Explicit Estimates in Inter-universal Teichmüller Theory (joint work w/ S. Mochizuki, I. Fesenko, Y. Hoshi, and W. Porowski)

Arata Minamide

RIMS, Kyoto University

September 7, 2021

Notations

$\mathfrak{Primes}$: the set of all prime numbers

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

Log-volume estimates for Θ-pilot objects (cf. [IUTchIII], Cor 3.12)

Theorem

Write

$$-|\log(\underline{\underline{\Theta}})| \in \mathbb{R} \cup \{\infty\}$$

for the (process.-normalized, mono-an.) log-volume of the "holomorphic hull" of the union of the possible images of a Θ-pilot object, rel. to the relevant Kum. isoms, in the multira'l rep'n of [IUTchIII], Thm 3.11, (i), which we regard as sub. to (Ind1), (Ind2), (Ind3);

Log-volume estimates for Θ-pilot objects (cf. [IUTchIII], Cor 3.12)

Theorem

Write

$$-|\log(\underline{\underline{\Theta}})| \in \mathbb{R} \cup \{\infty\}$$

for the (process.-normalized, mono-an.) log-volume of the "holomorphic hull" of the union of the possible images of a Θ-pilot object, rel. to the relevant Kum. isoms, in the multira'l rep'n of [IUTchIII], Thm 3.11, (i), which we regard as sub. to (Ind1), (Ind2), (Ind3);

$$-|\log(\underline{\underline{q}})| \in \mathbb{R}$$

for the (process.-normalized, mono-an.) log-volume of the image of a q-pilot object, rel. to the relevant Kum. isoms, in the multirad'l rep'n.

Log-volume estimates for Θ-pilot objects (cf. [IUTchIII], Cor 3.12)

Theorem

Write

$$-|\log(\underline{\underline{\Theta}})| \;\in\; \mathbb{R} \cup \{\infty\}$$

for the (process.-normalized, mono-an.) log-volume of the "holomorphic hull" of the union of the possible images of a Θ-pilot object, rel. to the relevant Kum. isoms, in the multira'l rep'n of [IUTchIII], Thm 3.11, (i), which we regard as sub. to (Ind1), (Ind2), (Ind3);

$$-|\log(\underline{\underline{q}})| \;\in\; \mathbb{R}$$

for the (process.-normalized, mono-an.) log-volume of the image of a $\underline{\underline{q}}$*-pilot object, rel. to the relevant Kum. isoms, in the multirad'l rep'n.*

Then it holds that $-|\log(\underline{\underline{\Theta}})| \in \mathbb{R}$, *and* $-|\log(\underline{\underline{\Theta}})| \geq -|\log(\underline{\underline{q}})|$.

Results in [IUTchIV]

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

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

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

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

$\mathfrak{q}_\lambda$: the arithmetic divisor det'd by the q-parameters 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 "$\mathcal{K}$")

Let $d \in \mathbb{Z}_{>0}$, $\epsilon \in \mathbb{R}_{>0} \cap \mathbb{R}_{\leq 1}$,

$\mathcal{K} \subseteq \overline{\mathbb{Q}} \setminus \{0, 1\}$: 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 $\mathcal{K}^{\leq d} \stackrel{\text{def}}{=} \{\lambda \in \mathcal{K} \mid [\mathbb{Q}(\lambda) : \mathbb{Q}] \leq d\}$ 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 $B(d, \epsilon, \mathcal{K})$.

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

Let $d \in \mathbb{Z}_{>0}$, $\epsilon \in \mathbb{R}_{>0} \cap \mathbb{R}_{\leq 1}$,

$\mathcal{K} \subseteq \overline{\mathbb{Q}} \setminus \{0, 1\}$: 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 $\mathcal{K}^{\leq d} \stackrel{\text{def}}{=} \{\lambda \in \mathcal{K} \mid [\mathbb{Q}(\lambda) : \mathbb{Q}] \leq d\}$ 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 $B(d, \epsilon, \mathcal{K})$.

Proof: By applying

- the finiteness of $\{\lambda \in \mathcal{K}^{\leq d} \mid \deg(\mathfrak{q}_\lambda) \leq \gamma\}$ $(\gamma \in \mathbb{R}_{>0})$ (cf. Northcott's theorem),

- $\sharp\{j($"arithmetic" elliptic curve over a field of char. zero$)\} = 4$ (cf. Takeuchi's list),
- the prime number theorem,
- the theory of Galois actions on torsion points of elliptic curves (cf. [GenEll]),

we conclude that for all but finitely many $\lambda \in \mathcal{K}^{\leq d}$, there exists a prime number l_λ such that

- $\sharp\{j($"arithmetic" elliptic curve over a field of char. zero$)\} = 4$ (cf. Takeuchi's list),
- the prime number theorem,
- the theory of Galois actions on torsion points of elliptic curves (cf. [GenEll]),

we conclude that for all but finitely many $\lambda \in \mathcal{K}^{\leq d}$, there exists a prime number l_λ such that

(i) $^\exists$an initial Θ-data $(\overline{\mathbb{Q}}/F_\lambda,\ E_\lambda,\ l_\lambda,\ \dots)$ s.t. E_λ has good red. at every $\in \mathbb{V}(F_\lambda)^{\mathrm{good}} \cap \mathbb{V}(F_\lambda)^{\mathrm{non}}$ that does not divide $2l_\lambda$

(In the following, we shall write

$\mathfrak{q}_\lambda^{\mathrm{bad}}$: the arithmetic divisor det'd by "restricting $\mathfrak{q}_\lambda$ to $\mathbb{V}_{\mathrm{mod}}^{\mathrm{bad}}$".)

(ii) $\frac{1}{6} \cdot \deg(\mathfrak{q}_\lambda^{\mathrm{bad}}) \;\leq\; (1 + \frac{20 d_\lambda}{l_\lambda}) \cdot (\deg(\mathfrak{d}_\lambda) + \deg(\mathfrak{f}_\lambda)) + 20 \cdot \delta_\lambda \cdot l_\lambda$,

where $d_\lambda := [\mathbb{Q}(\lambda) : \mathbb{Q}]$, $\delta_\lambda := 2^{12} \cdot 3^3 \cdot 5 \cdot d_\lambda$ (cf. (i); "Cor 3.12")

(iii) $\mathrm{ord}_{l_\lambda}(q_\Box) \;<\; \deg(\mathfrak{q}_\lambda)^{1/2}$, where $\mathbb{V}(F_\lambda) \ni \Box | l_\lambda$

(iv) $\deg(\mathfrak{q}_\lambda)^{1/2} \;\leq\; l_\lambda \;\leq\; 10 \cdot \delta \cdot \deg(\mathfrak{q}_\lambda)^{1/2} \cdot \log(2 \cdot \delta \cdot \deg(\mathfrak{q}_\lambda))$

where $\delta := 2^{12} \cdot 3^3 \cdot 5 \cdot d$

(ii) $\frac{1}{6} \cdot \deg(\mathfrak{q}_\lambda^{\mathrm{bad}}) \ \leq \ (1 + \frac{20 d_\lambda}{l_\lambda}) \cdot (\deg(\mathfrak{d}_\lambda) + \deg(\mathfrak{f}_\lambda)) + 20 \cdot \delta_\lambda \cdot l_\lambda$,
where $d_\lambda := [\mathbb{Q}(\lambda) : \mathbb{Q}]$, $\delta_\lambda := 2^{12} \cdot 3^3 \cdot 5 \cdot d_\lambda$ (cf. (i); "Cor 3.12")

(iii) $\mathrm{ord}_{l_\lambda}(q_\Box) \ < \ \deg(\mathfrak{q}_\lambda)^{1/2}$, where $\mathbb{V}(F_\lambda) \ni \Box | l_\lambda$

(iv) $\deg(\mathfrak{q}_\lambda)^{1/2} \ \leq \ l_\lambda \ \leq \ 10 \cdot \delta \cdot \deg(\mathfrak{q}_\lambda)^{1/2} \cdot \log(2 \cdot \delta \cdot \deg(\mathfrak{q}_\lambda))$
where $\delta := 2^{12} \cdot 3^3 \cdot 5 \cdot d$

Then it follows from (i), (iii) [cf. also the "compactness" of $\mathcal{K}$] that

$$\lambda \ \mapsto \ \frac{1}{6}\deg(\mathfrak{q}_\lambda) - \frac{1}{6}\deg(\mathfrak{q}_\lambda^{\mathrm{bad}}) - \deg(\mathfrak{q}_\lambda)^{1/2}\log(2\delta\deg(\mathfrak{q}_\lambda))$$

is bounded. On the other hand, it follows from (ii), (iv) that

$$\frac{1}{6}\deg(\mathfrak{q}_\lambda^{\mathrm{bad}}) \;\leq\; (1+\delta\cdot\deg(\mathfrak{q}_\lambda)^{-1/2})(\deg(\mathfrak{d}_\lambda)+\deg(\mathfrak{f}_\lambda)) + 200\delta^2\cdot\deg(\mathfrak{q}_\lambda)^{1/2}\log(2\delta\deg(\mathfrak{q}_\lambda)).$$

$$\tfrac{1}{6}\deg(\mathfrak{q}_\lambda^{\mathrm{bad}}) \;\leq\; (1+\delta\cdot\deg(\mathfrak{q}_\lambda)^{-1/2})(\deg(\mathfrak{d}_\lambda)+\deg(\mathfrak{f}_\lambda)) + 200\delta^2\cdot\deg(\mathfrak{q}_\lambda)^{1/2}\log(2\delta\deg(\mathfrak{q}_\lambda)).$$

In particular, these two displays imply that $\lambda \mapsto$

$$(1-\tfrac{2}{5}\tfrac{(60\delta)^2\log(2\delta\deg(\mathfrak{q}_\lambda))}{\deg(\mathfrak{q}_\lambda)^{1/2}})\tfrac{1}{6}\deg(\mathfrak{q}_\lambda) - (1+\tfrac{\delta}{\deg(\mathfrak{q}_\lambda)^{1/2}})(\deg(\mathfrak{d}_\lambda)+\deg(\mathfrak{f}_\lambda))$$

is bounded.

$$\frac{1}{6}\deg(\mathfrak{q}_\lambda^{\mathrm{bad}}) \;\leq\; (1+\delta\cdot\deg(\mathfrak{q}_\lambda)^{-1/2})(\deg(\mathfrak{d}_\lambda)+\deg(\mathfrak{f}_\lambda)) + 200\delta^2\cdot\deg(\mathfrak{q}_\lambda)^{1/2}\log(2\delta\deg(\mathfrak{q}_\lambda)).$$

In particular, these two displays imply that $\lambda \mapsto$

$$(1-\tfrac{2}{5}\tfrac{(60\delta)^2\log(2\delta\deg(\mathfrak{q}_\lambda))}{\deg(\mathfrak{q}_\lambda)^{1/2}})\tfrac{1}{6}\deg(\mathfrak{q}_\lambda)-(1+\tfrac{\delta}{\deg(\mathfrak{q}_\lambda)^{1/2}})(\deg(\mathfrak{d}_\lambda)+\deg(\mathfrak{f}_\lambda))$$

is bounded. By enlarging our "exceptional set", we conclude that

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

is bounded. This completes the proof of Theorem.

$$\tfrac{1}{6}\deg(\mathfrak{q}_\lambda^{\mathrm{bad}}) \;\le\; (1+\delta\cdot\deg(\mathfrak{q}_\lambda)^{-1/2})(\deg(\mathfrak{d}_\lambda)+\deg(\mathfrak{f}_\lambda)) + 200\delta^2\cdot\deg(\mathfrak{q}_\lambda)^{1/2}\log(2\delta\deg(\mathfrak{q}_\lambda)).$$

In particular, these two displays imply that $\lambda \mapsto$

$$(1-\tfrac{2}{5}\tfrac{(60\delta)^2\log(2\delta\deg(\mathfrak{q}_\lambda))}{\deg(\mathfrak{q}_\lambda)^{1/2}})\tfrac{1}{6}\deg(\mathfrak{q}_\lambda)-(1+\tfrac{\delta}{\deg(\mathfrak{q}_\lambda)^{1/2}})(\deg(\mathfrak{d}_\lambda)+\deg(\mathfrak{f}_\lambda))$$

is bounded. By enlarging our "exceptional set", we conclude that

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

is bounded. This completes the proof of Theorem.

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

($*$): the "version with $\mathcal{K}$ removed" of Theorem (cf. [GenEll]).

Theorem (Corollary of $(*)$ — ABC Conjecture for number fields)

Let $d \in \mathbb{Z}_{>0}$, $\epsilon \in \mathbb{R}_{>0} \cap \mathbb{R}_{\leq 1}$.

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

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

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

Theorem (Corollary of $(*)$ — ABC Conjecture for number fields)

Let $d \in \mathbb{Z}_{>0}$, $\epsilon \in \mathbb{R}_{>0} \cap \mathbb{R}_{\leq 1}$.

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

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

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

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

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

Computations concerning (ii)

For $\gamma \in \mathbb{R}$, we shall write $\lfloor \gamma \rfloor$ (resp. $\lceil \gamma \rceil$) for the largest integer $\leq \gamma$ (resp. the smallest integer $\geq \gamma$).

$\{k_i\}_{i \in I}$: a finite set of p-adic local fields ($\mathcal{O}_{k_i}$: the ring of integers)

e_i (resp. $\mathfrak{d}_i$): the abs. ram. index (resp. the order of an gen. of δ_{k_i})

$$a_i \overset{\text{def}}{=} \begin{cases} \frac{1}{e_i} \lceil \frac{e_i}{p-2} \rceil & (p > 2) \\ 2 & (p = 2) \end{cases} \qquad b_i \overset{\text{def}}{=} \lfloor \frac{\log(p \cdot e_i/(p-1))}{\log(p)} \rfloor - \frac{1}{e_i}$$

$$a_I \overset{\text{def}}{=} \sum_{i \in I} a_i, \qquad b_I \overset{\text{def}}{=} \sum_{i \in I} b_i, \qquad \mathfrak{d}_I \overset{\text{def}}{=} \sum_{i \in I} \mathfrak{d}_i$$

$\mu^{\log}_{k_I}$: the (nor'd) log-vol. on $k_I \overset{\text{def}}{=} \otimes_{i \in I} k_i$ s.t. $\mu^{\log}_{k_I}(\otimes_{i \in I} \mathcal{O}_{k_i}) = 0$

Lemma

For $\lambda \in \frac{1}{e_i}\mathbb{Z}$, *write* $p^{\lambda}\mathcal{O}_{k_i}$ *for the fractional ideal generated by any element* $x \in k_i$ *s.t.* $\mathrm{ord}(x) = \lambda$. *Let*

$$\phi : \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \bigotimes_{i \in I} \log_p(\mathcal{O}_{k_i}^{\times}) \xrightarrow{\sim} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \bigotimes_{i \in I} \log_p(\mathcal{O}_{k_i}^{\times})$$

be an automorphism of the finite dimensional $\mathbb{Q}_p$*-vector space that induces an automorphism of the submodule* $\bigotimes_{i \in I} \log_p(\mathcal{O}_{k_i}^{\times})$.

Lemma

For $\lambda \in \frac{1}{e_i}\mathbb{Z}$, *write* $p^\lambda \mathcal{O}_{k_i}$ *for the fractional ideal generated by any element* $x \in k_i$ *s.t.* $\mathrm{ord}(x) = \lambda$. *Let*

$$\phi : \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \bigotimes_{i \in I} \log_p(\mathcal{O}_{k_i}^\times) \overset{\sim}{\to} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \bigotimes_{i \in I} \log_p(\mathcal{O}_{k_i}^\times)$$

be an automorphism of the finite dimensional $\mathbb{Q}_p$*-vector space that induces an automorphism of the submodule* $\bigotimes_{i \in I} \log_p(\mathcal{O}_{k_i}^\times)$.

(i) *Write* $I^* \overset{\mathrm{def}}{=} \{i \in I \mid e_i > p-2\}$. *For any* $\lambda \in \frac{1}{e_{i_0}}\mathbb{Z}$, $i_0 \in I$,

$$\phi(p^\lambda (\otimes_{i \in I} \mathcal{O}_{k_i})^\sim) \bigcup p^{\lfloor \lambda \rfloor} \bigotimes_{i \in I} \tfrac{1}{2p} \log_p(\mathcal{O}_{k_i}^\times)$$

$$\subseteq p^{\lfloor \lambda - \mathfrak{d}_I - a_I \rfloor} \bigotimes_{i \in I} \log_p(\mathcal{O}_{k_i}^\times) \subseteq p^{\lfloor \lambda - \mathfrak{d}_I - a_I \rfloor - b_I} (\otimes_{i \in I} \mathcal{O}_{k_i})^\sim.$$

Moreover, we have

$$\mu_{k_I}^{\log}(p^{\lfloor \lambda - \mathfrak{d}_I - a_I \rfloor - b_I}(\otimes_{i \in I}\mathcal{O}_{k_i})^{\sim})$$

$$\leq \ (-\lambda + \mathfrak{d}_I + 1)\log(p) + \sum_{i \in I^*}(3 + \log(e_i)).$$

Moreover, we have

$$\mu_{k_I}^{\log}(p^{\lfloor \lambda - \mathfrak{d}_I - a_I \rfloor - b_I}(\otimes_{i \in I} \mathcal{O}_{k_i})^{\sim})$$

$$\leq \ (-\lambda + \mathfrak{d}_I + 1) \log(p) + \sum_{i \in I^*} (3 + \log(e_i)).$$

(ii) Suppose that $p > 2$ and $e_i = 1$ $({}^{\forall} i \in I)$. Then

$$\phi((\otimes_{i \in I} \mathcal{O}_{k_i})^{\sim}) \ \subseteq \ \bigotimes_{i \in I} \tfrac{1}{2p} \log_p(\mathcal{O}_{k_i}^{\times}) \ = \ (\otimes_{i \in I} \mathcal{O}_{k_i})^{\sim}.$$

Moreover, we have

$$\mu_{k_I}^{\log}((\otimes_{i \in I} \mathcal{O}_{k_i})^{\sim}) \ = \ 0.$$

In the following discussion, for simplicity, write

$$(\overline{F}/F,\ E,\ l,\ \dots) \stackrel{\mathrm{def}}{=} (\overline{\mathbb{Q}}/F_\lambda,\ E_\lambda,\ l_\lambda,\ \dots).$$

In the following discussion, for simplicity, write

$$(\overline{F}/F,\ E,\ l,\ \dots) \stackrel{\text{def}}{=} (\overline{\mathbb{Q}}/F_\lambda,\ E_\lambda,\ l_\lambda,\ \dots).$$

($\Rightarrow\ K = F(E[l]) \supseteq F \supseteq F_{\text{mod}}$: the field of moduli of E)

$d_{\text{mod}} \stackrel{\text{def}}{=} [F_{\text{mod}} : \mathbb{Q}] \geq e_{\text{mod}} \stackrel{\text{def}}{=}$ the max. ram. index of $F_{\text{mod}}/\mathbb{Q}$

$d^*_{\text{mod}} \stackrel{\text{def}}{=} 2^{12} \cdot 3^3 \cdot 5 \cdot d_{\text{mod}} \geq e^*_{\text{mod}} \stackrel{\text{def}}{=} 2^{12} \cdot 3^3 \cdot 5 \cdot e_{\text{mod}}$

$\mathbb{V}_{\mathbb{Q}}^{\text{non}} \stackrel{\text{def}}{=} \mathbb{V}(\mathbb{Q})^{\text{non}} \supseteq \mathbb{V}_{\mathbb{Q}}^{\text{dst}} \stackrel{\text{def}}{=} \{v_{\mathbb{Q}} \in \mathbb{V}_{\mathbb{Q}}^{\text{non}} \mid v_{\mathbb{Q}}$ ramifies in $K\}$

In the following discussion, for simplicity, write

$$(\overline{F}/F,\ E,\ l,\ \dots) \stackrel{\text{def}}{=} (\overline{\mathbb{Q}}/F_\lambda,\ E_\lambda,\ l_\lambda,\ \dots).$$

($\Rightarrow\ K = F(E[l]) \supseteq F \supseteq F_{\text{mod}}$: the field of moduli of E)

$d_{\text{mod}} \stackrel{\text{def}}{=} [F_{\text{mod}} : \mathbb{Q}] \geq e_{\text{mod}} \stackrel{\text{def}}{=}$ the max. ram. index of $F_{\text{mod}}/\mathbb{Q}$

$d^*_{\text{mod}} \stackrel{\text{def}}{=} 2^{12} \cdot 3^3 \cdot 5 \cdot d_{\text{mod}} \geq e^*_{\text{mod}} \stackrel{\text{def}}{=} 2^{12} \cdot 3^3 \cdot 5 \cdot e_{\text{mod}}$

$\mathbb{V}^{\text{non}}_{\mathbb{Q}} \stackrel{\text{def}}{=} \mathbb{V}(\mathbb{Q})^{\text{non}} \supseteq \mathbb{V}^{\text{dst}}_{\mathbb{Q}} \stackrel{\text{def}}{=} \{v_{\mathbb{Q}} \in \mathbb{V}^{\text{non}}_{\mathbb{Q}} \mid v_{\mathbb{Q}}$ ramifies in $K\}$

Let us compute an upper bound for the

> *(process.-normalized, mono-an.) log-volume of the "holomorphic hull" of the union of the possible images of a Θ-pilot object, rel. to the relevant Kum. isoms, in the multira'l rep'n of [IUTchIII], Thm 3.11, (i), which we regard as sub. to (Ind1), (Ind2), (Ind3)*

(A) Let $v_{\mathbb{Q}} \in \mathbb{V}_{\mathbb{Q}}^{\mathrm{dst}}$. Fix j $(\in \{1, 2, \ldots, l^*\})$ and the collection

$$\{v_i\}_{i \in \mathbb{S}^{\pm}_{j+1}}$$

of [not necessarily distinct] elements of $\mathbb{V}(F_{\mathrm{mod}})_{v_{\mathbb{Q}}}$. Write $\underline{v}_i \in \underline{\mathbb{V}}$ $\stackrel{\sim}{\to} \mathbb{V}(F_{\mathrm{mod}})$ for the elem't corr. to v_i.

(A) Let $v_{\mathbb{Q}} \in \mathbb{V}_{\mathbb{Q}}^{\mathrm{dst}}$. Fix j $(\in \{1, 2, \dots, l^*\})$ and the collection

$$\{v_i\}_{i \in \mathbb{S}^{\pm}_{j+1}}$$

of [not necessarily distinct] elements of $\mathbb{V}(F_{\mathrm{mod}})_{v_{\mathbb{Q}}}$. Write $\underline{v}_i \in \underline{\mathbb{V}} \xrightarrow{\sim} \mathbb{V}(F_{\mathrm{mod}})$ for the elem't corr. to v_i. Then, by applying Lem, (i), we obtain an upper bound on the component of the log-volume in question corresponding to the tensor product of the $\mathbb{Q}$-spans of the log-shells associated to the collection $\{v_i\}_{i \in \mathbb{S}^{\pm}_{j+1}}$ as follows:

(A) Let $v_{\mathbb{Q}} \in \mathbb{V}_{\mathbb{Q}}^{\mathrm{dst}}$. Fix j $(\in \{1, 2, \dots, l^*\})$ and the collection

$$\{v_i\}_{i \in \mathbb{S}^{\pm}_{j+1}}$$

of [not necessarily distinct] elements of $\mathbb{V}(F_{\mathrm{mod}})_{v_{\mathbb{Q}}}$. Write $\underline{v}_i \in \underline{\mathbb{V}}$ $\xrightarrow{\sim} \mathbb{V}(F_{\mathrm{mod}})$ for the elem't corr. to v_i. Then, by applying Lem, (i), we obtain an upper bound on the component of the log-volume in question corresponding to the tensor product of the $\mathbb{Q}$-spans of the log-shells associated to the collection $\{v_i\}_{i \in \mathbb{S}^{\pm}_{j+1}}$ as follows:

$$(-\lambda + \mathfrak{d}_I + 1)\log(p_{v_{\mathbb{Q}}}) + 4(j+1)\iota_{v_{\mathbb{Q}}} \log(e^*_{\mathrm{mod}} \cdot l)$$

— where $\lambda = \begin{cases} \frac{j^2}{2l}\mathrm{ord}(q_{\underline{v}_j}) & (\underline{v}_j \in \underline{\mathbb{V}}^{\mathrm{bad}}) \\ 0 & (\underline{v}_j \in \underline{\mathbb{V}}^{\mathrm{good}}) \end{cases}$ $\iota_{v_{\mathbb{Q}}} = \begin{cases} 1 & (p_{v_{\mathbb{Q}}} \le e^*_{\mathrm{mod}} l) \\ 0 & (p_{v_{\mathbb{Q}}} > e^*_{\mathrm{mod}} l) \end{cases}$

(B) Let $v_{\mathbb{Q}} \in \mathbb{V}_{\mathbb{Q}}^{\mathrm{non}} \setminus \mathbb{V}_{\mathbb{Q}}^{\mathrm{dst}}$. Fix $j \ (\in \{1, 2, \ldots, l^{*}\})$ and $\{v_i\}_{i \in \mathbb{S}_{j+1}^{\pm}}$ as in (A).

(B) Let $v_{\mathbb{Q}} \in \mathbb{V}_{\mathbb{Q}}^{\mathrm{non}} \setminus \mathbb{V}_{\mathbb{Q}}^{\mathrm{dst}}$. Fix $j\ (\in \{1, 2, \dots, l^{*}\})$ and $\{v_i\}_{i \in \mathbb{S}_{j+1}^{\pm}}$ as in (A). Then, by applying Lem, (ii), we obtain an upper bound on the comp. of the log-vol. in question corr. to the tensor prod. of the $\mathbb{Q}$-spans of the log-shells assoc. to $\{v_i\}_{i \in \mathbb{S}_{j+1}^{\pm}}$ as follows:

(B) Let $v_{\mathbb{Q}} \in \mathbb{V}_{\mathbb{Q}}^{\mathrm{non}} \setminus \mathbb{V}_{\mathbb{Q}}^{\mathrm{dst}}$. Fix $j \; (\in \{1, 2, \dots, l^{*}\})$ and $\{v_i\}_{i \in \mathbb{S}_{j+1}^{\pm}}$ as in (A). Then, by applying Lem, (ii), we obtain an upper bound on the comp. of the log-vol. in question corr. to the tensor prod. of the $\mathbb{Q}$-spans of the log-shells assoc. to $\{v_i\}_{i \in \mathbb{S}_{j+1}^{\pm}}$ as follows:

$$0$$

(B) Let $v_{\mathbb{Q}} \in \mathbb{V}_{\mathbb{Q}}^{\mathrm{non}} \setminus \mathbb{V}_{\mathbb{Q}}^{\mathrm{dst}}$. Fix $j\ (\in \{1, 2, \dots, l^{*}\})$ and $\{v_i\}_{i \in \mathbb{S}_{j+1}^{\pm}}$ as in (A). Then, by applying Lem, (ii), we obtain an upper bound on the comp. of the log-vol. in question corr. to the tensor prod. of the $\mathbb{Q}$-spans of the log-shells assoc. to $\{v_i\}_{i \in \mathbb{S}_{j+1}^{\pm}}$ as follows:

$$0$$

(C) Let $v_{\mathbb{Q}} \in \mathbb{V}_{\mathbb{Q}}^{\mathrm{arc}}$. Fix $j\ (\in \{1, 2, \dots, l^{*}\})$ and $\{v_i\}_{i \in \mathbb{S}_{j+1}^{\pm}}$ as in (A). Then we obtain an upper bound on the comp. of the log-vol. in question corr. to the tensor prod. of the $\mathbb{Q}$-spans of the log-shells assoc. to $\{v_i\}_{i \in \mathbb{S}_{j+1}^{\pm}}$ as follows:

$$(j+1) \cdot \log(\pi)$$

After computing a "weighted average upper bound", i.e.,

$$\left(\frac{1}{[F_{\mathrm{mod}}:\mathbb{Q}]}\right)^{j+1} \sum_{v_0,\dots,v_j \in \mathbb{V}(F_{\mathrm{mod}})_{v_{\mathbb{Q}}}} \prod_{0 \le i \le j} [(F_{\mathrm{mod}})_{v_i} : \mathbb{Q}_{v_{\mathbb{Q}}}](-)$$

and then a "procession-normalized upper bound", i.e.,

$$\frac{1}{l^*} \sum_{1 \le j \le l^*} (-)$$

for each $v_{\mathbb{Q}} \in \mathbb{V}_{\mathbb{Q}}$, by summing over $v_{\mathbb{Q}} \in \mathbb{V}_{\mathbb{Q}}$ these estimates, we obtain an upper bound on $-|\log(\underline{\underline{\Theta}})|$ as follows:

After computing a "weighted average upper bound", i.e.,

$$(\frac{1}{[F_{\mathrm{mod}}:\mathbb{Q}]})^{j+1} \sum_{v_0,\dots,v_j \in \mathbb{V}(F_{\mathrm{mod}})_{v_\mathbb{Q}}} \prod_{0\le i\le j} [(F_{\mathrm{mod}})_{v_i} : \mathbb{Q}_{v_\mathbb{Q}}](-)$$

and then a "procession-normalized upper bound", i.e.,

$$\frac{1}{l^*} \sum_{1\le j\le l^*} (-)$$

for each $v_\mathbb{Q} \in \mathbb{V}_\mathbb{Q}$, by summing over $v_\mathbb{Q} \in \mathbb{V}_\mathbb{Q}$ these estimates, we obtain an upper bound on $-|\log(\underline{\underline{\Theta}})|$ as follows:

$$\frac{l+1}{4}\Big\{(1+\frac{12 d_{\mathrm{mod}}}{l})\cdot(\deg(\mathfrak{d}_\lambda)+\deg(\mathfrak{f}_\lambda)) + 10\cdot e^*_{\mathrm{mod}}\cdot l$$

$$-\frac{1}{6}\cdot(1-\frac{12}{l^2})\cdot\log(\mathfrak{q}^{\mathrm{bad}}_\lambda)\Big\} - \frac{1}{2l}\cdot\deg(\mathfrak{q}^{\mathrm{bad}}_\lambda)$$

On the other hand, since $-|\log(\underline{\underline{\Theta}})| \geq -|\log(\underline{\underline{q}})| = -\frac{1}{2l} \cdot \deg(\mathfrak{q}_{\lambda}^{\mathrm{bad}})$, we conclude that

On the other hand, since $-|\log(\underline{\underline{\Theta}})| \geq -|\log(\underline{\underline{q}})| = -\frac{1}{2l} \cdot \deg(\mathfrak{q}_\lambda^{\mathrm{bad}})$, we conclude that

$$\frac{1}{6} \cdot (1 - \frac{12}{l^2}) \cdot \deg(\mathfrak{q}_\lambda^{\mathrm{bad}}) \leq$$
$$(1 + \frac{12 d_{\mathrm{mod}}}{l}) \cdot (\deg(\mathfrak{d}_\lambda) + \deg(\mathfrak{f}_\lambda)) + 10 \cdot e^*_{\mathrm{mod}} \cdot l,$$

On the other hand, since $-|\log(\underline{\underline{\Theta}})| \geq -|\log(\underline{\underline{q}})| = -\frac{1}{2l} \cdot \deg(\mathfrak{q}_\lambda^{\mathrm{bad}})$, we conclude that

$$\frac{1}{6} \cdot (1 - \frac{12}{l^2}) \cdot \deg(\mathfrak{q}_\lambda^{\mathrm{bad}}) \;\leq\; (1 + \frac{12 d_{\mathrm{mod}}}{l}) \cdot (\deg(\mathfrak{d}_\lambda) + \deg(\mathfrak{f}_\lambda)) + 10 \cdot e^*_{\mathrm{mod}} \cdot l,$$

hence that

$$\frac{1}{6} \cdot \deg(\mathfrak{q}_\lambda^{\mathrm{bad}}) \;\leq\; (1 + \frac{20 d_{\mathrm{mod}}}{l}) \cdot (\deg(\mathfrak{d}_\lambda) + \deg(\mathfrak{f}_\lambda)) + 20 \cdot d^*_{\mathrm{mod}} \cdot l.$$

Goal of this joint work:

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.

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

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 functions properly at the place 2

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 functions properly 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

Étale 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

$X^{\log} \stackrel{\text{def}}{=} (X, \{o\} \subseteq X)$: 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

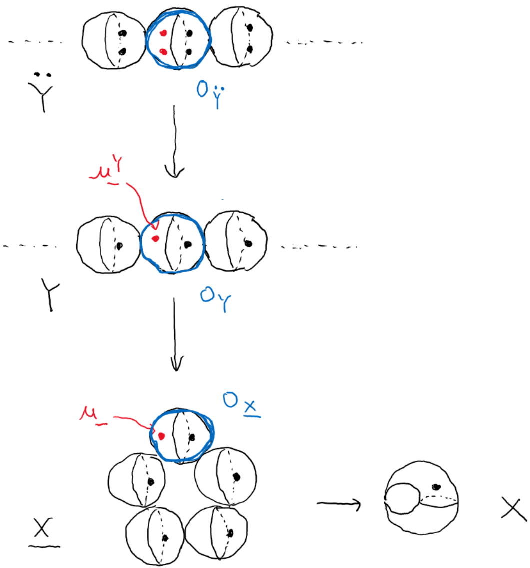
$$\underline{\mathbb{Z}} \stackrel{\text{def}}{=} \text{Gal}(Y^{\log}/X^{\log}) \quad (\cong \mathbb{Z}).$$

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

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

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

Special fibers



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 $\ddot{Y}^{\log}$.

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.

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"

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

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

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

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

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

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

Assume: $p \neq 2$

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

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

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 $j \in \underline{\mathbb{Z}}$

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

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

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 $\ddot{\Theta}$.

• 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 $j \in \underline{\mathbb{Z}}$.

• 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 $p = 2$.

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 $\underline{X}(k)$.

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

$$6\text{-torsion points of } \underline{X}(k).$$

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

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

L: 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 $\Leftrightarrow$ $n \in \{2, 4, 6\}$

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

$$6\text{-torsion points of } \underline{X}(k).$$

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

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

L: 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: $\ddot{\Theta}(-\ddot{u}) = -\ddot{\Theta}(\ddot{u})$; $\ddot{\Theta}(\ddot{u}^{-1}) = -\ddot{\Theta}(\ddot{u})$; $\ddot{\Theta}(\zeta_{12})$ is unit at $^{\forall}$bad places.

Heights

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

Heights

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

Definition

Let F be a number field; $\alpha \in F$. Then for $\Box \in \{\mathrm{non}, \mathrm{arc}\}$, we shall write

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

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

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

Heights

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

Definition

Let F be a number field; $\alpha \in F$. Then for $\Box \in \{\mathrm{non}, \mathrm{arc}\}$, we shall write

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

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

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.

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.

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.

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

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

Remark

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

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)

Remark

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

Definition

A number field F is mono-complex $\stackrel{\mathrm{def}}{\Leftrightarrow} \sharp\mathbb{V}(F)^{\mathrm{arc}} = 1$
($\Leftrightarrow F$ 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 $h^{\mathrm{tor}}_{\mathrm{arc}}(\alpha) \leq h^{\mathrm{tor}}_{\mathrm{non}}(\alpha)$.

Remark

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

Definition

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

Proposition (Important property of $h^{\text{tor}}_{\Box}$)

F: a mono-complex number field

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

Proof: This follows immediately from the product formula.

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

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

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

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

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

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

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 $h_{\text{arc}}^{\mathfrak{S}\text{-tor}}(E) \leq h_{\text{non}}^{\mathfrak{S}\text{-tor}}(E)$.

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.

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 "$\deg(\mathfrak{q}_\lambda) = h_{\mathrm{non}}(j(E_\lambda))$".

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 $h_{\square}(j(E))$)

We have

$$0 \leq h_{\mathrm{non}}^{\mathfrak{S}\text{-tor}}(E) - h_{\mathrm{non}}(j(E)) \leq 8\log 2,$$
$$-11\log 2 \leq h_{\mathrm{arc}}^{\mathfrak{S}\text{-tor}}(E) - h_{\mathrm{arc}}(j(E)) \leq 2\log 2.$$

Auxiliary numerical results

Theorem (j-invariants of "arithmetic" elliptic curves — due to Sijsling)

j("arithmetic" elliptic curve over a field of char. zero) $\in$

$$\{\tfrac{488095744}{125},\ \tfrac{1556068}{81},\ 1728,\ 0\}.$$

Auxiliary numerical results

Theorem (j-invariants of "arithmetic" elliptic curves — due to Sijsling)

j("arithmetic" elliptic curve over a field of char. zero) $\in$

$$\{\tfrac{488095744}{125},\ \tfrac{1556068}{81},\ 1728,\ 0\}.$$

Theorem (Effective ver. of PNT — due to Axler, Rosser-Schoenfeld)

For $x \in \mathbb{R}_{\geq 2}$, write

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

Then for any real number $x \geq 5 \cdot 10^{20}$ (resp. $\geq 10^{15}$), it holds that

$$\pi(x) \leq 1.022 \cdot \tfrac{x}{\log(x)} \quad \text{(resp. } |\theta(x) - x| \leq 0.00071 \cdot x).$$

Main Results

Theorem (Effective ABC for mono-complex number fields)

Let $d \in \{1, 2\}$, $\epsilon \in \mathbb{R}_{>0} \cap \mathbb{R}_{\leq 1}$. Write

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

Then 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

$$H_F(a, b, c) \ < \ 2^{5d/2} \cdot \exp(\tfrac{d}{4} \cdot h_d(\epsilon)) \cdot (\Delta_F \cdot \mathrm{rad}_F(a, b, c))^{\frac{3}{2}+\epsilon}.$$

Theorem (Effective version of a conjecture of Szpiro)

Let $\epsilon \in \mathbb{R}_{>0} \cap \mathbb{R}_{\leq 1}$; a, b, c be nonzero coprime integers such that

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

Then we have

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

Theorem (Effective version of a conjecture of Szpiro)

Let $\epsilon \in \mathbb{R}_{>0} \cap \mathbb{R}_{\leq 1}$; a, b, c be nonzero coprime integers such that

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

Then we have

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

Corollary (Application to Fermat's Last Theorem)

Let $p > 3.35 \cdot 10^9$ be a prime number. Then there does not exist any triple (x, y, z) of positive integers such that

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

holds (cf. [Coppersmith], [Mihăilescu]).