Effective versions of Serre's open image theorem for elliptic curves

Alina-Carmen Cojocaru
Princeton University/MSRI Berkeley

April 2006

1. INTRODUCTION

- K a *number field*

- $E/K : y^2 = x^3 + Ax + B$

  an *elliptic curve* over K, of conductor N_E.

- for a rational prime ℓ,

  $$E[\ell] := \{P \in E(\mathbb{C}) : \ell P = \mathcal{O}\}$$

  the *ℓ-th division group* of E.

Then:

- $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$;

- $K(E[\ell])/K$ is a finite Galois extension.

Thus there exists a natural representation

$$\rho_{E/K,\ell} : \mathrm{Gal}(K(E[\ell])/K) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Properties of $\rho_{E/K,\ell}$:

1. $\rho_{E/L,\ell}$ is injective.

2. **(Complex Multiplication theory)**

Suppose E/L is *with CM* by L .

Then

$$\text{Gal}(L(E[\ell])/L) \simeq \left(\frac{\mathcal{O}_L}{\ell\mathcal{O}_L}\right)^* \quad \forall(\ell, 6N_E) = 1;$$

in particular,

$$\rho_{E/K,\ell} \text{ is not surjective.}$$

3. **(J-P. Serre, 1972)**

Suppose E/K is *without CM*. Then

$\exists\ c(E, K)$ such that

$$\rho_{E/K,\ell} \text{ is surjective} \qquad \forall \ell \geq c(E, K).$$

OR

$\exists\ A(E,K)$ such that

$\rho_{E/K,n}$ is surjective for all n coprime to $A(E,K)$.

2. Questions

Question 1 (Serre, 1981)

Is there an effective description of $c(E, K)$ in terms of E and K?

Question 2 (Serre, 1972 & 1981)

Is it true that $c(E, K) = c(K)$?

Reformulation of Serre's uniformity question

Let

$$S_{E/K} := \{\ell : \rho_{E/K,\ell} \text{ is } \textbf{not} \text{ surjective}\},$$

$$S_K := \cup_{E/K \text{ non-CM}} S_{E/K}.$$

Serre's theorem says that

$$S_{E/K} \text{ is finite.}$$

Can one also show that S_K finite?

FURTHER REFINEMENTS

- $B :=$ Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$
- $N_s :=$ normalizer of a split Cartan C_s subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$
- $N_{ns} :=$ normalizer of a non-split Cartan C_{ns} subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$
- $D :=$ subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ whose projective image is S_4, A_4 or A_5

Fact

If $\rho_{E/K,\ell}$ is not surjective, then

$\mathrm{Im}\,\rho_{E/K,\ell} \subseteq H$ for some $H \in \{B, N_s, N_{ns}, D\}$.

Refined Serre's question

For H as above, is

$$S_K^H := \cup_{E/K \text{ non-CM}} \{\ell : \mathrm{Im}\, \rho_{E/K,\ell} \subseteq H\}$$

finite?

2. SOME MOTIVATION

2.1. Lang-Trotter constants

2.2. Diophantine equations

3. FINITENESS OF $S_{\mathbb{Q}}^{D}$

By using local methods:

Serre's Theorem (1970s)

$$S_{\mathbb{Q}}^{D} \subseteq \{\ell \leq 13\}.$$

4. FINITENESS OF $S_{\mathbb{Q}}^{B}$

Mazur's Theorem (1978)

Let ℓ be a prime such that $\exists\, E/\mathbb{Q}$ which admits a $\mathbb{Q}$-rational ℓ-isogeny. Then

$$\ell \in \{2, 3, 5, 7, 3, 13; 11, 17, 19, 37, 163\}.$$

Corollary 1

$$S_{\mathbb{Q}}^{B} \subseteq \{\ell \leq 37\}.$$

Corollary 2

If $E/\mathbb{Q}$ semistable, then $\rho_{E/\mathbb{Q},\ell}$ surjective for all $\ell \geq 11$.

- $X(\ell)$:= the complete modular curve of level ℓ which parameterizes elliptic curves $E/\mathbb{Q}$ together with chosen bases of $E[\ell]$

- For $H \leq \mathrm{GL}_2(\mathbb{F}_\ell)$,

$$X_H(\ell) := X(\ell)/H$$

<u>Fact</u> The curve $X_H(\ell)$ classifies elliptic curves $E/\mathbb{Q}$ (up to $\bar{\mathbb{Q}}$-isom.) such that $\operatorname{Im} \rho_{E/\mathbb{Q},\ell} \subseteq H$.

Reformulation of Serre's question

Are

$$X_B(\ell)(\mathbb{Q}),\ X_{N_s}(\ell)(\mathbb{Q}),\ X_{N_{ns}}(\ell)(\mathbb{Q}),\ X_D(\ell)(\mathbb{Q})$$

trivial for ℓ sufficiently large?

4. FINITENESS OF $S_{\mathbb{Q}}^{N_s}$, $S_{\mathbb{Q}}^{N_{ns}}$???

4.1 Momose's Theorem (1984)

Let ℓ be a prime.

Let $E/\mathbb{Q}$ be non-CM and such that

- $j(E) \notin \mathbb{Z}\left[\frac{1}{2\ell}\right]$
- $\mathrm{Im}\, \rho_{E/\mathbb{Q},\ell} \subseteq N_s$.

Then

$$\ell = 13 \text{ or } \ell \leq 7.$$

4.2. Connection with congruence primes

Theorem (Imin Chen, 2000)

Let ℓ be an odd prime.

Let $E/\mathbb{Q}$ be non-CM, of conductor N_E, and with associated newform $f_E \in S_2(\Gamma_0(N_E), \mathbb{Z})$.

1. If $\mathrm{Im}\, \rho_{E/\mathbb{Q},\ell} \subseteq N_s$ or N_{ns}, then

$$\ell \text{ is a congruence prime for } f_E.$$

2. If $3 < \ell \nmid N_E$ and

$$\text{Im}\, \rho_{E/\mathbb{Q},\ell} \subseteq N_{ns},$$

then $\exists$ newforms

$$g \in S_2(\Gamma_1(M)), \;\; h \in S_2(\Gamma_0(M))$$

such that

(a) g, h are induced from a Grossencharacter of the quadratic field cut out by the Dirichlet character

$\epsilon : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{Im}\, \rho_{E/\mathbb{Q},\ell} \to N_{ns}/C_{ns} \simeq \{\pm 1\}$

(b) $f \equiv g (\text{mod}\, \lambda)$ and $f \equiv h (\text{mod}\, \lambda)$ for λ prime above ℓ.

Remark Bounding congruence primes is related to bounding the degree of the modular parameterizations of elliptic curves over $\mathbb{Q}$;

this, in turn, is related to the ABC conjecture.

We will see this connection once again...

4.3 Parent's Theorem (2003)

$X_{N_s}(\ell)(\mathbb{Q})$ is trivial if

$\ell \geq 11$, $\ell \neq 13, 37$, and $\ell \notin \mathcal{A}$,

where

$\mathcal{A} := \{$ primes which are simultaneously a square mod 3, mod 4, mod 7
and a square mod at least five of
8, 11, 19, 43, 67, 163 $\}$.

(the density of $\mathcal{A}$ is 0.986...)

5. EFFECTIVE RESULTS FOR $S_{\mathbb{Q}}^N$

5.1. Isogeny estimates

By using upper estimates for the degree of an isogeny over $\bar{K}$ between (principally polarized) abelian varieties/K:

Masser-Wüstholz Theorem (1992)

There exist absolute constants c, γ such that:

if E/K is a non-CM elliptic curve over a number field K, then

$$\text{Im}\,\rho_{E/K,\ell} = \text{GL}_2(\mathbb{F}_\ell)$$

for any prime $\ell \nmid \text{disc}(K/\mathbb{Q})$ such that

$$\ell > c \cdot \max\{|K : \mathbb{Q}|, h(E)\}^\gamma,$$

where $h(E)$ is the Weil height of E.

Remark 1 One can replace $h(E)$ with $\log H(E)$, where $H(E)$ is the naive height of E.

Remark 2 The constants c, γ are effective, but huge; e.g.

$$\gamma < 10^{25{,}000};$$

worked out by Takashi Kawamura (2003).

Remark 3 If $K = \mathbb{Q}$, we can use the modularity of $E/\mathbb{Q}$; thus there is a nontrivial surjective rational morphism

$$\phi : X_0(N_E) \longrightarrow E.$$

There is a relation between $\deg \phi$ and $h(E)$:

$$(1-\varepsilon)\log N_E + 2h(E)$$

$$< \log \deg \phi + O(1) <$$

$$(1+\varepsilon)\log N_E + 2h(E) \ \ \forall \varepsilon > 0.$$

Now we can invoke <u>the degree conjecture</u>

$$\deg \phi = \mathrm{O}_\varepsilon(N_E^{2+\varepsilon})$$

to get:

<u>Theorem</u>

If $\ell \geq c(\log N_E)^\gamma$, then $\mathrm{Im}\,\rho E/\mathbb{Q}, \ell = \mathrm{GL}_2(\mathbb{F}_\ell)$.

5.2 Serre's criterion

Let $E/\mathbb{Q}$ be non-CM, of conductor N_E.

Let $\ell \neq 37, \geq 19$ be such that $\rho_{E/\mathbb{Q},\ell}$ is **not** surjective.

Let

$$\epsilon : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \{\pm 1\}$$

be the quadratic Dirichlet character mentioned before.

Then:

1. ϵ is unramified outside N_E;

2. $\ell \mid a_p(E)$ for any prime $p \nmid N_E$ such that $\epsilon(p) = -1$.

Another reformulation of Serre's question

Find an upper bound for the least prime p_0 such that

- $p_0 \nmid N_E$;
- $\epsilon(p_0) = -1$;
- $a_{p_0}(E) \neq 0$.

By combining this with Serre's criterion and Hasse's bound $|a_{p_0}| < 2\sqrt{p_0}$, we will get an upper bound for ℓ.

General strategy

Twist $E/\mathbb{Q}$ by the character ϵ and get an elliptic curve $E'/\mathbb{Q}$.

Since $E/\mathbb{Q}$ is non-CM, there are infinitely many primes p such that

$$a_p(E) \neq a_p(E').$$

Also, one can show that $E'/\mathbb{Q}$ has good reduction outside N_E.

FIND A WAY to estimate (perhaps in terms of N_E) the least prime p_0 such that

- $p_0 \nmid N_E$
- $a_{p_0}(E) \neq a_{p_0}(E')$.

(I) Use effective versions of the Chebotarev density theorem:

Serre's Theorem (1981)

Assume GRH.

Let $E/\mathbb{Q}$ be non-CM, of conductor N_E.

If $\ell \geq 19, \ell \neq 37$ and

$$\ell \geq c(\log N_E)(\log\log 2N_E)^2,$$

then $\operatorname{Im} \rho_{E/\mathbb{Q},\ell} = \mathrm{GL}_2(\mathbb{F}_\ell)$.

(II) Use modularity and theory of modular forms:

Theorem (A. Kraus 1995; A.C. Cojocaru 2001)

Let $E/\mathbb{Q}$ be non-CM, of conductor N_E.

If

$$\ell \geq cN_E(\log\log N_E)^{1/2},$$

then $\operatorname{Im} \rho_{E/\mathbb{Q},\ell} = \mathrm{GL}_2(\mathbb{F}_\ell)$.

(III) Use modularity and the Rankin-Selberg method:

$$\sum_{\substack{n \le x \\ (n, N_E)=1}} [\tilde{a}_n(f_E) - \tilde{a}_n(f_{E'})]^2 = \text{Main term} + \text{error}.$$

A.C. Cojocaru and R. Murty –work in progress:

Expect to find $\theta < 1$ such that

$$\operatorname{Im} \rho_{E/\mathbb{Q},\ell} = \mathrm{GL}_2(\mathbb{F}_\ell)$$

for all

$$\ell \ge c N_E^{\theta}.$$

6. AVERAGE RESULTS

- $\mathcal{F}$ infinite family of elliptic curves E/K

- $\mathcal{E}_{\ell_0} := \{E \in \mathcal{F} : \exists \ell \geq \ell_0 \text{ s.th. } \rho_{E/K,\ell} \textbf{ not } \text{surj.}\}$

Question

Can we show that

$$\frac{|\mathcal{E}_{\ell_0}|}{|\mathcal{F}|} = 0?$$

6.1 Two-parameter average

Let

$$\alpha := x^2, \quad \beta := x^3.$$

Let $A, B \in \mathbb{Z}$,

$$|A| \leq \alpha, \quad |B| \leq \beta,$$

such that

$$E_{A,B} : y^2 = x^3 + Ax + B$$

elliptic curve/$\mathbb{Q}$.

Take

$\mathcal{F}(x) := \{(A, B) \in \mathbb{Z}^2 : |A| \leq \alpha, |B| \leq \beta, E_{A,B}/\mathbb{Q}$ e.c$\}$.

Theorem (W. Duke, 1995):

$$\lim_{x \to \infty} \frac{|\mathcal{E}_2(x)|}{|\mathcal{F}(x)|} = 0.$$

Uses **Gallagher's two-dimensional large sieve**,

together with **Deuring's formula**

$$\#\{(A,B) \in \mathbb{F}_p^2 : a_p(E_{A,B}) = a\}$$

$$= \frac{1}{2}(p-1)H(4p-a^2) \quad \forall\, p \geq 5$$

and **Hurwitz's formula**

$$\sum_{a \equiv \tau (\mathrm{mod}\, \ell)} H(4p-a^2)$$

$$= 2\frac{\ell + \left(\frac{\tau^2-4\delta}{\ell}\right)}{\ell^2-1}(p-1) + \mathrm{O}(\ell p^{1/2})$$

for $p \equiv \delta (\mathrm{mod}\, \ell)$.

6.2 One-parameter average

Let $A(t), B(t) \in \mathbb{Z}[t]$ such that

$$E/\mathbb{Q}(t) : y^2 = x^3 + A(t)x + B(t)$$

e.c./$\mathbb{Q}(t)$ with $j \notin \mathbb{Q}$.

Let $\Delta_{A,B} := -16\left[4A(t)^3 + 27B(T)^2\right]$.

Let $S := \{t_0 \in \mathbb{Q} : \Delta_{A,B}(t_0) = 0\}$.

Take

$$\mathcal{F}(T) := \left\{t_0 = \frac{m}{n} \in \mathbb{Q} \backslash S : \max\{|m|, |n|\} \leq T\right\}.$$

<u>Theorem (A.C. Cojocaru and C. Hall, 2005)</u>

$$\lim_{T \to \infty} \frac{|\mathcal{E}_{17}(T)|}{|\mathcal{F}(T)|} = 0.$$

Uses **Gallagher's two-dimensional large sieve**,

together with **effective version of Igusa's theorem** about division fields of elliptic curves over function fields:

Igusa's Theorem (1959)

Let:

- $C/\mathbb{F}_q$ proper, smooth, geom. connected curve
- $K := \mathbb{F}_q(C)$
- E/K elliptic curve with $j \notin \mathbb{F}_q$
- ℓ rational prime s.th. $q \equiv 1 \pmod{\ell}$

Then

$$\exists\, c(E,K) \text{ such that}$$

$$\mathrm{Gal}(K(E[\ell])/K) \simeq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \quad \forall \ell \geq c(E,K).$$

Theorem (A.C. Cojocaru and C. Hall, 2005)

The constant $c(E, K)$ depends at most on the genus of K.

It can be calculated as

$$2 + \max\left\{\ell : \frac{1}{12}[\ell - (6 + 3\epsilon_2 + 4\epsilon_3)] \leq \text{genus}(K)\right\},$$

where

$$\epsilon_2 := \begin{cases} +1 & \text{if } \ell \equiv 1 (\text{mod}\, 4) \\ -1 & \text{otherwise,} \end{cases}$$

$$\epsilon_3 := \begin{cases} +1 & \text{if } \ell \equiv 1 (\text{mod}\, 3) \\ -1 & \text{otherwise.} \end{cases}$$

6.4 Remaining question

What about $\ell < \ell_0$?

- **Two-parameter average**:

  complete results by **D. Grant, 2000**

- **One-parameter average**:

  in progress...

7. CONCLUSIONS

- Is the function field result

$$c(E, K) = c(\text{genus}(K)) = \ldots$$

  best possible?

- Can we average over more general families?

- What can we say about (effective versions of) open image theorems for modular forms, abelian varieties, or Drinfeld modules?