IP Current Developments in Mathematics, 2004

Main Conjectures and Modular Forms

Christopher Skinner

1. Introduction

This paper reports on joint work with E. Urban that completes [1] a proof of the Main Conjecture of Iwasawa Theory for a broad class of elliptic curves and modular forms. As such, it is concerned mainly with special values of L-functions of modular forms and the ways which they get packaged together (such as in p-adic L-functions).

Roughly speaking, for an elliptic curve E over $\mathbf{Q}$ with ordinary reduction at a prime p this Main Conjecture avers the equality of the characteristic ideal of the Selmer group of E over the field $\mathbf{Q}_\infty$ - the unique Galois extension of $\mathbf{Q}$ with $\Gamma = \mathrm{Gal}\,(\mathbf{Q}_\infty/\mathbf{Q}) \cong \mathbf{Z}_p$ - and the ideal generated by the p-adic L-function of the elliptic curve, the equality being of ideals belonging to the completed group ring $\mathbf{Z}_p[\![\Gamma]\!]$. (Precise statements can be found in §3 below.) Great progress towards this conjecture was made by K. Kato [**K**] who essentially proved that the characteristic ideal divides the p-adic L-function. In our work we prove the opposite divisibility in many cases. More precisely, we prove such a divisibility with $\mathbf{Q}$ replaced by an auxiliary imaginary quadratic field K (see Theorem 3.4.2 below). In other words, we prove that the product of the p-adic L-function of E and that of its K-twist E_K divides the product of the characteristic ideals of the Selmer groups associated to E and E_K. Combining with Kato's results permits the separation of E from E_K.

Supported in part by a grant from the National Science Foundation and a fellowship from the David and Lucile Packard Foundation.

[1] The main results reported on herein - Theorems 3.4.2 and 4.1.6 - depend on the existence of certain Galois representations associated to automorphic forms on unitary groups of signature (2,2). The existence of such representations, while certainly conjectured, has not been fully established in the literature. We discuss this more in Remark 4.1.7.

The auxiliary quadratic field K appears because of the setting in which we work. Our proof follows along the lines of Wiles's proof of the Main Conjecture for totally real fields [**W**]. We work with Eisenstein series whose constant terms involve values of twists of the L-function of E and study congruences between these Eisenstein series and cuspforms. It turns out that the Eisenstein series most amenable to such a study are for a unitary group $GU(2,2)$, the definition of which requires the introduction of the quadratic field K.

This report and most of the results stated herein focus on the consequences of our work for the Main Conjecture for an elliptic curve E, but most of the results are valid for E replaced by any eigenform. Indeed, a technical feature of our proof is the necessity of working with eigenforms of weight greater than two. This is forced on us by the fact that weight two forms for $GU(2,2)$ are not cohomological and so there are not 'enough' congruences. But the missing congruences can be found by working with forms of higher weight. (This mirrors the situation for Dirichlet characters.)

While the focus of the research reported on here is GL_2-objects - modular forms and their L-functions - and certain of their generalizations - automorphic forms on Hermitian half-spaces - it is instructive to first consider the GL_1-case - the case of Dirichlet characters. Results and proofs from this case inspired both the conjectures motivating our work and the methods we have employed to approach them.

Following our discussion of the GL_1-case we recall the Iwasawa theory of elliptic curves and state our main results in this area. We then indicate the more general setting in which our proofs play out and outline the major features of our arguments.

As will often be passing between the complex and p-adic 'worlds,' to connect what happens in them we fix some field embeddings. First, for a number field F we fix an embedding $\bar{F} \hookrightarrow \mathbf{C}$. Then we fix for each finite place v an embedding $\bar{F}_v \hookrightarrow \mathbf{C}$ and an embedding $\bar{F} \hookrightarrow \bar{F}_v$ such that the composition of the two is just our previous embedding of $\bar{F}$ into $\mathbf{C}$. Among other things, these choices determine for each place v of F a decomposition group $D_v \subset G_F = \mathrm{Gal}\,(\bar{F}/F)$. We let $I_v \subseteq D_v$ be the inertia subgroup. We normalize class field theory so that uniformizers correspond to Frobenius elements. For a prime p we let $\varepsilon_p : G_F \to \mathbf{Z}_p^\times$ be the character giving the action of G_F on all pth-power roots of unity: $\sigma(\zeta) = \zeta^{\varepsilon(\sigma)}$. We let $\omega_p : G_F \to \mathbf{Z}_p^\times$ be the Teichmüller lift of ε modulo p. Since ω_p takes values in $\mu_{p-1} \subset \mathbf{Z}_p^\times$, our identification of $\mathbf{Z}_p$ with a subring of $\mathbf{C}$ permits ω_p to be viewed as a complex-valued character of G_F.

2. The GL_1-case

2.1. The set-up. The proto-typical special value formula is the class number formula of Dirichlet and Dedekind: Let F be a number field with ring of integers $\mathcal{O}_F$ and let $\zeta_F(s)$ be its Dedekind zeta function. Then

$$\mathrm{ord}_{s=0}\zeta_F(s) = \mathrm{rank}\,\mathcal{O}_F^\times \tag{2.1.1a}$$

and

$$\lim_{s\to 0} s^{-\mathrm{rank}\,\mathcal{O}_F^\times}\zeta_F(s) = -\frac{h_F R_F}{w_F}, \tag{2.1.1b}$$

where h_F is the class number of F, R_F is the regulator of the group of units $\mathcal{O}_F^\times$, and w_F is the number of roots of unity in F (the order of the torsion subgroup of the finitely-generated abelian group $\mathcal{O}_F^\times$).

Suppose now that $F = \mathbf{Q}(\mu_N)$, the field obtained by adjoining the Nth roots of unity. Then $\Delta_N = \mathrm{Gal}\,(F/\mathbf{Q}) \to (\mathbf{Z}/N\mathbf{Z})^\times$, $\sigma \mapsto (a \text{ s.t. } \sigma(\zeta) = \zeta^a \text{ for all } \zeta \in \mu_N)$, is an isomorphism. This isomorphism identifies characters of Δ_N with Dirichlet characters of conductor N. There is then a decomposition

$$\zeta_F(s) = \prod_{\chi\in\widehat{\Delta}_N} L(s,\chi), \tag{2.1.2}$$

the right-hand side being a product of Dirichlet L-series.

Since the Galois group Δ_N acts naturally on the unit group and class group of F, one is lead naturally to ask whether the decomposition in (2.1.2) is reflected in a similar refinement of the class number formula (2.1.1b). A positive answer was provided in work of Mazur and Wiles [**MW**], one consequence of which is the following.

THEOREM 2.1.3. *Let p be an odd prime. If $\chi \in \widehat{\Delta}_N$ has order prime to p and is odd (i.e., $\chi(-1) = -1$), then*

$$\#(\mathbf{Z}_p[\chi]/L(0,\chi)) = \#(C_F \otimes \mathbf{Z}_p[\chi])^{\bar{\chi}}, \tag{2.1.4}$$

where $\mathbf{Z}_p[\chi]$ is the ring of integers of the finite extension of $\mathbf{Q}_p$ obtained by adjoining the values of χ, C_F is the class group of F, and the superscript $\bar{\chi}$ denotes the $\bar{\chi}$-isotypical piece.

This theorem is a generalization of work of Herbrand and Ribet (cf. [**R**]) that proved the equivalence of the non-triviality of the two sides of (2.1.4) when $N = p$. It was in the work of Ribet that a connection to modular forms was made, a connection more fully exploited in the subsequent work of Mazur and Wiles [**MW**] and Wiles [**W**] and which we now attempt to explain. To simplify notation and keep the ideas at the forefront, we consider only the case where $N = p$ is an odd prime. Moreover, we will focus only on showing how non-triviality of the left-hand side of (2.1.4) implies non-triviality of the right-hand side, as this

contains most of the salient features. We will always assume that χ is odd.

2.2. Selmer groups. Class field theory permits the right-hand side of (2.1.4) to be interpreted as the order of a certain Galois cohomology group. Let

$$\mathrm{Sel}_p(\mathbf{Q},\chi) = \ker\left\{ H^1(G_{\mathbf{Q}}, \mathbf{Q}_p/\mathbf{Z}_p(\bar{\chi})) \to \prod_{\ell} H^1(I_\ell, \mathbf{Q}_p/\mathbf{Z}_p(\bar{\chi}))\right\},$$

where $\mathbf{Q}_p/\mathbf{Z}_p(\bar{\chi})$ is the $G_{\mathbf{Q}}$-module whose underlying group is the discrete group $\mathbf{Q}_p/\mathbf{Z}_p$ on which $G_{\mathbf{Q}}$ acts via the character $\bar{\chi}$, the arrow being the usual restriction map. This is an example of a *Selmer group*. Since restriction to $G_{\mathbf{Q}(\mu_p)}$ yields an identification

$$\begin{aligned} H^1(G_{\mathbf{Q}}, \mathbf{Q}_p/\mathbf{Z}_p(\bar{\chi})) &= H^1(G_{\mathbf{Q}(\mu_p)}, \mathbf{Q}_p/\mathbf{Z}_p(\bar{\chi}))^{\Delta_p} \\ &= \mathrm{Hom}_{\Delta_p}(G_{\mathbf{Q}(\mu_p)}, \mathbf{Q}_p/\mathbf{Z}_p(\bar{\chi})), \end{aligned}$$

it easily follows that $\mathrm{Sel}_p(\mathbf{Q},\chi)$ is identified with the 'unramified' homorphisms, i.e., those factoring through $\mathrm{Gal}(H_p/\mathbf{Q}(\mu_p))$ where H_p is the Hilbert class field of $\mathbf{Q}(\mu_p)$. Class field theory identifies $\mathrm{Gal}(H_p/\mathbf{Q}(\mu_p))$ with the class group $C_{\mathbf{Q}(\mu_p)}$. Thus $\mathrm{Sel}_p(\mathbf{Q},\chi)$ is identified with $\mathrm{Hom}_{\Delta_p}(C_{\mathbf{Q}(\mu_p)}, \mathbf{Q}_p/\mathbf{Z}_p(\bar{\chi}))$, whose order is clearly given by the right-hand side of (2.1.4).

The up-shot of this cohomological interpretation is that to prove that non-triviality of the left-hand side of (2.3) implies non-triviality of the right-hand side, one need only show that if $\mathrm{ord}_p L(0,\chi) > 0$ then then there exists a non-split $\mathbf{F}_p[G_{\mathbf{Q}}]$-extension

$$0 \to \mathbf{F}_p(\bar{\chi}) \to E \to \mathbf{F}_p \to 0$$

that splits over each inertia group I_ℓ; such extensions are classified by the p-torsion of $\mathrm{Sel}_p(\mathbf{Q},\chi)$. In other words, one needs to find a non-split Galois representation

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p), \quad \rho \cong \begin{pmatrix} \bar{\chi} & * \\ & 1 \end{pmatrix}, \tag{2.2.1}$$

that splits as a representation of each I_ℓ. Since modular forms are a good source for two-dimensional Galois representations, it is not unnatural that they enter the picture at this point.

2.3. Eisenstein series and Galois representations. Since ω_p factors through Δ_p (in fact ω_p generates $\widehat{\Delta}_p$) we can view both χ and ω_p as Dirichlet characters of conductor p. Bearing this in mind,

given each integer $k \geq 1$ let $\chi_k = \chi\omega_p^{1-k}$. There is then a holomorphic Eisenstein series

$$E_k(\chi) = L^p(1-k, \chi_k)/2 + \sum_{n=1}^{\infty} \sigma_{k-1}(\chi_k, n)e(nz),$$
$$\sigma_{k-1}(\chi_k, n) = \sum_{d>0, d|n, p\nmid d} \chi_k(d)d^{k-1},$$

of weight k, level p, and character χ_k. The L-series of $E_k(\chi)$ is $\zeta(s)L^p(s-k+1, \chi_k)$. The superscript '$p$' denotes the omission of the Euler factor at p.

Suppose that $\operatorname{ord}_p L^p(1-k, \chi_k) > 0$. Then $E_k(\chi)$ modulo p looks like the q-expansion of a cuspform, even an eigenform, modulo p. Assume that this can be made precise: there is an eigenform $f = \sum_{n=1}^{\infty} a_n q^n$ of weight k, level p, and character χ_k, having Fourier coefficients in the ring of integers $\mathcal{O}_F$ of some finite extension F of $\mathbf{Q}$ and such that

$$a_n \equiv \sigma_{k-1}(\chi_k, n) \bmod \mathfrak{p} \tag{2.3.1}$$

for some prime $\mathfrak{p}$ of F above p. Associated to f is a two-dimensional $F_{\mathfrak{p}}$-Galois representation

$$\rho_f : G_{\mathbf{Q}} \to \operatorname{Aut}_{F_{\mathfrak{p}}}(V), \quad \dim_{F_{\mathfrak{p}}}(V) = 2,$$

that is continuous and unramified away from p and such that

$$\operatorname{trace} \rho_f(\operatorname{Frob}_\ell) = a_\ell, \quad \ell \neq p. \tag{2.3.2}$$

2.4. Constructing elements in Selmer groups. Let $L \subset V$ be any $G_{\mathbf{Q}}$-stable $\mathcal{O}_{F_{\mathfrak{p}}}$-lattice. Then reducing L modulo $\mathfrak{p}$ yields a 2-dimensional $\mathbf{F}$-Galois representation

$$\bar{\rho}_f : G_{\mathbf{Q}} \to \operatorname{Aut}_{\mathbf{F}}(L/\mathfrak{p}),$$

where $\mathbf{F}$ is the residue field $\mathcal{O}_F/\mathfrak{p}$. Comparing (2.3.1) and (2.3.2) shows that the semi-simplification of $\bar{\rho}_f$ is equivalent to the sum of two characters $\mathbf{1} \oplus \chi$. Using the fact that ρ_f is not reducible, it is easy to see that L can be chosen so that

$$\bar{\rho}_f \cong \begin{pmatrix} 1 & * \\ & \chi \end{pmatrix}$$

is non-split. However, since ρ_f is unramified at each $\ell \neq p$, $\bar{\rho}_f$ splits as a representation of each corresponding I_ℓ. Furthermore, since it follows from (2.3.1) that a_p is a p-adic unit, f is a p-ordinary eigenform and so

$$\rho_f|_{D_p} \cong \begin{pmatrix} \chi_1 & * \\ & \chi_2 \end{pmatrix}, \quad \chi_2|_{I_p} = 1.$$

Since $\chi|_{I_p} \neq 1$, it can be easily deduced that $\bar{\rho}_f$ also splits as a representation of I_p. Then $\bar{\rho}_f \otimes \bar{\chi}$ provides the sought-for representation as in (2.2.1).

Clearly, the critical point in this proof is the existence of the eigenform f. In [**R**] Ribet achieves this by taking $k = 2$ and multiplying two suitable weight-one Eisenstein series, subtracting an appropriate multiple this product from $E_2(\chi)$, and then appealing to a lemma of Deligne and Serre. For k sufficiently large, the existence of f can also be deduced from the geometry of the modular curve $X_1(p)$. Fortunately, the choice of k is immaterial if we are only trying to prove that non-triviality of the left-hand side of (2.1.4) implies non-triviality of the right-hand side:

$$L^p(1-k,\chi_k) \equiv L^p(1-k',\chi_{k'}) \bmod p, \quad k' \geq k > 0.$$

However, at first-glance it would seem that working only with $k > 1$ would make it impossible to obtain the full strength of Theorem 2.1.3. This is a point where Iwasawa theory shows its power. The values $L(1-k,\chi_k)$, $k > 0$, can all be packaged into a single object - a p-adic L-function. Similary, the Selmer groups $\mathrm{Sel}_p(\mathbf{Q},\chi_k\varepsilon_p^{k-1})$ - defined as $\mathrm{Sel}_p(\mathbf{Q},\chi)$ was - can all be packaged into a larger Selmer group. Working with weights $k > 1$, one can refine the above arguments to relate the p-adic L-function to the larger Selmer group in such a way that one can then deduce the desired equality for $k = 1$ (i.e., Theorem 2.1.3). We do not enter into this here, but we do define the corresponding Iwasawa-theoretic objects when we move on to discuss elliptic curves and modular forms.

2.5. The strategy again. We recall the broad outlines of the strategy employed above to connect L-values to Selmer groups; it is the same strategy we follow in the case of elliptic curves and modular forms.

0. We start with some arithmetic object M (for 'motive') with attached L-function $L(M,s)$ and Selmer group $\mathrm{Sel}(M)$. There should be a conjectural relationship between the special value $L(M,0)$ and the order of $\mathrm{Sel}(M)$.
1. Show that $L(M,s) = L(\pi,s)$ for some automorphic representation π of some group G.
2. Associate to M (equivalently, to π) a special automorphic representation $\tau(M)$ of a higher-rank group H.
3. Show that the special value $L(M,0) = L(\pi,0)$ controls congruences between forms in the special representation $\tau(M)$ and forms in cuspidal representations that are "indigenous" to H.
4. Combine the Galois representations associated to cuspidal representations of H with the congruences from step 3 to produce elements in $\mathrm{Sel}(M)$.

In the case considered so far, $M = \chi_k\varepsilon_p^{k-1}$, $G = \mathrm{GL}_1$ (class field theory takes care of step 1), $H = \mathrm{GL}_2$, and $\tau = \tau(M)$ is the representation associated to $E_k(\chi)$.

3. Iwasawa theory of elliptic curves

Our presentation of the Iwasawa Theory of elliptic curves follows that in [**G1**]. In particular, we replace cohomology groups over $\mathbf{Q}_\infty$ with $G_{\mathbf{Q}}$-cohomology of 'big' representations.

3.1. Selmer groups. Let E be an elliptic curve over $\mathbf{Q}$. Let p be a prime and $T = T_pE = \varprojlim_n E[p^n]$ the Tate-module of E at p. Here $E[p^n]$ is the group of p^n-torsion points of E. Then T is naturally a $\mathbf{Z}_p$-module and $T \cong \mathbf{Z}_p^2$. Since $E[p^n] \subset E(\bar{\mathbf{Q}})$, the group of $\bar{\mathbf{Q}}$-points of E, the Galois group $G_{\mathbf{Q}}$ acts continuously on T. (That is, continuously with respect to the pro-finite topology on $G_{\mathbf{Q}}$ and the p-adic topology on T.) We denote this action by ρ. Let $A = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p$.

Consider the short-exact sequence

$$0 \to E[p^n] \to E(\bar{\mathbf{Q}}_p) \to E(\bar{\mathbf{Q}}_p) \to 0,$$

where the third arrow is $x \mapsto p^n x$. From the associated long-exact cohomology sequence we get an injection:

$$E(\mathbf{Q}_p)/p^nE(\mathbf{Q}_p) \hookrightarrow H^1(D_p, E[p^n]). \tag{3.1.1}$$

Using that $H^1(D_p, A) = \varinjlim_n H^1(D_p, E[p^n])$, the transition maps coming from the inclusion $E[p^n] \subset E[p^{n+1}]$, we deduce from (3.1.1) that there is an injection

$$E(\mathbf{Q}_p) \otimes \mathbf{Q}_p/\mathbf{Z}_p \hookrightarrow H^1(D_p, A). \tag{3.1.2}$$

We then associate to E its (standard) p-Selmer group $\mathrm{Sel}_p^{\mathrm{st}}(E)$ defined as the set of classes $c \in H^1(G_{\mathbf{Q}}, A)$ such that the restriction of c to $H^1(D_p, A)$ lies in the image of the map in (3.1.2) and for each place $v \neq p$ of $\mathbf{Q}$ the restriction to $H^1(D_v, A)$ is trivial. This is the p-primary part of the usual Selmer group associated to E.

Suppose now that E has ordinary reduction at p (meaning either good, ordinary reduction or bad, multiplicative reduction). Then there is a D_p-filtration

$$0 \subset T^+ \subset T$$

such that $T^+ \cong \mathbf{Z}_p$ and $T/T^+ \cong \mathbf{Z}_p$, with the D_p-action on the latter unramified. Let $A^+ = T^+ \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p$. The image of (3.1.2) lies in the kernel of the natural map from $H^1(D_p, A)$ to $H^1(I_p, A/A^+)$, and the p-Selmer group $\mathrm{Sel}_p(E)$ of E (which contains $\mathrm{Sel}_p^{\mathrm{st}}(E)$) is defined as

$$\mathrm{Sel}_p(E) = \ker\{H^1(G_{\mathbf{Q}}, A) \to H^1(I_p, A/A_v^+) \times \prod_{w \nmid p} H^1(D_w, A)\}.$$

This definition has the benefit of being given solely in terms of the Galois representation ρ.

The definition of $\mathrm{Sel}_p(E)$ can be generalized in many ways. For example, given a finite set Σ of primes different from p we define $\mathrm{Sel}_{p,\Sigma}(E)$

and $\mathrm{Sel}_p^{\Sigma}(E)$ just as we did $\mathrm{Sel}_p(E)$, but with $H^1(D_w, A)$ replaced by $H^1(I_w, A)$ and 0, respectively, for each $w \in \Sigma$. Then we have

$$\mathrm{Sel}_p(E) \subseteq \mathrm{Sel}_{p,\Sigma}(E) \subseteq \mathrm{Sel}_p^{\Sigma}(E). \tag{3.1.3}$$

For another example, let $\psi : G_{\mathbf{Q}} \to \bar{\mathbf{Q}}^{\times}$ be a finite character. Let $\mathcal{O}$ be the ring of integers of the finite extension of $\mathbf{Q}_p$ obtained by adjoining the values of ψ. We define $\mathrm{Sel}_p(E, \psi)$, $\mathrm{Sel}_{p,\Sigma}(E, \psi)$, and $\mathrm{Sel}_p^{\Sigma}(E, \psi)$ just as we did $\mathrm{Sel}_p(E)$, etc., only we replace T, T^+, A, A^+ with $T_\psi, T_\psi^+, A_\psi, A_\psi^+$, where the latter are defined by $T_\psi = T \otimes_{\mathbf{Z}_p} \mathcal{O}$, etc., and letting $G_{\mathbf{Q}}$ act on T_ψ by $\rho \otimes \psi$.

3.2. L-values. Still letting E be an elliptic curve over $\mathbf{Q}$, recall that E has an associated L-function:

$$L(E, s) = \prod_{\ell = \text{prime}} L_\ell(\ell^{-s})^{-1}, \quad L_\ell(X) = \det(1 - X\rho(\mathrm{Frob}_\ell)|V_{\ell', I_\ell}).$$

Here s is a complex variable, ℓ' is any prime different from ℓ, $V_{\ell'} = T_{\ell'}E \otimes_{\mathbf{Z}_{\ell'}} \bar{\mathbf{Q}}_{\ell'}$, and V_{ℓ', I_ℓ} is the maximal $\bar{\mathbf{Q}}_{\ell'}$-subquotient of $V_{\ell'}$ on which I_ℓ acts trivially. While this product only converges absolutely for s in the half-plane $\mathrm{Re}\,(s) > 3/2$, it is now known that $L(E, s)$ has an analytic continuation to a holomorphic function on the entire complex plane. Letting $\psi : G_{\mathbf{Q}} \to \bar{\mathbf{Q}}^{\times}$ be a finite character, we define $L(E, \psi, s)$ just as we did $L(E, s)$ but with $V_{\ell'}$ replaced with $V_{\ell'} \otimes \psi$ (meaning that the Galois action is twisted by ψ). This, too, has an analytic continuation to the whole complex plane. Given a finite set Σ of primes of $\mathbf{Q}$ we define $L^{\Sigma}(E, s)$ and $L^{\Sigma}(E, \psi, s)$ by dropping the factors at the primes in Σ. Clearly these also have analytic continuations to all of $\mathbf{C}$.

The celebrated conjectures of Birch-Swinnerton-Dyer and Bloch-Kato lead one to connect values of $L^{\Sigma}(E, \psi, s)$ to the orders of the Selmer groups $\mathrm{Sel}_p^{\Sigma}(E, \psi)$ as follows. Let Ω_E be the canonical period of E. Let N_E be the conductor of E and for each prime $\ell | N_E$ let c_ℓ be the p-part of the Tamagawa number at ℓ. Put $c_E = \prod_\ell c_\ell$. Let N_ψ be the conductor of ψ, let $n_\psi = \mathrm{ord}_p(N_\psi)$, and let $\tau(\psi^{-1})$ be the Gauss sum associated to ψ^{-1}. Let α be the unit root of $x^2 - a_p(E)x + p = 0$ if E has good reduction at p and otherwise let $\alpha = a_p(E)$. Let

$$L_{\mathrm{alg}}(E, \psi, 1) = a_\psi \tau(\psi^{-1}) \frac{L(E, \psi, 1)}{\Omega_E},$$

where

$$a_\psi = \begin{cases} 1 - \alpha^{-1}\psi^{-1}(\mathrm{Frob}_p) & n_\psi = 0 \text{ and } E \text{ has mult. red. at } p \\ (1 - \alpha^{-1}\psi^{-1}(\mathrm{Frob}_p))^2 & n_\psi = 0 \text{ and } E \text{ has good red. at } p \\ \alpha^{-n_\psi} & \text{otherwise.} \end{cases} \tag{3.2.1}$$

Let $L_{\mathrm{alg}}^{\Sigma}(E, \psi, 1)$ be defined similarly. Of course, if ψ is trivial, then we drop it from the notation. It is known that if $p > 2$, if $E[p]$ is an

absolutely irreducible $\mathbf{F}_p$-representation of $G_{\mathbf{Q}}$, and if ψ has odd order, then $L_{\text{alg}}(E,\psi,1), L^{\Sigma}_{\text{alg}}(E,\psi,1) \in \mathcal{O}$ (cf. [**GV**]).

CONJECTURE 3.2.2. *Suppose $E[p]$ is an absolutely irreducible $\mathbf{F}_p$-representation of $G_{\mathbf{Q}}$. Suppose also that $p > 2$ and ψ has odd order. Let Σ be a finite collection of primes different from p and containing all such that divide $N_E N_\psi$. Let $r_\psi = \operatorname{ord}_{s=1} L(E,\psi,1)$.*

(i) $r_\psi = \operatorname{rank}_{\mathcal{O}} \operatorname{Hom}_{\mathbf{Z}_p}(\operatorname{Sel}_p(E,\psi), \mathbf{Q}_p/\mathbf{Z}_p)$
$= \operatorname{rank}_{\mathcal{O}} \operatorname{Hom}_{\mathbf{Z}_p}(\operatorname{Sel}^{\Sigma}_p(E,\psi), \mathbf{Q}_p/\mathbf{Z}_p)$.

(ii) $\#(\mathbf{Z}_p/L_{\text{alg}}(E,1)) = c_E \cdot \#\operatorname{Sel}^{\text{st}}_p(E) \cdot \#(\mathbf{Z}_p/a)$.

(iii) $\#(\mathcal{O}/L_{\text{alg}}(E,\psi,1)) = \#\operatorname{Sel}_{p,\Sigma}(E,\psi)$.

(iv) $\#(\mathcal{O}/L^{\Sigma}_{\text{alg}}(E,\psi,1)) = \#\operatorname{Sel}^{\Sigma}_p(E,\psi)$.

REMARKS 3.2.3.

(a) The assumptions on p, $E[p]$, and ψ have been made to simplify the statement of the conjecture. In particular we have avoided discussing periods and situations where $L(E,\psi,s)$ as we have defined it is not the usual twist of the Dirichlet series $L(E,s)$ by the Dirichlet character associated to ψ. The most general Bloch-Kato-type conjectures encompass all these.

(b) When ψ is trivial, part (i) follows from the Birch-Swinnerton-Dyer Conjecture and the (conjectural) finiteness of the p-primary part of the Tate-Shafarevich group of E. In general this conjecture is weaker than the (refined) Birch-Swinnerton-Dyer Conjecture since no claims are being made about the leading Taylor coefficient in the expansion about $s = 1$ when $r_\psi \geq 1$.

(c) Parts (ii)–(iv) are weaker than part (i) when $L(E,\psi,1) = 0$ for they just imply the positivity of the rank.

(d) Parts (ii)–(iv) should be equivalent; what is clear is that

$$\#\operatorname{Sel}_{p,\Sigma}(E) | c_E \cdot \#\operatorname{Sel}^{\text{st}}_p(E) \cdot \#(\mathbf{Z}_p/a) \tag{3.2.4a}$$

if E does not have split multiplicative reduction at p, and that

$$\#\operatorname{Sel}^{\Sigma}_p(E,\psi,1) | \#\operatorname{Sel}_{p,\Sigma}(E,\psi) \cdot \prod_{\ell\in\Sigma} \#(\mathcal{O}/L_\ell(\psi,\ell^{-1})), \tag{3.2.4b}$$

where $L_\ell(\psi,\ell^{-s})$ is the local L-factor in the definition of $L(E,\psi,s)$ (so $L_\ell(\psi,\ell^{-s}) = L_\ell(\psi(\ell)\ell^{-s})$ if $\ell \nmid N_E$).

3.3. Main Conjectures. Let $\mathbf{Q}_\infty/\mathbf{Q}$ be the unique $\mathbf{Z}_p$-extension of $\mathbf{Q}$. That is, $\Gamma = \operatorname{Gal}(\mathbf{Q}_\infty/\mathbf{Q}) \cong \mathbf{Z}_p$. Let $\gamma \in \Gamma$ be a fixed topological generator. Given a pth-power root of unity ζ, we let $\psi_\zeta : G_{\mathbf{Q}} \to \bar{\mathbf{Q}}^\times$ be the finite order character defined by composing the canonical projection $G_{\mathbf{Q}} \twoheadrightarrow \Gamma$ with the finite-order character $\Gamma \to \bar{\mathbf{Q}}^\times$ that sends γ to ζ.

Let $\Lambda = \mathbf{Z}_p[\![\Gamma]\!]$. This is a complete, local Noetherian $\mathbf{Z}_p$-algebra with residue field $\mathbf{F}_p$. In fact $\Lambda \cong \mathbf{Z}_p[\![X]\!]$, via $\gamma \mapsto 1 + X$, so Λ is a regular ring. Let $\Psi : G_{\mathbf{Q}} \to \Lambda^\times$ be the canonical projection onto

Γ. Then for a pth-power root of unity ζ, $\Psi \bmod (\gamma - \zeta) = \psi_\zeta$. Let $\Lambda^\vee = \mathrm{Hom}_{\mathrm{cts}}(\Lambda, \mathbf{Q}_p/\mathbf{Z}_p)$, where the subscript 'cts' denotes continuous homomorphisms. This is a discrete Λ-module, the Λ-action being given by $(\lambda f)(x) = f(\lambda x)$ for $\lambda \in \Lambda$ and $f \in \Lambda^\vee$. We let $G_{\mathbf{Q}}$ act on it through the character Ψ.

Returning to the setup of Section 1, we let $M = M_E = T \otimes_{\mathbf{Z}_p} \Lambda^\vee$ and let G_Q act on this via $\rho \otimes \Psi$. Similarly we let $M^+ = T^+ \otimes_{\mathbf{Z}_p} \Lambda^\vee$. These are discrete Galois modules, and so we can speak of their Galois cohomology. Note that M is 'built from' all the modules A_{ψ_ζ}:

$$M[\gamma - \zeta] = A_{\psi_\zeta}, \quad M^+[\gamma - \zeta] = A^+_{\psi_\zeta}. \tag{3.3.1}$$

We attach Selmer groups to the pair M, M^+ just as we did for A_ψ, A^+_ψ. For any finite set Σ of primes different from p let

$$\mathrm{Sel}^\Sigma(M) = \ker\{H^1(G_{\mathbf{Q}}, M) \to H^1(I_p, M/M^+) \times \prod_{\ell \notin \Sigma, \ell \neq p} H^1(I_\ell, M)\}.$$

The relation (3.3.1) suggests these Selmer groups should be connected to those of §3.1. This is the content of the next proposition.

Proposition 3.3.2. *Suppose E has ordinary reduction at p and $E[p]$ is an absolutely irreducible $\mathbf{F}_p$-representation of $G_{\mathbf{Q}}$. Suppose also that Σ contains all primes different from p that divide N_E, the conductor of E. For a pth-power root of unity ζ,*

$$\mathrm{Sel}^\Sigma(M)[\gamma - \zeta] = \mathrm{Sel}^\Sigma_p(E, \psi_\zeta).$$

Note that $\mathrm{Sel}^\Sigma(M)$ is a discrete Λ-module, so $S^\Sigma(M) = \mathrm{Hom}_{\mathbf{Z}_p}(\mathrm{Sel}^\Sigma(M), \mathbf{Q}_p/\mathbf{Z}_p)$ is a compact Λ-module. It is not difficult to prove that $S^\Sigma(M)$ is in fact a finite Λ-module. In particular, under the hypotheses of Proposition 3.3.2 and whenever the conclusion of that proposition holds,

$$\#(S^\Sigma(M)/(\gamma - \zeta)S^\Sigma(M)) = \#\mathrm{Sel}^\Sigma_p(E, \psi_\zeta). \tag{3.3.3}$$

Since $S^\Sigma(M)$ is a finite Λ-module, the structure theory of such modules (finite $\mathbf{Z}_p[\![X]\!]$-modules) tells us that there is a quasi-isomorphism

$$S^\Sigma(M) \to \prod_{i=1}^m \Lambda/(f_i). \tag{3.3.4}$$

('Quasi-isomorphism' means finite-order kernel and cokernel.) We define the Λ-characteristic ideal I_E^Σ of $S^\Sigma(M)$ to be the ideal generated by $f_E^\Sigma = f_1 \cdots f_m$. The Main Conjecture of Iwasawa Theory of elliptic curves identifies a specific generator of I_E^Σ which is connected to L-values. We motivate this by assuming that the map in (3.3.4) is an

injection. Then, if $\phi_\zeta : \Lambda \twoheadrightarrow \mathbf{Z}_p[\zeta]$ is the map defined by $1 + X \mapsto \zeta$, ζ a pth-power roof of unity,

$$\#(S^\Sigma(M)/(\gamma - \zeta)S^\Sigma(M)) = \#(\mathbf{Z}_p[\zeta]/(\phi_\zeta(f_E^\Sigma)).$$

Combining this with (3.3.3) and Conjecture 3.2.2 implies, at least under the hypotheses of Conjecture 3.2.2 and Proposition 3.3.2, that $(\phi_\zeta(f_E^\Sigma))$ $= (L_{\text{alg}}^\Sigma(E, \psi_\zeta, 1))$. We can even dream that $I_E^\Sigma = (\mathcal{L})$, where $\mathcal{L} \in \Lambda$ is such that $\phi_\zeta(\mathcal{L}) = L_{\text{alg}}^\Sigma(E, \psi_\zeta, 1)$. Such an $\mathcal{L}$ is provided by the Mazur-Swinnerton-Dyer p-adic L-function for E.

PROPOSITION 3.3.5 ([**MSD**], [**GV**]). *Suppose E is an elliptic curve over $\mathbf{Q}$ with ordinary reduction at p. Let Σ be any finite collection of primes different from p. There is an element $\mathcal{L}_E^\Sigma \in \Lambda \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ such that for any pth-power root of unity ζ*

$$\phi_\zeta(\mathcal{L}_E^\Sigma) = L_{\text{alg}}^\Sigma(E, \psi_\zeta, 1).$$

Moreover, if p is odd and $E[p]$ is an absolutely irreducible $\mathbf{F}_p$-representation of $G_\mathbf{Q}$, then $\mathcal{L}_E^\Sigma \in \Lambda$.

Note that ϕ_ζ extends linearly to a surjection $\Lambda \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \twoheadrightarrow \mathbf{Q}_p[\zeta]$.

We can now state a version of the Main Conjecture for E.

CONJECTURE 3.3.6 (The Main Conjecture for Elliptic Curves). *Suppose E is an elliptic curve over $\mathbf{Q}$ with ordinary reduction at p*

(i) *$S^\Sigma(M)$ is a torsion Λ-module.*
(ii) *$I_E^\Sigma = (\mathcal{L}_E^\Sigma)$ in $\Lambda \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$.*
(iii) *If $\mathcal{L}_E^\Sigma \in \Lambda$ then $I_E^\Sigma = (\mathcal{L}_E^\Sigma)$ in Λ.*

REMARK 3.3.7. It is conjectured that $\mathcal{L}_E^\Sigma$ is always in Λ, so in effect Conjecture 3.3.6 asserts that I_E^Σ is generated by $\mathcal{L}_E^\Sigma$.

3.4. Some theorems. About ten years ago, K. Kato made great progress towards a proof of Conjecture 3.3.6. Using a construction of Beilinson, K-theory of modular curves, and the theory of Euler systems as developed by Kolyvagin and Rubin, he essentially proved half of the conjecture.

THEOREM 3.4.1 (Kato [**K**]). *Suppose E is an elliptic curve over $\mathbf{Q}$ with ordinary reduction at an odd prime p. Let Σ be a finite set of primes different from p.*

(i) *$S^\Sigma(M)$ is a torsion Λ-module.*
(ii) *$(\mathcal{L}_E^\Sigma) \subseteq I_E$ in $\Lambda \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$.*
(iii) *If E has good reduction at p and the representation*

$$\bar{\rho} = \rho \bmod p : G_\mathbf{Q} \to \operatorname{Aut}_{\mathbf{F}_p}(E[p]) \cong \mathrm{GL}_2(\mathbf{F}_p)$$

is surjective, then $(\mathcal{L}_E^\Sigma) \subseteq I_E^\Sigma$ in Λ.

This main ideas of [**K**] are nicely exposed in [**C**], [**S**], and [**Ru**].

Recently, in joint work with E. Urban, we have proven the opposite inclusion for many E's. In doing so we follow a method that originates in Ribet's proof of the converse of Herbrand's Theorem [**R**] but which was developed more fully in Wiles's proof of the Main Conjecture of Iwasawa Theory for totally real fields [**W**]. Roughly speaking, it combines the connection of L-values to congruences between Eisenstein series and cuspforms with the Galois representations associated to cuspforms to construct large subgroups of $\mathrm{Sel}^{\Sigma}(M)$. In our work the Eisenstein series and cuspforms are for the unitary groups $GU(2,2)$. Here I state one consequence of our results.

THEOREM 3.4.2 (Skinner-Urban [**SU1**]). *Suppose E is an elliptic curve over $\mathbf{Q}$ with ordinary reduction at an odd prime p. Let K be an imaginary quadratic field in which p splits. Let E_K be the K-twist of E. Let Σ be any finite set of primes different from E and containing all such that divide N_E or the discriminant of K. Suppose further that*

(a) *$E[p]$ is an absolutely irreducible $\mathbf{F}_p$-representation of $G_{\mathbf{Q}}$;*
(b) *there exists a prime $\ell || N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ.*

Then $I_E^{\Sigma} \cdot I_{E_K}^{\Sigma} \subseteq (\mathcal{L}_E^{\Sigma}\mathcal{L}_{E_K}^{\Sigma})$ in Λ.

As mentioned in the footnote in the introduction, this theorem is conditional in the following sense: our proof relies on a hypothesis that amounts to the existence of particular Galois representations associated to certain cuspforms on $GU(2,2)$. Recent work on the trace formula, particularly the so-called fundamental lemma, goes a long way towards establishing this hypothesis. See Remark 4.1.7 below for discussion of this point.

REMARK 3.4.3. The additional hypotheses (a) and (b) are used to compare various periods. Their roles in the proof are indicated in §4.2 below.

Combining these two theorems yields many instances of the Main Conjecture for elliptic curves. As an example of an easy-to-state consequence, we record the following.

THEOREM 3.4.4. *Suppose E is a semistable elliptic curve over $\mathbf{Q}$ and p is an odd prime at which E has good, ordinary reduction and for which $E[p]$ is an irreducible representation of $G_{\mathbf{Q}}$. Let Σ be any finite set of primes different from p.*

(i) *$I_E^{\Sigma} = (\mathcal{L}_E^{\Sigma})$ in $\Lambda \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$.*
(ii) *If $\bar{\rho} : G_{\mathbf{Q}} \to \mathrm{Aut}_{\mathbf{F}_p}(E[p])$ is surjective, then $I_E^{\Sigma} = (\mathcal{L}_E^{\Sigma})$ in Λ.*
(iii) *Conjecture* 3.1(iv) *holds provided Σ contains all primes different from p dividing the conductor N_E of E.*

(iv) $\operatorname{ord}_p(L(E,1)/\Omega_E) \leq \operatorname{ord}_p(c_E \cdot \#\mathrm{Sel}_p^{\mathrm{st}}(E))$ *with equality if* $c_E = 1$.

(v) *If* $L(E,1) = 0$ *then* $\operatorname{rank}_{\mathbf{Z}_p} \mathrm{Hom}_{\mathbf{Z}_p}(\mathrm{Sel}_p^{\mathrm{st}}(E), \mathbf{Q}_p/\mathbf{Z}_p) \geq 1$.

Remarks 3.4.5.

(a) If E is semistable then N_E is square-free, so if $\ell | N_E$ then $\ell || N_E$. Moreover, since E has good reduction at p and $N_E \neq 1$, there must be some prime dividing N_E. By work of Ribet it is known that for such an E and p, $E[p]$, if irreducible, can not be unramified at all primes different from p. So hypothesis (b) of Theorem 3.4.2 is always satisfied.

(b) To pass from Σ as in Theorem 3.4.2 to general Σ we make use of an argument of Greenberg based on Tate's duality theorems.

(c) To pass from the Main Conjecture to the equality of Conjecture 3.2.2(iv) we combine Proposition 3.3.2 with the observation, also due to Greenberg, that the map in (3.3.4) is an injection in the case under consideration.

(d) When $\operatorname{ord}_{s=1} L(E,s)$ is odd, the conclusion of part (v) follows from Nekovář's work on the parity conjecture [**N**] as well as from [**SU2**].

4. Eisenstein ideals for $GU(2,2)$ and Selmer groups for GL_2

4.1. The general set-up. We now replace the elliptic curve of §3 with a general eigenform $f \in S_k(N,\chi)$ of level N, weight $k \geq 2$, and character χ. Let $f = \sum_{n=1}^{\infty} a_n q^n$ be the Fourier expansion of f. We assume f is normalized so that $a_1 = 1$. We fix an odd prime p and assume that

$$p|N \quad \text{and} \quad |a_p|_p = 1. \tag{ord}$$

(That is, f is ordinary at p and even p-stabilized.) Write $N = N_0 p^r$, $p || N_0$, and write $\chi = \chi_0 \psi \omega_p^{2-k}$ with the conductor of χ_0 dividing N_0 and ψ of p-power order and of conductor p^{r+1}.

The form f is the specialization of an R-eigenform $\mathcal{F}$ for some integral domain R that is a finite $\mathbf{Z}_p[\![X]\!]$-algebra. That is, there is some $\mathcal{F} = \sum_{n=1}^{\infty} A_n q^n \in R[\![q]\!]$, $A_1 = 1$, such that if $\phi : R \to \bar{\mathbf{Q}}_p$ is any $\mathbf{Z}_p$-algebra homomorphism such that $\phi(1+X) = \zeta(1+p)^{m-2}$, $m \geq 2$ and ζ a p^rth root of unity, then $\phi(\mathcal{F}) = \sum_{n=1}^{\infty} \phi(A_n) q^n$ is the Fourier expansion of an eigenform of level $N_0 p^r$, weight m, and character $\chi_0 \psi_\zeta \omega_p^{2-m}$, and $f = \phi(\mathcal{F})$ for some such ϕ.

Let $\mathcal{X}$ be the set of $\mathbf{Z}_p$-homorphisms $\phi : R \to \bar{\mathbf{Q}}_p$ such that $\phi(1+X) = \zeta(1+p)^{m-2}$ for some $m \geq 2$ and some pth-power root of unity ζ. For each $\phi \in \mathcal{X}$ let $\mathcal{O}_\phi = \phi(R)$ and let F_ϕ be its field of fractions. Let $\rho_\phi : G_{\mathbf{Q}} \to \mathrm{GL}_2(F_\phi)$ be the usual p-adic representation associated to

the eigenform $\phi(\mathcal{F})$. It is well-known that ρ_ϕ stablizes a rank two $\mathcal{O}_\phi$-lattice. Let $\bar{\rho}$ be the absolute semi-simplification of the representation of $G_{\mathbf{Q}}$ on the reduction of such a lattice modulo the maximal ideal of $\mathcal{O}_\phi$. Up to isomorphism, this is independent of ϕ. (If f is the p-stabilized eigenform associated to an elliptic curve E, then $\bar{\rho}$ is the absolute semi-simplification of the $G_{\mathbf{Q}}$-representation on $E[p]$). To simplify matters we will assume that

(irr) $\qquad\qquad \bar{\rho}$ is irreducible.

We will also assume that for some $\sigma_0 \in D_p$

(dist) $\qquad\qquad \bar{\rho}(\sigma_0)$ has distinct eigenvalues.

One consequence of (irr) is that there is a continuous representation $\rho_{\mathcal{F}} : G_{\mathbf{Q}} \to \mathrm{GL}_2(R)$ such that composition with $\phi \in \mathcal{X}$ yields ρ_ϕ. A consequence of (ord) and (dist) is that

$$\rho_{\mathcal{F}}|_{D_p} \cong \begin{pmatrix} \Psi_1 & * \\ & \Psi_2 \end{pmatrix}, \quad \Psi_2|_{I_p} = 1, \Psi_2(\mathrm{Frob}_p) = A_p. \tag{4.1.1}$$

Now let K be an imaginary quadratic field in which p splits. Let K_∞/K be the compositum of all $\mathbf{Z}_p$-extensions of K. Then $H = \mathrm{Gal}(K_\infty/K) \cong \mathbf{Z}_p^2$. Let c denote the non-trivial element in $\mathrm{Gal}(K/\mathbf{Q})$. Then c acts on H by conjugation, and we have $H = H^+ \oplus H^-$, with c acting on $H^\pm$ by ± 1. Then $H/H^- \cong \Gamma$ (i.e, $K_\infty^{H^-} = K \cdot \mathbf{Q}_\infty$). Let $\gamma^\pm$ be a topological generator of $H^\pm$. Let $\Lambda_K = \mathbf{Z}_p[\![H]\!]$ and let $\Phi : G_K \to \Lambda_K^\times$ be the projection $G_K \twoheadrightarrow H$. Given a pair of pth-power roots of unity $\underline{\zeta} = (\zeta_-, \zeta_+)$, let $\psi_{\underline{\zeta}} : G_K \to \bar{\mathbf{Q}}^\times$ be the finite order character obtained by composing the projection $G_K \twoheadrightarrow H$ with the character $H \to \bar{\mathbf{Q}}^\times$ sending $\gamma^\pm$ to $\zeta_\pm$.

We associate a Selmer group $\mathrm{Sel}^\Sigma(\phi, \underline{\zeta})$ to each $\phi \in \mathcal{X}$, each character $\psi_{\underline{\zeta}}$, and each finite set Σ of finite places of K not dividing p. This is defined essentially just as we defined $\mathrm{Sel}_p^\Sigma(E, \psi)$ in §3.1. We leave the details to the assiduous readers; the definition is also easily extracted from the next paragraph.

Let $B = R \otimes_{\mathbf{Z}_p} \Lambda_K = R[\![H]\!]$ and let $B^\vee = \mathrm{Hom}_{\mathrm{cts}}(B, \mathbf{Q}_p/\mathbf{Z}_p)$. Let $\mathcal{T}$ be the rank two free R-module underlying $\rho_{\mathcal{F}}$ and let $\mathcal{T}^+ \subset \mathcal{T}$ be the rank one R-summand on which D_p acts via the character Ψ_1 in (4.1.1). Let $\mathcal{M} = \mathcal{T} \otimes_R B^\vee$ and $\mathcal{M}^+ = \mathcal{T}^+ \otimes_R B^\vee$. Let $\Psi : G_K \to \mathbf{Z}_p[[X]]^\times$ be the character such that $\gamma^+ \mapsto 1 + X$ and $\gamma^- \mapsto 1$. Let G_K act on $\mathcal{M}$ via $\Psi^{-1}\rho_{\mathcal{F}} \otimes \Phi$. Let Σ be a finite set of finite places of K not dividing

p. Let

$$\mathrm{Sel}^{\Sigma}(\mathcal{M}) = \ker\Big\{ H^1(G_K, \mathcal{M}) \\ \to \prod_{v|p} H^1(I_v, \mathcal{M}/\mathcal{M}^+) \times \prod_{w\nmid p, w\notin\Sigma} H^1(I_v, \mathcal{M})\Big\}.$$

These Selmer groups can be related to the others. Given $\phi \in \mathcal{X}$ and $\underline{\zeta} = (\zeta_-, \zeta_+)$, let $\tau = \tau(\phi, \underline{\zeta}) : B \to \bar{\mathbf{Q}}_p$ be the unique $\mathbf{Z}_p$-homomorphism agreeing with ϕ on R and sending $\gamma_\pm$ to $\zeta_\pm$. Let $\mathfrak{p}_\tau$ be the kernel of τ.

Proposition 4.1.2. *Suppose p is an odd prime and assume that* (ord)*,* (irr)*, and* (dist) *hold. Suppose Σ is a finite set of finite places of K not dividing p that contains all such that divide N_0.*

(i) *If $\tau = \tau(\phi, \underline{\zeta})$ then $\mathrm{Sel}^{\Sigma}(\phi, \underline{\zeta}) = \mathrm{Sel}^{\Sigma}(M)[\mathfrak{p}_\tau]$.*

(ii) *Suppose $\phi \in \mathcal{X}$ is such that $\phi(\mathcal{F})$ is the p-stabilization of an eigenform associated to an elliptic curve E. Let $\mathcal{O} = \phi(R)$ and let $\eta : B \twoheadrightarrow \mathcal{O}[\![T]\!]$ be the unique map that agrees with ϕ on R and sends S to 0. Let $\mathfrak{p}_\eta$ be the kernel of η. If $c\Sigma = \Sigma$ and Σ also contains all the ramified places of K, then*

$$\mathrm{Sel}^{\Sigma}(M_E) \otimes_{\mathbf{Z}_p} \mathcal{O} = \mathrm{Sel}^{\Sigma}(\mathcal{M})[\mathfrak{p}_\eta]^+ \qquad \text{and}$$
$$\mathrm{Sel}^{\Sigma}(M_{E_K}) \otimes_{\mathbf{Z}_p} \mathcal{O} = \mathrm{Sel}^{\Sigma}(\mathcal{M})[\mathfrak{p}_\eta]^-,$$

where the superscript $\pm$ denotes the ± 1-eigenspace for the action on $\mathrm{Sel}^{\Sigma}(\mathcal{M})$ of the non-trivial automorphism $c \in \mathrm{Gal}(K/\mathbf{Q})$.

Let $S^{\Sigma}(\mathcal{M}) = \mathrm{Hom}_{\mathbf{Z}_p}(\mathrm{Sel}^{\Sigma}(\mathcal{M}), \mathbf{Q}_p/\mathbf{Z}_p)$. This is a finite B-module. Since B is a Krull-domain we can associate to $S^{\Sigma}(\mathcal{M})$ a divisor $\mathcal{S}^{\Sigma}(\mathcal{M})$ defined as

$$\mathcal{S}^{\Sigma}(\mathcal{M}) = \sum_P \ell_P(S^{\Sigma}(\mathcal{M})_P) \cdot P,$$

where P runs over the height one primes of B and $\ell_P(\cdot)$ denotes the B_P-length. Then the general Main Conjecture for $\mathrm{Sel}^{\Sigma}(\mathcal{M})$ identifies $\mathcal{S}^{\Sigma}(\mathcal{M})$ with the divisor of some p-adic L-function. In particular, it is known that - at least under the hypothesis (ord) - there exists an element $\mathcal{L}^{\Sigma}_{\mathcal{F},K} \in B$ such that if $\tau = \tau(\phi, \underline{\zeta})$, $\phi(1+X) = \xi(1+p)^{m-2}$, then

$$\tau(\mathcal{L}^{\Sigma}_{\mathcal{F},K}) = a(\phi, \underline{\zeta}) L^{\Sigma}(\phi(\mathcal{F}), \omega_p^{m-2}\psi_{(\xi\zeta_+, \zeta_-)}, m-1), \tag{4.1.3}$$

where $a(\phi, \underline{\zeta})$ is an interpolation factor that is essentially

$$\text{period} \times \text{Gauss sum} \times \text{factor like that in (3.2.1)}.$$

The p-adic L-function $\mathcal{L}^{\Sigma}_{\mathcal{F},K}$ is known to interpolate L-values of each $\phi(\mathcal{F})$ at points other than $m-1$, but we do not pursue that point in this

paper. The important fact is that under the hypotheses of Proposition 4.1.2(ii)

$$\eta(\mathcal{L}^{\Sigma}_{\mathcal{F},K}) = \mathcal{L}^{\Sigma}_{E}\mathcal{L}^{\Sigma}_{E_K}. \tag{4.1.4}$$

We can formulate a Main Conjecture in the spirit of Conjecture 3.3.6.

Conjecture 4.1.5.
If (ord) *and* (irr) *hold, then* $\mathcal{S}^{\Sigma}(\mathcal{M}) = \mathrm{div}_B(\mathcal{L}^{\Sigma}_{\mathcal{F},K})$.

Among the results we prove in the direction of this conjecture is the following theorem.

Theorem 4.1.6 (Skinner-Urban [**SU1**]). *Suppose p is an odd prime and assume* (ord) *and* (irr) *hold. Suppose also that*

(a) $\chi_0 = 1$,
(b) *there exists $\ell || N_0$, $\ell \neq p$ and ℓ unramified in K, such that $\bar{\rho}$ is ramified at ℓ.*

Then $\ell_P(S^{\Sigma}(\mathcal{M})_P) \geq \mathrm{ord}_P(\mathcal{L}^{\Sigma}_{\mathcal{F},K})$ for all height one primes P of B.

Remarks 4.1.7.

(1) Theorem 3.4.2 follows from Theorem 4.1.6 and Proposition 4.1.2, essentially by a simple argument involving Fitting ideals.
(2) This result and others like it can also be combined with those of Bertollini and Darmon [**BD**] to deduce many instances of the anticyclotomic Main Conjecture for an elliptic curve and even two- and three-variable 'main conjectures'.
(3) As indicated in the footnote in the introduction, this theorem is conditional on the existence of certain p-adic Galois representations associated to certain irreducible, cuspidal automorphic representations π of $GU(2,2)$. In particular we need to have that if the infinity component π_∞ of π is a holomorphic discrete series (very regular weights suffice) and if for a prime p that splits in K, the p-component π_p is unramified and (nearly) ordinary, then there exists a four-dimensional p-adic Galois representation $\rho_\pi : G_K \to \mathrm{GL}_4(\bar{\mathbf{Q}}_p)$ such that
    - ρ_π is unramified away from the primes dividing p, the discriminant of K, and the primes at which π is ramified;
    - $\rho_\pi|_{D_v}$ is ordinary for each $v|p$ (and suitably compatible with π_p);
    - for all but finitely many unramified degree one primes w of K, the local L-function $L(\rho_\pi|_{D_w}, s)$ is a shift (depending on the weight of π) of the local L-factor at w of the standard L-function of π.

The existence of these ρ_π's has long been conjectured; however, it is not completely known. Recent progress on the trace formula, especially fundamental lemmas for unitary groups, goes a long way towards establishing this existence. The existence of four-dimensional representations is complicated by the fact that the representations expected to occur in the cohomology of the Shimura variety associated to $GU(2,2)$ are six-dimensional (should be the $\wedge^2\rho_\pi$'s). Existence of the ρ_π's and related properties will be discussed more fully in [**SU1**] and its companion papers. The role such representations play in the proof of Theorem 4.1.6 is indicated in Step 5 of §4.2. In the application it is also necessary to know that the ρ_π's that arise are irreducible; this is proved as needed.

4.2. The proof, very briefly. The proof of Theorem 4.1.6 follows the strategy outlined in §2.5. Roughly, this plays out as follows:

Step 1. We begin by associating to each $\phi \in \mathcal{X}$ and $\underline{\zeta}$ an Eisenstein series $E(\phi, \underline{\zeta})$ whose constant terms are multiplies of the L-values on the right-hand side of (4.1.3). This Eisenstein series is a holomorphic modular form on the Hermitian upper half-space of degree two with p-adic integral Fourier coefficients. In fact, there exists a formal q-expansion $\mathcal{E} = \sum_{t\geq 0} C_t q^t \in B[\![q^t]\!]$, with t running over a lattice of positive semi-definite Hermitian matrices in $M_2(K)$, such that if $\tau = \tau(\phi, \underline{\zeta})$ then $\tau(\mathcal{E}) = \sum \tau(C_t) q^t$ is the q-expansion of $E(\phi, \underline{\zeta})$. Moreover, each of the 'singular' fourier coefficients C_t (i.e., $\det(t) = 0$) is a multiple of $\mathcal{L}^{\Sigma}_{\mathcal{F},K}$. The existence of $\mathcal{E}$ and the integrality of the $E(\phi, \underline{\zeta})$'s follow from the 'pull-back' formulas of Shimura and from the hypothesis (ord), (irr). (The choices we make also ensure that $\mathcal{E}$ is p-ordinary.)

Step 2. Next we prove that for some pair $\phi, \underline{\zeta}$, some Fourier coefficient of $E(\phi, \underline{\zeta})$ is a p-adic unit. This is done by first calculating some Fourier coefficients, which turn out to be special values of Rankin-Selberg convolution L-functions of $\phi(\mathcal{F})$ and four-variable theta series associated to the Hermitian matrices t. Using hypthesis (b) of Theorem 4.1.6 together with (ord) and (irr) and results of Vatsal [**V**] we prove that one of these L-values is a unit. It then follows that some Fourier coefficient C_t of $\mathcal{E}$ lies in $B^\times$.

Step 3. Let $P \subset B$ be a height-one prime and let $r = \operatorname{ord}_P(\mathcal{L}^{\Sigma}_{\mathcal{F},K})$. From Step 1 and the theory of ordinary p-adic modular forms (as developed by Hida) we then show that there is a cuspform $\mathcal{G}_P \in B[\![q^t]\!]$ such that if $\mathcal{G}_P = \sum_{t>0} H_t q^t$ then

$$H_t \equiv C_t \bmod P^r. \tag{4.2.1}$$

That $\mathcal{G}_P$ is a cuspform means that for almost all $\tau = \tau(\phi, \zeta)$, $\tau(\mathcal{G}_P) = \sum \tau(H_t) q^t$ is a cuspform on the Hermitian upper half-space of degree two. (Under our hypotheses it is possible to prove the existence of $\mathcal{G}_P$

without recourse to the theory of Hida, but in general such a theory is probably needed, especially to deal with 'μ-invariants'.)

Step 4. We let $\mathbb{T}$ be the B-algebra generated by the action of the Hecke operators on a certain space of (p-ordinary) cuspforms in $B[\![q^t]\!]$ (this space depends on the many choices in the definition of $\mathcal{E}$; it contains each $\mathcal{G}_P$). This is a finite, reduced, torsion-free B-algebra. Let $J_{\mathcal{F}}^{\Sigma} \subseteq \mathbb{T}$ be the ideal generated by the Hecke relations annihilating $\mathcal{E}$ (these are therefore related to the coefficients of $\mathcal{F}$). From Step 2 and (4.2.1) we deduce that for any height one prime P of B

$$\ell_P((\mathbb{T}/J_{\mathcal{F}}^{\Sigma})_P) \geq \mathrm{ord}_P(\mathcal{L}_{\mathcal{F},K}^{\Sigma}). \tag{4.2.2}$$

This is sometimes referred to as an 'Eisenstein ideal' result. The inequality (4.2.2) is easily deduced from the observation that (4.2.1) implies there is a B-algebra surjection

$$\mathbb{T}_P/J_{\mathcal{F}}^{\Sigma}\mathbb{T}_P \twoheadrightarrow B_P/P^r B_P \tag{4.2.3}$$

given as follows. Let t_0 be such that $C_{t_0} \in B^{\times}$. Then the map (4.2.3) sends the hecke operator $h \in \mathbb{T}$ to $C_{t_0}^{-1} \times$ (the t_0th-Fourier coefficient of $h \cdot \mathcal{G}_P$) modulo P^r.

Step 5. This is an involved step. Using Galois representations associated to holomorphic eigenforms for the Hermitian upper half-space of degree two we construct, for each prime P as in the statement of Theorem 4.1.6, a B-submodule $S(P) \subseteq \mathrm{Sel}^{\Sigma}(\mathcal{M})$ such that its dual $S(P)^{\vee} = \mathrm{Hom}_{\mathbf{Z}_p}(S(P), \mathbf{Q}_p/\mathbf{Z}_p)$ satisfies $\ell_P(S(P)_P^{\vee})) \geq \ell_P((\mathbb{T}/J_{\mathcal{F}}^{\Sigma})_P)$. Combining this with (4.2.2) then yields Theorem 4.1.6.

The spirit of this step can be sketched as follows. Let P and r be as in Step 3. If $r \geq 1$, then (4.2.2) implies that there exists a finite, integrally closed extension B' of B, a prime $P' \subset B'$ extending P, and a cuspidal B'-eigenform $\mathcal{G}$ such that the hecke eigenvalues of $\mathcal{G}$ are congruent modulo P' to those $\mathcal{E}$. To simplify notation, we will assume $B' = B$ and $P' = P$. Let $k_P = B_P/PB_P$. Then, assuming the existence of the (conjectured) four-dimensional G_K-representations associated to the specializations $\tau(\mathcal{G})$, $\tau = \tau(\phi, \underline{\zeta})$, and the generic irreducibility of these representations, one can deduce the existence of a representation

$$\rho_P : G_K \to \mathrm{GL}_4(k_P), \quad \rho_P = \begin{pmatrix} \Phi^c\chi_{0\epsilon} & *' & *'' \\ 0 & \rho_{\mathcal{F}} & * \\ 0 & 0 & \Psi\Phi^{-1} \end{pmatrix}$$

that is unramified away from the primes above p and the places in Σ and is such that $\rho_P|_{D_p}$ is split but the quotient representation

$$\rho_P' = \begin{pmatrix} \rho_{\mathcal{F}} & * \\ 0 & \Psi\Phi^{-1} \end{pmatrix}$$

is not. From the existence of ρ_P' it is not difficult to deduce that $\ell_P(S^{\Sigma}(\mathcal{M})) \geq 1$.

4.3. More on the Eisenstein series. We conclude by indicating the definition of the Eisenstein series used in the above argument.

Let $\mathcal{O}_K$ be the ring of integers of the imaginary quadratic field K. For $n \geq 1$ an integer, let

$$J_n = \left(\begin{smallmatrix} & I_n \\ -I_n & \end{smallmatrix} \right)$$

and let G_n be the $\mathbf{Z}$-group scheme such that for any $\mathbf{Z}$-algebra A

$$G_n(A) = \{g \in \mathrm{GL}_{2n}(\mathcal{O}_K \otimes A) \ : \ gJ_n{}^t\bar{g} = \lambda_g J_n, \lambda_g \in A^\times\}.$$

Then $G_n(\mathbf{R})$ is the group usually denoted $GU(n,n)$. Let $G_n^+ = \{g \in G_n(\mathbf{R}) \ : \ \lambda_g > 0\}$.

Let P_n be the parabolic subgroup of G_n such that $P_n = L_n R_n$ with

$$L_n(A) = \left\{ \begin{pmatrix} a & & b & \\ & * & & \\ c & & d & \\ & & & x \end{pmatrix} \ : \ x \in (\mathcal{O}_K \otimes A)^\times, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in G_{n-1}(A) \right\}$$

its Levi component and R_n its unipotent radical. We identifiy $L_n = Res_{\mathcal{O}_K/\mathbf{Z}}\mathbf{G}_m \times G_{n-1}$ in the obvious way.

Let $\mathbf{H}_n = \{Z \in M_n(\mathbf{C}) \ : \ -i(Z - {}^t\bar{Z}) > 0\}$ be the Hermitian upper half-space of degree n. Then G_n^+ acts on $\mathbf{H}_n$ in the usual way:

$$g(Z) = (AZ + B)(CZ + D)^{-1}, \quad g = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix} \right), \quad A, B, C, D \in M_n(\mathbf{C}).$$

Also, for $g \in G_n^+(\mathbf{R})$ as above and $Z \in \mathbf{H}_n$, let $j_n(g, Z) = \det(CZ + D)$.

A holomorphic automorphic form of weight k on $\mathbf{H}_n$ with respect to a conguence subgroup $\Gamma \in G_n(\mathbf{Z})$ is a holomorphic function $F : \mathbf{H}_n \to \mathbf{C}$ such that

(i) $F(\gamma(Z)) = j_n(\gamma, Z)^k F(Z)$ for all $\gamma \in \Gamma$ and
(ii) for each $\sigma \in G_n(\mathbf{Q})$, $F|_k\sigma = j_n(\sigma, Z)^{-k} F(\sigma(Z))$ has a Fourier expansion

$$F|_k\sigma = \sum_{T \geq 0} c_\sigma(T) e(\mathrm{trace}\,(TZ)),$$

with T running over a lattice in the space of positive semi-definite Hermitian matrices in $M_n(K)$. (So F is a cuspform if $c_\sigma(T) = 0$ whenever $\det(T) = 0$.)

When $n = 2$ we drop it from our notation.

The connection to modular forms on GL_2 comes in the following way. There is an exact sequence

$$1 \to \mathbf{A}^\times \to \mathbf{A}_K^\times \times \mathrm{GL}_2(\mathbf{A}) \to G_1(\mathbf{A}) \to 1,$$

with the second arrow being the map $a \mapsto (a^{-1}, aI_2)$ and the third being $(a, A) \mapsto aA$. So given our classical eigenform f we associate to

it a function $\varphi : \mathrm{GL}_2(\mathbf{A}) \to \mathbf{C}$ in the usual way. Then given a Hecke character ψ of $\mathbf{A}_K^\times$ such that

$$\psi|_{\mathbf{A}^\times} = \chi \quad \text{and} \quad \psi_\infty(z) = (z/|z|)^{-k},$$

where χ is the character of f (equivalently, the central character of the automorphic representation of $\mathrm{GL}_2(\mathbf{A})$ generated by φ), we can associate to ψ and φ a function φ_ψ on $G_1(\mathbf{A})$: $\varphi_\psi(aA) = \psi(a)\varphi(A)$, $a \in \mathbf{A}_K^\times$, $A \in \mathrm{GL}_2(\mathbf{A})$. Given another Hecke character τ of $\mathbf{A}_K^\times$ such that $\tau_\infty(z) = (z/|z|)^{-k}$ we associate to the triple (τ, ψ, φ) a function $\Phi = \Phi_{\tau,\psi,\varphi}$ on $L(\mathbf{A})$: $\Phi(x, aA) = \tau(x)\psi(a)\varphi(A)$, $(x, aA) \in L_n(\mathbf{A})$.

Suppose now that $\delta = \delta_P$ is the usual modulus character of G associated to P. To define our Eisenstein series we make a choice of an an extension of Φ to G so that

$$\Phi(gw) = j(w, i)^{-k}\Phi(g), \quad w \in SU^+(2, 2).$$

Then we consider

$$E(g, s) = E(f, \tau, \psi; g, s) = \sum_{\gamma \in P(\mathbf{Q})\backslash G(\mathbf{Q})} \Phi(\gamma g)\delta(\gamma g)^{(1/2+s)/3}.$$

From this we obtain a classical, holomorphic automorphic form on the Hermitian half-space of degree 2 by setting

$$E(Z) = j(g, i)^k \lambda_g^{-k} E(g, (k-3)/2), \quad g \in G^+(\mathbf{R}),\ Z = g(i).$$

That the constant terms of $E(Z)$ involve the L-values of interest can be deduced from Langlands' general theory [**L**].

References

[BD] M. Bertolini and H. Darmon, *Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbf{Z}_p$-extensions*, Ann. of Math. (2) **162**(**1**) (2005), 1–64.

[C] P. Colmez, *La conjecture de Birch et Swinnerton-Dyer p-adique*, Astérisque, **294** (2004), 251–319.

[G1] R. Greenberg, *Iwasawa theory for p-adic representations*, Algebraic number theory, 97–137, Adv. Stud. Pure Math., **17**, Academic Press, Boston, MA, 1989.

[G2] R. Greenberg, *Iwasawa theory for motives*, in 'L-functions and arithmetic' (Durham, 1989), 211–233, London Math. Soc. Lecture Note Ser., **153**, Cambridge Univ. Press, Cambridge, 1991.

[GV] R. Greenberg and V. Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142**(**1**) (2000), 17–63.

[K] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, in 'Cohomologies p-adiques et applications arithmétiques. III', Astérisque **295** (2004), 117–290.

[L] R.P. Langlands, *Euler Products*, Yale University Press, 1971.

[MSD] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76**(**2**) (1984), 179–330.

[N] J. Nekovář, *On the parity of ranks of Selmer groups*, II, C.R. Acad. Sci. Paris Sér. I Math. **332**(**2**) (2001), 99–104.

[R] K. Ribet, *A modular construction of unramified p-extensions of* $\mathbf{Q}(\mu_p)$, Invent. Math. **34**(**3**) (1976), 151–162.

[Ru] K. Rubin, *Euler systems and modular elliptic curves*, in 'Galois Representations in Arithmetic Algebraic Geometry' (Durham, 1996), 351–367, London Math. Soc. Lecture Note Ser., **254**, Cambridge Univ. Press, Cambridge, 1998.

[S] A.J. Scholl, *An introduction to Kato's Euler systems*, in 'Galois Representations in Arithmetic Algebraic Geometry' (Durham, 1996), 379–460, London Math. Soc. Lecture Note Ser., **254**, Cambridge Univ. Press, Cambridge, 1998.

[SU1] C. Skinner and E. Urban, in progress.

[SU2] C. Skinner and E. Urban, *Sur les déformations p-adiques de certaines représentations automorphes*, to appear in J. Inst. Math. Jussieu.

[V] V. Vatsal, *Special values of anticyclotomic L-functions*, Duke Math. J. **116**(**2**) (2003), 219–261.

[W] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. (2) **131**(**3**) (1990), 493–540.

Department of Mathematics, University of Michigan, 2074 East Hall, 530 Church Street, Ann Arbor, MI 48109-0335
E-mail address: cskinner@umich.edu