of noncritical Belyi maps] to compute the constant "$C(d, \epsilon)$" explicitly.

Technical Difficulties of Explicit Computations

(i) We cannot use the compactness of "$\mathcal{K}$" at the place 2

$\Rightarrow$ We develop the theory of étale theta functions so that it works at the place 2

(ii) We cannot use the compactness of "$\mathcal{K}$" at the place ∞

$\Rightarrow$ By restricting our attention to "special" number fields, we "bound" the archimedean portion of the "height" of the elliptic curve "E_λ"

§2 Theta Functions

p, l: distinct prime numbers — where $l \geq 5$

K: a p-adic local field $\supseteq$ $\mathcal{O}_K$: the ring of integers

X: an elliptic curve $/K$ which has split multipl. red. $/\mathcal{O}_K$

$q \in \mathcal{O}_K$: the q-parameter of X

$X^{\log} \stackrel{\mathrm{def}}{=} (X, \{o\} \subseteq X)$: the smooth log curve $/K$ assoc. to X

In the following, we assume that

- $\sqrt{-1} \in K$
- $X[2l](\overline{K}) = X[2l](K)$
- $X^{\log}//\{\pm 1\}$ is a K-core

Now we have the following sequence of log tempered coverings:

$$\ddot{Y}^{\log} \xrightarrow{\mu_2} Y^{\log} \xrightarrow{l\cdot\underline{\mathbb{Z}}} \underline{X}^{\log} \xrightarrow{\underline{\mathbb{F}}_l} X^{\log}$$

— where

- $Y^{\log} \to \underline{X}^{\log} \to X^{\log}$ is det'd by the [graph-theoretic] universal covering of the dual graph of the special fiber of $X^{\log}$. Write

$$\underline{\mathbb{Z}} \stackrel{\mathrm{def}}{=} \mathrm{Gal}(Y^{\log}/X^{\log}) \ \ (\cong \mathbb{Z}).$$

- $\underline{X}^{\log} \to X^{\log}$ corresponds to $l \cdot \underline{\mathbb{Z}} \subseteq \underline{\mathbb{Z}}$. Write

$$\underline{\mathbb{F}}_l \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\underline{X}^{\log}/X^{\log}) \ \ (\cong \mathbb{F}_l).$$

- $\ddot{Y}^{\log} \to Y^{\log}$ is the double covering det'd by "$u = \ddot{u}^2$".

Write: For a curve $(-)$ over K,

$\mathrm{Ver}(-)$: the set of irreducible components of the special fiber of $(-)$

• First, we recall the def'n of evaluation points on $\ddot{Y}^{\log}$.

We fix a cusp of $\underline{X}^{\log}$ and refer to the zero cusp $\underline{X}^{\log}$.

$\Rightarrow$ $\underline{X}$ admits a str. of elliptic curve whose origin is the zero cusp.

$0_{\underline{X}} \in \mathrm{Ver}(\underline{X}^{\log})$: the irreducible comp. which contain the "origin"

Then we fix a lift. $\exists \in \mathrm{Ver}(Y^{\log})$ of $0_{\underline{X}} \in \mathrm{Ver}(\underline{X}^{\log})$ and write

$$0_Y \ \in \ \mathrm{Ver}(Y^{\log}).$$

$0_{\ddot{Y}} \in \mathrm{Ver}(\ddot{Y}^{\log})$: the irreducible comp. lying over $0_Y \in \mathrm{Ver}(\ddot{Y}^{\log})$

Note: Since $\mathrm{Ver}(Y^{\log})$ is a $\underline{\mathbb{Z}}$-torsor, we obtain a labeling

$$\underline{\mathbb{Z}} \overset{\sim}{\to} \mathrm{Ver}(Y^{\log}) \overset{\sim}{\to} \mathrm{Ver}(\ddot{Y}^{\log}).$$

Assume: $p \neq 2$

$\mu_{-} \in \underline{X}(K)$: the 2-torsion point — not equal to the origin — whose closure intersects $0_{\underline{X}} \in \mathrm{Ver}(\underline{X}^{\log})$

$\mu_{-}^{Y} \in Y(K)$: a $^{\exists!}$lift. of μ_{-} whose closure intersects $0_{Y} \in \mathrm{Ver}(Y^{\log})$

$\xi_{j}^{Y} \in Y(K)$: the image of μ_{-}^{Y} by the action of $j \in \underline{\mathbb{Z}}$

Definition

an evaluation point of $\ddot{Y}^{\log}$ labeled by $j \in \underline{\mathbb{Z}}$

$$\overset{\text{def}}{\Leftrightarrow} \text{ a lifting } \in \ddot{Y}(K) \text{ of } \xi_{j}^{Y} \in Y(K)$$

• Next, we recall the def'n of the theta function $\ddot{\Theta}$.

The function

$$\ddot{\Theta}(\ddot{u}) \stackrel{\text{def}}{=} q^{-\frac{1}{8}} \cdot \sum_{n \in \mathbb{Z}} (-1)^n \cdot q^{\frac{1}{2}(n+\frac{1}{2})^2} \cdot \ddot{u}^{2n+1}$$

on $\ddot{Y}^{\log}$ extends uniquely to a meromorphic function $\ddot{\Theta}$ on the stable model of $\ddot{Y}$, and satisfies the following property:

$$\ddot{\Theta}(\xi_j)^{-1} = \pm \ddot{\Theta}(\xi_0)^{-1} \cdot q^{\frac{j^2}{2}}.$$

— where $\xi_j \in \ddot{Y}(K)$ is an evaluation point labeled by $j \in \underline{\mathbb{Z}}$.

Definition

Write

$$\ddot{\Theta}_{\text{st}} \stackrel{\text{def}}{=} \ddot{\Theta}(\xi_0)^{-1} \cdot \ddot{\Theta}$$

and refer to $\ddot{\Theta}_{\text{st}}$ as a theta function of μ_2-standard type.

We want to develop the theory of Θ functions in the case of $p = 2$.

$\Rightarrow$ In this work, instead of "2-torsion points", we consider

6-torsion points of $\underline{X}(K)$!

Lemma (Well-definedness of the notion of "μ_6-standard type")

$n \in \mathbb{Z}_{>0}$: an even integer

k: an alg. cl. ch. zero fld. $\supseteq$ $\mu_{2n}^{\times}$: the set of pr. $2n$-th roots of unity

Γ_{-} (resp. Γ^{-}): the group of $\sharp = 2$ which acts on $\mu_{2n}^{\times}$ as follows:

$$\zeta \mapsto -\zeta \qquad (\text{resp. } \zeta \mapsto \zeta^{-1})$$

Then the action $\Gamma_{-} \times \Gamma^{-}$ on $\mu_{2n}^{\times}$ is transitive $\Leftrightarrow$ $n \in \{2, 4, 6\}$

Note: We have $\ddot{\Theta}(-\ddot{u}) = -\ddot{\Theta}(\ddot{u})$ and $\ddot{\Theta}(\ddot{u}^{-1}) = -\ddot{\Theta}(\ddot{u})$.

§3 Heights

First, we recall the notion of the Weil height of an algebraic number.

Definition

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

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

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

and refer to $h(\alpha)$ as the Weil height of α.

Observe: Let $n \in \mathbb{Q}$ be a positive integer. Then we have

$$h_{\mathrm{non}}(n) = 0, \quad h_{\mathrm{arc}}(n) = \log(n).$$

In this work, we introduce a variant of the notion of the Weil height.

Definition

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

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

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

and refer to $h^{\mathrm{tor}}(\alpha)$ as the toric height of α.

Observe: Let $n \in \mathbb{Q}$ be a positive integer. Then we have

$$h_{\mathrm{non}}(n) = \tfrac{1}{2}\log(n), \quad h_{\mathrm{arc}}(n) = \tfrac{1}{2}\log(n).$$

Remark

For $\alpha \in F^{\times}$, it holds that $h(\alpha) = h^{\mathrm{tor}}(\alpha)$.

Definition

A number field F is mono-complex $\overset{\mathrm{def}}{\Leftrightarrow}$ $\sharp\mathbb{V}(F)^{\mathrm{arc}} = 1$
($\Leftrightarrow F$ is either $\mathbb{Q}$ or an imaginary quadratic number field)

Proposition (Important property of $h^{\mathrm{tor}}_{\square}$)

F: a mono-complex number field

For $\alpha \in F^{\times}$, it holds that $h^{\mathrm{tor}}_{\mathrm{arc}}(\alpha) \leq h^{\mathrm{tor}}_{\mathrm{non}}(\alpha)$.

Proof: This follows immediately from the product formula.

Next, we introduce the notion of the "height" of an elliptic curve.

Definition

$F \subseteq \overline{\mathbb{Q}}$: a number field

E: an elliptic curve $/F \quad \overset{\sim}{\to}_{\overline{\mathbb{Q}}}$ "$y^2 = x(x-1)(x-\lambda)$" $\;(\lambda \in \overline{\mathbb{Q}} \setminus \{0,1\})$

Note: $\mathfrak{S}_3 \ {}^{\exists} \curvearrowright \ (\mathbb{P}_{\mathbb{Q}} \setminus \{0,1,\infty\})(\overline{\mathbb{Q}}) \ \overset{\sim}{\to} \ \overline{\mathbb{Q}} \setminus \{0,1\}$

For $\square \in \{\mathrm{non}, \mathrm{arc}\}$, we shall write

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

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

and refer to $h^{\mathfrak{S}\text{-tor}}(E)$ as the symmetrized toric height of E.

Proposition (Important property of $h_{\square}^{\mathfrak{S}\text{-tor}}$)

Suppose: $\mathbb{Q}(\lambda)$ is mono-complex

Then it holds that $h_{\mathrm{arc}}^{\mathfrak{S}\text{-tor}}(E) \leq h_{\mathrm{non}}^{\mathfrak{S}\text{-tor}}(E)$.

Proof: This follows immediately from the previous Proposition.

Now we note that we have an equality "$\deg(\mathfrak{q}_\lambda) = h_{\mathrm{non}}(j(E_\lambda))$".

Theorem (Comparison between $h_{\square}^{\mathfrak{S}\text{-tor}}(E)$ and $h_{\square}(j(E))$)

$^\exists$explicitly computable abs. const. C_1, C_2, C_3, $C_4 \in \mathbb{R}$ s.t.

$$C_1 \leq h_{\mathrm{non}}^{\mathfrak{S}\text{-tor}}(E) - h_{\mathrm{non}}(j(E)) \leq C_2,$$

$$C_3 \leq h_{\mathrm{arc}}^{\mathfrak{S}\text{-tor}}(E) - h_{\mathrm{arc}}(j(E)) \leq C_4.$$

§4 Some Remarks on Explicit Computations

Theorem (Effective ver. of the PNT — due to Rosser and Schoenfeld)

$^{\exists}$explicitly computable $\xi_{\mathrm{prm}} \in \mathbb{R}_{\geq 5}$ s.t. for $^{\forall}x \geq \xi_{\mathrm{prm}}$, it holds that

$$\frac{2}{3} \cdot x \;\leq\; \sum_{p:\mathrm{prime} \;\leq\; x} \log(p) \;\leq\; \frac{4}{3} \cdot x.$$

Theorem (j-invariant of "special" elliptic curves — due to Sijsling)

k: an alg. closed field of char. zero

E: an elliptic curve $/k$

Suppose: $E \setminus \{o\}$ fails to admit a k-core.

Then it holds that $j(E) \in \{\frac{488095744}{125}, \frac{1556068}{81}, 1728, 0\}$.

§5 Expected Main Results

Expected Theorem (Effective ABC for mono-complex number fields)

$d \in \{1, 2\} \quad \epsilon \in \mathbb{R}_{>0}$

Then $^{\exists}$explicitly computable $C(d, \epsilon) \in \mathbb{R}_{>0}$ — that depends only on d and ϵ — s.t. for

- F: a mono-complex number field — where $d = [F : \mathbb{Q}]$
- (a, b, c) : a triple of elements $\in F^{\times}$ — where $a + b + c = 0$

we have

$$H_F(a, b, c) < C(d, \epsilon) \cdot (\Delta_F \cdot \mathrm{rad}_F(a, b, c))^{\frac{3}{2}+\epsilon}.$$

Expected Corollary (Application to Fermat's Last Theorem)

$^{\exists}$explicitly computable $n_0 \in \mathbb{Z}_{\geq 3}$ s.t. if $n \geq n_0$, then no triple (x, y, z) of positive integers satisfies

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