Explicit Serre's open image theorem for rational elliptic curves

Lorenzo Furio

17 April 2024

Open Image Theorem

Definition

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

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

and

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

Open Image Theorem

Definition

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

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

and

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

Theorem (Serre, 1972)

If ${}^{E}\!/\!_{K}$ is an elliptic curve without CM, then the image of ρ_E is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ 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 $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ 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 $K = \mathbb{Q}$.

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 'vertical' bound on the index of the image of local representations ρ_{E,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 'vertical' bound on the index of the image of local representations ρ_{E,p^∞};
- $\rightarrow$ 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 $\mathrm{GL}_2(\mathbb{F}_p)$.

Existent bounds

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*

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

Existent bounds

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*

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

- *There is a constant C such that*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < C(68N(1 + \log\log N)^{\frac{1}{2}})^{24\omega(N)}.$$

Existent bounds

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*

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

- *There is a constant C such that*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im} \rho_E] < C(68N(1 + \log\log N)^{\frac{1}{2}})^{24\omega(N)}.$$

- *Assuming GRH there is a constant C such that*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im} \rho_E] < (C \log N(\log\log 2N)^3)^{24\omega(N)}.$$

Existent bounds

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*
$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < C \max\{1, \mathrm{h}(j)\}^{\gamma}.$$
- *There is a constant C such that*
$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < C(68N(1+\log\log N)^{\frac{1}{2}})^{24\omega(N)}.$$
- *Assuming GRH there is a constant C such that*
$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < (C\log N(\log\log 2N)^3)^{24\omega(N)}.$$

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

Theorem (F., 2024?)

Let E be a non-CM elliptic curve over $\mathbb{Q}$. There exist explicit constants C_1, C_2 such that

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < C_1(\mathrm{h}_{\mathcal{F}}(E) + 32)^{3.531}$$

and

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \mathrm{Im}\,\rho_E] < C_2(\mathrm{h}_{\mathcal{F}}(E) + 23.5)^{3+O\left(\frac{1}{\log\log \mathrm{h}_{\mathcal{F}}(E)}\right)},$$

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

Theorem (F., 2024?)

Let E be a non-CM elliptic curve over $\mathbb{Q}$. There exist explicit constants C_1, C_2 such that

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im} \rho_E] < C_1(\mathrm{h}_{\mathcal{F}}(E) + 32)^{3.531}$$

and

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im} \rho_E] < C_2(\mathrm{h}_{\mathcal{F}}(E) + 23.5)^{3+O\left(\frac{1}{\log\log \mathrm{h}_{\mathcal{F}}(E)}\right)},$$

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

Main improvements:

- Classification of the possible images modulo p^n;

Theorem (F., 2024?)

Let E be a non-CM elliptic curve over $\mathbb{Q}$. There exist explicit constants C_1, C_2 such that

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im} \rho_E] < C_1(\mathrm{h}_{\mathcal{F}}(E) + 32)^{3.531}$$

and

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im} \rho_E] < C_2(\mathrm{h}_{\mathcal{F}}(E) + 23.5)^{3+O\left(\frac{1}{\log\log \mathrm{h}_{\mathcal{F}}(E)}\right)},$$

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

Main improvements:

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

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

Im $\rho_{E,p}$ can be contained in

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

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

Im $\rho_{E,p}$ can be contained in

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

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

Im $\rho_{E,p}$ can be contained in

- **'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 of two types

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

Im $\rho_{E,p}$ can be contained in

- **'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 of two types
  - **split**: This doesn't occur for $p > 13$ (Bilu–Parent, 2011).

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

Im $\rho_{E,p}$ can be contained in

- **'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 of two types
  - **split**: This doesn't occur for $p > 13$ (Bilu–Parent, 2011).
  - **non-split**: we don't know.

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

Im $\rho_{E,p}$ can be contained in

- **'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 of two types
  - **split**: This doesn't occur for $p > 13$ (Bilu–Parent, 2011).
  - **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.

Possible images modulo p^n

Theorem (Zywina, 2011)

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

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

Possible images modulo p^n

Theorem (Zywina, 2011)

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

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

Remark

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

Possible images modulo p^n

Theorem (Zywina, 2011)

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

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

Remark

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

Theorem

If $p > 37$ and $\rho_{E,p}$ is not surjective, then $\operatorname{Im} \rho_{E,p} = C_{ns}^+(p)$.

Remark

Combining these two results, we notice that it is sufficient to bound all the prime powers p^n such that $\operatorname{Im} \rho_{E,p^n} \subseteq C_{ns}^+(p^n)$.

Possible images modulo p^n

Theorem (F.,2024)

Suppose that $p > 5$ *and* $\operatorname{Im} \rho_{E,p} \subseteq C_{ns}^{+}(p)$.
If n *is the smallest integer such that* $\operatorname{Im} \rho_{E,p^\infty} \supset I + p^n M_2(\mathbb{Z}_p)$ *and* $n > 2$, *then*

$$\operatorname{Im} \rho_{E,p^n} = C_{ns}^{+}(p^n).$$

Possible images modulo p^n

Theorem (F.,2024)

Suppose that $p > 5$ and $\operatorname{Im} \rho_{E,p} \subseteq C_{ns}^+(p)$.
If n is the smallest integer such that $\operatorname{Im} \rho_{E,p^\infty} \supset I + p^n M_2(\mathbb{Z}_p)$ and $n > 2$, then

$$\operatorname{Im} \rho_{E,p^n} = C_{ns}^+(p^n).$$

Remark

In this case, we have that $[\mathrm{GL}_2(\mathbb{Z}_p) : \operatorname{Im} \rho_{E,p^\infty}] \leq p^{2n}$.

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 $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$. We have that

$$\Lambda < 2^{\omega(\Lambda)+1} \cdot 10^{3.5}(\max\{\mathrm{h}_{\mathcal{F}}(E), 985\} + 4\omega(\Lambda)\log 2),$$

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 $\operatorname{Im}\rho_{E,p} \subseteq C_{ns}^{+}(p)$. We have that

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

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

Theorem (F. – Lombardo, F.)

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

$$\Lambda < 2908 \cdot 2^{\omega(\Lambda)} \left(h_{\mathcal{F}}(E) + 2\log\Lambda + \frac{3}{2}\log\left(h_{\mathcal{F}}(E)+1\right) + 5 \right).$$

In particular,

$$\Lambda < 26000\,(h_{\mathcal{F}}(E)+32)^{1.177} \quad \text{and} \quad \Lambda < 2908\,h_{\mathcal{F}}(E)^{1+O\left(\frac{1}{\log\log h_{\mathcal{F}}(E)}\right)}.$$

Thank you for your attention