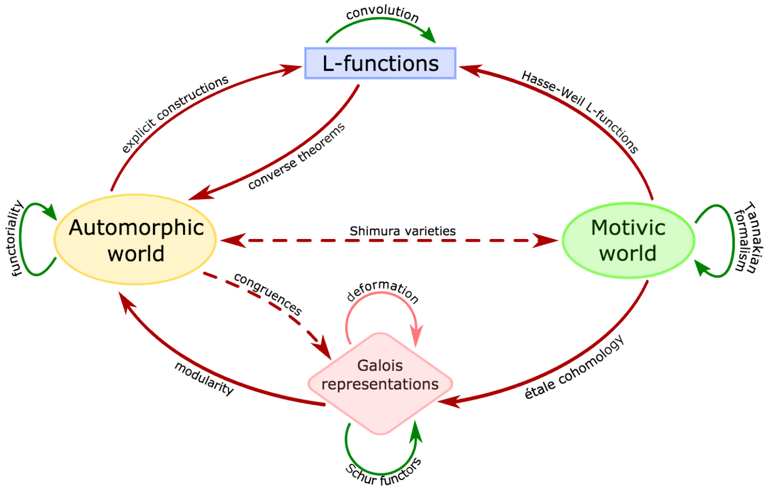
MULTIPLICITY ONE THEOREMS
VIA GALOIS REPRESENTATIONS

S. Aniruddha

Indian Institute of Science Education and Research, Bhopal

Algebra-Number Theory Seminar 2022



convolution
L-functions
explicit constructions
converse theorems
Hasse-Weil L-functions
functoriality
Automorphic world
Shimura varieties
Motivic world
Tannakian formalism
congruences
deformation
Galois representations
modularity
étale cohomology
Schur functors

The philosophy of a **multiplicity one theorem** can be stated (vaguely) as follows:

If two global objects satisfy certain local properties at enough primes, then the objects are same.

The name *multiplicity-one* comes from the theory of automorphic representations (not discussed in the talk).

AIM FOR THE TALK

To state (and prove) such theorems in the context of **elliptic curves**, **modular forms**, and **Galois representations**.

A. O. L. Atkin and J. Lehner. “Hecke operators on $\Gamma_0(m)$”. In: *Math. Ann.* 185 (1970), pp. 134–160 prove the following result (loc. cit. Lemma 24) for newforms.

Theorem (A multiplicity one for modular forms)

Let $f_1(z) = \sum_{n\geq 1} a(f_1, n)q^n$, $f_2(z) = \sum_{n\geq 1} a(f_2, n)q^n$ be two newforms of level N such that

$$a(f_1, p) = a(f_2, p) \quad \text{for all } p \nmid N.$$

Then $f_1 = f_2$.

Table of Contents

Let K be a field with $\mathrm{Char}(K) \neq 2, 3$ and let $\overline{K}$ be a fixed algebraic closure of K.

DEFINITION

An elliptic curve E over K (denoted by E/K) is a smooth projective curve in $\mathbb{P}^2(\overline{K})$ given by an equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \quad a, b \in K.$$

EXAMPLE

The curve $E : Y^2Z = X^3 - XZ^2$ is an elliptic curve over $\mathbb{Q}$.

Let K be a field with $\mathrm{Char}(K) \neq 2, 3$ and let $\overline{K}$ be a fixed algebraic closure of K.

Definition

An elliptic curve E over K (denoted by E/K) is a smooth projective curve in $\mathbb{P}^2(\overline{K})$ given by an equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \quad a, b \in K.$$

Example

The curve $E : Y^2Z = X^3 - XZ^2$ is an elliptic curve over $\mathbb{Q}$.

An elliptic curve E/K can also be seen as

$$\{[x, y, 1] \in \mathbb{P}^2(\overline{K}) \mid y^2 = x^3 + ax + b\} \bigcup \{[0, 1, 0]\}.$$

The point $O_E := [0, 1, 0]$ is called as the point at infinity.

- There is a group law on E,

$$+ : E \times E \to E, \quad (P, Q) \mapsto P + Q,$$

proved using the *Riemann–Roch Theorem*, with respect to which O_E is the identity of E.

- There is a group law on E,

$$+ : E \times E \to E, \quad (P, Q) \mapsto P + Q,$$

proved using the *Riemann–Roch Theorem*, with respect to which O_E is the identity of E.

- Define the **multiplication-by-m map**

$$[m] : E \to E, \quad P \mapsto \underbrace{P + \cdots + P}_{m\text{-times}}.$$

- The map $[m]$ is a group homomorphism. Denote its kernel by $E[m]$.

Torsion points on an elliptic curve

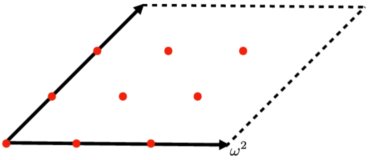


Figure: 3-torsion points on a torus. Source: Google

- It is seen that if $\mathrm{Char}(K) = 0$, then

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}),$$

for all $m > 1$. (For $K = \mathbb{C}$, $E[m]$ is m-torsion points on a torus.)

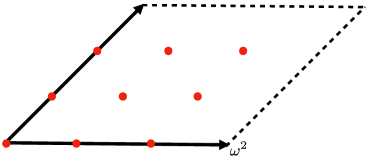


FIGURE: 3-torsion points on a torus. Source: Google

- It is seen that if $\mathrm{Char}(K) = 0$, then

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}),$$

  for all $m > 1$. (For $K = \mathbb{C}$, $E[m]$ is m-torsion points on a torus.)
- Note that the above groups ($\mathbb{Z}$-modules) are same for all elliptic curves over K. We will see later, for $K = \mathbb{Q}$, that the absolute Galois group G_K acts on $E[m]$, and they are different as G_K-modules for different elliptic curves.

DEFINITION

Let E_1, E_2 be two elliptic curves over K. An **isogeny** between E_1 and E_2 is a morphism of varieties which is also a homomorphism of groups.

If there is a non-zero isogeny $E_1 \to E_2$, then we say that E_1 and E_2 are **isogenous**.

EXAMPLE (FROBENIUS ISOGENY)

Let $E/\mathbb{F}_p$ be an elliptic curve. The map

$$\varphi_p : E \to E, \quad [a, b, c] \to [a^p, b^p, c^p],$$

is seen to be an isogeny.

An elliptic curve $E/\mathbb{Q}$ (by change of variable) can be seen as the solution set of the cubic equation

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}.$$

For a prime p, the **reduction mod** p of E is the curve $\tilde{E}_p$ over $\mathbb{F}_p$ given by

$$y^2 = x^3 + \overline{a}x + \overline{b},$$

where $\overline{a}$ is the image of a under the projection map $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

An elliptic curve $E/\mathbb{Q}$ (by change of variable) can be seen as the solution set of the cubic equation

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}.$$

For a prime p, the **reduction mod** p of E is the curve $\tilde{E}_p$ over $\mathbb{F}_p$ given by

$$y^2 = x^3 + \overline{a}x + \overline{b},$$

where $\overline{a}$ is the image of a under the projection map $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Definition

A prime p is said to be a **prime of good reduction** for E if $p \nmid \mathrm{disc}(x^3 + ax + b)$. Equivalently, it is seen that the curve $\tilde{E}_p$ is an elliptic curve over $\mathbb{F}_p$.

NOTATION

For an elliptic curve $E/\mathbb{F}_p$, denote $E(\mathbb{F}_p)$ for the $\mathbb{F}_p$-rational points on E, i.e.

$$E(\mathbb{F}_p) = \{[x, y, 1] \in E |\ x, y \in \mathbb{F}_p\} \cup \{O_E\}.$$

- Let E, E' be two elliptic curves over $\mathbb{Q}$.
- For a prime p of good reduction for E (resp. E'), let $\tilde{E}_p(\mathbb{F}_p)$ (resp. $\tilde{E}'_p(\mathbb{F}_p)$) denote the $\mathbb{F}_p$-rational points in the respective reductions mod p.

NOTATION

For an elliptic curve $E/\mathbb{F}_p$, denote $E(\mathbb{F}_p)$ for the $\mathbb{F}_p$-rational points on E, i.e.

$$E(\mathbb{F}_p) = \{[x, y, 1] \in E \mid x, y \in \mathbb{F}_p\} \cup \{O_E\}.$$

- Let E, E' be two elliptic curves over $\mathbb{Q}$.
- For a prime p of good reduction for E (resp. E'), let $\tilde{E}_p(\mathbb{F}_p)$ (resp. $\tilde{E}'_p(\mathbb{F}_p)$) denote the $\mathbb{F}_p$-rational points in the respective reductions mod p.

THEOREM (MULTIPLICITY ONE THEOREM)

If $|\tilde{E}_p(\mathbb{F}_p)| = |\tilde{E}'_p(\mathbb{F}_p)|$ for all primes p of good reduction for E and E', then E and E' are isogenous.

Table of Contents

- Let F be a field, $\overline{F}$ be a fixed algebraic closure of F, and let G_F denote the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$.
- G_F is a **compact** topological group with the *Krull topology*. A basic open set around $\sigma \in G_F$ is defined, for a finite extension L/F, as

$$B(\sigma, L) = \{\tau \in G_F \mid \tau = \sigma \text{ on } L\} = \sigma \mathrm{Gal}(\overline{F}/L).$$

Definition

Let R be a topological ring. A **Galois representation** of G_F into R is a continuous representation $G_F \to \mathrm{GL}_n(R)$, for some $n \geq 1$.

EXAMPLE: ARTIN REPRESENTATIONS

- Let L/F be a finite Galois extension, i.e. $\mathrm{Gal}(L/F)$ is a finite group. Consider a representation $\rho : \mathrm{Gal}(L/F) \to \mathrm{GL}_n(\mathbb{C})$. It is continuous with the *discrete topology* on $\mathrm{Gal}(L/F)$.
- Composing the above representation with the restriction map $G_F \to \mathrm{Gal}(L/F)$, sending $\sigma \to \sigma|_L$, we have a representation of G_F,

$$\tilde{\rho} : G_F \to \mathrm{Gal}(L/F) \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{C}).$$

- The map $G_F \to \mathrm{Gal}(L/F)$ is continuous, implying that $\tilde{\rho}$ is a Galois representation.

- Let L/F be a finite Galois extension, i.e. $\mathrm{Gal}(L/F)$ is a finite group. Consider a representation $\rho : \mathrm{Gal}(L/F) \to \mathrm{GL}_n(\mathbb{C})$. It is continuous with the *discrete topology* on $\mathrm{Gal}(L/F)$.
- Composing the above representation with the restriction map $G_F \to \mathrm{Gal}(L/F)$, sending $\sigma \to \sigma|_L$, we have a representation of G_F,

$$\tilde{\rho} : G_F \to \mathrm{Gal}(L/F) \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{C}).$$

- The map $G_F \to \mathrm{Gal}(L/F)$ is continuous, implying that $\tilde{\rho}$ is a Galois representation.
- **Theorem.** *Every Galois representation $\rho : G_F \to \mathrm{GL}_n(\mathbb{C})$ factors through a finite Galois extension, i.e. there is a finite Galois extension L/F such that*

$$\rho : G_F \to \mathrm{Gal}(L/F) \to \mathrm{GL}_n(\mathbb{C}).$$

THE BRAUER–NESBITT THEOREM

- By representation theory of finite groups, for a finite group G, two representations $\rho_1, \rho_2 : G \to \mathrm{GL}_n(\mathbb{C})$ with same traces are isomorphic. That is, if $\mathrm{Tr}(\rho_1(g)) = \mathrm{Tr}(\rho_2(g))$ for all g, then ρ_1 and ρ_2 are isomorphic.

The Brauer–Nesbitt theorem

- By representation theory of finite groups, for a finite group G, two representations $\rho_1, \rho_2 : G \to \mathrm{GL}_n(\mathbb{C})$ with same traces are isomorphic. That is, if $\mathrm{Tr}(\rho_1(g)) = \mathrm{Tr}(\rho_2(g))$ for all g, then ρ_1 and ρ_2 are isomorphic.

This is generalised in the following theorem for Galois representations.

Theorem

Let K be a topological field with $\mathrm{Char}(K) = 0$. If $\rho_1, \rho_2 : G_F \to \mathrm{GL}_n(K)$ are two ***semi-simple*** *Galois representations with same trace, i.e.*

$$\mathrm{Tr}(\rho_1(g)) = \mathrm{Tr}(\rho_2(g))$$

for all $g \in G_F$. then ρ_1 and ρ_2 are isomorphic.

- By representation theory of finite groups, for a finite group G, two representations $\rho_1, \rho_2 : G \to \mathrm{GL}_n(\mathbb{C})$ with same traces are isomorphic. That is, if $\mathrm{Tr}(\rho_1(g)) = \mathrm{Tr}(\rho_2(g))$ for all g, then ρ_1 and ρ_2 are isomorphic.

This is generalised in the following theorem for Galois representations.

THEOREM

Let K be a topological field with $\mathrm{Char}(K) = 0$. If $\rho_1, \rho_2 : G_F \to \mathrm{GL}_n(K)$ are two ***semi-simple*** *Galois representations with same trace, i.e.*

$$\mathrm{Tr}(\rho_1(g)) = \mathrm{Tr}(\rho_2(g))$$

for all $g \in G_F$. then ρ_1 and ρ_2 are isomorphic.

- A semi-simple representation is a representation isomorphic to the **direct sum of irreducible representations**. Note that all representations of finite groups into $\mathrm{GL}_n(\mathbb{C})$ are semisimple.

- By representation theory of finite groups, for a finite group G, two representations $\rho_1, \rho_2 : G \to \mathrm{GL}_n(\mathbb{C})$ with same traces are isomorphic. That is, if $\mathrm{Tr}(\rho_1(g)) = \mathrm{Tr}(\rho_2(g))$ for all g, then ρ_1 and ρ_2 are isomorphic.

This is generalised in the following theorem for Galois representations.

THEOREM

Let K be a topological field with $\mathrm{Char}(K) = 0$. If $\rho_1, \rho_2 : G_F \to \mathrm{GL}_n(K)$ are two ***semi-simple*** *Galois representations with same trace, i.e.*

$$\mathrm{Tr}(\rho_1(g)) = \mathrm{Tr}(\rho_2(g))$$

for all $g \in G_F$. then ρ_1 and ρ_2 are isomorphic.

- A semi-simple representation is a representation isomorphic to the **direct sum of irreducible representations**. Note that all representations of finite groups into $\mathrm{GL}_n(\mathbb{C})$ are semisimple.
- Instead of checking the traces at all $g \in G_F$, is it enough to check the traces at a smaller set? (A dense subset would do, but which one?)

Let us recall some notations and definitions.

- Let $L/\mathbb{Q}$ be a Galois extension. For a prime p in $\mathbb{Q}$, let $I_p(L) < \mathrm{Gal}(L/\mathbb{Q})$ be the **inertia group** of L at p.
- If $I_p(L) = 1$, then we say p is **unramified** in L.

Let us recall some notations and definitions.

- Let $L/\mathbb{Q}$ be a Galois extension. For a prime p in $\mathbb{Q}$, let $I_p(L) < \mathrm{Gal}(L/\mathbb{Q})$ be the **inertia group** of L at p.
- If $I_p(L) = 1$, then we say p is **unramified** in L.
- For an unramified prime p in L, we have the **Frobenius conjugacy class**

$$\mathrm{Frob}_{p,L} \subset \mathrm{Gal}(L/\mathbb{Q}).$$

Let us recall some notations and definitions.

- Let $L/\mathbb{Q}$ be a Galois extension. For a prime p in $\mathbb{Q}$, let $I_p(L) < \mathrm{Gal}(L/\mathbb{Q})$ be the **inertia group** of L at p.
- If $I_p(L) = 1$, then we say p is **unramified** in L.
- For an unramified prime p in L, we have the **Frobenius conjugacy class**

$$\mathrm{Frob}_{p,L} \subset \mathrm{Gal}(L/\mathbb{Q}).$$

Proposition

If all but finitely many primes are unramifed in L, then the set

$$\{\mathrm{Frob}_{p,L} \mid p \text{ is unramified in } L\}$$

is dense in $\mathrm{Gal}(L/\mathbb{Q})$.

The proof uses **Chebotarev Density Theorem**.

Trace of Frobenius

Definition

A representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(R)$ is said to be **unramified at** p if $I_p(\overline{\mathbb{Q}}_p) \subseteq \ker \rho$.

Trace of Frobenius

Definition

A representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(R)$ is said to be **unramified at** p if $I_p(\overline{\mathbb{Q}}_p) \subseteq \ker \rho$.

- A **Frobenius element** at p in $G_{\mathbb{Q}}$ is an element Frob_p such that its restriction to L,

$$\mathrm{Frob}_p|_L \in \mathrm{Frob}_{p,L},$$

  for all finite Galois extensions $L/\mathbb{Q}$ in which p is unramified.
- It can be seen that any two Frobenius elements are either conjugates of each other, or they differ my an inertia element, i.e. if $\mathrm{Frob}_p, \mathrm{Frob}'_p$ are Frobenius elements at p, then

$$\mathrm{Frob}_p = \tau \mathrm{Frob}'_p \tau^{-1}, \quad \tau \in G_{\mathbb{Q}},$$

$$\text{or, } \mathrm{Frob}_p = \mathrm{Frob}'_p i, \;\; i \in I_p(\overline{\mathbb{Q}}_p).$$

DEFINITION

A representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(R)$ is said to be **unramified at** p if $I_p(\overline{\mathbb{Q}}_p) \subseteq \ker \rho$.

- A **Frobenius element** at p in $G_{\mathbb{Q}}$ is an element Frob_p such that its restriction to L,

$$\mathrm{Frob}_p|_L \in \mathrm{Frob}_{p,L},$$

  for all finite Galois extensions $L/\mathbb{Q}$ in which p is unramified.
- It can be seen that any two Frobenius elements are either conjugates of each other, or they differ my an inertia element, i.e. if $\mathrm{Frob}_p, \mathrm{Frob}'_p$ are Frobenius elements at p, then

$$\mathrm{Frob}_p = \tau \mathrm{Frob}'_p \tau^{-1}, \quad \tau \in G_{\mathbb{Q}},$$
$$\text{or, } \mathrm{Frob}_p = \mathrm{Frob}'_p i, \ i \in I_p(\overline{\mathbb{Q}}_p).$$

- From the definition, and the previous remark, if ρ is unramified at p, then $\mathrm{Tr}(\rho(\mathrm{Frob}_p))$ is **well-defined** for a Frobenius element Frob_p at p. Moreover, as $\det$ is also invariant in a conjugacy class, $\det(\rho(\mathrm{Frob}_p))$ is also well defined.

A multiplicity one theorem for Galois representations

Theorem

Let K be a topological field and let $\rho_1, \rho_2 : G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$ be two ***semi-simple*** *Galois representations which are unramified outside a finite set S of primes in $\mathbb{Q}$. If*

$$\mathrm{Tr}(\rho_1(\mathrm{Frob}_p)) = \mathrm{Tr}(\rho_2(\mathrm{Frob}_p)), \quad \text{for all } p \notin S,$$

then ρ_1 and ρ_2 are isomorphic.

THEOREM

Let K be a topological field and let $\rho_1, \rho_2 : G_{\mathbb{Q}} \to \mathrm{GL}_n(K)$ be two ***semi-simple*** *Galois representations which are unramified outside a finite set S of primes in $\mathbb{Q}$. If*

$$\mathrm{Tr}(\rho_1(\mathrm{Frob}_p)) = \mathrm{Tr}(\rho_2(\mathrm{Frob}_p)), \quad \text{for all } p \notin S,$$

then ρ_1 and ρ_2 are isomorphic.

Proof. From continuity of ρ_i's and the proposition mentioned in the previous slide, it follows that $\mathrm{Tr}(\rho_1(g)) = \mathrm{Tr}(\rho_2(g))$ for all $g \in G_{\mathbb{Q}}$. Hence, the theorem follows by Brauer–Nesbitt Theorem. □

Table of Contents

Galois action on torsion points

For a prime ℓ, we "attach" a Galois representation $G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{Q}_\ell)$ to an elliptic curve $E/\mathbb{Q}$.

- Let $\mathbb{Q}_\ell$ denote the completion of $\mathbb{Q}$ under the ℓ-adic norm $|\cdot|_\ell$.

GALOIS ACTION ON TORSION POINTS

For a prime ℓ, we "attach" a Galois representation $G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{Q}_\ell)$ to an elliptic curve $E/\mathbb{Q}$.

- Let $\mathbb{Q}_\ell$ denote the completion of $\mathbb{Q}$ under the ℓ-adic norm $|\cdot|_\ell$.
- Let $\mathbb{Z}_\ell = \{x \in \mathbb{Q}_\ell \mid |x|_\ell \leq 1\}$ be the valuation ring of $\mathbb{Q}_\ell$.

Galois action on torsion points

For a prime ℓ, we "attach" a Galois representation $G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{Q}_\ell)$ to an elliptic curve $E/\mathbb{Q}$.

- Let $\mathbb{Q}_\ell$ denote the completion of $\mathbb{Q}$ under the ℓ-adic norm $|\cdot|_\ell$.
- Let $\mathbb{Z}_\ell = \{x \in \mathbb{Q}_\ell \mid |x|_\ell \leq 1\}$ be the valuation ring of $\mathbb{Q}_\ell$.
- For $m > 0$, recall the set of ℓ^m-torsion points $E[\ell^m]$. We can see that points in $E[\ell^m]$ belong to $\mathbb{P}^2_{\overline{\mathbb{Q}}}$, i.e. if $[x, y, 1] \in E[\ell^m]$, then $x, y \in \overline{\mathbb{Q}}$. Hence, $G_{\mathbb{Q}}$ acts on $E[\ell^m]$ by

$$\sigma \cdot [x, y, 1] = [\sigma(x), \sigma(y), 1].$$

Moreover, we stated before that

$$E[\ell^m] \cong (\mathbb{Z}/\ell^m\mathbb{Z}) \times (\mathbb{Z}/\ell^m\mathbb{Z}).$$

For a prime ℓ, we "attach" a Galois representation $G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{Q}_\ell)$ to an elliptic curve $E/\mathbb{Q}$.

- Let $\mathbb{Q}_\ell$ denote the completion of $\mathbb{Q}$ under the ℓ-adic norm $|\cdot|_\ell$.
- Let $\mathbb{Z}_\ell = \{x \in \mathbb{Q}_\ell \mid |x|_\ell \leq 1\}$ be the valuation ring of $\mathbb{Q}_\ell$.
- For $m > 0$, recall the set of ℓ^m-torsion points $E[\ell^m]$. We can see that points in $E[\ell^m]$ belong to $\mathbb{P}^2_{\overline{\mathbb{Q}}}$, i.e. if $[x, y, 1] \in E[\ell^m]$, then $x, y \in \overline{\mathbb{Q}}$. Hence, $G_{\mathbb{Q}}$ acts on $E[\ell^m]$ by

$$\sigma \cdot [x, y, 1] = [\sigma(x), \sigma(y), 1].$$

  Moreover, we stated before that

$$E[\ell^m] \cong (\mathbb{Z}/\ell^m\mathbb{Z}) \times (\mathbb{Z}/\ell^m\mathbb{Z}).$$

- This gives a **mod ℓ^m representation** $G_{\mathbb{Q}} \to \mathrm{Aut}(E[\ell^m]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z})$.

Galois action on torsion points

For a prime ℓ, we "attach" a Galois representation $G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{Q}_\ell)$ to an elliptic curve $E/\mathbb{Q}$.

- Let $\mathbb{Q}_\ell$ denote the completion of $\mathbb{Q}$ under the ℓ-adic norm $|\cdot|_\ell$.
- Let $\mathbb{Z}_\ell = \{x \in \mathbb{Q}_\ell \mid |x|_\ell \leq 1\}$ be the valuation ring of $\mathbb{Q}_\ell$.
- For $m > 0$, recall the set of ℓ^m-torsion points $E[\ell^m]$. We can see that points in $E[\ell^m]$ belong to $\mathbb{P}^2_{\overline{\mathbb{Q}}}$, i.e. if $[x, y, 1] \in E[\ell^m]$, then $x, y \in \overline{\mathbb{Q}}$. Hence, $G_{\mathbb{Q}}$ acts on $E[\ell^m]$ by

$$\sigma \cdot [x, y, 1] = [\sigma(x), \sigma(y), 1].$$

Moreover, we stated before that

$$E[\ell^m] \cong (\mathbb{Z}/\ell^m\mathbb{Z}) \times (\mathbb{Z}/\ell^m\mathbb{Z}).$$

- This gives a **mod ℓ^m representation** $G_{\mathbb{Q}} \to \mathrm{Aut}(E[\ell^m]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z})$.
- This extends to an **ℓ-adic representation**

$$\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{Aut}\left(\varprojlim_m E[\ell^m]\right) \cong \mathrm{GL}_2(\mathbb{Z}_\ell) \subseteq \mathrm{GL}_2(\mathbb{Q}_\ell).$$

ℓ-ADIC TATE MODULE

- The $\mathbb{Z}_\ell[G_\mathbb{Q}]$-module $T_\ell(E) := \varprojlim E[\ell^m]$ is called as the $\mathbb{Z}_\ell$-*Tate module* of E.
- It is actually easier to work with the $\mathbb{Q}_\ell[G_\mathbb{Q}]$-module $V_\ell(E) := T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, called the **$\ell$-adic Tate module of E**.

- The $\mathbb{Z}_\ell[G_\mathbb{Q}]$-module $T_\ell(E) := \varprojlim E[\ell^m]$ is called as the $\mathbb{Z}_\ell$-*Tate module* of E.
- It is actually easier to work with the $\mathbb{Q}_\ell[G_\mathbb{Q}]$-module $V_\ell(E) := T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, called the **$\ell$-adic Tate module of** E.

THEOREM

Let $\rho_{E,\ell} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ be the ℓ-adic Galois representation attached to an elliptic curve $E/\mathbb{Q}$. Then,

- $\rho_{E,\ell}$ *is irreducible (hence, semi-simple).*
- $\rho_{E,\ell}$ *is unramified at primes $p \neq \ell$ of good reduction for E.*
- *For such good primes,*

$$\mathrm{Tr}(\rho_{E,\ell}(\mathrm{Frob}_p)) = a_p(E) := 1 + p - |\tilde{E}_p(\mathbb{F}_p)|; \quad (1)$$

$$\det(\rho_{E,\ell}(\mathrm{Frob}_p)) = p. \quad (2)$$

We prove a stronger theorem:

THEOREM

Let $E, E'/\mathbb{Q}$ be elliptic curves. Then, $|\tilde{E}_p(\mathbb{F}_p)| = |\tilde{E'}_p(\mathbb{F}_p)|$ for all primes p of good reduction for E and E' if and only if E and E' are isogenous.

Proof. If $|\tilde{E}_p(\mathbb{F}_p)| = |\tilde{E'}_p(\mathbb{F}_p)|$ for all primes p of good reduction for E and E', then

$$a_p(E) = a_p(E').$$

We prove a stronger theorem:

THEOREM

Let $E, E'/\mathbb{Q}$ be elliptic curves. Then, $|\tilde{E}_p(\mathbb{F}_p)| = |\tilde{E'}_p(\mathbb{F}_p)|$ for all primes p of good reduction for E and E' if and only if E and E' are isogenous.

Proof. If $|\tilde{E}_p(\mathbb{F}_p)| = |\tilde{E'}_p(\mathbb{F}_p)|$ for all primes p of good reduction for E and E', then

$$a_p(E) = a_p(E').$$

Since there are only finitely many bad primes, by the above mentioned *multiplicity one theorem for Galois representations*, we have

$$V_\ell(E) \cong V_\ell(E'),$$

as $\mathbb{Q}_\ell[G_\mathbb{Q}]$-modules.

We prove a stronger theorem:

THEOREM

Let $E, E'/\mathbb{Q}$ be elliptic curves. Then, $|\tilde{E}_p(\mathbb{F}_p)| = |\tilde{E}'_p(\mathbb{F}_p)|$ for all primes p of good reduction for E and E' if and only if E and E' are isogenous.

Proof. If $|\tilde{E}_p(\mathbb{F}_p)| = |\tilde{E}'_p(\mathbb{F}_p)|$ for all primes p of good reduction for E and E', then

$$a_p(E) = a_p(E').$$

Since there are only finitely many bad primes, by the above mentioned *multiplicity one theorem for Galois representations*, we have

$$V_\ell(E) \cong V_\ell(E'),$$

as $\mathbb{Q}_\ell[G_\mathbb{Q}]$-modules. The theorem then follows from the following result. □

THEOREM (FALTING'S ISOGENY THEOREM, [SIL09], THEOREM III.7.7)

Two elliptic curves over $\mathbb{Q}$ are isogenous iff they have isomorphic ℓ-adic Tate modules for some prime ℓ.

Table of Contents

Density of a set of primes

Let A be a set of primes in $\mathbb{Q}$. The (natural) **density** $\lambda(A)$ of A is the limit

$$\lim_{x\to\infty} \frac{\#\{p \in A \mid p \leq x\}}{\#\{p \leq x\}}, \text{ if it exists.}$$

Example

- If A is the set of primes in an AP $a + b\mathbb{Z}$, $\gcd(a, b) = 1$, then $\lambda(A) = 1/\phi(b)$.
- By an application of the Chebotarev density theorem (cf. [Ser81, §8]), we can prove that
$$\lambda(\{p \mid a_p(E)\}) = 0,$$
for elliptic curves without complex multiplication (i.e. $\mathrm{End}(E) = \mathbb{Z}$).
- (Bombieri) The set of primes ending with 1 doesn't have a natural density!

C. S. Rajan. "On strong multiplicity one for l-adic representations". In: *Internat. Math. Res. Notices* 3 (1998), pp. 161–172 proved the following result as a consequence of his **strong multiplicity theorem for Galois representations** with nice image (loc. cit. Theorem 2).

THEOREM (RAJAN, LEVEL 1 CASE)

Let $f(z) = \sum_{n\geq 1} a_f(n)q^n \in S(k_1, \mathrm{SL}_2(\mathbb{Z}))$ and $g(z) = \sum_{n\geq 1} a_g(n)q^n \in S(k_2, \mathrm{SL}_2(\mathbb{Z}))$ be Hecke eigenforms of level 1. If the density of primes p such that

$$a_f(p) = a_g(p)$$

is positive, then $f = g$.

M. Ram Murty and Sudhir Pujahari. “Distinguishing Hecke eigenforms”. In: *Proc. Amer. Math. Soc.* 145.5 (2017), pp. 1899–1904 proved the following theorem using analytical methods.

THEOREM (A STRONG MULTIPLICITY FOR LEVEL 1)

Let $f(z) = \sum_{n\geq 1} a_f(n)q^n \in S(k_1, \mathrm{SL}_2(\mathbb{Z}))$ and $g(z) = \sum_{n\geq 1} a_g(n)q^n \in S(k_2, \mathrm{SL}_2(\mathbb{Z}))$ be Hecke eigenforms of level 1. If the density of primes p such that

$$\frac{a_f(p)}{p^{k_1}} = \frac{a_g(p)}{p^{k_2}}$$

is positive, then $f = g$.

M. Ram Murty and Sudhir Pujahari. "Distinguishing Hecke eigenforms". In: *Proc. Amer. Math. Soc.* 145.5 (2017), pp. 1899–1904 proved the following theorem using analytical methods.

THEOREM (A STRONG MULTIPLICITY FOR LEVEL 1)

Let $f(z) = \sum_{n\geq 1} a_f(n)q^n \in S(k_1, \mathrm{SL}_2(\mathbb{Z}))$ and $g(z) = \sum_{n\geq 1} a_g(n)q^n \in S(k_2, \mathrm{SL}_2(\mathbb{Z}))$ be Hecke eigenforms of level 1. If the density of primes p such that

$$\frac{a_f(p)}{p^{k_1}} = \frac{a_g(p)}{p^{k_2}}$$

is positive, then $f = g$.

Soon after, Vijay M. Patankar and C. S. Rajan. "Distinguishing Galois representations by their normalized traces". In: *J. Number Theory* 178 (2017), pp. 118–125 proved the above theorem as a consequence of their generalization of Rajan's strong multiplicity for Galois representations with nice image.

THANK YOU

REFERENCES

[AL70] A. O. L. Atkin and J. Lehner. "Hecke operators on $\Gamma_0(m)$". In: *Math. Ann.* 185 (1970), pp. 134–160.

[MP17] M. Ram Murty and Sudhir Pujahari. "Distinguishing Hecke eigenforms". In: *Proc. Amer. Math. Soc.* 145.5 (2017), pp. 1899–1904.

[PR17] Vijay M. Patankar and C. S. Rajan. "Distinguishing Galois representations by their normalized traces". In: *J. Number Theory* 178 (2017), pp. 118–125.

[Raj98] C. S. Rajan. "On strong multiplicity one for l-adic representations". In: *Internat. Math. Res. Notices* 3 (1998), pp. 161–172.

[Ser81] Jean-Pierre Serre. "Quelques applications du théorème de densité de Chebotarev". In: *Inst. Hautes Études Sci. Publ. Math.* 54 (1981), pp. 323–401.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513.