RESEARCH OUTLINE

TREVOR ARNOLD

1. Introduction

My research is in the area of *algebraic number theory*, which, broadly construed, is the study of what is referred to below as *arithmetic objects*, by which is meant objects which can be defined by a collection of polynomials with rational coefficients. Examples of arithmetic objects of particular interest include: number fields (finite field extensions of the rational field $\mathbf{Q}$), which can be defined by a single irreducible polynomial in $\mathbf{Q}[x]$; elliptic curves, which can be defined by equations of the form $y^2 = x^3 + Ax + B$; and more complicated objects, such as modular and automorphic forms and abelian varieties.

Much of modern algebraic number theory is devoted to studying the relationship between two kinds of invariants attached to arithmetic objects. One kind of invariant attached to an arithmetic object M, the Selmer group $\mathrm{Sel}(M)$, is *algebraic* in nature, and depends on a fixed prime number p. The Selmer group is a finitely-generated module over the ring of p-adic integers $\mathbf{Z}_p$. There is also an *analytic* invariant attached to M: the complex L-function $L(M, s)$ is a complex-analytic function of one variable defined on some right half-plane $\mathrm{Re}\, s \gg 0$ which conjecturally admits meromorphic (often analytic) continuation to the entire complex plane. A very broad suite of conjectures collectively referred to as the *Bloch-Kato conjectures* relates the behavior of $L(M, s)$ at integer points to the size of $\mathrm{Sel}(M)$. For example, the $\mathbf{Z}_p$-rank of $\mathrm{Sel}(M)$ should equal the order of vanishing of $L(M, s)$ at an appropriate integer value.

Arithmetic objects often belong to *p-adic families*, which are, roughly speaking, collections $\mathcal{F}$ of objects which are congruent to each other, in an appropriate sense, modulo a sufficiently large power of our fixed prime number p. In many interesting cases, one can define Selmer groups $\mathrm{Sel}(\mathcal{F})$ and L-functions $\mathcal{L}(\mathcal{F})$ on the level of families which are analogous to those discussed above. A central theme in my work is that the context of families is one of the most fruitful in which to study the Bloch-Kato and related conjectures, for the reason that p-adic families are at once *analytic*, in the sense of p-adic analysis, and also *algebraic*, in the sense that they are built from congruences. Thus, Selmer groups and L-functions gain a common footing when viewed on the level of families. This circle of ideas is often referred to as *Iwasawa theory* after K. Iwasawa, who initiated it in order to study class groups of cyclotomic fields.

As indicated below, my research falls into two broad categories. The first, comprising the papers [1, 3, 4] and the work in progress [7], is work on questions arising from the study of specific arithmetic objects, especially modular forms and elliptic curves. The second, comprising the paper [2] and the works in progress [5, 6], studies the structure of more general Selmer groups in the context of Iwasawa theory, and can be viewed as an extrapolation to more general contexts of the techniques I've developed to study families of modular forms.

2. Modular forms and elliptic curves

Complex multiplication. The paper [1], based on my thesis work, investigates the Iwasawa theory of modular forms which have *complex multiplication.* The study of such a form f is essentially equivalent to the study of a certain Grössencharacter ψ_f over a quadratic imaginary field K. Let $p > 3$ be a prime not dividing the level of f at which f is *ordinary*, i.e., the pth Fourier coefficient $a_p(f)$ of f is a p-adic unit. Let K_∞/K be the *anticyclotomic* $\mathbf{Z}_p$-extension, i.e., the unique $\mathbf{Z}_p$-extension K_∞/K such that $K_\infty/\mathbf{Q}$ is Galois and such that complex conjugation acts on $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbf{Z}_p$ by inversion. We then study the p-adic family $\mathcal{F}$ of characters obtained by twisting ψ_f by finite characters of Γ.

The classical L-function $L(\psi_f, s)$ has analytic continuation to all of $\mathbf{C}$ and satisfies a functional equation relating its values at s and $k - s$, where k is the weight of f. Set $\Lambda = \mathbf{Z}_p[\![\Gamma]\!]$, the completed group ring. A construction of Katz [11] supplies a p-adic L-function $\mathcal{L}(\mathcal{F}) \in \Lambda$ p-adically interpolating the values of L-functions of characters belonging to the p-adic family described above, among which is the *central* L-value $L(\psi_f, k/2)$. In fact, the motivation for studying the Iwasawa theory of ψ_f over this particular choice of K_∞ is that all the L-values interpolated by $\mathcal{L}(\mathcal{F})$ are central points in the applicable functional equations. The parity of the order of vanishing of $L(\psi_f, s)$ at its central point reveals itself in the following way over K_∞.

Theorem 1 ([1, Thms. 2.1, 2.2])**.** *If the order of vanishing of $L(\psi_f, s)$ at its central point is even, then $\mathrm{Sel}(\mathcal{F})$ is a torsion Λ-module and for every height 1 prime $\mathfrak{p} \subseteq \Lambda$, $\mathfrak{p} \neq (p)$,*

$$\mathrm{length}_{\Lambda_\mathfrak{p}} \left(\Lambda/\mathcal{L}(\mathcal{F})\right)_\mathfrak{p} = \mathrm{length}_{\Lambda_\mathfrak{p}} \mathrm{Sel}(\mathcal{F})_\mathfrak{p}.$$

If the order of vanishing is odd, then $\mathrm{Sel}(\mathcal{F})$ is a rank 1 Λ-module.

In the case of odd order of vanishing, it is possible to determine the characteristic ideal of the torsion submodule $\mathrm{Sel}(\mathcal{F})_{\Lambda\text{-tors}}$ in terms of the derivative of a 2-variable p-adic L-function. A relatively straightforward consequence of the above theorem (using the close relationship between ψ_f and f) is the following statement towards the Bloch-Kato conjecture for f. Note that no assumption is made on the sign of the functional equation.

Corollary 2 ([1, Thm. 3.11])**.** *If f is a p-ordinary modular form with complex multiplication, then $L(f, s)$ vanishes at its central point $s = k/2$ if and only if $\mathrm{Sel}(f)$ is infinite.*

In the non-ordinary case, it seems like that statements similar to Theorem 1 and Corollary 2 could be proved. This is an interesting possibility for future work.

Hida families. The assumption that a modular form has complex multiplication is somewhat restrictive, so it is natural to ask whether there is some setting in which results analogous to Theorem 1 hold for modular forms which do not necessarily have complex multiplication. The papers [3] and [4] and the work in progress [7] all study the case of a general p-ordinary modular forms. Given a p-ordinary modular form f, there is no way in general to associate a quadratic imaginary field or Grössencharacter to f. Thus, the anticyclotomic Iwasawa algebra Λ considered in [1] must be replaced by some other p-adic ring naturally associated to f. By work of Hida [9], every p-ordinary modular form can, in a suitable sense, be put into an ordinary p-adic family $\mathcal{F}$ of modular forms. An appropriate replacement for Λ is supplied by the ordinary modular deformation ring $\mathbf{H} = \mathbf{H}_{\mathcal{F}}^{\mathrm{ord}}$ associated to $\mathcal{F}$ by Hida.

Suitable hypotheses on the form f (including p-ordinarity and irreducibility of the residual representation for f) allow the construction of a Selmer group $\mathrm{Sel}(\mathcal{F})$ for $\mathcal{F}$ (or, more precisely, the self-dual twist of $\mathcal{F}$), which is a finitely-generated $\mathbf{H}$-module. This Selmer group is related by a control theorem to the p-Selmer groups $\mathrm{Sel}(g)$ for the modular forms g belonging to $\mathcal{F}$, which are related in turn by the Bloch-Kato conjectures to the central values of the classical L-functions $L(g, s)$. Moreover, by work of Greenberg-Stevens, Kitagawa, Ochiai, and others, there is a p-adic L-function $\mathcal{L}(\mathcal{F}) \in \mathbf{H}[\![X]\!]$ associated to $\mathcal{F}$, analogous to the Katz p-adic L-function for a Grössencharacter, which interpolates the values of the classical L-functions $L(g, s)$ at integer points for the modular forms g belonging to the family $\mathcal{F}$. With suitable normalization, the specialization $\mathcal{L}(\mathcal{F})|_{X=0}$ interpolates the *central* values of the $L(g, s)$. As in the case of complex multiplication, the modular forms belonging to the family $\mathcal{F}$ share a common sign in the functional equation for their L-functions. The analogues of Theorem 1 above should, be true in this setting and should imply that Corollary 2 is true for *all* modular forms. The paper [4] proves these statements subject to certain non-vanishing conjectures for Galois cohomology classes arising from the Euler system constructed by Kato [10].

Theorem 3 ([4, Thm. 2.1]). *Assuming some non-vanishing conjectures (cf. the description of* [3] *below), if the sign of $\mathcal{F}$ is not -1, then* $\mathrm{Sel}(\mathcal{F})$ *is a torsion* $\mathbf{H}$-*module and we have the equality*

$$\mathrm{length}_{\mathbf{H}_{\mathfrak{p}}} \mathrm{Sel}(\mathcal{F})_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}}(\mathcal{L}(\mathcal{F})|_{X=0}).$$

for all but an explicit finite set of height 1 *primes* $\mathfrak{p} \subseteq \mathbf{H}$. *In case the sign of $\mathcal{F}$ is -1,* $\mathrm{Sel}(\mathcal{F})$ *has generic rank* 1 *over* $\mathbf{H}$.

The work in progress [7] describes the torsion submodule of $\mathrm{Sel}(\mathcal{F})$ in the case of sign -1 in terms of $\frac{d}{dX}\mathcal{L}(\mathcal{F})$ and will possibly also weaken the hypotheses of the theorem.

Hida has extended his construction of p-adic families to ordinary automorphic forms for a large class of algebraic groups. In a few cases, Selmer groups can be attached to these families and the techniques described above for Hida families should also apply to these Selmer groups. One could study, for example, symmetric square Galois representations for modular forms using these generalized Hida families. This will be the subject of future work.

Non-vanishing conjectures. The related paper [3] relates non-vanishing conjectures for Kato's Euler system to other, similar, conjectures which are somewhat better understood (or at least have been around longer). The most important of these is a conjecture of Greenberg which states that the L-functions $L(g, s)$ as g runs over the members of the family $\mathcal{F}$ should, with finitely many exceptions, either have order of vanishing 0 or 1 at their central points depending on whether $L(f, s)$ vanishes to even or odd order, respectively, at its central point. A p-adic version of this conjecture is the statement that the order of vanishing of $\mathcal{L}(\mathcal{F})$ along $X = 0$ is either 0 or 1 (again, depending on the parity of the order of vanishing of $L(f, s)$ at its central point). The more difficult part of this conjecture is the odd case. Among the main results of [3] is the following.

Theorem 4 ([3, Thm. 4.14])**.** *Assume $L(f,s)$ vanishes to odd order at its central point. If Greenberg's "Hypothesis L"[1] for $\mathcal{F}$, the non-vanishing of $\left(\frac{d}{dX}\mathcal{L}(\mathcal{F})\right)|_{X=0}$, and a 2-variable main conjecture all hold, then Kato's Euler system for $\mathcal{F}$ is non-vanishing.*

Another topic treated in [3] is the generalization of a formula of Rubin [15] concerning p-adic height pairings on the Selmer groups associated to $\mathcal{F}$, which is useful for proving implications among the various conjectures under consideration. For example, the height pairing figures the following converse to Theorem 4.

Theorem 5 ([3, Thm. 1.6])**.** *Assume $L(f,s)$ vanishes to odd order at its central point and the p-adic height pairing for $\mathcal{F}$ is non-degenerate. If Kato's Euler system for $\mathcal{F}$ is non-vanishing, then $\left(\frac{d}{dX}\mathcal{L}(\mathcal{F})\right)|_{X=0}$ is non-zero.*

3. General Selmer groups

Parity. The paper [2] was motivated by an attempt to understand the interaction between complex multiplication and parity. Suppose K/k is a CM extension[2], and let K_∞/K be an extension with $\mathrm{Gal}(K_\infty/K) \cong \mathbf{Z}_p^d$ for some d and which is *dihedral* with respect to K/k, i.e., K_∞ is Galois over k and the complex conjugation in $\mathrm{Gal}(K/k)$ acts on $\mathrm{Gal}(K_\infty/K)$ by inversion. As explained in [2], one can prove a rather general parity theorem for "nice" p-ordinary representations $\rho : \mathrm{Gal}(\overline{k}/K) \to \mathrm{GL}_n(\mathbf{Z}_p)$ satisfying the following property generalizing the notion of complex multiplication to the context of p-adic Galois representations: for every continuous p-adic character $\xi : \mathrm{Gal}(K_\infty/K) \to \overline{\mathbf{Q}}_p^\times$, the induced representation $\mathrm{ind}_{K/k}(\rho \otimes \xi)$ is self-dual via a skew-symmetric pairing. One can think of such ρ as being "half" of a CM representation of $\mathrm{Gal}(\overline{k}/k)$.

Theorem 6 ([2, Thm. 1.5])**.** *With k, K, K_∞, and ρ as above, the Λ-torsion submodule of the Selmer group $\mathrm{Sel}_p(K_\infty, \rho)$ is pseudo-isomorphic[3] modulo p-torsion to a square[4] Λ-module.*

Work of Nekovář (cf. especially [14, Chap. 10]) provides a very general framework for investigating parity phenomena for self-dual representations. The case where ρ is itself is self-dual is also treated in [2], thereby giving new proofs of several results of Nekovář (cf. [14, 10.7.11–10.7.15]). An interesting aspect of this theorem is that shows how many of the parity results known for self-dual representations continue to hold for those representations which are "half" of a self-dual CM representation, even though such representations are not themselves self-dual.

Theorem 6 also has several applications in the context of CM elliptic curves, CM modular forms, and CM abelian varieties. If M/k is such an object whose p-adic Galois representation over k is isomorphic to $\mathrm{ind}_{K/k}\,\rho$ for a character ρ of

---

[1] This condition appears in [8, p. 339] and amounts to the assumption that the Selmer groups associated to $\mathcal{F}$ contain few classes which are trivial at p.

[2] A *CM extension* is a totally imaginary quadratic extension of a totally real number field.

[3] A *pseudo-isomorphism* is a Λ-module homomorphism the kernel and cokernel of which are annihilated by an ideal of height 2.

[4] A Λ-module M is *square* if $M \cong N \oplus N$ for some Λ-submodule $N \subseteq M$.

$\mathrm{Gal}(\overline{K}/K)$, then one sees from the theorem that the parity of the order of vanishing of $L(M,s)$ at its central point should be reflected in the *rank* of $\mathrm{Sel}_p(K_\infty,\rho)$ as a Λ-module. This information may be useful in finding the correct form of a main conjecture for M over K_∞. As shown in [2, §4], the theorem can also be used to give statements regarding the growth of ranks of CM abelian varieties in the tower K_∞/K and thereby gives a different approach to results following from the methods of Mazur-Rubin (cf. [12], [13]).

Techniques for general families. Euler systems are a fundamental tool in Iwasawa theory. Indeed, everything described in §2 relies in an essential way on the theory of Euler systems. An Euler system for a p-adic representation is a collection of classes in the Galois cohomology of the representation which are defined over a bunch of number fields and are assumed to satisfy certain specific norm-compatibility relations. Under appropriate hypotheses, the existence of an Euler system for a representation implies a bound on the Selmer group in terms of the Euler system classes, which can sometimes be related to p-adic L-functions.

One of the key technical difficulties in proving Theorem 3 above is an application of the Euler system theory to study Selmer groups for families with integrally closed coefficient ring $\mathbf{H}$, whereas previous applications have all assumed the coefficient rings to be regular. The work in progress [6] generalizes this technique to give Euler system bounds for a class of representations defined over arbitrary normal coefficient rings. The focus of [6] is a statement of the following type.

Theorem 7 (anticipated)**.** *Suppose given a p-adic family $\mathcal{F}$ of arithmetic objects satisfying suitable hypotheses which admits a Galois representation with normal coefficient ring R. If z is an Euler system for the family $\mathcal{F}$, then the "usual" Euler system bound for* $\mathrm{length}_{R_\mathfrak{p}} \mathrm{Sel}(\mathcal{F})$ *provided by z holds for all height 1 primes $\mathfrak{p} \subseteq R$ outside an explicit finite set.*

The techniques used to prove this theorem rely on the normality hypothesis in an essential way. It is natural to ask whether a similar statement might hold without this hypothesis. One goal of the work in progress [5] (joint with K. Koo) is to explore ways in which to calculate the invariants of $\mathrm{Sel}(\mathcal{F})$ in the case that the coefficient ring for the Galois representation associated with $\mathcal{F}$ is not necessarily normal. For the rings we study, the normalization $\widetilde{R}$ is a finite extension of R, so the normalized family $\widetilde{(}\mathcal{F})$ (obtained by tensoring $\mathcal{F}$ up to $\widetilde{R}$) is *isogenous* to $\mathcal{F}$ in a suitable sense. By studying how invariants of $\mathrm{Sel}(\mathcal{F})$ change with respect to isogeny in $\mathcal{F}$, we can relate the Selmer groups $\mathrm{Sel}(\mathcal{F})$ and $\mathrm{Sel}(\widetilde{\mathcal{F}})$ under some assumptions $\mathcal{F}$. This gives a way of obtaining information about general families, for example using Euler systems, by first normalizing and then applying techniques which apply to families with normal coefficient rings.

References

1. T. Arnold, *Anticyclotomic main conjectures for CM modular forms*, J. reine angew. Math. **606** (2007), 44–78.
2. ______, *Complex multiplication and parity in Iwasawa theory*, J. Number Theory **128** (2008), 2634–2654.
3. ______, *Hida families, p-adic heights, and derivatives*, Ann. Inst. Fourier **61** (2011), to appear.
4. ______, *On the main conjecture for a self-dual Hida family*, preprint (submitted).

5. ——— (with K. Koo), *Euler-Poincaré characteristics and change of Selmer group for big Galois representations*, in preparation.
6. ———, *Euler system techniques for normal rings*, in preparation.
7. ———, *On the main conjecture for a self-dual Hida family, II*, in preparation.
8. R. Greenberg, *On the structure of certain Galois cohomology groups*, Doc. Math. (2006), no. Extra Vol., 335–391 (electronic).
9. H. Hida, *Iwasawa modules attached to congruences of cusp forms*, Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 2, 231–273.
10. K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque (2004), no. 295, 117–290.
11. N. Katz, *p-adic interpolation of real analytic Eisenstein series*, Ann. of Math. (2) **104** (1976), no. 3, 459–571.
12. B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799.
13. ———, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612.
14. J. Nekovář, *Selmer complexes*, Astérisque (2005), no. 310.
15. K. Rubin, *Abelian varieties, p-adic heights and derivatives*, Algebra and number theory, Walter de Gruyter and Co., 1994, pp. 247–266.