Mod 5 icosahedral representations and a conjecture of Artin

Shu Sasaki

27th May 2011

Introduction

Let K be a number field. Let $\mathbb{A}_K$ denote the adele of K.

Let $\rho : G_K \to GL_n(\mathbb{C})$ be a n-dimensional continuous representation of the absoulte Galois group G_K of K. Let $L(\rho, s)$ be the (Artin) L-series

$$L(\rho, s) = \prod_v \det(1 - \rho^{I_v}(\mathrm{Frob}_v)(\mathbf{N}v)^{-s})^{-1}$$

in $s \in \mathbb{C}$ associated to ρ, where by ρ^{I_v} I mean the representation of G_v/I_v on the subspace of the inertia I_v invariants, $\mathbf{N}v = \#\mathcal{O}_K/v$, and Frob_v is the arithmetic Frobenius at v.

A theorem of Brauer asserts: $L(\rho, s)$ has meromorphic continuation to the whole of $\mathbb{C}$ (a piece of "group theory"; actually the Brauer's theorem is the genesis of "potential automorphy" by R.Taylor).

The Artin conjecture asserts: the L-series $L(\rho, s)$ has holomorphic continuation to $s \in \mathbb{C}$ except for a possible pole at $s = 1$.

If $\rho = \rho_1 + \rho_2$, $L(\rho, s) = L(\rho_1, s)L(\rho_2, s)$; so we may assume ρ is irreducible.

A conjecture of Langlands ("Langlands programme"), known more commonly as the *strong* Artin conjecture, predicts: there exists a cuspidal automorphic representation π of $GL_n(\mathbb{A}_K)$ such that $L(\rho, s) = L(\pi, s)$.

It is well-known that the strong Artin conjecture implies the Artin conjecture. As far as I know, D.Ramakrishnan wrote down a proof (an exercise in complex analysis).

If $n = 1$, this is the global class field theory: a canonical bijection between Hecke characters of $\mathbb{A}_K^\times$ (the "automorphic side") and Galois character (the "Galois side") of G_K.

If $n = 2$, let

$$\operatorname{proj}\rho : G_K \to GL_2(\mathbb{C}) \twoheadrightarrow PGL_2(\mathbb{C}) := GL_2(\mathbb{C})/\mathbb{C}^\times.$$

Then the image of $\operatorname{proj}\rho$ is either dihedral, tetrahedral (A_4), octahedral (S_4), or icosahedral (A_5).

The dihedral case is due to Artin himself. The tetrahedral case, and the octahedral case with $K = \mathbb{Q}$, ρ odd, is due to Langlands ("soluble base change"). Tunnell treats the octahedral case in general (still as a result of the soluble base change trick).

Except some computational evidence (Buhler, Frey, et al.), the icosahedral case was largely intractable (A_5 is not soluble)!

For brevity, I shall henceforth call a representation ρ icosahedral if the image of $\operatorname{proj} \rho$ is A_5.

If $n = 2$, K is a totally real field, and ρ is totally odd (i.e., the determinant of the image of complex conjugation with respect to every embedding of K into $\mathbb{R}$ is -1), then the strong Artin conjecture predicts: there exists a holomorphic cusp eigenform f over K such that $L(f, s) = L(\rho, s)$.

What about the "even" case? Well, this amounts to finding Maass forms...

AUTOMORPHIC TWO-DIMENSIONAL GALOIS REPRESENTATIONS

Let K be a totally real field. Let f be a holomorphic (Hilbert) cusp eigenform over K and $\pi(f)$ denote the cuspidal automorphic representation of $GL_2(\mathbb{A}_K)$ generated by f.

"$f \mapsto \pi(f) = \pi \mapsto \rho_\pi$" is established by

the regular weight case: Carayol ($[K : \mathbb{Q}]$ odd, or $[K : \mathbb{Q}]$ even and π is square-integrable at some finite place); Wiles (the ordinary case); Taylor ($[K : \mathbb{Q}]$ is even),

the parallel weight one case: Ragawski-Tunnell

the partial weight one case: Jarvis

In the following, when K is totally real, I will say "a (totally odd two-dimensional) p-adic/mod p representation ρ of G_K is modular".

By this, in characteristic zero, I will mean that there exists a holomorphic cusp eigenform f over K such that its associated Galois representation $\rho_f : G_K \to GL_2(L)$, where $L = \mathbb{Q}_p(\{a_{\mathfrak{n}}(f)\})$, is isomorphic to ρ.

In characteristic p, I shall mean that the semi-simplification (i.e., the direct sum of the Jordan-Holder constituents) of the reduction

$$\overline{\rho}_f : G_K \to GL_2(\mathcal{O}_L) \twoheadrightarrow GL_2(\mathcal{O}_L/\mathfrak{m}_L) \simeq GL_2(k_L)$$

of the "model" $G_K \to GL_2(\mathcal{O}_L)$ is isomorphic to ρ.

THE STRONG ARTIN CONJECTURE FOR ODD ICOSAHEDRAL REPRESENTATIONS

In 2001, Buzzard-Dickinson-Shepherd-Barron-Taylor "On icosahedral Artin representations" proved many new cases of the strong Artin conjecture for odd icosahedral $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$.

Which was followed by Taylor "On icosahedral Artin representations II", 2003.

These are based on Taylor's idea to "deduce" results about weight 1 forms from results about weight 2 forms, i.e., Wiles's idea about modularity of semi-stable elliptic curves over $\mathbb{Q}$.

More precisely,

(0) Fix an isomorphism $\mathbb{C} \simeq \overline{\mathbb{Q}}_p$ for *some* p. Let

$$\rho : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_L)$$

for a finite extension L of $\mathbb{Q}_p$, and let

$$\overline{\rho} : G_{\mathbb{Q}} \to GL_2(k_L)$$

be the "reduction mod p" of ρ.

(1) Prove that $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(k_L)$ is modular. This is commonly known as "Serre's conjecture for $\overline{\rho}$.

(2) Prove that $\overline{\rho}$ modular implies ρ modular. This, on the other hand, is known as Modular Lifting Theorem, or $R = T$.

(3) Combine (1) and (2) together, ρ is modular.

This is how Wiles proved an semistable elliptic curve over $\mathbb{Q}$ is modular when ρ is the Tate module $\rho_E : G_{\mathbb{Q}} \to GL(E(\overline{\mathbb{Q}}_p)[p^\infty]) \simeq GL_2(\mathbb{Z}_p)$.

(1) is given by "Langlands-Tunnell" with $p = 3$;

$$\overline{\rho}_{E,3} : G_{\mathbb{Q}} \to GL(E(\overline{\mathbb{Q}})[3]) \simeq GL_2(\mathbb{F}_3)$$

followed by an explicit homomorphism

$$GL_2(\mathbb{F}_3) \to GL_2(\mathbb{Z}(\sqrt{-2})) \subset GL_2(\mathbb{C})$$

is odd, irreducible, and soluble ($PGL_2(\mathbb{F}_3) \simeq S_4$). The composition is "modular" and therefore $\overline{\rho}_{E,3}$ is modular.

(2) is given by "$R = T$"; Wiles proves that, for *any* p, if $\overline{\rho}$ is a mod p representation $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$, which is modular and whose restriction to Gal$(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}))$ is absolutely irreducible, then

the set R of all deformations (*flat* at p) of $\overline{\rho}$

is isomorphic to

the set T of all deformations of $\overline{\rho}$ *arising from* (in the sense of Eichler-Shimura(-Deligne)) weight 2 cusp forms.

In particular, for p either 3 or 5, $\rho_E : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_p)$ associated to a semistable elliptic curve E over $\mathbb{Q}$ gives a $\mathbb{Z}_p$-valued point of Spec R, so it gives rises to a $\mathbb{Z}_p$-valued point of Spec T, hence ρ_E is modular.

Taylor's idea (1992) (for tackling the strong Artin conjecture in the icosahedral case) was to use this trick to prove modularity of odd icosahedral $\rho : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_L)$.

Slightly more precisely,

prove (2) that, given a p-adic representation

$$\rho : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_L)$$

whose *p-adic Hodge-Tate weights* are equal, and its $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(k_L)$ is modular, then ρ arises from a weight one form (which is much stronger than modularity of icosahedral ρ that we will need);

and prove (1) that odd icosahedral $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(k_L)$ is modular.

Results about modularity of mod p icosahedral representations of $G_{\mathbb{Q}}$.

Shepherd-Barron-Taylor (2001) If $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_4)$ is unramified at 3 and 5, then $\overline{\rho}$ is modular.

The theorem is, in fact, pre-Shimura-Taniyama (Breuil-Conrad-Diamond-Taylor). After S-T, the condition at 3 can be suppressed.

If $\overline{\rho}$ is unramifed at 2 and 5, and $\overline{\rho}(\mathrm{Frob}_2)$ has distinct eigenvalues, then $\overline{\rho}$ is modular.

Taylor (2003) If $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_5)$ is "I_3-distinguished" and "5-distinguished", then $\overline{\rho}$ is modular.

Of course,

Khare-Wintenberger (2009) Any odd, continuous, and irreducible $\overline{\rho}$ is modular (“Serre’s conjecture”).

However, if proj ρ is icosahedral, so is proj $\overline{\rho}$; and since only $PSL_2(\mathbb{F}_5)$ and $PSL_2(\mathbb{F}_4)$ are isomorphic to A_5, it would suffices to know modularity of $\overline{\rho}$ for $p = 2, 5$.

Results about MLTs.

Buzzard-Taylor (1999) For any odd p ($p = 2$ works if combined with Dickinson's "$R = T$ theorem") $\rho : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_L)$ arises from a weight one form if $\rho : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_L)$ is unramified at p, $\rho(\text{Frob}_p)$ has distinct eigenvalues, and $\overline{\rho}$ *is modular*.

Buzzard (2003) For any p, $\rho : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_L)$ arises from a weight one form if ρ is "potentially unramified at p" (i.e., $\rho(I_p)$ is finite), $\rho|_{G_p}$ is the direct sum of two characters of G_p which are distinct mod p, and $\overline{\rho}$ *is modular*.

Khare (1997) $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ arises from a weight one form if $\rho_p : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{Z}}_p) \subset GL_2(\overline{\mathbb{Q}}_p) \simeq GL_2(\mathbb{C})$, when reduced mod p, is modular for *many* p ("Serre" implies "Artin").

Me? Well, I can do a little better, and prove many new cases of the strong Artin conjecture for *totally odd* representations

$$\rho : G_F \to GL_2(\mathbb{C})$$

of the absolute Galois group G_F of a totally real field F.

Remark. It does not seem possible to generalise Khare-Wintenberger (while straightforward to check Khare's "Serre" $\Rightarrow$ "Artin" in the Hilbert case); and "Serre" + ("Serre" $\Rightarrow$ "Artin") to prove the strong Artin conjecture is probably not a good idea.

Theorem 1 *(S, 2010) Let F be a totally real field. Assume that* 5 *splits completely in F. Let $\rho : G_F \to GL_2(\mathbb{C})$ be a continuous, totally odd, and icosahedral representation of $G_F = \mathrm{Gal}(F^{\mathrm{alg}}/F)$.*

Suppose that, for every place $v|5$, the projective image of the decomposition group G_v has order 2 and the corresponding quadratic extension in F_v^{alg} of F_v is not $\mathbb{Q}_5(\sqrt{5})$.

Then the strong Artin conjecture for ρ holds.

Remark. Instead of the conditions above, I can prove the strong Artin conjecture assuming 2 splits completely in F (and slightly different condition at 2).

Remark. In fact, I can even do this for the totally ramified case...

Remark. And I have absolutely no idea how to remove the condition at 5.

Theorem 2 *(S, 2010) Let F be a totally real field. Suppose that a prime p is unramified in F. Let L be a finite extension of $\mathbb{Q}_p$ with maximal ideal $\mathfrak{m}_L$. Let $\rho : G_F \to GL_2(\mathcal{O}_L)$ be a representation of G_F which*

(1) ramifies at only finite many places of F;

(2) the restriction to $G_{F(\zeta_p)}$ of $\overline{\rho} = (\rho \bmod \mathfrak{m}_L)$ is absolutely irreducible and $\overline{\rho}$ arises from a Hilbert modular form;

(3) for any $v|p$, ρ is "nearly ordinary at v", i.e., the restriction $\rho|_{G_v}$ to the decomposition group G_v is of the form

$$\rho|_{G_v} \simeq \begin{pmatrix} \alpha_v & * \\ 0 & \beta_v \end{pmatrix}$$

such that

(3-1) $\alpha_v|_{I_v}$ and $\beta_v|_{I_v}$ are finite when restricted to the inertia group at v,

and

(3-2) $(\alpha_v \text{ mod } \mathfrak{m}_L) \neq (\beta_v \text{ mod } \mathfrak{m}_L)$.

Then there exists an overconvergent Hilbert modular form of weight 1 and the twist of its associated Galois representation is ρ.

In particular, if one furthermore assumes

(1) p *splits completely in* F

and

(2) ρ *is split at all* $v|p$, *i.e.,* $\rho|_{G_v}$ *is diagonalisable,*

then ρ *arises from a Hilbert modular form* f *of weight 1, and there exists an embedding* $\mathbb{Q}(\{a(\mathfrak{n}, f)\}) \hookrightarrow L$ *and, when followed by* any *embedding of* L *into* $\mathbb{C}$, *the strong Artin conjecture holds.*

So the part (2) is settled. How about (1)? Well, this is the part I'd like to talk to you about today.

Theorem 3 *(S, 2011) Let F be a totally real field. Assume that F is linearly disjoint from $\mathbb{Q}(\sqrt{5})$ (e.g. 5 is unramified in F). Let $\overline{\rho} : G_F \to GL_2(\overline{\mathbb{F}}_5)$ be a continuous and totally odd representation of G_F. Suppose that*

(1) $\overline{\rho}$ has projective image A_5;

(2) the projective image of the decomposition group G_v for every $v|5$ has order 2, and the quadratic extension of F_v corresponding to the projective image is not *$F_v(\sqrt{5})$.*

Then $\overline{\rho}$ is modular.

Proof.

"POTENTIALLY" LIFTING ICOSAHEDRAL REPRESENTATIONS

Find a totally real soluble extension F_1 of F such that $\overline{\rho}_1 := \overline{\rho}|_{G_{F_1}} : G_{F_1} \to GL_2(\mathbb{F}_5)$ has determinant the cyclotomic character.

So $\overline{\rho}_1$ "looks like" it arises from an elliptic curve.

To do this, observe that the obstruction for lifting $\overline{\rho} : G_F \to A_5 \simeq PSL_2(\mathbb{F}_5)$ to a *homomorphism* $G_F \to SL_2(\mathbb{F}_5)$ lies in $H^2(G_F, \{\pm 1\})$.

Since

$$H^2(G_F, \{\pm 1\}) \xrightarrow{\text{res}} \bigoplus_v H^2(G_{F_v}, \{\pm 1\}),$$

choose (by CFT) a bi-quadratic totally real extension F_1 of F in which the *finite* places v in F where the local obstructions are non-trivial, do *not* split completely.

At the infinite places, the local obstructions remain non-trivial.

On the other hand, the obstruction for lifting $G_F \to \{\pm 1\}$ to a character $G_{F(\sqrt{5})} \to \mathbb{F}_5^\times$ with square mod 5 cyclotomic character lies in $H^2(G_F, \{\pm 1\})$, and non-trivial exactly at the infinite places.

The obstructions for the two lifting problems (which are exactly at the infinite places) cancel out each other!

A MODULI SPACE OF MOTIVES

Let F_2 be the Galois closure over $\mathbb{Q}$ of an extension of F_1 in which $\sqrt{5}$ splits completely.

Find an elliptic curve E over a finite soluble extension F_2 of F_1 such that

(1) $\overline{\rho}_{E,3} : G_{F_2} \to GL(E[3]) \simeq GL_2(\mathbb{F}_3)$ is surjective;

(2) $\overline{\rho}_{E,3}|_{G_{F_2(\sqrt{-3})}}$ is absolutely irreducible

(3) E has (potentially) good ordinary reduction at every $v|5$

(4) $\overline{\rho}_{E,5} : G_{F_2} \to GL(E[5]) \simeq GL_2(\mathbb{F}_5)$ is isomorphic to $\overline{\rho}_2 := \overline{\rho}_1|_{G_{F_2}}$ (up to twist by a character).

To do this, consider a moduli space $Y_{\overline{\rho}_2}$ of elliptic curves over F_2 whose 5-torsions are isomorphic to $\overline{\rho}_2$. There are infinitely many F_2-rational points. Find a F_2-point of $Y_{\overline{\rho}_2}$

corresponding to an elliptic curve over F_2 which has (potentially) good ordinary reduction at every $v|5$. Then there *is* a F_2-point, which is close (for the 5-adic topology) to the point and which is *not* in the image (finite many points) of the F_2-points of $Y_{\overline{\rho}_2,0}(3) = \{(E,C)\}/\simeq$ *nor* in the image (finitely many points) of F_2-points of $Y_{\overline{\rho}_2,\mathrm{split}}(3) = \{(E,\{C,D\})\}/\simeq$.

POTENTIAL AUTOMORPHY

By Langlands-Tunnell, $E[3]$ is modular by (1). It follows from Kisin's MLT ($p = 3$), $\rho_{E,3}$ is modular (see (2)). By Falting's isogeny theorem, E is modular. In particular, $\overline{\rho}_{E,5}$ is modular and therefore, by (3), $\overline{\rho}_2$ is modular. By a generalisation of Taylor's argument in "Artin II", there is a lifting $\rho : G_F \to GL_2(\mathbb{Z}_5)$ of $\overline{\rho}$ such that $\rho|_{G_{F_2}}$ is a lifting of $\overline{\rho}_2$. By Skinner-Wiles ($p = 5$), $\rho|_{G_{F_2}}$ is modular. Since F_2 is a totally real soluble extension of F, by decent, ρ is modular. In which case $\overline{\rho}$ is modular. $\square$