Effective Open Image Theorem for Pairs of Elliptic Curves

Zhining Wei

Brown University
zhining_wei@brown.edu

Joint work with Tian Wang

36th Automorphic Forms Workshop
May 2024

Let E be a non-CM elliptic curve over $\mathbb{Q}$. Fix ℓ to be a prime number and $n \geq 1$. Denote by $E[\ell^n]$ the ℓ^n-torsion group of $E\left(\overline{\mathbb{Q}}\right)$. Then the ℓ-adic Tate module, denoted by $T_\ell(E)$, is defined to be

$$T_\ell(E) = \varprojlim_n E[\ell^n].$$

A standard result will show:

$$E[\ell] \simeq_{\mathbb{F}_\ell} \mathbb{F}_\ell \oplus \mathbb{F}_\ell \qquad\qquad T_\ell(E) \simeq_{\mathbb{Z}_\ell} \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell.$$

Galois representations

For $\sigma \in G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we can define actions on $E[\ell]$ and $T_\ell(E)$ by acting on the coordinates of each element.

This gives rises to the mod ℓ Galois representation

$$\overline{\rho_{E,\ell}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

and ℓ-adic Galois representation

$$\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell).$$

The second representation gives the adelic representation:

$$\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathbb{Z}}) = \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Galois representations

For $\sigma \in G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we can define actions on $E[\ell]$ and $T_\ell(E)$ by acting on the coordinates of each element.
This gives rises to the mod ℓ Galois representation

$$\overline{\rho_{E,\ell}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

and ℓ-adic Galois representation

$$\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell).$$

The second representation gives the adelic representation:

$$\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathbb{Z}}) = \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Galois representations

For $\sigma \in G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we can define actions on $E[\ell]$ and $T_\ell(E)$ by acting on the coordinates of each element.
This gives rises to the mod ℓ Galois representation

$$\overline{\rho_{E,\ell}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

and ℓ-adic Galois representation

$$\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell).$$

The second representation gives the adelic representation:

$$\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathbb{Z}}) = \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Serre's open image theorem

In 1972, Serre proved the following open image theorem:

Theorem (Serre)

Assume that E is non-CM. Then ρ_E is open, i.e., $\rho_E(G_{\mathbb{Q}})$ is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

- A key ingredient in proving Serre's open image theorem is, for sufficiently large ℓ, $\overline{\rho_{E,\ell}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is surjective. Currently, this is also known as Serre's open image theorem.
- A natural question is, what is the smallest number $c(E)$, such that for any $\ell > c(E)$, $\overline{\rho_{E,\ell}}$ is surjective?

Serre's open image theorem

In 1972, Serre proved the following open image theorem:

Theorem (Serre)

Assume that E is non-CM. Then ρ_E is open, i.e., $\rho_E(G_{\mathbb{Q}})$ is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

- A key ingredient in proving Serre's open image theorem is, for sufficiently large ℓ, $\overline{\rho_{E,\ell}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is surjective. Currently, this is also known as Serre's open image theorem.
- A natural question is, what is the smallest number $c(E)$, such that for any $\ell > c(E)$, $\overline{\rho_{E,\ell}}$ is surjective?

Serre's open image theorem

In 1972, Serre proved the following open image theorem:

Theorem (Serre)

Assume that E is non-CM. Then ρ_E is open, i.e., $\rho_E(G_{\mathbb{Q}})$ is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

- A key ingredient in proving Serre's open image theorem is, for sufficiently large ℓ, $\overline{\rho_{E,\ell}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is surjective. Currently, this is also known as Serre's open image theorem.
- A natural question is, what is the smallest number $c(E)$, such that for any $\ell > c(E)$, $\overline{\rho_{E,\ell}}$ is surjective?

Serre's uniformality conjecture

Serre porposed the following conjecture:

Conjecture (Serre)

For a no-CM elliptic curve E, one has

$$c(E) \leq 37.$$

Currently we cannot prove a uniform bound (except for some special families). The known results are related to the invariants of elliptic curves: e.g., the Faltings height $h(E)$, the naive height $H(E)$ or the conductor N_E.

Serre's uniformality conjecture

Serre porposed the following conjecture:

Conjecture (Serre)

For a no-CM elliptic curve E, one has

$$c(E) \leq 37.$$

Currently we cannot prove a uniform bound (except for some special families). The known results are related to the invariants of elliptic curves: e.g., the Faltings height $h(E)$, the naive height $H(E)$ or the conductor N_E.

Known results

Here are some known results towards the conjecture:

- (Masser-Wüstholz) $c(E) \ll (h(E)))^r$;
- (Kraus, Cojocaru) $c(E)c(E) \ll \mathrm{rad}(N_E)(1 + \log\log \mathrm{rad}(N_E))^{1/2}$;
- (Wang-Wei) $c(E) \ll_\epsilon N_E^{1/2+\epsilon}$
- Assume GRH,
  - (Serre) $c(E) \ll (\log \mathrm{rad}(N_E))(\log\log \mathrm{rad}(2N_E))^3$;
  - (Larson-Vaintrob) $c(E) \ll \log(N_E)$;
  - (Mayle-Wang) $c(E) \leq 964 \log \mathrm{rad}(2N_E) + 5760$
- (Mazur) If E is semistable, then $c(E) \leq 11$.
- (Duke) A Density result: for 100% of elliptic curves, $c(E) = 1$ (when the elliptic curves are ordered by naive height).

Pairs of elliptic curves

Let E_1, E_2 be two (non-CM) elliptic curves. Then $E_1 \times E_2$ is an abelian variety. Fix ℓ to be a prime. We can construct the mod ℓ Galois representation $\overline{\rho_{E_1 \times E_2, \ell}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell) \times_{\det} \mathrm{GL}_2(\mathbb{F}_\ell)$.

We also have the open image theorem (Serre) for $E_1 \times E_2$, that is, for sufficiently large ℓ, $\overline{\rho_{E_1 \times E_2, \ell}}$ is surjective.

A natural question is, what is the smallest integer $c(E_1 \times E_2)$ such that, for any $\ell > c(E_1 \times E_2)$, $\overline{\rho_{E_1 \times E_2, \ell}}$ is surjective?

Pairs of elliptic curves

Let E_1, E_2 be two (non-CM) elliptic curves. Then $E_1 \times E_2$ is an abelian variety. Fix ℓ to be a prime. We can construct the mod ℓ Galois representation $\overline{\rho_{E_1 \times E_2, \ell}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell) \times_{\det} \mathrm{GL}_2(\mathbb{F}_\ell)$.

We also have the open image theorem (Serre) for $E_1 \times E_2$, that is, for sufficiently large ℓ, $\overline{\rho_{E_1 \times E_2, \ell}}$ is surjective.

A natural question is, what is the smallest integer $c(E_1 \times E_2)$ such that, for any $\ell > c(E_1 \times E_2)$, $\overline{\rho_{E_1 \times E_2, \ell}}$ is surjective?

Pairs of elliptic curves

Let E_1, E_2 be two (non-CM) elliptic curves. Then $E_1 \times E_2$ is an abelian variety. Fix ℓ to be a prime. We can construct the mod ℓ Galois representation $\overline{\rho_{E_1 \times E_2, \ell}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell) \times_{\det} \mathrm{GL}_2(\mathbb{F}_\ell)$.

We also have the open image theorem (Serre) for $E_1 \times E_2$, that is, for sufficiently large ℓ, $\overline{\rho_{E_1 \times E_2, \ell}}$ is surjective.

A natural question is, what is the smallest integer $c(E_1 \times E_2)$ such that, for any $\ell > c(E_1 \times E_2)$, $\overline{\rho_{E_1 \times E_2, \ell}}$ is surjective?

Known results

- (Masser-Wüstholz) $c(E_1 \times E_2) \ll \max(h(E_1), h(E_2))^{\gamma}$
- (Wang-Wei) $c(E_1 \times E_2) \ll \max(N_{E_1}, N_{E_2})^{\gamma'}$ with $\gamma' > 1$
- (Mayle-Wang) Assume GRH, $c(E_1 \times E_2) \leq a \log(N_{E_1} N_{E_2}) + b$.
- (Jones) A Density result: for 100% pairs of elliptic curves, $c(E_1 \times E_2) = 1$ (when the elliptic curves are ordered by naive height).

Known results

- (Masser-Wüstholz) $c(E_1 \times E_2) \ll \max(h(E_1), h(E_2))^{\gamma}$
- (Wang-Wei) $c(E_1 \times E_2) \ll \max(N_{E_1}, N_{E_2})^{\gamma'}$ with $\gamma' > 1$
- (Mayle-Wang) Assume GRH, $c(E_1 \times E_2) \leq a \log(N_{E_1} N_{E_2}) + b$.
- (Jones) A Density result: for 100% pairs of elliptic curves, $c(E_1 \times E_2) = 1$ (when the elliptic curves are ordered by naive height).

Our main results

Let $N \geq 1$. Denote by $\mathcal{E}^s(N)$ the set of non-CM semistable elliptic curves ($\mathbb{Q}$-isogeny class) E with the conductor $N_E \leq N$.

Theorem (Wang-Wei)

One has

$$\lim_{N\to\infty} \frac{\#\{(E_1,E_2) \in \mathcal{E}^s(N)\times\mathcal{E}^s(N) : c(E_1\times E_2) \ll \max(N_{E_1},N_{E_2})^{\epsilon}\}}{|\mathcal{E}^s(N)|^2} = 1.$$

That is, for 100% *pairs of elliptic curves (ordered by the conductor), one has* $c(E_1\times E_2) \ll \max(N_{E_1},N_{E_2})^{\epsilon}$.

Our main results

Let $N \geq 1$. Denote by $\mathcal{E}^s(N)$ the set of non-CM semistable elliptic curves ($\mathbb{Q}$-isogeny class) E with the conductor $N_E \leq N$.

Theorem (Wang-Wei)

One has

$$\lim_{N\to\infty} \frac{\#\{(E_1, E_2) \in \mathcal{E}^s(N) \times \mathcal{E}^s(N) : c(E_1 \times E_2) \ll \max(N_{E_1}, N_{E_2})^{\epsilon}\}}{|\mathcal{E}^s(N)|^2} = 1.$$

That is, for 100% *pairs of elliptic curves (ordered by the conductor), one has* $c(E_1 \times E_2) \ll \max(N_{E_1}, N_{E_2})^{\epsilon}$.

Key observation

Let E be an elliptic curve and let $(p, N_E) = 1$. Let

$$a_p(E) = \operatorname{Tr} \rho_{E,\ell}(\mathrm{Frob}_p).$$

Denote by $p(E_1, E_2)$ the smallest prime p such that $(p, N_{E_1} N_{E_2}) = 1$ and $a_p(E_1) \neq \pm a_p(E_2)$.

Lemma

Assume the notations above, then

$$c(E_1 \times E_2) \ll \max\{c(E_1).\ c(E_2),\ \ 4^{\sqrt{p(E_1, E_2)}}\}.$$

Key observation

Let E be an elliptic curve and let $(p, N_E) = 1$. Let

$$a_p(E) = \operatorname{Tr} \rho_{E,\ell}(\mathrm{Frob}_p).$$

Denote by $p(E_1, E_2)$ the smallest prime p such that $(p, N_{E_1} N_{E_2}) = 1$ and $a_p(E_1) \neq \pm a_p(E_2)$.

Lemma

Assume the notations above, then

$$c(E_1 \times E_2) \ll \max\{c(E_1).\ c(E_2),\ \ 4\sqrt{p(E_1, E_2)}\}.$$

Key observation

Let E be an elliptic curve and let $(p, N_E) = 1$. Let

$$a_p(E) = \operatorname{Tr} \rho_{E,\ell}(\mathrm{Frob}_p).$$

Denote by $p(E_1, E_2)$ the smallest prime p such that $(p, N_{E_1} N_{E_2}) = 1$ and $a_p(E_1) \neq \pm a_p(E_2)$.

Lemma

Assume the notations above, then

$$c(E_1 \times E_2) \ll \max\{c(E_1).\ c(E_2),\ 4\sqrt{p(E_1, E_2)}\}.$$

- Since we only consider semistable elliptic curves, one has $c(E) \leq 11$. Therefore, it suffices to show

$$p(E_1, E_2) \ll \max(N_{E_1}, N_{E_2})^{\epsilon}.$$

- By modularity theorem, each $\mathbb{Q}$-isogeny class elliptic curves corresponds to a holomorphic newform f_E of weight 2 and level N_E. Furthermore, $a_p(E)$ is the p-th Fourier coefficient of f_E.
- The question becomes: given a family of holomorphic newforms (of same weight), how to distinguish them (more precisely, their symmetric square) by using least Fourier coefficients?

- Since we only consider semistable elliptic curves, one has $c(E) \leq 11$. Therefore, it suffices to show

$$p(E_1, E_2) \ll \max(N_{E_1}, N_{E_2})^{\epsilon}.$$

- By modularity theorem, each $\mathbb{Q}$-isogeny class elliptic curves corresponds to a holomorphic newform f_E of weight 2 and level N_E. Furthermore, $a_p(E)$ is the p-th Fourier coefficient of f_E.
- The question becomes: given a family of holomorphic newforms (of same weight), how to distinguish them (more precisely, their symmetric square) by using least Fourier coefficients?

- Since we only consider semistable elliptic curves, one has $c(E) \leq 11$. Therefore, it suffices to show

$$p(E_1, E_2) \ll \max(N_{E_1}, N_{E_2})^{\epsilon}.$$

- By modularity theorem, each $\mathbb{Q}$-isogeny class elliptic curves corresponds to a holomorphic newform f_E of weight 2 and level N_E. Furthermore, $a_p(E)$ is the p-th Fourier coefficient of f_E.
- The question becomes: given a family of holomorphic newforms (of same weight), how to distinguish them (more precisely, their symmetric square) by using least Fourier coefficients?

Zero density theorem

- If we want to prove a strong bound for arbitray pairs, this can be hard. That is because, such questions are related to the zero free regions of L-functions.
- If we consider the families, the problem becomes much easier since we have zero density estimates, which tells us, for most L-functions in a given family, the zero free region is "large."

Zero density theorem

- If we want to prove a strong bound for arbitray pairs, this can be hard. That is because, such questions are related to the zero free regions of L-functions.
- If we consider the families, the problem becomes much easier since we have zero density estimates, which tells us, for most L-functions in a given family, the zero free region is "large."

Zero density theorem

- If we want to prove a strong bound for arbitray pairs, this can be hard. That is because, such questions are related to the zero free regions of L-functions.
- If we consider the families, the problem becomes much easier since we have zero density estimates, which tells us, for most L-functions in a given family, the zero free region is "large."

Main steps

- Establish zero density estimates for symmetric square L-function and symmetric forth L-functions for $\mathcal{E}^s(N)$.
- Fix $E_0 \in \mathcal{E}^s(N)$. Establish (uniform) zero density estimates for $L(s, \mathrm{sym}^2 f_{E_0} \times \mathrm{sym}^2 f_E)$.
- Apply the explicit formula to find the upper bound $p(E_1, E_2)$.

Main steps

- Establish zero density estimates for symmetric square L-function and symmetric forth L-functions for $\mathcal{E}^s(N)$.
- Fix $E_0 \in \mathcal{E}^s(N)$. Establish (uniform) zero density estimates for $L(s, \mathrm{sym}^2 f_{E_0} \times \mathrm{sym}^2 f_E)$.
- Apply the explicit formula to find the upper bound $p(E_1, E_2)$.

Main steps

- Establish zero density estimates for symmetric square L-function and symmetric forth L-functions for $\mathcal{E}^s(N)$.
- Fix $E_0 \in \mathcal{E}^s(N)$. Establish (uniform) zero density estimates for $L(s, \mathrm{sym}^2 f_{E_0} \times \mathrm{sym}^2 f_E)$.
- Apply the explicit formula to find the upper bound $p(E_1, E_2)$.

In our paper, we also considered the following questions:

- We replace the conductor by the minimal discriminant. In this case, we can drop the "semistable" condition. This relies on a more delicate zero density estimate result.
- We also consider to order the elliptic curves by the conductors without the "semistable" condition. This is an ongoing project.

In our paper, we also considered the following questions:

- We replace the conductor by the minimal discriminant. In this case, we can drop the "semistable" condition. This relies on a more delicate zero density estimate result.
- We also consider to order the elliptic curves by the conductors without the "semistable" condition. This is an ongoing project.

In our paper, we also considered the following questions:

- We replace the conductor by the minimal discriminant. In this case, we can drop the "semistable" condition. This relies on a more delicate zero density estimate result.
- We also consider to order the elliptic curves by the conductors without the "semistable" condition. This is an ongoing project.

Thanks!

References I