

Overview

My research is in the area of algebraic number theory. Primarily I study modular forms, the Galois representations associated to them, and p -adic families of such objects. I am also interested in the arithmetic of 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.

A fundamental problem is to determine the image of a given Galois representation. This was first done by Serre [15] for the p -adic Galois representations $\rho_{E,p}$ associated to an elliptic curve E/\mathbb{Q} . He showed that if E does not have complex multiplication (CM) then $\rho_{E,p}$ is surjective for all but finitely many primes p . Furthermore the image of $\rho_{E,p}$ is open for all p . Serre’s result is an example of a general pattern governing the expected behavior of images of Galois representations.

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” is vague and depends on the situation. In the case of elliptic curves, the relevant symmetry is complex multiplication. In the 1980s, Ribet and Momose determined, up to finite error, the image of a Galois representation coming from a classical modular form without CM and thus showed that such images are “large” [12, 14]. Their proof introduced new symmetries of modular forms known as “conjugate self-twists”. Indeed, if $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathcal{O})$ arises from a modular form, then one can talk about the subring \mathcal{O}_0 of \mathcal{O} fixed by all conjugate self-twists. Ribet and Momose proved that the intersection of $\mathrm{Im} \rho$ with $\mathrm{SL}_2(\mathcal{O}_0)$ is open in $\mathrm{SL}_2(\mathcal{O}_0)$.

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 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 fixed by all such twists. The following theorem is the main result of my thesis [8].

Theorem 1 (Lang [8]). *Let F be a non-CM Hida family. Assume that $\bar{\rho}_F$ is absolutely irreducible and satisfies a technical but mild regularity condition. Then there is a nonzero \mathbb{I}_0 -ideal \mathfrak{a}_0 such that the image of ρ_F contains all matrices in $\mathrm{SL}_2(\mathbb{I}_0)$ that are congruent to the identity modulo \mathfrak{a}_0 .*

I have a secondary interest in the arithmetic of elliptic curves. My group at the Women in Numbers 3 workshop 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/\mathbb{Q} is an elliptic curve, K is an imaginary quadratic field, and p is a rational prime of good reduction for E that splits in K . We implemented our algorithm in Sage [16] and computed the first examples of shadow lines. The resulting paper will appear in the proceedings volume [1].

Thesis

Background. I now give some definitions and notation to make the statement of Theorem 1 more precise. Fix a prime p , and assume for simplicity that $p \geq 5$. Let $\Lambda = \mathbb{Z}_p[[T]]$ and \mathbb{I} be an integral domain that is finite flat over Λ . Fix embeddings of an algebraic closure $\bar{\mathbb{Q}}$ of \mathbb{Q} into \mathbb{C} and $\bar{\mathbb{Q}}_p$.

Definition 1 (Hida [5], Wiles [17]). A formal power series $F = \sum_{n=1}^{\infty} A_n q^n \in \mathbb{I}[[q]]$ is a *Hida family* if $A_p \in \mathbb{I}^\times$ and for every integer $k \geq 2$ and every prime ideal \mathfrak{P} of \mathbb{I} lying over $(1 + T - (1 + p)^k)\Lambda$, we have:

- $A_n \bmod \mathfrak{P}$ is in $\overline{\mathbb{Q}}$ (rather than just $\overline{\mathbb{Q}_p}$), and
- $f_{\mathfrak{P}} := \sum_{n=1}^{\infty} (A_n \bmod \mathfrak{P}) q^n$ gives the q -expansion of a classical modular form of weight k .

Hida showed that every p -ordinary classical modular form of weight at least 2 arises from a unique such family [5]. Furthermore, there is a Galois representation $\rho_F : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{I})$ that is unramified almost everywhere. For all primes ℓ at which ρ_F is unramified, $\mathrm{tr} \rho_F(\mathrm{Frob}_{\ell}) = A_{\ell}$, where Frob_{ℓ} is the conjugacy class of a Frobenius element at ℓ [4].

Definition 2. An automorphism σ of \mathbb{I} is a *conjugate self-twist* of a Hida family $F = \sum_{n=1}^{\infty} A_n q^n \in \mathbb{I}[[q]]$ if there exists a non-trivial Dirichlet character η_{σ} such that

$$\sigma(A_{\ell}) = \eta_{\sigma}(\ell) A_{\ell}$$

for almost all primes ℓ . We say F has *complex multiplication (CM)* if the identity automorphism is a conjugate self-twist of F .

Ideas in the Proof of Theorem 1. The key result is a lifting theorem showing when a conjugate self-twist of an arithmetic specialization $f_{\mathfrak{P}}$ of F can be lifted to a conjugate self-twist of the entire family F . The ideas that go into the lifting theorem will be briefly explained in the next paragraph. Using the lifting theorem, there is a series of reduction steps to conclude that the theorem of Ribet and Momose is sufficient to prove Theorem 1. An important tool in these reduction steps is a \mathbb{Z}_p -Lie algebra of Pink [13] that is associated to $\mathrm{Im} \rho_F$, which allows us to reduce our problem to linear algebra. Hida observed that the ordinarity of ρ_F can be used to give Pink's Lie algebra a Λ -algebra structure [6], and this structure is critical to the proof.

I now give a brief outline of the proof of the lifting theorem. A conjugate self-twist σ of an arithmetic specialization $f_{\mathfrak{P}}$ of F induces an automorphism $\bar{\sigma}$ of the residue field \mathbb{F} . Using deformation theory, I lift $\bar{\sigma}$ to an automorphism Σ of the entire universal deformation ring $R_{\bar{\rho}_F}$ of $\bar{\rho}_F$ and show that Σ satisfies certain properties. Using automorphic methods I show that Σ preserves a certain Hecke algebra, \mathbb{T} . Since $\mathrm{Spec} \mathbb{I}$ is an irreducible component of $\mathrm{Spec} \mathbb{T}$, we see that Σ must send $\mathrm{Spec} \mathbb{I}$ to another irreducible component $\Sigma^* \mathrm{Spec} \mathbb{I}$ of $\mathrm{Spec} \mathbb{T}$. The properties of Σ force the two components $\mathrm{Spec} \mathbb{I}$ and $\Sigma^* \mathrm{Spec} \mathbb{I}$ to intersect at an arithmetic point. Since the Hecke algebra is étale over Λ at arithmetic points, Σ must descend to an automorphism of \mathbb{I} , as desired.

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].

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

1. If $\text{Im } \rho_F \supseteq \text{SL}_2(\mathbb{F}_p)$, then $\mathfrak{c}_{0,F} = \mathbb{I}_0$. That is, $\text{Im } \rho_F \supseteq \text{SL}_2(\mathbb{I}_0)$.
2. Suppose that $\bar{\rho}_F$ is absolutely irreducible and $\bar{\rho}_F \cong \text{Ind}_M^{\mathbb{Q}} \bar{\psi}$ for an imaginary quadratic field M in which p splits and a character $\bar{\psi} : \text{Gal}(\bar{\mathbb{Q}}/M) \rightarrow \bar{\mathbb{F}}_p^\times$. Assume M is the only such quadratic field. Under minor conditions on the tame level of F , 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 .

Note that 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].

In proving case (1) of the conjecture, I will make use of Manoharmayum's recent work that shows $\text{Im } \rho_F \supseteq \text{SL}_2(W)$ for a finite unramified extension W of \mathbb{Z}_p [9]. This will be combined with the Λ -module structure on the Pink Lie algebra associated to $\text{Im } \rho_F$ that was used in the proof of Theorem 1 to get the desired result.

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].

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.

Analogue of the Mumford-Tate Conjecture in p -adic families. Another way to describe the work of Ribet and Momose is that they proved the Mumford-Tate Conjecture for compatible systems of Galois representations associated to classical modular forms. Hida has proposed an analogue of the Mumford-Tate Conjecture for p -adic families of Galois representations. For an arithmetic prime \mathfrak{P} of \mathbb{I} , write $\text{MT}_{\mathfrak{P}}$ for the Mumford-Tate group of the compatible system containing $\rho_{f_{\mathfrak{P}}}$, so $\text{MT}_{\mathfrak{P}}$ is an algebraic group over \mathbb{Q} . Let $\kappa(\mathfrak{P}) = \mathbb{I}_{\mathfrak{P}}/\mathfrak{P}_{\mathfrak{P}}$, and write $G_{\mathfrak{P}}$ for the Zariski closure of $\text{Im } \rho_{f_{\mathfrak{P}}}$ in $\text{GL}_2(\kappa(\mathfrak{P}))$. Let $G_{\mathfrak{P}}^{\circ}$ be the connected component of the identity of $G_{\mathfrak{P}}$ and $G_{\mathfrak{P}}'$ the (closed) derived subgroup of $G_{\mathfrak{P}}$. Finally, let Γ_F denote the group generated by the conjugate self-twists of a non-CM Hida family F .

Conjecture 2 (Hida). Assume F is non-CM. There is a simple algebraic group G' , defined over \mathbb{Q}_p , such that for all arithmetic primes \mathfrak{P} of \mathbb{I} one has $G_{\mathfrak{P}}' \cong G' \times_{\mathbb{Q}_p} \kappa(\mathfrak{P})$ and $\text{Res}_{\mathbb{Q}_p}^{\kappa(\mathfrak{P})} G_{\mathfrak{P}}$ is (the ordinary factor of) $\text{MT}_{\mathfrak{P}} \times_{\mathbb{Q}} \mathbb{Q}_p$. Furthermore, the component group $G_{\mathfrak{P}}/G_{\mathfrak{P}}^{\circ}$ is canonically isomorphic to the Pontryagin dual of the decomposition group of \mathfrak{P} in Γ_F .

By obtaining a sufficiently precise understanding of images of Galois representations attached to Hida families through the first project, I plan to prove results along the lines of Conjecture 2. I have some preliminary results relating the Pontryagin dual of Γ_F to the quotient $(\text{Im } \rho_F)/(\text{Im } \rho_F|_H)$ for a certain finite index normal subgroup H of $G_{\mathbb{Q}}$.

Completing this research objective, or even any preliminary results in this direction, would reveal that the images of classical specializations of the Galois representation attached to a Hida family are even more related to one another than previously thought. Not only would they arise as specializations of some group in $\text{GL}_2(\mathbb{I})$, they could all be found simply by base change from a single group, at least up to abelian error.

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, submitted, July 2015.
- [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] PINK, R. Classification of pro- p subgroups of SL_2 over a p -adic ring, where p is an odd prime. *Compos. Math.* 88, 3 (1993), 251–264.
- [14] RIBET, K. A. On l -adic representations attached to modular forms. II. *Glasgow Math. J.* 27 (1985), 185–194.
- [15] SERRE, J.-P. *Abelian ℓ -adic representations and elliptic curves*. W. A. Benjamin, Inc., 1968.

- [16] A. STEIN, W., ET AL. *Sage Mathematics Software*. The Sage Development Team, <http://www.sagemath.org>.
- [17] WILES, A. On ordinary λ -adic representations associated to modular forms. *Invent. Math.* 94, 3 (1988), 529–573.