Modular Galois Represemtations

Manal Alzahrani

November 9, 2015

Contents

1 Introduction: Last Formulation of QA

Recall that the goal of Weinstein's paper was to find the solution to the following simple equation:

QA: Let $f(x) \in \mathbb{Z}[x]$ irreducible. Is there a "rule" which determine whether $f(x)$ split modulo p, for any prime $p \in \mathbb{Z}$?

This question can be reformulated using algebraic number theory, since there is a relation between the splitting of $f_p(x) \cong f(x)(\text{mod } p)$ and the splitting of p in $L = \mathbb{Q}(\alpha)$, where α is a root of $f(x)$. Therefore, we can ask the following question instead:

QB: Let $L/\mathbb{Q}$ a number field. Is there a "rule" determining when a prime in $\mathbb{Q}$ split in L?

Let $L'/\mathbb{Q}$ be a Galois closure of $L/\mathbb{Q}$. Since a prime in $\mathbb{Q}$ split in L if and only if it splits in L', then to answer **QB** we can assume that $L/\mathbb{Q}$ is Galois.

Recall that if $p \in \mathbb{Z}$ is a prime, and $\mathcal{P}$ is a maximal ideal of $\mathcal{O}_L$, then a Frobenius element of $\mathrm{Gal}(L/\mathbb{Q})$ is any element of $\mathrm{Frob}_{\mathcal{P}}$ satisfying the following condition,

$$x^{\mathrm{Frob}_{\mathcal{P}}} \equiv x^p (\mathrm{mod}\ \mathcal{P}),\ \forall x \in \mathcal{O}_L.$$

If p is unramifed in L, then $\mathrm{Frob}_{\mathcal{P}}$ element is unique. Furthermore,

$$p \text{ split in } \ L \iff \mathrm{Frob}_{\mathcal{P}} = 1 \text{ in } \mathrm{Gal}(L/\mathbb{Q}).$$

To to find another formulation of **QB**, we will use Galois representations. Let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$, recall the following:

1.1 Absolute Galois Group of $\mathbb{Q}$:

The absolute Galois group of $\mathbb{Q}$ is the group of automorphisms of $\overline{\mathbb{Q}}$, denoted by,

$$G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),$$

since $\overline{\mathbb{Q}}$ is the union of all Galois number fields $F \subseteq \overline{\mathbb{Q}}$, then

$$\forall \sigma \in G_{\mathbb{Q}} \Longrightarrow \sigma|_F \in \mathrm{Gal}(F/\mathbb{Q}),$$

these restrictions are compatible, i.e.

$$\sigma_F = \sigma_{F'}|_F \text{ if } F \subset F'.$$

Conversely, every compatible system of automorphism $\{\sigma_F\}$ over all Galois number fields F defines an automorphism of $\overline{\mathbb{Q}}$. Therefore,

$$G_{\mathbb{Q}} = \varprojlim_{F} \mathrm{Gal}(F/\mathbb{Q}).$$

1.2 Absolute Frobenius Element over $p \in \mathbb{Q}$:

For a prime $p \in \mathbb{Z}$, let

$$\begin{aligned}\mathcal{P} \subseteq \overline{\mathbb{Z}} &= \{\alpha \in \overline{\mathbb{Q}} : \exists f \in \mathbb{Z}[x] \text{ monic s.t. } f(\alpha) = 0\}\\ &= \bigcup_K \mathcal{O}_K\\ &= \text{The ring of algebraic integers,}\end{aligned}$$

be a maximal ideal over p, i.e. $\mathcal{P}|p\overline{\mathbb{Z}}$.

The *Decomposition group of* $\mathcal{P}$ is

$$D_{\mathcal{P}} = \{\sigma \in G_{\mathbb{Q}} : \mathcal{P}^{\sigma} = \mathcal{P}\},$$

thus each $\sigma \in D_{\mathcal{P}}$ acts on $\overline{\mathbb{Z}}/\mathcal{P}$, as

$$(x + \mathcal{P})^{\sigma} = x^{\sigma} + \mathcal{P},$$

which can be viewed as an action on $\overline{\mathbb{F}}_p$, since $\overline{\mathbb{Z}}/\mathcal{P} \hookrightarrow \overline{\mathbb{F}}_p$.

Let $G_{\mathbb{F}_p} = \mathrm{Aut}(\overline{\mathbb{F}_p})$ denote the absolute Galois group of $\mathbb{F}_p$, then we have the following surjective reduction map,

$$D_{\mathcal{P}} \to G_{\mathbb{F}_p}.$$

Let $\sigma_p \in G_{\mathbb{F}_p}$ be the Frobenius automorphism on $\overline{\mathbb{F}}_p$, which $x \mapsto x^p$ for all $x \in \overline{\mathbb{F}}_p$.

An *absolute Frobenius element over* p is any preimage of the Frobenius automorphism $\sigma_p \in G_{\mathbb{F}_p}$, denoted by $\mathrm{Frob}_{\mathcal{P}}$. It is defined up to the kernel of the reduction map, which is called the *inertia group of* $\mathcal{P}$:

$$I_{\mathcal{P}} = \{\sigma \in D_{\mathcal{P}} : x^{\sigma} \equiv x \pmod{\mathcal{P}} \ \forall x \in \overline{\mathbb{Z}}\}.$$

It has the following properties:

- For each Galois number field F, the restriction map

$$G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q}),$$

  takes an absolute Frobenius element to a corresponding Frobenius element over F,

$$\mathrm{Frob}_{\mathcal{P}}|_F = \mathrm{Frob}_{\mathcal{P}_F},$$

  where $\mathcal{P}_F = \mathcal{P} \cap F$.

- Since all maximal ideals of $\overline{\mathbb{Z}}$ over p are conjugate to $\mathcal{P}$, we have that

$$\mathrm{Frob}_{\mathcal{P}^{\sigma}} = \sigma^{-1}\mathrm{Frob}_{\mathcal{P}}\ \sigma,\ \ \sigma \in G_{\mathbb{Q}}.$$

1.3 Galois Representations :

A Galois representation ρ is a continuous homomorphism

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_n(K),$$

where K is a topological field.

We want to know the values of $\rho(\sigma)$ for $\sigma \in G_{\mathbb{Q}}$. In particular, we want to evaluate ρ at the absolute Frobenius element:

- The notation $\rho(\mathrm{Frob}_{\mathcal{P}})$ is well defined if and only if $I_{\mathcal{P}} \subset \mathrm{Ker}\rho$, since $\mathrm{Frob}_{\mathcal{P}}$ is defined up to $I_{\mathcal{P}}$.

- If $\mathcal{P}, \mathcal{P}'$ lie over p, then there exists some $\sigma \in G_{\mathbb{Q}}$ such that

$$\mathcal{P}' = \mathcal{P}^{\sigma}$$
$$\Rightarrow I_{\mathcal{P}'} = \sigma^{-1} I_{\mathcal{P}} \sigma.$$

  So, if $I_{\mathcal{P}} \subset \mathrm{Ker}\rho$, then $I_{\mathcal{P}'} \subset \mathrm{Ker}\rho$. Therefore,

$$\rho(\mathrm{Frob}_{\mathcal{P}'}) = \rho(\sigma^{-1}\mathrm{Frob}_{\mathcal{P}}\ \sigma) = \rho^{-1}(\sigma)\rho(\mathrm{Frob}_{\mathcal{P}})\rho(\sigma).$$

  So, the primes lying over p define a conjugacy class in $GL_n(K)$. Since all elements in this conjugacy class have the same characteristic polynomial, we see that the characteristic polynomial only depend on p.

Definition 1.1. ρ is *unramfied* at a p if $I_{\mathcal{P}} \subset \mathrm{Ker}\rho$ for any maximal ideal $\mathcal{P} \subset \overline{\mathbb{Z}}$ lying over p.

Definition 1.2. Two representations ρ, ρ' are said to be *equivalent* if there exists $M \in GL_n(K)$ such that

$$\rho'(\sigma) = M^{-1}\rho(\sigma)M,\ \forall \sigma \in G_{\mathbb{Q}}.$$

Definition 1.3. Let $c \in G_{\mathbb{Q}}$ be complex conjugation then ρ is said to be *odd* if $\det(\rho(c)) = -1$, and *even* if $\det(\rho(c)) = 1$.

Let V be an n dimensional vector space over K, then $GL_n(K) = GL(V)$.

Definition 1.4. A representation ρ is said to be *irreducible* if V is not zero and if no vector subspace is stable under $G_{\mathbb{Q}}$ except 0 and V.

Now, after defining Galois representations we want to try to find a solution to the following question:

QC: Given a Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_n(K),$$

is there a "rule" for determining the conjugacy class of $\rho(\mathrm{Frob}_{\mathcal{P}})$ when p is unramfied?

2 Modular Galois Representation

The following theorem, Theorem 4.4.1 in Weinstein's paper, is a construction due to Deligne and Serre, which associate a 2- dimensional Galois representation with modular forms.

Theorem 2.1. *Let $g(\tau) = \sum_{n\geq 1} a_n(g)q^n$ be a cuspidal eigenform of weight k, level N, and character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, normalized so that $a_1 = 1$.*
Let F be a number field containing $a_n(g)$ and the values of χ.

- *Suppose $k \geq 2$. Then for all primes $\mathcal{P}$ of F there exists an odd irreducible Galois representation*

  $$\rho_{g,\mathcal{P}} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(F_p)$$

  where F_p is the completion of F with respect to the $p-adic$ absolute value, such that for all ℓ prime to N and $\mathcal{P}$, $\rho_{g,\mathcal{P}}$ is unramfied at ℓ and the characteristic polynomial of $\rho_{g,\mathcal{P}}(Frob_\ell)$ is

  $$x^2 - a_\ell(g)x + \chi(\ell)\ell^{k-1}.$$

- *Suppose $k = 1$. Then there exists an odd irreducible Galois representation*

  $$\rho_g : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{C}),$$

  such that for all ℓ prime to N, ρ_g is unramfied at ℓ, and the characteristic polynomial of $\rho_g(Frob_\ell)$ is

  $$x^2 - a_\ell(g)x + \chi(\ell).$$

We call an odd, irreducible, 2-dimensional Galois representation associated to a cuspidal eigenform *Modular*, if it arises in the way described in Theorem 2.1.

Note that for any modular Galois representation the characteristic polynomial is a "rule" determining the conjugacy class of $\rho(\mathrm{Frob}_p)$ unramfied at p.

Therefore, for modular Galois representation we have an answer to **QC**.

3 Modular Galois Representations and FLT

The question of which Galois representations are modular is closely related to Fermat's Last Theorem.

Theorem 3.1 (Fermat's Last Theorem). *$x^n + y^n = z^n$ has no nontrivial integer solutions when $n > 3$.*

It can be reduced to the case $n = p$, p prime such that $p \geq 5$.

To see this link, we will be interested in Galois representations coming from geometry. Recall the following:

Let $E : y^2 = f(x)$ be an elliptic curve such that $f(x) \in \mathbb{Q}[x]$, and take $m \geq 2$.

Definition 3.1. The *m-torsion subgroup of E*, is

$$E[m] = \{P \in E : [m]P = 0\}.$$

Proposition 3.1. *If $m \neq 0$, $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.*

Since $G_{\mathbb{Q}}$ acts on $E[m]$, we have the following representation

$$G_{\mathbb{Q}} \to Aut(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z})$$

Definition 3.2. Let $p \in \mathbb{Z}$. The p-adic *Tate module* of E is the group

$$T_p(E) = \varprojlim_n E[p^n],$$

where the inverse limit taken with respect to the natural maps

$$E[p^{n+1}] \xrightarrow{[p]} E[p^n].$$

Proposition 3.2. *As a $\mathbb{Z}_p$-module, the Tate module has the following structure:*

$$T_p(E) \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

The p-adic representation of $G_{\mathbb{Q}}$ associated to E is the homomorphism

$$\rho_{p,E} : G_{\mathbb{Q}} \to \mathrm{Aut}(T_p(E)) \cong GL_2(\mathbb{Z}_p) \subseteq GL_2(\mathbb{Q}_p),$$

induced by the action of $G_{\mathbb{Q}}$ on the p^n-torsion points.

Therefore, we obtained a 2-dimensional representation of $G_{\mathbb{Q}}$ over a field of characteristic zero.

Also, recall that $\rho_{p,E}$ is unrammfied at primes ℓ such that $\ell \nmid p\triangle$, where $\triangle$ =discriminant of $f(x)$, and for such ℓ the characteristic polynomial of $\rho_{p,E}(\mathrm{Frob}_\ell)$ is:

$$\det(xI - \rho_{p,E}(\mathrm{Frob}_\ell)) = x^2 - (\ell + 1 - N_\ell)x + \ell, \tag{1}$$

where N_ℓ is the number of points of E with coordinates in the finite field $\mathbb{F}_\ell$.

Definition 3.3. We say E *is modular* if the Galois representation $\rho_{p,E}$ is modular.

Therefore, from Theorem 2.1, E is modular if there exist a cuspidal eigenform g of weight k and character χ, such that for almost all primes ℓ the characteristic polynomial of Frob_ℓ is

$$x^2 - a_\ell(g)x + \chi(\ell)\ell^{k-1}, \tag{2}$$

comparing (1) with (2), we say E is modular if there exists a cuspidal eigenform of weight 2 and trivial character χ, such that for almost all primes, the number of points on E with coordinates in $\mathbb{F}_\ell$ is $\ell + 1 - a_\ell(g)$.

Now, what does this have to do with FLT ?

Take $E : y^2 = x(x-A)(x-B)$ such that $A, B \in \mathbb{Z}$ and $(A, B) = 1$, then E is semistable.[1]

Proposition 3.3. *Assume that E is modular and $p|AB(A-B) = \triangle_E$ exactly with a power divisible by p i.e. $p^{np} \parallel AB(A-B)$. Then, $\rho_{E,p}$ is modular of level* $N = 2 \prod_{\substack{\ell | AB(A-B) \\ \ell \text{ prime} \\ \ell^m \| AB(A-B) \text{ s.t. } p \nmid m}} \ell.$

Now, take $A = x^p, B = -y^p$. Assume $A - B = x^p + y^p = z^p$. Then if E is modular and $p^{np} \parallel -x^p y^p z^p = -(xyz)^p$ for some n, then $\rho_{E,p}$ is modular of level

$$N = 2 \prod_{\substack{\ell | -(xyz)^p \\ \ell^n \| -(xyz)^p \text{ s.t. } p \nmid n}} \ell = 2 \times 1,$$

[1] we say that E is semistable at all p if $f(x) \equiv f_p(x) (\mathrm{mod} p)$ has at least two different roots module p.

which means that $\rho_{E,p}$ is modular of level 2, but since there are no nontrivial cusp forms of weight 2 and level 2, we get a contradiction.

So we showed that if there exists a nontrivial solution of $x^p + y^p = z^p$, then E is not modular.

It has been proven that

Theorem 3.2 (The Shimura-Taniyama-Weil Conjecture)**.** *Every elliptic curve defined over the rational numbers is modular.*

which implies Fermat's claim.

4 Modular Artin Representations

In the previous section, we saw that the Tate module of an elliptic curve gives an example of 2-dimensional modular p-adic Galois representation which was associated with a cuspidal eigenform of weight 2.

In this section, we discuss the case of 2-dimensional Artin representations, i.e.

$$\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{C}).$$

Conjecture. *Let $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ be an odd irreducible Galois representation. Then, ρ is equivalent to ρ_g for some cuspidal eignform g of weight 1.*

where ρ_g is the Artin representation associated to g by the Deligne and Serre construction.

This construction is the two dimensional case of Artin conjecture, which can be stated for all dimensions in terms of the analytic continuation of an L-function attached to ρ.

A large part of the conjecture was proved by Langlands and was extended by Tunnel. They proved the following:

Theorem 4.1. *$\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ odd irreducible Galois representations such that $\rho(G_{\mathbb{Q}})$ is solvable.* [2] *Then ρ is equivalent to ρ_g for some cuspidal eigenform g of weight 1.*

Since an Artin representation has a finite image, $\rho(G_{\mathbb{Q}})$ can be classified by its projective image, which is a finite subgroup in the projective general linear group $PGL_2(\mathbb{C}) \cong GL_2(\mathbb{C})/\{\text{nonzero scalar matrices}\}$.

[2] A group G is solvable if there is a chain

$$G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_s = G$$

such that G_{i+1}/G_i is abelian.

Theorem 4.2. *If H is a finite subgroup of $PGL_2(\mathbb{C})$, then H is isomorphic to one of the following groups:*

- *the cyclic group C_n of order n, $n > 0$.*
- *the dihedral group D_{2n} of order $2n$, $n > 1$.*
- *terahedral A_4.*
- *octahedral S_4.*
- *icosahedral A_5.*

Therefore, the only excluded case in the previous theorem is when the projective image of $\rho(G_{\mathbb{Q}})$ is isomorphic to A_5, which was proven later by Khare and Wintenberger. As a result, the 2-dimensional Artin conjecture was proven for all cases.

If the projective image of $\rho(G_{\mathbb{Q}})$ is dihedral, then the required eigen form g is a theta function, which is similar to the one appearing in Example 3.14 and Example 3.4.2 of Weinstein's paper :

for a polynomial $f(x) = x^4 - 2$, the splitting field of f over $\mathbb{Q}$ is $L = \mathbb{Q}(i, \sqrt[4]{2})$, and $\mathrm{Gal}(L/\mathbb{Q}) \cong D_8$ generated by:

$$\begin{aligned} r(\sqrt[4]{2}) &= i\sqrt[4]{2}, & \qquad s(\sqrt[4]{2}) &= \sqrt[4]{2} \\ r(i) &= i, & s(i) &= -i \end{aligned}$$

which satisfies the relations $r^4 = 1, s^2 = 1$ and $srs^{-1} = r^{-1}$.

The group D_8 has a 2-dimensional representation which sends:

$$r \longmapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$
$$s \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Therefore, we can construct a 2-dimensional Artin representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{C}),$$

which factors through $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$.

References

[1] Diamond, F., & Shurman, J. (2005). A first course in modular forms. New York: Springer.

[2] Silverman, J. (2009). The Arithmetic of Elliptic Curves (2nd ed.). New York: Springer-Verlag.

[3] Frey, G. (2009). The Way to the Proof of Fermat's Last Theorem. Ann. Fac. Sci. Toulouse Math, 18(S2), 5-23. http://dx.doi.org/10.5802/afst.1227.