National Academy of Sciences Colloquium

Elliptic Curves and Modular Forms

(NAS Colloquium) Elliptic Curves and Modular Forms

ISBN
978-0-309-05875-9

39 pages
8.5 x 11
1998

Proceedings of the National Academy of Sciences

COLLOQUIUM

ON

ELLIPTIC CURVES AND MODULAR FORMS

NATIONAL ACADEMY OF SCIENCES

WASHINGTON, D.C. 1997

NATIONAL ACADEMY OF SCIENCES

Colloquium Series

In 1991, the National Academy of Sciences inaugurated a series of scientific colloquia, five or six of which are scheduled each year under the guidance of the NAS Council's Committee on Scientific Programs. Each colloquium addresses a scientific topic of broad and topical interest, cutting across two or more of the traditional disciplines. Typically two days long, colloquia are international in scope and bring together leading scientists in the field. Papers from colloquia are published in the *Proceedings of the National Academy of Sciences (PNAS).*

SPEAKERS

Elliptic Curves and Modular Forms

National Academy of Sciences

Washington, DC
March 15–17, 1996

Ken Ribet (UNIVERSITY OF CALIFORNIA, BERKELEY)
John Coates (UNIVERSITY OF CAMBRIDGE)
Bernadette Perrin-Riou (UNIVERSITE DE PARIS-SUD)
Kazuya Kato (TOKYO INSTITUTE OF TECHNOLOGY)
Haruzo Hida (UNIVERSITY OF CALIFORNIA, LOS ANGELES)
Ralph Greenberg (UNIVERSITY OF WASHINGTON)
Robert Coleman (UNIVERSITY OF CALIFORNIA, BERKELEY)
Goro Shimura (PRINCETON UNIVERSITY)
Jean-Marc Fontaine (UNIVERSITE DE PARIS-SUD)
Gerald Faltings (MAX-PLACK-INSTITUT, BONN)
Fred Diamond (UNIVERSITY OF CAMBRIDGE)
Richard Taylor (OXFORD UNIVERSITY)

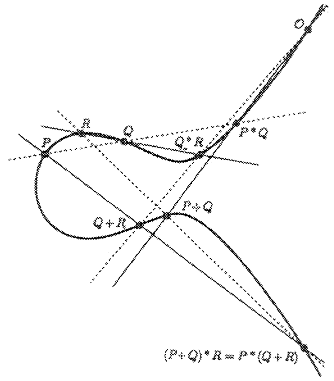
PROCEEDINGS

OF THE

NATIONAL ACADEMY OF SCIENCES

OF THE UNITED STATES OF AMERICA

Table of Contents



The amazing consequences of elliptic curves play a key role in the number theory. Elliptic curves are smooth cubic plane curves with a "flex point" at infinity. As has been known for centuries, there is a natural way of "adding" two points on an elliptic curve to get a third so that the sum of any three collinear points yields the point at infinity. In the diagram above, the graph of an elliptic curve is drawn, along with straight lines illustrating the associativity of the law of addition.

Papers from a National Academy of Sciences Colloquium on Elliptic Curves and Modular Forms

Proc. Natl. Acad. Sci. USA
Vol. 94, p. 11109, October 1997
Colloquium Paper

This paper is an introduction to the following papers, which were presented at a colloquium entitled "Elliptic Curves and Modular Forms," organized by Barry Mazur and Karl Rubin, held March 15–17, 1996, at the National Academy of Sciences in Washington, DC.

Introduction

BARRY MAZUR[*] AND KARL RUBIN[†]

[*]Department of Mathematics, Harvard University, Cambridge, MA 02138; and [†]Department of Mathematics, Ohio State University, Columbus, OH 43210

The colloquium "Elliptic Curves and Modular Forms" was held at the National Academy of Sciences in Washington, DC, March 15–17, 1996. The topics covered by this colloquium have been extraordinarily active lately. These topics have played an essential role in some of the exciting recent work on classical problems, including Fermat's Last Theorem. They will surely continue to be central to further developments in Number Theory. The 11 articles to follow are the texts of addresses given during this colloquium. These articles range from the study of "p-adic Galois representations, L functions, modular forms, and the p-adic congruences they satisfy" (as in the articles by John Coates, Robert Coleman, Fred Diamond, Jean-Marc Fontaine, Ralph Greenberg, Haruzo Hida, Bernadette Perrin-Riou, and Richard Taylor) to the study of the delicate geometry of modular curves and Shimura varieties (as in the articles by Gerd Faltings and Ken Ribet) to the analytic number-theoretic study of Zeta functions and Eisenstein series of classical groups (as in the article by Goro Shimura).

Proc. Natl. Acad. Sci. USA
Vol. 94, pp. 11110–11114, October 1997
Colloquium Paper

This paper was presented at a colloquium entitled "Elliptic Curves and Modular Forms," organized by Barry Mazur and Karl Rubin, held March 15–17, 1996, at the National Academy of Sciences in Washington, DC.

Parametrizations of elliptic curves by Shimura curves and by classical modular curves

KENNETH A. RIBET AND SHUZO TAKAHASHI

Mathematics Department, University of California, Berkeley, CA 94720-3840

ABSTRACT **Fix an isogeny class $\mathscr{A}$ of semistable elliptic curves over Q. The elements of $\mathscr{A}$ have a common conductor *N*, which is a square-free positive integer. Let *D* be a divisor of *N* which is the product of an even number of primes—i.e., the discriminant of an indefinite quaternion algebra over Q. To *D* we associate a certain Shimura curve $X_0^D(N/D)$, whose Jacobian is isogenous to an abelian subvariety of $J_0(N)$. There is a unique $A \in \mathscr{A}$ for which one has a nonconstant map $\pi_D : X_0^D(N/D) \to A$ whose pullback $A \to \mathrm{Pic}^0(X_0^D(N/D))$ is injective. The degree of π_D is an integer δ_D which depends only on *D* (and the fixed isogeny class $\mathscr{A}$). We investigate the behavior of δ_D as *D* varies.**

Let $f = \Sigma a_n(f)e^{2\pi inz}$ be a weight-two newform on $\Gamma_0(N)$, where $N = DM$ is the product of two relatively prime integers D and M and where D is the discriminant of an indefinite quaternion division algebra over **Q**. Assume that the Fourier coefficients of f are rational integers, so that f is associated with an isogeny class $\mathscr{A}$ of elliptic curves over **Q**. Among the curves in $\mathscr{A}$ is a distinguished element A, the strong modular curve attached to f. Shimura (1) has constructed A as an optimal quotient of $J_0(N)$. Thus A is the quotient of $J_0(N)$ by an abelian subvariety of this Jacobian. Composing the standard map $X_0(N) \hookrightarrow J_0(N)$ with the quotient $\xi: J_0(N) \to A$, we obtain a covering $\pi: X_0(N) \to A$ whose degree δ is an integer which depends only on f.

The integer δ has been regarded with intense interest for the last decade. For one thing, primes dividing δ are "congruence primes for f": if p divides δ, then there is a mod p congruence between f and a weight-two cusp form on $\Gamma_0(N)$ which has integral coefficients and is orthogonal to f under the Petersson inner product. (See, e.g., Section 5 of ref. 2 for a precise statement.) For another, it is known that a sufficiently good upper bound for δ will imply the *ABC* Conjecture (3, 4). More precisely, as R. Murty explains in ref. 24, the *ABC* Conjecture follows from the conjectural bound

$$\delta \overset{?}{=} O(N^{2+\varepsilon}) \text{ for all } \varepsilon > 0.$$

(For a partial converse, see ref. 5.) While δ is easy to calculate in practice (6), it seems more difficult to manage theoretically. Murty (24), has summarized what bounds are known at present.

This note concerns relations between δ and analogues of δ in which $J_0(N)$ is replaced by the Jacobian of a Shimura curve.

To define these analogues, it is helpful to give a characterization of δ in which π does not appear explicitly. For this, note that the map $\xi^\vee: A^\vee \hookrightarrow J_0(N)^\vee$ which is dual to ξ may be viewed as a homomorphism $A \to J_0(N)$, since Jacobians of curves (and elliptic curves in particular) are canonically self-dual. The image of $\xi^\vee$ is a copy of A which is embedded in $J_0(N)$. The composite $\xi \circ \xi^\vee \in \mathrm{End}\, A$ is necessarily multiplication by some integer; a moment's reflection shows that this integer is δ. Let $\Gamma_0^D(M)$ be the analogue of $\Gamma_0(M)$ in which **SL**(2, **Z**) is replaced by the group of norm-1 units in a maximal order of the rational quaternion algebra of discriminant D. Let $X_0^D(M)$ be the Shimura curve associated with $\Gamma_0^D(M)$ and let $J' = J_0^D(M)$ be the Jacobian of $X_0^D(M)$. The correspondence of Shimizu and Jacquet–Langlands (7) relates f to a weight-two newform f' for the group $\Gamma_0^D(M)$; the form f' is well defined only up to multiplication by a nonzero constant. Associated to f' is an elliptic curve A' which appears as an optimal quotient $\xi' : J' \to A'$ of J'. Using the techniques of Ribet (8) or the general theorem of Faltings (9), one proves that A and A' are isogenous—i.e., that A' belongs to $\mathscr{A}$. We define $\delta^D(M) \in \mathbf{Z}$ as the composite $\xi' \circ (\xi')^\vee$.

To include the case $D = 1$ in formulas below, we set $\delta^1(N) = \delta$.

Roberts (10) and Bertolini and Darmon (section 5 of ref. 11) have pointed out that the Gross–Zagier formula and the conjecture of Birch and Swinnerton-Dyer imply relations between δ and $\delta^D(M)$ in $\mathbf{Q}^*/(\mathbf{Q}^*)^2$. Bertolini and Darmon allude to the possibility that there may be a simple, precise formula for the ratio $\delta/\delta^D(M)$. The relation which they envisage involves local factors for the elliptic curves A and A' at the primes $p|D$.

While these factors may well be different for the two elliptic curves, we will ignore this subtlety momentarily and introduce only those factors which pertain to A. Suppose, then, that p is a prime dividing D, so that A has multiplicative reduction at p. Let c_p be the number of components in the fiber at p for the Néron model of A; i.e., $c_p = \mathrm{ord}_p\Delta$, where Δ is the minimal discriminant of A. As was mentioned above, δ controls congruences between f and newforms other than f in the space S of weight-two forms on $\Gamma_0(N)$; analogously, $\delta^D(M)$ controls congruences between f and other forms in the D-new subspace of S. At the same time, level-lowering results such as those of Ribet (12) lead to the expectation that the c_p control congruences between f and D-old forms in S. This yields the heuristic formula:

$$\delta^D(M) \overset{??}{=} \delta^1(N)/\prod_{p|D} c_p.$$

Equivalently, one can consider factorizations $N = MpqD$, where p and q are distinct prime numbers, $D \geq 1$ is the product of an even number of distinct primes, and the four numbers p, q, D, and M are relatively prime. The formula displayed above amounts to the heuristic relation

$$\delta^{pqD}(M) \overset{??}{=} \frac{\delta^D(pqM)}{c_p c_q} \qquad \textbf{[1]}$$

for each factorization $N = MpqD$. Although simple examples show that Eq. **1** is not correct as stated, we will prove that a suitably modified form of it is valid in many cases.

To state our results, we need to be more precise about the numbers c_p and c_q which appear above. We set:

$$J = J_0^D(Mpq),\ J' = J_0^{Dpq}(M).$$

Let $\xi : J \to A$ and $\xi' : J' \to A'$ be the optimal quotients of J and J' for which A and A' lie in $\mathscr{A}$. (This is a change of notation, since we have been taking A to be an optimal quotient of $J_0(N)$; the new elliptic curve A is the unique curve isogenous to the original A which appears as an optimal quotient of J.) Let c_p and c_q be defined for A as above; i.e., $c_p = \mathrm{ord}_p\Delta(A)$ and $c_q = \mathrm{ord}_q\Delta(A)$. Note that c_p, for instance, may be viewed as the order of the group of components of the fiber at p of the Néron model for A. This group is cyclic. Let c'_p and c'_q be defined analogously, with A' replacing A. Notice that $\mathrm{ord}_\ell c_p = \mathrm{ord}_\ell c'_p$ and $\mathrm{ord}_\ell c_q = \mathrm{ord}_\ell c'_q$ for each prime ℓ such that $A[\ell]$ is irreducible. Indeed, the curves A and A' are isogenous over $\mathbf{Q}$. The irreducibility hypothesis on $A[\ell]$ implies that any rational isogeny $A \to A'$ of degree divisible by ℓ factors through the multiplication-by-ℓ map on A. Hence there is an isogeny $\varphi : A \to A'$ whose degree is prime to ℓ. If $d = \deg \varphi$, the map φ induces an isomorphism between the prime-to-d parts of the component groups of A and A', both in characteristic p and in characteristic q.

THEOREM 1. *One has*

$$\delta^{pqD}(M) = \frac{\delta^D(pqM)}{c'_p c_q}\mathcal{E}(D, p, q, M)^2,$$

where the "error term" $\mathcal{E}(D, p, q, M)$ is a positive divisor of $c'_p c_q$. Further, suppose that M is square free but not a prime number,[†] *and let ℓ be a prime number which divides $\mathcal{E}(D, p, q, M)$. Then the Gal($\overline{\mathbf{Q}}/\mathbf{Q}$)-module $A[\ell]$ is reducible.*

In our proof of the theorem, we shall first prove a version of the displayed formula in which $\mathcal{E}(D, p, q, M)$ is expressed in terms of maps between component groups in characteristics p and q. (See *Theorem 2* below.) We then prove the second assertion of *Theorem 1*.

Before undertaking the proof, we illustrate *Theorem 1* by considering a series of examples. As the reader will observe, these examples show in particular that the "error term" $\mathcal{E}(D, p, q, M)$ is not necessarily divisible by all primes ℓ for which $A[\ell]$ is reducible.

For the first example, take $M = 1$, $D = 1$, and $pq = 14$. Thus $N = 14$, so that the curves A and A' lie in the unique isogeny class of elliptic curves over $\mathbf{Q}$ with conductor 14. [There is a unique weight-two newform on $\Gamma_0(14)$.] According to the tables of Antwerp IV, there are six curves in this isogeny class [ref. 13, p. 82]. The curve A is identified as [14C] in the notation of ref. 13. We have $A = J_0(14)$; and $A' = J_0^{14}(1)$, so that $\delta^1(14) = \delta^{14}(1) = 1$. Since $c_2 = 6$ and $c_7 = 3$, *Theorem 1* yields the pair of equalities

$$3{\cdot}c'_2 = \mathcal{E}(1, 2, 7, 1)^2,\ 6{\cdot}c'_7 = \mathcal{E}(1, 7, 2, 1)^2;$$

there are two equalities because there are two choices for the ordered pair (p, q). By *Theorem 1*, the integers $\mathcal{E}(1, 2, 7, 1)$ and $\mathcal{E}(1, 7, 2, 1)$ are divisible only by the primes 2 and 3. Indeed, we see (once again from ref. 13) that these are the only primes ℓ for which $A[\ell]$ is reducible. Looking further at the tables, we see that there is a unique curve A' in the isogeny class of A for which $3c'_2$ is the square of an integer. This curve is [14D]. Thus we have $A' = $ [14D], as Kurihara determined in ref. 14.

There are five similar examples of products pq for which $J_0^{pq}(1)$ has genus one, namely 2·17, 2·23, 3·5, 3·7, and 3·11. [See, e.g., the table of Vignéras (ref. 15, p. 122).] In each of the five cases, we shall see that $A' = J_0^{pq}(1)$ can be determined as a specific elliptic curve of conductor pq with a small amount of detective work. [We suspect that this detective work was done 15 years ago by J.-F. Michon (see refs. 16 and 17).]

To begin with, we note that in each case there is a single weight-two newform on $\Gamma_0(pq)$ with integral coefficients, i.e., a single isogeny class of elliptic curves of conductor pq. The strong modular elliptic curve A of conductor pq is identified in ref. 13. Knowing this curve, we have at our disposal c_p and c_q. Further, the integer $\delta^1(pq)$ is available from Cremona's table (ref. 6, pp. 1247–1250).

In the two cases $pq = 3{\cdot}5$ and $3{\cdot}7$, A coincides with the Jacobian $J_0(pq)$. In this circumstance, an easy argument based on *Proposition 1* below shows that the local invariants of A and $A' = J_0^{pq}(1)$ are "flipped"—we have $c'_p = c_q$ and $c'_q = c_p$. After glancing at p. 82 of ref. 13, one sees that $A' = $ [15C] in the first of the two cases and $A' = $ [21D] in the second.

Let us now discuss the remaining three cases, 2·17, 2·23, and 3·11, where Cremona's table gives the values 2, 5, and 3 (respectively) for $\delta^1(pq)$. Using *Theorem 1* and the value $\delta^{pq}(1) = 1$ in each case, we obtain equations which express c'_p and c'_q as products of known rational numbers and unknown square integers. These are enough to determine A'. Indeed, when $pq = 34$, we have

$$1 = \frac{2}{6c'_{17}}\mathcal{E}(1, 17, 2, 1)^2,$$

so that $3c'_{17}$ is a square. We then must have $A' = $ [34C]. When $pq = 46$, $2c'_{23}$ is a square, and we conclude $A' = $ [23B]. When $pq = 33$, $2c'_{11}$ is a square and thus $A' = $ [33B].

In the six examples we have discussed so far, an alternative approach would have been to read off the numbers c'_p and c'_q from a formula of Jordan and Livné (section 2 of ref. 18; see Theorem 4.3 of ref. 8). As we have seen, A' is determined in each case by these local invariants.

For an example with a different flavor, we take f to be the modular form associated with the curve $A = $ [57E] of ref. 13. This curve is isolated in its isogeny class; i.e., $A[\ell]$ is irreducible for all ℓ. In particular, $A' = A$. Because $A[\ell]$ is irreducible for all ℓ, the theorem gives $\mathcal{E}(1, 3, 19, 1) = 1$. Hence

$$\delta^{57}(1) = \delta^1(57)/(c_3c_{19}).$$

Now Cremona's table (ref. 6, p. 1247) yields the value $\delta^1(57) = 4$; also, one has $c_3 = 2$, $c_{19} = 1$. Thus we find $\delta^{57}(1) = 2$. This relation is confirmed by results of D. Roberts (10), who shows, more precisely, that A is the quotient of $X_0^{57}(1)$ by its Atkin–Lehner involution w_{57}.

Next, we consider the elliptic curves of conductor $N = 714 = 2{\cdot}3{\cdot}7{\cdot}17$, which are tabulated in Cremona's book (19). These curves fall into nine isogeny classes, A–I. Four of these classes, B, C, E and H, contain precisely one element. In other words, the four elliptic curves 714B1, 714C1, 714E1, and 714H1 are isolated in their isogeny classes. For each elliptic curve, *Theorem 1* expresses $\delta^{714}(1)$ as well as the six degrees $\delta^{pq}(714/pq)$ for $pq|714$ in terms of $\delta^1(714)$ and the integers c_p for $p|714$. These numbers are available from refs. 6 and 19. The most striking of the four elliptic curves is perhaps 714H1. For this curve, $c_2 = c_3 = c_7 = c_{17} = 1$ and $\delta^1(714) = 40$. Hence $\delta^{714}(1)$ and all degrees $\delta^{pq}(714/pq)$ are equal to 40.

For a final example, we consult further tables of John Cremona which are available by anonymous ftp from euclid.ex.ac.uk in /pub/cremona/data. Let A be the curve denoted 1001C1, which has Weierstrass data [0, 0, 1, −199, 1092]. Its minimal discriminant is $-7^2 11^3 13^2$. This curve is isolated in its isogeny class, which suggests that $\mathcal{E}(1, 7, 13, 11) = 1$. Since 11 is a prime, the second part of *Theorem 1* yields no information. However, by *Proposition 3* below, $\mathcal{E}(1, 7, 13, 11)$ divides both c_7 and c_{13}. Each of these integers is 2, so that we may conclude at least that $\mathcal{E}(1, 7, 13, 11)$ is 1 or 2. Cremona's tables give the value $\delta^1(1001) = 1008$; hence

[†] In a forthcoming article, the second author expects to study the excluded case where M is a prime number.

$\delta^{7\cdot 13}(11)$ is either 252 or 1008.‡ On the other hand, since c_7 and c_{11} are relatively prime, we find that $\mathscr{E}(1, 7, 11, 13) = 1$. Thus $\delta^{7\cdot 11}(13) = 1008/6 = 168$. Similarly, $\delta^{11\cdot 13}(7) = 168$.

The First Assertion of *Theorem 1*

If V is an abelian variety over $\mathbf{Q}$ and ℓ is a prime, let $\Phi(V, \ell)$ be the group of components of the fiber at ℓ of the Néron model of V. This group is a finite étale group scheme over Spec $\mathbf{F}_\ell$, i.e., a finite abelian group furnished with a canonical action of $\mathrm{Gal}(\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell)$. The association $V \mapsto \Phi(V, \ell)$ is functorial. For example, as we noted above, if A is an elliptic curve with multiplicative reduction at p, then $\Phi(A, p)$ is a cyclic group of order c_p.

The maps ξ and ξ' induce homomorphisms

$$\xi_* : \Phi(J, q) \to \Phi(A, q),\ \xi'_* : \Phi(J', p) \to \Phi(A', p).$$

Here is a version of the first assertion of *Theorem 1* in which $\mathscr{E}(D, p, q, M)$ appears with a precise value.

THEOREM 2. *One has*

$$\delta^{pqD}(M) = \frac{\delta^D(pqM)}{c'_p c_q}\,\mathscr{E}(D, p, q, M)^2,$$

where $\mathscr{E}(D, p, q, M) = \#\mathit{image}\,\xi_* \cdot \#\mathit{coker}\ \xi'_*$.

To prove the theorem, we compare the character groups of algebraic tori which are associated functorially to the mod p reduction of J' and the mod q reduction of J. Recall that the former reduction is described by the well known theory of Cerednik and Drinfeld (20–22), while the latter falls into the general area studied by Deligne and Rapoport (23). [Although Deligne and Rapoport provide only the briefest discussion of the case $D > 1$, what we need will follow from recent results of K. Buzzard (31).] Our comparison is based on the oft-exploited circumstance that the two reductions involve the arithmetic of the same definite rational quaternion algebra: that algebra whose discriminant is Dq.

To state the result which is needed, we introduce some notation: if V is an abelian variety over $\mathbf{Q}$ and ℓ is a prime number, let T be the toric part of the fiber over $\mathbf{F}_\ell$ of the Néron model for V and write $\mathscr{X}(V, \ell)$ for the character group $\mathrm{Hom}_{\overline{\mathbf{F}}_\ell}(T, \mathbf{G}_\mathrm{m})$. Thus $\mathscr{X}(V, \ell)$ is a free abelian group which is furnished with compatible actions of $\mathrm{Gal}(\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell)$ and $\mathrm{End}_\mathbf{Q}\,V$. At least in the case when V has semistable reduction at ℓ, there is a canonical bilinear pairing

$$u_V : \mathscr{X}(V, \ell) \times \mathscr{X}(V^\vee, \ell) \to \mathbf{Z}$$

which was introduced by Grothendieck (Theorem 10.4 of ref. 25). If, moreover, V is canonically self-dual (e.g., if V is the Jacobian of a curve or a product of Jacobians), then the monodromy pairing u_V is a pairing on $\mathscr{X}(V, \ell)$ (in the sense that it is defined on the product of two copies of this group).

The relation between $\Phi(V, \ell)$ and the character groups $\mathscr{X}$ is as follows (Theorem 11.5 of ref. 25): there is a natural exact sequence

$$0 \to \mathscr{X}(V, \ell) \xrightarrow{\alpha} \mathrm{Hom}(\mathscr{X}(V, \ell), \mathbf{Z}) \to \Phi(V, \ell) \to 0$$

in which α is obtained from u_V by the standard formula $(\alpha(x))(y) = u_V(x, y)$.

PROPOSITION 1. *There is a canonical exact sequence*

$$0 \to \mathscr{X}(J', p) \xrightarrow{\iota} \mathscr{X}(J, q) \to \mathscr{X}(J'', q) \times \mathscr{X}(J'', q) \to 0,$$

where $J'' = J_0^D(qM)$. The sequence is compatible with the action of Hecke operators T_n for n prime to N, which operate in the usual way on J, J', and J''. Moreover, the map ι is compatible with the monodromy pairings on $\mathscr{X}(J', p)$ and $\mathscr{X}(J, q)$ in the sense that $u_{J'}(x, y) = u_J(\iota x, \iota y)$ for all $x, y \in \mathscr{X}(J', p)$.

When $D = 1$, the proposition was proved in ref. 12. (See especially Theorem 4.1 of ref. 12.) The case $D > 1$ can be handled in an analogous way, thanks to K. Buzzard's analogue (31) of the Deligne–Rapoport theorem (23). This theme is explored in the work of Jordan and Livné (26) and L. Yang (27).

Let $\mathscr{L}$ be the "f-part" of $\mathscr{X}(J, q)$, defined for example as the group of characters $x \in \mathscr{X}(J, q)$ such that $T_n x = a_n(f)x$ for all n prime to N. [Recall that $a_n(f)$ is the nth coefficient of f.] It is not hard to check that $\mathscr{L}$ is isomorphic to $\mathbf{Z}$ and that in fact it is contained in $\mathscr{X}(J', p)$, viewed as a subgroup of $\mathscr{X}(J, q)$ via ι. Indeed, consider the decomposition of J as a product up to isogeny of simple abelian varieties over $\mathbf{Q}$. One of the factors is A, which occurs with multiplicity 1, and the other factors are non-f: they correspond to newforms of level dividing N whose nth coefficients cannot coincide with the $a_n(f)$ for all n prime to N. Hence $\mathscr{L} \otimes \mathbf{Q}$ is the tensor product with $\mathbf{Q}$ of the character group of the toric part of $A_{\mathbf{F}_q}$; this shows that $\mathscr{L}$ has rank 1. A similar computation shows that $\mathscr{L} \cap \mathscr{X}(J', p)$ has rank 1, since A occurs up to isogeny exactly once in J' and since A has multiplicative reduction at p. The image of $\mathscr{L}$ in $\mathscr{X}(J'', q) \times \mathscr{X}(J'', q)$ is thus finite; it is zero since $\mathscr{X}(J'', q)$ is torsion free.

Fix a generator g of $\mathscr{L}$ and set $\tau = u_J(g, g)$. An arbitrary nonzero element t of $\mathscr{L}$ may be written ng, where n is a nonzero integer. We then have $u_J(t, t) = n^2\tau$.

By the theorem of Grothendieck (25) that was cited above, c_q may be interpreted as $u_A(x, x)$, where x is a generator of $\mathscr{X}(A, q)$ and where u_A is the monodromy pairing arising from the mod q reduction of A. Meanwhile, the map $\xi : J \to A$ induces by pullback a homomorphism $\xi^* : \mathscr{X}(A, q) \to \mathscr{X}(J, q)$ and the dual of ξ induces similarly a homomorphism $\xi_* : \mathscr{X}(J, q) \to \mathscr{X}(A, q)$. The two homomorphisms are adjoint with respect to the monodromy pairings:

$$u_J(\xi^* x, y) = u_A(x, \xi_* y) \text{ for all } x \in \mathscr{X}(A, q), y \in \mathscr{X}(J, q).$$

Notice, however, that $\xi_* \circ \xi^*$ is multiplication by $\delta := \delta^D(pqM)$ on $\mathscr{X}(A, q)$, since it is induced by the endomorphism "multiplication by δ" of A. Thus

$$\delta u_A(x, x) = u_A(x, \xi_*(\xi^* x)) = u_J(\xi^* x, \xi^* x)$$

for all $x \in \mathscr{X}(A, q)$. On taking x to be a generator of $\mathscr{X}(A, q)$, we find

$$\delta c_q = (\mathscr{L} : \mathscr{X}(A, q))^2 \cdot \tau,$$

where we view $\mathscr{X}(A, q)$ as embedded in $\mathscr{L}$ by ξ^*. A similar argument applied to A' mod p yields $\delta' c'_p = (\mathscr{L} : \mathscr{X}(A', p))^2 \cdot \tau$, where $\delta' = \delta^{Dpq}(M)$. [To prove this relation, one must view $\mathscr{L}$ as a subgroup of $\mathscr{X}(J', p)$ and interpret τ as $u_{J'}(t, t)$, where $g = \iota t$. The legitimacy of this interpretation stems from the compatibility among ι, u_J, and $u_{J'}$.]

We emerge with the preliminary formula

$$\frac{\delta' c'_p}{(\mathscr{L} : \mathscr{X}(A', p))^2} = \frac{\delta c_q}{(\mathscr{L} : \mathscr{X}(A, q))^2}.$$

After isolating δ' on one side of the equation, we see that *Theorem 2* is implied by the following result:

PROPOSITION 2. *Let ξ_* and ξ'_* be the homomorphisms $\Phi(J, q) \to \Phi(A, q)$ and $\Phi(J', p) \to \Phi(A', p)$ which are induced by ξ and ξ' on component groups. Then $(\mathscr{L} : \mathscr{X}(A, q)) = \#\mathit{coker}\ \xi_*$ and $(\mathscr{L} : \mathscr{X}(A', p)) = \#\mathit{coker}\ \xi'_*$.*

‡The forthcoming results of the second author which were mentioned earlier should prove that $\mathscr{E}(1, 7, 13, 11) = 1$ and that $\delta^{7\cdot 13}(11) = 252$.

Proof: The two formulas are analogous; we shall prove only the assertion relative to ξ_*. Because of the assumption that $\xi : J \to A$ is an optimal quotient, the map $\xi^\vee : A \to J$ is injective. One deduces from this the surjectivity of the map on character groups $\xi_* : \mathscr{X}(J, q) \to \mathscr{X}(A, q)$. Consider the commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathscr{X}(A, q) \arrow[r] & \mathrm{Hom}(\mathscr{X}(A, q),\mathbf{Z}) \arrow[r] & \Phi(\mathrm{A}, \mathrm{q}) \arrow[r] & 0 \\
0 \arrow[r] & \mathscr{X}(J, q) \arrow[r] \arrow[u] & \mathrm{Hom}(\mathscr{X}(J, q),\mathbf{Z}) \arrow[r] \arrow[u] & \Phi(J, q) \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

in which the three vertical maps are induced by ξ. [For instance, the central vertical map is $\mathrm{Hom}(\xi^*, \mathbf{Z})$, where $\xi^* : \mathscr{X}(A, q) \to \mathscr{X}(J, q)$ is an injective map between free abelian groups of finite rank.] The exactness of the rows is guaranteed by Theorem 11.5 of ref. 25. Because the left-hand vertical map is surjective, the cokernels of $\mathrm{Hom}(\xi^*, \mathbf{Z})$ and the right-hand ξ_* may be identified.

It is clear that the order of coker($\mathrm{Hom}(\xi^*, \mathbf{Z})$) coincides with the order of the torsion subgroup of coker(ξ^*). Since $\mathscr{X}(J, q)/\mathscr{L}$ is torsion free by the definition of $\mathscr{L}$, we obtain first the formula

$$\#\mathrm{coker}(\mathrm{Hom}(\xi^*,\mathbf{Z})) = (\mathscr{L} : \mathscr{X}(A, q))$$

and then the desired equality. ■

The Second Assertion of *Theorem 1*

We assume from now on that N is square free and that ℓ is a prime for which $A[\ell]$ is irreducible. We should mention in passing that the irreducibility hypothesis holds for one $A \in \mathscr{A}$ if and only if it holds for all $A \in \mathscr{A}$. Indeed, the semisimplification of the mod ℓ Galois representation $A[\ell]$ depends only on $\mathscr{A}$. At the same time, $A[\ell]$ is irreducible if and only if its semisimplification is irreducible.

LEMMA 2. *There is a prime $r|N$ for which ℓ does not divide c_r.*

Proof: Suppose to the contrary that ℓ divides c_r for all $r|N$. Then the mod ℓ $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-representation $A[\ell]$ is *finite* at all primes (section 4.1 of ref. 28). If $\ell = 2$, this contradicts a theorem of Tate (29). If $\ell > 2$, a theorem of the first author (Theorem 1.1 of ref. 12) implies that $A[\ell]$ is modular of level 1 in the sense that it arises from the space of weight-two cusp forms on $\mathbf{SL}(2, \mathbf{Z})$. Since this space is zero, we obtain a contradiction in this case as well. ■

In order to prove the second assertion of *Theorem 1*, which concerns the "ℓ-part" of $\mathscr{E}(D, p, q, M)$, we will consider *varying* decompositions $N = D{\cdot}p{\cdot}q{\cdot}M$. In these decompositions, the isogeny class $\mathscr{A}$, and the integer N in particular, are understood to be invariant. We view the prime ℓ as fixed, and recall the hypothesis that $A[\ell]$ is irreducible. (If this irreducibility hypothesis holds for one $A \in \mathscr{A}$, then it holds for all A.) Set

$$e(D, p, q, M) := \ell^{\mathrm{ord}_\ell \mathscr{E}(D, p, q, M)},$$

so that $e(D, p, q, M)$ is the "ℓ-part" to be studied.

PROPOSITION 3. *If $N = DpqM$, then $e(D, p, q, M)$ is the order of the ℓ-primary part of the cokernel of*

$$\xi'_* : \Phi(J', p) \to \Phi(A', p).$$

Further, we have $e(D, p, q, M) = e(D, q, p, M)$, and $e(D, p, q, M)$ divides both c_p and c_q.

Proof: In view of *Theorem 2*, the first statement means that the ℓ-primary part of the image of $\xi_* : \Phi(J, q) \to \Phi(A, q)$ is trivial. For each prime number r which is prime to N, let T_r be the rth Hecke operator on J. It is a familiar fact that $\Phi(J, q)$ is Eisenstein in the sense that T_r acts on $\Phi(J, q)$ as $1 + r$ for all such r. This was proved by the first author in case $D = 1$ (see Theorem 3.12 of ref. 12 and ref. 30), and the result can be extended as needed in view of results of Buzzard (31) and Jordan and Livné (26).

It follows from the Eichler–Shimura relation that the image of ξ_* is annihilated by $a_r(f) - r - 1$ for all r. One deduces from this that the ℓ-primary part of the image is trivial: If not, then $a_r(f) \equiv r + 1 \bmod \ell$ for all r, and this implies that the semisimplification of $A[\ell]$ is reducible; cf. Theorem 5.2(c) of ref. 12.

To prove the second statement, we begin by noting that $e(D, p, q, M)$ divides c'_p. As we pointed out earlier, there is an isogeny $A \to A'$ of prime-to-ℓ degree. Indeed, A and A' are isogenous over $\mathbf{Q}$; on the other hand, the hypothesis on $A[\ell]$ implies that any rational isogeny $A \to A'$ of degree divisible by ℓ factors through the multiplication-by-ℓ map on A. Hence the ℓ-primary components of $\Phi(A, p)$ and $\Phi(A', p)$ are isomorphic, so that the largest powers of ℓ in c_p and c'_p are the same. Thus $e(D, p, q, M)$ divides c_p. Also, since an analogous reasoning shows that c_q and c'_q have the same valuations at ℓ, $e(D, p, q, M)$ depends symmetrically on p and q, as asserted. Finally, $e(D, p, q, M)$ divides both c_p and c_q, since it divides c_p and depends symmetrically on p and q. ■

COROLLARY. *If $N = dpqrsm$, where p, q, r, and s are primes and d is the product of an even number of primes, then*

$$e(rsd, p, q, m) = e(qsd, p, r, m)$$

and $e(d, r, s, pqm) = e(d, q, s, prm)$.

Proof: Each of the two integers in the displayed equality may be calculated as the order of the ℓ-primary part of the cokernel of $\xi'_* : \Phi(J^{dpqrs}(m), p) \to \Phi(A', p)$. This coincidence gives the first equality. To obtain the second from the first, we note that both $e(rsd, p, q, m)^2\, e(d, r, s, pqm)^2$ and $e(qsd, p, r, m)^2\, e(d, q, s, prm)^2$ are equal to the ℓ-part of the quantity $\delta^{dpqrs}(m)c_pc_qc_rc_s/\delta^d(pqrsm)$. ■

To finish the proof of *Theorem 1*, we assume from now on that M is not prime. To prove that $e(D, p, q, M) = 1$, it suffices to show that $e(D, p, q, M)$ divides c_r for each $r|N$. If $r = p$ or $r = q$, this divisibility is included in the statement of *Proposition 3*. Assume, next, that r is a divisor of D, and write $D = rsd$, where s is a prime. We have

$$e(D, p, q, M) = e(rsd, p, q, M) = e(qsd, p, r, M),$$

where the second equality follows from the *Corollary*. The latter number divides c_r, as required. Finally, suppose that r divides M. Since M is not prime, we may write $M = rsm$, where s is a prime. We have seen that $e(D, r, s, pqm) = e(D, q, s, prm)$. Permuting the roles of the four primes p, q, r, and s, we may write instead $e(D, p, q, rsm) = e(D, r, q, psm)$. The latter number is a divisor of c_r.

It is a pleasure to thank J. Cremona, H. Darmon, and D. Roberts for helpful conversations and correspondence. This article was supported in part by National Science Foundation Grant DMS 93-06898.

1. Shimura, G. (1973) *J. Math. Soc. Japan* **25,** 523–544.
2. Zagier, D. (1985) *Canad. Math. Bull.* **28,** 372–384.
3. Frey, G. (1987) *Prog. Math.* **71,** 39–51.
4. Frey, G. (1987) *J. Indian Math. Soc.* **51,** 117–145.
5. Mai, L. & Murty, R. (1994) *Contemp. Math.* **166,** 335–340.
6. Cremona, J. E. (1995) *Math. Comp.* **64,** 1235–1250.
7. Jacquet, H. & Langlands, R. P. (1970) *Automorphic Forms on* **GL(2)**, Lecture Notes in Mathematics (Springer, Berlin), Vol. 114.
8. Ribet, K. (1980) *C. R. Acad. Sci. Ser. A* **291**, A121–A123.
9. Faltings, G. (1983) *Invent. Math.* **73,** 349–366.
10. Roberts, D. (1989) Ph.D. thesis (Harvard University, Cambridge, MA).
11. Bertolini, M. & Darmon, H. (1997) *Ann. Math.*, in press.
12. Ribet, K. (1990) *Invent. Math.* **100,** 431–476.

13. Birch, B. J. & Kuyk, W., eds. (1975) *Modular Functions of One Variable IV*, Lecture Notes in Mathematics (Springer, Berlin) Vol. 476.
14. Kurihara, A. (1977) *J. Fac. Sci. Univ. Tokyo, Sec. IA* **25,** 277–300.
15. Vignéras, M.-F. (1980) *Arithmétique des Algèbres de Quaternions*, Lecture Notes in Mathematics (Springer, Berlin), Vol. 800.
16. Michon, J.-F. (1981) *Bull. Soc. Math. France* **109,** 217–225.
17. Michon, J.-F. (1984) *Prog. Math.* **51,** 185–197.
18. Jordan, B. & Livné, R. (1986) *Compositio Math.* **60,** 227–236.
19. Cremona, J. E. (1992) *Algorithms for Modular Elliptic Curves* (Cambridge Univ. Press, Cambridge, U.K.).
20. Cerednik, I. V. (1976) *Mat. Sb.* **100,** 59–88; English transl., (1976) *Math USSR Sb.* **29,** 55–78.
21. Drinfeld, V. G. (1976) *Funct. Anal. Prilozen.* **10,** 29–40; English transl., (1976) *Funct. Anal. Appl.* **10,** 107–115.
22. Boutot, J.-F. & Carayol, H. (1991) *Astérisque* **196–197,** 45–158.
23. Deligne, P. & Rapoport, M. (1973) *Les Schémas de Modules de Courbes Elliptiques*, Lecture Notes in Mathematics (Springer, Berlin) Vol. 349, pp. 143–316.
24. Murty, R. (1997) *Contemp. Math.*, in press.
25. Grothendieck, A. (1972) *SGA7 I, Exposé IX*, Lecture Notes in Mathematics (Springer, Berlin), Vol. 288, pp. 313–523.
26. Jordan, B. & Livné, R. (1995) *Duke Math. J.* **80,** 419–484.
27. Yang, L. (1996) Ph.D. thesis (City Univ. of New York, New York).
28. Serre, J.-P. (1987) *Duke Math. J.* **54,** 179–230.
29. Tate, J. (1994) *Contemp. Math.* **174,** 153–156.
30. Ribet, K. (1987–1988) *On the Component Groups and the Shimura Subgroup of $J_0(N)$*, Séminaire Théorie Nombres, Université Bordeaux. Exposé 6.
31. Buzzard, K. (1997) *Duke Math. J.* **87,** 591–612.

Proc. Natl. Acad. Sci. USA
Vol. 94, pp. 11115–11117, October 1997
Colloquium Paper

This paper was presented at a colloquium entitled "Elliptic Curves and Modular Forms," organized by Barry Mazur and Karl Rubin, held March 15–17, 1996, at the National Academy of Sciences in Washington, DC.

Euler characteristics and elliptic curves

JOHN COATES AND SUSAN HOWSON

Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, 16 Mill Lane, Cambridge, CB2 1SB, United Kingdom

ABSTRACT Let E be a modular elliptic curve over $\mathbb{Q}$, without complex multiplication; let p be a prime number where E has good ordinary reduction; and let F_∞ be the field obtained by adjoining to $\mathbb{Q}$ all p-power division points on E. Write G_∞ for the Galois group of F_∞ over $\mathbb{Q}$. Assume that the complex L-series of E over $\mathbb{Q}$ does not vanish at $s = 1$. If $p \geqslant 5$, we make a precise conjecture about the value of the G_∞-Euler characteristic of the Selmer group of E over F_∞. If one makes a standard conjecture about the behavior of this Selmer group as a module over the Iwasawa algebra, we are able to prove our conjecture. The crucial local calculations in the proof depend on recent joint work of the first author with R. Greenberg.

Let E be an elliptic curve defined over $\mathbb{Q}$. For simplicity, we shall assume throughout that E does not admit complex multiplication. Let p be a prime number, and write E_{p^n} ($n = 1, 2, \ldots$) for the group of p^n-division points on E. Write E_{p^∞} for the union of the E_{p^n} ($n = 1, 2, \ldots$). Put $F_\infty = \mathbb{Q}(E_{p^\infty})$, and let G_∞ denote the Galois group of F_∞ over $\mathbb{Q}$. By a theorem of Serre (1), G_∞ is an open subgroup of $GL(2, \mathbb{Z}_p)$, and hence is a p-adic Lie group of dimension 4. Assume from now on that $p \geqslant 5$, so that G_∞ has no p-torsion. By a refinement (2) of a theorem of Lazard (3), G_∞ then has p-cohomological dimension equal to 4. Let A be a p-primary abelian group, which is a discrete G_∞-module. We say that A has a finite G_∞-Euler characteristic if all of the cohomology groups $H^i(G_\infty, A)$ ($i \geqslant 0$) are finite. When A has finite G_∞-Euler characteristic, we define its Euler characteristic $\chi(G_\infty, A)$ by

$$\chi(G_\infty, A) = \prod_{i=0}^{4} \#(H^i(G_\infty, A))^{(-1)^i}.$$

The present note will be concerned with the calculation of the G_∞-Euler characteristic of the Selmer group $\mathcal{S}(F_\infty)$ of E over F_∞. We recall that this Selmer group is defined by the exactness of the sequence

$$0 \to \mathcal{S}(F_\infty) \to H^1(F_\infty, E_{p^\infty}) \to \prod_{\omega \text{ finite}} H^1(F_{\infty,\omega}, E), \qquad \textbf{[1]}$$

where ω runs over all finite places of F_∞; here $F_{\infty,\omega}$ denotes the union of the completions at ω of the finite extensions of $\mathbb{Q}$ contained in F_∞. Of course, $\mathcal{S}(F_\infty)$ has a natural structure as a G_∞-module, and we expect its Euler characteristic to be closely related to the Birch and Swinnerton-Dyer formula. Specifically, let $\text{Ш}(E)$ denote the Tate-Shafarevich group of E over $\mathbb{Q}$, and, for each finite prime v, let $c_v = [E(\mathbb{Q}_v) : E_0(\mathbb{Q}_v)]$, where, as usual, $E_0(\mathbb{Q}_v)$ is the subgroup of points with nonsingular reduction modulo v. Let $L(E, s)$ be the Hasse-Weil L-series of E over $\mathbb{Q}$. If B is an abelian group, we write $B(p)$ for its p-primary subgroup. If n is a positive integer, $n^{(p)}$ will denote the exact power of p dividing n. Finally, we denote by $\tilde{E}$ the reduction of E modulo p. We then define, for p where E has good reduction,

$$\rho_p(E/\mathbb{Q}) = \frac{\#(\text{Ш}(E)(p))\cdot\prod_v c_v^{(p)}\cdot\#(\tilde{E}(\mathbb{F}_p)(p))^2}{\#(E(\mathbb{Q})(p))^2}, \qquad \textbf{[2]}$$

where v runs over all finite places of $\mathbb{Q}$.

CONJECTURE 1. *Let E be a modular elliptic curve over $\mathbb{Q}$, without complex multiplication, such that $L(E, 1) \neq 0$. Let $p \geqslant 5$ be a prime number such that E has good ordinary reduction at p. Then $\mathcal{S}(F_\infty)$ has a finite G_∞-Euler characteristic, which is given by $\chi(G_\infty, \mathcal{S}(F_\infty)) = \rho_p(E/\mathbb{Q})$.*

This conjecture is suggested by the following considerations in Iwasawa theory. Let $\mathbb{Q}_\infty$ denote the unique extension of $\mathbb{Q}$ such that the Galois group Γ_∞ of $\mathbb{Q}_\infty$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}_p$. Of course, $\mathbb{Q}_\infty$ is contained in F_∞. Let $\mathcal{S}(\mathbb{Q}_\infty)$ be the Selmer group of E over $\mathbb{Q}_\infty$, which is defined by replacing F_∞ by $\mathbb{Q}_\infty$ in the exact sequence of Eq. **1**. Making the same hypotheses on E and p as in Conjecture 1, it is well known that $\mathcal{S}(\mathbb{Q}_\infty)$ has a finite Γ_∞-Euler characteristic, which is given by

$$\chi(\Gamma_\infty, \mathcal{S}(\mathbb{Q}_\infty)) = \rho_p(E/\mathbb{Q}); \qquad \textbf{[3]}$$

we recall that Γ_∞ has p-cohomological dimension equal to 1, so that $\chi(\Gamma_\infty, A) = \#(H^0(\Gamma_\infty, A))/\#(H^1(\Gamma_\infty, A))$ for any discrete p-primary Γ_∞-module A. Thus Conjecture 1 asserts that, under the hypotheses made on E and p, the G_∞-Euler characteristic of $\mathcal{S}(F_\infty)$ should be precisely equal to the Γ_∞-Euler characteristic of $\mathcal{S}(\mathbb{Q}_\infty)$. This is indeed what one would expect from the following heuristic argument. If H_∞ is any profinite group, let

$$I(H_\infty) = \varprojlim_{U} \mathbb{Z}_p[H_\infty/U], \qquad \textbf{[4]}$$

where U runs over all open subgroups of H_∞, be the Iwasawa algebra of H_∞. Write $\hat{A} = \text{Hom}\,(A, \mathbb{Q}_p/\mathbb{Z}_p)$ for the Pontrjagin dual of a discrete p-primary abelian group A. Under the hypotheses of Conjecture 1, it is known that $\widehat{\mathcal{S}(\mathbb{Q}_\infty)}$ is a finitely generated torsion module over $I(\Gamma_\infty)$, whereas the structure theory of such modules enables us to define the characteristic ideal $C(\mathcal{S}(\mathbb{Q}_\infty))$ of $\mathcal{S}(\mathbb{Q}_\infty)$ in $I(\Gamma_\infty)$. It is easy and well known to see that $C(\mathcal{S}(\mathbb{Q}_\infty))$ has a generator $\mu(\mathbb{Q}_\infty)$ such that

$$\int_{\Gamma_\infty} d\mu(\mathbb{Q}_\infty) = \chi(\Gamma_\infty, \mathcal{S}(\mathbb{Q}_\infty)), \qquad \textbf{[5]}$$

where we are now interpreting the elements of $I(\Gamma_\infty)$ as $\mathbb{Z}_p$-valued measures on Γ_∞. We do not at present know enough about the structure theory of $I(G_\infty)$-modules to be able to define the analogue $C(\mathcal{S}(F_\infty))$ of $C(\mathcal{S}(\mathbb{Q}_\infty))$. Nevertheless, one

© 1997 by The National Academy of Sciences 0027-8424/97/9411115-3$2.00/0
PNAS is available online at http://www.pnas.org.

is tempted to guess that there should be a generator $\mu(F_\infty)$ of $C(\mathcal{S}(F_\infty))$ such that

$$\int_{G_\infty} d\mu(F_\infty) = \chi(G_\infty, \mathcal{S}(F_\infty)). \qquad \textbf{[6]}$$

Moreover, the link, which may exist between these characteristic ideals and p-adic L-functions, suggests that $C(\mathcal{S}(F_\infty))$ should map to $C(\mathcal{S}(\mathbb{Q}_\infty))$ under the canonical surjection from $I(G_\infty)$ onto $I(\Gamma_\infty)$. This latter property would show that the two integrals on the left of Eqs. **4** and **5** are equal, for suitable generators of $C(\mathcal{S}(F_\infty))$ and $C(\mathcal{S}(\mathbb{Q}_\infty))$, and so explain the equality of the Euler characteristics.

In spite of the above heuristic argument, it does not seem easy to prove Conjecture 1. Let $F_0 = \mathbb{Q}(E_p)$, and let Σ_∞ denote the Galois group of F_∞ over F_0, so that Σ_∞ is a pro-p-group. We say that a module X over the Iwasawa algebra $I(\Sigma_\infty)$ is torsion if each element of X is annihilated by some non-zero element of $I(\Sigma_\infty)$. Our main result is the following.

THEOREM 2. *In addition to the hypotheses of Conjecture 1, assume that* $\widehat{\mathcal{S}(F_\infty)}$ *is torsion over the Iwasawa algebra* $I(\Sigma_\infty)$, *where* $\Sigma_\infty = G(F_\infty/F_0)$. *Then Conjecture 1 holds, and* $H^i(G_\infty, \mathcal{S}(F_\infty)) = 0$ *for* $i = 2, \cdots, 4$.

It has long been conjectured (see ref. 4) that $\widehat{\mathcal{S}(F_\infty)}$ is torsion over $I(\Sigma_\infty)$ for all E and all primes p where E has good ordinary reduction, but very little is known in this direction at present. In view of this, it may be worth noting the following weaker result, which we can prove without this assumption. By a theorem of Serre (5), the cohomology groups $H^i(G_\infty, E_{p^\infty})$ $(i \geqslant 0)$ are finite.

THEOREM 3. *Under the same hypotheses as in Conjecture 1, we have that* $H^0(G_\infty, \mathcal{S}(F_\infty))$ *is finite, and*

$$\#(H^0(G_\infty, \mathcal{S}(F_\infty)) = \rho_p(E/\mathbb{Q})\cdot\#(H^3(G_\infty, E_{p^\infty})). \qquad \textbf{[7]}$$

Sketch of the Proof of Theorem 3. Let S be a fixed finite set of nonarchimedean primes containing p and all primes where E has bad reduction. We write $\mathbb{Q}_s$ for the maximal extension of $\mathbb{Q}$ unramified outside S and ∞. For each $n \geqslant 0$, let $F_n = \mathbb{Q}(E_{p^{n+1}})$. We define, for $v \in S$,

$$\mathrm{J}_{\infty,v} = \varinjlim_{n} \bigoplus_{\omega|v} H^1(F_{n,\omega}, E)(p),$$

where ω runs over all primes of F_n dividing v, and the inductive limit is taken with respect to the restriction maps. Our proof is based on the following well known commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{S}(F_\infty)^{G_\infty} \arrow[r] & H^1(G(\mathbb{Q}_s/F_\infty), E_{p^\infty})^{G_\infty} \arrow[r, "\lambda_\infty"] & (\bigoplus_{v\in S} J_{\infty,v})^{G_\infty} \\
0 \arrow[r] & \mathcal{S}(\mathbb{Q}) \arrow[r] \arrow[u, "\alpha"] & H^1(G(\mathbb{Q}_s/\mathbb{Q}), E_{p^\infty} \arrow[r, "\lambda"] \arrow[u, "\beta"] & \bigoplus_{v\in S} H^1(\mathbb{Q}_v, E)(p), \arrow[u, "\gamma = \bigoplus_{v\in S}\gamma_v"]
\end{tikzcd}$$

where the vertical arrows are restriction maps.

LEMMA 4. *The map* γ *is surjective, and its kernel is finite of order* $\#(\tilde{E}(\mathbb{F}_p))^2\cdot\Pi_v c_v^{(p)}$.

Proof. This is a purely local calculation. For each $v \in S$, fix a place ω of F_∞ above v, and let Δ_ω denote the Galois group of $F_{\infty,\omega}$ over $\mathbb{Q}_v$. Assume first that $v \neq p$. Then

$$\mathrm{Ker}\ \gamma_v \xrightarrow{\sim} H^2(\Delta_\omega, E_{p^\infty}),\ \mathrm{Coker}\ \gamma_v \xrightarrow{\sim} H^2(\Delta_\omega, E_{p^\infty})$$

and simple calculations (cf. ref. 7, Lemma 13) then show that

$$\#(H^1(\Delta_\omega, E_{p^\infty})) = c_v^{(p)},\ H^2(\Delta_\omega, E_{p^\infty}) = 0.$$

Suppose next that $v = p$. The extension $F_{\infty,\omega}$ of $\mathbb{Q}_p$ is deeply ramified in the sense of ref. 8 because it contains the deeply ramified field $\mathbb{Q}_p(\mu_{p^\infty})$, where μ_{p^∞} denotes the group of all p-power roots of unity. We can therefore apply the principal results of ref. 8 to calculate Ker γ_p and Coker γ_p. We deduce that γ_p is surjective because $H^2(\Delta_\omega, \tilde{E}_{\mathrm{p}^\infty}) = 0$ and that Ker γ_p is finite, with order equal to

$$\#(H^0(\Delta_\omega, \tilde{E}_{p^\infty}))\#(H^1(\Delta_\omega, \tilde{E}_{p^\infty})) = \#(\tilde{E}(\mathbb{F}_p)(p))^2,$$

completing the proof of the lemma.

LEMMA 5. *Assume* $L(E, 1) \neq 0$. *Then* (i) $\mathcal{S}(\mathbb{Q})$ *is finite,* (ii) $H^2(G(\mathbb{Q}_S|\mathbb{Q}), E_{p^\infty}) = 0$, *and* (iii) *the cokernel of* λ *is finite of order equal to* $\#(E(\mathbb{Q})(p))$.

Proof. Assertion (*i*) is a fundamental result of Kolyvagin. Assertions (*ii*) and (*iii*) follow immediately from the finiteness of $\mathcal{S}(\mathbb{Q})$ and Cassels' variant of the Poitou-Tate sequence (cf. the proof of Theorem 12 of ref. 7).

LEMMA 6. *Assume that* $L(E, 1) \neq 0$. *Then the map* λ_∞ *in the above diagram is surjective.*

Proof. We make essential use of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$. The finiteness of $\mathcal{S}(\mathbb{Q})$ implies that $\widehat{\mathcal{S}(\mathbb{Q}_\infty)}$ is torsion over the Iwasawa algebra $I(\Gamma_\infty)$. A well known argument then shows that the sequence

$$0 \to \mathcal{S}(\mathbb{Q}_\infty) \to H^1(G(\mathbb{Q}_S/\mathbb{Q}_\infty), \mathrm{E}_{\mathrm{p}^\infty}) \to \bigoplus_{v\in S} H_{\infty,v} \to 0 \qquad \textbf{[8]}$$

is exact, where $H_{\infty,v} = \oplus_\omega H^1(\mathbb{Q}_{\infty,\omega}, E)$ (p) and ω runs over all places of $\mathbb{Q}_\infty$ dividing v. Next, we assert that $H^1(\Gamma_\infty, \mathcal{S}(\mathbb{Q}_\infty)) = 0$. Indeed, $H^1(\Gamma_\infty, \mathcal{S}(\mathbb{Q}_\infty))$ is finite because $\mathcal{S}(\mathbb{Q})$ is finite, whence $H^1(\Gamma_\infty, \mathcal{S}(\mathbb{Q}_\infty)) = 0$ because $\widehat{\mathcal{S}(\mathbb{Q}_\infty)}$ has no non-zero finite Γ_∞-submodule (see ref. 9). Hence, taking Γ_∞-invariants of the above exact sequence, we see that the natural map

$$\varphi_\infty : (H^1(G(\mathbb{Q}_S/\mathbb{Q}_\infty), E_{p^\infty}))^{\Gamma_\infty} \to \left(\bigoplus_{v\in S} H_{\infty,v}\right)^{\Gamma_\infty}$$

is surjective. But the surjectivity of φ_∞ and the surjectivity of γ together clearly show that γ_∞ is surjective, as required.

LEMMA 7 (J.-P. Serre, personal communication). *We have* $\chi(G_\infty, E_{p^\infty}) = 1$ *and* $H^4(G_\infty, E_{p^\infty}) = 0$.

To prove Theorem 3, one simply uses diagram chasing in the above diagram, combined with Lemmas 4–7.

Sketch of the Proof of Theorem 2. We begin with another purely local calculation. For each $v \in S$, let $J_{\infty,v}$ be the G_∞-module defined at the beginning of §2.

LEMMA 8. *For each* $v \in S$, *we have* $H^i(G_\infty, J_{\infty,v}) = 0$ *for all* $i \geqslant 1$.

Proof. Fix a place ω of F_∞ above v, and let Δ_ω denote the Galois group of $F_{\infty,\omega}$ over $\mathbb{Q}_v$. Then for all $i \geqslant 0$, we have

$$H^i(G_\infty, J_{\infty,v}) \xrightarrow{\sim} H^i(\Delta_\infty, H^1(F_{\infty,\omega}, E)(p)).$$

On the other hand, the results of ref. 8 show that $H^1(F_{\infty,\omega}, E)(p)$ is isomorphic as a Δ_∞-module to A_ω, where A_ω is defined to be $H^1(F_{\infty,\omega}, B_\omega)$, with $B_\omega = E_{p^\infty}$ or $\tilde{E}_{p^\infty}$, according as $v \neq p$ or $v = p$. One then proves that $H^i(\Delta_\omega, B_\omega) = 0$ for all $i \geqslant 2$. Using the Hochschild-Serre spectral sequence, it is then easy to show that $H^i(\Delta_\omega, A_\omega) = 0$ for all $i \geqslant 1$, as required.

If W is an abelian group, we define, as usual, $T_p(W) = \varprojlim (W)_{p^n}$, where $(W)_{p^n}$ denotes the kernel of multiplication by p^n

on W. We put $T_p(E)$ for $T_p(E_{p^\infty})$. For each integer $m \geqslant 0$, we define $R(F_m)$ by the exactness of the sequence

$$0 \to R(F_m) \to H^1(F_m, T_p(E)) \to \prod_{\omega} T_p(H^1(F_{m,\omega}, E)).$$

We then define

$$\mathcal{R}(F_\infty) = \varprojlim_{m} R(F_m),$$

where the projective limit is taken with respect to the corestriction maps from F_m to F_n when $m \geqslant n$. Recall that Σ_∞ denotes the Galois group of F_∞ over F_0.

LEMMA 9. *If $\widehat{\mathcal{S}(F_\infty)}$ is torsion over the Iwasawa algebra $I(\Sigma_\infty)$, then $\mathcal{R}(F_\infty) = 0$.*

Proof. This is analogous to the well known argument for the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$, which has already been implicitly used in proving exactness at the right hand end of Eq. **8** (we recall that $L(E, 1) \neq 0$ automatically implies that $\widehat{\mathcal{S}(\mathbb{Q}_\infty)}$ is torsion over $I(\Gamma_\infty)$). The only unexpected point is to note that the projective limit of the $E_{p^{n+1}}(n = 0, 1, \ldots)$ with respect to the norm maps from F_m to F_n when $m \geqslant n$ is in fact zero. Indeed, since G_∞ is open in $GL_2(\mathbb{Z}_p)$, one sees that, for all sufficiently large n, the norm map from F_n to F_{n-1} acts as multiplication by p^4 onto $E_{p^{n+1}}$, whence the previous assertion is plain.

We assume that for the rest of this section that $\mathcal{S}(F_\infty)$ is torsion over the Iwasawa algebra $I(\Sigma_\infty)$. Then we claim that

$$H^2(G(\mathbb{Q}_S/F_\infty), E_{p^\infty}) = 0, \qquad \textbf{[9]}$$

and that the sequence

$$0 \to \mathcal{S}(F_\infty) \to H^1(G(\mathbb{Q}_S/F_\infty), E_{p^\infty}) \xrightarrow{\Psi_\infty} \bigoplus_{v \in S} J_{\infty,v} \to 0 \qquad \textbf{[10]}$$

is exact. Indeed, applying Cassels' variant of the Poitou-Tate sequence to each of the fields $F_n(n = 0, 1, \ldots)$, and then passing to the inductive limit as $n \to \infty$ with respect to the restriction maps, we obtain an exact sequence

$$0 \to Coker(\Psi_\infty) \to \widehat{\mathcal{R}(F_\infty)} \to H^2(G(\mathbb{Q}_S/F_\infty), E_{p^\infty}) \to 0$$

whence Eqs. **9** and **10** follow immediately from Lemma 9. In fact, Eq. **9** is known to be true for all $p \ddagger 2$ without any additional hypothesis.

LEMMA 10. *Assume that $\widehat{\mathcal{S}(F_\infty)}$ is torsion over $I(\Sigma_\infty)$. Then $H^i(G_\infty, H^1(G(\mathbb{Q}_S/F_\infty), E_{p^\infty})) = 0$ for $i \geqslant 2$, and*

$$H^1(G_\infty, H^1(G(\mathbb{Q}_S/F_\infty), E_{p^\infty})) \overset{\sim}{\rightarrow} H^3(G_\infty, E_{p^\infty}). \qquad \textbf{[11]}$$

Proof. The assertion (Eq. **11**) follows from the Hochschild-Serre spectral sequence (cf. Theorem 3 of ref. 10) on using Eq. **9** and (*ii*) of Lemma 5. Similarly, the first assertion of Lemma 10 is an immediate consequence of Theorem 3 of ref. 10 and the fact that $G(\mathbb{Q}_S/F_\infty)$ has p-cohomological dimension $\leqslant 2$, together with the fact that $H^4(G_\infty, E_{p^\infty}) = 0$ (J.-P. Serre, personal communication).

To complete the proof of Theorem 2, we take G_∞-invariants of the exact sequence (Eq. **10**). Using Lemmas 6, 8, and 10, we deduce that

$$H^1(G_\infty, \mathcal{S}(F_\infty)) \overset{\sim}{\rightarrow} H^3(G_\infty, E_{p^\infty}),$$

and that $H^i(G_\infty, \mathcal{S}(F_\infty)) = 0$ for all $i \geqslant 2$. Hence, Theorem 2 follows from Theorem 3.

We finish with the following remark. Let K_∞ be the fixed field of the center of G_∞, and let H_∞ denote the Galois group of K_∞ over $\mathbb{Q}$. We conjecture that, under the same hypotheses as Conjecture 1, the H_∞-Euler characteristic of the Selmer group $\mathcal{S}(K_\infty)$ of E over K_∞ is finite and equal to $\rho_p(E/\mathbb{Q})$. If we assume that $\widehat{\mathcal{S}(F_\infty)}$ is torsion over $I(\Sigma_\infty)$, we can prove this conjecture for the Euler characteristic of $\mathcal{S}(K_\infty)$.

We are very grateful to J.-P. Serre for providing us with a proof that $\chi(G_\infty, E_{p^\infty}) = 1$. We also warmly thank B. Totaro for pointing out to us a result that revealed an error in an earlier version of this manuscript.

1. Serre, J.-P. (1972) *Invent. Math.* **15,** 259–331.
2. Serre J.-P. (1965) *Topology* **3,** 413–420.
3. Lazard, M. (1965) *Publ. Math. IHES* **26,** 1–219.
4. Harris, M. (1979) *Comp. Math.* **39,** 177–245.
5. Serre J.-P. (1964) *Izv. Akad. Nauk SSSR Ser. Mat.* **28,** 3–20.
6. Serre, J.-P. (1971) *Izv. Akad. Nauk SSSR Ser. Mat.* **35,** 731–737.
7. Coates, J. & McConnell, G. (1994) *J. London Math. Soc.* **50,** 243–269.
8. Coates, J. & Greenberg, R. (1996) *Invent. Math.* **124,** 129–174.
9. Greenberg, R. (1997) *Proc. Natl. Acad. Sci. USA* **94,** 11125–11128.
10. Hochschild, G. & Serre, J.-P. (1953) *Trans. Amer. Math. Soc.* **74,** 110–134.

Proc. Natl. Acad. Sci. USA
Vol. 94, pp. 11118–11120, October 1997
Colloquium Paper

This paper was presented at a colloquium entitled "Elliptic Curves and Modular Forms," organized by Barry Mazur and Karl Rubin, held March 15–17, 1996, at the National Academy of Sciences in Washington, DC.

p-adic *L* functions and trivial zeroes

BERNADETTE PERRIN-RIOU

Mathématique, Université de Paris-Sud, Bâtiment 425, F-91405 Orsay, France

ABSTRACT The following is adapted from the notes for the lecture. It announces results and conjectures about values of the *p*-adic *L* function of the symmetric square of an elliptic curve.

First let us give some examples of trivial zeroes. Let $K/\mathbb{Q}$ be an imaginary quadratic field such that p splits in K, η the associated quadratic Dirichlet character; the Euler factor of $L(\eta, s)$ at p is $1 - p^{-s}$. Choose an ideal $\mathcal{P}$ above p and a compatible embedding of an algebraic closure $\mathbb{Q}$ of $\mathbb{Q}$ in an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. There exists a Kubota–Leopoldt p-adic L function $L_p(\eta, s)$ such that for $n > 0$ and even,

$$L_p(\eta, 1-n) = (1 - (\eta\omega^{-n})(p)p^{n-1})L(\eta\omega^{-n}, 1-n).$$

THEOREM [Ferrero–Greenberg (1)].

$$L_p(\eta, 0) = 0$$

$$L_p'(\eta, 0) = -\ell_p(\eta)L(\eta, 0),$$

with $\ell_p(\eta) = \dfrac{\log_p q}{\mathrm{ord}_p q}$ *and* $q = \pi/\bar{\pi}$, $\mathcal{P}^h = (\pi)$.

Let $E/\mathbb{Q}$ be a modular elliptic curve with split multiplicative reduction at p. Mazur *et al.* (2) have constructed a p-adic L function $L_p(\mathrm{E}, s)$.

THEOREM [Greenberg–Stevens (3)].

$$L_p(E, 1) = 0$$

$$L_p'(E, 1) = \ell_p(E)L(E, 1),$$

with $\ell_p(E) = \dfrac{\log_p q_E}{\mathrm{ord}_p q_E}$ *and* q_E *the Tate parameter of* $E/\mathbb{Q}_p$.

It has been recently proved that $\ell_p(E)$ is nonzero: Barré-Sirieix *et al.* (12) proved that if $E/\overline{\mathbb{Q}}$ is a Tate curve at p, and if j_E is algebraic, then q_E is transcendental.

Finally, let E be a modular elliptic curve over $\mathbb{Q}$ and $1 - a_p p^s + p^{1-2s}$ the Euler factor at p of its L function. Let $M = Sym^2(h_1(E)) = Sym^2(h^1(E))$ (2). The Tate twist of M is M^* (1) $= \mathfrak{sl}(h_1(E)) = \mathfrak{sl}(h^1(E))$. The Euler factor at p of M is

$$(1 - p^{-1}p^{-s})(1 - \alpha^{-2}p^{-s})(1 - \beta^{-2}p^{-s}),$$

where $\alpha + \beta = a_p$, $\alpha\beta = p$. The Euler factor at p of $M^*(1)$ is

$$(1 - p^{-s})\left(1 - \frac{\alpha}{\beta}p^{-s}\right)\left(1 - \frac{\beta}{\alpha}p^{-s}\right).$$

When E has ordinary reduction, a p-adic L function has been constructed by interpolation of values of twists of $L(M, s)$ at $s = 0$ (4). The complex L function $L(M, s)$ is nonzero at $s = 0$ because 0 is inside the convergence domain of the Euler product.

Under a mild technical hypothesis, the following theorem has been proved:

THEOREM [Greenberg–Tilouine (5)]. *Assume* E *has multiplicative reduction at* p. *Then,*

$$L_p(M, 0) = 0$$

$$L_p'(M, 0) = \ell_p(M)\frac{L(M, 0)}{\Omega_\infty},$$

where Ω_∞ *is some explicit complex period and* $\ell_\mathrm{p}(\mathrm{M}) = \ell_\mathrm{p}(\mathrm{E})$.

So $L_p(M, s)$ has a simple zero [recall $\ell_p(E)$ is nonzero].

In general, a trivial zero should appear when 1 or p^{-1} annihilates the p-Euler factor. It means that the p-adic L function should have a zero of multiplicity strictly bigger than the one of the complex L function.

The following work has been done by Greenberg (6) (in the ordinary situation). (*i*) He gives a definition of some $\ell_p(M)$ in a very general case. In particular, for $M = Sym^2(h_1(E))$ with E having (good) ordinary reduction. (*ii*) He gives a conjecture for the behavior of the p-adic L function at the trivial zero (multiplicity order of the zero and behavior of the dominant coefficient of the expansion at this zero). (*iii*) He checks that one recovers theorems already proved.

In this talk, we look only at the case of the *symmetric square of an elliptic curve* with good reduction at p, we explain in this special case: (*i*) the construction of the Greenberg invariant in the ordinary case, (*ii*) a construction of a similar invariant in the supersingular case; (*iii*) the conjectural definition of the p-adic L function; (*iv*) a conjectural link between the p-adic L function and a conjectural special system, and (*v*) consequences on the p-adic L function and the trivial zero.

Section 1. Notations

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, $G_\mathbb{Q} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. In the following, M will designe $Sym^2(h_1(E))$. The p-adic realization of M is $V = M_p = Sym^2(V_p(E))$ with $V_p(E) = \mathbb{Q}_p \otimes \varprojlim_n E_{p^n}$. It's a p-adic representation of $G_\mathbb{Q}$ of dimension 3.

Let $\mathbf{D}_p(V)$ be the filtered φ-module associated to V by Fontaine's theory. If $\mathbf{D}_{dR}(M) = Sym^2(H^1_{dR}(E))[-2]$, there exists a natural isomorphism $\mathbf{D}_p(V) = \mathbb{Q}_p \otimes \mathbf{D}_{dR}(M)$. We describe the action of φ and the filtration explicitly. Let (e_0, e_{-1}, e_{-2}) be a basis such that $\varphi e_{-1} = p^{-1}e_{-1}$, $\varphi e_0 = \alpha^{-2}e_0$, $\varphi e_{-2} = \beta^{-2}e_{-2}$.

In the *ordinary case*, we can choose α to be in $\mathbb{Z}_p^\times$; the filtration is given by

$$\begin{cases} \mathrm{Fil}^0\mathbf{D}_p(V) = \mathbb{Q}_p\omega_\mathrm{e} \\ \mathrm{Fil}^{-1}\mathbf{D}_p(V) = \mathbb{Q}_p\omega_\mathrm{e} \oplus \mathbb{Q}_p(e_{-1} + \lambda e_{-2}), \end{cases}$$

where $\omega_\mathrm{e} = \dfrac{\lambda}{2}e_{-2} + e_{-1} + \dfrac{1}{2\lambda}e_0$ for some $\lambda \in \mathbb{Q}_p$ that we assume nonzero.

In the *supersingular case* (and $a_p = 0$, which is automatic if $p > 3$), V is a direct sum (as a $G_{\mathbb{Q}_p}$-representation): $V = W_1 \oplus W_2$ with

$$W_2 = \mathbb{Q}_p(1)(\varepsilon), \mathbf{D}_p(W_2) = \mathbb{Q}_p e_{-2},$$

$$\varphi e_{-2} = \beta^{-2} e_{-2} = -p^{-1} e_{-2}$$

and

$$\mathbf{D}_p(W_1) = \mathbb{Q}_p e_{-1} \oplus \mathbb{Q}_p e_{-0},\ \varphi e_{-1} = p^{-1} e_{-1},$$

$$\varphi e_0 = \alpha^{-2} e_0 = -p^{-1} e_0.$$

The filtration is given by

$$\begin{cases} \mathrm{Fil}^0 \mathbf{D}_p(V) = \mathbb{Q}_p \omega_{\mathrm{e}} \\ \mathrm{Fil}^{-1} \mathbf{D}_p(V) = \mathbb{Q}_p \omega_{\mathrm{e}} \oplus \mathbb{Q}_{\mathrm{p}} e_{-2} \end{cases},$$

with $\omega_{\mathrm{e}} = e_{-1} - e_0$ [for some suitable choice of (e_0, e_{-1}, e_{-2})].

In both cases, $\mathbf{D}_p(V)^{\varphi=p^{-1}} = \mathbb{Q}_p e_{-1}$. In supersingular case, take $\lambda = -1/2$.

Section 2. Greenberg Invariants

2.1. Ordinary Case. On V, there exists a filtration of p-adic representations of $G_{\mathbb{Q}_p} = Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$:

$$0 \subset \mathrm{Fil}_p^2 V \subset \mathrm{Fil}_p^1 V \subset V,$$

such that

$$\mathbf{D}_p(\mathrm{Fil}_p^2 V) = \mathbb{Q}_p e_{-2}$$

$\mathbf{D}p(\mathrm{Fil}p1V) = \mathbb{Q}pe{-}2 \oplus \mathbb{Q}pe{-}1$.

So there is a natural surjection $\mathrm{Fil}_p^1 V \to \mathbb{Q}_p(1)$. We choose e_{-1} such that the map

$$\mathbf{D}_p(V)^{\varphi=p^{-1}} \to \mathbf{D}_p(\mathrm{Fil}_p^1 V) \to \mathbf{D}_p(\mathbb{Q}_p(1)) = \mathbb{Q}_p$$

sends e_{-1} to 1.

It's easy to see that $H^1(\mathbb{Q}_p, \mathrm{Fil}_p^1 V) \cong H^1(\mathbb{Q}_p, V) = H_g^1(\mathbb{Q}_p, V)$ (we use the notation H_f^1, H_g^1 of Bloch–Kato). Recall that there is an isomorphism

$$H^1(\mathbb{Q}_p, \mathbb{Q}_p(1)) \cong \mathbb{Q}_p \otimes (\mathbb{Q}_p^{\times})_p \cong \mathbb{Q}_p \times \mathbb{Q}_p.$$

The first one is just Kummer theory where $(\mathbb{Q}_p^{\times})_p = \varprojlim_n \mathbb{Q}_p^{\times}/\mathbb{Q}_p^{\times p^n}$, the second one is given by $q \mapsto (\log_p q, \mathrm{ord}_p q)$ where $\log_p$ is the logarithm on $\mathbb{Q}_p^{\times}$ such that $\log_p p = 0$. So there is a map

$$\begin{array}{ccccc} H^1(\mathbb{Q}_p, V) \cong H^1(\mathbb{Q}_p, \mathrm{Fil}_p^1 V) & \to & H^1(\mathbb{Q}_p, \mathbb{Q}_p(1)) & \to & \mathbb{Q}_p \times \mathbb{Q}_p \\ x & \mapsto & q_{\mathbf{e}}(x) & \mapsto & (\log_p q_{\mathbf{e}}(x), \mathrm{ord}_p q_{\mathbf{e}}(x)). \end{array}$$

Definition. If $x \in H^1(\mathbb{Q}_p, V)$, let

$$\ell(x) = \frac{\log_p q_{\mathbf{e}}(x)}{\mathrm{ord}_p q_{\mathbf{e}}(x)} \in \mathbb{Q}_{\mathrm{p}} \cup \infty;$$

it depends only on the line $\mathbb{Q}_p x$.

Definition. If $\mathrm{x} \in \mathrm{H}^1(\mathbb{Q}, V)$ is a universal norm in the $\mathbb{Z}_p^{\times}$-cyclotomic extension, define

$$\ell_p(M) = \ell(x) \in \mathbb{Q}_p \cup \infty.$$

The universal norms are contained in $H_{f,\{p\}}^1(\mathbb{Q}, V)$ [elements of $H^1(\mathbb{Q}, V)$ which are unramified outside of p]. Thanks to Flach (7) and under technical conditions, (*i*) the universal norms are of dimension 1; (*ii*) $H_f^1(\mathbb{Q}, V) = 0$ and $\dim H_{f,\{p\}}^1(\mathbb{Q}, V) = 1$. So in the above definition, $\ell_p(M) = \ell(x)$ for any nonzero element x of $H_{f,\{p\}}^1(\mathbb{Q}, V)$.

2.2. Supersingular Case. The canonical map

$$\iota : \mathbf{D}_p(V)^{\varphi=p^{-1}} \to \mathbf{D}_p(W_1)/\mathrm{Fil}^0 \mathbf{D}_p(W_1) = t_{W_1},$$

is an isomorphism. On the other hand, by Bloch–Kato, there is a natural map

$$\lambda_g : H^1(\mathbb{Q}_p, V) = H_g^1(\mathbb{Q}_p, V) \to \mathbf{D}_p(V)^{\varphi=p^{-1}}.$$

Once having chosen $\log_p$ on $\mathbb{Q}_p^{\times}(\log_p p = 0)$, there is a canonical splitting of the inclusion

$$H_f^1(\mathbb{Q}_p, W_1) \to H_g^1(\mathbb{Q}_p, W_1),$$

and so we obtain an extension of the Boch–Kato logarithm $\log_{W_1}$ to $\mathrm{H}_g^1(\mathbb{Q}_p, W_1)$:

$$\log_{g,W_1} : H_g^1(\mathbb{Q}_p, W_1) \to t_{W_1}.$$

Definition. If $x = (x_1, x_2) \in H_g^1(\mathbb{Q}_p, V) = H_g^1(\mathbb{Q}_p, W_1) \oplus H_f^1(\mathbb{Q}_p, W_2)$, define $\ell(x) \in \mathbb{Q}_p \cup \infty$ by

$$\ell(x) \iota \circ \lambda_g(x) = \log_{g,W_1} x_1 \in t_{W_1}.$$

Definition. Define $\ell_p(M) = \ell(x)$ with x a universal norm in $H^1(\mathbb{Q}, V)$ [again, we can just take a nonzero element in $\mathrm{H}_{f,\{p\}}^1(\mathbb{Q}, V)$].

Section 3. *p*-adic *L* Functions

Let $G_\infty = Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^{\times}$ and $\mathbb{Z}_p[[G_\infty]]$ the continuous group algebra of G_∞. Define some algebras:

$$\mathcal{K}(G_\infty) \supset \mathcal{H}(G_\infty) \supset \mathbb{Z}_p[[G_\infty]].$$

Here $\mathcal{H}(G_\infty)$ is the algebra of elements in $\mathbb{Q}_p[[G_\infty]]$ which are $O(\log^r)$ for a suitable r: it means that $f \in \mathcal{H}(G_\infty)$ can be written $f = \Sigma_n a_n(\gamma - 1)^n$ with $\sup_{n>0} |a_n|/n^r < \infty$ (γ is a topological generator of the p-part of G_∞); $\mathcal{K}(G_\infty)$ is the total fraction ring of $\mathcal{H}(G_\infty)$. If η is a continuous character from G_∞ with values $\bar{\mathbb{Q}}_p^{\times}$, we can evaluate η on any element of $\mathcal{H}(G_\infty)$.

Conjecture (10): *For any $n \in \wedge^2 \mathbf{D}_p(V)$, there exists an element $\mathbf{L}_{\{p\}}^p(n) \in \mathcal{H}(G_\infty)$ such that for any nontrivial even character η of G_∞ of conductor p^a*

$$\eta(\mathbf{L}_{\{p\}}^p(n))\mathbf{e} = \frac{1}{2} \frac{\mathrm{G}(\eta)^2 L(M, \eta, 0)}{\Omega_{\infty, \omega_{\mathbb{Q}}}} \Omega_{p, \omega_{\mathbb{Q}}}((p\varphi)^{-a}(n))$$

where (*i*) $\mathbf{e}$ *is a basis of the $\mathbb{Q}$-vector space det $D_{dR} = \mathbb{Q}(-3)_{dR}$, and $\omega_{\mathbb{Q}}$ is a basis of* Fil^0 D_{dR}; (*ii*) $\Omega_{\infty,\omega\mathbb{Q}}\mathbf{e} = \omega_{\mathbb{Q}} \wedge n_B^+ \in \mathbb{C} \otimes$ det $\mathrm{D_{dR}}$ *with* $\mathrm{n_B^+}$ *a basis of* det $\mathrm{M_B^+}$[*for example of* det $Sym^2(\mathrm{H}_{\mathit{1}}(\mathrm{E}, \mathbb{Z}))^+$]; (*iii*) $\Omega_{p,\omega_{\mathbb{Q}}}$ (n) $= \omega_{\mathbb{Q}} \wedge$ n; and (*iv*) $\mathrm{G}(\eta)$ *is a Gauss sum associated to* η.

So $\eta(\mathbf{L}_{\{p\}}^p(n))\omega_{\mathbb{Q}} \wedge \mathrm{n}_B^+ = \frac{1}{2} G(\eta)^2 L_{\{p\}}(M, \eta, 0)\omega_{\mathbb{Q}} \wedge (p\varphi)^{-a}(n)$. We may see $\mathbf{L}_{\{p\}}^p(M) = \mathbf{L}_{\{p\}}^p$ as an element of $Hom_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes \wedge^2 D_{dR}(M), \mathcal{H}(G_\infty))$ and as a function of $s \in \mathbb{Z}_p$: if χ is the cyclotomic character,

$$\mathbf{L}_{\{p\}}^p(M, s) = \langle\chi\rangle^s(\mathbf{L}_{\{p\}}^p) \text{ and } \mathbf{L}_{\{p\}}^p(M, s, n) = \langle\chi\rangle^s(\mathbf{L}_{\{p\}}^p(n)),$$

with $n \in \wedge^2 \mathbf{D}_p(V)$. For any $\mathrm{f} \in \mathcal{H}(G_\infty)$, define $\partial(\mathrm{f}) = \frac{d}{ds} \langle \chi \rangle^{\mathrm{s}} (\mathrm{f}))|_{s=0}$.

Section 4. Logarithm

Let $K_n = \mathbb{Q}_p(\mu_{p^{n+1}})$ and $Z_\infty^1(\mathbb{Q}_p, T) = \varprojlim_n H^1(K_n, T)$ with $T = Sym^2(T_p(E))$. It's a $\mathbb{Z}_p[[G_\infty]]$-module of rank 3. Note π_0 the projection on $H^1(\mathbb{Q}_p, T)$. One can construct a map (9)

$$\mathcal{L}v = \mathcal{L} : Z_\infty^1(\mathbb{Q}_p, T) \to \mathcal{H}(G_\infty) \otimes \mathbf{D}_p(V).$$

Recall only some properties of $\mathcal{L}$ (the first one depends on a "reciprocity law" conjecture that seems to be proved now). If $x \in Z_\infty^1(\mathbb{Q}_p, T)$ (11):

$$\mathbf{1}(\mathscr{L}(x)) = (1-\varphi)\lambda_g(\pi_0(x)) \in \mathbf{D}_p(V)^{\varphi=p^{-1}}.$$

If $\pi_0(x) \in H^1_e(\mathbb{Q}_p, T)$,

$$(1-\varphi)^{-1}(1-p^{-1}\varphi^{-1})\partial(\mathscr{L}(x)) \equiv \log\pi_0(x) \quad \bmod \mathrm{Fil}^0\mathbf{D}_p(V).$$

Section 5. Special Systems and *p*-adic *L* Functions

There should exist a special element $c_p^{\mathrm{spec}} \in \mathbb{Q}_p \otimes \varprojlim_n H^1(\mathbb{Q}(\mu_{p^{n+1}}), T)$ such that the p-adic L function should be defined by the formula

$$\mathbf{L}^p_{\{p\}}(n)\mathbf{e} = \mathscr{L}(c_p^{spec}) \wedge n,$$

for any $n \in \wedge^2 \mathbf{D}_p(V)$.

Define $c_p^{flach}(p) = \pi_0\,(c_p^{spec}) \in H^1(\mathbb{Q}, V)$.

CONJECTURE:

$$\lambda_g(c_p^{\mathrm{flach}}(p)) = \frac{1}{2}\left(1-\frac{\alpha}{\beta}\right)\left(1-\frac{\beta}{\alpha}\right)\frac{L(M,0)}{\Omega_{\infty,\omega_{\mathbb{Q}}}}\,\pi_{[-1]}(\omega_{\mathbb{Q}}),$$

where $\pi_{[-1]}$ is the projection on $\mathbf{D}_{\mathrm{p}}(\mathrm{V})^{\varphi=p^{-1}}$ with respect to the other eigenspaces of φ.

In the ordinary case, it means that

$$\mathrm{ord}_p q_{\mathbf{e}}(c_p^{flach}(p)) = \frac{1}{2}\left(1-\frac{\alpha}{\beta}\right)\left(1-\frac{\beta}{\alpha}\right)\frac{L(M,0)}{\Omega_{\infty,\omega_e}},$$

or

$$\mathrm{ord}_p q_{\mathbf{e}}(c_p^{flach}(p))\omega_{\mathbf{e}} \wedge n_B^+ = \frac{1}{2}\left(1-\frac{\alpha}{\beta}\right)\left(1-\frac{\beta}{\alpha}\right)L(M,0)\mathrm{e}.$$

Section 6. Some Theorems

We assume the existence of c_p^{spec} and the fact that the p-adic L function can be calculated by the formula $\mathbf{L}^p_{\{p\}}(n)\mathrm{e} = \mathscr{L}(c_p^{spec}) \wedge n$.

THEOREM: *The function $\mathbf{L}^p_{\{p\}}$ is nonzero at the trivial character* **1** *if and only if $c_p^{\mathrm{flach}}(p) \notin \mathrm{H}^1_{\mathrm{f}}(\mathbb{Q}, T)$ and one has*

$$\mathbf{1}(\mathbf{L}^p_{\{p\}}(n))\mathbf{e} = (1-p^{-1})\lambda_g(c_p^{\mathrm{flach}}(p)) \ \wedge\ n.$$

In particular, by using Flach's theorem (7), $\mathbf{L}^p_{\{p\}}$ is nonzero if and only if $c_p^{\mathrm{flach}}(p)$ is nonzero.

Assume $c_p^{flach}(\mathrm{p}) \neq 0$. Let $\mathbf{L}^{p,sc}_{\{p\}} = \mathbf{L}^p_{\{p\}}(e_{-1} \wedge e_{-2}) \in \mathscr{H}\,(G_\infty)$.

THEOREM: *The function $\mathbf{L}^{p,sc}_{\{p\}}$ has a zero at* **1** *which is simple if and only if $\ell_p(M) \neq 0$ and one has*

$$\partial(\mathbf{L}^{p,sc}_{\{p\}})\mathrm{e}_{-1} = \frac{1}{2\lambda}\,(1-\alpha^{-2})\left(1-\frac{\alpha}{\beta}\right)^{-1}\ell_p(M)\lambda_g(c_p^{\mathrm{flach}}(p)).$$

THEOREM: *The following formulas are equivalent*

$$\lambda_g(c_p^{\mathrm{flach}}(p)) = \frac{1}{2}\left(1-\frac{\alpha}{\beta}\right)\left(1-\frac{\beta}{\alpha}\right)\frac{L(M,0)}{\Omega_{\infty,\omega_{\mathbb{Q}}}}\,\pi_{[-1]}(\omega_{\mathbb{Q}}),$$

$$(1-p^{-1}\varphi^{-1})\mathbf{1}(\mathbf{L}^p_{\{p\}})\mathrm{e} = \frac{1}{2}\frac{L_{\{p\}}(M,0)}{\Omega_{\infty,\omega_{\mathbb{Q}}}}\,(1-\varphi)\Omega_{p,\omega_{\mathbb{Q}}},$$

$$\partial(\mathbf{L}^{p,sc}_{\{p\}}) = \frac{1}{2}\ell_p(M)(1-\alpha^{-2})\left(1-\frac{\beta}{\alpha}\right)\frac{L(M,0)}{\Omega_{\infty,\omega_{\mathbb{Q}}}}\,\Omega_p^{sc},$$

where $\Omega^{sc}_{p,\omega_{\mathbb{Q}}} \in \mathbb{Q}_p$ is defined by Ω^{sc}_{p,ω_Q} $\mathrm{e} = \omega_{\mathbb{Q}} \wedge e_{-1} \wedge e_{-2}$.

In the ordinary case, $\mathbf{L}^{p,sc}_{\{p\}}$ should be the p-adic function already known, the last formula is then the formula conjectured by Greenberg.

Section 7. Even More Speculations

$c_p^{\mathrm{flach}}(p)$ should come from a motivic element: so it would exist in any of the l-adic realizations of M; call it $c_l^{flach}(p) \in H^1(\mathbb{Q}, M_l)$, this element should again have good reduction outside of p. For $l \neq p$, let $\mathbf{D}_l(M) = M_l^{I_p}$; there is a map

$$\lambda_g^l : H^1(\mathbb{Q}_p, M_l) \to \mathbf{D}_l(M)^{Frob_p^{-1}=p^{-1}},$$

and for $l = p$,

$$\lambda_g^p : H^1(\mathbb{Q}_p, M_p) \to \mathbf{D}_p(M)^{\varphi=\mathrm{p}^{-1}}.$$

We have

$$\dim_{\mathbb{Q}_l}\mathbf{D}_l(M)^{Frob_p^{-1}=p^{-1}} = \dim_{\mathbb{Q}_p}\mathbf{D}_p(M_p)^{\varphi=p^{-1}}.$$

A candidate of such an element has been constructed by Flach. On the other hand, there exists a natural $\mathbb{Q}$-vector space $\mathscr{D}$ such that

$$\mathbb{Q}_l \otimes_{\mathbb{Q}} \mathscr{D} = \mathbf{D}_l(M)^{Frob_p^{-1}=p^{-1}} \text{ or } \mathbf{D}_p(M)^{\varphi=p^{-1}}.$$

It can be described in terms of the Néron–Severi group of the reduction E × E at p (8). We would like to compare $\lambda_g^l(c_l^{flach}(p))$ for different l and give a link with the p-adic L function (work in preparation). For $l \neq p$, see calculations of Flach (7).

1. Ferrero, B. & Greenberg, R. (1978) *Invent. Math.* **50,** 91–102.
2. Mazur, B., Tate, J. & Teitelbaum, J. (1986) *Invent. Math.* **84,** 1–48.
3. Greenberg, R. & Stevens, G. (1993) *Invent. Math.* **111,** 407–447.
4. Coates, J. & Schmidt, K. (1987) *J. Reine. Angew. Math.* **375,** 104–156.
5. Greenberg, R. & Tilouine, J., in preparation.
6. Greenberg, R. (1994) *Contemp. Math.* **165,** 149–181.
7. Flach, M. (1992) *Invent. Math.* **109,** 307–327.
8. Langer, A. & Saito, S. (1996) Torsion Zero-Cycles on the Self-Product of a Modular Elliptic Curve, preprint.
9. Perrin-Riou, B. (1994) *Invent. Math.* **115,** 81–149.
10. Perrin-Riou, B. (1995) *Astérisque* **229**.
11. Perrin-Riou, B. (1995) in *Proceedings of the International Congress on Mathematics*, ed. Chatterji, S. D. (Birkhäuser, Basel), pp. 400–410.
12. Barré-Sirieix, K., Diaz, G., Gramain, F. & Philibert, G. (1996) *Invent. Math.* **124,** 1–9.

Proc. Natl. Acad. Sci. USA
Vol. 94, pp. 11121–11124, October 1997
Colloquium Paper

This paper was presented at a colloquium entitled "Elliptic Curves and Modular Forms," organized by Barry Mazur and Karl Rubin, held March 15–17, 1996, at the National Academy of Sciences in Washington, DC.

Adjoint modular Galois representations and their Selmer groups

(*p*-adic *L*-function/class number formula/main conjecture)

HARUZO HIDA*†, JACQUES TILOUINE‡, AND ERIC URBAN‡

*Department of Mathematics, University of California, Los Angeles, CA 90095-1555; and ‡Institut Galilée, Université de Paris-Nord, Avenue Jean-Baptiste Clement, 93430 Villetaneuse, France

ABSTRACT In the last 15 years, many class number formulas and main conjectures have been proven. Here, we discuss such formulas on the Selmer groups of the three-dimensional adjoint representation ad(ϕ) of a two-dimensional modular Galois representation ϕ. We start with the *p*-adic Galois representation ϕ_0 of a modular elliptic curve *E* and present a formula expressing in terms of $L(1, \mathrm{ad}(\phi_0))$ the intersection number of the elliptic curve *E* and the complementary abelian variety inside the Jacobian of the modular curve. Then we explain how one can deduce a formula for the order of the Selmer group $\mathrm{Sel}(\mathrm{ad}(\phi_0))$ from the proof of Wiles of the Shimura–Taniyama conjecture. After that, we generalize the formula in an Iwasawa theoretic setting of one and two variables. Here the first variable, *T*, is the weight variable of the universal *p*-ordinary Hecke algebra, and the second variable is the cyclotomic variable *S*. In the one-variable case, we let ϕ denote the *p*-ordinary Galois representation with values in $GL_2(\mathbf{Z}_p[[T]])$ lifting ϕ_0, and the characteristic power series of the Selmer group $\mathrm{Sel}(\mathrm{ad}(\phi))$ is given by a *p*-adic *L*-function interpolating $L(1, \mathrm{ad}(\phi_k))$ for weight $k + 2$ specialization ϕ_k of ϕ. In the two-variable case, we state a main conjecture on the characteristic power series in $\mathbf{Z}_p[[T, S]]$ of $\mathrm{Sel}(\mathrm{ad}(\phi) \otimes \nu^{-1})$, where ν is the universal cyclotomic character with values in $\mathbf{Z}_p[[S]]$. Finally, we describe our recent results toward the proof of the conjecture and a possible strategy of proving the main conjecture using *p*-adic Siegel modular forms.

The talk at the conference on Elliptic Curves and Modular Forms at the National Academy of Sciences was presented by H.H. The purpose of the talk was to describe formulas giving the characteristic ideal of the Selmer group of the Galois representations as in the title in terms of their *L*-values. We fix a prime $p \geq 5$. Although we can treat the general case, allowing ramification at finitely many primes and ∞, to keep the paper short, we assume that the ramification is concentrated on $\{p, \infty\}$.

1. Selmer Groups

Let *G* be the Galois group of the maximal extension $\mathbf{Q}^{(p)}/\mathbf{Q}$ unramified outside $\{p, \infty\}$. Let $\mathcal{O}$ be a valuation ring finite flat over $\mathbf{Z}_p$ with residue field $\mathbf{F}$. We start with a two-dimensional continuous representation $\phi : G \to GL_2(A)$ for a complete (noetherian) local $\mathcal{O}$-algebra *A* with residue field $\mathbf{F} = A/m_A$. The power series ring $\mathcal{O}[[T_1, \ldots, T_r]]$ is an example of such *A*. We let *G* act on $V = A^2$ via ϕ and on End(*V*) by conjugation: $\phi \otimes \phi^\vee(\sigma)x = \phi(\sigma)x\phi(\sigma)^{-1}$. We look at its three-dimensional factor $\mathrm{ad}(\phi) : G \to GL_3(A)$ acting on trace zero subspace $V(\mathrm{ad}(\phi))$ in End(*V*). Thus $\phi \otimes \phi^\vee = \mathrm{ad}(\phi) \oplus \mathbf{1}$. Let $\bar{\phi} = \phi \bmod m_A$. We assume the following three conditions:

(AI) *The restriction of* $\bar{\phi}$ *to Gal* $(\mathbf{Q}^{(\mathrm{p})}/\mathbf{Q}(\sqrt{(-1)^{(\mathrm{p}-1)/2}\mathrm{p}}))$ *is absolutely irreducible;*

(Ord) *For each decomposition group* D *over* p, $\phi|_{\mathrm{D}} \cong \left(\begin{smallmatrix}\delta & * \\ 0 & \varepsilon\end{smallmatrix}\right)$ *with unramified* δ;

(Reg) $\delta \bmod \mathrm{m_A} \neq \varepsilon \bmod \mathrm{m_A}$.

Condition AI is equivalent to the absolute irreducibility of $\mathrm{ad}(\bar{\phi})$ over *G*. We write $V(\delta) \subset V$ for the δ-eigen subspace, and for each *A*-submodule *X* of $V(\mathrm{ad}(\phi))$, let $X^* = X \otimes_A A^*$ for the Pontryagin dual $A^* = \mathrm{Hom}_{\mathcal{O}}(A, \mathbf{Q}_p/\mathbf{Z}_p)$ of *A*. We put $V_+ = \{\xi \in V(\mathrm{ad}(\phi)) \subset \mathrm{End}(V) \mid \xi(V(\delta)) = 0\}$. Then we define the Selmer group for ad(ϕ), as a special case of Greenberg's definition (ref. 1; see also ref. 2):

$$\mathrm{Sel}(\mathrm{ad}(\phi)) = \ker(H^1(G, V(\mathrm{ad}(\phi))^*) \to H^1(I, V(\mathrm{ad}(\phi))^*/V_+^*))$$

for the inertia subgroup *I* of *D*. This is a generalization of the class group; for example, taking a quadratic character χ of *G*,

$$\mathrm{Sel}(\chi) = \ker(H^1(G, V(\chi)^*) \to H^1(I, V(\chi)^*))$$

is the χ-part of the *p*-class group of the quadratic extension *F* fixed by $\ker(\chi)$. Thus if $A = \mathcal{O}$ and if $L(1, \mathrm{ad}(\phi)) \neq 0$, a naive guess is that $\mathrm{Sel}(\mathrm{ad}(\phi))$ is finite and that its order is the p-part of $L(1, \mathrm{ad}(\phi))$ up to a transcendental factor. The finiteness is first shown by Flach (3) and then by Wiles (4). We discuss later some good cases where this guess works well. We generalize the above definition to a tensor product $\mathrm{ad}(\phi) \otimes \varepsilon$ with a character $\varepsilon : G \to B^\times$ for a complete noetherian $\mathcal{O}$-algebra *B*, replacing *A* by $A\hat{\otimes}_{\mathcal{O}}B$ and V_+ by $V_+(\mathrm{ad}(\phi) \otimes \varepsilon) = V_+ \hat{\otimes} B$:

$$\mathrm{Sel}(\mathrm{ad}(\phi)\otimes\varepsilon) = \ker(H^1(G,V(\mathrm{ad}(\phi)\otimes\varepsilon)^*)$$
$$\to H^1(I,V(\mathrm{ad}(\phi)\otimes\varepsilon)^*/V_+(\mathrm{ad}(\phi)\otimes\varepsilon)^*)),$$

which is a discrete module over $A\hat{\otimes}_{\mathcal{O}}B$.

2. Elliptic Curves over Q

For simplicity, we suppose that ϕ_0 is the Galois representation on $H^1(E_{/\bar{\mathbf{Q}}}, \mathbf{Z_p})$ for a modular elliptic curve $E_{/\mathbf{Q}}$ inside the Jacobian $J = J_0(p)$ of the modular curve $X_0(p)$. Thus *E* has multiplicative reduction at *p* and has good reduction outside *p*. Taking the dual of the inclusion $E \subset J$, we have a quotient map $\pi : J \to E$. Then $J = E + A$ for $A = \ker(\pi)$, and $E \cap A$ is a finite group of square order. For a Néron differential ω on the Néron model $E_{/\mathbf{Z}}$, by a result of Mazur (5) corollary 4.1, we may assume that $\pi^*\omega = 2^e(2\pi i f_0(z)dz)$ for a primitive form $f_0 \in S_2(\Gamma_0(p))$ and $e \in \mathbf{Z}$. Choosing a base $c_\pm$ of $\pm$-eigenspace of $H_1(E(\mathbf{C}), \mathbf{Z})$ under complex conjugation, we define $\Omega_\pm$ by $\int_{c_\pm} \omega$ after normalizing $c_\pm$ as described below. The following formula was proven 15 years ago in ref. 6 (see also ref. 7):

†To whom reprint requests should be addressed.

$$\text{(IN1)}\qquad \frac{L(1,\,\mathrm{ad}(\phi_0))}{C^{-1}(2\pi i)\Omega_+\Omega_-} = \sqrt{|E\cap A|} \in \mathbf{Z}$$

(intersection number formula),

where $C = 2^{a+2e}p(p-1)$ for $2^a = [H_1(E(\mathbf{C}), \mathbf{Z}) : \mathbf{Z}c_+ \oplus \mathbf{Z}c_-]$. We define the canonical period $U(f_0)$ of f_0 by $C^{-1}(2\pi i)\Omega_+\Omega_-$. In ref. 6, to get formula IN1, we used the period determinant

$$u = \left|\begin{pmatrix} \int_{c_1}\omega & \int_{c_2}\omega \\ \int_{c_1}\bar{\omega} & \int_{c_2}\bar{\omega} \end{pmatrix}\right|$$

for a $\mathbf{Z}$-base $\{c_1, c_2\}$ of $H_1(E(\mathbf{C}), \mathbf{Z})$ in place of $\Omega_+\Omega_-$ (see ref. 6, formula 6.20b). Writing $\omega_\pm = (\omega \pm \bar{\omega})/2$, we see $\int_{c_\pm} \omega = \pm \int_{c_\pm} \omega_\pm$, and thus $\Omega_+ \in \mathbf{R}$ and $\sqrt{-1}\Omega_- \in \mathbf{R}$. Replacing $c_\pm$ by their negative if necessary, we may assume that $\Omega_+ > 0$ and $\sqrt{-1}$ $\Omega_- > 0$. Under this normalization, formula IN1 is correct. Then by definition, $2^a u = \sqrt{-1}\Omega_+\Omega_-$, and we can deduce formula IN1 from ref. 6, theorem 6.1, by just remarking that $L^*_{f_0}/L_{f_0} \cong E \cap A$ under the notation of the theorem quoted.

Actually, a formula similar to formula IN1 is proven in ref. 6 for the Galois representation attached to any holomorphic primitive form of weight ≥2. The formula is generalized later to cohomological cusp forms on $GL(2)$ over imaginary quadratic fields in ref. 8.

Let H be the subalgebra of End(J) generated by Hecke operators $T(n)$. Then π induces the projection $\lambda : H \to \mathbf{Z} \subset \mathrm{End}(E)$ and another projection $\lambda' : H \to \mathrm{End}(A)$. Then we define two finite modules:

$$C_0 = Im(\lambda) \otimes_H Im(\lambda') \text{ and}$$

$$C_1 = \Omega_{H/\mathbf{Z}} \otimes_{H,\lambda} Im(\lambda) \cong \ker(\lambda)/\ker(\lambda)^2.$$

It is proven in ref. 7 (equation 5.8b) that

$$(E \cap A)_p \cong (C_{0,p})^2$$

as H modules. Note that Spec(C_0) is the scheme theoretic intersection of Spec($Im(\lambda)$) and Spec($Im(\lambda')$) *in* Spec(H). Thus we get

$$\text{(IN2)}\qquad p\text{-part of } \frac{L(1,\,\mathrm{ad}(\phi_0))}{U(f_0)} = |C_{0,p}|$$

(intersection number formula in Spec(H)).

Recently, Taylor and Wiles (4, 9) have shown that $|C_{0,p}| = |C_{1,p}|$, and Wiles (4) has shown

$$\mathrm{C}_{1,p} \cong \mathrm{Sel}(\mathrm{ad}(\phi_0)).$$

This formula is a key to Wiles' proof of Fermat's last theorem. The fact that Sel(ad(ϕ_0)) has a natural map into $\mathrm{C}_{1,p}$ was first discovered by Mazur through his deformation theory of Galois representations (10). The above formula is conjectured in ref. 11 after proving the surjectivity of the map besides other relevant results.

Anyway, under the various assumptions on p that we made, we finally get a formula for the order of Sel(ad(ϕ_0)):

$$\text{(CN1)}\qquad p\text{-part of } \frac{L(1,\,\mathrm{ad}(\phi_0))}{U(f_0)} = |\mathrm{Sel}(\mathrm{ad}(\phi_0))|$$

(order formula of Selmer group).

3. One-Variable Case

The cusp form $f_0 \in S_2(\Gamma_0(p))$ can be lifted to a p-adic family of p-ordinary common eigenforms $f_k = \sum_{n=1}^{\infty} a(n; f_k)q^n \in S_{k+2}(\Gamma_0(p), \omega^{-k})$ ($k \geq 0$) for the Teichmüller character ω (cf. ref. 12, chapter 7, theorem 7.3.7). For this, we need to fix an embedding $i_p : \bar{\mathbf{Q}} \hookrightarrow \bar{\mathbf{Q}}_p$. Then "$p$-ordinarity" of f_k implies that the pth coefficient of f_k in its q-expansion satisfies $|a(p; f_k)|_p = 1$. Note that, by the multiplicative reduction hypothesis, $a(p; f_0) = \pm 1$. This family yields a Galois representation $\phi : G \to GL_2(\Lambda)$ for a finite flat $\mathbb{O}[[T]]$-algebra Λ (ref. 12, section 7.5). For simplicity, we assume $\Lambda = \mathbb{O}[[T]]$. Then writing as ϕ_k the specialization of ϕ via $1 + T \mapsto u^k$ for $u = 1 + p$, ϕ_k is the Galois representation of the cusp form f_k. Then the Pontryagin dual Sel*(ad(ϕ)) of Sel(ad(ϕ)) is shown by Wiles and Taylor to be a torsion $\mathbb{O}[[T]]$-module of finite type, and its characteristic power series is given by the characteristic power series of the Λ-adic congruence module $C_{0,\Lambda}$.

Before giving the definition of $C_{0,\Lambda}$, we note that we have taken cohomological formulation of Galois representations. In this paper, we characterize Galois representations by the characteristic polynomial of geometric Frobenii Frob_q at primes $q \neq p$. For example, ϕ_k is characterized by

$$\det(1 - \phi_k(\mathrm{Frob}_q)X) = 1 - a(q; f_k)X - \omega^{-k}(q)q^{k+1}X^2.$$

This normalization is dual to the one taken in ref. 4, but it is all right for our purpose because $\mathrm{ad}(\phi_k) = \mathrm{ad}(\phi_k^\vee)$.

To define $\mathrm{C}_{0,\Lambda}$, we need to introduce the space S_Λ of p-ordinary Λ-adic cusp forms. For that, we consider the subspace $S_{k+2}(\Gamma_0(p), \omega^{-k}; \bar{\mathbf{Q}})$ of $S_{k+2}(\Gamma_0(p), \omega^{-k})$ made of cusp forms f with $a(n; f) \in \bar{\mathbf{Q}}$ for all n. We consider the $\bar{\mathbf{Q}}_p$-span $S_{k+2}(\Gamma_0(p), \omega^{-k}; \bar{\mathbf{Q}}_p)$ of $S_{k+2}(\Gamma_0(p), \omega^{-k}; \bar{\mathbf{Q}})$ in $\bar{\mathbf{Q}}_p[[q]]$ via q-expansion. We write $S^{\mathrm{ord}}_{k+2}(\Gamma_0(p), \omega^{-k}; \bar{\mathbf{Q}}_p)$ for the subspace of $S_{k+2}(\Gamma_0(p), \omega^{-k}; \bar{\mathbf{Q}}_p)$ spanned by all p-ordinary eigenforms. An element $\mathcal{F} \in S_\Lambda$ is a formal q-expansion $\sum_{n=1}^{\infty} a_n(T)q^n \in \Lambda[[q]]$ such that the specialization $\mathcal{F}_k$ via $1 + T \mapsto u^k$ is the q-expansion of an element in $S^{\mathrm{ord}}_{k+2}(\Gamma_0(p), \omega^{-k}; \bar{\mathbf{Q}}_p)$ for all $k \geq 0$. Then S_Λ is free of finite rank over Λ on which Hecke operators $T(n)$ naturally act (ref. 12, section 7.3). Hereafter we write $\mathcal{F}$ for the unique Λ-adic form such that $\mathcal{F}_k = f_k$ for all $k \geq 0$. Let H be the Λ-subalgebra of $\mathrm{End}_\Lambda(S_\Lambda)$ generated by $T(n)$ for all n, and define a Λ-algebra homomorphism $\lambda : H \to \Lambda$ by $\mathcal{F}|h = \lambda(h)\mathcal{F}$. We also have another λ' of H into $\mathrm{End}_\Lambda(\ker(\lambda))$ given by multiplication by $h \in H$ on $\ker(\lambda)$. Then we define

$$C_{0,\Lambda} = Im(\lambda) \otimes_H Im(\lambda') \text{ and}$$

$$C_{1,\Lambda} = \Omega_{H/\Lambda} \otimes_{H,\lambda} Im(\lambda) \cong \ker(\lambda)/\ker(\lambda)^2.$$

Then it is easy to see that $\mathrm{C}_{0,\Lambda} \cong \Lambda/(\eta(\mathrm{T}))$ for an element $\eta(T) \in \Lambda$. We can deduce from the result of Wiles and Taylor in ref. 4 (theorem 3.3) and ref. 9 that

$$(\eta(T)) = \mathrm{char}_\Lambda(C_{1,\Lambda}) \text{ and } C_{1,\Lambda} \cong \mathrm{Sel}^*(\mathrm{ad}(\phi)).$$

Here the characteristic ideal $\mathrm{char}_A(M)$ for a torsion A-module of finite type M over a normal noetherian ring A is given by the product of prime divisors P in A with exponent given by $\mathrm{length}_{A_P}M_P$ of the localization M_P at P. Note that, as shown in ref. 7 (theorem 0.1), for a canonical period $U(f_k)$ associated to f_k,

$$\text{(CN2)}\qquad \eta(u^k - 1) = \frac{L(1,\,\mathrm{ad}(\phi_k))}{U(f_k)}$$

up to p-adic units. This formula is not completely satisfactory, because the p-adic L-function $\eta(T)$ is determined only up to units in Λ. For Λ-adic forms of CM type, we can choose a suitable Katz p-adic L-function in place of η (11, 13–15). In general, we can only make a conjecture on the existence of a canonical p-adic L-function $L_p(\mathrm{ad}(\phi))$ with precise interpolation property (16), which generates $\mathrm{char}_\Lambda(\mathrm{Sel}^*(\mathrm{ad}(\phi))) = (\eta(\mathrm{T}))$ after extending scalar to the p-adic integer ring $\mathbb{O}_\Omega$ of the p-adic completion Ω of $\bar{\mathbf{Q}}_p$.

4. Two-Variable Case

Now we look at the universal character $\nu : G \to \mathbb{O}[[S]]^\times$ deforming the identity character of G. As already said, our formulation is cohomological, and hence $\nu(\mathrm{Frob}_q) = q\omega(q)^{-1}$ for geometric Frobenius Frob_q. Writing $\mathbf{Q}_\infty$ for the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$ and $\Gamma = \mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$, the tautological character: $\Gamma \hookrightarrow \mathbb{O}[[\Gamma]]$ induces the above ν for $S = \gamma - 1$ for a generator γ of Γ. Then we consider $\mathrm{Sel}^*(\mathrm{ad}(\phi) \otimes \nu^{-1})$, which is a module over $\mathbb{O}[[T, S]]$ of finite type (1). Classically, the Selmer group involving the cyclotomic variable S is defined in terms of cohomology groups over the cyclotomic $\mathbf{Z}_p$ tower $\mathbf{Q}_\infty$. As shown by Greenberg (ref. 1, proposition 3.2; see also ref. 2, section 3.1), our Selmer group $\mathrm{Sel}(\mathrm{ad}(\phi) \otimes \nu^{-1})$ over $\mathbf{Q}$ is isomorphic to the classical one over $\mathbf{Q}_\infty$. Recently, we have proven a control theorem for $\mathrm{Sel}(\mathrm{ad}(\phi) \otimes \nu^{-1})$ giving the following theorem.

THEOREM 1. *The module* $\mathrm{Sel}^*(ad(\phi) \otimes \nu^{-1})$ *is a torsion* $\mathbb{O}[[T, S]]$*-module of finite type. Moreover, the characteristic power series of* $\mathrm{Sel}^*(ad(\phi) \otimes \nu^{-1})$ *is of the form* $S\Psi(T, S)$ *in* $\mathbb{O}[[T, S]]$ *and* $\Psi(T, 0)|\eta(T)\ da/dT\ (T)$ *in* $\mathbb{O}[[T]]$*, where* $a(T)$ *is the eigen value of* $T(p)$ *for* $\mathcal{F}$ *lifting* f_0 (2). *In early* 1980*s, we constructed* (17) *a two-variable p*-adic *L*-function $L(T, S)$ in $\eta(T)^{-1}S\mathbb{O}[[T, S]]$ such that for even m with $-k \le m \le 0$,

$$\eta(u^k - 1)L(u^k - 1, u^m - 1) = *E(k, m)\,\frac{L(1 - m, \mathrm{ad}(\phi_k))}{(2\pi i)^{-2m}U(f_k)}$$

for a factor E like an Euler p-factor and a simple constant $*$. This L-function ηL again has ambiguity by units in Λ, although $L(T, S)$ is uniquely determined. In ref. 16, the existence of a canonical p-adic L-functions $L_p(\mathrm{ad}(\phi) \otimes \nu^{-1})$ in $\mathbb{O}[[T, S]]$ [for $\mathrm{ad}(\phi) \otimes \nu^{-1}$] with precise interpolation property is conjectured. In particular, we should have an equality:

$$L(T, S) = \frac{L_p(\mathrm{ad}(\phi) \otimes \nu^{-1})}{L_p(\mathrm{ad}(\phi))}.$$

Anyway, the denominator and the numerator are not yet known to exist in general in spite of the known existence of the ratio $L(T, S)$. Because of this, we need to use $\eta(T)$ as a replacement of $L_p(\mathrm{ad}(\phi))$.

THEOREM 2. (R. Greenberg and J. Tilouine). *Write* $\eta L(T, S) = S\Phi(T, S)$. *We have*

$$\Phi(0, 0) = \eta(0)\frac{da}{dT}(0) \textit{ up to units in } \mathbb{O}.$$

We know that $da/dT\,(0) \neq 0$ by the theorem of St. Etienne (18) due to four people at St. Etienne in France. Thus if one can prove the divisibility $\Phi|\Psi$ in $\mathbb{O}[[T, S]]$, the following conjecture follows.

MAIN CONJECTURE. *We have* $\Phi = \Psi$ *up to a unit in* $\mathbb{O}[[T, S]]$. *Actually this conjecture is close to being proven, assuming the following ordinarity conjecture on the local structure of Weissauer's Galois representations, as discussed in the lectures of E. Urban at the Mehta Research Institute (Allahabad, India). Let us explain Urban's strategy. First of all, there is a theory of (nearly)* p-ordinary $\mathbb{O}[[T, S]]$-adic forms on $GSp(4)$, developed mainly by Tilouine and Urban (19, 20). A cohomological Hecke eigenform f on $GSp(4)_{/\mathbf{Q}}$ is called nearly p-ordinary if its eigenvalues for two standard Hecke operators at p are p-adic units under the fixed embedding $\bar{\mathbf{Q}}$ into $\bar{\mathbf{Q}}_p$. Here the word cohomological means that the system of Hecke eigenvalues for f appears in the middle cohomology H^3 with coefficients in a polynomial representation L of a Siegel modular variety for $\mathrm{GL}(4)_{/\mathbf{Q}}$. In other words, f belongs to a discrete series representation whose Harish–Chandra parameter is the sum of the highest weight of L and the half sum of positive roots. For each cohomological eigenform f, Weissauer has attached a p-adic modular Galois representation ρ_f into $GL(4)$ with characteristic polynomials of Frobenii outside p given by the Hecke polynomial (see ref. 21). Here is the ordinarity conjecture for the Galois representation.

ORDINARITY CONJECTURE. *Assume that f is nearly p-ordinary. Then the image of the decomposition group at p of* ρ_f *is in a Borel subgroup of GSp(4). Weissauer's construction gave a compatible system of l*-adic representations attached to f, and ρ_f is one of its members. When ρ_f is crystalline, we have two characteristic polynomials at p. One is that of the crystalline Frobenius $L_{\mathrm{cris}}(X)$, and the other, $L_{\mathrm{et}}(X)$, is that of the Frobenius at p of a non-p-adic member of the compatible system. The p-ordinarity conjecture follows in this case if one can prove $L_{\mathrm{cris}}(X) = L_{\mathrm{et}}(X)$, which is a standard conjecture and is known to be true at least for constant sheaves (that is, so to speak, the weight 0 case).

It is enough to prove the ordinarity conjecture for crystalline ρ_f for the following reason. We can glue Weissauer's Galois representations by means of Taylor's pseudorepresentations and attach to each $\mathbb{O}[[T, S]]$-adic eigen cusp form $\mathcal{G}$ a Galois representation $\rho_{\mathcal{G}} : G \to GL_4(F_{\mathbb{I}})$ for the field of fractions $F_{\mathbb{I}}$ of a finite extension $\mathbb{I}$ of $\mathbb{O}[[T, S]]$. Thus at densely populated points on $\mathrm{Spec}(\mathbb{I})$, $\rho_{\mathcal{G}}$ specializes into Weissauer's Galois representations. Furthermore, $\rho_{\mathcal{G}}$ has densely populated specializations on $\mathrm{Spec}(\mathbb{I})$ which are crystalline at p. Thus if one can prove the p-ordinarity conjecture for crystalline specializations, the image under $\rho_{\mathcal{G}}$ of each decomposition group at p is in a Borel subgroup in $GSp(4)$, and hence the ordinarity conjecture for all specializations follows.

We now come back to the strategy for a proof of the Main Conjecture. We look at the Klingen-style $\mathbb{O}[[T, S]]$-adic Eisenstein series $\mathcal{E}$ induced from the Λ-adic form $\mathcal{F}$. The Galois representation $\rho_{\mathcal{E}}$ attached to $\mathcal{E}$ has values in the standard maximal parabolic subgroup, that is, it is of the following form:

$$\rho_{\mathcal{E}} \cong \begin{pmatrix} \phi & * \\ 0 & {}^t\phi^{-1} \otimes \nu\det(\phi) \end{pmatrix} \subset GSp_4(\mathbb{O}[[T, S]]).$$

The constant term of $\mathcal{E}$ at the nonstandard parabolic subgroup $\mathbb{P}$ is almost equal to $\mathcal{F}$ times $\eta(T)L(T, S)$. Here we mean by nonstandard the parabolic subgroup given by

$$\mathbb{P} = \left\{ \begin{pmatrix} * & 0 & * & * \\ * & * & * & * \\ * & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix} \in GSp(4) \right\}.$$

Thus the Eisenstein ideal *Eis* giving congruence between $\mathcal{E}$ and another $\mathbb{O}[[T, S]]$-adic cusp form $\mathcal{G}$ should be generated by $\eta(T)L(T, S)$. In particular, under the p-ordinarity conjecture, Urban has shown for such Eisenstein primes P dividing $\Phi(T, S)$, if $\mathcal{G} \equiv \mathcal{E} \bmod P$ for a cusp form $\mathcal{G}$, $\rho_{\mathcal{G}}$ has values in $GSp(4)$ and is irreducible. It was a nontrivial task to prove this because the representation is residually reducible. We also note that, to prove this, we again need the result of Wiles (4) proving the conjecture in ref. 11. The fact that $\rho_{\mathcal{G}}$ has values in $GSp(4)$ is essential in the proof because it guarantees that the adjoint action of $\rho_{\mathcal{E}}$ on the unipotent radical of the standard maximal parabolic subgroup is actually isomorphic to $\mathrm{ad}(\phi) \otimes \nu^{-1}$. The extension of $\nu\det(\phi) \otimes {}^t\phi^{-1} \bmod P$ by $\phi \bmod P$ induced from $\rho_{\mathcal{G}}$ can be made nonsplit because of the irreducibility of $\rho_{\mathcal{G}}$. This nontrivial extension gives rise to a nontrivial cocycle in $\mathrm{Sel}(\mathrm{ad}(\phi) \otimes \nu^{-1})$ under the Ordinarity Conjecture. This is a $GSp(4)$ version of an argument of Wiles in (22) applied to $GL(2)$. Since it is true for each height one prime P dividing *Eis*, we conclude that the Eisenstein ideal *Eis* of $\mathcal{E}$ divides Ψ, assuming the Ordinarity Conjecture. To establish the divisibility $\Phi|Eis$, in other words, to establish the congruence $\mathcal{G} \equiv \mathcal{E} \bmod P^e$ for $P^e|\Phi$, we need to have precise information on $\mathcal{E}$ (not just its existence), for example, its Fourier coefficients, its Whittaker model, and so on.

Although each author had already worked out some of their share of the work presented here before they visited the Mehta Research Institute of Mathematics and Mathematical Physics (MRI, Allahabad, India) in January and February, 1996, the coordination in bringing all the efforts into a general framework was done while they were visiting Allahabad. We are grateful to Prof. Dipendra Prasad at MRI for giving us the opportunity of working together and to the audience at MRI for patiently listening to our lectures on the subject whose formulation was not yet definite. H.H. acknowledges the support from the National Science Foundation during the preparation of the paper.

1. Greenberg, R. (1994) *Proc. Symp. Pure Math. (1994)* **55,** Part 2, 193–223.
2. Hida, H. (1996) *Séminaire de Théorie des Nombres, Paris, 1993–94*, LMS lecture notes series (Cambridge Univ. Press, Cambridge, U.K.), Vol. 235, pp. 89–132.
3. Flach, M. (1992) *Invent. Math.* **109,** 307–327.
4. Wiles, A. (1995) *Ann. Math.* **142,** 443–551.
5. Mazur, B. (1978) *Invent. Math.* **44,** 129–162.
6. Hida, H. (1981) *Invent. Math.* **63,** 225–261.
7. Hida, H. (1988) *Am. J. Math.* **110,** 323–382.
8. Urban, E. (1995) *Compositio Math.* **99,** 283–324.
9. Taylor, R. & Wiles, A. (1995) *Ann. Math.* **142,** 553–572.
10. Mazur, B. (1987) *Galois Group over* **Q**, Mathematical Sciences Research Institute publications (Springer, New York), Vol. 16.
11. Mazur, B. & Tilouine, J. (1990) *Publ. I.H.E.S.* **71,** 65–103.
12. Hida, H. (1993) *Elementary Theory of L-Functions and Eisenstein Series* (London Math. Soc. Student text, Cambridge Univ. Press, Cambridge, U.K.), Vol. 26.
13. Tilouine, J. (1988) *Compositio Math.* **65,** 265–320.
14. Tilouine, J. (1989) *Duke Math. J.* **59,** 629–673.
15. Hida, H. & Tilouine, J. (1994) *Invent. Math.* **117,** 89–147.
16. Hida, H. (1996) *On the Search of Genuine p-Adic Modular L-Functions* for $GL(n)$, Mémoires de Societe Mathematique de France (French Math. Soc., Paris), Vol. 67.
17. Hida, H. (1990) *Perspect. Math.* **11,** 93–142.
18. Barré-Sirieix, K., Diaz, G., Gramain, F. & Philibert, G. (1996) *Invent. Math.* **124,** 1–9.
19. Tilouine, J. & Urban, E. (1995) *C. R. Acad. Sci. Ser. I* **321,** 5–10.
20. Tilouine, J. & Urban, E. (1997) *Several Variable p-Adic Families of Siegel–Hilbert Cusp Eigensystems and Their Galois Representations,* preprint.
21. Weissaur, R. (1996) *A Special Case of the Fundamental Lemma, the Case of* $GSp_4(F)$*,* preprint.
22. Wiles, A. (1990) *Ann. Math.* **131,** 493–540.

Proc. Natl. Acad. Sci. USA
Vol. 94, pp. 11125–11128, October 1997
Colloquium Paper

This paper was presented at a colloquium entitled "Elliptic Curves and Modular Forms," organized by Barry Mazur and Karl Rubin, held March 15–17, 1996, at the National Academy of Sciences in Washington, DC.

The structure of Selmer groups

RALPH GREENBERG

Department of Mathematics, Box 354350, University of Washington, Seattle, WA 98195-4350

ABSTRACT The purpose of this article is to describe certain results and conjectures concerning the structure of Galois cohomology groups and Selmer groups, especially for abelian varieties. These results are analogues of a classical theorem of Iwasawa. We formulate a very general version of the Weak Leopoldt Conjecture. One consequence of this conjecture is the nonexistence of proper Λ-submodules of finite index in a certain Galois cohomology group. Under certain hypotheses, one can prove the nonexistence of proper Λ-submodules of finite index in Selmer groups. An example shows that some hypotheses are needed.

The results that I will describe here are motivated by a well-known theorem of Iwasawa. Let K be a finite extension of $\mathbb{Q}$. Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension of K, where p is any prime. Thus $K_\infty \subseteq K(\mu_{p^\infty})$ and $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, the additive group of p-adic integers. We let $\Lambda = \mathbb{Z}_p[[\Gamma]]$ be the completed group algebra of Γ over $\mathbb{Z}_p$, which is isomorphic (noncanonically) to the formal power series ring $\mathbb{Z}_p[[T]]$. Let M_∞ denote the maximal abelian pro-p extension of K_∞ unramified outside $\Sigma = \{p, \infty\}$. Let L_∞ denote the maximal abelian pro-p extension of K_∞ unramified at all primes of K_∞. Let $X = \mathrm{Gal}(M_\infty/K_\infty)$ and $Y = \mathrm{Gal}(L_\infty/K_\infty)$. In ref. 1, Iwasawa proves the following important result.

THEOREM (Iwasawa):

(i) *X and Y are finitely generated Λ-modules.*

(ii) *$\mathrm{Rank}_\Lambda(X) = r_2$, where r_2 denotes the number of complex primes of K.*

(iii) *Y is a torsion Λ-module.*

(iv) *X has no nonzero finite Λ-submodules.*

We remark also that if K_∞/K is an arbitrary $\mathbb{Z}_p$-extension, (*i*) and (*iii*) are true (due to Iwasawa). Statement (*ii*) should conjecturally be true. It is often referred to as the "Weak Leopoldt Conjecture" for K_∞/K and has the following interpretation. Let K_n denote the unique subfield of K such that K_n/K is cyclic of degree p^n. Let $\tilde{K}_n$ denote the compositum of all $\mathbb{Z}_p$-extensions of K_n. Then it is known that

$$\mathrm{Gal}(\tilde{K}_n/K_n) \cong \mathbb{Z}_p^{r_2 p^n + 1 + \delta_n},$$

where $\delta_n \geq 0$. Leopoldt's Conjecture states that $\delta_n = 0$. The Weak Leopoldt Conjecture states that δ_n is bounded as $n \to \infty$, which is equivalent to the assertion that $\mathrm{rank}_\Lambda(X) = r_2$. Also if statement (*ii*) holds, then so does statement (*iv*). (See proposition 4 of ref. 2.)

Returning to the cyclotomic $\mathbb{Z}_p$-extension K_∞/K, we can restate Iwasawa's theorem in terms of the Pontryagin duals

$$\mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p), \quad \mathrm{Hom}(Y, \mathbb{Q}_p/\mathbb{Z}_p),$$

which are subgroups of $H^1(G_{K_\infty}, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}(\mathrm{Gal}(K_\infty^{\mathrm{ab}}/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$ defined by imposing certain local conditions. They are examples of what have come to be called "Selmer groups." Iwasawa's results then become: (*i*) $\mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)$ and $\mathrm{Hom}(Y, \mathbb{Q}_p/\mathbb{Z}_p)$ are cofinitely generated Λ-modules. (*ii*) $\mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)$ has Λ-corank r_2. (*iii*) $\mathrm{Hom}(Y, \mathbb{Q}_p/\mathbb{Z}_p)$ is Λ-cotorsion. (*iv*) $\mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)$ has no proper Λ-submodules of finite index.

Now consider an abelian variety A defined over K with good, ordinary reductions at the primes of K lying over p. We denote by $\mathrm{Sel}_A(K_\infty)_p$ the p-primary subgroup of the classical Selmer group for A over K_∞. Over K_n, this Selmer group is defined as follows.

$$\mathrm{Sel}_A(K_n)_p = \ker\Big(H^1(G_{K_n}, A[p^\infty]) \to \bigoplus_v J_v(K_n)\Big),$$

where $J_v(K_n) = \bigoplus_{\eta|v} (H^1(K_{n,\eta}, A[p^\infty])/L_\eta)$. Here $A[p^\infty]$ denotes the p-power torsion points on $A(\bar{K})$, v runs over all primes of K, η over the primes of K_n lying over v, and L_η denotes the image of the local Kummer homomorphism for A over the η-adic completion $K_{n,\eta}$ of K_n. We define $J_v(K_\infty) = \varinjlim_n J_v(K_n)$ (with obvious maps). Then $\mathrm{Sel}_A(K_\infty)_p = \varinjlim_n \mathrm{Sel}_A(K_n)_p$ can be defined by

$$\begin{aligned}\mathrm{Sel}_A(K_\infty)_p &= \ker\Big(H^1(K_\infty, A[p^\infty]) \to \bigoplus_v J_v(K_\infty)\Big)\\ &= \ker\Big(H^1(K_\Sigma/K_\infty, A[p^\infty]) \to \bigoplus_{v\in\Sigma} J_v(K_\infty)\Big),\end{aligned}$$

where Σ is a finite set of primes of K containing all primes of K where A has bad reduction as well as all primes dividing p or ∞. In the early 1970s, Mazur made the following conjecture, where K_∞/K is assumed to be the cyclotomic $\mathbb{Z}_p$-extension.

CONJECTURE (Mazur): *$\mathrm{Sel}_A(K_\infty)_p$ is Λ-cotorsion.*

One can weaken the assumption that A has good, ordinary reduction at all $\mathfrak{p}$ dividing p. For each $\mathfrak{p}|p$, let $h_\mathfrak{p}$ denote the height of the formal group associated to the Neron model for A over the integers in any finite extension of $K_\mathfrak{p}$ where A achieves semistable reduction. Let $g = \dim(A)$. Then Mazur's conjecture should be true if K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension and $h_\mathfrak{p} = g$ for all primes $\mathfrak{p}$ of K lying over p. Using results of ref. 3, one can show that $\mathrm{Sel}_A(K_\infty)_p$ has positive Λ-corank if $h_\mathfrak{p} > g$ for at least one $\mathfrak{p}|p$ and for any $\mathbb{Z}_p$-extension in which $\mathfrak{p}$ is ramified. On the other hand, we should remark that there may exist noncyclotomic $\mathbb{Z}_p$-extensions of K where $\mathrm{Sel}_A(K_\infty)_p$ fails to be Λ-cotorsion even if A has good, ordinary reduction at all $\mathfrak{p}|p$. For example, this can occur if K_∞ is the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field K. See ref. 4 for a discussion of this issue.

I now will describe various consequences if we assume that K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension, A has good, ordinary reduction at all primes of K over p, and $\mathrm{Sel}_A(K_\infty)_p$ is Λ-cotorsion.

Consequence 1: The Λ-corank of $H^1(K_\Sigma/K_\infty, A[p^\infty])$ can be determined. For $i = 0$, 1, and 2, the Λ-modules $H^i(K_\Sigma/K_\infty, A[p^\infty])$ are cofinitely generated and their coranks are related by their Euler–Poincaré characteristic

$$\sum_{i=0}^{2}(-1)^i\mathrm{corank}_\Lambda(H^1(K_\Sigma/K_\infty, A[p^\infty]) = -[K:\mathbb{Q}]\dim(A).$$

From this one gets the lower bound $\mathrm{corank}_\Lambda(H^1(K_\Sigma/K_\infty, A[p^\infty])) \geq [K:\mathbb{Q}]\dim(A)$, with equality if and only if $H^2(K_\Sigma/K_\infty, A[p^\infty])$ is Λ-cotorsion (since $H^0(K_\Sigma/K_\infty, A[p^\infty])$ is obviously Λ-cotorsion). The calculation of the above global Euler–Poincaré characteristic is a consequence of results of Poitou and Tate for finite Galois modules over number fields. Using their results over local fields one can prove the following fact:

$$\mathrm{Corank}_\Lambda(\bigoplus_{v\in\Sigma} J_v(K_\infty)) = [K:\mathbb{Q}]\dim(A).$$

The definition of the Selmer group and the assumption that $\mathrm{Sel}_A(K_\infty)_p$ is Λ-cotorsion then imply that $\mathrm{corank}_\Lambda(H^1(K_\Sigma/K_\infty, A[p^\infty])) = [K:\mathbb{Q}]\dim(A)$.

Consequence 2: The map $\gamma{:}H^1(K_\Sigma/K_\infty, A[p^\infty]) \to \bigoplus_{v\in\Omega} J_v(K_\infty)$ is surjective. It is clear by comparing the Λ-coranks that the cokernel of this map will be Λ-cotorsion. The surjectivity is a consequence of studying the behavior of the corresponding cokernels over the K_n's. One uses the known fact that $A[p^\infty]^{G_{K_\infty}}$ is finite.

Consequence 3: In addition to the above assumptions, assume that at least one of the following hold: (*i*) $A^t(K)$ has no p-torsion. (*ii*) For some $v \nmid p$, $A[p^\infty]^{I_v}$ is finite. (*iii*) For some $\mathfrak{p}|p$, $e(\mathfrak{p}/p) \leq p-2$. Then $\mathrm{Sel}_A(K_\infty)_p$ has no proper Λ-submodules of finite index.

The proof of this consequence is discussed in a much more general context in ref. 5. In (*ii*), I_v denotes the inertia subgroup of G_{K_v}. If A is an elliptic curve, then (*ii*) is equivalent to A having additive reduction at some $v \nmid p$. In (*iii*), $e(\mathfrak{p}/p)$ is the ramification index; this assumption clearly holds if $p > [K:\mathbb{Q}] + 1$. Assumption (*i*) also holds if p is sufficiently large, at least for a fixed A and K.

I want to add several remarks about these consequences. Consequence 1 should be true more generally, without the stringent assumptions made above. For any abelian variety defined over K and for any $\mathbb{Z}_p$-extension K_∞/K, it is conjecturally true that $H^1(K_\Sigma/K_\infty, A[p^\infty])$ has Λ-corank equal to $[K:\mathbb{Q}]\dim(A)$. This is equivalent to the assertion that $H^2(K_\Sigma/K_\infty, A[p^\infty])$ is Λ-cotorsion. I will state later a much more general conjecture which will also include the Weak Leopoldt Conjecture stated earlier.

Concerning consequence 2, let Ω denote a finite set of primes of K not dividing p or ∞. Define a "nonprimitive" Selmer group $\mathrm{Sel}_A^\Omega(K_\infty)_p$ by

$$\mathrm{Sel}_A^\Omega(K_\infty)_p = \ker(H^1(K_\infty, A[p^\infty]) \to \bigoplus_{v\notin\Omega} J_v(K_\infty)).$$

Thus $\mathrm{Sel}_A(K_\infty)_p \subseteq \mathrm{Sel}_A^\Omega(K_\infty)_p$. Choose a finite set Σ as before, but also containing Ω. The surjectivity of γ gives an isomorphism

$$\mathrm{Sel}_A^\Omega(K_\infty)_p/\mathrm{Sel}_A(K_\infty)_p \cong \bigoplus_{v\in\Omega} J_v(K_\infty).$$

This isomorphism has an interesting interpretation in connection with Mazur's "Main Conjecture" which asserts that the characteristic ideal of the Λ-module $\mathrm{Sel}_A(K_\infty)_p^\wedge$ is generated by a certain element $\theta_A \in \Lambda$ associated to the p-adic L-function for A over K. The existence of this p-adic L-function is known only under very restrictive hypotheses, e.g., if $K = \mathbb{Q}$ and A is a modular elliptic curve. But if it exists, then it is easy to construct a "nonprimitive" analogue with an interpolation property involving values of the Hasse–Weil L-function for A with the Euler factors for primes in Ω omitted. One could then define an element $\theta_A^\Omega \in \Lambda$. It turns out that $\theta_A^\Omega = \mathcal{P}_\Omega{\cdot}\theta_A$, where $\mathcal{P}_\Omega$ generates the characteristic ideal of $\bigoplus_{v\in\Omega} J_v(K_\infty)^\wedge$. Thus the main conjecture is equivalent to a nonprimitive analogue asserting that the characteristic ideal of $\mathrm{Sel}_A^\Omega(K_\infty)_p^\wedge$ is generated by θ_A^Ω.

Concerning consequence 3, some restrictive hypotheses are necessary. Here is an example to show that. Let $K = \mathbb{Q}(\mu_5)$ and $p = 5$. Let E be the elliptic curve/$\mathbb{Q}$ of conductor 11 such that $E(\mathbb{Q})$ is trivial. (The other two elliptic curves of conductor 11 are isogenous to E and contain a $\mathbb{Q}$-rational point of order 5.) Now $K_\infty = \mathbb{Q}(\mu_{5^\infty})$ and $\mathrm{Gal}(K_\infty/\mathbb{Q}) \cong \Delta \times \Gamma$, where $\Delta = \mathrm{Gal}(K/\mathbb{Q})$. Let ω denote the Teichmuller character of Δ. Then we can decompose $\mathrm{Sel}_A(K_\infty)_p$ by the action of Δ:

$$\mathrm{Sel}_A(K_\infty)_p = \bigoplus_{i=0}^{3} \mathrm{Sel}_A(K_\infty)_p^{\omega^i}.$$

One can determine the structure as a Λ-module of each factor. The result is that the Pontryagin dual of $\mathrm{Sel}_A(K_\infty)_p^{\omega^i}$ is isomorphic to: $\Lambda/5^2\Lambda$ if $i = 0$, 0 if $i = 1$, the maximal ideal $M \subseteq \Lambda/5^2\Lambda$ (which has index 5) if $i = 2$, and $\mathbb{Z}/5\mathbb{Z}$ if $i = 3$. Thus $\mathrm{Sel}_A(K_\infty)_p$ has a Λ-submodule of index $p = 5$, the kernel of projecting to the ω^3 factor.

It is interesting to note that Iwasawa's μ-invariant for $\mathrm{Sel}_A(K_\infty)_p$ is nonzero in the above example. Mazur first gave such examples in ref. 6, e.g. $X_0(11)$ for $p = 5$, $K = \mathbb{Q}$ in which case he showed that $\mu = 1$. The behavior of the μ-invariant under isogenies has been studied by Schneider (7) [and in a more general context by Perrin-Riou (8)]. Using their results, the following conjecture would predict the value of μ. Conjecture: *μ can be made zero by isogeny.* For $X_0(11)$ and for $K = \mathbb{Q}$, $p = 5$, the isogenous elliptic curve $E = X_0(11)/\mu_5$ will have $\mathrm{Sel}_A(K_\infty)_p = 0$.

We will now formulate a general version of the Weak Leopoldt Conjecture, which gives a prediction of the Λ-corank of $H^2(K_\Sigma/K_\infty, M)$ and, as a consequence, $H^1(K_\Sigma/K_\infty, M)$ for a very general $\mathrm{Gal}(K_\Sigma/K)$-module M. The previously stated version is the special case $M = \mathbb{Q}_p/\mathbb{Z}_p$, on which $\mathrm{Gal}(K_\Sigma/K)$ acts trivially (and Σ = the set of primes of K lying over p or ∞). Various generalizations and special cases have been considered by Schneider (7), Greenberg (9), Coates and McConnell (10), and Perrin-Riou (11). The form we will give here is inspired by the thesis of McConnell. Let V be a finite dimensional $\mathbb{Q}_p$-representation space for $\mathrm{Gal}(K_\Sigma/K)$, where Σ is a finite set of primes of K containing the primes over p and ∞. Let T be a Galois-invariant $\mathbb{Z}_p$-lattice in V. Let $d = \dim_{\mathbb{Q}_p}(V)$, $d_v^\pm = \dim_{\mathbb{Q}_p}(V^\pm)$ for the real primes of K, where $V^\pm$ denotes the (±1)-eigenspaces for a complex conjugation above v. Let $M = V/T$. Let K_∞/K be any $\mathbb{Z}_p$-extension. It is known that both $H^1(K_\Sigma/K_\infty,, M)$ and $H^2(K_\Sigma/K_\infty, M)$ are cofinitely generated Λ-modules (where $\Lambda = \mathbb{Z}_p[[\Gamma]]$, $\Gamma = \mathrm{Gal}(K_\infty/K)$) and that

$$\mathrm{corank}_\Lambda(H^1(K_\Sigma/K_\infty, M)) = \mathrm{corank}_\Lambda(H^2(K_\Sigma/K_\infty, M)) + \delta,$$

where $\delta = r_2d + \Sigma_{v\,\mathrm{real}}\, d_v^-$. (See ref. 9, proposition 3. The Euler–Poincaré characteristic for M over K_∞ is $-\delta$.) For any prime v of K, we let $H_v^2(K_\infty, M) = \varinjlim_n (\bigoplus_{\eta|v} H^2(K_{n,\eta}, M))$, where for each n, η runs over the primes of K_n lying over v. One can prove the following result.

PROPOSITION. *The natural map $H^2(K_\Sigma/K_\infty, M) \to \bigoplus_{v\in\Sigma} H_v^2(K_\infty, M)$ is surjective. The kernel is Λ-cofree.*

Our version of the Weak Leopoldt Conjecture is the following.

CONJECTURE. *The map $H^2(K_\Sigma/K_\infty, M) \to \bigoplus_{v\in\Sigma} H_v^2(K_\infty, M)$ is an isomorphism.*

One can show that if v does not split completely in K_∞/K, then $H_v^2(K_\infty, M) = 0$. However, primes can split completely in a $\mathbb{Z}_p$-extension K_∞/K. For example, the archimedean primes of K will split completely. If K is an imaginary quadratic field, then every nonarchimedean prime v of K not dividing p will split completely in one $\mathbb{Z}_p$-extension of K. [This is obvious because $\mathrm{Gal}(\tilde{K}/K) \cong \mathbb{Z}_p^2$ and the decomposition subgroup for v is isomorphic to $\mathbb{Z}_p$.] If v is inert in $K/\mathbb{Q}$, then v splits completely in the anticyclotomic $\mathbb{Z}_p$-extension of K. It is conjectured that for any other $\mathbb{Z}_p$-extension of K at most one prime of K can split completely. (One can prove that at most two can.)

I discuss several special cases. First assume that K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension. Then the above conjecture states that

$$H^2(K_\Sigma/K_\infty,M) \cong \bigoplus_{v|\infty} H_v^2(K_\infty, M),$$

because nonarchimedean primes of K cannot split completely in K_∞/K. If p is odd, then $H_v^2(K_\infty, M) = 0$ for $v|\infty$ and hence conjecturally $H^2(K_\Sigma/K_\infty, M) = 0$. If $p = 2$, then $H_v^2(K_\infty, M)$ can be nontrivial. It is $(\Lambda/2\Lambda)$-cofree and its $(\Lambda/2\Lambda)$-corank equals $\dim_{\mathbb{Z}/2\mathbb{Z}}(M(K_v)/M(K_v)_{\mathrm{div}})$, where $M(K_v) = H^0(K_v, M)$. In the special case where $M = A[p^\infty]$, where A is an abelian variety/K, $M(K_v)/M(K_v)_{\mathrm{div}} \cong A(K_v)/A(K_v)_{\mathrm{con}}$, the group of connected components. This can be nontrivial if $K_v \cong \mathbb{R}$.

Let K_∞/K be any $\mathbb{Z}_p$-extension. Consider $M = \mathbb{Q}_p/\mathbb{Z}_p$ and $\Sigma = \{p, \infty\}$. Then $H_v^2(K_\infty, M) = 0$ for all v. Also,

$$H^1(K_\Sigma/K_\infty, M) = \mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p),$$

where $X = \mathrm{Gal}(M_\infty/K_\infty)$, M_∞ denoting as before the maximal abelian pro-p extension of K_∞ unramified outside Σ. In this case, $\delta = r_2$ and the above conjecture states that $H^1(K_\Sigma/K_\infty, M)$ should have Λ-corank r_2—i.e., $\mathrm{rank}_\Lambda(X)$ should equal r_2. This is the Weak Leopoldt Conjecture for the $\mathbb{Z}_p$-extension K_∞/K, as stated earlier.

Let K_∞/K be any $\mathbb{Z}_p$-extension. Consider $M = \mu_{p^\infty} = \mathbb{Q}_p(1)/\mathbb{Z}_p(1)$. Let Σ be a finite set containing all primes over p and ∞. Then it is not difficult to prove the Weak Leopoldt Conjecture for M and K_∞/K. (This proof is given in ref. 5.) In this case $H_v^2(K_\infty, M)$ has positive Λ-corank if v is a nonarchimedean prime which splits completely in K_∞/K. Thus $H^2(K_\Sigma/K, M)$ can have positive Λ-corank.

Let $M = A[p^\infty]$. Then $H_v^2(K_\infty, M) = 0$ for all nonarchimedean v (and for any $\mathbb{Z}_p$-extension K_∞/K). The Weak Leopoldt Conjecture states that $H^2(K_\Sigma/K_\infty, M) = 0$ if p is any odd prime. There are some known cases. For example, if A is an elliptic curve/$\mathbb{Q}$, K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension, and $K/\mathbb{Q}$ is abelian, then the conjecture is settled if A has complex multiplication and good, ordinary reduction at p [Rubin (12), where he proves Mazur's conjecture in this case], if A has complex multiplication and good, supersingular reduction at p (McConnell), and, more generally if E is modular and has good reduction at p (Kato). All of these results use a nonvanishing theorem of Rohrlich for the Hasse–Weil L-function.

Let $R_2(K_\infty,\Sigma, M)=\ker(H^2(K_\Sigma/K_\infty, M)\to\bigoplus_{v\in\Sigma} H_v^2(K_\infty, M))$. The Weak Leopoldt Conjecture for M and K_∞/K then asserts that $R_2(K_\infty, \Sigma, M) = 0$. We want to state an equivalent version (inspired by McConnell). Let $V^* = \mathrm{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p(1))$ and $T^* = \mathrm{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p(1))$. Let $M^* = V^*/T^*$. Define

$$R_1(K_\infty, \Sigma, M^*) = \ker(H^1(K_\Sigma/K_\infty, M^*) \to \bigoplus_{v\in\Sigma} H_v^1(K_\infty, M^*)).$$

Then, as a consequence of Tate's global duality theorem, one can show that $R_2(K_\infty, \Sigma, M)$ and $R_1(K_\infty, \Sigma, M^*)$ have the same Λ-corank. The Weak Leopoldt Conjecture then asserts that $R_1(K_\infty, \Sigma, M^*)$ is Λ-cotorsion.

Let F_∞ denote the fixed field for the kernel of the action of G_{K_∞} on M^*. Let $H = \mathrm{Gal}(F_\infty/K_\infty)$. Thus the action of G_{K_∞} on M^* factors through H. Let L_{F_∞} denote the maximal abelian pro-p extension of F_∞, which is unramified at all primes of F_∞. Then $G = \mathrm{Gal}(F_\infty/K)$ acts on $Y_{F_\infty} = \mathrm{Gal}(L_{F_\infty}/F_\infty)$. Here G is a p-adic Lie group, H is a closed subgroup, and one has an exact sequence $1 \to H \to G \to \Gamma \to 1$. One also has the restriction map

$$R_1(K_\infty, \Sigma, M^*) \xrightarrow{\rho} \mathrm{Hom}_H(Y_{F_\infty}, M^*).$$

The kernel of ρ is a subgroup of $H^1(H, M^*)$, which is Λ-cotorsion. We assume now that K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension. Then the cokernel of ρ is also Λ-cotorsion. Thus the Weak Leopoldt Conjecture would then be equivalent to asserting that $\mathrm{Hom}_H(Y_{F_\infty}, M^*)$ is Λ-cotorsion. A theorem of Harris (13) states that Y_{F_∞} is a torsion-module over $\mathbb{Z}_p[[G_0]]$ in a certain sense, where G_0 is a suitable open subgroup of G. If we replace K by a finite extension contained in F_∞ (so that G_K acts trivially on $M^*[p]$), then H is a pro-p group. Assume that $\mu(K_\infty/K) = 0$, which of course is a well-known conjecture of Iwasawa. This means that $Y_{K_\infty} = \mathrm{Gal}(L_{K_\infty}/K_\infty)$ is a finitely generated $\mathbb{Z}_p$-module, where L_{K_∞} is the maximal abelian pro-p extension of K_∞ unramified everywhere (denoted by L_∞ earlier). By studying the map $Y_{F_\infty}/I_H Y_{F_\infty} \to Y_{K_\infty}$, where I_H is the augmentation ideal of $\mathbb{Z}_p[[H]]$, and by using a version of Nakayama's lemma, one finds that Y_{F_∞} must be a finitely generated $\mathbb{Z}_p[[H]]$-module. But the Weak Leopoldt Conjecture for M (and for the cyclotomic $\mathbb{Z}_p$-extension K_∞/K) would then follow because $\mathrm{Hom}_H(Y_{F_\infty}, M^*)$ would consequently be cofinitely generated as a $\mathbb{Z}_p$-module and therefore Λ-cotorsion.

Continuing to assume that K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension, let $M^*(t)$ denote the tth Tate twist, where $t \in \mathbb{Z}$. Assume that $\mu_p \subseteq K$ (or $\mu_4 \subseteq K$ if $p = 2$). Then another equivalent form of the Weak Leopoldt Conjecture for M and K_∞/K is the following statement: $R_1(K, \Sigma, M^*(t))$ is finite for all but finitely many $t \in \mathbb{Z}$. Here

$$R_1(K, \Sigma, M^*(t)) = \ker(H^1(K_\Sigma/K, M^*(t)) \to \bigoplus_{v\in\Sigma} H^1(K_v, M^*(t))),$$

which has finite $\mathbb{Z}_p$-corank for all t. This formulation illustrates the "Deformation" point of view since $M^*(t) = V^*(t)/T^*(t)$ and $T^*(t)$, $t \in \mathbb{Z}$, are specializations of a representation $\mathrm{Gal}(K_\Sigma/K) \to GL_d(\Lambda)$, which is a deformation of T^* (the "cyclotomic" deformation as defined in ref. 14).

The Weak Leopoldt Conjecture for M and for an arbitrary $\mathbb{Z}_p$-extension K_∞/K has two consequences, which are analogues of parts of Iwasawa's theorem stated earlier. The first is the obvious consequence that one could then determine the Λ-corank of $H^2(K_\Sigma/K_\infty, M)$ and hence of $H^1(K_\Sigma/K_\infty, M)$, in terms of the Euler–Poincaré characteristic δ for M and the $\mathbb{Z}_p$-corank of the local Galois cohomology groups $H^2(K_v, M)$ for those $v \in \Sigma$ which split completely in K_∞/K. The second consequence is the following result.

PROPOSITION: *Assume that the Weak Leopoldt Conjecture holds for M and K_∞/K. Then $H^1(K_\Sigma/K_\infty, M)$ has no proper Λ-submodule of finite index.*

I would like to now discuss briefly Selmer groups associated to modular forms. To illustrate, consider $\Delta = \sum_{n=1}^\infty \tau(n)q^n$, where τ is Ramanujan's tau-function. We let V denote $V_p(\Delta)$, the p-adic representation associated to Δ. Let $M = V/T$, where $T = T_p(\Delta)$ is a $G_\mathbb{Q}$-invariant $\mathbb{Z}_p$-lattice. Let $\Sigma = \{p, \infty\}$. Assume p is odd. Then the Selmer group for M over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ has the following definition.

$$S_M(\mathbb{Q}_\infty) = \ker(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, M) \to H^1(\mathbb{Q}_{p,\infty}, M)/L_p),$$

where $L_p = H_f^1(\mathbb{Q}_{p,\infty}, M) = \varinjlim_n H_f^1(\mathbb{Q}_{p,n}, M)$. Here $\mathbb{Q}_{\mathrm{p},\infty} = \cup_n\mathbb{Q}_{\mathrm{p,n}}$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$, $\mathbb{Q}_{p,n}$ is the nth layer. For any finite extension $F/\mathbb{Q}_p$, $H_f^1(F, M)$ denotes the image in $H^1(F, M)$ of $H_f^1(F_v, V)$, the $\mathbb{Q}_p$-subspace of $H^1(F_v, V)$ defined by Bloch and Kato. In the so-called ordinary case [which means $p \nmid \tau(p)$], one can describe L_p as follows. It is known that there exists a one-dimensional $\mathbb{Q}_p$-subspace W of V which is $G_{\mathbb{Q}_p}$-invariant and such that V/W is unramified for the action of $G_{\mathbb{Q}_p}$. Let N denote the image of W under the map $V \to M$. Then it turns out that

$$L_p = H^1_f(\mathbb{Q}_{p,\infty}, M) = \mathrm{Im}(H^1(\mathbb{Q}_{p,\infty}, N) \to H^1(\mathbb{Q}_{p,\infty}, M)).$$

In contrast, if $p|\tau(p)$, then it seems likely that $H^1_f(\mathbb{Q}_{p,\infty}, M) = H^1(\mathbb{Q}_{p,\infty}, M)$. Then it would follow that $S_M(\mathbb{Q}_\infty) = H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, M)$. This has been proven by Perrin-Riou if $p\|\tau(p)$.

If $p \nmid \tau(p)$, then $S_M(\mathbb{Q}_\infty)$ is Λ-cotorsion (proved by Kato). We consider two ordinary primes: $p = 11$, $p = 23$. In ref. 15, I have calculated the structure of $S_M(\mathbb{Q}_\infty)$ for these primes (even as a Λ-module for $p = 11$). As groups, $S_M(\mathbb{Q}_\infty) \cong \mathbb{Q}_p/\mathbb{Z}_p$ in both cases. The idea behind the calculation is to use certain congruences between modular forms: $\Delta \equiv \mathrm{f}_E(\mathrm{mod}\ 11)$, where f_E is the modular form of weight 2 associated to $X_0(11)$, and $\Delta \equiv \mathrm{f}_\rho(\mathrm{mod}\ 23)$, where f_ρ is the weight 1 modular form associated to a certain dihedral two-dimensional Artin character. One can use an easily verified fact that $S_M(\mathbb{Q}_\infty)[p] = S_{M[p]}(\mathbb{Q}_\infty)$, where one defines the Selmer group for the finite Galois module $M[p]$ in a way analogous to the definition of $S_M(\mathbb{Q}_\infty)$, using the subgroup $N[p]$ of $M[p]$. (One needs mild hypotheses on M to verify this fact.) One can calculate the Selmer group over $\mathbb{Q}_\infty$ for $V_p(X_0(11))$ and for $V_p(\rho)$ (modulo $\mathbb{Z}_p$-lattices). This allows one to show that in both cases $S_M(\mathbb{Q}_\infty)$has order p. One concludes that $S_M(\mathbb{Q}_\infty) \cong \mathbb{Q}_p/\mathbb{Z}_p$ by using the result that $S_M(\mathbb{Q}_\infty)$ has no proper Λ-submodule of finite index [and hence $S_M(\mathbb{Q}_\infty)$ cannot be finite]. A very general result of this nature is proved in ref. 9 under rather restrictive hypotheses, and much more generally in ref. 5. However, as indicated earlier, there are cases where such a result fails to be true.

This work was partially supported by a National Science Foundation grant.

1. Iwasawa, K. (1973) *Ann. Math.* **98,** 246–326.
2. Greenberg, R. (1978) *Invent. Math.* **47,** 85–99.
3. Coates, J. & Greenberg, R. (1996) *Invent. Math.* **124,** 129–174.
4. Mazur, B. (1983) in *Proceedings of the International Congress of Mathematicians* (Polish Scientific Publishers, Warsaw), pp. 185–211.
5. Greenberg, R., in preparation.
6. Mazur, B. (1972) *Invent. Math.* **18,** 183–266.
7. Schneider, P. (1987) *J. Indian Math. Soc.* **52,** 159–170.
8. Perrin-Riou, B. (1989) *Adv. Stud. Pure Math.* **17,** 347–358.
9. Greenberg, R. (1989) *Adv. Stud. Pure Math.* **17,** 97–137.
10. Coates, J. & McConnell, G. (1994) *J. London Math. Soc.* **50,** 243–269.
11. Perrin-Riou, B. (1995) *Astérisque* **229**.
12. Rubin, K. (1988) *Invent. Math.* **93,** 701–713.
13. Harris, M. (1979) *Comp. Math.* **39,** 177–245.
14. Greenberg, R. (1994) *Proc. Symp. Pure Math.* **55,** 193–223.
15. Greenberg, R. (1991) *LMS Lecture Notes* (Cambridge Univ. Press, Cambridge), Vol. 153, pp. 211–234.

Proc. Natl. Acad. Sci. USA
Vol. 94, pp. 11129–11132, October 1997
Colloquium Paper

This paper was presented at a colloquium entitled "Elliptic Curves and Modular Forms," organized by Barry Mazur and Karl Rubin, held March 15–17, 1996, at the National Academy of Sciences in Washington, DC.

On the coefficients of the characteristic series of the U-operator

ROBERT F. COLEMAN

Department of Mathematics, University of California, Berkeley, CA 94720-3840

ABSTRACT A conceptual proof is given of the fact that the coefficients of the characteristic series of the U-operator acting on families of overconvegent modular forms lie in the Iwasawa algebra.

Introduction

In this document, I attempt to "explain" why the formula for the characteristic power series for the U-operator acting on families of completely continuous p-adic modular forms (see section B4 of ref. 2) looks the way it does. In other words, I give a conceptual proof of the part of theorem B6.1, when p is odd, which is evident from the explicit formulas (see appendix I of ref. 1) and which asserts that the coefficients of this series lie in the Iwasawa algebra $\mathbf{\Lambda} = \mathbf{Z}_p[[\mathbf{Z}_p^*]]$. I also prove that this series analytically continues to a larger space. This was asserted by this theorem and is not evident from the formulas (I have not proven this assertion when $p = 2$). I use the operator called U in section B4 of ref. 1, which is the U_p-operator on weight 0 overconvergent forms twisted by a family of Eisenstein series $\mathbf{E}$ (see section 1 below). The key point is that the q-expansion coefficients of $\mathbf{E}$ lie in $\Lambda \subset \mathbf{\Lambda}$. This is enough to prove that the function $\mathbf{E}_p$ whose q-expansion is $\mathbf{E}(q)/\mathbf{E}(q^p)$ lies in $\Lambda\hat{\otimes}A^0(Z)$ where Z is the connected component of the ordinary locus containing the cusp ∞ in $X_1(\mathbf{q})$ [a sort of affinoid q-expansion principle (see Theorem 2.1 below)]. The operator U acts on $\Lambda\hat{\otimes}A^0(Z_N)$ and if it were completely continuous that would basically do it, but it's not. I am forced into some technicalities to get around this difficulty in sections 3 and 4. I complete the proof in section 5, and in section 6, I prove theorem B6.2 of ref. 1, when p is odd, which asserts that this characteristic series "controls" forms of higher level.

Some notation: Fix a prime p. Let $\mathbf{q} = 4$ if $p = 2$ and p otherwise. Let $\Lambda = \mathbf{Z}_p[[1 + \mathbf{q}\mathbf{Z}_p]]$.

If X is a rigid analytic space and Y is a reduced affinoid with good reduction, let $Y_X = Y \times X$ and $A^\dagger(Y_X/X)$ denote the ring of overconvergent rigid analytic functions on Y_X over X (see section A5 of ref. 1). If $\mathcal{B}$ is the rigid space of continuous characters on $1 + \mathbf{q}\mathbf{Z}_p$ with values in $\mathbf{C}_p^*$, it is conformal over $\mathbf{Q}_p$ to the open unit disk. I can and do think of Λ as rigid functions on $\mathcal{B}$ defined over $\mathbf{Q}_p$ bounded by 1. If Y is the affinoid unit disk with parameter T, let $A^0(X)[T]^\dagger$ denote $A^\dagger(Y_x) \cap A^0(Y_x)$. Identifying $\mathcal{B}$ with the open unit disk, we may regard Λ as $\mathbf{Z}_p[[S]]$. Then, for each $0 < t < 1$ and $\Sigma_n^\infty b_n S^n \in \Lambda$, set

$$\left| \sum_{n=0}^{\infty} b_n S^n \right|_t = \mathrm{Max}_n\{|b_n| t^n\}.$$

If $t \in |\mathbf{C}_p|$, this is the norm obtained upon mapping an element of Λ into $A^0(B[t])$ and then taking the supremum norm of its image. Then, if $t \le s < 1$, $\log_t(s) > 0$ and one can easily check

$$|f|_t \le |f|_s \le |f|_t^{\log_t(s)}.$$

Let I be the maximal ideal in Λ. Suppose $t < 1$, then $f \in I^n$ implies

$$|f|_t \le \mathrm{Max}\{|p|^n, t^n\},$$

and if $n \le \mathrm{Min}\{\log_t(|f|_t), -\log_p(|f|_t)\}$, $f \in I^n$.

We deduce:

PROPOSITION 1.1. *All the norms* $|\ |_t$, *for* $0 < t < 1$, *are equivalent and induce the* I*-adic topology on* Λ.

COROLLARY 1.1.1. *The image of* Λ *in* $A^0(B)$ *is closed.*

I define $\Lambda[X]^\dagger$ to be the subring of $\Lambda[[X]]$ consisting of elements of the form

$$\sum_{n=0}^{\infty} \lambda_n X^n$$

for which there exists an $a > 0$ in $\mathbf{R}$ such that $\lambda_n \in I^{[an]}$ for large n. Then, $f(X) \in \Lambda[X]^\dagger$ if and only if the image of $f(X)$ in $A^0(B[t])[[X]]$ lies in $A^0(B[t])[X]^\dagger$ for some $t < 1$ if and only if the image of $f(X)$ in $A^0(B[t])[[X]]$ lies in $A^0(B[t])[X]^\dagger$ for all $t < 1$. Thus

LEMMA 1.2. $A^\dagger(B[1]_{\mathcal{B}}/\mathcal{B})^0 \cong \Lambda[X]^\dagger$.

2. A q-Expansion Principle

In this section, I will prove:

THEOREM 2.1 (q-*expansion principle*). *Suppose,* $t \in |C_p|$ *and* $0 < t < 1$. *Then, if* $G \in A^\dagger(Z_{B[t]}/B[t])$ *and* $G(q) \in \Lambda[[q]]$, G *uniquely analytically continues to an element of* $A^\dagger\ (Z_{\mathcal{B}}/\mathcal{B})^0$.

LEMMA 2.2. *There exists a finite morphism f from* $Z^\dagger$ *onto* $B[1]^\dagger$ *such that* $f^{-1}(0) = \infty$ *and, f is separated.*

Proof: Let $\bar{Z}$ be the reduction of Z and D be the divisor of degree zero on $\bar{Z}$, $s[\bar{\infty}] - \Sigma_{i=1}^s[e_i]$, where $\{e_1, \ldots, e_s\}$ is the set of points at ∞ (the supersingular points) on $\bar{Z}$. Then mD is principal for some positive integer m. Suppose m is minimal. If $\bar{f}$ is a function on the completion of $\bar{Z}$ with divisor D, $\bar{f}:\bar{Z} \to \bar{B}[1]$ is a finite separated morphism such that $\bar{f}^{-1}(0) = \infty$. We may now apply theorem A-1 of ref. 2 with $A = \mathbf{Z}_p$, $B = A^0(B[1]^\dagger)$, $C = A^0(Z^\dagger)$ and $D = \mathbf{Z}_p[X]/X^m$, thought of as the ring of the closed subscheme $m\infty$ of $Z^\dagger$, to conclude there is a lifting of f to an overconvergent function f on Z which gives a finite morphism of degree s from $Z^\dagger$ onto $B[1]^\dagger$ with the property $f^{-1}(0) = \infty$. ■

Proof of the q-expansion principle:

Let G be as in the statement of the theorem. Let f be as in the lemma. Suppose f has degree d. Let Tr_f denote the trace map from $A(Z^\dagger)$ to $A(B[1]^\dagger)$. Let X be the standard parameter on $\mathbf{A}^1$. Regarding q as a parameter at ∞, the fact that f is totally ramified above 0 implies that Tr_f extends naturally to a map from $\mathbf{Z}_p[[q]]$ to $\mathbf{Z}_p[[X]]$. Hence, we may write

$$Tr_f(q^n) = \sum_{m \geq 0} a_{n,m} X^m,$$

where $a_{n,m} \in \mathbf{Z}_p$. In fact, $a_{n,m} = 0$ for $m < n/d$. For $r \in A^0(Z^\dagger)$, we may write

$$rG(q) = \sum_n \lambda_n q^n,$$

where $\lambda_n \in \Lambda$. Now f extends to a finite morphism from $(Z_{B[t]}/B[t])^\dagger$ to $(B[1]_{B[t]}/B[t])^\dagger$ and we extend Tr_f accordingly. Then,

$$Tr_f(rG) = \sum_n \lambda_n \sum_m a_{n,m} X^m$$

$$= \sum_m \left(\sum_n a_{n,m} \lambda_n \right) X^m.$$

We know, by the above, that, for each m, the coefficient of X^m is a finite sum so lies in Λ. We also know $Tr_f(rG) \in A^\dagger(B[1]_{B[t]}/B[t])$. Since this is true for all $r \in A^0(Z^\dagger)$ we conclude $DG \in A^\dagger(Z_{\mathcal{B}}/\mathcal{B})$ where D generates the discriminant ideal in $\mathbf{Z}_p[X]^\dagger$ of $A^0(Z^\dagger)/\mathbf{Z}_p[X]^\dagger)$. Since $\bar{f}$ is separated, $p \nmid D$. The principle will follow from:

LEMMA 2.3. *Let* $\mathrm{t} \in |\mathbf{C}_\mathrm{p}| \cap$ *(0, 1). Suppose* $\mathrm{a(X)} \in \mathrm{A^0(B)[X]^\dagger}$ *and there exists a* $\mathrm{D(X)} \in \mathbf{Z}_\mathrm{p}\mathrm{[X]^\dagger}$ *such that* $\mathrm{p} \nmid \mathrm{D(X)}$ *and* $\mathrm{D(X)a(X)} \in \Lambda\mathrm{[X]^\dagger}$, *then* $\mathrm{a(X)} \in \Lambda\mathrm{[X]^\dagger}$.

Proof: Let $A = A^0(B[t])$. Suppose

$$D(X)a(X) = \sum_{n \geq 0} \lambda_n X^n,$$

where $\lambda_n \in \Lambda$ and $|\lambda_n|_t \leq \delta^n$ for some $\delta < 1$ and large n. Let d be the degree of the reduction of $D(X)$ modulo p which is defined because $\bar{D} \neq 0$. Using the division algorithm, we may write $X^n = D(X)h_n(X) + r_n(X)$ where $r_n(X)$ is either 0 or a polynomial over $\mathbf{Z}_p$ of degree strictly less than d and $h_n(X) \in \mathbf{Z}_p[X]^\dagger$. [We first know we can do this with $h_n(X) \in \mathbf{Z}_p\langle X\rangle$. Then the equation $X^n - r_n(X) = D(X)h_n(X)$ implies $h_n(X) \in \mathbf{Z}_p[X]^\dagger$.] It follows that,

$$D(X)a(X) = D(X) \sum_n \lambda_n h_n(X) + \sum_n \lambda_n r_n(X).$$

Since $|\lambda_n|_t \leq \delta^n$ for large n, we conclude both sums converge in $A[X]^\dagger$. The second sum must be 0 since it has degree strictly less than d. Since $A[X]^\dagger$ is an integral domain, we conclude

$$a(X) = \sum_n \lambda_n h_n(X).$$

The lemma follows from the fact that Λ is closed in A by Corollary 1.1.1. ■

Now suppose $b_1, \ldots, b_d$ is a basis for $A^0(Z^\dagger)$ over $\mathbf{Z}_p[X]^\dagger$. We may write, uniquely,

$$G = a_1(X)b_1 + a_2(X)b_2 + \cdots + a_d(X)b_d,$$

where $a_i(X) \in A^0(B[t])[X]^\dagger$. Then I apply the lemma to $a(X) = a_i(X)$ and deduce the theorem. ■

Let $\mathbf{E}(q)$ denote the element of $\Lambda[[q]]^*$ such that $\kappa(\mathbf{E}[q]) = E_\kappa(q)$. Recall, for $t < |\pi|$, I proved in corollary B4.1.2 of ref. 1, there exists a rigid analytic function F_0 on $Z_{B[t]}$, overconvergent relative to $B[t]$, such that $F_0(\kappa, q) = E_\kappa(q)/E_\kappa(q^p)$ for $\kappa \in B[t]$. I deduce,

COROLLARY 2.1.1. *There is an element* $\mathbf{E}_\mathrm{p} \in A^\dagger(\mathrm{Z}_{\mathcal{B}}/\mathcal{B})$ *bounded by 1 on* $\mathrm{Z}_{\mathcal{B}}$ *whose* q*-expansion is* $\mathbf{E}(\mathrm{q})/\mathbf{E}(\mathrm{q^p})$.

3. Continuous Versus Completely Continuous Operators

Suppose L is a complete subring of A, P and N are Banach modules over A and L, respectively, and $\iota{:}P \hookrightarrow N\hat{\otimes}_L A$ is a continuous injective homomorphism.

PROPOSITION 3.1. *Suppose u is a continuous linear operator on N such that* $u \otimes 1$ *preserves* $\iota(P)$ *and* $\iota^{-1}u\iota = u_P$ *is a completely continuous operator on P. Then, if there exists an orthonormal basis* $B := \{b_i\}_{i\in I}$ *for N over L and a map* $r{:}B \to A^*$ *such that* $B^* = \{r(b)b \otimes 1{:}b \in B\}$ *is contained in* $\iota(P)$ *and* $\iota^{-1}(B^*)$ *is an orthonormal basis for P, det*$(1 - Tu_P) \in L[[T]]$.

Proof: For $b \in B$, let $b^* = r(b)b \otimes 1$ and for a subset S of I, let $\pi_s{:}P \to P$ be the projector onto the subspace P_s spanned by $\{b_i^*{:}i \in S\}$ as defined in lemma A1.6 of ref. 1. Then by theorem A2.1 and lemma A1.6 of ref. 1,

$$\det(1 - Tu_P) = \lim_S \det(1 - T(\pi_S \circ u_P)|P_S),$$

as S ranges over finite subsets of I. Now since $\det(1 - T(\pi_S \circ u_P)|P_S)$ is independent of the choice of basis of P_S over A and its matrix with respect to the basis $\{b_i^*/r(b_i){:}i \in S\}$ has entries in L, we see that $\det(1 - T(\pi_S \circ u_P)|P_S) \in L[T]$. Since L is a complete subring of A, the proposition follows. ■

We will be able to apply this to the operator U because,

LEMMA 3.2. *Suppose X is a minimal underlying affinoid of a basic wide open W. Then there exists an orthonormal basis B of A(X) and an underlying affinoid Y of W such that Y strictly contains X and there exists a map r from B to K* such that* $\{r(e)e{:}e \in B\}$ *is an orthonormal basis of* $A(Y)$.

(Compare proposition 1 of ref. 3.)

This will be an immediate consequence of Corollary 4.2.1, which is a more precise version.

4. Orthonormal Bases of Wide Open Neighborhoods

Let K be a finite extension of $\mathbf{Q}_p$ contained in $\mathbf{C}_p$, R the ring of integers of K, and $\mathbf{F}$ the residue field of R. Below, the symbol r will always refer to an element of $|\mathbf{C}_p|$. Note, however, that for any given r one might have to replace K by a finite extension so that $r \in |K|$. Suppose that G is a finite Abelian group of order prime to p such that the $|G|$-th roots of unity are contained in K.

Suppose W is a basic wide open defined over K with minimal underlying affinoid X such that $W - X$ has s connected components $U_1, \ldots, U_s$ (see ref. 4). Suppose in addition that G acts faithfully on W and preserves X. For $1 \leq i \leq s$ and $\sigma \in G$ let $1 \leq \sigma(i) \leq s$ be such that $\sigma(U_i) = U_{\sigma(i)}$. Let $z_i{:}U_i \to B(0, 1)\backslash\{0\}$ be a uniformizing parameter such that the subset of U_i where $|z_i| \geq r$ is nonempty and connected to X for any $r < 1$. Suppose in addition that there exist $c(\sigma, i) \in R$ such that $\sigma^* z_i = c(\sigma, i)z_{\sigma(i)}$ (this we can arrange by using appropriate projectors like Eq. **1** below corresponding to the fixers in G of elements $1 \leq i \in s$). It follows that $c(\sigma, i) \in R^*$. For $r \leq 1$, let $X_r = W - \cup\{x \in U_i{:}|z_i(x)| < r\}$. Then for r close to 1, $r < 1$, X_r is an underlying affinoid of W which is a strict neighborhood of X and is preserved by G.

The affine $\bar{X}$ has s points at ∞, $P_1, \ldots, P_s$ corresponding to the U_i and is acted on faithfully by G [since $(|G|, p) = 1$]. For $f \in \mathbf{F}(\bar{X})$, $f \neq 0$ let

$$M(f) = -Max\{u_{P_i}(f)\}.$$

Let $m(f) = \{i{:} - v_{P_i}(f) = M(f)\}$. Let T_i be a parameter at P_i, which lifts to z_i and for $i \in m(f)$, let $c_i(f) \in F$ be such that

$$v_{P_i}(f - c_i(f)T_i^{-M(f)}) > -M(f).$$

Let A be the ring $\mathbf{F}[y_1, y_2, \ldots, y_s]/\{y_iy_j{:}i \neq j\}$ and let G act on A so that

$$\sigma^* y_i = \bar{c}(\sigma,i)y_{\sigma(i)} \quad \text{for} \quad \sigma \in G.$$

Also let $\lambda(f)$ be the element of A,

$$\sum_{i \in m(f)} c_i(f) y_i^{M(f)}.$$

It follows that $\deg(\lambda(f)) = M(f)$ and $\lambda(\sigma^* f)) = \sigma^*\lambda(f)$. Let B be the subring of A generated by $\lambda(f)$ where f ranges over $\mathcal{O}_x(\overline{X}), f \neq 0$. Then by Riemann–Roch $B \supset I := \oplus y_i^N A$ for some positive integer N. Moreover, B/I is finite dimensional over $\mathbf{F}$ and is acted on by G. Let H be a basis of B/I each element of which is an eigenvector for the action of G. Then the set

$$T = H \cup \{y_i^{nN+j}: 1 \leq i \leq s, 0 \leq j < N, n \geq 0\},$$

is a basis of B. Let t be a map from T to $\mathbf{F}(\overline{X})$, such that $\lambda(t(a)) = a$, $\sigma^*t(h) = et(h)$ if $h \in H$ and $\sigma^*h = eh$ and

$$t(y_i^{nN+j}) = \begin{cases} t(y_i^N)^n & \text{if } j = 0 \\ t(y_i^N)^{n-1}t(y_i^{N+j}) & \text{if } 0 < j < N. \end{cases}$$

Then $\{t(a): a \in T\}$ is a basis for $\mathbf{F}(\overline{X})$. For $\varepsilon \in Hom(G, R^*)$, let

$$\pi_\varepsilon = \frac{1}{|G|} \sum_{\sigma \in G} \varepsilon^{-1}(\sigma)\sigma \in R[G]. \qquad \textbf{[1]}$$

Note that if $a \in T$, $\pi_\varepsilon a = 0$ or $\deg(\pi_\varepsilon a) = \deg(a)$. It follows that if $\pi_\varepsilon(a) \neq 0$,

$$M(\pi_\varepsilon t(a)) = M(t(a)). \qquad \textbf{[2]}$$

Now, let $f_i = t(y_i^N)$, $g_{ij} = t(y_i^{N+j})$ and k_l, $1 \leq l \leq m$, be elements in $\mathbf{F}[\{a_h, b_i, c_{j\ k}\}_{h \in H, 1 \leq i,j \leq s, 0 < k < N}]$ which generate the ideal consisting of f such that

$$f(t(h), f_i, g_{jk}) = 0.$$

Let K_l be a lifting of k_l to $R[\{a_h, b_i, c_{ij}\}_{h \in H, 1 \leq i,j \leq s, 0 < k < N}]$. Then the equations

$$K_l(a_h, b_i, c_{jk}) = 0,$$

determine an affine scheme χ which lifts $\overline{X}$ and so there is an isomorphism from $X^\dagger$ to its weak completion such that the pullbacks of a_h, b_i, and c_{ij} are liftings of $t(h)$, $t(y_i^N)$ and $t(y_i^{N+j})$. For $u \in T$ call the lifting of $t(u)$ in $X^\dagger$ made by taking the appropriate product of these pullbacks $\tilde{t}(u)$. Let $V = \{\tilde{t}(u): u \in H \text{ or } u = f_i^{N+j}, 1 \leq i \leq s, 0 \leq j < N\}$. Let $U_{ir} = U_i \cap X_r$.

Lemma 4.1. *If r is close enough to 1, $r < 1$, and $J \in V$, $r^{M(\bar{J})}|J|U_{ir}$ equals 1 if $i \in m(\bar{J})$ and is strictly less than 1 otherwise. Moreover, if $i \in m(\bar{J})$,*

$$|r^{M(\bar{J})}J - c_i(\bar{J})(r/z_i)^{M(\bar{J})}|U_{ir} < 1.$$

It follows that if r is close to 1 and $J \in V$ that $|J|_{Xr} = r^{-M(\bar{J})}$ and, in particular, if $|\mathrm{a}| = r$,

$$A(X_r) \cong K\langle\{a^{M(h)}a_h, a^{M(f_i)}b_i, a^{M(g_{jk})}c_{jk}\}\rangle/(\{K_l(a_h, b_i, c_{jk})\}).$$

Proposition 4.2. *For r close enough to 1, $r \leq 1$, the R-algebra $A^0(X_r)$ is the completion of the subalgebra generated over R by the elements $\{a^{M(J)}J: J \in V\}$ and if $r < 1$ its reduction, $\overline{A}(X_r)$ is G-isomorphic to B.*

Proof: This proposition is immediate when $r = 1$ so suppose $r < 1$. Let C be the above complete subalgebra. We know, for r close to 1, $C \otimes \mathbf{Q}_p = A(X_r)$ so by lemma 3.11 of ref. 5 we only have to prove: (*i*) for all $f \in C$, there exists a $c \in R$ such that $f/c \in C - mC$, (*ii*) $A^0(X_r)$ is integral over C and (*iii*) C/mC is reduced. Now, (*i*) follows after making a finite extension if necessary, (*ii*) follows from proposition 6.3.4/1 of ref. 7, and the above description of $A(X_r)$ and finally, (*iii*) (as well as the second part of the proposition) will follow, once we exhibit a G-isomorphism $C/mC \to B$.

To see the latter, first note that elements in $A^0(U_{ir})$ may be written in the form $\Sigma_{-\infty}^{\infty} a_n z_i^n$ where $a_n \in R$ and $|a_n|r^n \to 0$ as $|n| \to \infty$ and so $\overline{A}(U_{ir})$ is isomorphic to $\mathbf{F}((z_i))$. If we map C in to $\oplus_\mathrm{i} \mathrm{A}^0(U_{ir})$ and then reduce we get, after mapping the reduction of $z_i$toy$_i$, a homomorphism

$$C/mC \to \oplus\, \mathbf{F}((y_i)).$$

Using the previous lemma, we see that for r close to 1, this factors through a surjection onto B which is a G-homomorphism by construction.

Now we produce the inverse to this homomorphism. For $J \in V$, let $J_a = a^{M(\bar{J})}J$. Consider the correspondence $\lambda(\bar{J}) \mapsto J_a$ mod mC from $\overline{V}$ to V mod mC. It suffices to show that for r sufficiently close to 1 this extends to an R-algebra homomorphism $B \to C/mC$. Let Y_m be the subset of B consisting of elements of the form $\Pi_{f \in \overline{V}} f^{n(f)}$ such that $\Sigma_{f \in \overline{V}} n(f)M(f) = m$ and let $Y = \cup_m Y_m$. If $z \in Y_m$ we will say $\deg(z) = m$. Then $\mathcal{I}$ is generated by a finite set of relations of the form

$$\sum_{y \in Y_m} a_y\lambda(y) = 0.$$

(These relations may include single monomial relations.) For each relation of this form, there must be a relation of the form

$$\sum_{y \in Y_m} a_y y + \sum_{\substack{z \in Y \\ \deg(z) < m}} b_z z = 0,$$

on $\mathbf{F}(\overline{X})$. If $\tilde{a}_y$ and $\tilde{b}_y$ are liftings of the coefficients and $\tilde{y}$ and $\tilde{z}$ are the liftings of the monomials y and z obtained by lifting $t(u)$ to $\tilde{t}(u)$ for $u \in T$. Then, because χ lifts X, there must be a relation of the form

$$\sum_{y \in Y_m} \tilde{a}_y\tilde{y} + \sum_{\substack{z \in Y \\ \deg(z) < m}} \tilde{b}_z\tilde{z} = \alpha h,$$

where h is a polynomial in $\{v \in V\}$ with coefficients in R and $\alpha \in R$, $|\alpha| < 1$. It follows that

$$\sum_{y \in Y_m} A_y r^m\tilde{y} + \sum_{\substack{z \in Y \\ \deg(z) < m}} r^{m-\deg(z)}B_m r^{\deg(z)}\tilde{z} = r^m\alpha h.$$

Since $r^n\tilde{u}$ for $u \in V_n$ is a product of elements of the form J_a for $J \in V$ and $r^m\alpha h$ is in mC for r close to one, since h is a polynomial, we see that for r close to 1 we have a homomorphism from B onto C/mC which takes $\lambda(\bar{J})$ to J_a as desired.

For a character $\varepsilon \in Hom(G, R^*)$ and an R module M on which G acts, set $M(\varepsilon) = \pi_\varepsilon M$.

Corollary 4.2.1. *Let r be as in the proposition and suppose $|a| = r$. Then the set*

$$\{a^{M(u)}\tilde{t}(u):\ u \in T\},$$

is an orthonormal basis for $A(X_r)$. Moreover, if $\varepsilon \in \mathrm{Hom}(G, R^*)$ and $S \subset T$ is such that $\{\pi_\varepsilon(s): s \in S\}$ is a basis for $B(\varepsilon)$, then

$$\{a^{M(s)}\pi_\varepsilon(\tilde{t}(s)):\ s \in S\},$$

is an orthonormal basis for $A(X_r)(\varepsilon)$.

5. End of Proof

Fix a positive integer N prime to p. Let X be connected component of the ordinary locus of $X_1(N\mathbf{q})$ containing the cusp ∞ and U be the operator on $A^\dagger(X_{\mathcal{B}}/\mathcal{B})$,

$$U(f) = U_{(0)}(\mathbf{E}_p f),$$

where $U_{(0)}$ is the weight zero U-operator, which is an operator on $A(X)^\dagger$. This is the analytic continuation of the operator with the same name in remark B4.2 of ref. 1. We have a natural action of $(\mathbf{Z}/p\mathbf{Z})^*$ on $X_1(N\mathbf{q})$ via diamond operators. (Note that this is intentionally trivial when $p = 2$, unfortunately.)

Let D be a disk around zero contained in $\mathcal{B}$ and Y a strict affinoid neighborhood of X stable under the action of $(\mathbf{Z}/p\mathbf{Z})^*$ such that $\mathbf{E}_p$ converges on Y_D. (This exists, by Corollary 2.1.1.) Let ε: $(\mathbf{Z}/p\mathbf{Z})^* \to \mathbf{Z}_p^*$ be a character. By Corollary 4.2.1 (and the properties of $U_{(0)}$), we may suppose we have an orthonormal basis B of $A^0(X)(\varepsilon)$ over K^0 (we allow K to be as large as necessary and then eliminate this choice later) satisfies the hypotheses of Proposition 3.1, with $A = K$, $L = K^0$, $N = A^0(X)(\varepsilon)$ and $P = A(Y)(\varepsilon)$. It follows that $\{1 \otimes b{:}b \in B\}$ is an orthonormal basis for $A^0(X_D)(\varepsilon)$ over $A^0(D)$ which also satisfying these hypotheses with $N = A^0(X_D)(\varepsilon)$ and $P = A(Y_D)(\varepsilon)$. We conclude from Proposition 3.1 that the characteristic series of U acting on $A(Y_D)(\varepsilon)$, which is the series labeled $P_\varepsilon(s, T)$ in section B3 of ref. 1 when $p \neq 2$ and is the series labeled there $P_N(s, T)$ when $p = 2$, lies in $A^0_K(D)[[T]]$. Since this is true for all D, we see that it lies in $A^0_{\mathbf{C}_p}(\mathcal{B})[[T]]$. However, we know, *a priori* (using arguments as in the proof of theorem B3.2 of ref. 1, that it lies in $\mathbf{Q}_p[[S, T]]$. Hence,

THEOREM 5.1. (i) *If* p *is odd the characteristic series of* U *acting on* $\mathrm{A}(\mathrm{X}_{\mathcal{W}})^\dagger$ *over* A(W), $\mathrm{Q_N(T)}$ (*see lemma B3.7 of ref. 1*), *lies in* Λ[[T]] *and converges on* W × $\mathbf{C}_\mathrm{p}$. (*ii*) *If p = 2, the characteristic series of* U *acting on* $\mathrm{A}(\mathrm{X}_{\mathcal{B}})^\dagger$ *over* $\mathrm{A}(\mathcal{B})$, $\mathrm{P_N(s, T)}$, *lies in* Λ[[T]] *and converges on* $\mathcal{B} \times \mathbf{C}_\mathrm{p}$.

In fact, if we were only worrying about modular forms on $\Gamma_0(N)$ (i.e., without character), we could have used a Katz basis (see section 2.6 of ref. 6). Indeed, suppose, for now, $p \geq 5$. Let $\{b_{a,1} \ldots, b_{a,n_i}\}$ be a $\mathbf{Z}_p$ basis for $B(N, 0, a)$. Then we have an orthonormal basis for $\mathrm{A(X_r) = S(K, r, N, 0)}$

$$\left\{\frac{r^a b_{a,i}}{E^a_{p-1}}{:}a \geq 0{,}1 \leq i \leq n_i\right\},$$

for all $r \in R$, $r \neq 0$. This is good enough to apply the results of section 3 in this case.

6. Higher Level

In this section, I prove theorem B6.2 of ref. 1 when p is odd. That is, I prove,

THEOREM 6.1. *Suppose p is odd. If $\kappa(x) = \chi(x)\langle\langle x\rangle\rangle^k$ where k is an integer, $\chi{:}\mathbf{Z}^*_p \to \mathbf{C}^*_p$ is a character of finite order and $p^n = LCM(p, f_\chi)$, then $\kappa(Q_N)(T)$ is the characteristic series of the U-operator acting on overconvergent modular forms of level N pn, weight k, and character χ.*

Proof: The proof of this is very simple, given what we now know. Let α be the character on $\mathbf{Z}^*_p, x \mapsto \kappa(\langle\langle x\rangle\rangle)$ and $\psi = \kappa/\alpha$. Then $\psi = \tau^i$ for some i. If $M(N\,p^n, k, \chi)$ denotes the Banach space of overconvergent modular forms of level Np^n, weight k and character χ (of some fixed yet to be determined radius), then, the map

$$F \mapsto F/E_\alpha,$$

is an isomorphism from $M(N\,p^n, k, \chi)$ onto the Banach space $M(N\,p, 0, \psi)$ and thus the characteristic series of U on $M(Np^n, k, \chi)$ is the characteristic series of the operator $G \mapsto U_{(0)}((E_\alpha(q)/E_\alpha(q^p))G)$ acting on $M(N\,p, 0, \psi)$. Since $\alpha(\mathbf{E}_p(q)) = E_\alpha(q)/E_\alpha(q^p)$, the theorem follows. ■

1. Coleman, R., *Inventiones*, **127,** 417–479.
2. Coleman, R. (1985) *Ann. Math*. **121,** 111–168.
3. Fresnel, J. (1984) *Astérisque* **119-120,** 140–150 (appendix).
4. Coleman, R. (1989) *Compositio* **72,** 205–235.
5. Coleman, R. & McCallum, W. (1988) *J. Reine Angew. Math.* **385,** 41–101.
6. Katz, N. (1972) *Springer Lecture Notes* **350,** 69–190.
7. Bosch, S., Guntzer, U. & Remmert, R. (1984) *Non-Archimedean Analysis* (Springer, New York).

Proc. Natl. Acad. Sci. USA
Vol. 94, pp. 11133–11137, October 1997
Colloquium Paper

This paper was presented at a colloquium entitled "Elliptic Curves and Modular Forms," organized by Barry Mazur and Karl Rubin, held March 15–17, 1996, at the National Academy of Sciences in Washington, DC.

Zeta functions and Eisenstein series on classical groups

GORO SHIMURA

Department of Mathematics, Fine Hall, Princeton University, Princeton, NJ 08544

ABSTRACT We construct an Euler product from the Hecke eigenvalues of an automorphic form on a classical group and prove its analytic continuation to the whole complex plane when the group is a unitary group over a CM field and the eigenform is holomorphic. We also prove analytic continuation of an Eisenstein series on another unitary group, containing the group just mentioned defined with such an eigenform. As an application of our methods, we prove an explicit class number formula for a totally definite hermitian form over a CM field.

Section 1. Given a reductive algebraic group G over an algebraic number field, we denote by G_{A}, G_{a}, and G_{h} its adelization, the archimedean factor of G_{A}, and the nonarchimedean factor of G_{A}. We take an open subgroup D of G_{A} of the form $D = D_0G_{\mathrm{a}}$ with a compact subgroup D_0 such that $D_0 \cap G_{\mathrm{a}}$ is maximal compact in G_{a}. Choosing a specific type of representation of $D_0 \cap G_{\mathrm{a}}$, we can define automorphic forms on G_{A} as usual. For simplicity we consider here the forms invariant under $D_0 \cap G_{\mathrm{h}}$. Each Hecke operator is given by $D\tau D$, with τ in a subset $\mathfrak{X}$ of G_{A}, which is a semigroup containing D and the localizations of G for almost all nonarchimedean primes. Taking an automorphic form $\mathbf{f}$ such that $\mathbf{f}|D\tau D = \lambda(\tau)\mathbf{f}$ with a complex number $\lambda(\tau)$ for every $\tau \in \mathfrak{X}$ and a Hecke ideal character χ of F, we put

$$\mathfrak{T}(s, \mathbf{f}, \chi) = \sum_{\tau \in D\backslash\mathfrak{X}/D} \lambda(\tau)\chi(\nu_0(\tau))N(\nu_0(\tau))^{-s}, \qquad \textbf{[1.1]}$$

where $\nu_0(\tau)$ is the denominator ideal of τ and $N(\nu_0(\tau))$ is its norm. Now our first main result is that if G is symplectic, orthogonal, or unitary, then

$$\Lambda(s, \chi)\mathfrak{T}(s, \mathbf{f}, \chi) = \prod_{\mathfrak{p}} W_{\mathfrak{p}}[\chi(\mathfrak{p})N(\mathfrak{p})^{-s}]^{-1}, \qquad \textbf{[1.2]}$$

where $\Lambda(s, \chi)$ is an explicitly determined product of L-functions depending on χ, $W_{\mathfrak{p}}$ is a polynomial determined for each $v \in \mathbf{h}$ whose constant term is 1, and $\mathfrak{p}$ runs over all the prime ideals of the basic number field. This is a purely algebraic result concerning only nonarchimedean primes.

Let $Z(s, \mathbf{f}, \chi)$ denote the right-hand side of Eq. **1.2**. As our second main result, we obtain a product $\mathfrak{G}(s)$ of gamma factors such that $\mathfrak{G}Z$ can be continued to the whole s-plane as a meromorphic function with finitely many poles, when G is a unitary group of an arbitrary signature distribution over a CM field, and $\mathbf{f}$ corresponds to holomorphic forms.

Now these problems are closely connected with the theory of Eisenstein series E on a group G' in which G is embedded. To describe the series, let $\mathfrak{Z}'$ denote the symmetric space on which G' acts. Then the series as a function of $(z, s) \in \mathfrak{Z}' \times \mathbf{C}$ can be given (in the classical style) in the form

$$E(z, s; \mathbf{f}, \chi) = \sum_{\alpha \in A} \delta(z, s, \mathbf{f}, \chi)\|\alpha, \quad A = (P \cap \Gamma)\backslash\Gamma, \qquad \textbf{[1.3]}$$

where Γ is a congruence subgroup of G', and P is a parabolic subgroup of G' which is a semidirect product of a unipotent group and $G \times GL_m$ with some m. The adelized version of δ will be explicitly described in Section 5. Now our third main result is that there exists an explicit product $\mathfrak{G}'$ of gamma factors and an explicit product Λ' of L-functions such that $\mathfrak{G}'(s)\Lambda'(s)Z(s, \mathbf{f}, \chi)E(z, s; \mathbf{f}, \chi)$ can be continued to the whole s-plane as a meromorphic function with finitely many poles.

Though the above results concern holomorphic forms, our method is applicable to the unitary group of a totally definite hermitian form over a CM field. In this case, we can give an explicit class number formula for such a hermitian form, which is the fourth main result of this paper.

Section 2. For an associative ring R with identity element, we denote by $R^{\times}$ the group of all its invertible elements and by R_n^m the R-module of all $m \times n$ matrices with entries in R. To indicate that a union $X = \cup_{i \in I} Y_i$ is disjoint, we write $X = \sqcup_{i \in I} Y_i$.

Let K be an associative ring with identity element and an involution ρ. For a matrix x with entries in K, we put $x^* = {}^tx^{\rho}$, and $\hat{x} = (x^*)^{-1}$ if x is square and invertible. Given a finitely generated left K-module V, we denote by $GL(V)$ the group of all K-linear automorphisms of V. We let $GL(V)$ act on V on the right; namely we denote by $w\alpha$ the image of $w \in V$ under $\alpha \in GL(V)$. Given $\varepsilon = \pm 1$, by an ε-hermitian form on V, we understand a biadditive map $\varphi: V \times V \rightarrow K$ such that $\varphi(x, y)^{\rho} = \varepsilon\varphi(y, x)$ and $\varphi(ax, by) = a\varphi(x, y)b^{\rho}$ for every $a, b \in K$. Assuming that φ is nondegenerate, we put

$$G^{\varphi} = G(\varphi) = G(V, \varphi) = \{\gamma \in GL(V) | \varphi(x\gamma, y\gamma) = \varphi(x, y)\}. \qquad \textbf{[2.1]}$$

Given (V, φ) and (W, ψ), we can define an ε-hermitian form $\varphi \oplus \psi$ on $V \oplus W$ by

$$(\varphi \oplus \psi)(x + y, x' + y') = \varphi(x, x') + \psi(y, y')$$
$$(x, x' \in V; y, y' \in W). \qquad \textbf{[2.2]}$$

We then write $(V \oplus W, \varphi \oplus \psi) = (V, \varphi) \oplus (W, \psi)$. If both φ and ψ are nondegenerate, we can view $G^{\varphi} \times G^{\psi}$ as a subgroup of $G^{\varphi \oplus \psi}$. The element (α, β) of $G^{\varphi} \times G^{\psi}$ viewed as an element of $G^{\varphi \oplus \psi}$ will be denoted by $\alpha \times \beta$ or by (α, β). Given a positive integer r, we put $H_r = I_r' \oplus I_r$, $I_r = I_r' = K_r^1$ and

$$\eta_r(x + u, y + v) = u \cdot {}^ty^{\rho} + \varepsilon x \cdot {}^tv^{\rho} \quad (x, y \in I_r'; u, v \in I_r). \qquad \textbf{[2.3]}$$

We shall always use H_r, I_r', I_r, and η_r in this sense. We understand that $H_0 = \{0\}$ and $\eta_0 = 0$.

Hereafter we fix V and a nondegenerate φ on V, assuming that K is a division ring whose characteristic is different from 2. Let J be a K-submodule of V which is totally φ-isotropic, by which we mean that $\varphi(J, J) = 0$. Then we can find a decomposition $(V, \varphi) = (Z, \zeta) \oplus (H, \eta)$ and an isomorphism f of $(H,$

η) onto (H_r, η_r) such that $f(J) = I_r$. In this setting, we define the parabolic subgroup P_J^φ of G^φ relative to J by

$$P_J^\varphi = \{\pi \in G^\varphi | J\pi = J\}, \qquad \textbf{[2.4]}$$

and define homomorphisms $\pi_\zeta^\varphi : P_J^\varphi \to G^\zeta$ and $\lambda_J^\varphi : P_J^\varphi \to GL(J)$ such that $z\alpha - z\pi_\zeta^\varphi(\alpha) \in J$ and $w\alpha = w\lambda_J^\varphi(\alpha)$ if $z \in Z$, $w \in J$, and $\alpha \in P_J^\varphi$.

Taking a fixed nonnegative integer m, we put

$$(W, \psi) = (V, \varphi) \oplus (H_m, \eta_m), \quad (X, \omega) = (W, \psi) \oplus (V, -\varphi). \qquad \textbf{[2.5]}$$

We can naturally view $G^\psi \times G^\varphi$ as a subgroup of G^ω. Since $W = V \oplus H_m$, we can put $X = V \oplus H_m \oplus V$ with the first summand V in W, and write every element of X in the form (u, h, v) with $(u, h) \in V \oplus H_m = W$ and $v \in V$. Put

$$U = \{(v, i, v) | v \in V, i \in I_m\}.$$

Observing that U is totally ω-isotropic, we can define P_U^ω.

PROPOSITION 1. *Let $\lambda(\varphi)$ be the maximum dimension of totally φ-isotropic K-submodules of V. Then*

$$P_U^\omega \backslash G^\omega / [G^\psi \times G^\varphi] \qquad \textbf{[2.6]}$$

has exactly $\lambda(\varphi)$ orbits. Moreover,

$$P_U^\omega [G^\psi \times G^\varphi] = \sqcup_{\beta,\xi} P_U^\omega((\xi \times 1_H)\beta, 1_V), \qquad \textbf{[2.7]}$$

with ξ running over G^φ and β over $P_I^\psi G^\psi$, where $H = H_m$ and $I = I_m$.

In fact, we can give an explicit set of representatives $\{\tau_e\}_{e=1}^{\lambda(\varphi)}$ for Eq. **2.6** and also an explicit set of representatives for $P_U^\omega \backslash P_U^\omega \tau_e [G^\psi \times G^\varphi]$ in the same manner as in Eq. **2.7**. This proposition plays an essential role in the analysis of our Eisenstein series $E(z, s; \mathbf{f}, \chi)$.

Section 3. In this section, K is a locally compact field of characteristic 0 with respect to a discrete valuation. Our aim is to establish the Euler factor $W_\mathfrak{p}$ of Eq. **1.2**. We denote by $\mathfrak{r}$ and $\mathfrak{q}$ the valuation ring and its maximal ideal; we put $q = [\mathfrak{r}:\mathfrak{q}]$ and $|x| = q^{-\nu}$ if $x \in K$ and $x \in \pi^\nu \mathfrak{r}^\times$ with $\nu \in \mathbf{Z}$. We assume that K has an automorphism ρ such that $\rho^2 = 1$, and put $F = \{x \in K \mid x^\rho = x\}$, $\mathfrak{g} = F \cap \mathfrak{r}$, and $\mathfrak{d}^{-1} = \{x \in K \mid \mathrm{Tr}_{K/F}(x\mathfrak{r}) \subset \mathfrak{g}\}$ if $K \neq F$. We consider (V, φ) as in Section 2 with $V = K_n^1$ and φ defined by $\varphi(x, y) = x\varphi y^*$ for $x, y \in V$ with a matrix φ of the form

$$\varphi = \begin{bmatrix} 0 & 0 & \varepsilon\delta^{-\rho}1_r \\ 0 & \theta & 0 \\ \delta^{-1}1_r & 0 & 0 \end{bmatrix}, \ \theta = \varepsilon\theta^* \in GL_t(K), \ \delta \in K^\times, \qquad \textbf{[3.1]}$$

where $t = n - 2r$. We assume that θ is anisotropic and also that

$$\varepsilon = \pm 1 \text{ and } \delta = 2 \text{ if } K = F, \qquad \textbf{[3.2a]}$$

$$\varepsilon = 1, \ \delta\mathfrak{r} = \mathfrak{d}, \text{ and } \delta^\rho = -\delta \text{ if } K \neq F. \qquad \textbf{[3.2b]}$$

Thus our group G^φ is orthogonal, symplectic, or unitary. The element δ of Eq. **3.2b** can be obtained by putting $\delta = u - u^\rho$ with u such that $\mathfrak{r} = \mathfrak{g}[u]$. We include the case $rt = 0$ in our discussion. If $t = 0$, we simply ignore θ; this is always so if $K = F$ and $\varepsilon = -1$. We have $\varphi = \theta$ if $r = 0$.

Denoting by $\{e_i\}$ the standard basis of K_n^1, we put

$$J = \sum_{i=1}^{r} Ke_{r+t+i}, \ T = \sum_{i=1}^{t} Ke_{r+i},$$

$$M = \sum_{i=1}^{r} (\mathfrak{r}e_i + \mathfrak{r}e_{r+t+i}) + N, \ N = \{u \in T | \varphi(u, u) \in \mathfrak{g}\},$$

$$C = \{\gamma \in G^\varphi | M\gamma = M\}, \ E = GL_r(\mathfrak{r}).$$

Then $G^\varphi = P_J^\varphi C$. We choose $\{e_{r+i}\}_{i=1}^t$ so that $N = \Sigma_{i=1}^t \mathfrak{r}e_{r+i}$. Then we can find an element λ of $\mathfrak{r}_t^t$ such that

$$\theta = \delta^{-1}\lambda + \varepsilon(\delta^{-1}\lambda)^*. \qquad \textbf{[3.3]}$$

Put

$$S = S^r = \{h \in K_r^r | h^* = -\varepsilon(\delta^\rho/\delta)h\}. \qquad \textbf{[3.4]}$$

We can write every element of P_J^φ in the form

$$\xi = \begin{bmatrix} a & b & c \\ 0 & e & f \\ 0 & 0 & d \end{bmatrix}, \ \hat{a} = d \in GL_r(K), \ e \in G^\theta,$$

$$b \in K_t^r, f = -\delta e\theta b^* d, c = (s - b\lambda b^*)d, s \in S. \qquad \textbf{[3.5]}$$

If $t = 0$, we simply ignore b, e, and f, so that $\xi = \begin{bmatrix} a & sd \\ 0 & d \end{bmatrix}$; we have $\xi = e$ if $r = 0$.

We consider the Hecke algebra $\mathfrak{R}(E, GL_r(K))$ consisting of all formal finite sums $\Sigma c_x ExE$ with $c_x \in \mathbf{Q}$ and $x \in GL_r(K)$, with the law of multiplication defined as in ref. 1. Taking r indeterminates $t_1, \ldots, t_r$, we define a $\mathbf{Q}$-linear map

$$\omega_0 : \mathfrak{R}(E, GL_r(K)) \to \mathbf{Q}[t_1, \ldots, t_r, t_1^{-1}, \ldots, t_r^{-1}] \qquad \textbf{[3.6]}$$

as follows; given ExE with $x \in GL_r(K)$, we can put $ExE = \sqcup_y Ey$ with upper triangular y whose diagonal entries are $\pi^{e_1}, \ldots, \pi^{e_r}$ with $e_i \in \mathbf{Z}$. Then we put

$$\omega_0(ExE) = \sum_y \omega_0(Ey), \quad \omega_0(Ey) = \prod_{i=1}^{r} (q^{-i}t_i)^{e_i}. \qquad \textbf{[3.7]}$$

Next we consider the Hecke algebra $\mathfrak{R}(C, G^\varphi)$ consisting of all formal finite sums $\Sigma c_\tau C\tau C$ with $c_\tau \in \mathbf{Q}$ and $\tau \in G^\varphi$. We then define a $\mathbf{Q}$-linear map

$$\omega : \mathfrak{R}(C, G^\varphi) \to \mathbf{Q}[t_1, \ldots, t_r, t_1^{-1}, t. \ldots, t_r^{-1}] \qquad \textbf{[3.8]}$$

as follows; given $C\tau C$ with $\tau \in G^\varphi$, we can put $C\tau C = \sqcup_\xi C\xi$ with $\xi \in P$ of form Eq. **3.5**. We then put

$$\omega(C\tau C) = \sum_\xi \omega(C\xi), \quad \omega(C\xi) = \omega_0(Ed_\xi), \qquad \textbf{[3.9]}$$

where ω_0 is given by Eq. **3.6** and d_ξ is the d-block in Eq. **3.5**. We can prove that this is well defined and gives a ring-injection.

Given $x \in K_n^m$, we denote by $\nu_0(x)$ the ideal of $\mathfrak{r}$ which is the inverse of the product of all the elementary divisor ideals of x not contained in $\mathfrak{r}$; we put then $\nu(x) = [\mathfrak{r}:\nu_0(x)]$. We call x primitive if $\mathrm{rank}(x) = \mathrm{Min}(m, n)$ and all the elementary divisor ideals of x are $\mathfrak{r}$.

PROPOSITION 2. *Given ξ as in Eq.* **3.5**, *suppose that both e and $(\delta\theta)^{-1}(e - 1)$ have coefficients in $\mathfrak{r}$ if $t > 0$. Let $a = g^{-1}h$ with primitive $[g\ h] \in \mathfrak{r}_{2r}^r$ and $gb = j^{-1}k$ with primitive $[j\ k] \in \mathfrak{r}_{r+t}^r$. Then*

$$\nu_0((\delta\varphi)^{-1}(\xi - 1)) = \det(ghj^2)\nu_0(jgsg^*j^*),$$

where we take $j = 1_r$ if $t = 0$.

We now define a formal Dirichlet series $\mathfrak{T}$ by

$$\mathfrak{T}(s) = \sum_{\tau \in A} \omega(C\tau C)\nu(\tau)^{-s}, \quad A = C\backslash G^\varphi/C. \qquad \textbf{[3.10]}$$

This is a formal version of the Euler factor of Eq. **1.2** at a fixed nonarchimedean prime.

THEOREM 1. *Suppose that $\delta\varphi \in GL_n(\mathfrak{r})$; put $p = [\mathfrak{g}:\mathfrak{g} \cap \mathfrak{q}]$. (Thus $p = q$ if $K = F$.) Then*

$$\mathfrak{T}(s) = \frac{1 - p^{-s}}{1 - p^{r-s}} \prod_{i=1}^{r} \frac{(1 - p^{2i-2s})}{(1 - p^{r-s}t_i)(1 - p^{r-s}t_i^{-1})}$$

$$(K = F,\ \varepsilon = -1),$$

$$\mathfrak{T}(s) = \prod_{i=1}^{r} \frac{(1 - p^{2i-2-2s})}{(1 - p^{r+t-2-s}t_i)(1 - p^{r-s}t_i^{-1})} \quad (K = F,\ \varepsilon = 1),$$

$$\mathfrak{T}(s) = \frac{\prod_{i=1}^{2r} (1 - \theta^{i-1}p^{i-1-2s})}{\prod_{i=1}^{r} (1 - q^{r+t-1-s}t_i)(1 - q^{r-s}t_i^{-1})} \quad (K \neq F).$$

Here $\theta^i = 1$ if i is even; when i is odd, θ^i is -1 or 0 according as $\mathfrak{d} = \mathfrak{r}$ or $\mathfrak{d} \neq \mathfrak{r}$.

This can be proved in the same manner as in ref. 2 by means of *Proposition 2*.

Since we are going to take localizations of a global unitary group, we have to consider $G^\varphi = G(V, \varphi)$ of Eq. **2.1** with $V = K_n^1$, $K = F \times F$, and ρ defined by $(x, y)^\rho = (y, x)$, where F is a locally compact field of characteristic 0 with respect to a discrete valuation. Let $\mathfrak{g}$ and $\mathfrak{p}$ be the valution ring of F and its maximal ideal; put $\mathfrak{r} = \mathfrak{g} \times \mathfrak{g}$ and $p = [\mathfrak{g}:\mathfrak{p}]$. We consider $\mathfrak{R}(C, G^\varphi)$ with $C = G^\varphi \cap GL_n(\mathfrak{r})$. Then the projection map pr of $GL_n(K)$ onto $GL_n(F)$ gives an isomorphism $\eta:\mathfrak{R}(C, G^\varphi) \rightarrow \mathfrak{R}(E_1, GL_n(F))$, where $E_1 = GL_n(\mathfrak{g})$. To be explicit, we have $\eta(C(x, {}^t x^{-1})C) = E_1 x E_1$. Let ω_1 denote the map of Eq. **3.6** defined with n, E_1, and F in place of r, E, and K. Putting $\omega = \omega_1 \circ \eta$, we obtain a ring-injection

$$\omega:\mathfrak{R}(C, G^\varphi) \rightarrow \mathbf{Q}[t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1}]. \qquad \textbf{[3.11]}$$

For $z = (x, y) \in K_n^n$ with $x, y \in F_n^n$ put $\nu_1(z) = \nu(x)$ and $\nu_2(z) = \nu(y)$, where ν is defined with respect to $\mathfrak{g}$ instead of $\mathfrak{r}$. We then put

$$\mathfrak{T}(s, s') = \sum_{\tau \in R} \omega(C\tau C)\nu_1(\tau)^{-s}\nu_2(\tau)^{-s'}, \quad R = C\backslash G^\varphi/C. \qquad \textbf{[3.12]}$$

Then we obtain

$$\mathfrak{T}(s, s') = \prod_{i=1}^{n} \frac{1 - p^{i-1-s-s'}}{(1 - p^{n-s}t_i^{-1})(1 - p^{-1-s'}t_i)}. \qquad \textbf{[3.13]}$$

Section 4. We now take a totally imaginary quadratic extension K of a totally real algebraic number field F of finite degree. We denote by $\mathbf{a}$ (resp. $\mathbf{h}$) the set of archimedean (resp. nonarchimedean) primes of F; further we denote by $\mathfrak{g}$ (resp. $\mathfrak{r}$) the maximal order of F (resp. K). Let V be a vector space over K of dimension n. We take a K-valued nondegenerate ε-hermitian form φ on V with $\varepsilon = 1$ with respect to the Galois involution of K over F, and define G^φ as in Section 2. For every $v \in \mathbf{a} \cup \mathbf{h}$ and an object X, we denote by X_v its localization at v. For $v \in \mathbf{h}$ not splitting in K and for $v \in \mathbf{a}$, we take a decomposition

$$(V_v, \varphi_v) = (T_v, \theta'_v) \oplus (H_{r_v}, \eta_{r_v}) \qquad \textbf{[4.1]}$$

with anisotropic θ'_v and a nonnegative integer r_v. Put $t_v = \dim(T_v)$. Then $n = 2r_v + t_v$. If n is odd, then $t_v = 1$ for every $v \in \mathbf{h}$. If n is even, then $t_v = 0$ for almost all $v \in \mathbf{h}$ and $t_v = 2$ for the remaining $v \in \mathbf{h}$. If n is odd, by replacing φ by $c\varphi$ with a suitable $c \in F$, we may assume that φ is represented by a matrix whose determinant times $(-1)^{(n-1)/2}$ belongs to $N_{K/F}(K)$.

We take and fix an element κ of K such that $\kappa^\rho = -\kappa$ and $i\kappa_v\varphi_v$ has signature $(r_v + t_v, r_v)$ for every $v \in \mathbf{a}$. Then $G(i\kappa_v\varphi_v)$ modulo a maximal compact subgroup is a hermitian symmetric space which we denote by $\mathfrak{Z}_v^\varphi$. We take a suitable point $\mathbf{i}_v$ of $\mathfrak{Z}_v^\varphi$ which plays the role of "origin" of the space. If $r_v = 0$, we understand that $\mathfrak{Z}_v^\varphi$ consists of a single point $\mathbf{i}_v$. We put $\mathfrak{Z}^\varphi = \Pi_{v \in \mathbf{a}} \mathfrak{Z}_v^\varphi$. To simplify our notation, for $x \in K_{\mathbf{A}}^\times$ or $x \in (\mathbf{C}^\times)^{\mathbf{a}}$, $a \in \mathbf{Z}^{\mathbf{a}}$, and $c \in (\mathbf{C}^\times)^{\mathbf{a}}$, we put

$$x^a = \prod_{v \in \mathbf{a}} x_v^{a_v}, \quad |x|^c = \prod_{v \in \mathbf{a}} (x_v \bar{x}_v)^{c_v/2}. \qquad \textbf{[4.2]}$$

For $\xi \in G_v^\varphi$ and $w \in \mathfrak{Z}_v^\varphi$, we define $\xi w \in \mathfrak{Z}_v^\varphi$ in a natural way and define also a scalar factor of automorphy $j_\xi(w)$ so that $\det(\xi)^{r_v} j_\xi(w)^{-n}$ is the jacobian of ξ. Given k, $\nu \in \mathbf{Z}^{\mathbf{a}}$, $z \in \mathfrak{Z}^\varphi$, and $\alpha \in G_{\mathbf{A}}^\varphi$, we put

$$\alpha z = (\alpha_v z_v)_{v \in \mathbf{a}}, \quad j_\alpha^{k,\nu}(z) = \det(\alpha)^\nu j_\alpha(z)^k. \qquad \textbf{[4.3]}$$

Then, for a function $f:\mathfrak{Z}^\varphi \rightarrow \mathbf{C}$, we define $f\|_{k,\nu}\alpha:\mathfrak{Z}^\varphi \rightarrow \mathbf{C}$ by

$$(f\|_{k,\nu}\alpha)(z) = j_\alpha^{k,\nu}(z)^{-1} f(\alpha z) \qquad (z \in \mathfrak{Z}^\varphi). \qquad \textbf{[4.4]}$$

Now, given a congruence subgroup Γ of G^φ, we denote by $\mathfrak{M}_{k,\nu}^\varphi(\Gamma)$ the vector space of all holomorphic functions f on $\mathfrak{Z}^\varphi$ which satisfy $f\|_{k,\nu}\gamma = f$ for every $\gamma \in \Gamma$ and also the cusp condition if G^φ is of the elliptic modular type. We then denote by $\mathfrak{S}_{k,\nu}^\varphi(\Gamma)$ the set of all cusp forms belonging to $\mathfrak{M}_{k,\nu}^\varphi(\Gamma)$. Further, we denote by $\mathfrak{M}_{k,\nu}^\varphi$ resp. $\mathfrak{S}_{k,\nu}^\varphi$ the union of $\mathfrak{M}_{k,\nu}^\varphi(\Gamma)$ resp. $\mathfrak{S}_{k,\nu}^\varphi(\Gamma)$ for all congruence subgroups Γ of G. If φ is anisotropic, we understand that $\mathfrak{S}_{0,\nu}^\varphi = \mathbf{C}$.

Let D be an open subgroup of $G_{\mathbf{A}}^\varphi$ such that $D \cap G_{\mathbf{h}}^\varphi$ is compact. We then denote by $\mathfrak{S}_{k,\nu}^\varphi(D)$ the set of all functions $\mathbf{f}$: $G_{\mathbf{A}}^\varphi \rightarrow \mathbf{C}$ satisfying the following conditions:

$$\mathbf{f}(\alpha x w) = \mathbf{f}(x) \text{ if } \alpha \in G^\varphi \text{ and } w \in D \cap G_{\mathbf{h}}^\varphi; \qquad \textbf{[4.5]}$$

for every $p \in G_{\mathbf{h}}^\varphi$ there exists an element $f_p \in \mathfrak{S}_{k,\nu}^\varphi$ such that

$$\mathbf{f}(py) = (f_p\|_{k,\nu}y)(\mathbf{i}^\varphi) \text{ for every } y \in G_{\mathbf{a}}^\varphi, \text{ where } \mathbf{i}^\varphi = (\mathbf{i}_v)_{v \in \mathbf{a}}. \qquad \textbf{[4.6]}$$

We now take D in a special form. We take a maximal $\mathfrak{r}$-lattice M in V whose norm is $\mathfrak{g}$ in the sense of ref. 3 (p. 375) and put

$$C = \{\alpha \in G_{\mathbf{A}}^\varphi | M_v\alpha_v = M_v \text{ for every } v \in \mathbf{h}\}, \qquad \textbf{[4.7]}$$

$$\tilde{M} = \{x \in V | \varphi(x, M) \subset \mathfrak{d}^{-1}\}, \qquad \textbf{[4.8]}$$

$$D = D^\varphi = \{\gamma \in C | \tilde{M}_v(\gamma_v - 1) \subset \mathfrak{c}_v M_v \text{ for every } v \in \mathbf{h}\}, \qquad \textbf{[4.9]}$$

where $\mathfrak{d}$ is the different of K relative to F and $\mathfrak{c}$ is a fixed integral $\mathfrak{g}$-ideal. Clearly $\tilde{M}$ is an $\mathfrak{r}$-lattice in V containing M, and we easily see that D^φ is an open subgroup of $G_{\mathbf{A}}^\varphi$. We assume that

$$v|\mathfrak{c} \text{ if } \tilde{M}_v \neq M_v. \qquad \textbf{[4.10]}$$

Define a subgroup $\mathfrak{X}$ of $G_{\mathbf{A}}^\varphi$ by

$$\mathfrak{X} = \{y \in G_{\mathbf{A}}^\varphi | y_v \in D \text{ for every } v|\mathfrak{c}\}. \qquad \textbf{[4.11]}$$

We then consider the algebra $\mathfrak{R}(D, \mathfrak{X})$ consisting of all the finite linear combinations of $D\tau D$ with $\tau \in \mathfrak{X}$ and define its action on $\mathfrak{S}_{k,\nu}^\varphi(D)$ as follows. Given $\tau \in \mathfrak{X}$ and $\mathbf{f} \in \mathfrak{S}_{k,\nu}^\varphi(D)$, take a finite subset Y of $G_{\mathbf{h}}^\varphi$ so that $D\tau D = \sqcup_{\eta \in Y} D\eta$ and define $\mathbf{f}|D\tau D:G_{\mathbf{A}}^\varphi \rightarrow \mathbf{C}$ by

$$(\mathbf{f}|D\tau D)(x) = \sum_{\eta \in Y} \mathbf{f}(x\eta^{-1}) \quad (x \in G_{\mathbf{A}}^\varphi). \qquad \textbf{[4.12]}$$

These operators form a commutative ring of normal operators on $\mathfrak{S}^{\varphi}_{k,\nu}(D)$.

For $x \in G^{\varphi}_{\mathbf{A}}$, we define an ideal $\nu_0(x)$ of $\mathfrak{r}$ by

$$\nu_0(x) = \prod_{v\in\mathbf{h}} \nu_0(x_v), \qquad \mathbf{[4.13]}$$

where $\nu_0(x_v)$ is defined as in Section 3 with respect to an $\mathfrak{r}_v$-basis of M_v. Clearly $\nu_0(x)$ depends only on CxC.

Let $\mathbf{f}$ be an element of $\mathfrak{S}^{\varphi}_{k,\nu}(D)$ that is a common eigenfunction of all the $D\tau D$ with $\tau \in \mathfrak{X}$, and let $\mathbf{f}|D\tau D = \lambda(\tau)\mathbf{f}$ with $\lambda(\tau) \in \mathbf{C}$. Given a Hecke ideal character χ of K such that $|\chi| = 1$, define a Dirichlet series $\mathfrak{T}(s, \mathbf{f}, \chi)$ by

$$\mathfrak{T}(s,\mathbf{f},\chi) = \sum_{\tau\in D\backslash\mathfrak{X}/D} \lambda(\tau)\chi^*(\nu_0(\tau))N(\nu_0(\tau))^{-s}, \qquad \mathbf{[4.14]}$$

where χ^* is the ideal character associated with χ and $N(\mathfrak{a})$ is the norm of an ideal $\mathfrak{a}$. Denote by χ_1 the restriction of χ to $F^{\times}_{\mathbf{A}}$, and by θ the Hecke character of F corresponding to the quadratic extension K/F. For any Hecke character ξ of F, put

$$L_{\mathfrak{c}}(\mathrm{s}, \xi) = \prod_{\mathfrak{p}\nmid\mathfrak{c}} [1-\xi^*(\mathfrak{p})N(\mathfrak{p})^{-s}]^{-1}. \qquad \mathbf{[4.15]}$$

From *Theorem 1* and Eq. **3.13**, we see that

$$\mathfrak{T}(s, \mathbf{f}, \chi) \prod_{i=1}^{n} L_{\mathfrak{c}}(2s - i + 1, \chi_1\theta^{i-1})$$

$$= \prod_{\mathfrak{q}\nmid\mathfrak{c}} W_{\mathfrak{q}}[\chi^*(\mathfrak{q})N(\mathfrak{q})^{-s}]^{-1} \qquad \mathbf{[4.16]}$$

with a polynomial $W_{\mathfrak{q}}$ of degree n whose constant term is 1, where $\mathfrak{q}$ runs over all the prime ideals of K prime to $\mathfrak{c}$. Let $Z(s, \mathbf{f}, \chi)$ denote the function of Eq. **4.16**. Put

$$\Gamma_m(s) = \pi^{m(m-1)/2} \prod_{k=0}^{m-1} \Gamma(s - k). \qquad \mathbf{[4.17]}$$

THEOREM 2. *Suppose that* $\chi_{\mathbf{a}}(b) = b^{\mu}|b|^{i\kappa-\mu}$ *with* $\mu \in \mathbf{Z}^{\mathbf{a}}$ *and* $\kappa \in \mathbf{R}^{\mathbf{a}}$ *such that* $\Sigma_{v\in\mathbf{a}}\,\kappa_v = 0$. *Put* $m = k + 2\nu - \mu$ *and*

$$\mathfrak{R}(s, \mathbf{f}, \chi) = \prod_{v\in\mathbf{a}} \gamma_v(s + (i\kappa_v/2))\cdot Z(s, \mathbf{f}, \chi)$$

with γ_v *defined by*

$$\gamma_v(s) = p_v(s)q_v(s)\Gamma_{r_v}\left(s - n + r_v + \frac{k_v + |m_v|}{2}\right)$$

$$\cdot\,\Gamma_{n-r_v}\left(s - r_v + \frac{|\mu_v - 2\nu_v|}{2}\right),$$

$$p_v(s) = \begin{cases} \Gamma_{r_v}\left(s + \dfrac{|k_v - m_v|}{2}\right)\Gamma_{r_v}\left(s + \dfrac{k_v - m_v}{2}\right)^{-1} & \text{if } m_v \geq 0, \\ \Gamma_{r_v}\left(s - \dfrac{k_v + m_v}{2}\right)\Gamma_{r_v}\left(s - \dfrac{k_v - m_v}{2}\right)^{-1} & \text{if } m_v < 0, \end{cases}$$

$$q_v(s) = \prod_{i=1}^{n-\ell-1} \Gamma\left(s - \frac{\ell}{2} - \left[\frac{i}{2}\right]\right)$$

$$\cdot\,\Gamma\left(s - \frac{\ell}{2 - i}\right)^{-1}, \quad \ell = |\mu_v - 2\nu_v|.$$

Then $\mathfrak{R}(s, \mathbf{f}, \chi)$ *can be continued to the whole s-plane as a meromorphic function with finitely many poles, which are all simple. It is entire if* $\chi_1 \neq \theta^{\nu}$ *for* $\nu = 0, 1$.

We can give an explicitly defined finite set of points in which the possible poles of $\mathfrak{R}$ belong. Notice that p_v and q_v are polynomials; in particular, $p_v = 1$ if $0 \leq m_v \leq k_v$ and $q_v = 1$ if $|\mu_v - 2\nu_v| \geq n - 1$.

The results of the above type and also of the type of *Theorem 3* below were obtained in refs. 2, 4, and 5 for the forms on the symplectic and metaplectic groups over a totally real number field. The Euler product of type Z, its analytic continuation, and its relationship with the Fourier coefficients of $\mathbf{f}$ have been obtained by Oh (6) for the group G^{φ} as above when $\varphi = \eta_r$.

Section 5. We now put $(W, \psi) = (V, \varphi) \oplus (H_m, \eta_m)$ as in Eq. **2.5** with (V, φ) of Section 4 and $m \geq 0$. Writing simply $I = I_m$, we can consider the parabolic subgroup P^{ψ}_I of G^{ψ}. We put $P^{\psi} = P^{\psi}_I$ for simplicity, $\lambda_0(\alpha) = \det(\lambda^{\psi}_I(p))$ for $p \in P^{\psi}$, and

$$L = \sum_{i=1}^{m} (\mathfrak{r}\varepsilon_i + \mathfrak{d}^{-1}\varepsilon_{m+n+i}) + M, \qquad \mathbf{[5.1]}$$

with M of Section 4 and the standard basis $\{\varepsilon_i, \varepsilon_{m+n+i}\}^{m}_{i=1}$ of H_m. We can define the space $\mathfrak{Z}^{\psi}$ and its origin $\mathbf{i}^{\psi}$ in the same manner as for G^{φ}. We then put

$$C^{\psi} = \{x \in G^{\psi}_{\mathbf{A}}|Lx = L\}, \quad C^{\psi}_0 = \{x \in C^{\psi}|x(\mathbf{i}^{\psi}) = \mathbf{i}^{\psi}\}, \qquad \mathbf{[5.2]}$$

$$D^{\psi} = \{x \in C^{\psi}|\tilde{M}_v(e_v - 1) \subset \mathfrak{c}_v M_v \text{ for every } v \in \mathbf{h}\}. \qquad \mathbf{[5.3]}$$

Here e_v is the element of $\mathrm{End}(V_v)$ defined for x_v by $wx_v - we_v \in (H_m)_v$ for $w \in V_v$. We define an $\mathbf{R}$-valued function h on $G^{\psi}_{\mathbf{A}}$ by

$$h(x) = |\lambda_0(p)|_{\mathbf{A}} \text{ if } x \in pC^{\psi}_0 \text{ with } p \in P_{\mathbf{A}}. \qquad \mathbf{[5.4]}$$

Taking $\mathbf{f} \in \mathfrak{S}^{\varphi}_{k,\nu}(D^{\varphi})$ and χ as in Section 4, we define $\mu: G^{\psi}_{\mathbf{A}} \to \mathbf{C}$ as follows: $\mu(x) = 0$ if $x \notin P^{\psi}_{\mathbf{A}}D^{\psi}$; if $x = pw$ with $p \in P^{\psi}_{\mathbf{A}}$ and $w \in D^{\psi} \cap C^{\psi}_0$, then we put

$$\mu(x) = \chi(\lambda_0(p))^{-1}\chi_{\mathfrak{c}}(\lambda_0(w))^{-1}j^{k,\nu}_w(\mathbf{i}^{\psi})^{-1}\mathbf{f}(\pi^{\psi}_{\varphi}(p)), \qquad \mathbf{[5.5]}$$

where $\chi_{\mathfrak{c}} = \Pi_{v|\mathfrak{c}}\,\chi v$. Then we define $E(x, s)$ for $x \in G^{\psi}_{\mathbf{A}}$ and $s \in \mathbf{C}$ by

$$E(x, s) = E(x, s; \mathbf{f}, \chi, \mathrm{D}^{\psi}) = \sum_{\alpha\in A} \mu(\alpha x)h(\alpha x)^{-s},$$

$$A = P^{\psi}_I\backslash G^{\psi}. \qquad \mathbf{[5.6]}$$

This is meaningful if $\chi_{\mathbf{a}}(b) = b^{k+2\nu}|b|^{i\kappa-k-2\nu}$ with $\kappa \in \mathbf{R}^{\mathbf{a}}$, $\Sigma_{v\in\mathbf{a}}\,\kappa_v = 0$, and the conductor of χ divides $\mathfrak{c}$. We take such a χ in the following theorem. The series of Eq. **5.6** is the adelized version of a collection of several series of the type in Eq. **1.3**.

THEOREM 3. *Define* γ_v *as in* Theorem 2 *with* $m = 0$. *Put*

$$\gamma'_v(s) = q'(s,|k_v|)\gamma_v(s)q_v(s)^{-1}\Gamma_m(s - n + (k_v/2)),$$

$$q'(s, \ell) = \prod_{i=1}^{m+n-\ell-1} \Gamma\left(s - \frac{\ell}{2} - \left[\frac{i}{2}\right]\right)\Gamma\left(s - \frac{\ell}{2} - i\right)^{-1}.$$

Then the product

$$\prod_{v\in\mathbf{a}} \gamma'_v(s + (i\kappa_v/2)) \prod_{j=n}^{m+n-1} \cdot L_{\mathfrak{c}}(2s - j, \chi_1\theta^j)$$

$$\cdot Z(s, \mathbf{f}, \chi)E(x, s; \mathbf{f}, \chi, D^{\psi})$$

can be continued to the whole s-*plane as a meromorphic function with finitely many poles, which are all simple.*

We can give an explicitly defined finite set of points in which the possible poles of the above product belong.

Section 6. Let G be an arbitrary reductive algebraic group over $\mathbf{Q}$. Given an open subgroup U of $G_{\mathbf{A}}$ containing $G_{\mathbf{a}}$ and such that $U \cap G_{\mathbf{h}}$ is compact, we put $U^a = aUa^{-1}$ and $\Gamma^a = G \cap U^a$ for every $a \in G_{\mathbf{A}}$. We assume that $G_{\mathbf{a}}$ acts on a symmetric space $\mathfrak{W}$, and we let G act on $\mathfrak{W}$ via its projection to $G_{\mathbf{a}}$. We also assume that $\Gamma^a\backslash\mathfrak{W}$ has finite measure, written $\mathrm{vol}(\Gamma^a\backslash\mathfrak{W})$, with respect to a fixed $G_{\mathbf{a}}$-invariant measure on $\mathfrak{W}$. Taking a complete set of representatives $\mathfrak{B}$ for $G\backslash G_{\mathbf{A}}/U$, we put

$$\sigma(G, U) = \sigma(U) = \sum_{a\in\mathfrak{B}} [\Gamma^a \cap T{:}1]^{-1}\mathrm{vol}(\Gamma^a\backslash\mathfrak{W}), \qquad \textbf{[6.1]}$$

where T is the set of elements of G which act trivially on $\mathfrak{W}$, and we assume that $[\Gamma^a \cap T{:}1]$ is finite. Clearly $\sigma(U)$ does not depend on the choice of $\mathfrak{B}$. We call $\sigma(G, U)$ the mass of G with respect to U. If $G_{\mathbf{a}}$ is compact, we take $\mathfrak{W}$ to be a single point of measure 1 on which $G_{\mathbf{a}}$ acts trivially. Then we have

$$\sigma(G, U) = \sigma(U) = \sum_{a\in\mathfrak{B}} [\Gamma^{\mathrm{a}}{:}1]^{-1}. \qquad \textbf{[6.2]}$$

We can show that $\sigma(U') = [U{:}U']\sigma(U')$ if U' is a subgroup of U. If strong approximation holds for the semisimple factor of G, then it often happens that both $[\Gamma^a \cap T{:}1]$ and $\mathrm{vol}(\Gamma^a\backslash\mathfrak{W})$ depend only on U, so that

$$\sigma(G, U) = \sigma(U) = \#(G\backslash G_{\mathbf{A}}/U)[\Gamma^1 \cap T{:}1]^{-1}\mathrm{vol}(\Gamma^1\backslash\mathfrak{W}). \qquad \textbf{[6.3]}$$

If $G_{\mathbf{a}}$ is compact and U is sufficiently small, then $\Gamma^a = \{1\}$ for every a, in which case we have $\sigma(U) = \#(G\backslash G_{\mathbf{A}}/U)$. If U is the stabilizer of a lattice L in a vector space on which G acts, then $\#(G\backslash G_{\mathbf{A}}/U)$ is the number of classes in the genus of L. Therefore, $\sigma(U)$ may be viewed as a refined version of the class number in this sense.

Coming back to the unitary group G^φ of Section 4, we can prove the following theorem.

THEOREM 4. *Suppose that $G^\varphi_{\mathbf{a}}$ is compact. Let M be a $\mathfrak{g}$-maximal lattice in V of norm $\mathfrak{g}$ and let $\mathfrak{d}$ be the different of K relative to F. Define an open subgroup D of $G^\varphi_{\mathbf{A}}$ by Eq.* **4.9** *with an integral ideal $\mathfrak{c}$. If n is odd, assume that φ is represented by a matrix whose determinant times $(-1)^{(n-1)/2}$ belongs to $N_{K/F}(K)$; if n is even, assume that $\mathfrak{c}$ is divisible by the product $\mathfrak{e}$ of all prime ideals for which $t_v = 2$. Then*

$$\sigma(G^\varphi, D) = 2\cdot\left\{\prod_{k=1}^{n}(n-k)\right\}^d D_F^{(n^2-n)/2}N(\mathfrak{c})^{n^2}$$

$$\cdot A\prod_{k=1}^{n}\{N(\mathfrak{d})^{k/2}D_F^{1/2}(2\pi)^{-kd}L_{\mathfrak{c}}(k, \theta^k)\},$$

where $d = [F{:}\mathbf{Q}]$, D_F is the discriminant of F, and $A = 1$ or $A = N(\mathfrak{e})^nN(\mathfrak{d})^{-n/2}$ according as n is odd or even.

If n is odd, we can also consider $\sigma(D')$ for

$$D' = \{\gamma \in C | M_v(\gamma_v - 1) \subset \mathfrak{c}_vM_v \text{ for every } v \in \mathbf{h}\} \qquad \textbf{[6.4]}$$

with an arbitrary integral ideal $\mathfrak{c}$. Then $\sigma(D') = 2^{-\tau}\sigma(D)$, where τ is the number of primes in F ramified in K.

Section 7. Let us now sketch the proof of the above theorems. The full details will be given in ref. 7. We first take $\mathfrak{B} \subset G^\varphi_{\mathbf{h}}$ so that $G^\varphi_{\mathbf{A}} = \sqcup_{b\in\mathfrak{B}}G^\varphi bD^\varphi$. Given $E(x, s)$ as in Eq. **5.6**, for each $q \in G^\psi_{\mathbf{h}}$ we can define a function $E_q(z, s)$ of $(z, s) \in \mathfrak{Z}^\psi \times \mathbf{C}$ by

$$E(qy, s) = E_q(y(\mathbf{i}^\psi), s)j_y^{k,\nu}(\mathbf{i}^\psi)^{-1} \text{ for every } y \in G^\psi_{\mathbf{a}}. \qquad \textbf{[7.1]}$$

The principle is the same as in Eq. **4.6**, and so it is sufficient to prove the assertion of *Theorem 3* with $E_q(z, s)$ in place of $E(x, s)$. In particular, we can take q to be $q = b \times 1_{2m}$ with $b \in \mathfrak{B}$. Define (X, ω) as in Eq. **2.5**. Then there is an isomorphism of (X, ω) to (H_{m+n}, η_{m+n}) which maps P^ω_U of *Proposition 1* to the standard parabolic subgroup P of $G(\eta_{m+n})$. Therefore, we can identify $\mathfrak{Z}^\omega$ with the space $\mathfrak{h}^{\mathbf{a}}$ with

$$\mathfrak{h}=\{z \in \mathbf{C}^{m+n}_{m+n} | i(z^* - z) \text{ is positive definite}\}. \qquad \textbf{[7.2]}$$

We can also define an Eisenstein series $E'(x, s; \chi)$ for $x \in G^\omega_{\mathbf{A}}$ and $s \in \mathbf{C}$, which is defined by Eq. **5.6** with $(G(\eta_{m+n})_{\mathbf{A}}, P, 1)$ in place of $(G^\psi_{\mathbf{A}}, P^\psi, \mathbf{f})$. Taking E' and $(q, a) \in G^\omega_{\mathbf{h}}$ (with $a \in \mathfrak{B}$) in place of $E(x, s)$ and q, we can define a function $E'_{q,a}(\mathfrak{z}, s)$ of $(\mathfrak{z}, s) \in \mathfrak{h}^{\mathbf{a}} \times \mathbf{C}$ in the same manner as in Eq. **7.1**. There is also an injection ι of $\mathfrak{Z}^\psi \times \mathfrak{Z}^\varphi$ into $\mathfrak{h}^{\mathbf{a}}$ compatible with the embedding $G^\psi \times G^\varphi \to G(\eta_{m+n})$. We put then

$$g^\circ(z, w) = \delta(w, z)^{-k}g(\iota(z, w)) \quad (z \in \mathfrak{Z}^\psi, w \in \mathfrak{Z}^\varphi) \qquad \textbf{[7.3]}$$

for every function g on $\mathfrak{h}^{\mathbf{a}}$, where $\delta(w, z)$ is a natural factor of automorphy associated with the embedding ι. Take a Hecke eigenform $\mathbf{f}$ as in Section 4 and define f_a by the principle of Eq. **4.6**. Then, employing *Proposition 1*, we can prove

$$A(s)\mathfrak{T}(s, \mathbf{f}, \chi)E_q(z, s)$$

$$= \sum_{a\in\mathfrak{B}}\int_{\Phi_a}(E'_{q,a})^o(z, w; s)f_a(w)\delta(w)^k dw, \qquad \textbf{[7.4]}$$

where $q = b \times 1_{2m}$, A is a certain gamma factor, and $\Phi_a = \Gamma^a\backslash\mathfrak{Z}^\varphi$. The computation is similar to, but more involved than, that of ref. 4 (Section 4). Since the analytic nature of $E'_{q,a}$ can be seen from the results of ref. 8, we can derive *Theorem 3* from Eq. **7.4**.

Take $m = 0$. Then $\psi = \varphi$ and $E_q(z, s) = f_b(z)$. Then the analytic nature of $\mathfrak{T}$ $(s, \mathbf{f}, \chi)$, and consequently that of $Z(s, \mathbf{f}, \chi)$, can be derived from Eq. **7.4**. However, here we have to assume that $\chi_{\mathbf{a}}(b) = b^{k+2\nu}|b|^{i\kappa-k-2\nu}$ with $\kappa \in \mathbf{R}^{\mathbf{a}}$, $\Sigma_{v\in\mathbf{a}}\,\kappa_v = 0$, and the conductor of χ divides $\mathfrak{c}$. The latter condition on $\mathfrak{c}$ is a minor matter, but the condition on $\chi_{\mathbf{a}}$ is essential. To obtain $Z(s, \mathbf{f}, \chi)$ with an arbitrary χ, we have to replace $E'_{q,a}$ by $\mathfrak{D}E''_{q,a}$, where E'' is a series of type E' with $2\nu - \mu$ in place of k and $\mathfrak{D}$ is a certain differential operator on $\mathfrak{h}^{\mathbf{a}}$.

As for *Theorem 4*, we take again $\psi = \varphi$ and observe that a constant function can be taken as $\mathbf{f}$ if $G^\varphi_{\mathbf{a}}$ is compact. The space $\mathfrak{Z}^\varphi$ consists of a single point. The integral on the right-hand side of Eq. **7.4** is merely the value $(E'_{q,a})^\circ(z, w; s)$. We can compute its residue at $s = n$ explicitly. Comparing it with the residue on the left-hand side, we obtain *Theorem 4* when $\mathfrak{c}$ satisfies Eq. **4.10**. If n is odd, we can remove this condition by computing a group index of type $[U{:}U']$.

1. Shimura, G. (1971) *Introduction to the Arithmetic Theory of Automorphic Functions* (Iwanami Shoten and Princeton Univ. Press, Princeton), Publ. Math. Soc. Japan, No. 11.
2. Shimura, G. (1994) *Inv. Math.* **116,** 531–576.
3. Shimura, G. (1964) *Ann. Math.* **83,** 369–409.
4. Shimura, G. (1995) *Inv. Math.* **119,** 539–584.
5. Shimura, G. (1995) *Inv. Math.* **121,** 21–60.
6. Oh, L. (1996) Ph.D. thesis (Princeton University, Princeton).
7. Shimura, G. (1997) *Euler Products and Eisenstein Series* (Am. Math. Soc., Providence, RI), CBMS Series 93, in press.
8. Shimura, G. (1983) *Duke Math. J.* **50,** 417–476.

Proc. Natl. Acad. Sci. USA
Vol. 94, pp. 11138–11141, October 1997
Colloquium Paper

This paper was presented at a colloquium entitled "Elliptic Curves and Modular Forms," organized by Barry Mazur and Karl Rubin, held March 15–17, 1996, at the National Academy of Sciences, Washington, DC.

Deforming semistable Galois representations

JEAN-MARC FONTAINE

Université de Paris-Sud, Mathématique, Bâtiment 425, F-91405 Orsay Cedex, France

ABSTRACT Let V be a p-adic representation of $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$. One of the ideas of Wiles's proof of FLT is that, if V is the representation associated to a suitable autromorphic form (a modular form in his case) and if V' is another p-adic representation of $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$ "closed enough" to V, then V' is also associated to an automorphic form. In this paper we discuss which kind of local condition at p one should require on V and V' in order to be able to extend this part of Wiles's methods.

Geometric Galois Representations (refs. 1 and 2; exp. III and VIII). Let $\bar{\mathbf{Q}}$ be a chosen algebraic closure of $\mathbf{Q}$ and $G = Gal(\bar{\mathbf{Q}}/\mathbf{Q})$. For each prime number ℓ, we choose an algebraic closure $\bar{\mathbf{Q}}_\ell$ of $\mathbf{Q}_\ell$ together with an embedding of $\bar{\mathbf{Q}}$ into $\bar{\mathbf{Q}}_\ell$ and we set $G_\ell = Gal(\bar{\mathbf{Q}}_\ell/\mathbf{Q}_\ell) \subset G$. We choose a prime number p and a finite extension E of $\mathbf{Q}_p$.

An *E-representation* of a profinite group J is a finite dimensional E vector space equipped with a linear and continuous action of J.

An *E-representation* V of G is said to be *geometric* if

(*i*) it is unramified outside of a finite set of primes;

(*ii*) it is potentially semistable at p (we will write pst for short).

[The second condition implies that V is de Rham, hence Hodge-Tate, and we can define its *Hodge-Tate numbers* $h^r = h^r(V) = dim_E\,(C_p(r) \otimes_{\mathbf{Q}_p} V)^{G_p}$ where $C_p(r)$ is the usual Tate twist of the p-adic completion of $\bar{\mathbf{Q}}_p$ (one has $\Sigma_{r\in\mathbf{Z}} h^r = d$). It implies also that one can associate to V a representation of the Weil-Deligne group of $\mathbf{Q}_p$, hence a conductor $N_V(p)$, which is a power of p].

Example: If X is a proper and smooth variety over $\mathbf{Q}$ and $m \in \mathbf{N}$, $j \in Z$, then the p-adic representation $H^m_{et}(X_{\bar{\mathbf{Q}}}, \mathbf{Q}_p(j))$ is geometric.

[Granted the smooth base change theorem, the representation is unramified outside of p and the primes of bad reduction of X. Faltings (3) has proved that the representation is crystalline at p in the good reduction case. It seems that Tsuji (4) has now proved that, in case of semistable reduction, the representation is semistable. The general case can be deduced from Tsuji's result using de Jong's (5) work on alterations].

CONJECTURE (1). *If V is a geometric irreducible E-representation of G, then V comes from algebraic geometry, meaning that there exist X, m, j such that V is isomorphic, as a p-adic representation, to a subquotient of $E \otimes_{\mathbf{Q}_p} H^m_{et}(X_{\bar{\mathbf{Q}}}, \mathbf{Q}_p(j))$.*

Even more should be true. Loosely speaking, say that a geometric irreducible E-representation V of G is *a Hecke representation* if there is a finite $\mathbf{Z}_p$-algebra $\mathcal{H}$, generated by Hecke operators acting on some automorphic representation space, equipped with a continuous homomorphism $\rho : G \to GL_d(\mathcal{H})$, "compatible with the action of the Hecke operators," such that *V comes from $\mathcal{H}$* (i.e., is isomorphic to the one we get from ρ via a map $\mathcal{H} \to E$). Then any geometric Hecke representation of G should come from algebraic geometry and any geometric irreducible representation should be Hecke.

At this moment, this conjecture seems out of reach. Nevertheless, for an irreducible two-dimensional representation of G, to be geometric Hecke means to be a Tate twist of a representation associated to a modular form. Such a representation is known to come from algebraic geometry. Observe that the heart of Wiles's proof of FLT is a theorem (6, th. 0.2) asserting that, if V is a suitable geometric Hecke E-representation of dimension 2, then any geometric E-representation of G which is "close enough" to V is also Hecke.

It seems clear that Wiles's method should apply in more general situations to prove that, starting from a suitable Hecke E-representation of G, any "close enough" geometric representation is again Hecke. The purpose of these notes is to discuss possible generalizations of the notion of "close enough" and the possibility of extending local computations in Galois cohomology which are used in Wiles's theorem. More details should be given elsewhere.

Deformations (7–9). Let $\mathcal{O}_E$ be the ring of integers of E, π a uniformizing parameter and $k = \mathcal{O}_E/\pi\mathcal{O}_E$ the residue field.

Denote by $\mathcal{C}$ the category of local noetherian complete *$\mathcal{O}_E$-algebras* with residue field k (we will simply call the objects of this category $\mathcal{O}_E$-algebras).

Let J be a profinite group and $Rep^f_{\mathbf{Z}_p}(J)$ the category of $\mathbf{Z}_p$-modules of finite length equipped with a linear and continuous action of J. Consider a strictly full subcategory $\mathcal{D}$ of $Rep^f_{\mathbf{Z}_p}(J)$ stable under subobjects, quotients, and direct sums.

For A in $\mathcal{C}$, an *A-representation T* of J is an A-module of finite type equipped with a linear and continuous action of J. We say that *T lies in D* if all the finite quotients of T viewed as Z_p-representations of J are objects of $\mathcal{D}$. The A-representations of J lying in $\mathcal{D}$ form a full subcategory $\mathcal{D}(A)$ of the category $Rep^{tf}_A(J)$ of A-representations of J.

We say T is *flat* if it is flat (⇔ free) as an A-module.

Fix u a (flat !)-k-representation of J lying in $\mathcal{D}$. For any A in $\mathcal{C}$, let $F(A) = F_{u,J}(A)$ be the set of isomorphism classes of flat A-representations T of J such that $T/\pi T \simeq u$. Set $F_{\mathcal{D}}(A) = F_{u,J,\mathcal{D}}(A) =$ the subset of $F(A)$ corresponding to representations which lie in $\mathcal{D}$.

PROPOSITION. *If $H^0(J, \mathfrak{gl}(u)) = k$ and $dim_k H^1(J, \mathfrak{gl}(u)) < +\infty$, then F and $F_{\mathcal{D}}$ are representable.*

(The ring $R_{\mathcal{D}} = R_{u,J,\mathcal{D}}$ which represents $F_{\mathcal{D}}$ is a quotient of the ring $R = R_{u,J}$ representing F.)

Fix also a flat $\mathcal{O}_E$-representation U of J lifting u and lying in $\mathcal{D}$. Its class defines an element of $F_{\mathcal{D}}(\mathcal{O}_E) \subset F(\mathcal{O}_E)$, hence augmentations $\varepsilon_U{:}R \to \mathcal{O}_E$ and $\varepsilon_{U,\mathcal{D}}{:}R_{\mathcal{D}} \to \mathcal{O}_E$.

Set $\mathcal{O}_n = \mathcal{O}_E/\pi^n\mathcal{O}_E$ and $U_n = U/\pi^n U$. If $\mathfrak{p}_U = ker\ \varepsilon_U$ and $\mathfrak{p}_{U,\mathcal{D}} = ker\ \varepsilon_{U,\mathcal{D}}$, we have canonical isomorphisms

$$\begin{array}{ccccc} ((\mathfrak{p}_U+\pi^n R)/(\mathfrak{p}_U^2+\pi^n R))^* & \simeq & Ext^1_{\mathcal{O}_n[J]}(U_n, U_n) & \simeq & H^1(J, \mathfrak{gl}(U_n)) \\ \cup & & \cup & & \cup \\ (\mathfrak{p}_{U,\mathcal{D}}+\pi^n R_{\mathcal{D}})/(\mathfrak{p}_{U,\mathcal{D}}^2+\pi^n R_{\mathcal{D}})^* & \simeq & Ext^1_{\mathcal{O}_n,\mathcal{D}}(U_n, U_n) & =: & H^1_{\mathcal{D}}(J, \mathfrak{gl}(U_n)) \end{array}$$

Close Enough to V Representations. We fix a geometric E-representation V of G (morally a "Hecke representation").

We choose a G-stable $\mathcal{O}_E$-lattice U of V and assume $u = U/\pi U$ absolutely irreducible (hence V is a fortiori absolutely irreducible).

We fix also a finite set of primes S containing p and a full subcategory $\mathcal{D}_p$ of $Rep^f_{\mathbf{Z}_p}(G_p)$, stable under subobjects, quotients, and direct sums.

For any E-representation W of G_p, we say *W lies in $\mathcal{D}_p$* if a G_p-stable lattice lies in $\mathcal{D}_p$.

We say an E-representation of G is *of type* $(S, \mathcal{D}_p)$ if it is unramified outside of S and lies in $\mathcal{D}_p$.

Now we assume V is of type $(S, \mathcal{D}_p)$. We say an E-representation V' of G is $(S, \mathcal{D}_p)$*-close to V* if:

(i) given a G-stable lattice U' of V', then $U'/\pi U' \simeq u$;

(ii) V' is of type $(S, \mathcal{D}_p)$.

Then, if $\mathbf{Q}_S$ denote the maximal Galois extension of $\mathbf{Q}$ contained in $\bar{\mathbf{Q}}$ unramified outside of S, deformation theory applies with $J = G_S = Gal(\mathbf{Q}_S/\mathbf{Q})$ and $\mathcal{D}$ the full subcategory of $Rep^f_{\mathbf{Z}_p}(G_S)$ whose objects are T's which, viewed as representations of G_p, are in $\mathcal{D}_p$. But if we want the definition of $(S, \mathcal{D}_p)$-close to V to be good for our purpose, it is crucial that the category $\mathcal{D}_p$ is *semistable*, i.e., is such that any E-representation of G_p lying in $\mathcal{D}_p$ is pst.

We would like also to be able to say something about the conductor of an E-representation of G_p lying in $\mathcal{D}_p$. Since $H^1_{\mathcal{D}}(J, \mathfrak{gl}(U_n))$ is the kernel of the natural map

$$H^1(G_S, \mathfrak{gl}(U_n)) \rightarrow H^1_{\mathcal{D}_p}(G_p, \mathfrak{gl}(U_n)),$$

it is better also if we are able to compute $H^1_{\mathcal{D}_\mathrm{p}}(G_p, \mathfrak{gl}(U_n))$.

In the rest of these notes, we will discuss some examples of such semistable categories $\mathcal{D}_p$'s.

Examples of Semi-Stable $\mathcal{D}_p$'s.

Example 1: The category $\mathcal{D}^{cr}_p$ (application of (10); cr, crystalline).

For any $\mathcal{O}_E$-algebra A, consider the category $MF(A)$ whose objects are A-module M of finite type equipped with

(i) a decreasing filtration (indexed by $\mathbf{Z}$),

$$\ldots Fil^i\, M \supset Fil^{i+1}\, M \supset \ldots,$$

by sub-A-modules, direct summands as $\mathbf{Z}_p$-modules, with $Fil^i\, M = M$ for $i \ll 0$ and $= 0$ for $i \gg 0$;

(ii) for all $i \in \mathbf{Z}$, an A-linear map $\phi^i : Fil^i\, M \rightarrow M$, such that $\phi^i\, |_{Fil^{i+1}\, M} = p\phi^{i+1}$ and $M = \Sigma Im\ \phi^i$.

With an obvious definition of the morphisms, $MF(A)$ is an A-linear abelian category.

For $a \leq b \in \mathbf{Z}$, we define $MF^{[a,b]}(A)$ to be the full subcategory of those M, such that $Fil^a\, M = M$ and $Fil^{b+1}\, M = 0$. If $a < b$, we define also $MF^{]a,b]}(A)$ as the full subcategory of $MF^{[a,b]}(A)$ whose objects are those M with no nonzero subobjects L with $Fil^{a+1}\, L = 0$.

As full subcategories of $MF(A)$, $MF^{[a,b]}(A)$ and $MF^{]a,b]}(A)$ are stable under taking subobjects, quotients, direct sums, and **extensions.**

If $\bar{\mathbf{Z}}_p$ denote the p-adic completion of the normalization of $\mathbf{Z}_p$ in $\bar{\mathbf{Q}}_p$, the ring

$$A_{cris} = \underrightarrow{\lim}\, H^0((Spec(\bar{\mathbf{Z}}_p/p)/W_n)_{crys}, struct.sheaf)$$

is equipped with an action of G_p and a morphism of Frobenius $\phi : A_{cris} \rightarrow A_{cris}$. There is a canonical map $A_{cris} \rightarrow \bar{\mathbf{Z}}_p$ whose kernel is a divided power ideal J. Moreover, for $0 \leq i \leq p - 1$, $\phi(J^{[i]}) \subset p^i A_{cris}$. Hence, because A_{cris} has no p-torsion, we can define for such an i, $\phi^i : J^{[i]} \rightarrow A_{cris}$ as being the restriction of ϕ to $J^{[i]}$ divided out by p^i.

For M in $MF^{[-(p-1),0]}(A)$, we then can define $Fil^o(A_{cris} \otimes M)$ as the sub-A-module of $A_{cris} \otimes_{\mathbf{Z}p} M$, which is the sum of the images of the $Fil^i A_{cris} \otimes Fil^{-i}M$, for $0 \leq i \leq p - 1$. We can define $\phi^o : Fil^0(A_{cris} \otimes M) \rightarrow A_{cris} \otimes M$ as being $\phi^i \otimes \phi^{-i}$ on $Fil^i\, A_{cris} \otimes Fil^{-i}\, M$. If we set

$$\underline{U}(M) = (Fil^O(A_{cris} \otimes_{z_p} M))_{\phi^0=1,}$$

this is an A-module of finite type equipped with a linear and continuous action of G_p. We get in this way an A-linear functor

$$\underline{U} : MF^{[-(p-1),0]}(A) \rightarrow Rep^{ft}_A(G_p)$$

which is exact and faithful. Moreover, the restriction of $\underline{U}$ to $MF^{]-(p-1),0]}(A)$ is fully faithful. We call $\mathcal{D}^{cr}_p(A)$ the essential image.

PROPOSITION. *Let V' be an E-representation of G_p. Then V' lies in $\mathcal{D}^{cr}_p$ if and only if the three following conditions are satisfied*:

(i) *V' is crystalline (i.e., V' is pst with conductor $N_{V'}(p) = 1$);*

(ii) *$h^r(V') = 0$ if $r > 0$ or $r < -p + 1$;*

(iii) *V' has no nonzero subobject V'' with $V''(-p + 1)$ unramified.*

Moreover (11), *if X is a proper and smooth variety over $\mathbf{Q}_p$ with good reduction and if $r,n \in$* N *with $0 \leq r \leq p - 2$, $H^r_{et}(X_{\bar{\mathbf{Q}}_\mathbf{p}}, \mathbf{Z}/p^n\mathbf{Z})$ is an object of $\mathcal{D}^{cr}_p(\mathbf{Z}_\mathrm{p})$.*

Remarks: (i) Define $\mathcal{D}^{ff}_p$ as the full subcategory of $Rep^f_{\mathbf{Z}_p}(G_p)$, whose objects are representations which are isomorphic to the general fiber of a finite and flat group scheme over $\mathbf{Z}_p$. If $p \neq 2$, $\mathcal{D}^{ff}_p$ is a full subcategory **stable under extensions** of $\mathcal{D}^{cr}_p$ (this is the essential image of $MF^{[-1,0]}(\mathbf{Z}_p)$).

(ii) Deformations in $\mathcal{D}^{cr}_p$ don't change Hodge type: if V,V' are E-representations of G_p, lying in $\mathcal{D}^{cr}_p$ and if one can find lattices U of V and U' of V' such that $U/\pi U \simeq U'/\pi U'$, then $h^r(V) = h^r(V')$ for all $r \in \mathbf{Z}$ (if $U/\pi U = \underline{U}(M)$, $h^r(V) = dim_k gr^{-r}M$).

Computation of $H^1_{\mathcal{D}^{cr}_p}$. This can be translated in terms of the category $MF(\mathcal{O}_E) \supset MF^{]-p+1,0]}(\mathcal{O}_E)$.

In $MF(\mathcal{O}_E)$, define $H^i_{MF}(\mathbf{Q}_p, M)$ as being the i^{th} derived functor of the functor $Hom_{MF(\mathcal{O}_E)}(\mathcal{O}_E, -)$. These groups are the cohomology of the complex

$$Fil^0\, M \xrightarrow{1-\phi} M \rightarrow 0 \rightarrow 0 \rightarrow \ldots$$

If we set $t_M = M/Fil^0M$, this implies $lg_{\mathcal{O}_E} H^1_{\mathcal{D}^{cr}_p}(\mathbf{Q}_p, M) = lg_{\mathcal{O}_E} H^0 + lg_{\mathcal{O}_E} t_M$.

Hence, if U is a G_p-stable lattice of an E-representation V of G_p lying in $\mathcal{D}^{cr}_p$, and if, for any $i \in \mathbf{Z}$, $h_r = h_r(V)$, with obvious notations, we get $H^1_{\mathcal{D}^{cr}_p}(\mathbf{Q}_p, \mathfrak{gl}(U_n)) = Ext^1_{MF^{]-p+1,0]}(A)}(M_n, M_n) = Ext^1_{MF(A)}(M_n, M_n) = H^1_{MF}(\mathbf{Q}_p, End_{\mathcal{O}_E}(M_n))$ and $lg_{\mathcal{O}_E} H^1_{\mathcal{D}^{cr}_p}(\mathbf{Q}_p, \mathfrak{gl}(U_n)) = lg_{\mathcal{O}_E}\ H^0(\mathbf{Q}_p, \mathfrak{gl}(U_n)) + nh$, where $h = \Sigma_{i<j} h_i h_j$ [this generalizes a result of Ramakrishna (9)].

A Special Case. Of special interest is the case where $H^0(\mathbf{Q}_p, \mathfrak{gl}(u)) = k$, which is equivalent to the representability of the functor $F_{u,G_p,\mathcal{D}^{cr}_p}$. In this case, $H^1_{\mathcal{D}^{cr}_p}(\mathbf{Q}_p, \mathfrak{gl}(U_n)) \simeq (\mathcal{O}_n)^{h+1}$ and $H^1_{\mathcal{D}^{cr}_p}(\mathbf{Q}_p, \mathfrak{sl}(U_n)) \simeq (\mathcal{O}_n)^h$. Moreover, because there is no H^2, the deformation problem is smooth, hence $R_{u,G_p,\mathcal{D}^{cr}_p} \simeq \mathcal{O}_E[[X_0, X_1, X_2, \ldots, X_h]]$.

Example 2: $\mathcal{D}^{na}_p$ (the naive generalization of $\mathcal{D}^{cr}_p$ to the semistable case).

For any $\mathcal{O}_E$-algebra A, we can define the category $MFN(A)$ whose objects consist of a pair (M, N) with M object of $MF(A)$ and $N : M \rightarrow M$ such that

(i) $N(Fil^iM) \subset Fil^{i-1}M$,

(ii) $N\phi^i = \phi^{i-1}N$.

With an obvious definition of the morphisms, this is an abelian A-linear category and $MF(A)$ can be identified to the full subcategory of $MFN(A)$ consisting of M's with $N = 0$.

We have an obvious definition of the category $MFN^{]-p+1,0]}(A)$. There is a natural way to extend $\underline{U}$ to a functor

$$\underline{U} : MFN^{]-p+1,0]}(A) \rightarrow Rep^f_{Z_p}(G_p)$$

again exact and fully faithful. We call $\mathcal{D}^{cr}_p(A)$ the essential image.

There is again a simple characterization of the category $\mathcal{D}^{na}_p(E)$ of E-representations of G_p lying in $\mathcal{D}^{na}_p$ as a suitable full subcategory of the category of semistable representations with crystalline semisimplification. Moreover:

If $p \neq 2$, the category of semistable V values with $h^r(V) = 0$ if $r \notin \{0, -1\}$ is a full subcategory **stable under extensions** of $\mathcal{D}_p^{na}(E)$.

For $0 \leq r < p - 1$, let $\mathcal{D}_p^{ord,r}$ the full subcategory of $Rep^f_{\mathbf{Z}_p}(G_p)$ of T's such that there is a filtration (necessarily unique)

$$0 = F_{r+1}T \subset F_rT \subset \ldots F_1T \subset F_0T = T$$

such that $gr_iT(-i)$ is unramified for all i; then $\mathcal{D}_p^{ord,r}$ is a full subcategory of $\mathcal{D}_p^{na}$ **stable under extensions**.

Again, in $\mathcal{D}_p^{na}$, deformations don't change Hodge type. The conductor may change.

Computation of $H^1_{\mathcal{D}_p^{na}}(\mathbf{Q}_p, \mathfrak{gl}(U_n))$. As before, this can be translated in terms of the category $MFN(\mathcal{O}_E) \supset MFN^{]-p+1,0]}(\mathcal{O}_E)$: if we define $H^i_{MFN}(\mathbf{Q}_p, M)$ as the i^{th}-derived functor, in the category $MFN(\mathcal{O}_E)$, of the functor $Hom_{MFN(\mathcal{O}_E)}(\mathcal{O}_E, -)$, these groups are the cohomology of the complex

$$Fil^0M \to Fil^{-1}M \oplus M \to M \to 0 \to 0 \to \ldots$$

(with $x \mapsto (Nx, (1 - \phi^0)x)$ and $(y, z) \mapsto (1 - \phi^{-1})y - Nz)$. Again, in this case, $H^1_{\mathcal{D}_p^{na}}(\mathbf{Q}_p, \mathfrak{gl}(U_n)) = Ext^1_{MFN^{]-p+1,0]}(A)}(M_n, M_n) = Ext^1_{MFN(A)}(M_n, M_n) = H^1_{MFN}(\mathbf{Q}_p, End_{\mathcal{O}_E}(M_n))$. But,

(i) the formula for the length is more complicated, and

(ii) the (local) deformation problem is not always smooth.

Example 3: $\mathcal{D}_p^{st}$ [the good generalization of $\mathcal{D}_p^{cr}$ to the semistable case, theory due to Breuil (12)].

Let $S = \mathbf{Z}_p{<}u{>}$ be the divided power polynomial algebra in one variable u with coefficients in $\mathbf{Z}_p$. If $v = u - p$, we have also $S = \mathbf{Z}_p{<}v{>}$. Define:

(a) Fil^iS as the ideal of S generated by the $v^m/m!$, for $m \geq i$;

(b) ϕ as the unique $\mathbf{Z}_p$-endomorphism such that $\phi(u) = u^p$;

(c) N as the unique $\mathbf{Z}_p$-derivation from S to S such that $N(u) = -u$.

For $r \leq p - 1$, ϕ^r: $Fil^rS \to S$ is defined by $\phi^r(x) = p^{-r}\phi(x)$.

If $r \leq p - 2$, let $'\mathcal{M}_0^r$ be the category whose objects consist of:

(i) an S-module $\mathcal{M}$,

(ii) a sub-S-module $Fil^r\mathcal{M}$ of $\mathcal{M}$ containing $Fil^rS.\mathcal{M}$,

(iii) a linear map ϕ^r: $Fil^r\mathcal{M} \to \mathcal{M}$, such that $\phi^r(sx) = \phi^r(s).\phi(x)$ (where ϕ: $\mathcal{M} \to \mathcal{M}$ is defined by $\phi(x) = \phi^r(v^rx)/\phi^r(v^r))$, with an obvious definition of the morphisms. We consider the full subcategory $\mathcal{M}_0^r$ of $'\mathcal{M}_0^r$ whose objects satisfy

(i) as an S-module $\mathcal{M} \simeq \oplus_{1 \leq i \leq d} S/p^{n_d}S$ for suitable integers d and $(n_i)_{1 \leq i \leq d}$;

(ii) as an S-module $\mathcal{M}$ is generated by the image of ϕ^r.

Finally, define $\mathcal{M}^r$ as the category whose objects are objects $\mathcal{M}$ of $\mathcal{M}_0^r$ equipped with a linear endomorphism

$$N : \mathcal{M} \to \mathcal{M}$$

satisfying

(i) $N(sx) = N(s).x + s.N(x)$ for $s \in S, x \in \mathcal{M}$,

(ii) $v.N(Fil^r\mathcal{M}) \subset Fil^r\mathcal{M}$,

(iii) if $x \in Fil^r\mathcal{M}$, $\phi^1(v).N(\phi^r(x)) = \phi^r(v.N(x))$.

This turns out to be an abelian Z_p-linear category and we call $MFB^{[-r,o]}(\mathbf{Z}_p)$ the opposite category.

For A an $\mathcal{O}_E$-algebra, one can define in a natural way the category $MFB^{[-r,o]}(A)$ (for instance, if A is artinian, an object of this category is just an object of $MFB^{[-r,o]}(\mathbf{Z}_p)$ equipped with an homomorphism of A into the ring of the endomorphisms of this object).

Breuil defines natural "inclusions":

$$MFB^{[-r-1,o]}(A) \subset MFB^{[-r,o]}(A) \text{ (if } r + 1 \leq p - 2),$$

$$MF^{[-r,o]}(A) \subset MFN^{[-r,o]}(A) \subset MFB^{[-r,o]}(A).$$

Moreover, the simple objects of $MF^{[-r,o]}(k)$, $MFN^{[-r,o]}(k)$, and $MFB^{[-r,o]}(k)$ are the same. Breuil extends $\underline{U}$ to $MFB^{[-r,o]}(A)$ and proves that this functor is again exact and fully faithful. We call $\mathcal{D}_p^{st,r}(A)$ the essential image.

Let V be an E-representation of G_p. Breuil proves that, if V lies in $\mathcal{D}_p^{st,r}$ then V is semistable and $h^m(V) = 0$ if $m{>}0$ or $m < -r$. Conversely, it seems likely that if V satisfies these two conditions, V lies in $\mathcal{D}_p^{st,r}$. This is true if $r = 1$, and it has been proven by Breuil if $E = \mathbf{Q}_p$ and V is of dimension 2. More importantly, Breuil proved also

PROPOSITION (13). *Let X be a proper and smooth variety over* $\mathbf{Q}_p$. *Assume X as semistable reduction and let* r, n $\in \mathbf{N}$ *with 0* $\leq$ r $\leq$ p$-$2; *then* $H^r_{et}(X_{\bar{\mathbf{Q}}_p}, \mathbf{Z}/p^n\mathbf{Z})$ *is an object of* $\mathcal{D}_p^{st,r}(\mathbf{Z}_p)$.

When working with $\mathcal{D}_p^{st,r}$, *deformation may change the Hodge type* (the conductor also). The computation of $H^1_{\mathcal{D}_p^{st,r}}(\mathbf{Q}_p, \mathfrak{gl}(U_n))$ still reduces to a computation in $MFB^{[-r,o]}(\mathcal{O}_E)$ (or equivalently in $\mathcal{M}^r$). This computation becomes difficult in general but can be done in specific examples.

Final Remarks. Let L be a finite Galois extension of $\mathbf{Q}_p$ contained in $\bar{\mathbf{Q}}_p$, $\mathcal{O}_L$ the ring of integers and $e_L = e_L/\mathcal{D}_p$.

(a) Call $\mathcal{D}_p^{ff,L}$, the full subcategory of $\underline{Rep^f_{\mathbf{Z}_p}(G_p)}$ whose objects are representations which, when restricted to $Gal(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$, extends to a finite and flat group scheme over $\mathcal{O}_L$. If $e_L \leq p - 1$, an E-representation V lies in $\mathcal{D}_p$ if and only if it becomes crystalline over L and $h^m(V) = 0$ for $m \notin \{0, -1\}$). If $e_L < p - 1$, Conrad (14) defines an equivalence between $\mathcal{D}_p^{ff,L}$ and a nice category of filtered modules equipped with a Frobenius and an action of $Gal(L/\mathbf{Q}_p)$. Using it, one can get the same kind of results as we described for $\mathcal{D}_p^{cr}$. For $e_L = p - 1$, the same thing holds if we require that the representation of $Gal(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ extends to a connected finite and flat group scheme over $\mathcal{O}_L$.

(b) More generally, Breuil's construction should extend to E-representations becoming semistable over L with $h^m(V) = 0$ if $m > 0$ or $< -(p - 1)/e_L$ ($\leq -(p - 1)/e_L$ with a "grain de sel").

(c) Let $Rep\mathbf{Q}_p(G_p)^r_{cris,L}$ (resp. $Rep\mathbf{Q}_p(G_p)^r_{st,L}$) be the category of $\mathbf{Q}_p$-representations V of G_p becoming crystalline over L (resp. semistable) with $h^m(V) = 0$ if $m > 0$ or $m < -r$. Let $\mathcal{D}_p^{cris,r,L}$ (resp. $\mathcal{D}_p^{st,r,L}$) be the full subcategory of $Rep^f_{\mathbf{Z}_p}(G_p)$ consisting of T's for which one can find an object V of $Rep\mathbf{Q}_p(G_p)^r_{cris,L}$ (resp. $Rep\mathbf{Q}_p(G_p)^r_{st,L}$) G_p-stable lattices $U' \subset U$ of V such that $T \simeq U/U'$. I feel unhappy not being able to prove the following:

Conjecture. $C_p^{cris,r,L}$ *(resp.* $C_p^{st,r,L}$*): Let V be a* $\mathbf{Q}_p$-*representation of V lying in* $\mathcal{D}_p^{cris,r,L}$ (resp. $\mathcal{D}_p^{st,r,L}$). *Then V an object of* $Rep_{\mathbf{Q}_p}(G_p)^r_{cris,L}$ *(resp.* $Rep_{\mathbf{Q}_p}(G_p)^r_{st,L}$*)*.

The only cases I know $C_p^{cris,r,L}$ are $r = 0$, $r = 1$, and $e_L \leq p - 1$, $r \leq p - 1$, and $e_L = 1$. The only cases I know $C_p^{st,r,L}$ are $r = 0$, $r = 1$, and $e_L \leq p - 1$. Of course, each time we know the answer is yes, this implies that the category is semistable.

This paper was partially supported by the Institut Universitaire de France and Centre National de la Recherche Scientifique, Unité de Recherche Associée D0752.

1. Fontaine, J.-M. & Mazur, B. (1995) *Geometric Galois Representations*, Hong Kong Conference on Elliptic Curves and Modular Forms (International Press, Boston), pp. 41–78.
2. Périodes p-adiques, Astérisque 223 (1994) *Soc. Math. de France.*
3. Faltings, G. (1989) in *Algebraic Analysis, Geometry and Number Theory* (The Johns Hopkins University Press, Baltimore, MD), pp. 25–80.
4. Tsuji, T. *On Syntomic Cohomology of Higher Degree of a Semi-Stable Family*, preprint.
5. de Jong, A. J. (1995) *Smoothness, Semi-Stability, and Alterations*, preprint.
6. Wiles, A. (1995) *Ann. Math.* **141,** 443–551.
7. Schlessinger, M. (1968) *Trans. A. M. S.* **130,** 208–222.
8. Mazur, B. (1989) in *Galois Groups Over Q* (M.S.R.I. Publications, Springer), pp. 385–437.

9. Ramakrishna, R. (1993) *Comp. Math.* **87,** 269–286.
10. Fontaine, J.-M. & Laffaille, G. (1982) *Construction de Représentations p-adiques* Ann. Scient. E. N. S. **15,** 547–608.
11. Fontaine, J.-M. & Messing, W. (1987) *p-adic Periods and p-adic étale Cohomology, Contemporary Mathematics* **67,** 179–207.
12. Breuil, C. (1995) *Construction de Représentations p-adiques Semi-Stables*, Université de Paris-Sud, preprint.
13. Breuil, C. (1996) *Cohomologie étale de Torsion et Cohomologie Cristalline en Réduction Semi-Stable*, Université de Paris-Sud, preprint.
14. Conrad, B. (1996) *Finite Honda Systems and Supersingular Elliptic Curves*, Ph.D. (Princeton University, Princeton).

Proc. Natl. Acad. Sci. USA
Vol. 94, p. 11142, October 1997
Colloquium Paper

This paper was presented at a colloquium entitled "Elliptic Curves and Modular Forms," organized by Barry Mazur and Karl Rubin, held March 15–17, 1996, at the National Academy of Sciences in Washington, DC.

Integrality of Tate-cycles

GERD FALTINGS

Max-Planck-Institut für Mathematik, Gottfried-Claren-Strasse 26, 53225 Bonn, Germany

ABSTRACT **We explain a technical result about *p*-adic cohomology and apply it to the study of Shimura varieties. The technical result applies to algebraic varieties with torsion-free cohomology, but for simplicity we only treat abelian varieties.**

Suppose A is an abelian variety over V, a p-adic discrete valuation ring with perfect residue field k. Let $V_0 = W(k) \subseteq V$ denote the maximal unramified subring, $V_0 \subseteq K_0$ and $V \subseteq K$ the fraction fields. If π is a uniformizer of V, then π satisfies an Eisenstein equation $f(\pi) = 0$, and $V \cong V_0[T]/(f(T))$. Let R_V denote the p-adically completed PD-hull of V_0[T] along $(f(T))$.

Associated to A there are the étale cohomology

$$H^i_{ét}(A) = H^i_{ét}(A \otimes_V \bar{K}, \mathbb{Z}_p) \qquad \textbf{[1]}$$

and the crystalline cohomology

$$H^i_{cr}(A) = H^i_{cr}(A/R_V, \mathbb{O}). \qquad \textbf{[2]}$$

The étale cohomology $H^i_{ét}(A)$ is a free Z_{p}-module with a continuous action of $Gal(\bar{K}/K)$, while $H^i_{cr}(A)$ is a filtered free R_V-module with a Frobenius-endomorphism Φ. These are related by Fontaine's isomorphism

$$H^i_{ét}(A) \otimes B_{cris} \cong H^i_{cr}(A) \otimes B_{cris}, \qquad \textbf{[3]}$$

which after inverting p allows one to recover one cohomology from the other.

An étale Tate cycle of degree r is a Galois-invariant element

$$\psi_{ét} \in H^{2r}_{ét}(A)(r). \qquad \textbf{[4]}$$

A crystalline Tate cycle of degree r is an element

$$\psi_{cr} \in H^{2r}_{cr}(A), \qquad \textbf{[5]}$$

which lies in the $r - th$ stage of the Hodge filtration and is annihilated by $\Phi - p^{\mathrm{r}}$.

By Fontaine's comparison the $\mathbb{Q}_{\mathrm{p}}$-vector spaces of étale and crystalline Tate cycles are isomorphic. We show:

Theorem. *If $r \leq p - 2$ then $\psi_{\text{ét}}$ is integral, if and only if, the corresponding ψ_{cr} is integral.*

The proof uses techniques developed previously.

A. Vasiu (2) has used this result to show that certain Shimura varieties classifying abelian varieties with higher-order Tate cycles have good reduction. He obtains smooth models for them by normalizing the moduli-space of abelian varieties in the generic fiber of the Shimura variety. To control this normalization one uses the valuative criterion, together with the theorem applied to the Tate cycles defining the Shimura variety.

1. Faltings, G. (1994) *Integral Crystalline Cohomology Over Very Ramified Valuation Rings*, preprint.
2. Vasiu, A. (1995) *Integral Canonical Models for Shimura Varieties of Preabelian Type*, preprint.

© 1997 by The National Academy of Sciences 0027-8424/97/9411142-1$2.00/0
PNAS is available online at http://www.pnas.org.

Proc. Natl. Acad. Sci. USA
Vol. 94, pp. 11143–11146, October 1997
Colloquium Paper

This paper was presented at a colloquium entitled "Elliptic Curves and Modular Forms," organized by Barry Mazur and Karl Rubin, held March 15–17, 1996, at the National Academy of Sciences in Washington, DC.

Congruences between modular forms: Raising the level and dropping Euler factors

FRED DIAMOND

Department of Pure Mathematics and Mathematical Statistics, 16 Mill Lane, University of Cambridge, Cambridge CB2 1SB, United Kingdom

ABSTRACT We discuss the relationship among certain generalizations of results of Hida, Ribet, and Wiles on congruences between modular forms. Hida's result accounts for congruences in terms of the value of an *L*-function, and Ribet's result is related to the behavior of the period that appears there. Wiles' theory leads to a class number formula relating the value of the *L*-function to the size of a Galois cohomology group. The behavior of the period is used to deduce that a formula at "nonminimal level" is obtained from one at "minimal level" by dropping Euler factors from the *L*-function.

An example of a congruence between modular forms is provided by the newforms

$$f(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n\tau} \text{ and } g(\tau) = \sum_{n=1}^{\infty} b_n e^{2\pi i n\tau}$$

of levels 11 and 77, respectively, whose first few Fourier coefficients are found in Table 1. One can show that, in fact, $a_n \equiv b_n \bmod 3$ for all n not divisible by 7. (See Theorem 5.1 below.)

We shall discuss the relationship among the following three results concerning congruences to a newform f of weight 2 and level N. We assume that K is a number field containing the coefficients of f and restrict our attention to congruences mod powers of a prime λ dividing ℓ.

- A formula of Hida (1) measuring congruences to f in terms of the value of an L-function.
- A result of Ribet (2) that establishes the existence of certain systematic congruences between f and forms of level Np (such as the one above).
- A theorem of Wiles (3), completed by his work with Taylor (4), which shows that all suitable deformations of Galois representations associated to f actually arise from forms congruent to f.

Hida's formula, though not part of the logical structure of ref. 3, provides some insight into the role played in Wiles' proof by a certain generalization of Ribet's result. This generalization can be interpreted as the invariance of a period appearing in Hida's formula. Using this invariance, one shows that Wiles' theorem at minimal level implies the theorem at nonminimal level.

Remark 1.1: We are concerned here mainly with Ribet's "raising the level" result, rather than his "lowering the level" result of ref. 5. We remark that Hida also found systematic congruences between f and forms of level $N\ell^r$. We shall not discuss these, but focus on congruences between f and forms of level Nd with d not divisible by ℓ.

Table 1. Fourier coefficients

n	1	2	3	4	5	6	7	8
a_n	1	−2	−1	2	1	2	−2	0
b_n	1	1	2	−1	−2	2	−1	3

Notation and Review

We fix a prime ℓ and embeddings $\bar{\mathbf{Q}} \to \bar{\mathbf{Q}}_\ell$ and $\bar{\mathbf{Q}} \to \mathbf{C}$. Suppose that K is a number field contained in $\mathbf{C}$ and let λ denote the prime of $\mathcal{O}_K$ determined by our choice of embeddings. Let $\mathcal{O}$ denote the localization of $\mathcal{O}_K$ at λ.

We suppose that f is a newform of weight 2, level N_f and character χ_f with coefficients in K. The Eichler–Shimura construction associates to f an ℓ-adic representation

$$\rho_f\colon \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\bar{\mathbf{Q}}_\ell)$$

such that if p does not divide $N_f\ell$, then ρ_f is unramified at p and $\rho_f(\mathrm{Frob}_p)$ has characteristic polynomial

$$X^2 - a_p(f)X + \chi_f(p)p. \qquad \textbf{[1]}$$

We let $\bar{\rho}_f$ denote the semisimplification of the reduction of f. If f and g are newforms of weight 2, then we write $f \sim g$ if $\bar{\rho}_f$ is equivalent to $\bar{\rho}_g$. By the Cebotarev density theorem and the Brauer–Nesbitt theorem, we have $f \sim g$ if and only if $a_p(f) \equiv a_p(g)$ for all primes p not dividing $N_fN_g\ell$, the congruence being modulo the maximal ideal of the integral closure of $\mathbf{Z}_\ell$ in $\bar{\mathbf{Q}}_\ell$.

We assume throughout that ℓ is odd, ℓ^2 does not divide N_f, and ℓ does not divide the conductor of χ_f. We assume also that the restriction of $\bar{\rho}_f$ to Gal $(\bar{\mathbf{Q}}/F)$ is irreducible where F is the quadratic subfield of $\mathbf{Q}(\zeta_\ell)$. It is convenient to distinguish two sets of primes which can create technical problems.

- We let S_f denote the set of primes p such that $\rho_f|D_p$ is not minimally ramified in the sense of ref. 6.
- We let P_f denote the set of primes $\rho \neq \ell$ such that $\bar{\rho}_f^{I_p} = 0$, but $\mathrm{ad}^0(\bar{\rho}_f)^{I_p} \neq 0$.

If p is not in $P_f \cup \ell$, then p is in S_f if and only if the powers of p differ in the conductors of ρ_f and $\bar{\rho}_f$. In the introductory example, we have $S_f = P_f = P_g = \varnothing$, and $S_g = \{7\}$.

Counting Congruences

We assume that N is divisible by N_f but not by ℓ^2 and let

$$\mathcal{F}_N = \{\text{weight 2 newforms } g \text{ such that } g \sim f\ N_g|N \text{ and } \chi_f = \chi_g\}.$$

Let $\mathbf{T}_N$ denote the $\mathcal{O}$-subalgebra of $\Pi_{g\in F_N}\mathbf{C}$ generated by the set of T_p for p not dividing $N\ell$, where T_p denotes $(a_p(g))_g$. Then $\mathbf{T}_N$ is a local ring, free over $\mathcal{O}$ of rank equal to the cardinality of F_N.

Consider the homomorphism $\pi_f{:}\mathbf{T}_N \to \mathcal{O}$ defined by projection to the f coordinate. Define ideals of $\mathbf{T}_N$ by

$$I_f = \ker \pi_f \quad = \{x \in \mathbf{T} | x_f = 0\}$$

$$J_f = \mathrm{Ann}_{\mathbf{T}_N} I_f = \{x \in \mathbf{T} | x_g = 0 \text{ for all } g \neq f\}.$$

Then the ideal $\pi_f(J_f)$ has finite index in $\mathcal{O}$, and is called a *congruence ideal*. This is a variant of the notion of a congruence module used in refs. 1 and 2.

To see how it measures congruences, consider again the above example with f of level 11. We suppose that $N = 77$ and $\ell = 3$. Then $\mathbf{T}_{77}$ can be identified with

$$\{(x,y) \in \mathcal{O} \times \mathcal{O} | x \equiv y \bmod 3\mathcal{O}\},$$

and we find that the congruence ideal is $3\mathcal{O}$.

We consider also some useful variants. Suppose that Σ is a finite set of primes containing S_f. We let F_Σ denote the set

$$\{\text{weight 2 new forms } g \text{ such that } g \ \sim f,$$

$$S_g \subset ,\Sigma, \ell^2 \nmid N_g \text{ and } \chi_f$$

$$= \chi_g\}.$$

We then define $\mathbf{T}_\Sigma$ as above, but using the set F_Σ instead of F_N. We denote the resulting congruence ideal $C_{f,\Sigma}$. If f is replaced by the newform associated to a twist, then $\mathbf{T}_\Sigma$ is replaced by a ring to which it is canonically isomorphic, and we obtain the same congruence ideal. So we suppose from now on that χ_f is of order not divisible by ℓ.

If Σ contains P_f, then F_Σ can be identified with F_{N_Σ} for a certain integer N_Σ. Assuming this holds, we shall also associate to f and Σ a cohomology congruence ideal.

Let $\Gamma_H(N_\Sigma)$ denote the maximal subgroup of $\Gamma_0(N_\Sigma)$ in which $\Gamma_1(N_\Sigma)$ has ℓ-power order. Let $\mathbf{T}$ denote the $\mathcal{O}$-subalgebra of

$$\mathrm{End}(S_2(\Gamma_H(N_\Sigma)))$$

generated by the Hecke operators T_n for $n \geq 1$. We let f_Σ denote the normalized $\mathbf{T}$-eigenform characterized by

- the newform associated to f_Σ is f;
- $a_p(f_\Sigma) = 0$ for primes p in $\Sigma - \{\ell\}$;
- $a_l(f_\Sigma)$ is a unit in $\mathcal{O}$ if ℓ divides N_Σ;

where we have enlarged K if necessary. Consider the prime ideal θ in $\mathbf{T}$ defined as the kernel of the map $\mathbf{T} \to \mathcal{O}$ arising from f_Σ, and let $\mathbf{m}$ denote the maximal ideal generated by θ and λ. If $\bar{\rho}_f$ is irreducible, the completion of $\mathbf{T}_\Sigma$ at its maximal ideal can be identified with the completion of $\mathbf{T}$ at $\mathbf{m}$. (See section 4.2 of ref. 7.)

We now define a cohomology congruence ideal using the cohomology of the modular curve $X_\Sigma = X_H(N_\Sigma) = \Gamma_H(N_\Sigma)\backslash\mathcal{H}^*$. We have a natural action of $\mathbf{T}$ on

$$H^1(X_\Sigma,\mathcal{O}).$$

We choose a basis $\{x, y\}$ for the rank two submodule $M = H^1(X_\Sigma,\mathcal{O})[\theta]$, the intersection of the kernels of the elements of θ. We define the cohomology congruence ideal

$$C^{\mathrm{coh}}_{f,\Sigma} = \langle x,y \rangle \mathcal{O},$$

where $\langle , \rangle$ is the perfect pairing on $H^1(X_\Sigma,\mathcal{O})$ gotten from $x \cup Wy$, where W is the Atkin–Lehner involution. One checks the following (see section 4.4 of ref. 7).

LEMMA 3.1. *The ideal $C_{f,\Sigma}$ is contained in $C^{coh}_{f,\Sigma}$. Furthermore if the completion $H^1(X_\Sigma,\mathcal{O})_{\mathbf{m}}$ is free over $\mathbf{T} \cong \mathbf{T}_\Sigma$, then equality holds.*

Remark 3.2: The freeness of $H^1(X_\Sigma,\mathcal{O})$ is equivalent to $H^1(X_\Sigma,k)[\mathbf{m}]$ being two-dimensional over k, which is known under our hypotheses through work of Mazur *et al.* (see section 2.1 of ref. 3).

Relation with L-Functions

Hida's formula relates $C^{\mathrm{coh}}_{f,\Sigma}$ to the value of an L-function. We consider the L-function associated to the Galois representation $\mathrm{ad}^0\rho_f$. This L-function is defined by analytic continuation of the Euler product

$$L(\mathrm{ad}^0 f,s) = \prod_p L_p(\mathrm{ad}^0 f,s), \qquad \textbf{[2]}$$

where for primes p not dividing N_f, the Euler factor $L_p(\mathrm{ad}^0\rho_f,s)$ is

$$[(1 - \alpha_p\beta_p^{-1}p^{-s})(1 - p^{-s})(1 - \beta_p\alpha_p^{-1}p^{-s})]^{-1}$$

α_p and β_p being the roots of Eq. **1**. We shall not give here the recipe for the Euler factors at primes p dividing N_f. We remark, however, that $L(\mathrm{ad}^0 f,s)$ remains the same if f is replaced by the newform associated to a twist, and that if N_f is minimal among such newforms, then $L_p(\mathrm{ad}^0 f,s)$ for p dividing N_f is one of the following:

$$(1 - p^{-1-s})^{-1}, (1 - p^{-s})^{-1}, (1 + p^{-s})^{-1} \text{ or } 1.$$

If Σ is a finite set of primes, then we write $L^\Sigma(ad^0 f,s)$ for the function obtained by omitting the Euler factors at the primes in Σ.

Suppose now that Σ contains $P_f \cup S_f$ as at the end of preceding section. We let ω denote the class in $H^1(X_\Sigma,\mathbf{C})$ associated to the holomorphic differential $2\pi i f_\Sigma(\tau)d\tau$ on X_Σ. We let ω' denote the class associated to the antiholomorphic differential $\overline{W\omega^c}$ where ω^c is defined using $f^c_\Sigma = \Sigma \bar{a}_n(f_\Sigma)e^{2\pi i n\tau}$ instead of f_Σ.

Viewing M as contained in $H^1(X_\Sigma,\mathbf{C})$, we find that the span of x and y coincides with that of ω and ω'. We write A for the matrix in $GL_2(\mathbf{C})$ such that

$$A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \omega \\ \omega' \end{pmatrix}.$$

Define the period Ω to be the determinant of A. (Note that because we have chosen a basis for M, Ω is well defined only up to a unit in $\mathcal{O}$.) Set $\delta = 3$ if ℓ is in Σ, 1 if $\ell | N_f$ but $\ell \notin \Sigma$, and 0 otherwise. Hida's formula can then be stated as follows:

THEOREM 4.1. *$C^{\mathrm{coh}}_{f,\Sigma}$ is generated by*

$$\frac{L^\Sigma(ad^0 f,1)\ell^\delta}{i\pi\Omega}$$

The proof uses results of Shimura to express the Petersson inner product of f with itself in terms of the value of the L-function. In particular, the ratio is an element of $\mathcal{O}$.

Recall that we have assumed here that Σ contains $P_f \cup S_f$, but the formula actually holds assuming only that Σ contains S_f. However, we have not explained how to define Ω in that situation. We shall see that in fact

THEOREM 4.2. *Ω is independent of Σ.*

So we could use any Σ containing $S_f \cup P_f$ to define Ω. From the theorem, we also see precisely how $C^{\mathrm{coh}}_{f,\Sigma}$ varies with Σ: Adding primes other than ℓ to Σ simply corresponds to dropping the corresponding Euler factors from the L-function. Furthermore, we shall see that the congruences established by Ribet are related to the theorem, which is essentially a reformulation of Wiles' generalization (3) of Ribet's result.

Dropping Euler Factors

Ribet's result (2) on "raising the level" is the following theorem:

THEOREM 5.1. *If p does not divide N_f then the following are equivalent:* (a) *There exists g such that $f \sim g$, $\chi_f = \chi_g$ and $N_g = dp$ for some divisor d of N_f.*

(b) *The congruence $a_p(f)^2 \equiv \chi_f(p)(p+1)^2$* mod λ *holds.*

The introductory example is a congruence as in the theorem. We take $p = 7$ and λ dividing 3. Because $a_p(f) = -2$, we see there must be a form g congruent to f with $N_g = 77$ (because $N_g = 7$ is impossible).

The direction (a) $\Rightarrow$ (b) of the theorem follows from consideration of the representation $\bar{\rho}_f$. We give the idea of the proof in the case $p \neq \ell$: If there exists a g as in the theorem, then the ratio of the eigenvalues of $\bar{\rho}_f$ (Frob$_p$) must be $p^{\pm 1}$mod λ. Then one applies the formula

$$a_p(f)^2 - \chi_f(p)(p+1)^2 = -\chi_f(p)(p - \alpha_p\beta_p{}^{-1})(p - \beta_p\alpha_p{}^{-1}).$$

The direction (b) $\Rightarrow$ (a) is closely related to Theorem 4.2, which shows that

$$C^{\mathrm{coh}}_{f,\Sigma\cup\{p\}} = (p-1)(a_p(f)^2 - \chi_f(p)(p+1)^2)C^{\mathrm{coh}}_{f,\Sigma}$$

if p is not in Σ and does not divide N_f. Ribet's proof relies on a comparison of cohomology congruence ideals, but his setup is slightly different from the one here. He compares cohomology congruence ideals at level N_f and N_fp, with the result that the factor of $p - 1$ does not occur.

To prove Theorem 4.2, one defines a certain $\mathbf{T}_{\Sigma'}$-linear injection

$$\phi: H^1(X_\Sigma, \mathcal{O})_{\mathbf{m}} \hookrightarrow H^1(X_{\Sigma'}, \mathcal{O})_{\mathbf{m}'} \text{ for } \Sigma' \supset \Sigma.$$

It is defined so that $\phi(M) \subset M'$ where $'$ indicates we are using Σ' instead of Σ. We may even normalize the map so that this restriction, tensored with $\mathbf{C}$, sends f_Σ to $f_{\Sigma'}$, i.e., the map drops Euler factors. The key ingredient in the proof of independence is the following generalization by Wiles of a lemma of Ribet:

LEMMA 5.2. *ϕ has torsion-free cokernel.*

This is proved using a result of Ihara whose role in the comparison of cohomology congruence ideals is identified in Ribet's work.

It follows that ϕ induces an isomorphism $M \to M'$, and we conclude that $A = A'$ using $\phi(x), \phi(y)$ as a basis for M'. From Theorem 4.2 we deduce:

COROLLARY 5.3. *Suppose that $\Sigma' \supset \Sigma \supset P_f \cup S_f$. If ℓ is not in $\Sigma' - \Sigma$*, then let *$\varepsilon = 0$. Otherwise let $\varepsilon = 2$ or 3 according to whether or not N_f is divisible by ℓ. Then*

- $C^{coh}_{f,\Sigma} = \ell^{-\varepsilon} C^{coh}_{f,\Sigma'} \Pi_{p \in \Sigma' - \Sigma} L_p(ad^0 f, 1)$,
- *and if* $\mathrm{C}_{f,\Sigma} = C^{coh}_{f,\Sigma}$, *then*

$$C_{f,\Sigma'} \subset \ell^{\varepsilon} C_{f,\Sigma} \prod_{p \in \Sigma' - \Sigma} L_p(ad^0 f, 1)^{-1}. \quad [3]$$

Relation with Selmer Groups

Using Mazur's theory of deformations of Galois representations, one associates a ring R_Σ and a universal deformation

$$\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(R_\Sigma)$$

of $\bar{\rho}_f$ minimally ramified outside Σ (see ref. 6). Here we work over the completion $\mathcal{O}$ of $\hat{\mathcal{O}}$, which we view as contained in $\bar{\mathbf{Q}}_\ell$. Supposing that Σ contains S_f, we obtain a homomorphism $\pi_{f,\Sigma}$: $R_\Sigma \to \bar{\mathbf{Q}}_\ell$ from ρ_f and the universal property. The $\hat{\mathcal{O}}$-module

$$\Phi_{f,\Sigma} = \ker \pi_{f,\Sigma} / (\ker \pi_{f,\Sigma})^2$$

can be described using Galois cohomology. In fact we have a canonical isomorphism

$$\mathrm{Hom}_{\mathcal{O}}(\Phi_{f,\Sigma}, K/\mathcal{O}) \cong \mathrm{H}^1_\Sigma(\mathrm{G}_{\mathbf{Q}}, \mathrm{L} \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell / \mathbf{Z}_\ell) \quad [4]$$

where L is gotten from ad$^0\rho_f$. The group on the right is sometimes called a Selmer group. The subscript Σ indicates that for $p \notin \Sigma$ the cohomology classes are supposed to restrict to elements of $H^1_f(G_p, L \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell / \mathbf{Z}_\ell)$ (as defined in ref. 8). There is also a possibly weaker condition imposed at $p = \ell$ if it is in Σ (3, 9). The universal property of the deformation also yields a surjective homomorphism ϕ_Σ from R_Σ to the completion of $\mathbf{T}_\Sigma$. The key result of Wiles (3) and its generalization in (9) is that ϕ_Σ is an isomorphism (6, 7).

This result turns out to be related to the comparison of the congruence ideal $C_{f,\Sigma}$ with the Fitting ideal of $\Phi_{f,\Sigma}$, which we denote $D_{f,\Sigma}$. (Recall that if $\Phi_{f,\Sigma}$ has finite length d, then its Fitting ideal is generated by λ^d, and if the length is infinite than the Fitting ideal is trivial.) On the one hand, an easy commutative algebra argument shows that

$$D_{f,\Sigma} \subset \hat{C}_{f,\Sigma}. \quad [5]$$

On the other hand, a deeper commutative algebra argument shows that equality holds in Eq. **5** if and only if the following hold: (a) ϕ_Σ is an isomorphism, and (b) $\mathbf{T}_\Sigma$ is a complete intersection.

One first proves the two assertions in the case $\Sigma = \emptyset$, so to get started one needs the existence of f such that $S_f = \emptyset$. This existence is a version of Serre's epsilon conjecture, and the most difficult step in the proof is Ribet's theorem on lowering the level (5). Assuming that we also have $P_f = \emptyset$, Taylor and Wiles (4) show that $\mathbf{T}_\emptyset$ is a complete intersection, and using this fact Wiles (3) shows that $\phi_\emptyset$ is an isomorphism. Their proofs use the generalization of Mazur's result discussed in Remark 3.2, and from which we also deduce

$$D_{f,\Sigma} = \hat{C}_{f,\Sigma} = \hat{C}^{\mathrm{coh}}_{f,\Sigma} \quad [6]$$

if $\Sigma = S_f = P_f = \emptyset$.

Combining the inclusion Eq. **3** with its counterpart

$$D_{f,\Sigma'} \supset \ell^{\varepsilon} D_{f,\Sigma} \prod_{p \in \Sigma' - \Sigma} L_p(\mathrm{ad}^0 f, 1)^{-1}$$

resulting from a Galois cohomology argument, we find that Eq. **6** holds for arbitrary Σ provided $S_f = P_f = \emptyset$. Hence we have (a) and (b), and therefore $D_{f,\Sigma} = \hat{C}_{f,\Sigma}$, assuming only that $\Sigma \supset S_f$ and $P_f = \emptyset$. Applying the result of remark 3.2, we get Eq. **6** as well in that case.

Remark 6.1: Improvements to these arguments, due to Faltings, Lenstra, Fujiwara, and the author (10) establish (a), (b), and Eq. **6** simultaneously (first for $\Sigma = \emptyset$, then in general) without appealing to Remark 3.2.

If P_f is not empty, then we can sometimes get empty P_f for a twist, but in general we appeal to ref. 9 to get (a) and (b) in the case of $\Sigma = S_f = \emptyset$, along with Eq. **3** if $\Sigma' = P_f$. We conclude that

THEOREM 6.2. *Keep the above hypotheses and notation.*

- *For arbitrary Σ, (a) and (b) hold.*
- *If Σ contains S_f, then $\dfrac{L^\Sigma(ad^0 f, 1)\ell^\delta}{i\pi\Omega}$ is a generator for $D_{f,\Sigma}$.*
- *If Σ contains $S_f \cup P_f$, then Eq.* **6** holds.

Remark 6.3: Coates and Flach have pointed out that one can deduce form the theorem a formula relating the order of $H^1_\emptyset$ $(G_{\mathbf{Q}}, \mathbf{L} \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell / \mathbf{Z}_\ell)$ to $L^\Sigma(\mathrm{ad}^0 f, 1)$. To relate the orders of $H^1_\emptyset$ and H^1_Σ, one uses a variant of proposition 5.14 (ii) of ref. 8. In the case of f corresponding to an elliptic curve, see section 3 of ref. 11 for this variant and ref. 12 for a discussion of the relation with the Tamagawa number conjecture (8).

The author is grateful to M. Flach for comments on an earlier draft. This research was supported by the Engineering and Physical Sciences Research Council (Grant No. GR/J4761).

1. Hida, H. (1981) *Inv. Math.* **63**, 225–261.
2. Ribet, K. A. (1984) in *Proceedings of the International Congress of Mathematicians, Vol. 1 (Warsaw, 1983),* eds. Ciesielski, Z. & Olech, C. (PWN, Warsaw), pp. 503–514.
3. Wiles, A. (1995) *Ann. Math.* **141,** 443–551.
4. Taylor, R. & Wiles, A. (1995) *Ann. Math.* **141,** 553–572.
5. Ribet, K. A. (1990) *Inv. Math.* **100,** 431–476.
6. Diamond, F. (1997) in *Modular Forms and Fermat's Last Theorem*, eds. Cornell, G., Silverman, J. & Stevens, G. (Springer, New York), in press.
7. Darmon, H., Diamond, F. & Taylor, R. (1996) in *Current Developments in Mathematics, 1995*, eds., Bott, R., Jaffe, A., Hopkins, M., Singer, I., Stroock, D. & Yau, S. T. (International Press, Cambridge, MA), pp. 1–154.
8. Bloch, S. & Kato, K. (1990) in *The Grothendieck Festschrift, Vol. I,* eds., Cartier, P., Illusie, L., Katz, N. M., Laumon, G., Manin, Yu. & Ribet, K. A. (Birkhauser, Boston), pp. 333–400.
9. Diamond, F. (1996) *Ann. Math.* **144,** 137–166.
10. Diamond, F. (1997) *Inv. Math.*, in press.
11. Coates, J. & Sydenham, A. (1995) in *Elliptic Curves, Modular Forms and Fermat's Last Theorem*, eds. Coates, J. & Yau, S. T. (International Press, Cambridge, MA), pp. 2–21.
12. Flach, M. (1993) in *Séminaire de Théorie des Nombres, Paris, 1991–92,* ed. David. S. (Birkhauser, Boston), pp. 23–36.

Proc. Natl. Acad. Sci. USA
Vol. 94, pp. 11147–11148, October 1997
Colloquium Paper

This paper was presented at a colloquium entitled "Elliptic Curves and Modular Forms," organized by Barry Mazur and Karl Rubin, held March 15–17, 1996, at the National Academy of Sciences in Washington, DC.

On degree 2 Galois representations over $\mathbb{F}_4$

NICHOLAS SHEPHERD-BARRON* AND RICHARD TAYLOR†

*Cambridge University, 16 Mill Lane, Cambridge, CB2 1SB, United Kingdom; and †Mathematics Institute, Oxford University, 24-29 St. Giles, Oxford, OX1 3LB, United Kingdom

ABSTRACT We discuss proofs of some new special cases of Serre's conjecture on odd, degree 2 representations of $G_{\mathbb{Q}}$.

We shall call a simple abelian variety $A/\mathbb{Q}$ modular if it is isogenous over $\mathbb{Q}$ to a factor of the Jacobian of a modular curve. If $A/\mathbb{Q}$ is a modular abelian variety then $F = \mathrm{End}^0(A/\mathbb{Q})$ is a number field of degree $\dim A$. Replacing A by an isogenous (over $\mathbb{Q}$) abelian variety we may assume that $\mathrm{End}(A/\mathbb{Q}) = \mathcal{O}_F$. If λ is a prime of $\mathcal{O}_F$ with residue characteristic l, then $G_{\mathbb{Q}}$ acts on $A[\lambda] \otimes \bar{\mathbb{F}}_l$, so that there is a continuous representation $\rho_{A,\lambda}$: $G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_l)$. We shall call a representation arising in this way modular. If c denotes complex conjugation then $\det \rho_{A,\lambda}(c) = -1$, i.e., $\rho_{A,\lambda}$ is odd.

The following two conjectures have been extremely influential. The first is a generalization of the Shimura–Taniyama conjecture, the second is due to Serre (1).

CONJECTURE 1: *If* A/$\mathbb{Q}$ *is a simple abelian variety and End*^{0}(A/$\mathbb{Q}$) *is a number field of degree dim* A *then* A *is modular.*

CONJECTURE 2: *If* ρ: $\mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_1)$ *is odd and irreducible then* ρ *is modular.*

Very little is known about Serre's conjecture, but we do have the following deep result of Langlands (2) and Tunnell (3).

THEOREM 1: *If* ρ: $G_{\mathbb{Q}} \to GL_2(\mathbb{F}_2)$ *or* $GL_2(\mathbb{F}_3)$ *is odd and absolutely irreducible then* ρ *is modular*.

Recent work of Wiles (4) completed by Taylor and Wiles (5) and extended by Diamond (6) proves the following theorem.

THEOREM 2: *Suppose* $A/\mathbb{Q}$ *is a simple abelian variety and that* $End(A/\mathbb{Q})$ *is the ring of integers in a number field, F, of degree dim A. Suppose also that there is a prime* λ *of* $\mathcal{O}_F$ *with residue characteristic* $l \neq 2$ *such that A has semi-stable reduction at l,* $\rho_{A,\lambda}$ *restricted to* $G_{\mathbb{Q}(\sqrt{(-1)^{(l-1)/2}l})}$ *is absolutely irreducible and* $\rho_{A,\lambda}$ *is modular. Then A is modular.*

In ref. 7 we obtain a few new cases of Serre's conjecture. In fact we prove the following theorem.

THEOREM 3: *1. If* ρ: $G_{\mathbb{Q}} \to GL_2(\mathbb{F}_5)$ *has determinant the cyclotomic character and if* $\#\rho(I_3)|10$ *then* ρ *is modular.*

2. If ρ: $\mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_4)$ *is unramified at 3 and 5 then* ρ *is modular.*

This is an easy consequence of the two theorems cited above and the following algebro-geometric result. By a $\sqrt{5}$ abelian surface we shall mean a triple (A, λ, i) where A is an abelian surface, λ: $A \xrightarrow{\sim} A^{\vee}$ is a principal polarization and i: $\mathbb{Z}[(1 + \sqrt{5})/2] \hookrightarrow \mathrm{End}(A)$, which has image fixed by the Rosati involution coming from λ (that is, λ is $\mathbb{Z}[(1 + \sqrt{5})/2]$-linear).

THEOREM 4: *1. If* ρ: $G_{\mathbb{Q}} \to GL_2(\mathbb{F}_5)$ *has determinant the cyclotomic character then there exists an elliptic curve* $E/\mathbb{Q}$ *such that* $\rho \cong \rho_{E,5}$ *and* $\rho_{E,3}$: $G_{\mathbb{Q}} \to GL_2(\mathbb{F}_3)$ *is surjective.*

2. If ρ: $G_{\mathbb{Q}} \to SL_2(\mathbb{F}_4)$ *then there is a* $\sqrt{5}$ *abelian surface* $(A,$ λ, $i)/\mathbb{Q}$ *such that* $\rho \cong \rho_{A,2}$ *and* $\rho_{A,\sqrt{5}}$: $G_{\mathbb{Q}} \to GL_2(\mathbb{F}_5)$ *is surjective.*

Part 1 of this theorem is a slight generalization of an old result of Hermite (8); see also refs. 9 and 10. [We remark that the analogous statement for representations $G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/4\mathbb{Z})$ is false.] In this form (except for the surjectivity of $\rho_{E,3}$) one of us (R.T.) pointed it out to Wiles in 1992 and explained how it could be used to deduce part 1 of Theorem 3 from the Shimura–Taniyama conjecture (see ref. 4). Part 2 seems to be new. The same argument also gives the following result [recall that $SL_2(\mathbb{F}_4) \cong A_5$].

PROPOSITION 1: *Let K be a field of characteristic zero,* $f \in K[X]$ *a quintic polynomial with discriminant d and* L/K *the splitting field for f. Then there is a* $\sqrt{5}$ *abelian surface* $A/K(\sqrt{d})$ *such that* $L = K(\sqrt{d})(A[2])$.

We will now sketch the proof of part 2 of Theorem 4 (see ref. 7 for the details). Let Y denote the cubic surface

$$\sum_{i=1}^{5} y_i = \sum_{i=1}^{5} y_i^3 = 0.$$

It has an obvious action of S_5. The 27 lines on Y divide into 3 orbits of length 15, 6, and 6 under the action of A_5. The lines in the orbit of length 15 are all defined over $\mathbb{Q}$. We will let Y^0 denote their complement. The other 12 lines are each defined over $\mathbb{Q}(\sqrt{5})$. The lines in each orbit of length 6 are disjoint.

Y^0 is the open subspace of the coarse moduli space of $\sqrt{5}$ abelian surfaces with full level 2 structure which parametrizes $\sqrt{5}$ abelian surfaces which are not the product of two elliptic curves. [Over $\mathbb{C}$ this was discovered by Hirzebruch (see for example ref. 11).] We can twist Y and Y^0 by ρ: $G_{\mathbb{Q}} \to SL_2(\mathbb{F}_4) \cong A_5$ to obtain Y_ρ and Y_ρ^0. Then Y_ρ is still a cubic surface because the action of A_5 extends to one on the ambient $\mathbb{P}_3$ which itself lifts to a homomorphism $A_5 \to GL_4$. Y_ρ also contains 6 disjoint lines collectively defined over $\mathbb{Q}(\sqrt{5})$ and blowing them down we obtain $\mathbb{P}_2/\mathbb{Q}(\sqrt{5})$ (again because the action of A_5 lifts to a representation $A_5 \to GL_3$). If X_ρ denotes the restriction of scalars from $\mathbb{Q}(\sqrt{5})$ to $\mathbb{Q}$ of Y_ρ then we deduce that $X_\rho/\mathbb{Q}$ is a rational 4-fold. There is also a dominant rational map θ: $X_\rho \to Y_\rho$ which on geometric points sends a pair (y_1, y_2) to the third point of intersection of the line y_1y_2 with Y_ρ. We deduce that Y_ρ^0 contains many rational points.

Unfortunately, a rational point $y \in Y_\rho^0$ does not necessarily give rise to a $\sqrt{5}$ abelian surface A which is defined over $\mathbb{Q}$. However if it does then $\rho \cong \rho_{A,2}$. Over Y^0 there is no universal abelian surface. However there is a canonical $\mathbb{P}_1$-bundle C/Y^0 (for the Zariski topology) and six sections $s_1, \ldots, s_6$, such that if $y \in Y^0(\bar{\mathbb{Q}})$ then the $\sqrt{5}$ abelian surface parametrized by y is the Jacobian of the double cover of C_y ramified exactly at $s_1(y), \ldots, s_6(y)$. The action of A_5 extends to C, where it permutes $s_1, \ldots, s_6$ transitively, so that we get a $\mathbb{P}_1$-bundle C_ρ/Y_ρ^0 (now for the étale topology). A point of $Y_\rho^0(\mathbb{Q})$ gives rise to a $\sqrt{5}$ abelian surface if and only if it is in the image of $C_\rho(\mathbb{Q})$. Although C_ρ/Y_ρ^0 is not split, one can show that its pull back to X_ρ is split. Thus points in $\theta(X_\rho(\mathbb{Q}))$ do correspond to $\sqrt{5}$ abelian surfaces defined over $\mathbb{Q}$. This is sufficient to prove part

© 1997 by The National Academy of Sciences 0027-8424/97/9411147-2$2.00/0
PNAS is available online at http://www.pnas.org.

2 of Theorem 4. [To show that the pull back of C_ρ to X_ρ splits we first show that it extends outside codimension two and hence is equivalent to a constant bundle (as X_ρ is rational). Then we find one rational point on it above the boundary of X_ρ.]

1. Serre, J.-P. (1987) *Duke Math.* **54,** 179–230.
2. Langlands, R. (1980) *Base Change for GL(2)* (Princeton Univ. Press, Princeton).
3. Tunnell, J. (1981) *Bull. Am. Math. Soc.* **5,** 173–175.
4. Wiles, A. (1995) *Ann. Math.* **141,** 443–551.
5. Taylor, R. & Wiles, A. (1995) *Ann. Math.* **141,** 553–572.
6. Diamond, F. (1996) *Ann. Math.* **144,** 137–166.
7. Shepherd-Barron, N. I. & Taylor, R. (1997) *J. Am. Math. Soc.*, in press.
8. Hermite, C. (1858) *Comptes Rendus* **46**.
9. Klein, R. (1888) *Lectures on the Icosahedron*, trans. Morrice, G. G. (Trübner, London).
10. Serre, J.-P. (1986) in *Oeuvres III* **123** (reprinted 1986, Springer).
11. van der Geer, G. (1988) *Hilbert Modular Surfaces* (Springer, New York).