SCHOLAR: Conference in honor of Ram Murty’s 60th birthday

From $p$-adic to Artin representations: a story in three vignettes

Henri Darmon

Montréal, October 15, 2013
Artin representations

Definition

An Artin representation is a continuous representation

\[ \varrho : G_\mathbb{Q} \rightarrow \text{GL}_n(\mathbb{C}), \quad G_\mathbb{Q} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}). \]

Artin $L$-function:

\[ L(\varrho, s) = \prod_\ell \det((1 - \sigma_\ell \ell^{-s})|_{V_\varrho \ell})^{-1}. \]

$\sigma_\ell =$ Frobenius element at $\ell$;

$V_\varrho =$ complex vector space realising $\varrho$;

$I_\ell =$ inertia group at $\ell$. 
The Artin conjecture

Conjecture

The $L$-function $L(\varrho, s)$ extends to a holomorphic function of $s \in \mathbb{C}$ (except for a possible pole at $s = 1$).

- One-dimensional representations factor through abelian quotients, and their study amounts to class field theory for $\mathbb{Q}$:

\[ L(\varrho, s) = L(\chi, s), \]

where $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ is a Dirichlet character.

- This talk will focus mainly on two-dimensional representations which are odd: $\varrho(\sigma_\infty)$ has eigenvalues 1 and $-1$. 
The role of Dirichlet characters in the study of odd two-dimensional Artin representations is played by *cusp forms of weight one*:

**Definition**

A cusp form of weight one, level $N$, and (odd) character $\chi$ is a holomorphic function $g : \mathcal{H} \rightarrow \mathbb{C}$ satisfying

$$g \left( \frac{az + b}{cz + d} \right) = \chi(d)(cz + d)g(z).$$

Such a cusp form has a *fourier expansion*:

$$g = \sum a_n(g)q^n, \quad q = e^{2\pi i z}.$$
The strong Artin conjecture

**Conjecture**

If $\varrho$ is an odd, irreducible, two-dimensional representation of $G_{\mathbb{Q}}$, there is a cusp form $g$ of weight one, level $N = \text{cond}(\varrho)$, and character $\chi = \text{det}(\varrho)$, satisfying

$$L(\varrho, s) = L(g, s).$$

$L(g, s) = \sum_n a_n(g) n^{-s}$

is the *Hecke $L$-function* attached to $g$. 
Theorem (Deligne-Serre)

Let \( g \) be a weight one eigenform. There is an odd two-dimensional Artin representation

\[ \varrho_g : G_{\mathbb{Q}} \longrightarrow \text{GL}_2(\mathbb{C}) \]

satisfying

\[ L(\varrho_g, s) = L(g, s). \]
The first step of the proof relies crucially on congruences between modular forms:

**Proposition**: For each prime $\ell$, there exists an eigenform $g_\ell \in S_\ell(N, \chi)$ of weight $\ell$ satisfying

$$g \equiv g_\ell \pmod{\ell}.$$ 

Idea:

- Multiply $g$ by the Eisenstein series $E_{\ell-1}$ of weight $\ell - 1$, to obtain a mod $\ell$ eigenform with the right fourier coefficients;

- lift this mod $\ell$ eigenform to an eigenform with coefficients in $\bar{\mathbb{Q}}$. 
First vignette, cont’d: étale cohomology

It was already known, thanks to Deligne, how to associate Galois representations to eigenforms of weight $\ell \geq 2$: they occur in the étale cohomology of certain Kuga-Sato varieties.

$E :=$ universal elliptic curve over $X_1(N)$;

$W_\ell(N) = E \times X_1(N) \cdots \times X_1(N) E$ (\(\ell - 2\) times);

$V_{g_\ell} := H^{\ell-1}_{et}(W_\ell(N)\bar{\mathbb{Q}}, \mathbb{Q}_\ell)[g_\ell].$

**Conclusion:** For each $\ell$ there exists a mod $\ell$ representation

$\varrho_\ell : G_\mathbb{Q} \longrightarrow \text{GL}_2(\bar{\mathbb{F}}_\ell)$

satisfying

$\text{trace}(\varrho_\ell(\sigma_p)) = a_p(g) \pmod{\ell}, \quad \text{for all } p \nmid N\ell.$
Using \textit{a priori} estimates on the size of \( a_p(g) \), and some group theory, the size of the image of \( \varrho_\ell \) is \textit{bounded independently of} \( \ell \).

Hence the \( \varrho_\ell \)'s can be pieced together into a \( \varrho \) with finite image and values in \( \text{GL}_2(\mathbb{C}) \).
Note the key role played in this proof by:

- Congruences between weight one forms and modular forms of higher weights;

- Geometric structures — Kuga-Sato varieties, and their associated étale cohomology groups — which allow the construction of associated $\ell$-adic Galois representations.
Second vignette: the Strong Artin Conjecture

Theorem

Let \( \varrho \) be an odd, irreducible, two-dimensional Artin representation. There exists an eigen-cuspform \( g \) of weight one satisfying

\[
L(g, s) = L(\varrho, s).
\]

- This theorem is now completely proved, over \( \mathbb{Q} \), thanks to the proof of the Serre conjectures by Khare and Wintenberger.

- Prior to that, significant progress on the conjecture was achieved based on a program of Taylor building on the fundamental modularity lifting theorems of Wiles.

- The “second vignette” is concerned with the broad outline of Taylor’s approach.
Scond vignette: Classification of Artin representations

By projective image, in order of increasing arithmetic complexity:

A. Reducible representations (sums of Dirichlet characters).

B. Dihedral, induced from an imaginary quadratic field.

C. Dihedral, induced from a real quadratic field.

D. Tetrahedral case: projective image $A_4$.

E. Octahedral case: projective image $S_4$.

F. Icosahedral case: projective image $A_5$. 
Second vignette: the status of the Artin conjecture

Cases A-C date back to Hecke, while D and E can be handled via techniques based on *solvable base change*.

The interesting case is the icosahedral case, where \( \varrho \) has projective image \( A_5 \).

**Technical hypotheses**: Assume \( \varrho \) is unramified at 2, 3 and 5, and that \( \varrho(\sigma_2) \) has distinct eigenvalues.
Theorem

There exists a principally polarised abelian surface $A$ with $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] \hookrightarrow \text{End}(A)$ such that

- $A[2] \simeq \overline{V}_q$ as $G_{\mathbb{Q}}$-modules;
Second vignette: the propagation of modularity

**Langlands-Tunnel**: $E[3]$ is modular.

**Wiles’ modularity lifting, at 3**: $T_3(E) := \lim_{\leftarrow, n} E[3^n]$ is modular.

Hence $E$ is modular, hence $E[5] = A[\sqrt{5}]$ is as well.

**Modularity lifting, at $\sqrt{5}$**: $T_{\sqrt{5}}(A)$ is modular.

Hence $A$ is modular, hence so is $A[2] = \overline{V_\rho}$.

**Modularity lifting, at 2**: The representation $\rho$ is 2-adically modular, i.e., it corresponds to a 2-adic overconvergent modular form of weight one.
The theory of companion forms produces two distinct overconvergent 2-adic modular forms attached to $\varrho$. (Using the distinctness of the eigenvalues of $\varrho(\sigma_2)$.)

Buzzard-Taylor. A suitable linear combination of these forms can be extended to a classical form of weight one. (A key hypothesis on $\varrho$ that is exploited is the triviality of $\varrho(I_2)$.)

This beautiful strategy has recently been extended to totally real fields by Kassaei, Sasaki, Tian, ...
A dominant theme in both vignettes is the rich interplay between Artin representations and ℓ-adic and mod ℓ representations, via congruences between the associated modular forms, (of weight one, and weight ≥ 2, where the geometric arsenal of étale cohomology becomes available.)
Third vignette: the Birch and Swinnerton-Dyer conjecture

Let $E$ be an elliptic curve over $\mathbb{Q}$. Hasse-Weil-Artin $L$-series

$$L(E, \varrho, s) = L(V_p(E) \otimes V_\varrho, s).$$

**Conjecture (BSD)**

The $L$-series $L(E, \varrho, s)$ extends to an entire function of $s$ and

$$\text{ord}_{s=1} L(E, \varrho, s) = r(E, \varrho) := \dim_\mathbb{C} E(\overline{\mathbb{Q}})^{\varrho},$$

where

$$E(\overline{\mathbb{Q}})^{\varrho} = \text{hom}_{G_{\mathbb{Q}}}(V_{\varrho}, E(\overline{\mathbb{Q}}) \otimes \mathbb{C}).$$

**Remark:** $r(E, \varrho)$ is the multiplicity with which the Artin representation $V_\varrho$ appears in the Mordell-Weil group of $E$ over the field cut out by $\varrho$. 
A special case of the equivariant BSD conjecture is

Conjecture

\[ \text{If } L(E, \varrho, 1) \neq 0, \text{ then } r(E, \varrho) = 0. \]

- If \( \varrho \) is a quadratic character, it follows from the work of Gross-Zagier-Kolyvagin, combined with a non-vanishing result on \( L \)-series due to Bump-Friedberg Hoffstein and Murty-Murty.

- If \( \varrho \) is one-dimensional, it follows from the work of Kato.

- If \( \varrho \) is induced from a non-quadratic ring class character of an imaginary quadratic field, it follows from work of Bertolini, D., Longo, Nekovar, Rotger, Seveso, Vigni, Zhang,... building on the fundamental breakthroughs of Gross-Zagier and Kolyvagin.
Assume that

- $\varrho = \varrho_1 \otimes \varrho_2$, where $\varrho_1$ and $\varrho_2$ are odd irreducible Artin representations of dimension two.

- The conductors of $E$ and $\varrho$ are relatively prime.

- $\det(\varrho_1) = \det(\varrho_2)^{-1}$, and hence in particular $\varrho$ is self-dual.

**Theorem (D, Victor Rotger)**

*If $L(E, \varrho, 1) \neq 0$, then $r(E, \varrho) = 0$.***
The Mordell-Weil group injects into a global Galois cohomology group

\[ E(\overline{\mathbb{Q}})^{\rho} \longrightarrow H_f^1(\mathbb{Q}, V_p(E) \otimes V_{\rho}). \]

**Local and global duality, and the Poitou-Tate sequence:** In order to bound \( r(E, \varrho) \), it *suffices* to show that the natural map

\[ H^1(\mathbb{Q}, V_p(E) \otimes V_{\rho}) \longrightarrow \frac{H^1(\mathbb{Q}_p, V_p(E) \otimes V_{\rho})}{H_f^1(\mathbb{Q}_p, V_p(E) \otimes V_{\rho})} \]

is *surjective*.

Thus the problem of bounding \( E(\overline{\mathbb{Q}})^{\rho} \) translates into the problem of constructing global cohomology classes with “sufficiently singular” local behaviour at \( p \).
Third vignette: modularity

Thanks to the modularity results alluded to in the first two vignettes, one can associate to \((E, \varrho_1, \varrho_2)\):

- An eigenform \(f\) of weight two, with \(L(f, s) = L(E, s)\).
- Eigenforms \(g\) and \(h\) of weight one, with \(L(g, s) = L(\varrho_1, s)\) and \(L(h, s) = L(\varrho_2, s)\).
- We then have an identification

\[
L(E, \varrho_1 \otimes \varrho_2, s) = L(f \otimes g \otimes h, s)
\]

of the Hasse-Weil-Artin \(L\)-function with the Garret-Rankin triple product \(L\)-function attached to \((f, g, h)\).
Third vignette: the theme of $p$-adic variation

**Theorem (Hida)**

There exist Hida families

$$g = \sum_n a_n(g, k)q^n, \quad h = \sum_n a_n(h, k)q^n,$$

of modular forms, specialising to $g$ and $h$ in weight one.

The Fourier coefficients $a_n(g, k)$ and $a_n(h, k)$ are rigid analytic functions on weight space $\mathcal{W} := \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$.

For each integer $k \geq 2$, we obtain a pair $(g_k, h_k)$ of classical forms of higher weight $k$. These converge to $(g, h)$ $p$-adically as $k \to 1$ in $\mathcal{W}$. 
Third vignette: generalised diagonal cycles

When \( k \geq 2 \), we can construct classes

\[
\kappa(f, g_k, h_k) \in H^1(\mathbb{Q}, V_p(E) \otimes V_p(g_k) \otimes V_p(h_k)(k - 1))
\]

from the images of \textit{generalised Gross-Kudla-Schoen cycles} in

\[
\text{CH}^k(X_0(N) \times W_k(N) \times W_k(N))_0.
\]

\textit{p-adic étale Abel-Jacobi map:}

\[
\text{CH}^k(X_0(N) \times W_k(N) \times W_k(N))_0
\]
\[
\rightarrow H^1(\mathbb{Q}, H^{2k-1}_{et}(X_0(N) \times W_k(N) \times W_k(N))_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)(k))
\]
\[
\rightarrow H^1(\mathbb{Q}, H^1_{et}(X_0(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)(1) \otimes H^{k-1}_{et}(W_k(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p) \otimes^2 (k - 1))
\]
\[
\rightarrow H^1(\mathbb{Q}, V_p(E) \otimes V_p(g_k) \otimes V_p(h_k)(k - 1)).
\]
The technical heart of the proof has two parts:

- The classes $\kappa(f, g_k, h_k)$ interpolate to a $p$-adic analytic family of cohomology classes, as $k$ varies over $W$. In particular, we can consider the $p$-adic limit

$$\kappa(f, g, h) := \lim_{k \to 1} \kappa(f, g_k, h_k).$$

**Theorem (Reciprocity law)**

The class $\kappa (f, g, h)$ is non-cristalline, i.e., has non-zero image in

$$\frac{H^1(Q_p, V_p(E) \otimes V_\varphi)}{H^1_f(Q_p, V_p(E) \otimes V_\varphi)}$$

if and only if $L(E, \varphi, 1) \neq 0$. 
Application to ring class fields of real quadratic fields

Of special interest is the case where \( V_{\varrho_1} \) and \( V_{\varrho_2} \) are induced from finite order characters \( \chi_1 \) and \( \chi_2 \) (of mixed signature) of the same real quadratic field \( K \):

\[
V_{\varrho_1} \otimes V_{\varrho_2} = \text{Ind}_K^Q(\psi) \oplus \text{Ind}_K^Q(\tilde{\psi}), \quad \psi = \chi_1\chi_2, \quad \tilde{\psi} = \chi_1\chi'_2.
\]

The characters \( \psi \) and \( \tilde{\psi} \) are ring class characters of \( K \).

Theorem

Assume that \((E, K)\) satisfies the analytic non-vanishing condition of the next slide. Then, for all ring class characters \( \psi : \text{Gal}(H/K) \to \mathbb{C}^\times \) of \( K \) of conductor prime to \( N_E \),

\[
L(E/K, \psi, 1) \neq 0 \Rightarrow (E(H) \otimes \mathbb{C})\psi = 0.
\]
Given an elliptic curve $E/\mathbb{Q}$ and a (real) quadratic field $K$, the non-vanishing condition is:

**Non-vanishing condition**: There exist even and odd quadratic twists $E'$ of $E$ such that

$$L(E'/K, 1) \neq 0.$$

**Question**: When is this condition satisfied for $(E, K)$?

**Theorem** (Bump-Friedberg-Hoffstein, Murty, Murty). There exist infinitely many quadratic twists $E'$ of $E$ for which $L(E'/\mathbb{Q}, 1) \neq 0$ and also infinitely many for which $L'(E'/\mathbb{Q}, 1) \neq 0$. 
Non-vanishing of $L$-series

M. Ram Murty
V. Kumar Murty

Non-vanishing of $L$-Functions and Applications
Tetrahedral and Octahedral forms

Assume throughout that \( N_E \) is coprime to the discriminant of \( P(x) \).

**Theorem**

Let \( P \) be a polynomial of degree 4 with Galois group \( A_4 \) and no real roots, and let \( K \) be any subfield of its splitting field. Then \( L(E/K, 1) \neq 0 \Rightarrow E(K) \) is finite.

**Theorem**

Let \( P \) be a polynomial of degree 4 with Galois group \( S_4 \) and at least two non-real roots, and assume that \( L(E, \epsilon, 1) \neq 0 \), where \( \epsilon \) is the quadratic character attached to the discriminant of \( P \). Then, for any subfield \( K \) of the splitting field of \( P \), \( L(E/K, 1) \neq 0 \Rightarrow E(K) \) is finite.
An icosahedral application

**Theorem**

Let $P$ be a polynomial of degree 5 with Galois group $A_5$ and a single real root, and let $K$ be the quintic field generated by a root of $P$. Then

$$\text{ord}_{s=1} L(E, s) = \text{ord}_{s=1} L(E/K, s) \Rightarrow \text{rank}(E(\mathbb{Q})) = \text{rank}(E(K)).$$

**Explanation:** $\text{Ind}_K^{\mathbb{Q}} 1 = 1 \oplus V_1 \otimes V_2$, where $V_1$ and $V_2$ are odd two-dimensional representations of the binary icosahedral group.

The method says nothing (as far as we can tell!) about the arithmetic of $E$ over the field generated by a root of Lagrange’s sextic resolvent of $P(x)$. 
Happy 60th Birthday, Ram!