Contemporary Mathematics
Volume 165, 1994

On the Conjecture of Mazur, Tate, and Teitelbaum

RALPH GREENBERG AND GLENN STEVENS

§0. Introduction

Let E be an elliptic curve defined over $\mathbf{Q}$. Assuming that E is modular and has stable reduction modulo a given prime p, one can associate to E a p-adic L-function $L_p(E,s)$. If E has split multiplicative reduction at p then the interpolation property defining $L_p(E,s)$ implies that $L_p(E,1)=0$. This is an example of a so-called trivial zero—the vanishing is forced by the Euler-like factor that arises in the interpolation property. In this article, we will sketch a proof of a formula for $L_p'(E,1)$ which was discovered experimentally by Mazur, Tate, and Teitelbaum [**Mz-T-T**]. To make the idea behind the proof transparent, we will make several simplifying assumptions. The proof in general is given in [**G-S**], covering also the p-adic L-function attached to any normalized newform of weight 2 for $\Gamma_1(Np)$ ($p \nmid N$) whose pth Fourier coefficient is equal to 1. In §5 we will show how Hida theory and the results of §2 can be used to prove a special case of Ribet's "lowering the conductor theorem".

Define the $\mathcal{L}$-invariant $\mathcal{L}_p(E)$ by

$$\mathcal{L}_p(E) = \frac{\log_p(q)}{\operatorname{ord}_p(q)} \tag{0.1}$$

where $q \in \mathbf{Q}_p^\times$ is any element ($\neq 1$) in the kernel of Tate's uniformization

$$\lambda\colon \overline{\mathbf{Q}}_p^\times \longrightarrow E(\overline{\mathbf{Q}}_p).$$

Here $\log_p\colon \mathbf{Q}_p^\times \to \mathbf{Z}_p$ is the usual p-adic logarithm on $\mathbf{Z}_p^\times$, extended to $\mathbf{Q}_p^\times$ by the convention $\log_p(p)=0$, and $\operatorname{ord}_p\colon \mathbf{Q}_p^\times \to \mathbf{Z}$ is the normalized valuation. Since $\ker(\lambda)$ is infinite cyclic, the definition (0.1) is independent of q. The main result is the following.

1991 *Mathematics Subject Classification.* Primary 11F67; Secondary 11G40.
Supported in part by grants from the National Science Foundation.

This paper is in final form and no version of it will be submitted for publication elsewhere.

the theorem is equivalent to the assertion that

$$\alpha_p'(2) = -\frac{1}{2}\mathcal{L}_p(E). \tag{0.2}$$

The key to the proof of (0.2) is that $\mathcal{L}_p(E)$ can be described in terms of the representation space $V(E) = Ta_p(E) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ of the local Galois group $G_{\mathbf{Q}_p}$ and that there exists an analytic family V_k of 2-dimensional representations of $G_{\mathbf{Q}}$ (and hence of $G_{\mathbf{Q}_p}$) parameterized by the p-adic variable k in a neighborhood of 2, which specializes at $k = 2$ to $V_2 = V(E)$. For arbitrary k, $\alpha_p(k)$ is the eigenvalue of Frobenius acting on the (1-dimensional) unramified quotient of V_k.

The first examples of two-variable p-adic L-functions were constructed by Manin and Vishik [**M1, M2, M-V**] as a p-adic analogue of Hecke L-functions associated to an imaginary quadratic field K. A more precise version, in this case, is provided by Katz's two-variable p-adic L-function [**Kz**]. The two variables correspond to the possible "infinity types" for grossencharacters of K. If the elliptic curve E has complex multiplication, then the p-adic L-function with properties (i), (ii), (iii) above can be obtained as a special case of Katz's p-adic L-function. In this case $\alpha_p(k)$ can be described quite precisely. Essentially it is just the $(k-1)$st power of the p-adic unit eigenvalue α_p for E. If E has split multiplicative reduction at p, then $j(E)$ is not integral and so E is not a CM elliptic curve. Nevertheless, based on Hida's construction of p-adic families of ordinary modular forms, one can associate to any modular elliptic curve E which is ordinary (in the sense that the p-th Fourier coefficient of the corresponding modular form f_E is a p-adic unit) a two-variable p-adic L-function with the properties (i), (ii), (iii) above. However, without the simplifying assumptions stated below, we can only assume analyticity in (k, s) for k in some neighborhood of 2. This is, of course, sufficient for the argument outlined above. The existence of such two-variable p-adic L-functions was first proved by Mazur in some cases [**Mz**] and more generally by Kitagawa [**Ki**]. Though we cannot describe $\alpha_p(k)$ explicitly, its characterization as the eigenvalue of Frobenius on the unramified quotient of the Galois representation V_k is enough information to verify (0.2).

We want to mention one other case of a trivial zero. The Kubota-Leopoldt p-adic L-function $L_p(\psi, s)$ associated to a Dirichlet character ψ (with values in $\overline{\mathbf{Q}}_p$) satisfies the property $L_p(\psi, 0) = (1 - \psi_1(p))L_\infty(\psi_1, 0)$ where $\psi_1 = \psi w^{-1}$. Now assume that we have trivial zero, i.e. that $\psi_1(p) = 1$ so that $L_p(\psi, 0) = 0$. A formula for $L_p'(\psi, 0)$ is derived in [**F-G**]. It seems likely that one can give a proof of this result by again making use of a two-variable p-adic L-function. The idea is similar, though the details (which we have not carried out) are more involved. Let K be an imaginary quadratic field in which p splits, chosen so that $K \cap K_{\psi_1} = \mathbf{Q}$ where K_{ψ_1} is the cyclic extension of $\mathbf{Q}$ cut out by ψ_1, regarded now as an Artin character. One considers the branch of Katz's two-variable p-adic L-function which includes in its domain of definition the character $\psi_1|_{G_K} = \psi_{1,K}$. This p-adic L-function vanishes at $\psi_{1,K}$. We normalize the p-adic variables (k, s) so that $\psi_{1,K}$ corresponds to $(k, s) = (0, 0)$. In the "cyclotomic" direction, $L_p(k, s)$ should

THEOREM. *Let p be a prime ≥ 5 and let E be a modular elliptic curve with split multiplicative reduction at p. Then*

$$L_p'(E,1) = \mathcal{L}_p(E)\frac{L_\infty(E,1)}{\Omega_E}.$$

Here $L_\infty(E,z)$ is the Hasse-Weil L-function of E/Q and Ω_E is the positive Neron period of E.

Let ϕ be any quadratic Dirichlet character and let E_ϕ denote the corresponding quadratic twist of E. If $\phi(p) = 1$, then $E_\phi \cong E$ over $\mathbf{Q}_p$ and hence E_ϕ also has split multiplicative reduction at p and $\mathcal{L}_p(E_\phi) = \mathcal{L}_p(E)$. By a theorem of Waldspurger, $L_\infty(E_\phi, 1) \neq 0$ for infinitely many such ϕ's. So we could, alternatively, define the $\mathcal{L}$-invariant $\mathcal{L}_p(E)$ to be the ratio $L_p'(E_\phi,1)/(L_\infty(E_\phi,1)/\Omega_{E_\phi})$ for any ϕ satisfying $\phi(p) = 1$ and $L_\infty(E_\phi,1) \neq 0$—assuming, of course, that this ratio is independent of the choice of ϕ.

Here is an outline of the rather simple idea behind the proof. Let $\epsilon_\infty = \pm 1$ denote the sign in the functional equation for $L_\infty(E,z)$. Assuming that E has split multiplicative reduction at p, $L_p(E,s)$ satisfies the functional equation

$$L_p(E,2-s) = \epsilon_p \langle N\rangle^{s-1} L_p(E,s)$$

where $\epsilon_p = -\epsilon_\infty$, N is the conductor of E and $\langle N\rangle = N\omega^{-1}(N)$ where ω is the Teichmüller character. If $\epsilon_\infty = -1$, then $\epsilon_p = +1$ and the above theorem is obvious. Both sides are zero. So we may assume that $\epsilon_p = -1$. One can construct a "two-variable" p-adic L-function $L_p(k,s)$ associated to E, which is defined and analytic for all $s \in \mathbf{Z}_p$ and for all k in some neighborhood of 2 in $\mathbf{Z}_p$. This p-adic L-function satisfies several properties:

(i) $L_p(2,s) = L_p(E,s)$ for all $s \in \mathbf{Z}_p$;

(ii) $L_p(k,k-s) = \epsilon_p\langle N\rangle^{s-\frac{1}{2}k} L_p(k,s)$;

(iii) $L_p(k,1) = \left(1-\alpha_p(k)^{-1}\right)L_p^*(k)$ where $L_p^*(k)$ is a p-adic analytic function of k such that $L_p^*(2) = L_\infty(E,1)/\Omega_E$.

We will describe the function $\alpha_p(k)$ below. We just point out here that $\alpha_p(k)$ is an analytic function of k and $\alpha_p(2) = 1$. Thus (iii) implies that $\dfrac{\partial L_p}{\partial k}(2,1) = \alpha_p'(2)\dfrac{L_\infty(E,1)}{\Omega_E}$. Also, since we have assumed $\epsilon_p = -1$, (ii) implies that $L_p(k,s)$ vanishes identically along the line $s = k/2$ and therefore the derivative at $(k,s) = (2,1)$ in that direction is certainly zero. Hence, if we can compute $\alpha_p'(2)$, then we can find all the directional derivatives for $L_p(k,s)$ at $(k,s) = (2,1)$. In particular, we will obtain a new expression for $\dfrac{\partial L_p}{\partial s}(2,1)$ which, by (i), we already know is equal to $L_p'(E,1)$. To be precise, the linear terms in the Taylor expansion at $(k,s) = (2,1)$ will be of the form $c(-\frac{1}{2}(k-2)+(s-1))$ where $c = -2\alpha_p'(2)L_\infty(E,1)/\Omega_E$. We have $L_p'(E,1) = c$ and therefore the formula in factor as a product of two Kubota-Leopoldt p-adic L-functions, one of which is $L_p(\psi, s)$. This has been proved by B. Gross under a certain restrictive hypothesis. Calculating the derivative in this direction and using a formula of Leopoldt involving cyclotomic units for the other factor would yield the value of $L'_p(\psi, 0)$. There is a "weight" direction in which one has a factorization analogous to property (iii) above, as mentioned in the previous paragraph. One can calculate the derivative in this direction since $\alpha_p(k)$ is simply a power of some fixed $\alpha \in 1+p\mathbf{Z}_p$ and the value at $k = 0$ of $L^*_p(k)$ comes from a formula of Katz involving elliptic units. One must then determine the direction in which the linear term at $(k, s) = (0, 0)$ vanishes. Now a theorem of Rubin (the so-called two-variable Main Conjecture) allows one to relate the above branch of Katz's p-adic L-function to a characteristic ideal of a certain Galois group, which is an Iwasawa module for $\mathrm{Gal}(\tilde{K}_\infty/K)$ where $\tilde{K}_\infty$ is the composite of the $\mathbf{Z}_p$-extensions of K: $\mathrm{Gal}(\tilde{K}_\infty/K) \cong \mathbf{Z}_p^2$. But it turns out that one can identify the direction where the linear term vanishes for the generator of the characteristic ideal and hence for Katz's p-adic L-function. As an example, assume that ψ_1 has values in $\mathbf{Z}_p^\times$. Then there is a certain $\mathbf{Z}_p$-extension of KK_{ψ_1} in which $\mathrm{Gal}(KK_{\psi_1}/K)$ acts by $\psi_{1,K}$. Since p splits in the extension $KK_{\psi_1}/\mathbf{Q}$, this determines a certain $\mathbf{Z}_p$-extension of $\mathbf{Q}_p$. In defining Katz's p-adic L-function, one chooses one of the two primes of K over p. By completing K at the other prime, the $\mathbf{Z}_p$-extension of $\mathbf{Q}_p$ determines a certain $\mathbf{Z}_p$-extension of K itself. By a genus theoretic argument, one can prove this $\mathbf{Z}_p$-extension corresponds to the direction in which the $\psi_{1,K}$-branch of Katz's p-adic L-function has at least a double zero.

Notation.

In the following, p will denote a rational prime. As in the work of Hida [**H1**, **H2**] we will often add the technical hypothesis $p \geq 5$. We let $\overline{\mathbf{Q}}$ denote the field of algebraic numbers in $\mathbf{C}$ and let $\overline{\mathbf{Q}}_p$ be a fixed algebraic closure of $\mathbf{Q}_p$. We also fix once and for all an embedding

$$\overline{\mathbf{Q}} \subseteq \overline{\mathbf{Q}}_p. \tag{0.3}$$

Letting $G_{\mathbf{Q}} := Gal(\overline{\mathbf{Q}}/\mathbf{Q})$ and $G_{\mathbf{Q}_p} := Gal(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ we note that (0.3) induces a natural injective restriction map $G_{\mathbf{Q}_p} \subseteq G_{\mathbf{Q}}$.

The group $\mathbf{Z}_p^\times$ of p-adic units decomposes canonically as the product of the group of principal units $1 + p\mathbf{Z}_p$ and the group μ_{p-1} of $(p-1)$th roots of unity.

$$\mathbf{Z}_p^\times = (1 + p\mathbf{Z}_p) \times \mu_{p-1}$$
$$a = \langle a \rangle \cdot \omega(a)$$

We denote the projection to principal units by $\langle \cdot \rangle$. The projection to roots of unity is given by the Teichmüller character ω.

Let $\mathbf{Z}_p[[\mathbf{Z}_p^\times]]$ denote the completed group ring of $\mathbf{Z}_p^\times$ and for each $a \in \mathbf{Z}_p^\times$ let $[a] \in \mathbf{Z}_p[[\mathbf{Z}_p^\times]]$ denote the corresponding element of $\mathbf{Z}_p[[\mathbf{Z}_p^\times]]$. For each continuous character $\kappa : \mathbf{Z}_p^\times \longrightarrow \overline{\mathbf{Q}}_p^\times$ we denote by the same symbol the unique continuous ring homomorphism $\kappa : \mathbf{Z}_p[[\mathbf{Z}_p^\times]] \longrightarrow \overline{\mathbf{Q}}_p$ sending $[a]$ to $\kappa(a)$ for all $a \in \mathbf{Z}_p^\times$. Contained in $\mathbf{Z}_p[[\mathbf{Z}_p^\times]]$ we have the Iwasawa algebra

$$\Lambda := \mathbf{Z}_p[[1 + p\mathbf{Z}_p]] \subseteq \mathbf{Z}_p[[\mathbf{Z}_p^\times]].$$

For $r \in \mathbf{Z}_p$ let $\sigma_r : \Lambda \longrightarrow \mathbf{Z}_p$ be the continuous homomorphism associated to the continuous character $1 + p\mathbf{Z}_p \longrightarrow \mathbf{Z}_p^\times$ defined by $\sigma_r : a \mapsto a^r$. Then each element $\alpha \in \Lambda$ gives rise to an analytic function on $\mathbf{Z}_p$ defined by

$$r \longmapsto \sigma_r(\alpha).$$

The ring of all such functions is the ring of *Iwasawa functions.*

§1. A Theorem of Hida

Fix a positive integer N prime to p and let $r \geq 0$. Let $\mathcal{S}_k(\Gamma_1(Np^r), \overline{\mathbf{Q}})$ denote the space of weight k cusp forms of level Np^r whose fourier coefficients are algebraic. Define

$$\mathcal{S}_k(\Gamma_1(Np^r)) := \mathcal{S}_k(\Gamma_1(Np^r), \overline{\mathbf{Q}}) \otimes_{\overline{\mathbf{Q}}} \overline{\mathbf{Q}}_p \tag{1.0.1}$$

where the tensor product is with respect to our fixed embedding (0.3). We say that a Hecke eigenform $f \in \mathcal{S}_k(\Gamma_1(Np^r))$ is *ordinary at* p if the eigenvalue a_p of the Hecke operator T_p is a p-adic unit. In that case, the Euler factor at p of the L-function of f has a factorization $(1 - \alpha p^{-s})(1 - \beta p^{-s})$ where α is a p-adic unit and β is divisible by p. We call α the *unit root of Frobenius* and β the *non-unit root of Frobenius.* Note that if $r > 0$ then $\beta = 0$.

Definition. We say that a Hecke eigenform $f \in \mathcal{S}_k(\Gamma_1(Np^r)$ is a p-stabilized ordinary newform of tame conductor N if one of the following is true.

- f is a newform of conductor Np^r; or
- there is a newform g of conductor N such that $f(z) = g(z) - \beta g(pz)$ for z in the upper half-plane where β is the non-unit root of Frobenius attached to g.

Note that in either case, the formula $f(z) = g(z) - \beta g(pz)$ is correct for some ordinary newform g whose non-unit root of Frobenius is β. In the first case we just take $g = f$ and $\beta = 0$. We call f the p-stabilized ordinary newform associated to g. For a modular elliptic curve E with good ordinary or multiplicative reduction at p we let f_E be the p-stabilized ordinary newform associated to the newform attached E. Note that for the associated complex L-functions we have the identity $(1 - \beta p^{-s})L_\infty(E, s) = L_\infty(f_E, s)$.

We have the following important result of Hida [**H1, H2**], Mazur, and Wiles [**Mz-W, W**] on p-adic analytic families of p-stabilized ordinary newforms. For a disk $U \subseteq \mathbf{Z}_p$, we let $\mathcal{A}_U$ denote the space of analytic functions $\alpha : U \longrightarrow \mathbf{Z}_p$. Recall the Galois groups $G_{\mathbf{Q}} := Gal(\overline{\mathbf{Q}}/\mathbf{Q})$, $G_{\mathbf{Q}_p} := Gal(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ and the natural injection $G_{\mathbf{Q}_p} \subseteq G_{\mathbf{Q}}$ induced by the embedding (0.3).

(1.0.2) THEOREM. *Let E be a modular elliptic curve of tame conductor N with good ordinary or multiplicative reduction at the prime $p \geq 5$. Then there is an open disk $U \subseteq \mathbf{Z}_p$ about 2, a formal q-expansion $\mathbf{f} = \sum_{n=1}^{\infty} \alpha_n q^n$ in $\mathcal{A}_U[[q]]$ and a Galois representation $\rho : G_{\mathbf{Q}} \longrightarrow GL_2(\mathcal{A}_U)$ satisfying the following properties.*

- **a.** *For each integer $k \geq 2$ in U, the power series $\mathbf{f}_k := \sum_{n=1}^{\infty} \alpha_n(k) q^n \in \mathbf{Z}_p[[q]]$ is the q-expansion of a non-zero p-stabilized ordinary newform of tame conductor N, weight k and character ω^{2-k}. Moreover, $\mathbf{f}_2 = f_E$.*
- **b.** *For each integer $k \geq 2$ in U, the Galois representation $\rho_k : G_{\mathbf{Q}} \longrightarrow GL_2(\mathbf{Z}_p)$, obtained by composing ρ with the specialization map $\alpha \mapsto \alpha(k)$, is equivalent to Deligne's representation associated to $\mathbf{f}_k$. In particular, ρ_2 is equivalent to the Galois representation attached to the p-adic Tate module of E.*
- **c.** *For all $k \in \mathbf{Z}_p$ the local Galois representation $\rho_k|_{G_{\mathbf{Q}_p}} : G_{\mathbf{Q}_p} \longrightarrow GL_2(\mathbf{Z}_p)$ has the form $\rho_k|_{G_{\mathbf{Q}_p}} = \begin{pmatrix} \chi_0 \langle \chi_0 \rangle^{k-2} \varphi_k^{-1} & * \\ 0 & \varphi_k \end{pmatrix}$ where φ_k is the unramified character sending a Frobenius element to $\alpha_p(k)$ and $\langle \chi_0 \rangle : G_{\mathbf{Q}_p} \longrightarrow \mathbf{Z}_p^\times$ is the local Galois character obtained by composing the cyclotomic character χ_0 with projection to the principal units.*

The first two assertions follow from [**H1, H2**] and the third assertion follows from [**Mz-W**] and [**W**] Theorem 2.2.2. Though we do not provide any details of the proof, it will be useful to describe how $\mathbf{f}$ and ρ are constructed. In (1.1.5) we will make an additional simplifying assumption, under which we may assume that all of the functions arising in the theorem are actually Iwasawa functions. In general they live in a finite extension of the Iwasawa algebra.

1.1. The universal ordinary modular p-adic Galois representation.

For each integer $r > 0$, let $X_{r/\mathbf{Q}}$ be the complete modular curve associated to $\Gamma_0(N) \cap \Gamma_1(p^r)$ and endowed with Shimura's canonical $\mathbf{Q}$-structure in which the 0-cusp is rational [**Sh2**]. Let $J_{r/\mathbf{Q}}$ be the Jacobian of X_r and let $Ta_p(J_r)$ be the p-adic Tate module of J_r. We define the *abstract Λ-adic Hecke algebra* of tame conductor N to be the free polynomial algebra

$$\mathcal{H} = \mathbf{Z}_p[[\mathbf{Z}_p^\times]][T_n \, (n \in \mathbf{Z}^+)]$$

generated over $\mathbf{Z}_p[[\mathbf{Z}_p^\times]]$ by T_n ($n \in \mathbf{Z}^+$). We let $\mathcal{H}$ act on J_r, and hence also on $Ta_p(J_r)$, by letting $\mathbf{Z}_p^\times$ act via the Nebentype operators and T_n act via the nth (covariant) Hecke correspondence. For each pair of integers $r_1 \geq r_2 > 0$, the natural projection $X_1(Np^{r_1}) \longrightarrow X_1(Np^{r_2})$ induces a Galois equivariant map of Tate modules $Ta_p(J_{r_1}) \longrightarrow Ta_p(J_{r_2})$ which commutes with the action of $\mathcal{H}$, hence we may form the projective limit and obtain an $\mathcal{H}[G_{\mathbf{Q}}]$-module

$$Ta_p(J_\infty) := \varprojlim_r Ta_p(J_r).$$

Shimura [**Sh1, O**] was the first to recognize the significance of $Ta_p(J_\infty)$. In [**H1, H2**], Hida extended Shimura's ideas in some quite beautiful and surprising directions by studying the ordinary part of $Ta_p(J_\infty)$. More precisely, there is a canonical decomposition

$$Ta_p(J_\infty) = Ta_p(J_\infty)^0 \oplus Ta_p(J_\infty)^{nil}$$

into $\mathcal{H}[G_{\mathbf{Q}}]$-modules such that the Hecke operator T_p acts invertibly on $Ta_p(J_\infty)^0$ and topologically nilpotently on $Ta_p(J_\infty)^{nil}$. Along with many other striking results, Hida has proven the remarkable fact that $Ta_p(J_\infty)^0$ is a *free* Λ*-module of finite rank.* Moreover, if we let $t = [1+p] - 1 \in \Lambda$ (or any other generator of the augmentation ideal) then the sequence

$$(1.1.1) \qquad 0 \longrightarrow Ta_p(J_\infty)^0 \xrightarrow{t} Ta_p(J_\infty)^0 \longrightarrow Ta_p(J_1)^0 \longrightarrow 0$$

is exact.

Now suppose E is a modular elliptic curve of tame conductor N with either good ordinary or multiplicative reduction at the prime p and let $f_E = \sum_{n=1}^\infty a_n q^n$ be the associated p-stabilized ordinary newform, normalized so that $a_1 = 1$. Now define $\lambda_E : \mathcal{H} \longrightarrow \mathbf{Z}_p$ by mapping $\mathbf{Z}_p^\times$ to 1 and each Hecke operator T_n to a_n. We let $\mathcal{H}$ act on the Tate module $Ta_p(E)$ via λ_E. (Note that if the conductor of E is N, prime to p, then according to these conventions T_p acts via the unit root of Frobenius, not the trace of Frobenius as in [**D**]). Fix a modular parametrization $X_1 \longrightarrow E$ and let $Ta_p(J_1)^0 \longrightarrow Ta_p(E)$ be the induced homomorphism on Tate modules. This map commutes with the action of $G_{\mathbf{Q}}$ as well as with the action just defined for $\mathcal{H}$. We have the following theorem of Hida asserting, among other things, that $Ta_p(E)$ can be lifted to an $\mathcal{H}$-eigenspace in $Ta_p(J_\infty)^0$.

(1.1.2) THEOREM. *There is an integral domain $\mathcal{R}_E$ finite and flat over Λ and a surjective Λ-homomorphism $h_E : \mathcal{H} \longrightarrow \mathcal{R}_E$ with the following properties.*

(1) $\mathcal{R}_E$ is unramified over the augmentation ideal P_0 in Λ.

(2) The homomorphism $\lambda_E : \mathcal{H} \longrightarrow \mathbf{Z}_p$ factors through h_E, i.e. there is a homomorphism $\pi_E : \mathcal{R}_E \longrightarrow \mathbf{Z}_p$ such that $\lambda_E = \pi_E \circ h_E$.

(3) Let $\mathbf{T}_E \subseteq Ta_p(J_\infty)^0 \otimes_\Lambda \mathcal{R}_E$ be the $\mathcal{R}_E$-submodule consisting of elements on which $\mathcal{H}$ acts via h_E. Then $\mathbf{T}_E$ has rank 2 as an $\mathcal{R}_E$-module (i.e. if $\mathcal{K}_E$ is the fraction field of $\mathcal{R}_E$, then $\mathbf{T}_E \otimes_{\mathcal{R}_E} \mathcal{K}_E$ has dimension 2 over $\mathcal{K}_E$).

The ingredients in Theorem 1.0.2 can now be described as follows. For each positive integer n, we let $\alpha_n := h_E(T_n) \in \mathcal{R}_E$ and define $\mathbf{f}_E := \sum_{n=1}^\infty \alpha_n q^n \in \mathcal{R}_E[[q]]$. Also, let $\rho_E : G_{\mathbf{Q}} \longrightarrow Aut_{\mathcal{R}_E}(\mathbf{T}_{\mathcal{R}_E})$ be the representation of Galois on $\mathbf{T}_E$. To pass from $\mathbf{f}_E$ and ρ_E to the data $\mathbf{f}$ and ρ prescribed in theorem (1.0.2) we proceed as follows. Recall, first of all, that for each $k \in \mathbf{Z}_p$ the character $1 + p\mathbf{Z}_p \longrightarrow \mathbf{Z}_p^\times$ defined by $a \mapsto a^{k-2}$ extends to a continuous homomorphism $\sigma_{k-2} : \Lambda \longrightarrow \mathbf{Z}_p$. For each $\alpha \in \Lambda$ we define

$$(1.1.3) \qquad \alpha(k) := \sigma_{k-2}(\alpha).$$

Then the functions $\alpha(k)$, for $\alpha \in \Lambda$ are the well-known Iwasawa functions on $\mathbf{Z}_p$. In particular, the map $\alpha \mapsto \alpha(k)$ endows $\mathcal{A}_U$ with a natural structure as Λ-module for every disk U in $\mathbf{Z}_p$. Since the Λ-algebra $\mathcal{R}_E$ is finite and unramified over the augmentation ideal P_0 of Λ, it follows that for a sufficiently small disk U about 2 in $\mathbf{Z}_p$, there is a unique Λ-homomorphism

$$\mathcal{R}_E \longrightarrow \mathcal{A}_U. \tag{1.1.4}$$

The formal q-expansion $\mathbf{f}$ is obtained by applying this homomorphism to the coefficients of $\mathbf{f}_E$ and the Galois representation ρ is obtained by tensoring $\mathbf{T}_E$ over $\mathcal{R}_E$ with $\mathcal{A}_U$.

We will frequently invoke the following simplifying hypothesis.

(1.1.5) HYPOTHESIS. $\mathcal{R}_E = \Lambda$.

(1.1.6) Example. Let $p = 11$, $N = 1$, and let E be the modular elliptic curve $X_1(11)$, which has split multiplicative reduction at p. In this case $J_1 = E$, hence the Tate module $Ta_p(J_1)$ is a free rank two $\mathbf{Z}_p$-module. Then from Hida's exact sequence (1.1.1) and an application of the compact version of Nakayama's lemma, we see that $Ta_p(J_\infty)^0$ is a free rank two Λ-module. Hence we must have $\mathcal{R}_E = \Lambda$ and $\mathbf{T}_E = Ta_p(J_\infty)^0$.

In the final section of the paper, we will give another example of an elliptic curve with split multiplicative reduction at p for which $\mathcal{R}_E$ is not Λ.

§2. The $\mathcal{L}$-Invariant and Deformations of Local Galois Representations

Let E be a modular elliptic curve with split multiplicative reduction at the prime p, which we now assume to satisfy $p \geq 5$. Let $\mathbf{f} = \sum_{n=1}^{\infty} \alpha_n(k)q^n \in \mathcal{A}_U[[q]]$ be the analytic family of q-expansions given by Hida's theorem 1.0.2. In this section we prove the following result establishing a connection between the pth coefficient of $\mathbf{f}$ and the $\mathcal{L}$-invariant of E defined by (0.1).

(2.0.1) THEOREM. *Let $\alpha_p(k)$ be the p-adic analytic function attached to the pth coefficient of Hida's Λ-adic modular form. Then*

$$\alpha_p(2) = 1 \qquad \textit{and} \qquad \alpha_p'(2) = -\frac{1}{2}\mathcal{L}_p(E).$$

The first assertion, $\alpha_p(2) = 1$, follows at once from the identity $\mathbf{f}_2 = f_E$ and the fact that E has split multiplicative reduction at p. The proof of the expression for the derivative rests on two interpretations of the $\mathcal{L}$-invariant and a connection between them expressed by Tate duality. Both interpretations depend on the simple fact that for any $\mathbf{Q}_p[G_{\mathbf{Q}_p}]$-module W, there is a one-one correspondence

$$\left\{\begin{matrix}\text{non-trivial extensions}\\ \text{of } \mathbf{Q}_p \text{ by } W\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{one-dimensional subspaces}\\ \text{of } H^1(W)\end{matrix}\right\}. \tag{2.0.2}$$

where $H^n(-)$ denotes cohomology with respect to the group $G_{\mathbf{Q}_p}$. Indeed, if X is a $G_{\mathbf{Q}_p}$-module, then X is an extension of $\mathbf{Q}_p$ by W if and only if there is an exact sequence of $G_{\mathbf{Q}_p}$-modules

$$0 \longrightarrow W \longrightarrow X \longrightarrow \mathbf{Q}_p \longrightarrow 0.$$

This sequence is non-split precisely when the map $H^0(X) \longrightarrow H^0(\mathbf{Q}_p)$ vanishes, in which case the image of $H^0(\mathbf{Q}_p)$ in $H^1(W)$ under the coboundary map is a one-dimensional subspace of $H^1(W)$. Conversely, if $\xi : G_{\mathbf{Q}_p} \longrightarrow W$ is a non-zero 1-cocycle, then define $X = W \times \mathbf{Q}_p$ with $G_{\mathbf{Q}_p}$ acting by the formula $g(w, \lambda) = (g(w) + \lambda\xi(g), \lambda)$ for $g \in G_{\mathbf{Q}_p}$. It is easy to verify that X is a nontrivial extension of $\mathbf{Q}_p$ by W if and only if ξ represents a non-zero cohomology class in $H^1(W)$ and that the isomorphism class of X depends only on the line spanned by the cohomology class of ξ in $H^1(W)$.

2.1. Kummer theory and the group of Tate periods.

Kummer theory gives us a canonical isomorphism

$$H^1(\mathbf{Q}_p(1)) \;\cong\; \mathbf{Q}_p^\times \hat{\otimes} \mathbf{Q}_p \;:=\; \varprojlim_n \left(\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times p^n} \right) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p. \tag{2.1.1}$$

Thus each $q \in \mathbf{Q}_p^\times$ determines a cohomology class $\gamma_q \in H^1(\mathbf{Q}_p(1))$, which we will refer to as the Kummer class associated to q. More precisely, letting μ_{p^n} be the group of p^nth roots of unity, and choosing a compatible sequence, $(\,q^{1/p^n}\,)_n$ of p-power roots of q, we can define a sequence of 1-cocycles $\xi_n : G_{\mathbf{Q}_p} \longrightarrow \mu_{p^n}$ by $\xi_n(\sigma) = (q^{1/p^n})^{\sigma - 1}$ for $\sigma \in G_{\mathbf{Q}_p}$. The sequence ξ_n determines a 1-cocycle $\xi : G_{\mathbf{Q}_p} \longrightarrow \mathbf{Z}_p(1)$. We define the Kummer class γ_q to be the element of $H^1(\mathbf{Q}_p(1))$ determined by ξ.

Now let $E_{/\mathbf{Q}_p}$ be an elliptic curve over $\mathbf{Q}_p$ with split multiplicative reduction. Set $V(E) = Ta_p(E) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ where $Ta_p(E)$ is the Tate module of E. Let q_E be a generator of the group of Tate periods and consider the analytic isomorphism

$$E(\overline{\mathbf{Q}}_p) \cong \overline{\mathbf{Q}}_p^\times / q_E^{\mathbf{Z}}.$$

given by the Tate parametrization. For each integer $n > 0$ there is a canonical exact sequence $0 \to \mu_{p^n} \to E[p^n] \to \mathbf{Z}/p^n\mathbf{Z} \to 0$ of $G_{\mathbf{Q}_p}$-modules. Passing to the projective limit and tensoring with $\mathbf{Q}_p$ we obtain the following fundamental exact sequence

$$0 \longrightarrow \mathbf{Q}_p(1) \longrightarrow V(E) \longrightarrow \mathbf{Q}_p \longrightarrow 0. \tag{2.1.2}$$

We have the following simple result whose proof is a straightforward calculation.

(2.1.3) PROPOSITION. *Let $E_{/\mathbf{Q}_p}$ be an elliptic curve with split multiplicative reduction and let $q \in \mathbf{Q}_p^\times$ be any nontrivial element of the group $q_E^{\mathbf{Z}}$ of Tate periods. Then the Kummer class γ_q spans the line in $H^1(\mathbf{Q}_p(1))$ associated to the extension (2.1.2).*

2.2. Infinitesimal deformations.

Let $\tilde{\mathbf{Q}}_p := \mathbf{Q}_p[t]/t^2$ be the ring of polynomials over $\mathbf{Q}_p$ modulo t^2.

(2.2.1) Definition. Let V be a finite dimensional $\mathbf{Q}_p[G_{\mathbf{Q}_p}]$-module. We will say that a $\tilde{\mathbf{Q}}_p[G_{\mathbf{Q}_p}]$-module $\tilde{V}$ is an *infinitesimal deformation of* V if $\tilde{V}$ is free as a $\tilde{\mathbf{Q}}_p$-module and $\tilde{V}/t\tilde{V} \cong V$ as a $G_{\mathbf{Q}_p}$-module.

In particular, we see that if $\tilde{V}$ is an infinitesimal deformation of V, then both $\tilde{V}/t\tilde{V}$ and $t\tilde{V}$ are isomorphic to V. So we have an exact sequence of $G_{\mathbf{Q}_p}$-modules

$$0 \longrightarrow V \longrightarrow \tilde{V} \longrightarrow V \longrightarrow 0.$$

Hence $\tilde{V}$ is an extension of V by V.

For example, $\tilde{\mathbf{Q}}_p$ with trivial Galois action is an infinitesimal deformation of $\mathbf{Q}_p$. More generally, if $\psi : G_{\mathbf{Q}_p} \longrightarrow \tilde{\mathbf{Q}}_p^\times$ is a nontrivial continuous Galois character satisfying the congruence $\psi(\sigma) \equiv 1 \pmod{t}$ for every $\sigma \in G_{\mathbf{Q}_p}$ then the twist $\tilde{\mathbf{Q}}_p(\psi)$ of $\tilde{\mathbf{Q}}_p$ by ψ is an infinitesimal deformation of $\mathbf{Q}_p$. In particular $\tilde{\mathbf{Q}}_p(\psi)$ is a nonsplit extension of $\mathbf{Q}_p$ by $\mathbf{Q}_p$, hence determines a line in $H^1(\mathbf{Q}_p)$ as in (2.0.2). It is a simple matter to describe this line. Differentiation with respect to t induces a continuous isomorphism $\frac{d}{dt} : 1 + t\mathbf{Q}_p \longrightarrow \mathbf{Q}_p$ from the multiplicative subgroup $1 + t\mathbf{Q}_p \subseteq \tilde{\mathbf{Q}}_p^\times$ to the additive group $\mathbf{Q}_p$. Hence, the composition of ψ with d/dt is an nonzero additive character $\frac{d\psi}{dt} : G_{\mathbf{Q}_p} \longrightarrow \mathbf{Q}_p$. Since $Hom(G_{\mathbf{Q}_p}, \mathbf{Q}_p) = H^1(\mathbf{Q}_p)$, we may interpret $d\psi/dt$ as a cohomology class in $H^1(\mathbf{Q}_p)$ and the line $\mathbf{Q}_p \frac{d\psi}{dt} \subseteq H^1(\mathbf{Q}_p)$ it spans is easily seen to correspond to $\tilde{\mathbf{Q}}_p(\psi)$ under (2.0.2). Indeed, we have the following proposition.

(2.2.2) PROPOSITION. *The correspondence $\tilde{\mathbf{Q}}_p(\psi) \leftrightarrow \mathbf{Q}_p \frac{d\psi}{dt}$ induces a one-one correspondence*

$$\left\{ \begin{array}{c} \textit{Nontrivial infinitesimal} \\ \textit{deformations of } \mathbf{Q}_p \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{One-dimensional} \\ \textit{subspaces of } H^1(\mathbf{Q}_p) \end{array} \right\}$$

Moreover, $d\psi/dt$ spans the line in $H^1(\mathbf{Q}_p)$ associated to $\tilde{\mathbf{Q}}_p(\psi)$.

2.3. Tate duality.

From Kummer theory and class field theory we know that each of the cohomology groups $H^1(\mathbf{Q}_p(1))$ and $H^1(\mathbf{Q}_p)$ is a two-dimensional $\mathbf{Q}_p$-vector space. Moreover, Tate duality gives us a perfect pairing

$$(2.3.1) \qquad \langle\ ,\ \rangle : H^1(\mathbf{Q}_p(1)) \times H^1(\mathbf{Q}_p) \longrightarrow H^2(\mathbf{Q}_p(1)) = \mathbf{Q}_p$$

Hence a line in either one of the cohomology groups $H^1(\mathbf{Q}_p(1))$, $H^1(\mathbf{Q}_p)$ determines a line in the other one – namely, its orthogonal complement. In the light of (2.0.2) and (2.2.2) this means that there is a natural one-one correspondence

$$(2.3.2) \qquad \left\{ \begin{array}{c} \text{non-trivial extensions} \\ \text{of } \mathbf{Q}_p \text{ by } \mathbf{Q}_p(1) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{non-trivial infinitesimal} \\ \text{deformations of } \mathbf{Q}_p \end{array} \right\}.$$

Let $G_{\mathbf{Q}_p}^{ab}$ be the abelianized Galois group and let $\sigma : \mathbf{Q}_p^\times \longrightarrow G_{\mathbf{Q}_p}^{ab}$ be the local Artin symbol, normalized so that σ_p is the inverse of a Frobenius element. With this normalization, the cyclotomic character χ_0 is given by $\chi_0(\sigma_u) = u$ for $u \in \mathbf{Z}_p^\times$. Moreover, the Tate pairing is explicitly given by the formula

$$\langle \gamma_q, \xi \rangle = \xi(\sigma_q) \tag{2.3.3}$$

for arbitrary $q \in \mathbf{Q}_p^\times$ and $\xi \in H^1(\mathbf{Q}_p)$, where γ_q is the Kummer class of q defined in section 2.1.

(2.3.4) THEOREM. *Let $E_{/\mathbf{Q}_p}$ be an elliptic curve with split multiplicative reduction and let $\psi : G_{\mathbf{Q}_p} \longrightarrow \tilde{\mathbf{Q}}_p^\times$ be a nontrivial character which is $\equiv 1$ modulo t. Then the following statements are equivalent.*

a. $\dfrac{d\psi}{dt}(\sigma_{q_E}) = 0.$

b. *$V(E)$ corresponds to $\tilde{\mathbf{Q}}_p(\psi)$ under (2.3.2).*

c. *There is an infinitesimal deformation $\tilde{V}$ of $V(E)$ and a commutative diagram*

$$\begin{tikzcd}
0 \arrow[r] & \tilde{\mathbf{Q}}_p(1) \arrow[r] \arrow[d] & \tilde{V} \arrow[r] \arrow[d] & \tilde{\mathbf{Q}}_p(\psi) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbf{Q}_p(1) \arrow[r] & V(E) \arrow[r] & \mathbf{Q}_p \arrow[r] & 0.
\end{tikzcd}$$

in which the top row is an exact sequence of $\tilde{\mathbf{Q}}_p[G_{\mathbf{Q}_p}]$-modules and the vertical maps are reduction modulo t.

Proof. The equivalence of **a** and **b** is an immediate consequence of the above discussion and the explicit description of the Tate pairing (2.3.3). Indeed, from (2.3.3), we have $\dfrac{d\psi}{dt}(\sigma_{q_E}) = 0$ if and only if γ_{q_E} is orthogonal to $d\psi/dt$ with respect to the Tate pairing. But by proposition 2.1.3, γ_{q_E} spans the line in $H^1(\mathbf{Q}_p(1))$ determined by $V(E)$ and by proposition (2.2.2), $d\psi/dt$ spans the line in $H^1(\mathbf{Q}_p)$ determined by the infinitesimal deformation $\tilde{\mathbf{Q}}_p(\psi)$.

Next we show **b**$\Longrightarrow$**c**. Suppose $V(E)$ corresponds to $\tilde{\mathbf{Q}}_p(\psi)$ under (2.3.2). Then we can give an explicit construction of $\tilde{V}$ as follows. Let γ denote a cocycle representing the cohomology class of γ_{q_E}. Then the function

$$G \times G \longrightarrow \mathbf{Q}_p(1)$$
$$(g_1, g_2) \longmapsto \gamma(g_1) \cdot \frac{d\psi}{dt}(g_2)$$

is a 2-cocycle representing the cup product of γ_{q_E} and $d\psi/dt$. Since this cup product vanishes, there is a 1-cochain $\xi : G \longrightarrow \mathbf{Q}_p(1)$ whose coboundary is the above map. Hence, for all $(g_1, g_2) \in G \times G$, we have $\xi(g_1 g_2) - \chi_0(g_1)\xi(g_2) - \xi(g_1) = \gamma(g_1)\dfrac{d\psi}{dt}(g_2)$. Now define for each $g \in G$

$$\tilde{\rho}(g) \;=\; \begin{pmatrix} \chi_0(g) & \gamma(g) + t\xi(g) \\ 0 & \psi(g) \end{pmatrix} \in GL_2(\tilde{\mathbf{Q}}_p).$$

A simple calculation shows that $\tilde{\rho} : G \longrightarrow GL_2(\tilde{\mathbf{Q}}_p)$ is a group homomorphism. We let $\tilde{V}$ denote $\tilde{\mathbf{Q}}_p^2$ equipped with the Galois action induced by $\tilde{\rho}$. It is a simple matter now to construct the commutative diagram of part **c** of the proposition. This proves **b**$\Longrightarrow$**c**.

Conversely, suppose we have a commutative diagram as in **c**. We must show that γ_{q_E} is orthogonal to $d\psi/dt$ with respect to the Tate pairing. From the diagram in **c** we obtain a commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathbf{Q}_p(1) \arrow[r] \arrow[d] & V(E) \arrow[r] \arrow[d] & \mathbf{Q}_p \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \tilde{\mathbf{Q}}_p(1) \arrow[r] \arrow[d] & \tilde{V} \arrow[r] \arrow[d] & \tilde{\mathbf{Q}}_p(\psi) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbf{Q}_p(1) \arrow[r] \arrow[d] & V(E) \arrow[r] \arrow[d] & \mathbf{Q}_p \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

in which the rows and columns are exact. Since the leftmost vertical row splits, the connecting homomorphism $d : H^1(\mathbf{Q}_p(1)) \longrightarrow H^2(\mathbf{Q}_p(1))$ vanishes. On the other hand, letting $\delta_\psi : H^0(\mathbf{Q}_p) \longrightarrow H^1(\mathbf{Q}_p)$ be the connecting homomorphism of degree 0 attached to the rightmost vertical row, and letting $\delta_i : H^i(\mathbf{Q}_p) \longrightarrow H^{i+1}(\mathbf{Q}_p(1))$ (i=0,1) be the connecting homomorphism of degree i associated to the bottom row (or, equivalently, the top row), we obtain a commutative diagram

$$\begin{tikzcd}
H^0(\mathbf{Q}_p) = \mathbf{Q}_p \arrow[r, "\delta_0"] \arrow[d, "\delta_\psi"] & H^1(\mathbf{Q}_p(1)) \arrow[d, "d=0"] \\
H^1(\mathbf{Q}_p) \arrow[r, "\delta_1"] & H^2(\mathbf{Q}_p(1))
\end{tikzcd}$$

But since $\delta_\psi(1) = d\psi/dt$, this shows that $d\psi/dt$ lies in the kernel of δ_1. On the other hand, by proposition 2.1.3, we have γ_{q_E} is in the image of δ_0. So **b** will follow if we can show that the kernel of δ_1 is orthogonal to the image of δ_0.

Note that multiplication induces a perfect pairing $\mathbf{Q}_p(1) \times \mathbf{Q}_p \longrightarrow \mathbf{Q}_p(1)$. Moreover, as a simple verification shows, there is a unique symplectic pairing $V(E) \times V(E) \longrightarrow \mathbf{Q}_p(1)$ with respect to which the homomorphisms $i : \mathbf{Q}_p(1) \longrightarrow V(E)$ and $\pi : V(E) \longrightarrow \mathbf{Q}_p$ are transposes of one another. (Indeed this is the Weil pairing, but we will not need this fact). Hence the fundamental sequence $0 \longrightarrow \mathbf{Q}_p(1) \longrightarrow V(E) \longrightarrow \mathbf{Q}_p \longrightarrow 0$ is self-dual with respect to these pairings, and then by duality, the connecting homomorphisms $\delta_0 : H^0(\mathbf{Q}_p) \longrightarrow H^1(\mathbf{Q}_p(1))$ and $\delta_1 : H^1(\mathbf{Q}_p) \longrightarrow H^2(\mathbf{Q}_p(1))$ are transposes under the Tate pairing. In particular, the image of δ_0 is orthogonal to the kernel of δ_1. This proves **c**$\Longrightarrow$**b** and completes the proof of the proposition.

2.4. Proof of Theorem 2.0.1.

Let $E_{/\mathbf{Q}}$ be our modular elliptic curve with split multiplicative reduction at p. Let $\mathrm{f} = \sum_{n=1}^{\infty} \alpha_n(k) q^n \in \mathcal{A}_U[[q]]$ be the formal q-expansion given by theorem 1.0.2, where U is a suitable p-adic neighborhood of 2. Consider the representation $\rho : G_{\mathbf{Q}_p} \longrightarrow GL_2(\mathcal{A}_U)$ given by theorem (1.0.2)**c**. Then from (1.0.2)**c** we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{A}_U(\chi_0\langle\chi_0\rangle^{k-2}\varphi_k^{-1}) \arrow[r] \arrow[d] & \mathcal{A}_U^2 \arrow[r] \arrow[d] & \mathcal{A}_U(\varphi_k) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbf{Q}_p(1) \arrow[r] & V(E) \arrow[r] & \mathbf{Q}_p \arrow[r] & 0
\end{tikzcd} \tag{2.4.1}$$

of $G_{\mathbf{Q}_p}$-representations where $\varphi_k : G_{\mathbf{Q}_p} \longrightarrow \mathcal{A}_U^\times$ is the unramified character with $\varphi_k(Frob_p) = \alpha_p(k)$, the bottom row is the fundamental sequence associated to E, and the vertical arrows are given by specialization to $k = 2$.

In order to obtain a diagram of the form appearing in proposition 2.3.4**c**, we must twist the terms in the first row of (2.4.1) so that the leftmost term is $\mathcal{A}_U(\chi_0)$. This is accomplished by twisting each term of (2.4.1) by $\varphi_k\langle\chi_0\rangle^{2-k}$. Since this character specializes to the trivial character at $k = 2$, we obtain a commutative diagram

(2.4.2)

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{A}_U(\chi_0) \arrow[r] \arrow[d] & \mathcal{A}_U^2(\varphi_k\langle\chi_0\rangle^{2-k}) \arrow[r] \arrow[d] & \mathcal{A}_U(\varphi_k^2\langle\chi_0\rangle^{2-k}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbf{Q}_p(1) \arrow[r] & V(E) \arrow[r] & \mathbf{Q}_p \arrow[r] & 0
\end{tikzcd}$$

Letting $t := k - 2 \in \mathcal{A}_U$ we have $\mathcal{A}_U/(t^2) \cong \tilde{\mathbf{Q}}_p$. Hence, reducing the terms of (2.4.2) modulo t^2 and setting $\tilde{V} := \tilde{\mathbf{Q}}_p^2(\varphi_k\langle\chi_0\rangle^{2-k})$ we obtain a diagram

$$\begin{tikzcd}
0 \arrow[r] & \tilde{\mathbf{Q}}_p(1) \arrow[r] \arrow[d] & \tilde{V} \arrow[r] \arrow[d] & \tilde{\mathbf{Q}}_p(\psi) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbf{Q}_p(1) \arrow[r] & V(E) \arrow[r] & \mathbf{Q}_p \arrow[r] & 0
\end{tikzcd} \tag{2.4.3}$$

where $\psi = \varphi_k^2\langle\chi_0\rangle^{2-k}$ considered modulo t^2. Applying proposition 2.3.4 we obtain the identity

$$\frac{d\psi}{dk}(\sigma_{q_E}) = 0. \tag{2.4.4}$$

Writing $q_E = p^n u$ where $n = ord_p(q_E)$ and $u \in \mathbf{Z}_p^\times$ and recalling that $\varphi_k(\sigma_p) = \varphi_k(Frob_p)^{-1}$ and $\varphi_k(Frob_p) = \alpha_p(k)$ we obtain $\psi(\sigma_{q_E}) = \alpha_p(k)^{-2n}\langle u\rangle^{2-k}$. Now differentiate this with respect to k and set $k = 2$. Recalling that $\alpha_p(2) = 1$ and using (2.4.4) we obtain the equality $-2ord_p(q_E) \cdot \alpha_p'(2) - \log_p(q_E) = 0$. The desired result

$$\alpha_p'(2) = -\frac{1}{2}\frac{\log_p(q_E)}{ord_p(q_E)}$$

now follows at once. This completes the proof of theorem 2.0.1.

§3. p-Adic L-Functions

In this chapter we recall the construction of two-variable p-adic L-functions associated to Λ-adic cusp forms. Mazur [**Mz**] was the first to construct examples of these two-variable p-adic L-functions. Kitagawa [**Ki**] (this volume) generalized Mazur's construction to associate a two-variable p-adic L-function to any ordinary Λ-adic cusp form. A different construction was given with certain additional properties in [**G-S**]. We will recall the details of that construction, but only under the additional hypothesis that $\mathcal{R}_E = \Lambda$.

Let E be a modular elliptic curve over $\mathbf{Q}$ having conductor M with either good ordinary or multiplicative reduction at p. Then we can factor the conductor of E as $M = Np^e$ where N is the tame conductor of E and $e = 0$ or 1 depending on whether the reduction at p is good or multiplicative. Let $L_\infty(E,s)$, $s \in \mathbf{C}$, be the complex L-function and $L_p(E,s)$, $s \in \mathbf{Z}_p$, be the p-adic L-function of E. The precise definition of $L_p(E,s)$ depends linearly on a choice of a non-zero real period Ω_E of some rational regular differential on E. It is customary to let Ω_E be the positive generator of the group of real periods of a Neron differential on E, but any non-zero choice will suffice.

Both the complex and the p-adic L-functions satisfy functional equations with respect to the substitution $s \mapsto 2 - s$. More precisely, if we put

$$\Lambda_\infty(E,s) = M^{s/2}(2\pi)^{-s}\Gamma(s)L_\infty(E,s) \qquad \text{and} \qquad \Lambda_p(E,s) = \langle N\rangle^{s/2}L_p(E,s)$$

then

$$\Lambda_\infty(E,2-s) = \epsilon_\infty\Lambda_\infty(E,s) \qquad \text{and} \qquad \Lambda_p(E,2-s) = \epsilon_p\Lambda_p(E,s).$$

for an appropriate choice of signs $\epsilon_\infty = \pm 1$ and $\epsilon_p = \pm 1$. Note that in the first functional equation s is a complex variable, but in the second s is a p-adic variable. The relationship between ϵ_∞ and ϵ_p is given by

$$\text{(3.0.1)} \qquad \epsilon_p = \begin{cases} -\epsilon_\infty & \text{if } E \text{ has split multiplicative reduction at } p; \\ \\ \epsilon_\infty & \text{otherwise.} \end{cases}$$

See section 3.8 for an explanation of this relationship. The main goal of this chapter is to outline a proof of the following theorem.

(3.0.2) THEOREM. *Let $p \geq 5$ be prime and let E be a modular elliptic curve of tame conductor N with either good ordinary or multiplicative reduction at p. Let α, β, respectively, be the unit root and the non-unit root of Frobenius at p. Let $\alpha_p = h_E(T_p) \in \mathcal{R}_E$ and let $\alpha_p(k) \in \mathcal{A}_U$, be the analytic function associated to α_p as in (1.1.4) defined on a neighborhood U of 2 in $\mathbf{Z}_p$. Then there are analytic functions $L_p(k,s)$ and $L_p^*(k,1)$, $k \in U$, $s \in \mathbf{Z}_p$, satisfying the following properties.*

1. $L_p(2,s) = L_p(E,s)$ *for all* $s \in \mathbf{Z}_p$.
2. $L_p(k,k-s) = \epsilon_p\langle N\rangle^{s-\frac{k}{2}}L_p(k,s)$.

3. $L_p(k,1) = \left(1 - \alpha_p(k)^{-1}\right) L_p^*(k,1)$.
4. $L_p^*(2,1) = \left(1 - \dfrac{\beta}{p}\right) \cdot \dfrac{L_\infty(E,1)}{\Omega_E}$.

In fact, for fixed $k \in U$, $L_p(k,s)$ is an Iwasawa function of s. If, moreover, $\mathcal{R}_E = \Lambda$ then $L_p(k,s)$ is an Iwasawa function of two variables (and in particular, we may take $U = \mathbf{Z}_p$).

The function $L_p^*(k,1)$ of this theorem is identical to the function $L_p^*(k)$ discussed in the introduction.

3.1. Generalities on p-Adic Measures.

For a compact totally disconnected topological space X we let $\mathrm{Cont}(X)$ denote the module of $\mathbf{Z}_p$-valued continuous functions on X and $\mathrm{Step}(X)$ denote the submodule of locally constant functions. We equip $\mathrm{Cont}(X)$ with the topology induced by the supremum norm and note that $\mathrm{Step}(X)$ is a dense submodule. We define the module of $\mathbf{Z}_p$-valued measures on X to be $\mathrm{Meas}(X) := \mathrm{Hom}_{\mathbf{Z}_p}(\mathrm{Step}(X), \mathbf{Z}_p)$. Every measure $\mu \in \mathrm{Meas}(X)$ is easily seen to have a unique extension to a continuous homomorphism $\mu : \mathrm{Cont}(X) \longrightarrow \mathbf{Z}_p$. Hence

$$\mathrm{Meas}(X) \cong \mathrm{Cont.Hom}_{\mathbf{Z}_p}(\mathrm{Cont}(X), \mathbf{Z}_p). \tag{3.1.1}$$

We endow $\mathrm{Meas}(X)$ with the weak topology dual to $\mathrm{Cont}(X)$.

It is customary to use measure theoretic conventions in reference to the elements of $\mathrm{Meas}(X)$. Thus, if $\mu \in \mathrm{Meas}(X)$ and $U \subseteq X$ is a compact open set, then we will often write $\mu(U)$ for the value of μ on the characteristic function of U. Similarly, if $f \in \mathrm{Cont}(X)$ then we will often use integral notation and write $\int f d\mu$ for $\mu(f)$ and $\int_U f d\mu$ for the value of μ on f times the characteristic function of U.

In the applications, X will be a compact open subset of either $\mathbf{Z}_p$ or $\mathbf{Z}_p \times \mathbf{Z}_p$.

(3.1.2) Definition.

a. The *one-variable p-adic L-function* associated to a measure $\nu \in \mathrm{Meas}(\mathbf{Z}_p^\times)$ is the function $L_p(\nu, -) : \mathbf{Z}_p \longrightarrow \mathbf{Z}_p$ defined by

$$L_p(\nu, s) = \int_{\mathbf{Z}_p^\times} \langle t \rangle^{s-1}\, d\nu(t), \quad s \in \mathbf{Z}_p.$$

b. The *two-variable p-adic L-function* associated to a measure $\mu \in \mathrm{Meas}(\mathbf{Z}_p^\times \times \mathbf{Z}_p)$ is the function $L_p(\mu, -, -) : \mathbf{Z}_p^2 \longrightarrow \mathbf{Z}_p$ defined by

$$L_p(\mu, k, s) = \int_{\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times} \langle x \rangle^{k-2} \langle y/x \rangle^{s-1}\, d\mu(x,y), \quad k, s \in \mathbf{Z}_p.$$

c. The *improved two-variable p-adic L-function* associated to a measure $\mu \in \mathrm{Meas}(\mathbf{Z}_p^\times \times \mathbf{Z}_p)$ is the function $L_p(\mu, -, -) : \mathbf{Z}_p \times \mathbf{N} \longrightarrow \mathbf{Z}_p$ defined by

$$L_p(\mu, k, s_0) = \int_{\mathbf{Z}_p^\times \times \mathbf{Z}_p} \langle x \rangle^{k-2} (y/x)^{s_0 - 1}\, d\mu(x,y), \quad k \in \mathbf{Z}_p,\ s_0 \in \mathbf{N}.$$

3.2. Measure Spaces as Iwasawa Modules.

For each $t \in \mathbf{Z}_p^\times$, let $\delta_t \in \mathrm{Meas}(\mathbf{Z}_p^\times)$ denote the Dirac distribution concentrated at t. Hence δ_t is characterized by the integration formula $\int f\,d\delta_t = f(t)$ for $f \in \mathrm{Cont}(\mathbf{Z}_p^\times)$. The map $t \mapsto \delta_t$ defines a continuous map $\mathbf{Z}_p^\times \longrightarrow \mathrm{Meas}(\mathbf{Z}_p^\times)$ and can therefore be uniquely extended to a continuous $\mathbf{Z}_p$-morphism

$$\mathbf{Z}_p[[\mathbf{Z}_p^\times]] \longrightarrow \mathrm{Meas}(\mathbf{Z}_p^\times). \tag{3.2.1}$$

In fact, this is well known to be an isomorphism.

Let $(\mathbf{Z}_p^2)'$ denote the set of *primitive* vectors in $\mathbf{Z}_p^2$ (i.e. vectors which are not divisible by p) and consider the canonical projection

$$(\mathbf{Z}_p^2)' \longrightarrow \mathbf{P}^1(\mathbf{Q}_p)$$

sending (x,y) in affine coordinates to $[x,y]$ in projective coordinates. The fibers of this map are just the orbits of the scalar action of $\mathbf{Z}_p^\times$. For X a compact open subset of $\mathbf{P}^1(\mathbf{Q}_p)$, we set

$$U(X) := \{\ (x,y) \in (\mathbf{Z}_p^2)' \mid [x,y] \in X\ \}. \tag{3.2.2}$$

Thus, $U(X)$ is just the preimage of X in $(\mathbf{Z}_p^2)'$. Now define

$$\mathbf{D}(X) := \mathrm{Meas}(U(X)). \tag{3.2.3}$$

When $X = \mathbf{P}^1(\mathbf{Q}_p)$, we will simplify the notation and write $\mathbf{D}$ instead of $\mathbf{D}(\mathbf{P}^1(\mathbf{Q}_p))$. For an arbitrary compact open set $X \subseteq \mathbf{P}^1(\mathbf{Q}_p)$, the scalar action of $\mathbf{Z}_p^\times$ on $U(X)$ induces a continuous action of $\mathbf{Z}_p^\times$ on $\mathbf{D}(X)$. Hence $\mathbf{D}(X)$ is endowed with a natural structure as continuous $\mathbf{Z}_p[[\mathbf{Z}_p^\times]]$-module.

3.3. Measure Spaces as Representation Spaces.

Let $M_2(\mathbf{Z}_p)$ denote the semigroup of 2×2 matrices over $\mathbf{Z}_p$. Viewing the elements of $\mathbf{Z}_p^2$ as row vectors, we let $M_2(\mathbf{Z}_p)$ act by matrix multiplication on the right. This induces an action of $M_2(\mathbf{Z}_p)$ on $\mathrm{Cont}(\mathbf{Z}_p^2)$ by the formula

$$(\sigma f)(v) = f(v\sigma), \text{ for } \sigma \in M_2(\mathbf{Z}_p) \text{ and } f \in \mathrm{Cont}(\mathbf{Z}_p^2).$$

Identifying $\mathrm{Cont}((\mathbf{Z}_p^2)')$ with the submodule of $\mathrm{Cont}(\mathbf{Z}_p^2)$ consisting of functions supported on $(\mathbf{Z}_p^2)'$, we see that $\mathrm{Cont}((\mathbf{Z}_p^2)') \subseteq \mathrm{Cont}(\mathbf{Z}_p^2)$ is preserved by the action of $M_2(\mathbf{Z}_p)$. We endow $\mathrm{Cont}((\mathbf{Z}_p^2)')$ with this action of $M_2(\mathbf{Z}_p)$ and endow $\mathbf{D}$ with the dual action. Hence, for $\mu \in \mathbf{D}$ and $\sigma \in M_2(\mathbf{Z}_p)$, $\mu|\sigma$ is determined by the integration formula

$$\int f\,d\mu|\sigma = \int (\sigma f)\,d\mu$$

for $f \in \mathrm{Cont}((\mathbf{Z}_p^2)')$. Note that this action commutes with the action of $\mathbf{Z}_p[[\mathbf{Z}_p^\times]]$ on $\mathbf{D}$ defined in section 3.2. Hence $\mathbf{D}$ is endowed with a natural structure as $\mathbf{Z}_p[[\mathbf{Z}_p^\times]][M_2(\mathbf{Z}_p)]$-module.

More generally, if X_1, X_2 are compact open subsets of $\mathbf{P}^1(\mathbf{Q}_p)$ and $\sigma \in M_2(\mathbf{Z}_p)$ satisfies $U(X_1)\sigma \cap (\mathbf{Z}_p^2)' \subseteq U(X_2)$, then σ induces a natural $\mathbf{Z}_p[[\mathbf{Z}_p^\times]]$-morphism

$$\mathbf{D}(X_1) \longrightarrow \mathbf{D}(X_2).$$

We will be interested in the special case $X_1 = X_2 = \mathbf{Z}_p$. Let $\Sigma_0(p)$ denote the subsemigroup of $M_2(\mathbf{Z}_p)$ defined by

$$\Sigma_0(p) = \left\{ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}_p) \;\middle|\; a \in \mathbf{Z}_p^\times, \text{ and } c \equiv 0 \text{ modulo } p \right\}.$$

A simple calculation confirms that $\Sigma_0(p)$ preserves $U(\mathbf{Z}_p)$, hence $\Sigma_0(p)$ induces a semigroup of endomorphisms of the $\mathbf{Z}_p[[\mathbf{Z}_p^\times]]$-module $\mathbf{D}(\mathbf{Z}_p)$.

3.4. Modular Symbols.

Let $\mathcal{D} := Div(\mathbf{P}^1(\mathbf{Q}))$ denote the group of divisors supported on the rational cusps $\mathbf{P}^1(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}$ of the upper half plane $\mathbf{H}$. Let $\mathcal{D}_0 \subseteq \mathcal{D}$ be the subgroup of divisors of degree zero. The group $GL_2(\mathbf{Q})$ acts by fractional linear transformations on $\mathcal{D}$ and on $\mathcal{D}_0$. If Σ is a subsemigroup of the semigroup $M_2(\mathbf{Z})$ of 2×2 integral matrices and if A is a right $\mathbf{Z}[\Sigma]$-module, then we define a right action of Σ on $\mathrm{Hom}_{\mathbf{Z}}(\mathcal{D}_0, A)$ by $\Phi \mapsto \Phi|\sigma$, for $\sigma \in \Sigma$, where

$$(\Phi|\sigma)(D) = \Phi(\sigma D)|\sigma$$

for all $D \in \mathcal{D}_0$.

(3.4.1) Definition. An element $\Phi \in \mathrm{Hom}_{\mathbf{Z}}(\mathcal{D}_0, A)$ will be called an A-valued *modular symbol* if the stabilizer of Φ in Σ contains a congruence subgroup of $SL_2(\mathbf{Z})$. If Γ is such a congruence subgroup then we say that Φ is a *modular symbol over* Γ. The module of all A-valued modular symbols will be denoted $\mathrm{Symb}(A)$ and the submodule of modular symbols over Γ will be denoted $\mathrm{Symb}_\Gamma(A)$.

Our interest in $\mathrm{Symb}_\Gamma(A)$ is motivated by the fact that this group is naturally isomorphic to the compactly supported cohomology group $H_c^1(\Gamma, A)$ whenever A is a $\mathbf{Z}[1/6][\Gamma]$-module (see **[A-S]**).

In this paper, A will be one of the modules $\mathbf{D}(X)$ or $L_k(R)$ where $k \geq 2$ is an integer. Here $\mathbf{D}(X)$ is the space of measures associated to a compact open subset X of $\mathbf{P}^1(\mathbf{Q}_p)$ as defined in (3.2.3) and $L_k(R) := Sym^{k-2}(R^2)$ is the R-module of homogeneous polynomials of degree $k-2$ in two variables X, Y with coefficients in a commutative ring R. We let Σ act on $L_k(R)$ by the formula $(F|g)(X,Y) = F\big((X,Y)g^*\big)$ for $g \in \Sigma$ and $F \in L_k(R)$, where $*$ is the main involution: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

(3.4.2) Definition. Fix an integer $k \geq 2$ and a commutative ring R. Then $\mathrm{Symb}(L_k(R))$ is called the module of *modular symbols of weight k over R.*

This terminology is motivated by the following well known example of Eichler and Shimura. Let $\mathcal{S}_k(\overline{\mathbf{Q}})$ be the space of weight k cusp forms of all levels having algebraic q-expansions and let $GL_2^+(\mathbf{Q})$ act on $\mathcal{S}_k(\overline{\mathbf{Q}})$ via the standard weight k action: for $f \in \mathcal{S}_k(\overline{\mathbf{Q}})$, and $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbf{Q})$, this action is given by $(f|\sigma)(z) := det(\sigma)^{k-1}(cz+d)^{-k}f(\sigma z)$ for z in the upper half-plane. To each $f \in \mathcal{S}_k(\overline{\mathbf{Q}})$ we associate the unique $\mathbf{Z}$-linear function $\psi_f : \mathcal{D}_0 \longrightarrow L_k(\mathbf{C})$ whose value on divisors of the form $\{c_2\} - \{c_1\} \in \mathcal{D}_0$, with $c_1, c_2 \in \mathbf{P}^1(\mathbf{Q})$ is given by

$$\psi_f\Big(\{c_2\} - \{c_1\}\Big) = 2\pi i \int_{c_1}^{c_2} f(z)(zX+Y)^{k-2}\,dz \tag{3.4.3}$$

where the integral is over the geodesic path in the upper half-plane joining c_1 to c_2. A straightforward calculation shows that for any $\sigma \in GL_2^+(\mathbf{Q})$ we have $\psi_f|\sigma = \psi_{f|\sigma}$. Hence ψ_f is a modular symbol of weight k over any congruence group for which f is modular.

3.5. Hecke Operators.

We define Hecke operators via the action of double cosets as in [**Sh2**]. For an arbitrary congruence subgroup $\Gamma \subseteq \Sigma$, we let $H(\Gamma, \Sigma)$ be the double coset algebra over $\mathbf{Z}$ associated to the pair (Γ, Σ). The action of $H(\Gamma, \Sigma)$ on A-valued modular symbols over Γ can be made explicit as follows. If $T(g) \in H(\Gamma, \Sigma)$ is the element associated to the double coset $\Gamma g \Gamma$, $g \in \Sigma$, then we can write $\Gamma g \Gamma$ as a finite disjoint union of right cosets, $\bigcup_i \Gamma g_i$. For a modular symbol $\Phi \in \mathrm{Symb}_\Gamma(A)$ we then define

$$\Phi|T(g) = \sum_i \Phi|g_i \in \mathrm{Symb}_\Gamma(A). \tag{3.5.1}$$

Now fix a positive integer M and let $\Sigma_0(M)$ be the subsemigroup of $GL_2(\mathbf{Q})$ consisting of non-singular integral matrices whose lower left-hand entry is divisible by M. Note that $\Gamma_0(M) := \Sigma_0(M) \cap SL_2(\mathbf{Q})$ is Hecke's congruence group of level M. We will make frequent use of the following standard Hecke operators $T_\ell(\ell$ prime), W_M, and $\iota \in H(\Gamma_0(M), \Sigma_0(M))$:

(3.5.2)

$$T_\ell = T\left(\begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}\right), \qquad W_M = T\left(\begin{pmatrix} 0 & -1 \\ M & 0 \end{pmatrix}\right), \qquad \iota = T\left(\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\right).$$

Note that the double cosets associated to each of the last two operators consists of only a single right coset. Hence the action of these operators on modular symbols (or modular forms, or cohomology) is given by the action of a single matrix. In particular, $\iota = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in \Sigma$ induces an involution $\Phi \mapsto \Phi|\iota$ on modular symbols. Hence, if multiplication by 2 is invertible on A, then we can decompose any modular symbol $\Phi \in \mathrm{Symb}_{\Gamma_0(N)}(A)$ in a unique way as a sum

$$\Phi = \Phi^+ + \Phi^- \tag{3.5.3}$$

where $\Phi^\pm|\iota = \pm\Phi^\pm$. Let $\mathrm{Symb}_{\Gamma_0(N)}(A) = \mathrm{Symb}_{\Gamma_0(N)}(A)^+ \oplus \mathrm{Symb}_{\Gamma_0(N)}(A)^-$ be the corresponding decomposition of the space of modular symbols.

We have the following theorem of Shimura [**Sh3**].

(3.5.4) THEOREM. *Let $f \in \mathcal{S}_k(\Gamma_0(M))$ be an common eigenform for the operators T_ℓ, ℓ prime, let $\mathcal{O}(f)$ be the ring of algebraic integers generated by the eigenvalues, and let $K(f)$ be the fraction field of $\mathcal{O}(f)$. Then for either choice of sign $\pm$, the Hecke eigenspace associated to f in $\mathrm{Symb}_{\Gamma_0(M)}(L_k(K(f)))^{\pm}$ is one dimensional over $K(f)$. Moreover, there are 'periods' $\Omega_f^{\pm} \in \mathbf{C}^\times$ such that the modular symbols $\varphi_f^{\pm} = (\Omega_f^{\pm})^{-1}\psi_f^{\pm}$ generate these eigenspaces and are defined over $\mathcal{O}(f)$, i.e. take values in $L_k(\mathcal{O}(f))$.*

3.6. The One-Variable p-adic L-functions of Mazur, Tate, and Teitelbaum.

Now suppose $M = Np$ where $p \nmid N$, and let $f \in \mathcal{S}_k(\Gamma_0(Np))$ be a p-ordinary eigenform. For simplicity we assume that the Fourier coefficients of f are rational integers, hence the eigenvalues of the operators T_ℓ are also integral. Let $a_p \in \mathbf{Z}$ be the eigenvalue of T_p on f. Our assumption that f is p-ordinary means just that a_p is not divisible by p. Now choose a real period Ω_f^+ as in theorem (3.5.4) so that the modular symbol $\varphi_f^+ := (\Omega_f^+)^{-1}\psi_f^+$ is defined over $\mathbf{Z}$. Define a measure $\nu_f \in \mathrm{Meas}(\mathbf{Z}_p^\times)$ by setting

$$\nu_f(a + p^m\mathbf{Z}_p) = a_p^{-m}\,\varphi_f^+\left(\left\{\frac{a}{p^m}\right\} - \{i\infty\}\right)\Bigg|_{X=0,Y=1} \tag{3.6.1}$$

for each $a \in \mathbf{Z}$ prime to p, and each $m > 0$. It follows from the fact that f is an eigenform for T_p with eigenvalue a_p that this defines a finitely additive function on the compact open subsets of $\mathbf{Z}_p^\times$. Since a_p is a p-adic unit, the values of ν_f are p-adic integers, hence the formulas above do indeed define an element $\nu_f \in \mathrm{Meas}(\mathbf{Z}_p^\times)$.

(3.6.2) Definition. The p-adic L-function associated to f and our fixed choice of a real period Ω_f^+ is defined to be

$$L_p(f,s) = L_p(\nu_f,s).$$

We have the following theorem.

(3.6.3) THEOREM. *Let s_0 be an integer with $0 < s_0 < k$. Then*

$$L_p(f,s_0) = a_p^{-m}\cdot\left(1 - a_p^{-1}\omega^{1-s_0}(p)p^{s_0-1}\right)\cdot\frac{\Lambda(f,\omega^{1-s_0},s_0)}{\Omega_f^+}.$$

For more details on the p-adic L-function and a proof of this theorem, see [**Mz-T-T**]. Note that the p-adic measure we have just described is a natural generalization to *p-stabilized* ordinary newforms of the p-adic measures associated to a p-ordinary newforms of conductor prime to p by Mazur and Swinnerton-Dyer [**Mz-SwD**]. Indeed, if g is a p-ordinary newform of conductor N, prime to p, and if f is the associated p-stabilized newform, then the measure associated to f as above is identical to the Mazur-Swinnerton-Dyer measure associated to the newform g.

3.7. p-Ordinary Λ-adic Modular Symbols.

As before, N is a positive integer that is not divisible by p. In this section we explain how one can lift the modular symbols associated to p-ordinary eigenforms $f \in \mathcal{S}_k(\Gamma_0(Np))$ to Λ-adic modular symbols, i.e. to elements of $\mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})$, where $\mathbf{D}$ is the $\mathbf{Z}_p[[\mathbf{Z}_p^\times]]$-module constructed in section 3.3. It is significant to notice that as we do this we remove the p from the level.

For an integer $k \geq 2$ we define the specializaton map $\phi_k : \mathbf{D} \longrightarrow L_k(\mathbf{Z}_p)$ by

$$\mu \overset{\phi_k}{\longmapsto} \int_{\mathbf{Z}_p^\times \times \mathbf{Z}_p} (xY - yX)^{k-2}\, d\mu(x,y). \tag{3.7.1}$$

A simple calculation shows that ϕ_k is a $\Gamma_0(Np)$-homomorphism. Hence ϕ_k induces a morphism $\mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D}) \xrightarrow{\phi_{k,*}} \mathrm{Symb}_{\Gamma_0(Np)}(L_k(\mathbf{Z}_p))$. Let $\phi^0_{k,*}$ denote the restriction of $\phi_{k,*}$ to the ordinary part. The key point is that we can determine both the image and the kernel of $\phi^0_{k,*}$.

Fix a topological generator $\gamma \in \mathbf{Z}_p^\times$ and let $[\gamma] \in \mathbf{Z}_p[[\mathbf{Z}_p^\times]]$ be the corresponding element of the completed group ring. For each $k \geq 2$, let $\pi_k := [\gamma] - \gamma^{k-2} \in \mathbf{Z}_p[[\mathbf{Z}_p^\times]]$. A straightforward calculation shows that $\pi_k \cdot \mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})$ is contained in the kernel of $\phi_{k,*}$. In fact, in [**G-S**] the following theorem is proved.

(3.7.2) THEOREM. *For each integer $k \geq 2$, the sequence*

$$0 \to \mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})^0 \xrightarrow{\pi_k} \mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})^0 \xrightarrow{\phi^0_{k,*}} \mathrm{Symb}_{\Gamma_0(Np)}(L_k(\mathbf{Z}_p))^0 \to 0$$

is an exact sequence of $\mathcal{H}$-modules.

We can refine this statement slightly by decomposing the exact sequence according to the action of the group μ_{p-1} of $(p-1)$th roots of unity. The canonical action of $\mathbf{Z}_p^\times$ on $\mathbf{D}$ restricts to an action of μ_{p-1}. For each integer r, let $\mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})_{\omega^r}$ be the Λ-submodule of $\mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})$ on which μ_{p-1} acts via ω^r. Now it is easy to see that π_k annihilates $\mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})_{\omega^r}$ unless $r \equiv k-2$ modulo $p-1$. Hence, letting $\lambda_k = [1+p] - (1+p)^{k-2} \in \Lambda$, we see that the theorem gives rise to the following exact sequence of Λ-modules.

$$0 \to \mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})^0_{\omega^{k-2}} \xrightarrow{\lambda_k} \mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})^0_{\omega^{k-2}} \xrightarrow{\phi^0_{k,*}} \mathrm{Symb}_{\Gamma_0(Np)}(L_k(\mathbf{Z}_p))^0 \to 0.$$

(3.7.3) COROLLARY. *The group $\mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})^0$ is a free Λ-module of finite rank. For each $k \geq 2$, the Λ-rank of $\mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})^0_{\omega^{k-2}}$ is equal to the $\mathbf{Z}_p$-rank of $\mathrm{Symb}_{\Gamma_0(Np)}(L_k(\mathbf{Z}_p))^0$.*

Proof. This is an immediate consequence of the above exact sequence and the compact version of Nakayama's Lemma.

(3.7.4) THEOREM. *Let E be a modular elliptic curve of tame conductor N with either good ordinary or multiplicative reduction at the prime $p \geq 5$. For simplicity, assume that Hida's deformation ring $\mathcal{R}_E$ satisfies Hypothesis (1.1.5): $\mathcal{R}_E = \Lambda$. Let $h_E : \mathcal{H} \longrightarrow \Lambda$ be the homomorphism given by Hida's theorem*

(1.1.2). Then for either choice of sign ±, the submodule of $\mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})^{0,\pm}$ *on which* $\mathcal{H}$ *acts via* h_E *has rank one as a* Λ*-module.*

Let $\psi_E \in \mathrm{Sym}_{\Gamma_0(Np)}(\mathbf{C})$ *be the modular symbol associated to the p-stabilized newform* f_E *as in (3.4.3) and fix a choice of periods* $\Omega_E^{\pm} \in \mathbf{C}^{\times}$ *as in theorem 3.5.4 so that the modular symbols* $\varphi_E^{\pm} := (\Omega_E^{\pm})^{-1}\psi_E^{\pm}$ *are defined over* $\mathbf{Z}_p$*, i.e.* $\varphi_E^{\pm} \in Symb_{\Gamma_0(Np)}(\mathbf{Z}_p)^{0,\pm}$*. Then there is a Hecke eigensymbol* $\Phi_E^{\pm} \in \mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})^{0,\pm}$ *such that*

(a) $\phi_{2,*}\Phi_E^{\pm} = \varphi_E^{\pm}$*, and*

(b) the Hecke operators act on $\Phi_E^{\pm}$ *via* h_E*.*

Sketch of the Proof. This is proved in detail in §6 of [G-S]. Here we will just recall the main ideas that go into the proof. The key observation is that the $\mathbf{Z}_p[[\mathbf{Z}_p^{\times}]][\Gamma_0(N)]$-module $\mathbf{D}$ is isomorphic to a projective limit of induced modules from the groups $\Gamma_r := \Gamma_0(N) \cap \Gamma_1(p^r)$ $(r \geq 1)$. More precisely, for each $r \geq 1$, let $\mathbf{D}_r := \left\{ \mu : \left((\mathbf{Z}/p^r\mathbf{Z})^2\right)' \longrightarrow \mathbf{Z}_p \right\}$ denote the module of $\mathbf{Z}_p$-valued functions on the set of *primitive* elements of $\left((\mathbf{Z}/p^r\mathbf{Z})^2\right)'$ equipped with the natural action of $\Gamma_0(N)$. The map $\Gamma_r\backslash\Gamma_0(N) \longrightarrow \left((\mathbf{Z}/p^r\mathbf{Z})^2\right)'$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (c,d) \bmod p^r$ is bijective hence induces an isomorphism $\mathbf{D}_r \cong \mathrm{Ind}_{\Gamma_r}^{\Gamma_0(N)}(\mathbf{Z}_p)$. Letting $\mathbf{D}_{r+1} \to \mathbf{D}_r$ $(r \geq 1)$ be defined by $\mu_{r+1} \mapsto \mu_r$, $\mu_r(x) = \displaystyle\sum_{y \equiv x \bmod p^r} \mu_{r+1}(y)$ we obtain a natural isomorphism $\mathbf{D} \cong \varprojlim_r \mathbf{D}_r$. A calculation confirms that the following diagram is commutative

$$\begin{tikzcd}
H^1_*(\Gamma_0(N),\, \mathbf{D}_{r+1}) \arrow[r] \arrow[d, "\sim"'] & H^1_*(\Gamma_0(N),\, \mathbf{D}_r) \arrow[d, "\sim"'] \\
H^1_*(\Gamma_{r+1},\, \mathbf{Z}_p) \arrow[r, "\mathrm{cores}"] & H^1_*(\Gamma_r,\, \mathbf{Z}_p)
\end{tikzcd}$$

where H^1_* denotes either H^1, H^1_c (compact supports), or H^1_{par} (parabolic cohomology := image of and H^1_c in H^1) and the vertical isomorphisms are obtained from Shapiro's theorem. Passing to the limit we thus obtain a natural isomorphism

$$H^1_*(\Gamma_0(N),\, \mathbf{D}) \cong \varprojlim_r H^1_*(\Gamma_r,\, \mathbf{Z}_p).$$

Now it is well known that there is an isomorphism of (covariant) Hecke modules $H^1_{\mathrm{par}}(\Gamma_r,\, \mathbf{Z}_p) \cong Ta_p(J_r)$ for each $r \geq 1$ (see [Sh], chapter 8), hence we obtain an isomorphism of (covariant) Hecke modules

$$H^1_{\mathrm{par}}(\Gamma_0(N),\, \mathbf{D}) \cong Ta_p(J_\infty).$$

(A small technical problem arises here since the Hecke operators defined in §3.5 are the *contravariant* ones; but we can salvage this by "turning the action around" by composing the above isomorphism with the W-operator W_N).

Applying Hida's theorem (1.1.2)(3) to this isomorphism we conclude that for either choice of sign ±, the h_E-eigensubmodule of $H^1_{\text{par}}(\Gamma_0(N),\,\mathbf{D})^{\pm,0}$ has rank one. Since $\text{Symb}_{\Gamma_0(N)}(\mathbf{D}) \cong H^1_c(\Gamma_0(N),\,\mathbf{D})$, we have a surjective map

$$\text{Symb}_{\Gamma_0(N)}(\mathbf{D}) \longrightarrow H^1_{\text{par}}(\Gamma_0(N),\,\mathbf{D})$$

whose kernel is "Eisenstein" (in particular, if ℓ is prime $\equiv 1 \bmod N$, then T_ℓ acts on the kernel by $1+\ell[\ell]$), hence the kernel has no nontrivial h_E-eigenvectors. It follows that the above map induces an injective homomorphism

$$\text{Symb}_{\Gamma_0(N)}(\mathbf{D})_{h_E} \longrightarrow H^1_{\text{par}}(\Gamma_0(N),\,\mathbf{D})_{h_E}$$

on the h_E-eigensubmodules and moreover that the cokernel of this map is a torsion Λ-module whose annihilator is not contained in the augmentation ideal. Theorem 3.7.4 is now an easy consequence.

3.8. Two-variable p-adic L-functions.

In this section, we will give a construction of two-variable p-adic L-functions based on the ideas of this chapter (compare Kitagawa [**Ki**], this volume). We are going to impose our simplifying hypothesis (1.1.5), but the general case is not much harder.

Let E be a modular elliptic curve defined over $\mathbf{Q}$ having conductor M and either good ordinary or multiplicative reduction at p. Choose a real period Ω_E for E so that the normalized modular symbol $\varphi_E = \Omega_E^{-1}\cdot\varphi_E \in \text{Symb}_{\Gamma_0(pN)}(\mathbf{Z}_p)^0$ takes p-integral values and let $L_p(E,s)$ be the associated p-adic L-function defined as in (3.6.2). Assume, for simplicity, that $\mathcal{R}_E \cong \Lambda$ and let $h_E : \mathcal{H} \longrightarrow \Lambda$ be the homomorphism of theorem 1.1.2.

Let f_E be the p-stabilized ordinary newform associated to E and let N be the tame conductor of f_E. The relationship between M and N is given by

$$M = \begin{cases} N & \text{if } E \text{ has good reduction at } p; \\ \\ Np & \text{if } E \text{ has multiplicative reduction at } p. \end{cases}$$

The Atkin-Lehner operators W_N, W_M act as involutions on $S_k(\Gamma_0(Np))$ and preserve the eigenspace spanned by f_E. Hence we have $f_E|W_N = w_N f_E$ and $f_E|W_M = w_M f_E$ where $w_N = \pm 1$ and $w_M = \pm 1$. Now it is a well known fact that $-w_M$ is the sign of the functional equation of E, i.e. in the notation of section 3.0, $\Lambda_\infty(E, 2-s) = -w_M\Lambda_\infty(E,s)$. Moreover, Mazur, Tate, and Teitelbaum showed that the p-adic L-function satisfies the functional equation $\Lambda_p(E,2-s) = -w_N\Lambda_p(E,s)$. (This functional equation is also a consequence of theorem 3.8.1 below). Hence $\epsilon_\infty = -w_M$ and $\epsilon_p = -w_N$.

The relationship between ϵ_∞ and ϵ_p described in (3.0.1) follows easily from this description of ϵ_∞ and ϵ_p. Indeed, if E has good reduction at p, then $M = N$, hence $w_M = w_N$. We know by Deligne-Rapoport [**D-R**] that E has multiplicative reduction at p if and only if $a_p = \pm 1$ and in that case a standard result of Atkin and Lehner tells us $w_M = -a_p w_N$. Combining these two cases we see that

$w_M = -w_N$ if and only if $a_p = 1$, which, according to [D-R], is equivalent to saying that E has split multiplicative reduction at p.

(3.8.1) THEOREM. *Let $\alpha_p = h_E(T_p) \in \Lambda$ and let $\alpha_p(k)$, $k \in \mathbf{Z}_p$, be the Iwasawa function associated to α_p as in 1.1.3. Then there are functions $L_p(k,s)$, $k, s \in \mathbf{Z}_p$ and $L_p^*(k,1)$, $k \in \mathbf{Z}_p$, which are Iwasawa functions in each of the p-adic variables k and s, and which satisfy the following properties.*

1. $L_p(2,s) = L_p(E,s)$ *for all* $s \in \mathbf{Z}_p$.
2. $L_p(k,s) = \epsilon_p \cdot \langle N\rangle^{\frac{k}{2}-s} \cdot L_p(k, k-s)$.
3. $L_p(k,1) = \left(1 - \alpha_p(k)^{-1}\right) L_p^*(k,1)$.
4. $L_p^*(2,1) = \left(1 - \dfrac{\beta}{p}\right) \dfrac{L_\infty(E,1)}{\Omega_E}$.

Proof. Let $\nu_E \in \mathrm{Meas}(\mathbf{Z}_p^\times)$ be the p-adic measure associated to the pair (E, Ω_E) as in (3.6.1). Let $\Phi_E = \Phi_E^+ \in \mathrm{Symb}_{\Gamma_0(N)}(\mathbf{D})^{0,+}$ be a Λ-adic modular symbol satsifying the conclusions of theorem 3.7.4. Let $\mu = \mu_E = \Phi_E(\{0\} - \{i\infty\}) \in \mathbf{D}$ and let $\nu \in \mathrm{Meas}(\mathbf{Z}_p^\times)$ be the measure determined by the integration formulas

$$\int f\, d\nu = \int_{\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times} f(y/x)\, d\mu(x,y)$$

for $f \in \mathrm{Cont}(\mathbf{Z}_p^\times)$. Now define the functions $L_p(k,s)$ and $L_p^*(k,1)$ by

$$L_p(k,s) = L_p(\mu,k,s) \qquad\qquad L_p^*(k,1) = L_p^*(\mu,k,1)$$

where the p-adic L-functions $L_p(\mu,-,-)$, $L_p^*(\mu,-,-)$ are as defined in (3.1.2).

To prove **1** we must prove $\nu = \nu_E$. So fix $a \in \mathbf{Z}_p^\times$ and $n > 0$. We have $\nu(a + p^n\mathbf{Z}_p) = \mu_E(U(a + p^n\mathbf{Z}_p))$. On the other hand, for each $\mathbf{x} \in \mathbf{P}^1(\mathbf{Q}_p)$, we choose a matrix $\beta(\mathbf{x}, p^n) \in \Sigma_0(N)$, one of whose rows is in $U(\mathbf{x}, p^n)$ and whose determinant is p^n. Now let $\mu_{\mathbf{x},p^n} = \Phi|\beta(\mathbf{x},p^n)(\{0\} - \{i\infty\}) \in \mathbf{D}$. It follows easily from the definitions that $\mu_{\mathbf{x},p^n}$ is supported on $U(\mathbf{x},p^n)$. We therefore have $\alpha_p^n\mu = \sum_{\mathbf{x}\in\mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z})} \mu_{\mathbf{x},p^n}$.

We therefore have

$$a_p^n\nu(a+p^n\mathbf{Z}_p) = a_p^n\cdot\mu(U(a+p^n\mathbf{Z}_p)) = (\alpha_p^n\mu)(U(a+p^n\mathbf{Z}_p)) = \mu_{a,p^n}(U(a+p^n\mathbf{Z}_p)).$$

But $\mu_{a,p^n} = \Phi\left(\left\{\frac{a}{p^n}\right\} - \{i\infty\}\right)|\beta(a,p^n)$ so we have

$$\mu_{a,p^n}(U(a+p^n\mathbf{Z}_p)) = \Phi\left(\left\{\frac{a}{p^n}\right\} - \{i\infty\}\right)(U(\mathbf{Z}_p)) = \varphi_E\left(\left\{\frac{a}{p^n}\right\} - \{i\infty\}\right).$$

Hence $\nu(a+p^n\mathbf{Z}_p) = a_p^{-n}\varphi_E\left(\left\{\frac{a}{p^n}\right\} - \{i\infty\}\right) = \nu_E(a+p^n\mathbf{Z}_p)$. This proves **1.**

To prove **2**, we first show $\mu|\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} = \epsilon_p[\langle N\rangle^{1/2}]\mu$. Indeed, since $\Phi|W_N^2 = \Phi|[-N] = [\langle N\rangle]\Phi$, we have $\Phi|W_N = \pm w_N[\langle N\rangle^{1/2}]\Phi$. Applying $\phi_{2,*}$ and using the fact that $\varphi_E|W_N = w_N\varphi_E$, we obtain $\Phi|W_N = w_N[\langle N\rangle^{1/2}]\Phi$. Now evaluate both sides of this identity on the divisor $\{0\} - \{i\infty\} \in \mathcal{D}_0$. Since the action of

W_N on Φ is given by the action of $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$, and since this matrix interchanges the cusps 0 and $i\infty$, the identity $\mu|\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} = \epsilon_p[\langle N\rangle^{1/2}]\mu$ follows from the equality $\epsilon_p = -w_N$. A simple calculation shows that **2** is just a reformulation of this identity.

Recall the identity $\alpha_p^n\mu = \sum_{\mathbf{x}\in\mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z})}\mu_{\mathbf{x},p^n}$. Setting $n = 1$ gives us

$$\alpha_p\mu = \sum_{\mathbf{x}\in\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})}\mu_{\mathbf{x},p}.$$

A simple calculation shows that

$$\alpha_p(k)\cdot L_p(k,s) = \sum_{a=1}^{p-1}\int \langle x\rangle^{k-2}\langle y/x\rangle^{s-1}\,d\mu_{a,p}(x,y)$$
$$\alpha_p(k)\cdot L_p^*(k,s_0) = \sum_{a=0}^{p-1}\int \langle x\rangle^{k-2}\langle y/x\rangle^{s_0-1}\,d\mu_{a,p}(x,y)$$

Hence, $\alpha_p(k)\cdot\big(L_p^*(k,1) - L_p(k,1)\big) = \int\langle x\rangle^{k-2}\,d\mu_{0,p}(x,y)$. But $\mu_{0,p}$ is given by $\mu_{0,p} = \mu|\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ and the function $(x,y)\mapsto\langle x\rangle^{k-2}$ on $U(\mathbf{Z}_p)$ is fixed by $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. It follows that the last integral is equal to

$$L_p^*(k,1) = \int_{U(\mathbf{Z}_p)}\langle x\rangle^{k-2}\,d\mu(x,y).$$

This proves $\alpha_p(k)\cdot\big(L_p^*(k,1) - L_p(k,1)\big) = L_p^*(k,1)$ and **3** follows.

Finally, we have $L_p^*(2,1) = \mu(\mathbf{Z}_p^\times\times\mathbf{Z}_p) = \phi_2\mu = \varphi_E(\{0\}-\{i\infty\}) = \dfrac{L_\infty(f_E,1)}{\Omega_E}$. Hence $L_p^*(2,1) = \dfrac{L_\infty(f_E,1)}{\Omega_E}$ and **4** follows from the equality $(1-\beta p^{-s})\cdot L_\infty(E,s) = L_\infty(f_E,s)$.

§4. Proof of the Main Theorem

In this section we prove our main theorem.

(4.1) THEOREM. *Let E be a modular elliptic curve over $\mathbf{Q}$ with split multiplicative reduction at the prime $p\ge 5$. Let Ω_E be the Neron period of E and let $L_p(E,s)$ be the associated p-adic L-function. Then*

$$\frac{d}{ds}L_p(E,s)\bigg|_{s=1} = \mathcal{L}_p(E)\cdot\frac{L_\infty(E,1)}{\Omega_E}.$$

Proof. We will give the proof only under the simplifying assumption that $\mathcal{R}_E = \Lambda$. Since E has split multiplicative reduction at p we have $\epsilon_p = -\epsilon_\infty$ by (3.0.1).

In case $\epsilon_p = 1$, the p-adic L-function has an even order zero at $s = 1$ and the complex L-function has an odd order zero at $s = 1$. Hence, in this case, the theorem is trivially true, since both sides of the desired equality vanish.

Now assume $\epsilon_p = -1$. Let $L_p(k, s)$ be a two variable p-adic L-function satisfying the properties listed in Theorem 3.0.2. From the functional equation (3.0.2.b) it follows that $L_p(k, k/2) = 0$ identically for $k \in \mathbf{Z}_p$. In particular, the linear terms in the Taylor expansion of $L_p(k, s)$ around the point $(k, s) = (2, 1)$ must vanish along the line $s = k/2$. Hence, there is a constant $c \in \mathbf{Z}_p$, such that

$$L_p(k, s) \sim c \cdot \left((s-1) - \frac{1}{2}(k-2)\right) \tag{4.2}$$

where $f(k, s) \sim g(k, s)$ means that the Taylor expansions of f and g at $(k, s) = (2, 1)$ agree modulo terms of order ≥ 2. The theorem will follow by calculating c in two ways.

Setting $k = 2$ in (4.2) and applying theorem (3.0.2.a) we obtain $L_p(E, s) \sim c(s-1)$, hence

$$c = \frac{d}{ds} L_p(E, s)\Big|_{s=1} . \tag{4.3}$$

On the other hand, setting $s = 1$ in (4.2) and using theorem (3.0.2.c) we obtain

$$\left(1 - \alpha_p(k)^{-1}\right) L_p^*(k, 1) \sim -\frac{1}{2} c(k-2). \tag{4.4}$$

Now recall from theorem 2.0.1 that $\alpha_p(2) = 1$. Hence differentiating (4.4) with respect to k and setting $k = 2$ gives us $-\frac{1}{2}c = \alpha_p'(2) L_p^*(2, 1)$. But by theorem 2.0.1 we also have $\alpha_p'(2) = -\frac{1}{2}\mathcal{L}_p(E)$, and by theorem (3.0.2.d) we have $L_p^*(2, 1) = \dfrac{L_\infty(E, 1)}{\Omega_E}$, so this last identity is equivalent to

$$-\frac{1}{2}c = -\frac{1}{2}\mathcal{L}_p(E) \cdot \frac{L_\infty(E, 1)}{\Omega_E}. \tag{4.5}$$

The theorem now follows immediately from a comparison of (4.3) and (4.5).

§5. Final Remarks

In this section we add a few final remarks.

(5.1) Proposition. *Let E be a modular elliptic curve with split multiplicative reduction at the prime $p \geq 5$. Suppose $\mathcal{L}_p(E) \notin p\mathbf{Z}_p$. Then*

$$\mathcal{R}_E \neq \Lambda.$$

Moreover, if N is the tame conductor (so the conductor is Np), then there is a weight two newform f of conductor N such that

$$f \equiv f_E \text{ modulo } p.$$

Remark. The hypothesis $\mathcal{L}_p(E) \notin p\mathbf{Z}_p$ in the proposition is equivalent to assuming that $p|ord_p(q_E)$ (or equivalently that $p|ord_p(j_E)$) and that the representation of $Gal(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ on the p-torsion group $E[p]$ is a *nonsplit* extension of $\mathbf{Z}/p\mathbf{Z}$ by μ_p. (In Serre's terminology this is equivalent to saying that $E[p]$ is "*un peu*" wildly ramified at p). Hence the conclusion that there is a newform f of conductor N satisfying the above congruence is a special case of Serre's conjecture (see [**S**] §2.9) and is a consequence of the work of Ribet [**R**].

Proof. Let E be a modular elliptic curve satisfying the hypotheses of the proposition. Let $\mathcal{R}_E$ be Hida's deformation ring and $h_E : \mathcal{H} \longrightarrow \mathcal{R}_E$ be the homomorphism associated to E as in proposition 1.1.2. Let $\alpha_p = h_E(T_p) \in \mathcal{R}_E$. Then according to theorem 2.0.1 $\alpha_p'(2) = -\frac{1}{2}\mathcal{L}_p(E) \notin p\mathbf{Z}_p$. But a simple calculation shows that the derivative of an arbitrary Iwasawa function takes values in $p\mathbf{Z}_p$. Hence, $\alpha_p(k)$ is not an Iwasawa function, and therefore $\alpha_p \notin \Lambda$. This proves the first assertion: $\mathcal{R}_E \neq \Lambda$.

To prove the second assertion, we need to recall another result due to Hida. Let $\mathbf{f} := \mathbf{f}_E \in \mathcal{R}_E[[q]]$ be the Λ-adic cusp form associated to f_E as in theorem 1.1.2. Let $\mathcal{X}_E := Hom_{cont}(\mathcal{R}_E, \overline{\mathbf{Q}}_p)$ be the set of continuous homomorphisms $\kappa : \mathcal{R}_E \longrightarrow \overline{\mathbf{Q}}_p$. Following Hida's conventions we refer to the elements of $\mathcal{X}_E$ as the "points" of $\mathcal{R}_E$ and view the elements of $\mathcal{R}_E$ as functions on $\mathcal{X}_E$ by setting $\alpha(\kappa) := \kappa(\alpha)$ for $\alpha \in \mathcal{R}_E$ and $\kappa \in \mathcal{X}_E$. Let $\sigma_0 : \Lambda \longrightarrow \mathbf{Z}_p$ be the augmentation homomorphism whose kernel is the augmentation ideal P_0. We say that a point $\kappa \in \mathcal{X}_E$ lies over σ_0 if the restriction of κ to Λ is σ_0. For each $\kappa \in \mathcal{X}_E$ we let

$$\mathbf{f}_\kappa := \sum_{n=1}^{\infty} \alpha_n(\kappa) q^n \in \overline{\mathbf{Q}}_p[[q]]$$

be the q-expansion obtained by specializing $\mathbf{f}$ to κ. We are interested in the q-expansions $\mathbf{f}_\kappa$ for κ lying over σ_0. The following result is due to Hida.

LEMMA. *The Λ-algebra $\mathcal{R}_E$ is unramified over the augmentation ideal $P_0 \subseteq \Lambda$. Moreover, for each $\kappa \in \mathcal{X}_E$ lying over σ_0, $\mathbf{f}_\kappa$ is a p-stabilized ordinary newform of tame conductor N.*

We can now prove the second assertion of the proposition. Let $\kappa_0 \in \mathcal{X}_E$ be the point for which $\mathbf{f}_{\kappa_0} = f_E$. We are going to prove that there is another point κ of $\mathcal{R}_E$ lying over σ_0 for which $\mathbf{f}_\kappa$ is not a newform of conductor Np. The proposition will then follow easily from Hida's theorem. Indeed, by Hida's theorem we know that $\mathbf{f}_\kappa$ is an ordinary p-stabilized newform of *tame* conductor N. Thus, if $\mathbf{f}_\kappa$ is not a newform, there must be a newform g of conductor N such that

$$\mathbf{f}_\kappa(z) = f(z) - \beta f(pz)$$

for z in the upper half plane, where β is the non-unit root of frobenius at p for f. In particular, $f \equiv \mathbf{f}_\kappa \equiv f_E$ modulo p.

To prove that there is such a point κ for which $\mathbf{f}_\kappa$ is not new, we use the following criterion.

Criterion. Suppose $\kappa \in \mathcal{X}_E$ lies over σ_0. Then f_κ is a newform $\iff \alpha_p(\kappa) = 1$.

Indeed, if $\mathbf{f}_\kappa$ is a newform, then $\alpha_p(\kappa) = \pm 1$, but since $\alpha_p(\kappa) \equiv \alpha_p(\kappa_0) = 1$ modulo p we have $\alpha_p(\kappa) = 1$. Conversely, if $\mathbf{f}_\kappa$ is not a newform, then $\alpha_p(\kappa)$ is one of the two roots of frobenius at p for a newform of conductor N. Hence $|\alpha_p(\kappa)| = \sqrt{p}$ by the Weil bounds, and in particular $\alpha_p(\kappa) \neq 1$. This establishes the criterion.

The proposition will therefore follow if we can show that $\alpha_p(\kappa) \neq 1$ for some κ lying over σ_0. Suppose, to the contrary, that $\alpha_p(\kappa) = 1$ for every such κ. Let $P(X) = X^n + \lambda_1 X^{n-1} + \cdots + \lambda_n \in \Lambda[X]$ be the minimal polynomial of $\alpha_p - 1$ over Λ and let $\mathcal{K}$ be the splitting field of $P(X)$ over the fraction field of Λ. The element $T = [1+p] - 1 \in \Lambda$ generates P_0. Let $\Lambda_{(T)}$ denote the localization of Λ at (T) and let $\mathcal{R}$ be the integral closure of $\Lambda_{(T)}$ in $\mathcal{K}$. Then $\Lambda_{(T)}$ is a discrete valuation ring and, by Hida's theorem, $\mathcal{R}$ is a Dedekind domain finite over $\Lambda_{(T)}$. Since we have assumed $\alpha_p(\kappa) = 1$ for all $\kappa \in \mathcal{X}_E$ lying over σ_0, it follows that $\alpha_p - 1$ is in every maximal ideal of $\mathcal{R}$. Hence $\dfrac{\alpha_p - 1}{T} \in \mathcal{R}$. But the minimal polynomial $Q(X) \in \Lambda_{(T)}[X]$ of $\dfrac{\alpha_p - 1}{T}$ over $\Lambda_{(T)}$ is given by

$$Q(X) = X^n + \lambda_1 T^{-1} X + \cdots + \lambda_n T^{-n}.$$

Hence $T^i|\lambda_i$ in $\Lambda_{(T)}$ for each $1 = 1, \ldots, n$ and consequently $T^i|\lambda_i$ in Λ for each i. Hence $\gamma := \dfrac{\alpha_p - 1}{T}$ is integral over Λ. But a simple calculation shows that

$$\gamma(2) = -\frac{1}{2}\frac{\mathcal{L}_p(E)}{\log_p(1+p)}$$

which is not integral over $\mathbf{Z}_p$, since, by hypothesis, $\mathcal{L}_p(E) \notin p\mathbf{Z}_p$. This gives us a contradiction and the proposition is proved.

5.2. Example.

Let f be the newform of conductor 280 labeled 280B in Cremona's tables [**Cr**]. Then f has rational fourier coefficients and there is an elliptic curve $E_{/\mathbf{Q}}$ for which $L(f,s) = L(E,s)$. Cremona's calculations strongly suggest (but do not prove) that $E = E'$ where E' is the curve $y^2 = x^3 - 412x + 3316$ of conductor 280 labeled 280B1 in the tables. Now E' has split multiplicative reduction at 5 and its $\mathcal{L}$-invariant is easily seen to satisfy the congruence

$$\mathcal{L}_5(E') \equiv 1 \text{ modulo } 5.$$

Indeed, the j-invariant is $j_{E'} = -30211716096/(5^5 \cdot 7^3)$, hence $ord_5(q_{E'}) = 5$ and, writing $q_{E'} = 5^5 \cdot u$ where $u \in \mathbf{Z}_5^\times$, we have $u \equiv 17$ modulo 25. Hence $\langle u \rangle \equiv 6$ modulo 25 and therefore $\log_p q_{E'} \equiv 5$ modulo 25. The congruence $\mathcal{L}_5(E') \equiv 1$ modulo 5 follows.

Now suppose that $E \cong E'$ (as predicted by the Taniyama-Shimura-Weil conjecture). Then, since $5 \nmid \mathcal{L}_5(E)$, proposition 5.1 implies $\mathcal{R}_E$ is not isomorphic to Λ and, moreover, that there is a newform f_1 of conductor 56 with $f_1 \equiv f$ mod 5.

According to the Antwerp tables [**B-K**] the space of weight two newforms of conductor 56 is two-dimensional and is spanned by two eigenforms with rational fourier coefficients, labeled $56A$ and $56C$ in the tables. By inspection, we see that the second of these newforms is not conguent to f modulo 5. Hence f_1 must be the newform labeled $56A$ in the Antwerp tables (which, according to the tables, is probably associated to the elliptic curve $E_1 : y^2 = x^3 - x^2 - 4$).

We therefore expect that there is a congruence $f \equiv f_1$ modulo 5. Indeed, the tables confirm that

$$a_n(f) \equiv a_n(f_1) \text{ modulo } 5, \qquad \text{for } n \leq 100.$$

The full congruence would follow from the above arguments if we could prove $E \cong E'$, or even if we could just prove that the representation of $Gal(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ on $E[5]$ is a *nonsplit* extension of $\mathbf{Z}/p\mathbf{Z}$ by μ_p.

References

[**A-S**] Ash, A., Stevens, G.: Modular forms in characteristic ℓ and special values of their L-functions. *Duke Math. J.* **53** (1986), No.3, 849-868.

[**Cr**] Cremona, J.E.: *Algorithms for modular elliptic curves.* Cambridge; New York, NY, USA: Cambridge University Press, 1992.

[**D**] Deligne, P.: Formes modulaires et représentations ℓ-adiques. Seminaire Bourbaki **355** (1969).

[**B-K**] Birch, B.J., Kuyk, W.: *Modular Forms of One Variable.* Lecture Notes in Mathematics **476**, Springer-Verlag, Berlin-Heidelberg-New York, 1975.

[**D-R**] Deligne, P., Rapoport, M.: Schémas de modules de courbes elliptiques. *Lect. Notes Math.*, **349** (1973), 143-316.

[**F-G**] Ferrero, B., Greenberg, R.: On the behaviour of p-adic L-functions at $s = 0$. *Invent. Math.* **50** (1978), 91-102.

[**G-S**] Greenberg, R., Stevens, G.: p-adic L-functions and p-adic periods of modular forms. *Invent. Math.* **111** (1993), 401-447.

[**H1**] Hida, H.: Galois representations into $GL_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms. *Invent. Math.* **85** (1986), 545-613.

[**H2**] Hida, H.: Iwasawa modules attached to congruences of cusp forms. *Ann. Sci. École Norm. Sup.* **19** (1986), 231-273.

[**Kz**] Katz, N.: p-Adic L-Functions for CM Fields. *Invent. Math.* **49** (1978), 199-297.

[**Ki**] Kitagawa, K.: On standard p-adic L-functions of families of elliptic cusp forms. This volume.

[**M1**] Manin, J.: Non-archimedean integration and p-adic Hecke-Langlands L-series, *Russian Math. Surveys*, **31**(1) (1972), 5-54.

[M2] Manin, J.: Periods of parabolic forms and p-adic Hecke series. *Math. Sbornik V*, 93 (134), (11), 1973.

[M-V] Manin, J., Vishik, S.: p-adic Hecke series for quadratic imaginary fields. *Math. Sbornik* (137), No. 3 (11), 1974.

[Mz] Mazur, B.: Two-variable p-adic L-functions. Unpublished Harvard Lecture Notes (1985).

[Mz-SwD] Mazur, B., Swinnerton-Dyer, P.: Arithmetic of Weil curves. *Invent. Math.* **25** (1974), 1-61.

[Mz-T-T] Mazur, B., Tate, J., Teitelbaum, J.: On p-adic analogs of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.* **84** (1986), 1-48.

[Mz-W] Mazur, B., Wiles, A.: On p-adic analytic families of Galois representations. *Compositio Math.* **59** (1986), 231-264.

[O] Ohta, M.: On ℓ-adic representations attached to automorphic forms. *Japan J. Math.* **8**, No. 1 (1982), 1-47.

[R] Ribet, K.: On modular representations of $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.* **100** (1990), 431-476.

[S] Serre, J-P.: Sur les représentations modulaires de degré 2 de $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.* **54**, No. 1 (1987), 179-230.

[Sh1] Shimura, G.: An ℓ-adic method in the theory of automorphic forms. (1968), unpublished.

[Sh2] Shimura, G.: *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton University Press, 1971.

[Sh3] Shimura, G.: On the periods of modular forms. *Math. Ann.* **229** (1977), 211-221.

[W] Wiles, A.: On ordinary λ-adic representations associated to modular forms. *Invent. Math.* **94** (1988), 529-573.

Mathematics Department, University of Washington, Seattle, WA 98195
E-mail address: greenber@math.washington.edu

Mathematics Department, Boston University, Boston, MA 02215
E-mail address: ghs@math.bu.edu