

Explicit Serre's open image theorem for elliptic curves over $\mathbb{Q}$

Lorenzo Furio

4 July 2025

Open Image Theorem

Definition

Let K be a number field and E/K an elliptic curve. Set $\mathbf{G}_K := \text{Gal}(\bar{K}/K)$ the absolute Galois group and $T_p := \varprojlim E[p^n]$ the p -adic Tate module of E . We define the Galois representations

$$\rho_{E,p^\infty} : \mathbf{G}_K \rightarrow \text{Aut}(T_p) \cong \text{GL}_2(\mathbb{Z}_p)$$

and

$$\rho_E : \mathbf{G}_K \rightarrow \prod_{p \text{ prime}} \text{GL}_2(\mathbb{Z}_p) = \text{GL}_2(\hat{\mathbb{Z}}).$$

Open Image Theorem

Definition

Let K be a number field and E/K an elliptic curve. Set $\mathbf{G}_K := \text{Gal}(\overline{K}/K)$ the absolute Galois group and $T_p := \varprojlim E[p^n]$ the p -adic Tate module of E . We define the Galois representations

$$\rho_{E,p^\infty} : \mathbf{G}_K \rightarrow \text{Aut}(T_p) \cong \text{GL}_2(\mathbb{Z}_p)$$

and

$$\rho_E : \mathbf{G}_K \rightarrow \prod_{p \text{ prime}} \text{GL}_2(\mathbb{Z}_p) = \text{GL}_2(\widehat{\mathbb{Z}}).$$

Theorem (Serre, 1972)

If E/K is an elliptic curve without CM, then the image of ρ_E is open in $\text{GL}_2(\widehat{\mathbb{Z}})$ and hence is a finite-index subgroup.

Uniformity Question

Theorem (Serre, 1972)

If E/K is an elliptic curve without CM, then the image of ρ_E is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and hence is a finite-index subgroup.

Question

Does there exist an integer $N = N(K)$ such that for every elliptic curve E/K without CM the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E]$ is smaller than N ?

Uniformity Question

Theorem (Serre, 1972)

If E/K is an elliptic curve without CM, then the image of ρ_E is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ and hence is a finite-index subgroup.

Question

Does there exist an integer $N = N(K)$ such that for every elliptic curve E/K without CM the index $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \mathrm{Im} \rho_E]$ is smaller than N ?

Conjecture

The question is true when $K = \mathbb{Q}$.

Uniformity Question

Theorem (Serre, 1972)

If E/K is an elliptic curve without CM, then the image of ρ_E is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ and hence is a finite-index subgroup.

Question

Does there exist an integer $N = N(K)$ such that for every elliptic curve E/K without CM the index $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \mathrm{Im} \rho_E]$ is smaller than N ?

Conjecture

The question is true when $K = \mathbb{Q}$.

current strategy $\rightarrow$ giving a 'horizontal' bound on the primes, showing that $\rho_{E,p}$ is surjective trying to exclude that $\mathrm{Im} \rho_{E,p}$ is contained in maximal proper subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$;

Uniformity Question

Theorem (Serre, 1972)

If E/K is an elliptic curve without CM, then the image of ρ_E is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and hence is a finite-index subgroup.

Question

Does there exist an integer $N = N(K)$ such that for every elliptic curve E/K without CM the index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E]$ is smaller than N ?

Conjecture

The question is true when $K = \mathbb{Q}$.

- current strategy $\rightarrow$ giving a 'horizontal' bound on the primes, showing that $\rho_{E,p}$ is surjective trying to exclude that $\mathrm{Im} \rho_{E,p}$ is contained in maximal proper subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$;
- $\rightarrow$ giving a 'vertical' bound on the index of the image of local representations ρ_{E,p^∞} .

Theorem (Zywina, 2011)

Let E be a non-CM elliptic curve over $\mathbb{Q}$ with $j = j(E)$. Let N be the product of primes for which E has bad reduction. There are constants C, γ such that

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E] < C \max\{1, h(j)\}^\gamma.$$

Theorem (Zywina, 2011)

Let E be a non-CM elliptic curve over $\mathbb{Q}$ with $j = j(E)$. Let N be the product of primes for which E has bad reduction. There are constants C, γ such that

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E] < C \max\{1, h(j)\}^\gamma.$$

Theorem (Lombardo, 2015)

Let E be a non-CM elliptic curve over a number field K . Setting $C = \exp(1.9 \cdot 10^{10})$ and $\gamma = 12395$ we have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E] < C([K : \mathbb{Q}] \max\{1, h_{\mathcal{F}}(E), \log[K : \mathbb{Q}]\})^\gamma.$$

Theorem (F., 2024)

Let E be a non-CM elliptic curve over $\mathbb{Q}$. We have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E] < 10^{21} (h_{\mathcal{F}}(E) + 40)^{4.42}$$

and

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E] < h_{\mathcal{F}}(E)^{3+O\left(\frac{1}{\log \log h_{\mathcal{F}}(E)}\right)},$$

where the function $O\left(\frac{1}{\log \log h_{\mathcal{F}}(E)}\right)$ is explicit.

Theorem (F., 2024)

Let E be a non-CM elliptic curve over $\mathbb{Q}$. We have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E] < 10^{21} (h_{\mathcal{F}}(E) + 40)^{4.42}$$

and

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E] < h_{\mathcal{F}}(E)^{3+O\left(\frac{1}{\log \log h_{\mathcal{F}}(E)}\right)},$$

where the function $O\left(\frac{1}{\log \log h_{\mathcal{F}}(E)}\right)$ is explicit.

Main improvements:

- Classification of the possible images modulo p^n ;

Theorem (F., 2024)

Let E be a non-CM elliptic curve over $\mathbb{Q}$. We have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E] < 10^{21} (h_{\mathcal{F}}(E) + 40)^{4.42}$$

and

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E] < h_{\mathcal{F}}(E)^{3+O\left(\frac{1}{\log \log h_{\mathcal{F}}(E)}\right)},$$

where the function $O\left(\frac{1}{\log \log h_{\mathcal{F}}(E)}\right)$ is explicit.

Main improvements:

- Classification of the possible images modulo p^n ;
- Bound on the product of the prime powers p^n for which $\mathrm{Im} \rho_{E,p^n}$ lies in the normaliser of a non-split Cartan;

Theorem (F., 2024)

Let E be a non-CM elliptic curve over $\mathbb{Q}$. We have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E] < 10^{21} (h_{\mathcal{F}}(E) + 40)^{4.42}$$

and

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E] < h_{\mathcal{F}}(E)^{3+O\left(\frac{1}{\log \log h_{\mathcal{F}}(E)}\right)},$$

where the function $O\left(\frac{1}{\log \log h_{\mathcal{F}}(E)}\right)$ is explicit.

Main improvements:

- Classification of the possible images modulo p^n ;
- Bound on the product of the prime powers p^n for which $\mathrm{Im} \rho_{E,p^n}$ lies in the normaliser of a non-split Cartan;
- Bound on the entanglement phenomenon.

Maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$

$\mathrm{Im} \rho_{E,p}$ can be contained in the following maximal subgroups:

- **'exceptional' subgroups:** Serre showed they cannot occur for $p > 13$.

Maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$

$\mathrm{Im} \rho_{E,p}$ can be contained in the following maximal subgroups:

- **'exceptional' subgroups:** Serre showed they cannot occur for $p > 13$.
- **Borel subgroups:** they don't occur for $p > 37$ (Mazur, 1978).

Maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$

$\mathrm{Im} \rho_{E,p}$ can be contained in the following maximal subgroups:

- **'exceptional' subgroups:** Serre showed they cannot occur for $p > 13$.
- **Borel subgroups:** they don't occur for $p > 37$ (Mazur, 1978).
- **Normalisers of Cartan subgroups:** Cartan subgroups can be

Maximal subgroups of $GL_2(\mathbb{F}_p)$

$\text{Im } \rho_{E,p}$ can be contained in the following maximal subgroups:

- **'exceptional' subgroups:** Serre showed they cannot occur for $p > 13$.
- **Borel subgroups:** they don't occur for $p > 37$ (Mazur, 1978).
- **Normalisers of Cartan subgroups:** Cartan subgroups can be
 - **split:** This doesn't occur for $p > 13$ (Bilu–Parent, Bilu–Parent–Rebolledo, 2011–2013).

Maximal subgroups of $GL_2(\mathbb{F}_p)$

$\text{Im } \rho_{E,p}$ can be contained in the following maximal subgroups:

- **'exceptional' subgroups:** Serre showed they cannot occur for $p > 13$.
- **Borel subgroups:** they don't occur for $p > 37$ (Mazur, 1978).
- **Normalisers of Cartan subgroups:** Cartan subgroups can be
 - **split:** This doesn't occur for $p > 13$ (Bilu–Parent, Bilu–Parent–Rebolledo, 2011–2013).
 - **non-split:** we don't know.

Maximal subgroups of $GL_2(\mathbb{F}_p)$

$\text{Im } \rho_{E,p}$ can be contained in the following maximal subgroups:

- **'exceptional' subgroups:** Serre showed they cannot occur for $p > 13$.
- **Borel subgroups:** they don't occur for $p > 37$ (Mazur, 1978).
- **Normalisers of Cartan subgroups:** Cartan subgroups can be
 - **split:** This doesn't occur for $p > 13$ (Bilu–Parent, Bilu–Parent–Rebolledo, 2011–2013).
 - **non-split:** we don't know.

Definition

Given an odd prime p , $\varepsilon \in \mathbb{Z}_p$ which is not a square modulo p and a positive integer n , we call a non-split Cartan subgroup

$$C_{ns}(p^n) := \left\{ \begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z}/p^n\mathbb{Z} \text{ not both } 0 \bmod p \right\}$$

and $C_{ns}^+(p^n) = C_{ns}(p^n) \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} C_{ns}(p^n)$ its normaliser.

Theorem (Zywina, 2011)

Suppose that $p > 3$ and $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$, for every $n \geq 1$ one of the following holds:

- $\text{Im } \rho_{E,p^n} \subseteq C_{ns}^+(p^n)$;
- $\text{Im } \rho_{E,p^\infty} \supset I + p^{4n} M_2(\mathbb{Z}_p)$.

Possible images modulo p^n

Theorem (Zywina, 2011)

Suppose that $p > 3$ and $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$, for every $n \geq 1$ one of the following holds:

- $\text{Im } \rho_{E,p^n} \subseteq C_{ns}^+(p^n)$;
- $\text{Im } \rho_{E,p^\infty} \supset I + p^{4n}M_2(\mathbb{Z}_p)$.

Remark

If $\text{Im } \rho_{E,p^\infty} \supset I + p^{4n}M_2(\mathbb{Z}_p)$, the index of the image is bounded by p^{16n} .

Theorem (F.,2024)

Suppose that $p > 5$ and $\mathrm{Im} \rho_{E,p} \subseteq C_{ns}^+(p)$. Let n be the largest integer such that $\mathrm{Im} \rho_{E,p^n} \subseteq C_{ns}^+(p^n)$. One of the following holds.

- $\mathrm{Im} \rho_{E,p^\infty} \supset I + p^n M_2(\mathbb{Z}_p)$
- $n = 1$, $\mathrm{Im} \rho_{E,p^\infty} \supset I + p^2 M_2(\mathbb{Z}_p)$, and $\# \mathrm{Im} \rho_{E,p^2} = 2p^3(p^2 - 1)$

Possible images modulo p^n

Theorem (F.,2024)

Suppose that $p > 5$ and $\mathrm{Im} \rho_{E,p} \subseteq C_{ns}^+(p)$. Let n be the largest integer such that $\mathrm{Im} \rho_{E,p^n} \subseteq C_{ns}^+(p^n)$. One of the following holds.

- $\mathrm{Im} \rho_{E,p^\infty} \supset I + p^n M_2(\mathbb{Z}_p)$
- $n = 1$, $\mathrm{Im} \rho_{E,p^\infty} \supset I + p^2 M_2(\mathbb{Z}_p)$, and $\# \mathrm{Im} \rho_{E,p^2} = 2p^3(p^2 - 1)$

Remark

In this case, we have that

$$[\mathrm{GL}_2(\mathbb{Z}_p) : \mathrm{Im} \rho_{E,p^\infty}] \leq \max\{p^{2n}, p^3\} \leq p^{3n}.$$

Bound in the Cartan case

Theorem (Le Fourn, 2016)

Let $E/\mathbb{Q}$ be a non-CM elliptic curve and let Λ be a product of odd primes p such that $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$. We have that

$$\begin{aligned}\Lambda &< 2^{\omega(\Lambda)+1} \cdot 10^{3.5} (\max\{h_{\mathcal{F}}(E), 985\} + 4\omega(\Lambda) \log 2) \\ &< h_{\mathcal{F}}(E)^{1+o(1)},\end{aligned}$$

where $\omega(\Lambda)$ is the prime divisor counting function.

Bound in the Cartan case

Theorem (Le Fourn, 2016)

Let $E/\mathbb{Q}$ be a non-CM elliptic curve and let Λ be a product of odd primes p such that $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$. We have that

$$\begin{aligned}\Lambda &< 2^{\omega(\Lambda)+1} \cdot 10^{3.5} (\max\{h_{\mathcal{F}}(E), 985\} + 4\omega(\Lambda) \log 2) \\ &< h_{\mathcal{F}}(E)^{1+o(1)},\end{aligned}$$

where $\omega(\Lambda)$ is the prime divisor counting function.

Theorem (F. 2024)

Let $E/\mathbb{Q}$ be a non-CM elliptic curve and let Λ be a product of odd p^n such that $\text{Im } \rho_{E,p^n} \subseteq C_{ns}^+(p^n)$. We have

$$\Lambda < 21000 (h_{\mathcal{F}}(E) + 40)^{1.308} \quad \text{and} \quad \Lambda < h_{\mathcal{F}}(E)^{1+O\left(\frac{1}{\log \log h_{\mathcal{F}}(E)}\right)}.$$

Combining the two results

Recall that when $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$ we have that

$$[\text{GL}_2(\mathbb{Z}_p) : \text{Im } \rho_{E,p^\infty}] \leq p^{3n}.$$

Combining the two results

Recall that when $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$ we have that

$$[\text{GL}_2(\mathbb{Z}_p) : \text{Im } \rho_{E,p^\infty}] \leq p^{3n}.$$

Let $\Lambda := \prod p^n$ be the largest number such that $\text{Im } \rho_{E,p^n} \subseteq C_{ns}^+(p^n)$ for every non-surjective prime p .

Combining the two results

Recall that when $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$ we have that

$$[\text{GL}_2(\mathbb{Z}_p) : \text{Im } \rho_{E,p^\infty}] \leq p^{3n}.$$

Let $\Lambda := \prod p^n$ be the largest number such that $\text{Im } \rho_{E,p^n} \subseteq C_{ns}^+(p^n)$ for every non-surjective prime p .

Since there are only finitely many classified cases in which $\text{Im } \rho_{E,p} \not\subseteq C_{ns}^+(p)$ and $\rho_{E,p}$ is not surjective, studying the entanglement phenomenon among all primes we obtain

$$\begin{aligned} [\text{GL}_2(\widehat{\mathbb{Z}}) : \text{Im } \rho_E] &\ll \Lambda^{o(1)} \prod_{p|\Lambda} [\text{GL}_2(\mathbb{Z}_p) : \text{Im } \rho_{E,p^\infty}] \\ &\leq \Lambda^{3+o(1)} \ll h_{\mathcal{F}}(E)^{3+o(1)}. \end{aligned}$$

Recall the classification for p -adic images.

Let $p > 5$ such that $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$, and let

$\pi_n : \text{GL}_2(\mathbb{Z}_p) \rightarrow \text{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ be the canonical projection. One of the following is true:

- $\text{Im } \rho_{E,p^\infty} = \pi_n^{-1}(C_{ns}^+(p^n))$ for some n
- $\text{Im } \rho_{E,p^\infty} = \pi_2^{-1}(G)$ for an explicit $G < \text{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ such that $\#G = 2p^3(p^2 - 1)$.

Recent improvement

Recall the classification for p -adic images.

Let $p > 5$ such that $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$, and let

$\pi_n : \text{GL}_2(\mathbb{Z}_p) \rightarrow \text{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ be the canonical projection. One of the following is true:

- $\text{Im } \rho_{E,p^\infty} = \pi_n^{-1}(C_{ns}^+(p^n))$ for some n
- $\text{Im } \rho_{E,p^\infty} = \pi_2^{-1}(G)$ for an explicit $G < \text{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$ such that $\#G = 2p^3(p^2 - 1)$.

We then used the bound

$$[\text{GL}_2(\mathbb{Z}_p) : \text{Im } \rho_{E,p^\infty}] \leq \max\{p^{2n}, p^3\} \leq p^{3n},$$

which is not that sharp.

Theorem (Bisatt–F.–Lombardo, *to appear soon*)

If $p > 7$, there exists $n \geq 1$ such that

$$\mathrm{Im} \, \rho_{E,p^\infty} = \pi_n^{-1} \left(C_{ns}^+(p^n) \right).$$

Theorem (Bisatt–F.–Lombardo, *to appear soon*)

If $p > 7$, there exists $n \geq 1$ such that

$$\mathrm{Im} \rho_{E,p^\infty} = \pi_n^{-1} \left(C_{ns}^+(p^n) \right).$$

Corollary

If $E/\mathbb{Q}$ is a non-CM elliptic curve we have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E] < h_{\mathcal{F}}(E)^{2+o(1)}.$$

Recent improvement

Theorem (Bisatt–F.–Lombardo, *to appear soon*)

If $p > 7$, there exists $n \geq 1$ such that

$$\mathrm{Im} \rho_{E,p^\infty} = \pi_n^{-1} \left(C_{ns}^+(p^n) \right).$$

Corollary

If $E/\mathbb{Q}$ is a non-CM elliptic curve we have

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im} \rho_E] < h_{\mathcal{F}}(E)^{2+o(1)}.$$

Idea of the proof:

Find a local obstruction to the existence of rational points on the modular curves X_G , using classification results for p -adic representations coming from geometric objects.

Thank you for your attention