Recent progress on Serre's uniformity question

Lorenzo Furio

8 July 2024

Serre's uniformity question

Definition

Let K be a number field and ${}^{E}\!/_{K}$ an elliptic curve. We define the Galois representations

$$\rho_{E,N} : \mathbf{G}_K \to \mathrm{Aut}(E[N]) \cong \mathrm{GL}_2\left({}^{\mathbb{Z}}\!/_{N\mathbb{Z}}\right),$$

$$\rho_{E,p^\infty} : \mathbf{G}_K \to \mathrm{Aut}(T_pE) \cong \mathrm{GL}_2(\mathbb{Z}_p) \quad \text{and} \quad \rho_E := \prod_{p \text{ prime}} \rho_{p^\infty}.$$

Theorem (Serre, 1972)

If ${}^{E}\!/_{K}$ is a non-CM elliptic curve, there exists a constant N such that for every prime $p > N$ the representation $\rho_{E,p}$ is surjective.

Question

Is N independent of the curve?

Current progress

Let $E/\mathbb{Q}$ be an elliptic curve without CM.

Theorem (Mazur, 1978)

If $p > 37$, then $\operatorname{Im} \rho_{E,p}$ is not contained in a Borel subgroup, hence it is either $\mathrm{GL}_2(\mathbb{F}_p)$ or it is contained in the normaliser of a Cartan subgroup.

Theorem (Bilu–Parent–Rebolledo, 2013)

If $p > 37$ then $\operatorname{Im} \rho_{E,p}$ is either $\mathrm{GL}_2(\mathbb{F}_p)$ or it is contained in the normaliser of a non-split Cartan subgroup.

Theorem (Le Fourn – Lemos, 2021)

If $p > 1.4 \cdot 10^7$ then $\operatorname{Im} \rho_{E,p}$ is either $\mathrm{GL}_2(\mathbb{F}_p)$ or the full normaliser of a non-split Cartan.

Theorem (F. – Lombardo, 2023)

Le Fourn–Lemos's theorem holds for $p > 37$.

Possible images modulo p^n

Let $E/_{\mathbb{Q}}$ be an elliptic curve without CM.

Theorem (F.,2024)

Suppose that $p > 5$ and $\operatorname{Im} \rho_{E,p} \subseteq C_{ns}^{+}(p)$. Let n be the smallest integer such that $\operatorname{Im} \rho_{E,p^\infty} \supset I + p^n M_2(\mathbb{Z}_p)$. One of the following holds:

- $\operatorname{Im} \rho_{E,p^n} = C_{ns}^{+}(p^n)$ *up to conjugation;*
- $n = 2$ *and* $\operatorname{Im} \rho_{E,p^n}$ *is a particular subgroup of order* $2(p^2 - 1)p^3$.

Bound on the adelic index

Theorem (Zywina, 2011)

Let E be a non-CM elliptic curve over $\mathbb{Q}$. There are constants C, γ such that

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

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

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

One can use the classification of images modulo p^n to obtain a **very small bound** when $K = \mathbb{Q}$...

Very small bound (F., in progress)

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \operatorname{Im} \rho_E] < 10^{22}(\mathrm{h}_{\mathcal{F}}(E) + 30)^5.$$

Compared with the previous result:

$$\begin{array}{ccc} \exp(1.9 \cdot 10^{10}) & \longrightarrow & 10^{22} \\ 12395 & \longrightarrow & 5 \end{array}$$