

Serre's Uniformity Question and proper subgroups of $C_{ns}^+(p)$

Lorenzo Furio

18 September 2023

Joint work with Davide Lombardo

Open Image Theorem

Definition

Let K be a number field and E/K an elliptic curve. Setting $\mathbf{G}_K := \text{Gal}(\bar{K}/K)$, we define the Galois representation

$$\rho_{E,p} : \mathbf{G}_K \rightarrow \text{Aut}(E[p]) \cong \text{GL}_2(\mathbb{F}_p).$$

Open Image Theorem

Definition

Let K be a number field and E/K an elliptic curve. Setting $\mathbf{G}_K := \text{Gal}(\overline{K}/K)$, we define the Galois representation

$$\rho_{E,p} : \mathbf{G}_K \rightarrow \text{Aut}(E[p]) \cong \text{GL}_2(\mathbb{F}_p).$$

Theorem (Serre, 1972)

If E/\mathbb{Q} is an elliptic curve without CM, then there exists an integer N_E such that for every prime $p > N_E$ the representation $\rho_{E,p}$ is surjective.

Open Image Theorem

Definition

Let K be a number field and E/K an elliptic curve. Setting $\mathbf{G}_K := \text{Gal}(\bar{K}/K)$, we define the Galois representation

$$\rho_{E,p} : \mathbf{G}_K \rightarrow \text{Aut}(E[p]) \cong \text{GL}_2(\mathbb{F}_p).$$

Theorem (Serre, 1972)

If E/\mathbb{Q} is an elliptic curve without CM, then there exists an integer N_E such that for every prime $p > N_E$ the representation $\rho_{E,p}$ is surjective.

Question (Serre's Uniformity Question)

Does there exist an integer N such that for every prime $p > N$ and for every elliptic curve E/\mathbb{Q} without CM the representation $\rho_{E,p}$ is surjective?

Serre's Uniformity Question

Theorem (Serre, 1972)

If E/\mathbb{Q} is an elliptic curve without CM, then there exists an integer N_E such that for every prime $p > N_E$ the representation $\rho_{E,p}$ is surjective.

Question

Does there exist an integer N such that for every prime $p > N$ and for every elliptic curve E/\mathbb{Q} without CM the representation $\rho_{E,p}$ is surjective?

Conjecture

$N = 37$.

Serre's Uniformity Question

Theorem (Serre, 1972)

If E/\mathbb{Q} is an elliptic curve without CM, then there exists an integer N_E such that for every prime $p > N_E$ the representation $\rho_{E,p}$ is surjective.

Question

Does there exist an integer N such that for every prime $p > N$ and for every elliptic curve E/\mathbb{Q} without CM the representation $\rho_{E,p}$ is surjective?

Conjecture

$N = 37$.

current strategy \rightarrow trying to exclude that $\text{Im } \rho_{E,p}$ is contained in maximal proper subgroups of $\text{GL}_2(\mathbb{F}_p)$.

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

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

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

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

$\text{Im } \rho_{E,p}$ 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 $GL_2(\mathbb{F}_p)$

$\text{Im } \rho_{E,p}$ 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 $GL_2(\mathbb{F}_p)$

$\text{Im } \rho_{E,p}$ 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:** Bilu–Parent (2011) showed that this doesn't occur for $p > 13$ via their Runge method for modular curves.

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

$\text{Im } \rho_{E,p}$ 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:** Bilu–Parent (2011) showed that this doesn't occur for $p > 13$ via their Runge method for modular curves.
 - **non-split:** we don't know.

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

$\text{Im } \rho_{E,p}$ 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:** Bilu–Parent (2011) showed that this doesn't occur for $p > 13$ via their Runge method for modular curves.
 - **non-split:** we don't know.

Notation

We call $C_{ns}(p)$ a non-split Cartan subgroup in $GL_2(\mathbb{F}_p)$ and $C_{ns}^+(p)$ its normaliser.

What do we know about the non-split Cartan case?

Let $p > 37$ be a prime and let E/\mathbb{Q} be an elliptic curve without CM such that $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$.

What do we know about the non-split Cartan case?

Let $p > 37$ be a prime and let E/\mathbb{Q} be an elliptic curve without CM such that $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$.

Definition

We call $G(p)$ the subgroup of $C_{ns}^+(p)$ of index 3 such that $G(p) \cap C_{ns}(p) = C_{ns}(p)^3$ (unique up to conjugation).

What do we know about the non-split Cartan case?

Let $p > 37$ be a prime and let E/\mathbb{Q} be an elliptic curve without CM such that $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$.

Definition

We call $G(p)$ the subgroup of $C_{ns}^+(p)$ of index 3 such that $G(p) \cap C_{ns}(p) = C_{ns}(p)^3$ (unique up to conjugation).

Theorem (Zywina, 2015)

There are just two possibilities:

- $\text{Im } \rho_{E,p} = C_{ns}^+(p)$;
- $\text{Im } \rho_{E,p} = G(p)$; *in this case $p \equiv 2 \pmod{3}$.*

What do we know about the non-split Cartan case?

Let $p > 37$ be a prime and let E/\mathbb{Q} be an elliptic curve without CM such that $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$.

Definition

We call $G(p)$ the subgroup of $C_{ns}^+(p)$ of index 3 such that $G(p) \cap C_{ns}(p) = C_{ns}(p)^3$ (unique up to conjugation).

Theorem (Zywina, 2015)

There are just two possibilities:

- $\text{Im } \rho_{E,p} = C_{ns}^+(p)$;
- $\text{Im } \rho_{E,p} = G(p)$; *in this case $p \equiv 2 \pmod{3}$.*

Theorem (Le Fourn–Lemos, 2021)

If $\text{Im } \rho_{E,p} = G(p)$, then $p < 1.4 \cdot 10^7$ and $j(E) \in \mathbb{Z}$.

What do we know about the split Cartan case?

Let $p > 37$ be a prime and let E/\mathbb{Q} be an elliptic curve without CM such that $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$.

Theorem (Le Fourn–Lemos, 2021)

If $\text{Im } \rho_{E,p} = G(p)$, then $p < 1.4 \cdot 10^7$ and $j(E) \in \mathbb{Z}$.

The theorem of Le Fourn and Lemos relies on the Runge's method for modular curves developed by Bilu and Parent.

What do we know about the split Cartan case?

Let $p > 37$ be a prime and let E/\mathbb{Q} be an elliptic curve without CM such that $\text{Im } \rho_{E,p} \subseteq C_{ns}^+(p)$.

Theorem (Le Fourn–Lemos, 2021)

If $\text{Im } \rho_{E,p} = G(p)$, then $p < 1.4 \cdot 10^7$ and $j(E) \in \mathbb{Z}$.

The theorem of Le Fourn and Lemos relies on the Runge's method for modular curves developed by Bilu and Parent.

Theorem (F.–Lombardo, 2023)

In this setting, we always have $\text{Im } \rho_{E,p} = C_{ns}^+(p)$.

Strategy of Le Fourn and Lemos

The strategy of the proof of le Fourn and Lemos follows three main steps:

Strategy of Le Fourn and Lemos

The strategy of the proof of le Fourn and Lemos follows three main steps:

- They show that $j \in \mathbb{Z}$ by applying Mazur's formal immersion method to a suitable quotient of the Jacobian of $X_{G(p)}$.

Strategy of Le Fourn and Lemos

The strategy of the proof of le Fourn and Lemos follows three main steps:

- They show that $j \in \mathbb{Z}$ by applying Mazur's formal immersion method to a suitable quotient of the Jacobian of $X_{G(p)}$.
- Applying Runge's method one can estimate some integer values of certain modular units and obtain that

$$|j| < 7\sqrt{p}.$$

Strategy of Le Fourn and Lemos

The strategy of the proof of le Fourn and Lemos follows three main steps:

- They show that $j \in \mathbb{Z}$ by applying Mazur's formal immersion method to a suitable quotient of the Jacobian of $X_{G(p)}$.
- Applying Runge's method one can estimate some integer values of certain modular units and obtain that

$$|j| < 7\sqrt{p}.$$

- Adapting Gaudron and Rémond's effective results on the degrees of minimal isogenies, one can show an 'effective surjectivity' theorem, obtaining

$$p < c \cdot \log |j|,$$

for some explicit constant c .

How to improve the strategy to always exclude $G(p)$

The strategy of Le Fourn and Lemos can be improved through three main innovations:

How to improve the strategy to always exclude $G(p)$

The strategy of Le Fourn and Lemos can be improved through three main innovations:

- Considering cancellation among roots of unity in modular units one can show, following Weil's strategy to bound Kloosterman sums, that

$$\cancel{|j| < 7\sqrt{p}} \longrightarrow |j| < 9\sqrt[4]{p}.$$

How to improve the strategy to always exclude $G(p)$

The strategy of Le Fourn and Lemos can be improved through three main innovations:

- Considering cancellation among roots of unity in modular units one can show, following Weil's strategy to bound Kloosterman sums, that

$$\cancel{|j| < 7\sqrt{p}} \longrightarrow |j| < 9\sqrt[4]{p}.$$

- The effective surjectivity theorem can be slightly improved, keeping the effective constant not too large and making it work for elliptic curves with small heights.

How to improve the strategy to always exclude $G(p)$

The strategy of Le Fourn and Lemos can be improved through three main innovations:

- Considering cancellation among roots of unity in modular units one can show, following Weil's strategy to bound Kloosterman sums, that

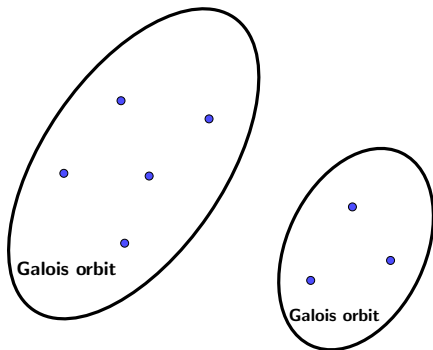
$$\cancel{|j| < 7\sqrt{p}} \longrightarrow |j| < 9\sqrt[4]{p}.$$

- The effective surjectivity theorem can be slightly improved, keeping the effective constant not too large and making it work for elliptic curves with small heights.
- A detailed study of the image of the inertia subgroups and the canonical subgroup of $E[p]$ allows one to show that the j -invariant must be of the form

$$j = c^3 \cdot p^k,$$

with $k \geq 4$. This allows us to filter the remaining cases and perform a feasible computation.

Runge's method for modular curves



The modular units defined over \mathbb{Q} of the curve $X_{G(p)}$ have zeros and poles on the cusps of the modular curve, and all the cusps in a same Galois orbit over \mathbb{Q} are of the same type (zero or pole).

The rank of the group of modular units up to constants is equal to the number of Galois orbits of cusps minus 1, hence we need at least 2 orbits for the existence of a non-trivial modular unit.

We need to find a modular unit U integral over $\mathbb{Z}[j]$, which is integer when valued in $j \in \mathbb{Z}$. This holds also for $p^3 U^{-1}$.

The combination of the estimates on modular units and the effective surjectivity theorem gives

$$p < 10^5,$$

which is slightly better than $p < 1.4 \cdot 10^7$.

The combination of the estimates on modular units and the effective surjectivity theorem gives

$$p < 10^5,$$

which is slightly better than $p < 1.4 \cdot 10^7$.

However the best improvement is achieved on the estimates on $\log |j|$, in particular we have

$$\log |j| \leq 40,$$

while the estimates by Le Fourn and Lemos give only $\log |j| \leq 27000$.

How can we further filter the j -invariants?

One can observe that j must be of the form

$$j = p^k \cdot c^3,$$

hence almost a cube. This allows us to divide by 3 on a 'logarithmic scale' the number of cases to consider.

How can we further filter the j -invariants?

One can observe that j must be of the form

$$j = p^k \cdot c^3,$$

hence almost a cube. This allows us to divide by 3 on a 'logarithmic scale' the number of cases to consider.

Moreover, one can show that j is 'large enough' by proving that $k \geq 4$. This can be achieved by studying the canonical subgroup of the corresponding elliptic curve.

The canonical subgroup

Let E/\mathbb{Q} be an elliptic curve with good reduction at p .

We know that the geometric p -torsion of the reduction modulo p of E is either $\mathbb{Z}/p\mathbb{Z}$ or 0 .

The canonical subgroup

Let E/\mathbb{Q} be an elliptic curve with good reduction at p .

We know that the geometric p -torsion of the reduction modulo p of E is either $\mathbb{Z}/p\mathbb{Z}$ or 0 . We have a sequence

$$0 \longrightarrow E_1[p] \longrightarrow E[p] \longrightarrow \tilde{E}[p] \longrightarrow 0$$

where \tilde{E} is the reduced curve modulo p and $E_1[p]$ are the p -torsion points which reduce to 0 modulo p .

The canonical subgroup

Let E/\mathbb{Q} be an elliptic curve with good reduction at p .

We know that the geometric p -torsion of the reduction modulo p of E is either $\mathbb{Z}/p\mathbb{Z}$ or 0. We have a sequence

$$0 \longrightarrow E_1[p] \longrightarrow E[p] \longrightarrow \tilde{E}[p] \longrightarrow 0$$

where \tilde{E} is the reduced curve modulo p and $E_1[p]$ are the p -torsion points which reduce to 0 modulo p .

If E has ordinary reduction, $\tilde{E}[p] \cong \mathbb{Z}/p\mathbb{Z}$ and hence $E_1[p]$ is a 'canonical' choice of a subgroup of order p of $E[p]$.

The canonical subgroup

Let E/\mathbb{Q} be an elliptic curve with good reduction at p . We know that the geometric p -torsion of the reduction modulo p of E is either $\mathbb{Z}/p\mathbb{Z}$ or 0. We have a sequence

$$0 \longrightarrow E_1[p] \longrightarrow E[p] \longrightarrow \tilde{E}[p] \longrightarrow 0$$

where \tilde{E} is the reduced curve modulo p and $E_1[p]$ are the p -torsion points which reduce to 0 modulo p .

If E has ordinary reduction, $\tilde{E}[p] \cong \mathbb{Z}/p\mathbb{Z}$ and hence $E_1[p]$ is a 'canonical' choice of a subgroup of order p of $E[p]$.

Remark

$E_1[p]$ is the subgroup of points of p -adic valuation greater than 0.

The canonical subgroup

Let K be a p -adic field ($p \neq 2$) and let E/K be an elliptic curve with good reduction at $\mathfrak{p} \mid p$.

The canonical subgroup

Let K be a p -adic field ($p \neq 2$) and let E/K be an elliptic curve with good reduction at $\mathfrak{p} \mid p$.

Definition

If there exists $\lambda \in \mathbb{R}$ such that

$$\{P \in E[p] : v_p(P) > \lambda\}$$

is a subgroup of order p , then this is called the *canonical subgroup*.

The canonical subgroup

Let K be a p -adic field ($p \neq 2$) and let E/K be an elliptic curve with good reduction at $\mathfrak{p} \mid p$.

Definition

If there exists $\lambda \in \mathbb{R}$ such that

$$\{P \in E[p] : v_p(P) > \lambda\}$$

is a subgroup of order p , then this is called the *canonical subgroup*.

Theorem (Lubin, 1979)

Let A be the Hasse invariant of E . The group $E[p]$ admits a canonical subgroup if and only if

$$v_p(A) < \frac{p}{p+1}.$$

The canonical subgroup

Let $p > 37$ be a prime and let E/\mathbb{Q} be a non-CM elliptic curve such that $\text{Im } \rho_{E,p} = G(p)$.

The canonical subgroup

Let $p > 37$ be a prime and let E/\mathbb{Q} be a non-CM elliptic curve such that $\text{Im } \rho_{E,p} = G(p)$.

- Since $\text{Im } \rho_{E,p} \subset C_{ns}^+(p)$ we know that E has potentially good reduction at p .

The canonical subgroup

Let $p > 37$ be a prime and let E/\mathbb{Q} be a non-CM elliptic curve such that $\text{Im } \rho_{E,p} = G(p)$.

- Since $\text{Im } \rho_{E,p} \subset C_{ns}^+(p)$ we know that E has potentially good reduction at p .
- Let \mathbb{Q}_p^{nr} be the maximal unramified extension of \mathbb{Q}_p and consider the base change of E to \mathbb{Q}_p^{nr} .

The canonical subgroup

Let $p > 37$ be a prime and let E/\mathbb{Q} be a non-CM elliptic curve such that $\text{Im } \rho_{E,p} = G(p)$.

- Since $\text{Im } \rho_{E,p} \subset C_{ns}^+(p)$ we know that E has potentially good reduction at p .
- Let \mathbb{Q}_p^{nr} be the maximal unramified extension of \mathbb{Q}_p and consider the base change of E to \mathbb{Q}_p^{nr} .
- Let K/\mathbb{Q}_p^{nr} be the minimal extension over which E acquires good reduction. It can be shown that $[K : \mathbb{Q}_p^{nr}] \in \{3, 6\}$.

The canonical subgroup

Let $p > 37$ be a prime and let E/\mathbb{Q} be a non-CM elliptic curve such that $\text{Im } \rho_{E,p} = G(p)$.

- Since $\text{Im } \rho_{E,p} \subset C_{ns}^+(p)$ we know that E has potentially good reduction at p .
- Let \mathbb{Q}_p^{nr} be the maximal unramified extension of \mathbb{Q}_p and consider the base change of E to \mathbb{Q}_p^{nr} .
- Let K/\mathbb{Q}_p^{nr} be the minimal extension over which E acquires good reduction. It can be shown that $[K : \mathbb{Q}_p^{nr}] \in \{3, 6\}$.
- If E admitted a canonical subgroup, there would be a subgroup of order p stable for the Galois action, hence the image of $\text{Gal}(\overline{\mathbb{Q}_p}/K)$ would be contained in a Borel subgroup.

The canonical subgroup

Let $p > 37$ be a prime and let E/\mathbb{Q} be a non-CM elliptic curve such that $\text{Im } \rho_{E,p} = G(p)$.

- Since $\text{Im } \rho_{E,p} \subset C_{ns}^+(p)$ we know that E has potentially good reduction at p .
- Let \mathbb{Q}_p^{nr} be the maximal unramified extension of \mathbb{Q}_p and consider the base change of E to \mathbb{Q}_p^{nr} .
- Let K/\mathbb{Q}_p^{nr} be the minimal extension over which E acquires good reduction. It can be shown that $[K : \mathbb{Q}_p^{nr}] \in \{3, 6\}$.
- If E admitted a canonical subgroup, there would be a subgroup of order p stable for the Galois action, hence the image of $\text{Gal}(\overline{\mathbb{Q}}_p/K)$ would be contained in a Borel subgroup.
- However, the image is contained in $C_{ns}^+(p)$, hence is diagonal. This cannot happen, because there must be an element of order $\frac{p^2-1}{6}$ (as shown by Serre).

The canonical subgroup

E doesn't admit a canonical subgroup, hence by Lubin's theorem

$$v_p(A) \geq \frac{p}{p+1}.$$

The canonical subgroup

E doesn't admit a canonical subgroup, hence by Lubin's theorem

$$v_p(A) \geq \frac{p}{p+1}.$$

If we take an integral model in \mathcal{O}_K

$$E : y^2 = x^3 + ax + b$$

the valuation of A must be contained in $\frac{1}{6}\mathbb{Z}$, and so $v_p(A) \geq 1$.

The canonical subgroup

E doesn't admit a canonical subgroup, hence by Lubin's theorem

$$v_p(A) \geq \frac{p}{p+1}.$$

If we take an integral model in \mathcal{O}_K

$$E : y^2 = x^3 + ax + b$$

the valuation of A must be contained in $\frac{1}{6}\mathbb{Z}$, and so $v_p(A) \geq 1$.

With some calculations, one can show that $v_p(A) = v_p(a)$.

Moreover, since the curve has good reduction $v_p(\Delta) = 0$. We have

$$v_p(j(E)) = v_p\left(12^3 \cdot \frac{(64a)^3}{\Delta}\right) = 3v_p(a) = 3v_p(A)$$

and hence $v_p(j) \geq 3$.

The canonical subgroup

E doesn't admit a canonical subgroup, hence by Lubin's theorem

$$v_p(A) \geq \frac{p}{p+1}.$$

If we take an integral model in \mathcal{O}_K

$$E : y^2 = x^3 + ax + b$$

the valuation of A must be contained in $\frac{1}{6}\mathbb{Z}$, and so $v_p(A) \geq 1$.

With some calculations, one can show that $v_p(A) = v_p(a)$.

Moreover, since the curve has good reduction $v_p(\Delta) = 0$. We have

$$v_p(j(E)) = v_p\left(12^3 \cdot \frac{(64a)^3}{\Delta}\right) = 3v_p(a) = 3v_p(A)$$

and hence $v_p(j) \geq 3$.

Finally, studying the image of the inertia one can show that

$3 \nmid v_p(j)$, so $p^4 \mid j$.

Conclusion

So far, we have obtained

$$p < 10^5 \quad \text{and} \quad \log |j| \leq 40.$$

So far, we have obtained

$$p < 10^5 \quad \text{and} \quad \log |j| \leq 40.$$

Since $p^4 \mid j$ we have

$$4 \log p \leq 40 \quad \implies \quad p < 22000.$$

So far, we have obtained

$$p < 10^5 \quad \text{and} \quad \log |j| \leq 40.$$

Since $p^4 \mid j$ we have

$$4 \log p \leq 40 \quad \implies \quad p < 22000.$$

To conclude, we test all primes $p < 22000$ and all (isom. classes of) elliptic curves with integral $|j| = |p^k \cdot c^3| \leq e^{40}$ by searching an element of $\text{Im } \rho_{E,p}$ which is not in $G(p)$.

Thank you for your attention