

Introduction

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, in a qualitative sense, the Galois representation associated to an ordinary p -adic family of modular forms has “large” image. My future research plans include improving the result to a quantitative form and obtaining a complete description of the images of such Galois representations. Part of this project will require explicit computations using the open source software Sage, a task in which I am excited to involve undergraduate researchers.

Galois representations are fundamental objects of study in modern number theory. The philosophy behind the study of Galois representations comes from a universal theme in mathematics: linearization. Namely, there is a complicated mysterious object that we want to understand because it encodes lots of interesting information. In our case it is the group $G_{\mathbb{Q}}$, the absolute Galois group of the rational numbers, \mathbb{Q} . Just as a geometer studies the tangent space of a complicated manifold or an applied mathematician uses linear approximations to study a non-linear partial differential equation, we want to study $G_{\mathbb{Q}}$ using one of the most powerful tools in mathematics: linear algebra. This is what representations do; they allow us to study a complicated group like $G_{\mathbb{Q}}$ 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, recall that a *ring* is a collection of elements that can be added and multiplied together, like the integers. For a ring A , 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 $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_n(A)$, and the image of ρ is the image of this function. One of the first examples of Galois representations arises from elliptic curves defined over \mathbb{Q} . 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.

A fundamental problem is to determine the image of a given Galois representation. After all, we could always take ρ to be the trivial representation, which sends every element of $G_{\mathbb{Q}}$ to the identity matrix. This does not tell us anything about $G_{\mathbb{Q}}$ because its image (the set consisting of the identity matrix) is so small. 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 $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_n(A)$ and a subring A_0 of A , we say ρ is A_0 -full if there is a non-zero A_0 -ideal \mathfrak{a} such that the image of ρ contains all elements of $\mathrm{SL}_n(A_0)$ 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 [14]. 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.*

Past Work

The notion of “symmetry” in the above heuristic 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 [12, 13]. They showed that ρ 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 [5]. 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} [4]. From ρ_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 1 (Lang [8]). *Let F be a non-CM Hida family. Under mild conditions on $\bar{\rho}_F$, ρ_F is \mathbb{I}_0 -full.*

I have also worked on the arithmetic of elliptic curves. With my collaborators, I studied shadow lines of elliptic curves, an invariant first defined by Mazur and Rubin [10]. Using explicit class field theory, we developed an algorithm to compute the shadow line of a triple (E, K, p) , where E is an elliptic curve over \mathbb{Q} , K is an imaginary quadratic field, and p is a rational prime that satisfy certain mild properties. We implemented our algorithm in Sage [15] to compute the first examples of shadow lines. Our paper will appear in a conference proceedings [1].

Future work

Determining the \mathbb{I}_0 -level and relation to p -adic L -functions. Theorem 1 guarantees that there is a non-zero \mathbb{I}_0 -ideal \mathfrak{a}_0 such that the image of ρ_F contains all determinant 1 matrices that are congruent to the identity modulo \mathfrak{a}_0 . The largest such ideal is called the \mathbb{I}_0 -level of ρ_F and is denoted $\mathfrak{c}_{0,F}$. A natural question is to determine the \mathbb{I}_0 -level. I plan to prove the following conjecture, which is a generalization of Hida’s Theorem II in [6], with the help of undergraduate researchers.

Conjecture 1. *Let F and p be as in Theorem 1.*

1. *If $\mathrm{Im} \rho_F \supseteq \mathrm{SL}_2(\mathbb{F}_p)$, then $\mathfrak{c}_{0,F} = \mathbb{I}_0$. That is, $\mathrm{Im} \rho_F \supseteq \mathrm{SL}_2(\mathbb{I}_0)$.*
2. *Suppose that $\bar{\rho}_F$ is absolutely irreducible and induced from a character $\bar{\psi} : \mathrm{Gal}(\bar{\mathbb{Q}}/M) \rightarrow \bar{\mathbb{F}}_p^\times$ for an imaginary quadratic field M . Under some technical conditions, there is a product \mathcal{L}_0 of anticyclotomic Katz p -adic L -functions such that $\mathfrak{c}_{0,F}$ is a factor of \mathcal{L}_0 . Furthermore, every prime factor of \mathcal{L}_0 is a factor of $\mathfrak{c}_{0,F}$ for some F .*

Even when $\mathbb{I} = \Lambda$, Conjecture 1 is stronger than Hida’s Theorem II [6]. Furthermore, Conjecture 1.1 is a natural extension of the work of Mazur-Wiles [11] and Fischman [3]. Proving Conjecture 1 would yield refined information about the images of Galois representations attached to Hida families. It is the first step in completely determining the images of such representations.

In proving case (1) of the conjecture, I will make use of Manoharmayum’s recent work that shows $\mathrm{Im} \rho_F \supseteq \mathrm{SL}_2(W)$ for a finite unramified extension W of \mathbb{Z}_p [9]. This will be combined with some techniques that I developed in the proof of Theorem 1 to get the desired result. Some of the

techniques in my thesis involve carefully manipulating certain (2×2) -matrices to make a certain Lie algebra large. These techniques are accessible to an undergraduate with some background in abstract algebra, so I plan to facilitate undergraduate research through this project.

In proving case (2), I will relate the \mathbb{I}_0 -level to the congruence ideal of F as in Hida's proof of Theorem II [6]. The connection to Katz p -adic L -functions is then obtained by relating the congruence ideal to the p -adic L -function through known cases of the Main Conjecture of Iwasawa Theory. The idea is that replacing the Λ -level in Hida's work with the more precise \mathbb{I}_0 -level will allow me to remove the ambiguity of the square factors that show up in Theorem II [6].

Computing \mathcal{O}_0 -levels of classical Galois representations. The goal of this project is to compute the level of Galois representations coming from classical modular forms and thus completely determine the image of such a representation. Let f a classical modular form and \mathfrak{p} an embedding of a fixed algebraic closure of \mathbb{Q} into a fixed algebraic closure of the p -adic numbers. Under certain conditions, one can associate to the pair (f, \mathfrak{p}) a Galois representation $\rho_{f, \mathfrak{p}} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathcal{O})$ for a certain ring \mathcal{O} . As discussed above, Ribet [13] and Momose [12] found a subring \mathcal{O}_0 of \mathcal{O} such that $\mathrm{Im} \rho_{f, \mathfrak{p}}$ is \mathcal{O}_0 -full. The ring theory of \mathcal{O}_0 is particularly simple; there one ideal π such that all other non-zero ideals of \mathcal{O}_0 are powers of π . Ribet and Momose show that, under certain conditions, there is a minimal non-negative integer $c(f, \mathfrak{p})$ such that $\mathrm{Im} \rho_{f, \mathfrak{p}}$ contains all matrices of determinant 1 that are congruent to the identity modulo $\pi^{c(f, \mathfrak{p})}$. Their work further shows that $c(f, \mathfrak{p}) = 0$ for all but finitely many primes \mathfrak{p} . However, relatively little is known about the case when $c(f, \mathfrak{p})$ is positive and the weight of f is greater than 2. I plan to study how $c(f, \mathfrak{p})$ changes as f varies over certain families of modular forms.

This project will have both theoretical and computational components. First, I will establish a relationship between $c(f, \mathfrak{p})$ and the congruence number of f , which should also be related to values of the Katz p -adic L -function, as suggested by the proof of Theorem II in [6]. Once this is established, I will guide my undergraduate research students to create a method in the open source software Sage [15] to compute $c(f, \mathfrak{p})$ by computing the congruence number of f . Sage can already compute congruence numbers, making the scope of this project manageable even for math majors who are new to research and programming. Using the new functionality, we will create a large data set of levels of classical Galois representations in Hida families, which will likely lead to new conjectures to be studied theoretically. I have experience working with Sage from my Women in Numbers 3 project [1] and from leading a project at Sage Days 69. Indeed, my Sage Days project consisted of writing a method to test whether a modular form is CM, a first step in the eventual program to compute $c(f, \mathfrak{p})$.

Other settings. The above projects can be studied in more general settings than representations valued in (2×2) -matrices. Hida and Tilouine proved an analogue of Hida's Theorem II [6] for representations valued in (4×4) -matrices [7]. There are two main difficulties they overcome in their work: the types of symmetries are much more complicated than CM versus non-CM, and a certain theory of Lie algebras is only valid for SL_2 . I hope to use the tools they developed to overcome these problems to study analogues of the above questions for larger matrices.

Tilouine and his collaborators proved an analogue of Theorem 1 in the non-ordinary GL_2 -setting [2] by building on the ideas in my thesis. They introduce the relative Sen operator to avoid my assumption that the representation is ordinary. This idea will be useful in studying the above questions in the non-ordinary setting.

References

- [1] BALAKRISHNAN, J., ÇIPERIANI, M., LANG, J., MIRZA, B., AND NEWTON, R. Shadow lines in the arithmetic of elliptic curves. to appear, 2015.
- [2] CONTI, A., IOVITA, A., AND TILOUINE, J. Big image of Galois representations attached to finite-slope p -adic families of modular forms. July 2015.
- [3] FISCHMAN, A. On the image of Λ -adic Galois representations. *Ann. Inst. Fourier (Grenoble)* 52, 2 (2002), 351–378.
- [4] HIDA, H. Galois representations into $\mathrm{GL}_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms. *Invent. Math.* 85, 3 (1986), 545–613.
- [5] HIDA, H. Iwasawa modules attached to congruences of cusp forms. *Ann. Sci. École Norm. Sup. (4)* 19, 2 (1986), 231–273.
- [6] HIDA, H. Big Galois representations and p -adic L -functions. *Compos. Math.* 151, 4 (2015), 603–664.
- [7] HIDA, H., AND TILOUINE, J. Big image of Galois representations and the congruence ideal. In *Arithmetic and Geometry* (2014), L. Dieulefait, G. Faltings, D. R. Heath-Brown, Y. V. Manin, B. Z. Moroz, and J.-P. Wintenberger, Eds., vol. 420, Cambridge University Press, pp. 217–254.
- [8] LANG, J. On the image of the Galois representation associated to a non-CM Hida family. http://www.math.ucla.edu/~jaclynlang/I_0_level_existence.pdf, to appear in *Algebra and Number Theory*.
- [9] MANOHARMAYUM, J. A structure theorem for subgroups of GL_n over complete local Noetherian rings with large residual image. *Proc. Amer. Math. Soc.* 143, 7 (2015), 2743–2758.
- [10] MAZUR, B., AND RUBIN, K. Studying the growth of Mordell-Weil. *Doc. Math.*, Extra Vol. (2003), 585–607.
- [11] MAZUR, B., AND WILES, A. On p -adic analytic families of Galois representations. *Compos. Math.* 59, 2 (1986), 231–264.
- [12] MOMOSE, F. On the l -adic representations attached to modular forms. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 28, 1 (1981), 89–109.
- [13] RIBET, K. A. On l -adic representations attached to modular forms. II. *Glasgow Math. J.* 27 (1985), 185–194.
- [14] SERRE, J.-P. *Abelian ℓ -adic representations and elliptic curves*. W. A. Benjamin, Inc., 1968.
- [15] A. STEIN, W., ET AL. *Sage Mathematics Software*. The Sage Development Team, <http://www.sagemath.org>.