

My research is in the area of algebraic number theory. I study modular forms, Galois representations,  $p$ -adic families of such objects, and elliptic curves. The main result of my thesis is that the Galois representation associated to an ordinary  $p$ -adic family of modular forms has “large” image.

The philosophy behind the study of Galois representations comes from a universal theme in mathematics: linearization. Namely, there is a complicated object that we want to understand; in our case it is the group  $G_{\mathbb{Q}}$ , the absolute Galois group of  $\mathbb{Q}$  (the rational numbers). Just as one studies the tangent space of a complicated manifold or uses linear approximations to study a non-linear partial differential equation, representations allow us to study  $G_{\mathbb{Q}}$  through its action on certain vector spaces. Thus we end up studying a collection of matrices known as the *image of the representation*, a kind of “shadow” of  $G_{\mathbb{Q}}$  inside matrices, which are more concrete objects.

More formally, if  $A$  is a ring, write  $\mathrm{GL}_n(A)$  for the collection of all invertible  $(n \times n)$ -matrices with entries in  $A$  and  $\mathrm{SL}_n(A)$  for the collection of matrices in  $\mathrm{GL}_n(A)$  that have determinant 1. A *Galois representation* is a (continuous) homomorphism  $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_n(A)$ . The *image* of  $\rho$  is all matrices in  $\mathrm{GL}_n(A)$  of the form  $\rho(\sigma)$  for  $\sigma \in G_{\mathbb{Q}}$ . Elliptic curves defined over  $\mathbb{Q}$  give rise to interesting Galois representations. If  $E$  is such an elliptic curve, then for each prime  $p$  there is a Galois representation  $\rho_{E,p} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{Z}_p)$ , where  $\mathbb{Z}_p$  is the  $p$ -adic integers.

The larger the image of a Galois representation, the more information we can recover about  $G_{\mathbb{Q}}$ . The following definition quantifies what it means for a representation to have large image. Given a representation  $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(A)$  and a subring  $A_0$  of  $A$ , we say  $\rho$  is  $A_0$ -full if there is a non-zero  $A_0$ -ideal  $\mathfrak{a}$  such that the image of  $\rho$  contains all elements of  $\mathrm{SL}_2(A_0)$  that are congruent to the identity modulo  $\mathfrak{a}$ . In the 1960s, Serre studied the images of Galois representations associated to elliptic curves. His work implies that, in the generic case (when  $E$  does not have something called *complex multiplication* (CM)),  $\rho_{E,p}$  is  $\mathbb{Z}_p$ -full. Serre’s result is an example of a general pattern governing the expected behavior of images of Galois representations that arise from geometry.

**Heuristic.** *The image of a Galois representation should be as large as possible, subject to the symmetries of the geometric object from which it arose.*

The notion of “symmetry” depends on the geometric object. The relevant symmetry for an elliptic curve  $E$  is CM, a condition that means that  $E$  has extra symmetries. In the 1980s, Ribet and Momose determined, up to finite error, the image of a Galois representation  $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathcal{O})$  associated to a classical modular form without CM. They showed that  $\rho$  is  $\mathcal{O}_0$ -full for a certain subring  $\mathcal{O}_0$  of  $\mathcal{O}$  cut out by new symmetries of modular forms known as “conjugate self-twists”.

In the 1980s Hida developed his theory of  $p$ -adic families of (ordinary) modular forms. To such a family  $F$ , Hida associated a Galois representation  $\rho_F : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{I})$  for a certain ring  $\mathbb{I}$ . From  $\rho_F$  one obtains a mod  $p$  representation  $\bar{\rho}_F$ . One can consider conjugate self-twists of  $F$  and form the ring  $\mathbb{I}_0$  cut out by such twists. The following theorem is the main result of my thesis.

**Theorem** (Lang). *Let  $F$  be a non-CM Hida family. Under mild conditions on  $\bar{\rho}_F$ ,  $\rho_F$  is  $\mathbb{I}_0$ -full.*