Potential automorphy: recent progress

Jack Thorne
University of Cambridge

European Research Council
Established by the European Commission

If p is an odd prime and a is an integer prime to p, then we define the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \bmod p \in ((\mathbb{Z}/p\mathbb{Z})^\times)^2; \\ -1 & \text{if } a \bmod p \notin ((\mathbb{Z}/p\mathbb{Z})^\times)^2. \end{cases}$$

Theorem (Gauss, 1796)

Let p, q be odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \text{ or } q \equiv 1 \bmod 4; \\ -1 & \text{if } p \equiv q \equiv 3 \bmod 4. \end{cases}$$

The law of quadratic reciprocity is closely related to the properties of *Gauss sums*

$$G(n) = \sum_{a=0}^{n-1} e^{2\pi i a^2/n}.$$

It is easy to show that if p, q are odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \frac{G(p)G(q)}{G(pq)}.$$

Moreover, $G(p)^2 = (-1)^{(p-1)/2}p$.

Determining the sign of the Gauss sum $G(p) = \pm\sqrt{(-1)^{(p-1)/2}p}$ is one route to proving quadratic reciprocity.

Cauchy (1840) gave a determination of the sign using the properties of the automorphic form

$$\theta(\tau) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 \tau},$$

defined for $\tau \in \mathfrak{H} = \mathbb{R} + i\mathbb{R}_{>0} \subset \mathbb{C}$.

$$\theta(i\epsilon + 2/p) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 \epsilon} e^{2\pi i n^2/p}$$
$$= \sum_{a=0}^{p-1} \left(e^{2\pi i a^2/p} \sum_{n\equiv a \bmod p} e^{-\pi (n\sqrt{\epsilon})^2} \right).$$

Consequently,

$$\lim_{\epsilon\to 0} \sqrt{\epsilon}\theta(i\epsilon + 2/p) = \frac{G(p)}{p} \int_{x=\infty}^{\infty} e^{-\pi x^2}\, dx.$$

$\theta(\tau)$ satisfies the transformation law

$$\theta(-1/\tau) = \sqrt{\tau/i} \cdot \theta(\tau).$$

Evaluating the limit $\lim_{\epsilon \to 0} \sqrt{\epsilon}\theta(i\epsilon + 2/p)$ instead using this transformation law leads to the desired determination

$$G(p) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \bmod 4; \\ i\sqrt{p} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

How does this generalize? Recall that $\mathbb{Q}$ has many absolute values: the usual one $|\cdot| = |\cdot|_\infty$, as well as a p-adic one $|p^n a/b|_p = p^{-n}$, for every prime p.

The completions with respect to these absolute values are the fields $\mathbb{R}$ of real numbers and $\mathbb{Q}_p$ of p-adic numbers, for every prime p.

We define the adèle ring

$$\mathbb{A}_\mathbb{Q} = \prod_{p\leq\infty}{}' \mathbb{Q}_p = \{(x_p) \in \prod_{p\leq\infty} \mathbb{Q}_p \mid \forall\forall p, |x_p|_p \leq 1\}.$$

It contains $\mathbb{Q}$ as a diagonally embedded discrete, cocompact subring, analogous to the subring $\mathbb{Z} \subset \mathbb{R}$.

If $E/\mathbb{Q}$ is a quadratic extension, then the norm gives a homomorphism $N_{E/\mathbb{Q}} : E^\times \to \mathbb{Q}^\times$. It extends to a homomorphism $N_p : (E \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times \to \mathbb{Q}_p^\times$ for every prime p.

We define a map $\nu_{E,p} : \mathbb{Q}_p^\times \to \{\pm 1\}$ by the formula

$$\nu_{E,p}(x) = \begin{cases} 1 & \text{if } x \in \text{image}(N_p); \\ -1 & \text{if } x \notin \text{image}(N_p). \end{cases}$$

We define a map $\nu_E : \mathbb{A}_{\mathbb{Q}}^\times \to \{\pm 1\}$ by the formula

$$\nu_E((x_p)_p) = \prod_p \nu_{E,p}(x_p).$$

$$\nu_E : \mathbb{A}_{\mathbb{Q}}^{\times} \to \{\pm 1\}$$

$$\nu_E((x_p)_p) = \prod_p \nu_{E,p}(x_p) = (-1)^{\#\{p | x_p \notin \text{image}(N_p)\}}.$$

Theorem

ν_E is a homomorphism, and $\nu_E(\mathbb{Q}^{\times}) = \{1\}$.

To recover the classical law of quadratic reciprocity, take $E = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2} p})$, and use $\nu_E(q) = 1$.

The ultimate generalization of this statement is class field theory.

It says that if K is a global field (a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_p(t)$), and if E/K is a Galois extension with abelian Galois group, then there is a canonical surjective homomorphism

$$\mathbb{A}_K^\times/K^\times \to \mathrm{Gal}(E/K),$$

with a kernel that can be described explicitly in terms of local data.

The adèle ring $\mathbb{A}_K = \prod_v{}' K_v$ is defined in exactly the same way in the case $K = \mathbb{Q}$; the product runs over the set of places (i.e. equivalence classes of non-trivial absolute values) of K.

What about non-abelian extensions? To describe these, we need to enter the framework of the Langlands program. Let K be a global field, and let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ denote its absolute Galois group.

Class field theory can be reformulated in terms of a bijection

$$\left\{ \begin{array}{c} \text{Homomorphisms} \\ G_K \to \mathbb{C}^\times \\ \text{of finite order} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Homomorphisms} \\ \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times \\ \text{of finite order} \end{array} \right\}.$$

Let ℓ be a prime different to the characteristic of K. The reciprocity conjecture in the Langlands program predicts the existence of a bijection

$$\left\{ \begin{array}{c} \text{Irreducible representations} \\ \rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell), \\ \text{algebraic} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Cuspidal automorphic} \\ \text{representations } \pi \\ \text{of } \mathrm{GL}_n(\mathbb{A}_K), \\ \text{algebraic} \end{array} \right\}.$$

A special case of this is an injection, for any global field K:

$$\left\{ \begin{array}{c} \text{Elliptic curves } E \\ \text{over } K \text{ with} \\ \mathrm{End}_K(E) = \mathbb{Z}, \\ \text{up to isogeny} \end{array} \right\} \hookrightarrow \left\{ \begin{array}{c} \text{Cuspidal automorphic} \\ \text{representations } \pi \\ \text{of } \mathrm{GL}_2(\mathbb{A}_K) \text{ of trivial} \\ \text{infinitesimal character} \end{array} \right\}.$$

(This is obtained from the previous statement by applying it to the representation $\rho_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ afforded by the ℓ-adic Tate module of an elliptic curve.)

A special case of *this* is a bijection, for any integer $N \geq 1$:

$$\left\{ \begin{array}{c} \text{Elliptic curves } E \\ \text{over } \mathbb{Q} \text{ of} \\ \text{conductor } N, \\ \text{up to isogeny} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Normalized newforms} \\ f = \sum_{n \geq 1} a_n q^n \\ \in S_2(\Gamma_0(N), \mathbb{Z}) \end{array} \right\}.$$

(This is obtained from the previous statement by using the interpretation of automorphic representations of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$ in terms of classical modular forms.)

A cuspidal automorphic form is a function $\varphi : \mathrm{GL}_n(\mathbb{A}_K) \to \mathbb{C}$ satisfying the following conditions:

1. For all $\gamma \in \mathrm{GL}_n(K)$ and for all $g \in \mathrm{GL}_n(\mathbb{A}_K)$, $\varphi(\gamma g) = \varphi(g)$.
2. (Some smoothness and growth conditions.)
3. (A cuspidality condition, implying that "φ does not come from any Levi subgroup of GL_n".)

By definition, a cuspidal automorphic representation π is an irreducible subquotient of the space of automorphic forms.

Example: let $\Delta(\tau) = q\prod_{n=1}^{\infty}(1-q^n)^{24}$, where $q = e^{2\pi i\tau}$.

Define a function $\varphi : \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}) \to \mathbb{C}$ by the formula

$$\varphi(\gamma g^{\infty} g_{\infty}) = \Delta\left(\frac{ai+b}{ci+d}\right)(ci+d)^{-12},$$

where

$$\gamma \in \mathrm{GL}_2(\mathbb{Q}),\ g^{\infty} \in \mathrm{GL}_2(\widehat{\mathbb{Z}}),\ \text{and } g_{\infty} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})^{\det>0}.$$

Then φ generates a cuspidal automorphic representation π_{Δ} of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$, which is algebraic.

$$\left\{ \begin{array}{c} \text{Irreducible representations} \\ \rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell), \\ \text{algebraic} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Cuspidal automorphic} \\ \text{representations } \pi \\ \text{of } \mathrm{GL}_n(\mathbb{A}_K), \\ \text{algebraic} \end{array} \right\}$$

We need to explain how ρ and π should be matched up under this bijection. The matching should be characterized in terms of the local data.

If v is a place of K (equivalently: an equivalence class of non-trivial absolute values on K) we write K_v for the completion, as in the definition of the adèle ring $\mathbb{A}_K = \prod'_v K_v$. Then there is an embedding $G_{K_v} \hookrightarrow G_K$ of Galois groups, well-defined up to conjugacy.

Any automorphic representation π admits a decomposition $\pi = \otimes'_v \pi_v$, where the π_v are irreducible representations of the groups $\mathrm{GL}_n(K_v)$.

Any representation $\rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ determines a system of restricted representations $\rho|_{G_{K_v}} : G_{K_v} \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$.

To each non-archimedean place v of K, we can associate the local objects $\rho|_{G_{K_v}}$ and π_v. These have associated L-factors

$$L(\rho|_{G_{K_v}}, s) \text{ and } L(\pi_v, s),$$

and we expect that these are equal. As a consequence, the global L-functions

$$L(\rho, s) = \prod_v L(\rho|_{G_{K_v}}, s) \text{ and } L(\pi, s) = \prod_v L(\pi_v, s)$$

should be equal.

What's known? We first focus on the case when K is a number field. In this case the most general results are in the case where π and ρ are supposed to be *regular* algebraic and K is a totally real or CM number field.

To say that ρ is regular algebraic is to say that its Hodge–Tate weights appear with multiplicity 1. The representations arising from elliptic curves have this property, but not e.g. the representations arising from abelian varieties of dimension $g > 1$.

If π is regular algebraic, then it can be realized in the cohomology of an arithmetic group.

Theorem

Let K be a totally real or CM number field. Then the arrow

$$\left\{ \begin{array}{c} \textit{Cuspidal automorphic} \\ \textit{representations } \pi \\ \textit{of } \mathrm{GL}_n(\mathbb{A}_K), \\ \textit{regular algebraic} \end{array} \right\} \to \left\{ \begin{array}{c} \textit{Representations} \\ \rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell) \end{array} \right\}$$

exists.

The proof of this theorem spanned a long period of time and is due to many people, including Clozel, Labesse, Harris, Taylor, Shin, Chenevier, . . .

Using base change, one can reduce to the case that K is a CM field. Let $c \in \mathrm{Aut}(K)$ denote complex conjugation. The theorem was first established in the case where π is conjugate self-dual, i.e. satisfies $\pi^c \cong \pi^\vee$ (as representations of $\mathrm{GL}_n(\mathbb{A}_K)$).

In this case, π can be expected to descend to an automorphic representation of a unitary group, and one can hope to realize the associated Galois representation in the cohomology of a Shimura variety.

The case where π is not conjugate self-dual is taken care of by constructing congruences between $\pi \boxplus \pi^{c,\vee}$ and representations Π of $\mathrm{GL}_{2n}(\mathbb{A}_K)$ which are conjugate self-dual. This allows one to construct a $2n$-dimensional representation R, which is then shown to be of the form $\rho \oplus (\rho^{c,\vee} \otimes \epsilon^{1-2n})$ (where ϵ is the ℓ-adic cyclotomic character).

The first proof, due to Harris–Lan–Taylor–T., uses overconvergent modular forms.

The second proof, due to Scholze, uses completed cohomology and the Hodge–Tate period map of a perfectoid Shimura variety.

We say that a Galois representation ρ is automorphic if it corresponds to an automorphic representation π, i.e. if it is in the image of the map

$$\left\{ \begin{array}{c} \text{Cuspidal automorphic} \\ \text{representations } \pi \\ \text{of } \mathrm{GL}_n(\mathbb{A}_K), \\ \text{regular algebraic} \end{array} \right\} \to \left\{ \begin{array}{c} \text{Representations} \\ \rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell) \end{array} \right\}$$

In the case $n = 2$ and $K = \mathbb{Q}$, we are quite close to being able to prove this map is bijective. In general, we can prove very little.

This motivates the definition of *potential* automorphy.

We say that a Galois representation $\rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ is potentially automorphic if there is a finite extension L/K such that $\rho|_{G_L}$ is automorphic.

$$\left\{ \begin{array}{c} \text{Representations} \\ \rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell) \end{array} \right\}$$

$$\downarrow$$

$$\left\{ \begin{array}{c} \text{Cuspidal automorphic} \\ \text{representations } \pi \\ \text{of } \mathrm{GL}_n(\mathbb{A}_L), \\ \text{regular algebraic} \end{array} \right\} \to \left\{ \begin{array}{c} \text{Representations} \\ \rho : G_L \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell) \end{array} \right\}$$

If a Galois representation is automorphic then it enjoys special properties (which are inherited from the corresponding automorphic representation π). For example:

- There is a number field $E = E_\rho \subset \overline{\mathbb{Q}}_\ell$ such that all but finitely many L-factors $L(\rho|_{G_{K_v}}, s)$ lie in $E[q_v^{-s}]$.
- The L-function $L(\rho, s)$ admits a meromorphic continuation and satisfies a functional equation.

In fact, one can show that these properties are enjoyed by Galois representations which are potentially automorphic too.

For regular algebraic Galois representations satisfying a self-duality condition, very strong potential automorphy theorems are known. For example:

Theorem (Patrikis–Taylor (2015), roughly stated)

Let K be a totally real field, and let $(\rho_\lambda)_\lambda$ be a compatible system of regular algebraic representations $\rho_\lambda : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\lambda)$, which of which is self-dual up to twist. Suppose moreover that there is an integer w such that each representation ρ_λ is pure of weight w. Then each the compatible system $(\rho_\lambda)_\lambda$ is potentially automorphic.

This builds on earlier work by Barnet-Lamb, Gee, Geraghty, Harris, Taylor, and others.

The first potential automorphy theorems were proved by Taylor. The main ingredients include:

1. Automorphy lifting theorems: roughly speaking, if $\rho, \rho' : G_K \to \mathrm{GL}_n(\mathbb{Z}_\ell)$ such that $\rho \bmod \ell = \rho' \bmod \ell$, and if ρ is automorphic, then so is ρ'.
2. Universally automorphic Galois representations: representations $\rho : G_K \to \mathrm{GL}_n(\mathbb{Z}_\ell)$ such that for any extension L/K, $\rho|_{G_L}$ is automorphic.
3. Moduli spaces of motives with fixed residual Galois representation.

Prototype argument for elliptic curves:

1. Let E be an elliptic curve over a number field K. Let A be a fixed elliptic curve over K with complex multiplication, and let $\ell \neq p$ be primes.
2. Let $Y(E[\ell], A[p])$ be the moduli space over K with classifies triples (C, ϕ_ℓ, ϕ_p), where C is an elliptic curve and $\phi_\ell : C[\ell] \to E[\ell]$, $\phi_p : C[p] \to A[p]$ are isomorphisms of finite group schemes.
3. Let L/K be an extension over which $Y(E[\ell], A[p])$ acquires a rational point, and let C be the corresponding elliptic curve. Applying an automorphy lifting theorem twice (first to $\rho_{C,p}$, then to $\rho_{E,\ell}|_{G_L}$), we see that E_L is automorphic.

The construction of the Galois representations attached to regular algebraic automorphic representations which are not conjugate self-dual has opened up the possibility of establishing potential automorphy theorems in this case too.

Theorem

Let K be a CM field (for example, an imaginary quadratic field), and let E be an elliptic curve over K with $\mathrm{End}_K(E) = \mathbb{Z}$. Then E is potentially automorphic.

This theorem is part of a work in progress by Allen, Calegari, Caraiani, Gee, Helm, Le Hung, Newton, Scholze, Taylor, and myself.

What about when K is a finite extension of $\mathbb{F}_p(t)$? L. Lafforgue proved in 2000 that for any $n \geq 1$, the correspondence

$$\left\{ \begin{array}{c} \text{Cuspidal automorphic} \\ \text{representations } \pi \\ \text{of } \mathrm{GL}_n(\mathbb{A}_K), \\ \text{algebraic} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Irreducible representations} \\ \rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell), \\ \text{algebraic} \end{array} \right\}$$

exists and has all desired properties (compatibility with L-functions, local Langlands correspondence, etc.).

One key input is the application of the Grothendieck–Lefschetz formula to understand the L-functions $L(\rho, s)$, independent of any relation with automorphic forms.

What about groups G other than GL_n?

Suppose that G is a split reductive group over $\mathbb{F}_p$, with finite centre. For example, one could take $G = \mathrm{SL}_n, \mathrm{Sp}_{2n}, \mathrm{SO}_n$ (a classical group) or $G = G_2, F_4$, or E_8 (an exceptional group).

Associated to G is its Langlands dual group, ${}^L G$. In our case, ${}^L G$ is a split reductive group over $\mathbb{Q}$ of Dynkin type dual to that of G (i.e. obtained by reversing the arrows in the Dynkin diagram). If $G = \mathrm{SL}_n$, then ${}^L G = \mathrm{PGL}_n$; if $G = E_8$, then ${}^L G = E_8$.

We then expect a correspondence

$$\left\{ \begin{array}{c} \text{Automorphic} \\ \text{representations } \pi \\ \text{of } G(\mathbb{A}_K) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Representations} \\ \rho : G_K \to {}^L G(\overline{\mathbb{Q}}_\ell) \end{array} \right\}$$

V. Lafforgue has constructed the "automorphic to Galois" direction of this conjectural correspondence:

$$\left\{ \begin{array}{c} \text{Automorphic} \\ \text{representations } \pi \\ \text{of } G(\mathbb{A}_K) \end{array} \right\} \to \left\{ \begin{array}{c} \text{Representations} \\ \rho : G_K \to {}^L G(\overline{\mathbb{Q}}_\ell) \end{array} \right\}$$

Furthermore, he has uncovered a whole new family of symmetries ("excursion operators") that act on automorphic forms, that refine and extend the action of the group $G(\mathbb{A}_K)$.

What about in the other direction?

Theorem (Böckle–Harris–Khare–T.)

Let G be a split simple group over $\mathbb{F}_p$, and let $\rho : G_K \to {}^L G(\overline{\mathbb{Q}}_\ell)$ be an everywhere unramified representation of Zariski dense image. Then ρ is potentially automorphic.

The most intricate part of the proof is the construction of "universally automorphic" Galois representations. These are constructed using input from the geometric Langlands program.

To describe this, let X be the smooth, projective curve over $\mathbb{F}_q$ with function field K, and let $\overline{X} = X_{\overline{\mathbb{F}}_q}$. Then there is a short exact sequence of étale fundamental groups:

$$1 \to \pi_1^{\text{ét}}(\overline{X}) \to \pi_1^{\text{ét}}(X) \to \pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{F}_q) \to 1.$$

Suppose that $\phi : \pi_1^{\text{ét}}(X) \to {}^L G(\overline{\mathbb{Q}}_\ell)$ is a homomorphism with the following properties:

1. $\phi(\pi_1^{\text{ét}}(\overline{X}))$ is contained in a unique maximal torus $\widehat{T}$ of ${}^L G$.
2. The induced action of $\pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{F}_q)$ on $\widehat{T}$ is elliptic (i.e. has trivial invariants in $X^*(\widehat{T})$.

In this case, Braverman–Gaitsgory's construction of geometric Eisenstein series implies that ϕ is automorphic.

If the action of $\pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{F}_q)$ on $\widehat{T}$ is through a Coxeter element of the Weyl group, then ϕ is often robust enough to be used in our automorphy lifting theorems.

Corollary

Let $\ell \neq p$ be a prime. Then there exist infinitely many pairs (X, π), where:

- *X is a smooth, projective curve over $\mathbb{F}_p$. We set $K = \mathbb{F}_p(X)$.*
- *π is a cuspidal and everywhere unramified automorphic representation of $E_8(\mathbb{A}_K)$ such that the associated Galois representation*

$$\rho : \pi_1^{ét}(X) \to E_8(\overline{\mathbb{Q}}_\ell)$$

  has Zariski dense image.