French–Korean Number Theory Webinar

18th October 2021

Richard GRIFFON
Université Clermont-Auvergne

Isogenies of elliptic curves over function fields

(joint with Fabien Pazuki)

Introduction

Variation of modular height over NF

Let E_1, E_2 be two isogenous elliptic curves over a number field F, and $\varphi : E_1 \to E_2$ be an isogeny between them.

Theorem A (Pazuki - '19)

$$|ht(j(E_1)) - ht(j(E_2))| \leq 10 + 12 \log \deg \varphi,$$

where $ht : \overline{\mathbb{Q}} \to \mathbb{R}_{\geq 0}$ is the Weil height.

Remarks

- One ingredient:

Theorem (Faltings - '80's)

$$|h_F(E_1/F) - h_F(E_2/F)| \leq \frac{1}{2} \log \deg \varphi,$$

where $h_F(.)$ is the Faltings' height.

- Theorem A is almost optimal (Szpiro–Ullmo).
- Application (Habbegger). Given $E/\overline{\mathbb{Q}}$ with no CM, and $B > 0$, $\{j(E') \in \overline{\mathbb{Q}} : E' \text{ is isogenous to } E \text{ and } ht(j(E')) \leq B\}$ is finite.

Isogeny estimate for elliptic curves over NF

Let E_1, E_2 be two isogenous elliptic curves over a number field F.

Theorem B (“Isogeny estimate”)

There exists an isogeny $\varphi_0 : E_1 \to E_2$ with

$$\deg \varphi_0 \leq c_0(F) \max\{1, ht(j(E_1)), ht(j(E_2))\}^2,$$

where $c_0(F)$ is a constant depending at most on (the degree of) F.

- Several successive improvements:
  Masser–Wüstholz (90’s), Pellarin (’01), Gaudron–Rémond (’14).
- Conjecture: uniform isogeny estimate?
  (Similar to Uniform torsion bound, Merel - ’94)
- Theorem B has numerous applications in Diophantine geometry.

Goal

There are versions of Theorem A and Theorem B for isogenous Drinfeld modules (Breuer–Pazuki–Razafinjatovo, and David–Denis).
It is natural to wonder:

Question

Can one formulate analogues of Theorems A and B in the context of elliptic curves over function fields?

Yes to both, as I'll explain.

Elliptic curves over function fields

Function field setting

Setting

Let $\mathbb{F}$ be a perfect field,
and $C/\mathbb{F}$ a smooth projective geometrically irreducible curve.
Write $K = \mathbb{F}(C)$ **for the function field of** C. We let $p = \mathrm{char}(\mathbb{F}) \geq 0$.

Arithmetic of K (and finite extensions of K) is analogous to that of a number field.

☐ **Height on $\overline{K}$:** There is a "Weil height" on $\overline{K}$,

$$ht_K : \overline{K} \to \mathbb{Q}_{\geq 0}.$$

For any $f \in K^\times$, f may be viewed as a morphism $f : C \to \mathbb{P}^1$ and

$$ht_K(f) = \deg(f).$$

Note: For $f \in \overline{K}$, $ht_K(f) = 0$ if and only if $f \in \overline{\mathbb{F}}$ (f is constant).

Elliptic curves over a function field

Let K'/K be a finite extension. One can write $K' = \mathbb{F}'(C')$.
Let E be an elliptic curve over K'.
E has a j-invariant $j(E) \in K'$, computed by the usual formulas.

☐ **Isotriviality:** We say that E is **non-isotrivial** if $j(E) \in \overline{K} \setminus \overline{\mathbb{F}}$.

We focus only on non-isotrivial elliptic curves.
(Isotrivial elliptic curves are better studied as elliptic curves over $\overline{\mathbb{F}}$).

Arithmetic of non-isotrivial elliptic curves over K' is analogous to that of elliptic curves over a number field.

Note: a non-isotrivial elliptic curve E "has no CM", that is: $\mathrm{End}(E) \simeq \mathbb{Z}$.

☐ **Inseparability degree:** For a non-isotrivial elliptic curve E over K', we let

$$\delta_i(E) := \deg_{\mathrm{ins}}(j(E)) = [K' : \mathbb{F}'(j(E))]_{\mathrm{insep}}.$$

($\delta_i(E) = 1$ if K has characteristic 0).

Height(s) of elliptic curves

Let K'/K be a finite extension, write $K' = \mathbb{F}'(C')$ as before.
Let E be an elliptic curve over K'.

□ **Modular height:** Define the modular height of E to be

$$\mathrm{h}_{\mathrm{mod}}(E) := ht_K(j(E)) \in \mathbb{Q}_{\geq 0}.$$

Note: $\mathrm{h}_{\mathrm{mod}}(E) = 0$ iff E is isotrivial.

□ **Differential height:** Let $\Delta(E/K') \in \mathrm{Div}(C')$ be the minimal discriminant divisor of E. The differential height of E/K' is

$$\mathrm{h}_{\mathrm{diff}}(E/K') := \frac{\deg(\Delta(E/K'))}{12 \cdot [K' : K]} \in \mathbb{Q}_{\geq 0}.$$

Analogue of Faltings' height for elliptic curves over a NF.
Note: $\mathrm{h}_{\mathrm{diff}}(E/K') = 0$ iff E has good reduction everywhere over K'.

Isogenies of elliptic curves

Let E_1, E_2 be two non-isotrivial elliptic curves over K'.

An isogeny $\varphi : E_1 \to E_2$ is a non-constant algebraic group morphism.

- **Degrees:** Let $\varphi : E_1 \to E_2$ be an isogeny. Then

$$\deg \varphi = \deg_{\mathrm{sep}}(\varphi) \cdot \deg_{\mathrm{ins}}(\varphi).$$

Then $\deg_{\mathrm{sep}}(\varphi) = |(\ker \varphi)(\overline{K})|$, and $\deg_{\mathrm{ins}}(\varphi) = 1$ or a power of p.

- **Dual:** an isogeny $\varphi : E_1 \to E_2$ has a dual $\widehat{\varphi} : E_2 \to E_1$ which has the same degree.

- **Biseparable isogenies:** An isogeny $\varphi : E_1 \to E_2$ is **biseparable** if both φ and its dual $\widehat{\varphi}$ are separable.
  - Automatic if $\mathrm{char}(K) = 0$,
  - Equivalent to $\deg \varphi$ coprime to $p = \mathrm{char}(K)$ if $p > 0$.

Frobenius/Verschiebung isogenies

Assume that K has positive characteristic p.

Let E be an elliptic curve over $\overline{K}$. For any power q of p,
write $E^{(q)}$ for the q-th Frobenius twist of E.

We have $j(E^{(q)}) = j(E)^q$.

The ***q*-th power Frobenius** is the isogeny $\mathrm{F}_q : E \to E^{(q)}$.
Its dual is called the ***q*-th power Verschiebung** isogeny $\mathrm{V}_q : E^{(q)} \to E$.

Fact: If E is non-isotrivial, F_q is purely inseparable of degree q,
and V_q is separable of degree q.

Variation of modular height in an isogeny class

Known results

Let E_1, E_2 be two non-isotrivial elliptic curves over a finite extension K' of K. Assume there is an isogeny $\varphi : E_1 \to E_2$.

☐ **Variation of differential height**

Theorem (? - 80's)

If φ is biseparable (i.e. has degree coprime to p), then

$$\mathrm{h}_{\mathrm{diff}}(E_1/K') = \mathrm{h}_{\mathrm{diff}}(E_2/K').$$

☐ **Comparison differential/modular heights**

Lemma (G. & Pazuki - '21)

There exists a finite extension K_{ss} of K such that

$$\mathrm{h}_{\mathrm{mod}}(E_i) = 12\,\mathrm{h}_{\mathrm{diff}}(E_i/K_{ss}).$$

If $\mathrm{char}(K) = 0$, we are done (all isogenies are biseparable).

Positive characteristic: Frobenius/Verschiebung

Let E/K' be a non-isotrivial elliptic curve. For any power q of p, there are two isogenies of degree q

$$\mathrm{F}_q : E \to E^{(q)} \qquad \text{and} \qquad \mathrm{V}_q : E^{(q)} \to E.$$

which are dual to each other.

Since $j(E^{(q)}) = j(E)^q$, we have $\mathrm{h}_{\mathrm{mod}}(E^{(q)}) = q \cdot \mathrm{h}_{\mathrm{mod}}(E)$.

Observations

- ☐ F_q multiplies $\mathrm{h}_{\mathrm{mod}}(E)$ by $q = \deg \mathrm{F}_q = \deg_{\mathrm{ins}} \mathrm{F}_q$.
- ☐ V_q divides $\mathrm{h}_{\mathrm{mod}}(E^{(q)})$ by $q = \deg \mathrm{V}_q = \deg_{\mathrm{ins}} \widehat{\mathrm{F}_q}$.
- ☐ Biseparable φ's preserve $\mathrm{h}_{\mathrm{diff}}$, which is related to $\mathrm{h}_{\mathrm{mod}}$.

Decomposition lemma

To conclude, we prove

Decomposition Lemma (G. & Pazuki - '21)

An isogeny $\varphi : E_1 \to E_2$ between non-isotrivial elliptic curves decomposes as

$$E_1 \xrightarrow{\mathsf{F}_q} E_1^{(q)} \xrightarrow{\psi} E_2^{(q')} \xrightarrow{\mathsf{V}_{q'}} E_2,$$

where $q = \deg_{\mathrm{ins}}(\varphi)$, ψ is biseparable, $q' = \deg_{\mathrm{ins}}(\widehat{\varphi})$.

Then note that

$$\frac{\mathrm{h}_{\mathrm{mod}}(E_2)}{\mathrm{h}_{\mathrm{mod}}(E_1)} = \underbrace{\frac{\mathrm{h}_{\mathrm{mod}}(E_1^{(q)})}{\mathrm{h}_{\mathrm{mod}}(E_1)}}_{=q} \cdot \underbrace{\frac{\mathrm{h}_{\mathrm{mod}}(E_2^{(q')})}{\mathrm{h}_{\mathrm{mod}}(E_1^{(q)})}}_{=1} \cdot \underbrace{\frac{\mathrm{h}_{\mathrm{mod}}(E_2)}{\mathrm{h}_{\mathrm{mod}}(E_2^{(q')})}}_{=1/q'} = \frac{q}{q'}.$$

Where $q/q' = \deg_{\mathrm{ins}}(\varphi)/\deg_{\mathrm{ins}}(\widehat{\varphi})$.

Our result

Theorem A (G. & Pazuki - '21)

Let $\varphi : E_1 \to E_2$ be an isogeny between two non-isotrivial elliptic curves over $\overline{K}$. Then

$$\mathrm{h}_{\mathrm{mod}}(E_2) = \frac{\deg_{\mathrm{ins}}(\varphi)}{\deg_{\mathrm{ins}}(\widehat{\varphi})} \cdot \mathrm{h}_{\mathrm{mod}}(E_1).$$

Comments:

- If $\mathrm{char}(K) = 0$: isogenies preserve the modular height!
- Differences with Theorem A in the NF case:
  exact relation between heights (not upper bound on the difference), involves inseparability degrees (not degrees).
- **An example:** Let $K = \mathbb{F}(t)$ with characteristic $\neq 2$,

$$E_1/K : y^2 = x(x+1)(x+t) \qquad \text{and} \qquad E_2/K : y^2 = x^3 + tx + 1.$$

  Then $\mathrm{h}_{\mathrm{mod}}(E_1) = 6$ and $\mathrm{h}_{\mathrm{mod}}(E_2) = 3$.
  Hence E_1 and E_2 are not isogenous.

A surprising consequence

Recall from the first slide:

Number field case (Habegger)

Let E be a non CM elliptic curve over $\overline{\mathbb{Q}}$. Consider the set

$$\{j(E') \in \overline{\mathbb{Q}} : E' \text{ is isogenous to } E \text{ and } ht(j(E')) \leq B\}$$

For any $B \geq 0$, this set is **finite**.

With our result, one can study

Function field case

Let $E/\overline{K}$ be a non-isotrivial elliptic curve. Consider

$$J_{bs}(E,B) = \left\{ j(E') \in \overline{K} : \begin{array}{c} E' \text{ is biseparably isogenous to } E \\ \text{and } \mathrm{h}_{\mathrm{mod}}(E') \leq B \end{array} \right\}$$

For $B \geq \mathrm{h}_{\mathrm{mod}}(E)$, the set $J_{bs}(E,B)$ is **infinite**.

An isogeny estimate for elliptic curves

Isogeny estimate

Setting is the same as before: $K = \mathbb{F}(C)$ is a function field.
We let $g(K)$ denote the genus of C.

Let E_1, E_2 be non-isotrivial isogenous elliptic curves defined over K.

Question

Can one find a "small" isogeny between E_1 and E_2?
"Small" = degree controlled in terms of invariants of E_1, E_2 and K.

We prove

Theorem B (G. & Pazuki - '21)

There exists an isogeny $\varphi_0 : E_1 \to E_2$ with

$$\deg \varphi_0 \leq 49 \max\{1, g(K)\} \cdot \max\left\{\frac{\delta_i(E_1)}{\delta_i(E_2)}, \frac{\delta_i(E_2)}{\delta_i(E_1)}\right\}.$$

Here $\delta_i(E_k)$ is the inseparability degree of $j(E_k) \in K$.

Comments

Theorem B (G. & Pazuki - '21)

Let E_1, E_2 be isogenous non-isotrivial elliptic curves defined over K. There exists an isogeny $\varphi_0 : E_1 \to E_2$ with

$$\deg \varphi_0 \leq \underbrace{49 \max\{1, g(K)\}}_{c_0(K)} \cdot \max\left\{ \frac{\delta_i(E_1)}{\delta_i(E_2)}, \frac{\delta_i(E_2)}{\delta_i(E_1)} \right\}.$$

- If $\mathrm{char}(K) = 0$, this is a **uniform isogeny estimate**.
- If $\mathrm{char}(K) > 0$, one cannot hope for a uniform statement. (In that setting, the dependence on E_1, E_2 is optimal).
- The value of the constant can sometimes be improved. For $g(K) = 0$, one can replace $c_0(K)$ by 25.
- Proof is different from the NF case.

Sketch of proof: reduction step

Let E_1, E_2 be isogenous non-isotrivial elliptic curves defined over K.

Goal: show that there is a "small" isogeny $\varphi_0 : E_1 \to E_2$.

☐ **Step 1: Reduction to a "biseparable situation"**

Lemma (G. & Pazuki - '21)

There are suitable Frobenius twists E_1' of E_1 and E_2' of E_2 such that E_1' **is biseparably isogenous to** E_2'.

Actually, $E_1' = E_1^{(q)}$ and $E_2' = E_2^{(q')}$ with

$$q, q' \leq \max\left\{\frac{\delta_i(E_1)}{\delta_i(E_2)}, \frac{\delta_i(E_2)}{\delta_i(E_1)}\right\}.$$

New goal: show that there is a "small" biseparable isogeny $E_1' \to E_2'$.
(Then "untwist" E_1' and E_2' to get an isogeny $E_1 \to E_2$)

Sketch of proof: minimisation

□ Step 2: Minimise degree of a biseparable isogeny

Among all biseparable isogenies $E'_1 \to E'_2$,
let $\varphi' : E'_1 \to E'_2$ be of minimal degree.

Since E'_1 has no CM, one shows that

- φ' has cyclic kernel $H' = (\ker \varphi')(\overline{K}) \subset E'_1(\overline{K})$,
- $|H'| = \deg \varphi'$ is coprime to p,
- and H' is $\mathrm{Gal}(\overline{K}/K)$-stable.

And $E'_2 \simeq E'_1/H'$.

We have a pair (E'_1, H') where

- E'_1 is a non-isotrivial elliptic curve over K,
- H' is a cyclic $\mathrm{Gal}(\overline{K}/K)$-stable subgroup of E'_1, $|H'|$ coprime to p.

Sketch of proof: the crucial step

☐ Step 3: Bound the degree of a cyclic biseparable isogeny

We have a pair (E_1', H') where

- E_1' is a non-isotrivial elliptic curve over K,
- H' is a cyclic $\mathrm{Gal}(\overline{K}/K)$-stable subgroup of E_1', $|H'|$ coprime to p.

Letting $N = |H'|$, such pairs are parametrised (up to $\overline{K}$-isomorphism) by non-cuspidal K-rational points on the modular curve $X_0(N)$.

From the data (E_1', H'), we thus get a K-rational point on $X_0(N)$.

Since $K = \mathbb{F}(C)$, we deduce a morphism $s : C \to X_0(N)_{/\mathbb{F}}$.
Fits in the commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{s} & X_0(N)_{/\mathbb{F}} \\ {\scriptstyle j(E_1')}\downarrow & & \downarrow \\ \mathbb{P}^1_{/\mathbb{F}} & \xrightarrow{\simeq} & X_0(1)_{/\mathbb{F}} \end{array}$$

In particular, $s : C \to X_0(N)_{/\mathbb{F}}$ is not constant.

Sketch of proof: the crucial step (II)

☐ Step 3: Bound the degree of a cyclic biseparable isogeny

We have a pair (E'_1, H') where

- E'_1 is a non-isotrivial elliptic curve over K,
- H' is a cyclic $\mathrm{Gal}(\overline{K}/K)$-stable subgroup of E'_1, $|H'|$ coprime to p.

Writing $N = |H'|$, we obtained a non-constant morphism

$$s : C \to X_0(N)_{/\mathbb{F}}.$$

By Riemann–Hurwitz, we thus have $g(X_0(N)_{/\mathbb{F}}) \leq g(C) = g(K)$.

But $g(X_0(N)_{/\mathbb{F}}) = g(X_0(N)_{/\mathbb{C}})$ grows linearly with N (Shimura).

Hence $N = |H'|$ is bounded! Precisely,

Proposition

Let E'_1 be a non-isotrivial elliptic curve over K. If E'_1 admits a subgroup H' as above. Then $|H'| \leq 49 \max\{1, g(K)\}$.

Sketch of proof: conclusion

☐ **Step 4: Conclusion**

Starting from isogenous elliptic curves E_1, E_2 over K, **Step 1** yields Frobenius twists E_1', E_2' which are biseparably isogenous.

By **Steps 2&3**, there exists a biseparable isogeny $\varphi' : E_1' \to E_2'$ with

$$\deg \varphi' \leq 49 \max\{1, g(K)\} = c_0(K).$$

Now compose φ' with the suitable $V_q : E_1' \to E_1$ or $V_{q'} : E_2' \to E_2$ to get an isogeny $\varphi_0 : E_1 \to E_2$.
Recall from Step 1 that $q, q' \leq \max\left\{\frac{\delta_i(E_1)}{\delta_i(E_2)}, \frac{\delta_i(E_2)}{\delta_i(E_1)}\right\}$.

Finally, there exists an isogeny $\varphi_0 : E_1 \to E_2$ with

$$\begin{aligned} \deg \varphi_0 &\leq \deg \varphi' \cdot \max\{q, q'\} \\ &\leq 49 \max\{1, g(K)\} \cdot \max\left\{\frac{\delta_i(E_1)}{\delta_i(E_2)}, \frac{\delta_i(E_2)}{\delta_i(E_1)}\right\}. \end{aligned}$$

☐

A corollary

We go back to the situation studied before:

Let $E/\overline{K}$ be a non-isotrivial elliptic curve. Consider

$$J_{bs}(E,B) = \left\{ j(E') \in \overline{K} : \begin{array}{c} E' \text{ is biseparably isogenous to } E \\ \text{and } \mathrm{h}_{\mathrm{mod}}(E') \leq B \end{array} \right\}$$

For $B \geq \mathrm{h}_{\mathrm{mod}}(E)$, the set $J_{bs}(E,B)$ is **infinite**.

With the help of Theorem B, we can prove

Proposition (G. & Pazuki '21)

Let $E/\overline{K}$ be a non-isotrivial elliptic curve. For any $B \geq 0$ and $D \geq 1$, let

$$J_{bs}(E,B,D) = \left\{ j(E') \in \overline{K} : \begin{array}{c} E' \text{ is biseparably isogenous to } E \\ \text{with } \mathrm{h}_{\mathrm{mod}}(E') \leq B \text{ and } [K(j(E')) : K] \leq D \end{array} \right\}.$$

This set is **finite**. Moreover $|J_{bs}(E,B,D)| \leq D^2\ \mathrm{h}_{\mathrm{mod}}(E)^2$.

Thank you
for your attention!