J. Coates[1] and R. Sujatha[2]

[1]Emmanuel College, Cambridge, CB2 3AP, England
[2]School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Colaba, Bombay 400 005, India
e-mail: J.H.Coates@dpmms.cam.ac.uk; sujatha@math.tifr.res.in

Abstract.

Keywords.

1. Introduction

In his important papers [16], [17], Wiles proved in most cases the so-called main conjecture for the cyclotomic $\mathbb{Z}_p$-extension of any totally real base field F, for all odd primes p, and for all abelian characters of $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ (we say most cases because his work only establishes the main conjecture up to μ-invariants for those abelian characters whose order is divisible by p). It would be technically too difficult for us in these introductory lectures to attempt to explain his proof in this generality. Instead, we have chosen the much more modest path of giving a sketch of his proof in the very special case that $F = \mathbb{Q}$, and for all abelian characters of $\mathbb{Q}$ of p-power conductor. In fact, our account of Wiles' proof in this case has been directly inspired by a series of lectures on this theme, which we attended, given by Chris Skinner in an instructional conference held at the Centre of Mathematical Sciences, Zhejiang University, Hangzhou, China, in August 2004. As Skinner's lectures were not written up, we thought it worthwhile to give here his account, insisting however that all inaccuracies in our version are of our own making. We remark that the proof as we have presented it here, makes use of the Ferrero-Washington theorem, asserting that $\mu = 0$ for the field obtained by adjoining all p-power roots of unity to $\mathbb{Q}$. However, we are grateful to C. Skinner for many helpful comments on our notes, including pointing put to us that a simple variant of the proof presented here avoids the use of the Ferrero-Washington theorem. We also stress that Wiles, in his work on the general case, had to overcome many addtional technical difficulties, for example the existence of the so-called trivial zeroes of p-adic L-function, and the fact that Leopoldt's conjecture is unknown for arbitrary totally real base fields. Moreover, at that time, it was not even known how to formulate the μ-invariant part of the main conjecture when the order of the character is divisible by p, whereas today we know how to do it in terms of K-theory. We also mention that other proofs of the main conjecture are known in this special case when $F = \mathbb{Q}$ (see [10], [14], [4]), but none of these generalise to base fields other than $\mathbb{Q}$. Finally, we thank the Department of Mathematics at POSTECH, South Korea, for

providing us with excellent working conditions during the preparation of the written version of our lectures.

In what follows, F will denote a totally real number field, and p is an odd prime. We write Σ_p for the set of primes of F above p. As always, μ_{p^∞} is the group of all p-power roots of unity. The cyclotomic character is denoted by

$$\chi_F : \mathrm{Gal}(\bar{\mathbb{Q}}/F) \to \mathbb{Z}_p^\times,$$

so that $\sigma(\zeta) = \zeta^{\chi_F(\sigma)}$ for all σ in the Galois group and ζ in μ_{p^∞}. Let δ be the extension degree $[F(\mu_p) : F]$, and put $\Delta = \mathrm{Gal}(F(\mu_p)/F)$. The cyclotomic $\mathbb{Z}_p$-extension of F contained in $F(\mu_{p^\infty})$ is denoted by F^{cyc} and we put $\Gamma = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$ so that $\Gamma \simeq \mathbb{Z}_p$. Recall that Leopoldt's conjecture for F is equivalent to the assertion that F^{cyc} is the unique $\mathbb{Z}_p$-extension of F. Finally for a complex variable s, $\zeta(F, s)$ will denote the complex zeta function of F, which is defined by

$$\zeta(F, s) = \prod_v (1 - (Nv)^{-s})^{-1}, \quad \mathrm{Re}(s) > 1.$$

In this first section, we state the "main conjecture" for our totally real number field F, but restricting our attention to powers of the Teichmüller character of F, rather than arbitrary abelian characters. Our starting point is the following theorem proved by Siegel [15].

Theorem 1.1 (Siegel). *For all even integers $n > 0$, we have $\zeta(F, 1 - n) \in \mathbb{Q}$.*

Siegel gave some nice formulae which allow one to compute these values by hand in some cases. For instance, if $F = \mathbb{Q}(\theta)$, where θ is a root of $x^3 - 9x + 1$, and F has discriminant 3×107. We have

$$\zeta(F, -1) = \pm 1, \quad \zeta(F, -3) = \pm \frac{3 \cdot 5 \cdot 37}{2}.$$

Definition 1.2. *Let G be any profinite group. The Iwasawa algebra $\Lambda(G)$ of G, is defined as*

$$\Lambda(G) = \varprojlim_U \mathbb{Z}_p[G/U],$$

where U runs over all open normal subgroups of G.

The ring $\Lambda(G)$ has a second interpretation as the ring of $\mathbb{Z}_p$-valued measures on G. Thus, given any continuous function $f : G \to \mathbb{C}_p$, where $\mathbb{C}_p = \hat{\bar{\mathbb{Q}}}_p$, is the completion of the algebraic closure of $\mathbb{Q}_p$ for the p-adic topology, one can define the integral $\int_G f d\mu$ in $\mathbb{C}_p$.

2. *p*-adic *L*-functions

In this section, we state the theorem of Cassou-Noguès–Deligne–Ribet, (but only in the special case we need) in various equivalent forms. Define

$$\mathcal{F}_\infty = F(\mu_{p^\infty}), \quad F_\infty = F(\mu_{p^\infty})^+, \quad \mathcal{G} = \mathrm{Gal}(\mathcal{F}_\infty/F), \quad G = \mathrm{Gal}(F_\infty/F).$$

Definition 2.1. *An element μ of the fraction ring of $\Lambda(G)$ is a pseudo-measure if $(\sigma - 1)\mu \in \Lambda(G)$ for all σ in G.*

We also put

$$\zeta^{(p)}(F, s) = \zeta(F, s) \times \prod_{v \mid p} (1 - (Nv)^{-s}). \tag{1}$$

Two different proofs of the following theorem were given about the same time by Deligne–Ribet [5] and P. Cassou-Noguès [3].

Theorem 2.2 (Deligne–Ribet, Cassou-Nogués). *There exists a unique pseudo-measure $\mu_{F,p}$ on G such that, for all even integers $k > 0$, we have*

$$\int_G \chi_F^k \, d\mu_{F,p} = \zeta^{(p)}(F, 1 - k).$$

There are several alternative ways of expressing this p-adic zeta function. We first explain the definition in terms of *branches*. We have

$$\mathrm{Gal}(\mathcal{F}_\infty/F) = \Delta \times \Gamma,$$

where Δ is isomorphic to $\mathrm{Gal}(F(\mu_p)/F)$ and Γ is isomorphic to $\mathrm{Gal}(F^{\mathrm{cyc}}/F)$. Put

$$\omega_F = \chi_F|_\Delta, \quad \kappa_F = \chi_F|_\Gamma.$$

It is traditional to call ω_F the Teichmüller character of F. The distinct characters of Δ are given by the ω_F^j $(j = 0, \ldots, \delta - 1)$. For s in $\mathbb{Z}_p$ and j even, the p-adic L-function $L_{F,p}(s, \omega_F^j)$ is defined as follows.

Definition 2.3. *For j even, $L_{F,p}(1 - s, \omega_F^j) = \int_G \omega_F^j \kappa_F^s \, d\mu_{F,p}$.*

It is immediate from the definition and the above theorem that, for all integers $k > 0$ with $k \equiv j \mod (p - 1)$, we have

$$L_{F,p}(1 - k, \omega_F^j) = \zeta^{(p)}(F, 1 - k).$$

The method of proof of the theorem shows more generally that, for all integers $k > 0$, we have

$$L_{F,p}(1 - k, \omega_F^j) = L^{(p)}(F, 1 - k, \omega_F^{j-k}); \tag{2}$$

here $L(F, s, \omega_F^{j-k})$ denotes the *complex L-function* of ω_F^{j-k}, and $L^{(p)}(F, s, \omega_F^{j-k})$ means this complex L-function with the Euler factors of the primes dividing p removed.

There is yet another way of expressing these p-adic L-functions. We note that

$$\Lambda(G) = \mathbb{Z}_p[\Delta'][[\Gamma]], \quad \text{where} \quad \Delta' = \mathrm{Gal}(F(\mu_p)^+/F).$$

Let $e_{\omega_F^j}$ $(j$ even$)$ be the idempotent of ω_F^j in $\mathbb{Z}_p[\Delta']$. Then

$$\mathbb{Z}_p[\Delta'] = \bigoplus_{\substack{j \bmod \delta \\ j \text{ even}}} e_{\omega_F^j} \mathbb{Z}_p[\Delta'],$$

and evaluation at w_F^j defines a $\mathbb{Z}_p$-isomorphism from $e_{\omega_F^j}\mathbb{Z}_p[\Delta']$ to $\mathbb{Z}_p$. Thus there is a canonical decomposition

$$\Lambda(G) \simeq \bigoplus_{\substack{j \bmod \delta \\ j \text{ even}}} \Lambda(\Gamma).$$

Now fix a topological generator γ of Γ. There is a unique $\mathbb{Z}_p$-algebra isomorphism from $\Lambda(\Gamma)$ onto $\mathbb{Z}_p[[T]]$ which maps γ to $1 + T$. Define

$$u = \chi_F(\gamma).$$

Hence the theorem of Cassou-Noguès–Deligne–Ribet can be stated as follows.

Theorem 2.4. *For each even integer j mod δ, there exists $W_{\omega_F^j}(T)$ in $\mathbb{Z}_p[[T]]$ such that*

$$L_{F,p}(s, \omega_F^j) = \begin{cases} W_{\omega_F^j}(u^s - 1) \text{ if } j \not\equiv 0 \bmod \delta \\ (W_{\omega_F^j}(u^s - 1))/(u^{1-s} - 1) \text{ if } j \equiv 0 \bmod \delta. \end{cases}$$

3. Statement of the "Main Conjecture"

We now give the statement of the "main conjecture" (Wiles' theorem) in various equivalent forms, but just for the even powers of ω_F. It turns out to be natural to consider two arithmetic $\mathcal{G}$-modules when one formulates this main conjecture. First, let M_∞ be the maximal abelian p-extension of F_∞, which is unramified outside the primes of F above p. Put

$$Y_\infty = \mathrm{Gal}(M_\infty/F_\infty). \tag{3}$$

Then Y_∞ is a compact $\mathbb{Z}_p$-module, which can be endowed with a continuous action of $G = \mathrm{Gal}(F_\infty/F)$ by defining $\sigma(y) = \tilde{\sigma} y \tilde{\sigma}^{-1}, \sigma \in G, y \in Y_\infty$), where $\tilde{\sigma}$ denotes any lifting of σ to $\mathrm{Gal}(M_\infty/F)$. This G-action extends by linearity and continuity to an action of the Iwasawa algebra $\Lambda(G)$. It is easy to see that Y_∞ is finitely generated over $\Lambda(G)$. A module N over $\Lambda(G)$ is said to be $\Lambda(G)$-torsion if every element of N is annihilated by a non-zero divisor in $\Lambda(G)$.

Theorem 3.1 (Iwasawa [8]). *The module Y_∞ is $\Lambda(G)$-torsion.*

For the second module, let $\mathcal{L}_\infty$ be the maximal unramified abelian p-extension of $\mathcal{F}_\infty = F(\mu_{p^\infty})$, and put

$$X_\infty = \mathrm{Gal}(\mathcal{L}_\infty/\mathcal{F}_\infty). \tag{4}$$

Analogously, X_∞ is also a module over the Iwasawa algebra $\Lambda(\mathcal{G})$. It is finitely generated over $\Lambda(\mathcal{G})$, and we have:

Theorem 3.2 (Iwasawa). *The module X_∞ is $\Lambda(\mathcal{G})$-torsion.*

Since p is odd, we can decompose X_∞ as

$$X_\infty = X_\infty^+ \oplus X_\infty^-,$$

where X_∞^ϵ ($\epsilon = \pm 1$) denotes the submodule of X_∞ on which the complex conjugation in $\mathcal{G}$ acts by ϵ. Very little is known about X_∞^+ (Greenberg has conjectured that X_∞^+ is finite for all F and all p, but no progress has been made towards the proof). However, there is a well-known connexion between the $\Lambda(\mathcal{G})$-modules Y_∞ and X_∞^-. If V is any $\Lambda(\mathcal{G})$-module, then we can change the action of $\mathcal{G}$ as follows. Firstly, we can define the new action of $\mathcal{G}$ by inverting the old action, i.e. defining $\sigma^{-1}(m)$ to be the new action of σ in $\mathcal{G}$ on m in V. We denote this new $\Lambda(\mathcal{G})$-module by $V^\bullet$. Secondly, we can twist by the inverse of the cyclotomic character, i.e. taking the new action of σ on m to be $\chi_F(\sigma)^{-1}\sigma(m)$. We denote this new $\Lambda(\mathcal{G})$-module by $V(-1)$. The proof of the following theorem uses both Kummer theory and the fact that all primes of F above p are ramified in F^{cyc}.

Theorem 3.3. *There is a $\Lambda(\mathcal{G})$-homomorphism from $(X_\infty^-)^\bullet$ to $Y_\infty(-1)$, with finite kernel and cokernel.*

Thanks to this theorem, we can state the "main conjecture" in two equivalent forms. As $G = \Delta' \times \Gamma$, where Δ' is cyclic of order dividing $p - 1$, there is a classical structure theory for finitely generated torsion $\Lambda(G)$-modules (cf. [2], [4, Appendix]). It asserts that, if V is any finitely generated torsion $\Lambda(G)$-module, there exists an exact sequence of $\Lambda(G)$-modules

$$0 \to \bigoplus_{i=1}^{r} \Lambda(G)/f_i\Lambda(G) \to V \to D \to 0,$$

where $f_1, \ldots, f_r$ are non-zero divisors in $\Lambda(G)$, and D is finite. Note that the map on the left is injective because the module $\oplus_{i=1}^{r} \Lambda(G)/f_i\Lambda(G)$ has no non-zero finite $\Lambda(G)$-submodule. We then define the *characteristic ideal* $\mathrm{char}_G(V)$ of V by:

$$\mathrm{char}_G(V) = f_1 \ldots f_r\Lambda(G).$$

The kernel of the augmentation homomorphism $\Lambda(G) \to \mathbb{Z}_p$ is denoted by $I(G)$.

Theorem 3.4 ("Main Conjecture"-first version). *We have*

$$\mathrm{char}_G(Y_\infty) = \mu_{F,p}\, I(G),$$

where $\mu_{F,p}$ is the Deligne-Ribet–Cassou–Noguès pseudo-measure on G.

For the second version, we break the modules Y_∞ and X_∞ into eigenspaces for the action of $\Delta = \mathrm{Gal}(F(\mu_p)/F)$. If V is any $\Lambda(\mathcal{G})$-module, then we can decompose it as

$$V = \bigoplus_{j \bmod \delta} V^{(j)}, \quad \text{where} \quad V^{(j)} = e_{\omega_F^j}\, V.$$

We view each $V^{(j)}$ separately as a $\Lambda(\Gamma)$-module. Recall that we have fixed a topological generator γ of Γ, which gives rise to an isomorphism of rings

$$\Lambda(\Gamma) \simeq \mathbb{Z}_p[[T]].$$

Analogously to the above, we can define the characteristic ideal $\mathrm{char}_\Gamma(M)$ of any finitely generated torsion $\Lambda(\Gamma)$-module M. We recall that $W_{\omega_F^j}$ denotes the power series in $\mathbb{Z}_p[[T]]$ which gives the p-adic L-function $L_{F,p}(s, \omega_F^j)$ as explained in the last result of §2.

Theorem 3.5 ("Main Conjecture"-second version). *Let i be any odd integer mod δ. Then*

$$\mathrm{char}_\Gamma(X_\infty^{(-i)}) = W_{\omega_F^{i+1}}(T)\,\mathbb{Z}_p[[T]]. \tag{5}$$

To prove the equivalence of the two versions, we note that if $H_i(T)$ is a generator of the characteristic ideal of $X_\infty^{(-i)}$ (i odd), then $H_i(u(1+T)^{-1} - 1)$ is a generator of the characteristic ideal of $Y_\infty^{(i+1)}$.

4. Overview of the proof of the main conjecture when $F = \mathbb{Q}$

In the remainder of these notes, we shall explain Wiles' proof of Theorem 3.5, but only in the special case when $F = \mathbb{Q}$. It is fair to say that the principles of the proof remain the same for an arbitrary totally real field F. Nevertheless, there are dramatic simplifications which occur when $F = \mathbb{Q}$ (for example Lemma 4.1 below does not have an elementary proof for fields other than $\mathbb{Q}$, nor do we know for such fields the analogue of the Ferrero-Washington theorem nor Leopoldt's conjecture). Also, for $F = \mathbb{Q}$, we need only work with elliptic modular forms rather than Hilbert modular forms.

We assume from now on that $F = \mathbb{Q}$, so that $\delta = p - 1$. We also simply write χ and ω rather than $\chi_\mathbb{Q}$ and $\omega_\mathbb{Q}$. Moreover, we choose γ to be the unique topological generator of Γ such that $\chi(\gamma) = 1 + p$. We have the classical formula

$$\zeta(\mathbb{Q}, 1 - k) = -B_k/k \quad (k = 2, 4, 6 \ldots)$$

where the Bernoulli numbers are defined by the expansion

$$t/(e^t - 1) = \sum_{n=0}^{\infty} B_n t^n/n!.$$

We begin with a classical lemma, which enables us to discard two eigenspaces in the proof of Theorem 3.5 (and these eigenspaces cause technical difficulties in Wiles' proof).

Lemma 4.1. *If $i \equiv \pm 1 \bmod (p-1)$, we have that $X_\infty^{(-i)} = 0$ and $W_{\omega^i}(T)$ is a unit in $\mathbb{Z}_p[[T]]$. Thus the assertion (5) holds for these two eigenspaces.*

Proof. We first consider the case when $i \equiv -1 \bmod (p-1)$. The fact that $W_{\omega^0}(T)$ is a unit in $\mathbb{Z}_p[[T]]$ can be seen, for example, using the classical von Staudt Clausen theorem, which asserts that $\mathrm{ord}_p(B_{p-1}) = -1$. Then

$$W_{\omega^0}((1+p)^{2-p} - 1) = (1+p)^{p-1} - 1) \times L_{\mathbb{Q},p}(2 - p, \omega^0) = \frac{B_{p-1}}{p-1}(1 - p^{p-2}).$$

Since $\text{ord}_p((1+p)^{p-1} - 1) = 1$, it follows that $W_{\omega^0}((1+p)^{2-p} - 1)$ is a p-adic unit, and hence $W_{\omega^0}(T)$ is a unit in $\mathbb{Z}_p[[T]]$. On the other hand, class field theory for $\mathbb{Q}$ proves that $\mathbb{Q}^{\text{cyc}}$ is the maximal abelian p-extension of $\mathbb{Q}$ unramified outside p, whence it follows easily that $Y_\infty^0 = 0$, where Y_∞ is given by (3) above. Since Y_∞ is pseudo-isomorphic to $(X_\infty)^\bullet(1)$ by Theorem 3.3, we conclude that $X_\infty^{(1)}$ is finite. In fact, it is well-known that X_∞^- has no non-zero finite Γ-submodule, and so it follows that $X_\infty^{(1)} = 0$. Next assume that $i \equiv 1 \bmod (p-1)$, and that $p \neq 3$. Then $\omega^2 \neq \omega^0$, and we have

$$W_{\omega^2}((1+p)^{-1} - 1) = L_{\mathbb{Q},p}(-1, \omega^2) = \frac{-B_2}{2}(1-p).$$

Since $B_2 = 1/6$, we see that $W_{\omega^2}((1+p)^{-1} - 1)$ is a p-adic unit, and so $W_{\omega^2}(T)$ is a unit in $\mathbb{Z}_p[[T]]$. On the other hand, a classical argument in Iwasawa theory shows that

$$(X_\infty^{(-1)})_\Gamma = \mathcal{C}^{(-1)}, \tag{6}$$

where $\mathcal{C}$ denotes the p-primary subgroup of the class group of $\mathbb{Q}(\mu_p)$. Then, using Nakayama's lemma, it will follow from (6), that $X_\infty^{(-1)} = 0$, provided we can show that $\mathcal{C}^{(-1)} = 0$. To prove this last assertion, we note that the classical theorem of Stickelberger shows that $\mathcal{C}^{(-1)}$ is annihilated by $L(\mathbb{Q}, 0, \omega)$. However,

$$L(\mathbb{Q}, 0, \omega) = L_{\mathbb{Q},p}(0, \omega^2) = W_{\omega^2}(0),$$

and this last quantity is a p-adic unit because $W_{\omega^2}(T)$ is a unit in $\mathbb{Z}_p[[T]]$. This completes the proof of the lemma. $\qquad\square$

From now on, i will be an odd integer mod $(p-1)$ satisfying

$$i \not\equiv -1 \bmod (p-1). \tag{7}$$

If d is in $\mathbb{Z}_p^\times$, we write $d = \omega(d)(1+p)^{e_d}$, with e_d in $\mathbb{Z}_p$.

The strategy for proving Theorem 3.5 is as follows. Let $\Lambda = \mathbb{Z}_p[[T]]$ be the ring of formal power series in T with coefficients in $\mathbb{Z}_p$. We recall that the Iwasawa algebra $\Lambda(\Gamma)$ is identified with Λ by mapping our canonical generator γ to $(1+T)$. In view of Lemma 4.1 and the analytic class number formula, it can be shown by a classical argument going back to Iwasawa that it suffices to prove that, for all odd integers $i \bmod p-1$, with $i \not\equiv \pm 1 \bmod p-1$, we have

$$\text{char}_\Gamma(X_\infty^{(-i)}) \subset W_{\omega^{(i+1)}}(T)\Lambda. \tag{8}$$

The proof employs techniques from modular forms to prove this assertion, and we quickly give some indications now of the underlying ideas. Let $\mathcal{E}^{(i)}(T)$ be the element of the formal power series ring $\Lambda[[q]]$, which is defined by

$$\mathcal{E}^{(i)}(T) = A_0^{(i)}(T) + \sum_{n=1}^\infty A_n^{(i)}(T)q^n, \tag{9}$$

where

$$A_0^{(i)}(T) = W_{\omega^{i+1}}((1+T)^{-1} - 1)/2, \quad \text{with} \quad L_{\mathbb{Q},p}(s, \omega^{i+1}) = W_{\omega^{i+1}}((1+p)^s - 1), \tag{10}$$

and

$$A_n^{(i)}(T) = \sum_{\substack{d|n \\ (d,p)=1}} \omega^i(d)(1+T)^{e_d} \quad (n \geq 1);$$

here we are viewing ω as a Dirichlet character modulo p in the usual fashion, and as above, we have written $d = \omega(d)(1 + p)^{e_d}$. This formal power series is the primaeval example of a Hida family (see [7]). For each integer $k \geq 2$, and any integer $j \bmod (p-1)$, let $M_k(p, \omega^j, \mathbb{Z}_p)$ denote the space of classical modular forms of level p, character ω^j, and with coefficients in $\mathbb{Z}_p$. We recall that the Λ-module $M(1, \omega^i, \Lambda)$ of Hida modular forms of level 1, character ω^i, with coefficients in Λ is defined to be the Λ-submodule of $\Lambda[[q]]$ consisting of f such that $\phi_k(f)$ belongs to $M_k(p, \omega^{1+i-k}, \mathbb{Z}_p)$, for all but a finite number of integers $k \geq 2$. Here ϕ_k is the $\mathbb{Z}_p$-algebra homomorphism from $\Lambda[[q]]$ to Λ defined by

$$\phi_k\left(\sum_{n=1}^{\infty} a_n(T)q^n\right) = \sum_{n=1}^{\infty} a_n((1+p)^{k-1} - 1)q^n. \tag{11}$$

For each prime l, we have the Hecke operators T_l in $\text{End}_\Lambda(M(1, \omega^i, \mathbb{Z}_p))$, and also the operators S_l for all l (see [7]). In the next section, we shall give the proof of the following theorem, which is basic for all of our subsequent arguments.

Theorem 4.2. *Assume* (7). *Then* $\mathcal{E}^{(i)}(T)$ *belongs to* $M(1, \omega^i, \Lambda)$. *Moreover, we have* $T_p(\mathcal{E}^{(i)}(T)) = \mathcal{E}^{(i)}(T)$, *and for each prime* $l \neq p$,

$$T_l(\mathcal{E}^{(i)}(T)) = (1 + \omega^i(l)(1+T)^{e_l})\mathcal{E}^{(i)}(T),$$

$$S_l(\mathcal{E}^{(i)}(T)) = \omega^i(l)l^{-1}(1+T)^{e_l}\mathcal{E}^{(i)}(T).$$

We recall that a classical modular form is said to be *ordinary* at p if its p-th Fourier coefficient is a p-adic unit. Let $M^{\text{ord}}(1, \omega^i, \Lambda)$ denote the space of ordinary Λ-adic modular forms of level 1 and character ω^i. By definition, it is the Λ-submodule consisting of all f in $M(1, \omega^i, \Lambda)$ such that $\phi_k(f)$ is a classical ordinary modular form for all but a finite number of integers $k \geq 2$. An important theorem of Hida (see [7]) asserts that $M^{\text{ord}}(1, \omega^i, \Lambda)$ is a free Λ-module of finite rank. Since the Hecke operator T_p fixes $\mathcal{E}^{(i)}(T)$, it follows that $\mathcal{E}^{(i)}(T)$ belongs to $M^{\text{ord}}(1, \omega^i, \Lambda)$, and in view of the above theorem, this leads to the definition of the *Eisenstein ideal*, which plays a central role in Wiles' proof. Let $\mathbb{H}_i$ be the Λ-subalgebra of the endomorphism ring of $M^{\text{ord}}(1, \omega^i, \Lambda)$ which is generated by the identity, the Hecke operators T_l for all primes l, and by the S_l for all primes $l \neq p$.

Definition 4.3. *The Eisenstein ideal* $\mathbb{I}_i$ *is the ideal of* $\mathbb{H}_i$ *generated by* $T_p - 1$ *and* $T_l - 1 - \omega^i(l)(1+T)^{e_l}$, $S_l - \omega^i(l)l^{-1}(1+T)^{e_l}$ *for all primes* $l \neq p$.

It is clear from Theorem 4.2 that $\mathcal{E}^{(i)}(T)$ is annihilated by the Eisenstein ideal $\mathbb{I}_i$.

Although the Eisenstein ideal is an ideal in the Hecke algebra $\mathbb{H}_i$, we need rather to work with the corresponding Hecke algebra for the ordinary Λ-adic cusp forms. Recall that $S(1, \omega^i, \Lambda)$ denotes the Λ-submodule of $M(1, \omega^i, \Lambda)$ consisting of all f such that, for all but a finite number of integers $k \geq 2$, $\phi_k(f)$ belongs to the space $S_k(p, \omega^{i+1-k}, \mathbb{Z}_p)$ of classical cusp forms of level p, character ω^{i+1-k}, weight k, and with coefficients in $\mathbb{Z}_p$. Also, define

$$S^{\mathrm{ord}}(1, \omega^i, \Lambda) = S(1, \omega^i, \Lambda) \cap M^{\mathrm{ord}}(1, \omega^i, \Lambda).$$

Then the operators T_l (l any prime) and S_l (l any prime $\neq p$) leave $S^{\mathrm{ord}}(1, \omega^i, \Lambda)$ stable. We can therefore define $\mathbb{T}_i$ to be the Λ-subalgebra of $\mathrm{End}_\Lambda(S^{\mathrm{ord}}(1, \omega^i, \Lambda))$ which is generated by the identity, T_l (for all l) and the S_l (for all $l \neq p$). Moreover, restriction to the subspace $S^{\mathrm{ord}}(1, \omega^i, \Lambda)$ clearly gives a canonical surjection from $\mathbb{H}_i$ onto $\mathbb{T}_i$, which allows us to view $\mathbb{T}_i$ as a $\mathbb{H}_i$-module.

The first key step in the proof of (8) is the following:

Theorem 4.4. *For all odd integers i with $i \not\equiv -1 \bmod (p-1)$, we have*

$$\mathrm{char}_\Lambda(\mathbb{T}_i/\mathbb{I}_i\mathbb{T}_i) \subset A_0^{(i)}(T)\Lambda. \tag{12}$$

To complete the proof of (8), one has to relate the Λ-module $\mathbb{T}_i/\mathbb{I}_i\mathbb{T}_i$ to the Λ-module $X_\infty^{(-i)}$. This is a beautiful and highly non-trivial argument, which seems to have been inspired by Ribet's work [13]. We explain it in some detail in the latter part of these notes. To carry it out, one is forced to enlarge the ring Λ, first by replacing Λ by the ring $\Lambda_\mathcal{O} = \mathcal{O}[[T]]$, where $\mathcal{O}$ is the ring of integers of some finite extension of $\mathbb{Q}_p$, and then by replacing $\Lambda_\mathcal{O}$ by the integral closure R of Λ in some finite extension of the fraction field of $\Lambda_\mathcal{O}$.

5. Eisenstein Families

The proof of Theorem 4.2 is entirely elementary, and we now give it. We continue to assume that i is an odd integer mod $(p-1)$, satisfying (7). Throughout, k will be an integer ≥ 2, and, if $f(T)$ is any element of Λ, we recall that $\phi_k(f) = f((1+p)^{k-1} - 1)$. The Weierstrass preparation theorem in Λ shows that $\phi_k(f) = 0$ for infinitely many integers $k \geq 2$ if and only if $f = 0$.

Put

$$\phi_k(\mathcal{E}^{(i)}(T)) = \sum_{n=0}^{\infty} a_n^{(k)} q^n.$$

From the definition of $\mathcal{E}^{(i)}(T)$, we have

(i) $a_0^{(k)} = \phi_k(A_0^{(i)}(T)) = L_{\mathbb{Q},p}(1-k, \omega^{i+1})/2 = L^{(p)}(\mathbb{Q}, 1-k, \omega^{i+1-k})/2,$ (13)

(ii) $a_n^{(k)} = \phi_k(A_n^{(I)}(T)) = \sum_{\substack{d|n \\ (d,p)=1}} \omega^{i+1-k}(d)d^{k-1} \quad (n \geq 1).$ (14)

We first show that $\mathcal{E}^{(i)}(T)$ belongs to $M(1, \omega^i, \Lambda)$. Suppose first that $\omega^{i+1-k} \neq \mathbf{1}$, or equivalently that ω^{i+1-k} has conductor p. It follows that

$$a_0^{(k)} = 1/2\ L(\mathbb{Q}, 1-k, \omega^{i+1-k}), c a_n^{(k)} = \sum_{d|n} \omega^{i+1-k}(d)d^{k-1} \quad (n \geq 1).$$

Thus $\phi_k(\mathcal{E}^{(i)}(T))$ is the classical Eisenstein series of weight k, level p, and character ω^{i+1-k}. On the other hand, if $\omega^{i+1-k} = \mathbf{1}$, we see that

$$\phi_k(\mathcal{E}^{(i)}(T)) = E_k(z) - p^{k-1}E_k(pz)$$

where E_k is the classical Eisenstein series of weight k and level 1 given by

$$E_k = \zeta(\mathbb{Q}, 1-k)/2 + \sum_{n=1}^{\infty} \left(\sum_{d|n} d^{k-1} \right) q^n. \tag{15}$$

Hence in all cases, $\phi_k(\mathcal{E}^{(i)}(T))$ belongs to $M_k(p, \omega^{i+1-k}, \mathbb{Z}_p)$, and this shows that $\mathcal{E}^{(i)}(T)$ is in $M(1, \omega^i, \Lambda)$.

For simplicity, write T_l for both the classical and Λ-adic Hecke operator attached to a prime number l. To show that $T_p \mathcal{E}^{(i)}(T) = \mathcal{E}^{(i)}(T)$, we must prove that

$$T_p \phi_k(\mathcal{E}^{(i)}(T)) = \phi_k(\mathcal{E}^{(i)}(T))$$

for all integers $k \geq 2$. In other words, we must prove that $a_n^{(k)} = a_{np}^{(k)}$ for all integers $n \geq 1$. But this last equation is obvious from the explicit expression (ii) above for $a_n^{(k)}$ when $n \geq 1$.

Now assume that l is a prime different from p. By the defintion of the Hecke operator T_l, we have

$$T_l(\mathcal{E}^{(i)}(T)) = \sum_{n=0}^{\infty} B_n^{(i)}(T)q^n,$$

where

$$B_n^{(i)}(T) = A_{nl}^{(i)}(T) + \delta_l \omega^i(l)\omega^i(l)(1+T)^{e_l} A_{n/l}^{(i)}(T);$$

here $\delta_l = 0$ or 1, according as $(l, n) = 1$ or $l|n$. Thus, to prove the assertion of Theorem 4.2 for the operator T_l, we must show that, for all $n \geq 0$, we have

$$B_n^{(i)}(T) = (1 + \omega^i(l)(1+T)^{e_l}) A_n^{(i)}(T). \tag{16}$$

This last equation is obvious when $n = 0$, and so we may assume that $n > 0$. Suppose first that $(l, n) = 1$. In view of this last assertion, every positive divisor of nl is of the form j or jl, where j runs over all positive divisors of n. But, by definition, we then have

$$B_n^{(i)}(T) = A_{nl}^{(i)}(T) = \sum_{\substack{j|n \\ (j,p)=1}} \omega^i(j)(1+T)^{e_l} + \sum_{\substack{j|n \\ (j,p)=1}} \omega^i(jl)(1+T)^{e_{jl}}.$$

Since $e_{jl} = e_j + e_l$, the equation (16) follows immediately in this case. Next suppose that $l|n$. Since $\delta_l = 1$ in this case, we see immediately that

$$B_n^{(i)}(T) = \sum_{\substack{d|nl \\ (d,p)=1}} \omega^i(d)(1+T)^{e_d} + \sum_{\substack{jl|n \\ (j,p)=1}} \omega^i(jl)(1+T)^{e_{jl}}.$$

Now we clearly have

$$\sum_{\substack{d|nl \\ (d,p)=1}} \omega^i(d)(1+T)^{e_d} = \sum_{\substack{d_1|n \\ (d_1,p)=1}} \omega^i(d_1)(1+T)^{e_{d_1}} + \sum_{\substack{d_2|n \\ (d_2,p)=1 \\ d_2 \nmid n}} \omega^i(d_2)(1+T)^{e_{d_2}}.$$

Since

$$\sum_{\substack{b|n \\ (b,p)=1}} \omega^i(bl)(1+T)^{e_{bl}} = \sum_{\substack{jl|n \\ (j,p)=1}} \omega^i(jl)(1+T)^{e_{jl}} + \sum_{\substack{d_2|nl \\ (d_2,p)=1 \\ d_2 \nmid n}} \omega^i(d_2)(1+T)^{e_{d_2}},$$

we see that we have again established equation (16). The proof of the final assertion of Theorem 4.2 is straightforward and we omit the details.

6. Ribet's theorem

Our aim in this section is to give a proof of Ribet's theorem, which will serve as an introduction to Wiles' proof [17] of the Main Conjecture (Theorem 3.4).

We continue to assume that our base field $F = \mathbb{Q}$, and we put $K = \mathbb{Q}(\mu_p)$. As earlier, $\Delta = \mathrm{Gal}(K/\mathbb{Q})$, and ω is the character giving the action of Δ on μ_p. Let $\mathcal{C}$ denote the p-primary subgroup of the ideal class group of K. Then, as before, we have the decomposition

$$\mathcal{C} = \bigoplus_{i \bmod (p-1)} \mathcal{C}^{(i)},$$

where $\mathcal{C}^{(i)} = e_{\omega^i}\mathcal{C}$.

Theorem 6.1 (Ribet [13]). *Assume k is an even number with $2 \leq k \leq p - 3$. If an odd prime p divides the numerator of $\zeta(\mathbb{Q}, 1 - k)$, then $\mathcal{C}^{(1-k)} \neq 0$.*

We are grateful to Skinner for communicating to us the following elegant variant of Ribet's original proof. We may assume that $p > 7$, since

$$\zeta(\mathbb{Q}, -1) = -1/12, \quad \zeta(\mathbb{Q}, -3) = 1/120.$$

Also,

$$\zeta(\mathbb{Q}, -5) = -1/252.$$

Hence the classical Eisenstein series E_4 and E_6 (see (15)) have p-adic integral Fourier expansions, with constant terms which are p-adic units. As k is even, we can find integers a, $b \geq 0$ so that $k = 4a + 6b$. Put $g = E_4^a E_6^b$, and define

$$h = E_k - (a_0(g))^{-1}\zeta(\mathbb{Q}, 1 - k)/2)g,$$

where $a_0(g)$ denotes the constant term of the q-expansion of g. In general, if f is any classical modular form, we write $\sum_{n=0}^{\infty} a_n(f)q^n$, for its Fourier expansion.

Since p is assumed to divide the numerator of $\zeta(\mathbb{Q}, 1-k)$, we conclude that

$$a_n(h) \equiv a_n(E_k) \bmod p \ (n \geq 1).$$

In particular, we obtain

$$a_p(h) \equiv 1 + p^{k-1} \equiv 1 \bmod p$$
$$a_l(h) \equiv 1 + l^{k-1} \equiv 1 + \omega^{k-1}(l) \bmod p \quad (l \neq p). \tag{17}$$

Let $S_k^{\mathrm{ord}}(p, \mathbb{Z}_p)$ denote the space of ordinary cusp forms of weight k, level p and coefficients in $\mathbb{Z}_p$. The Hecke operators T_l (l any prime) and S_l (l any prime $\neq p$) leave $S_k^{\mathrm{ord}}(p, \mathbb{Z}_p)$ stable, and we define $\mathbb{T}_{k,p}$ to be the $\mathbb{Z}_p$-subalgebra of $\mathrm{End}_{\mathbb{Z}_p}(S_k^{\mathrm{ord}}(p, \mathbb{Z}_p))$ generated by these operators and the identity endomorphism. Since $S_k^{\mathrm{ord}}(p, \mathbb{Z}_p)$ is a free $\mathbb{Z}_p$-module of finite rank, $\mathbb{T}_k$ is also a free $\mathbb{Z}_p$-module of finite rank. If t is in $\mathbb{T}_{k,p}$, we shall follow classical notation and write $f|t$ for the image under t of an element f of $S_k^{\mathrm{ord}}(p, \mathbb{Z}_p)$. We now define a $\mathbb{Z}_p$-algebra homomorphism

$$\pi_k : \mathbb{T}_{k,p} \to \mathbb{F}_p$$

by

$$\pi_k(t) = a_1(h|t) \bmod p. \tag{18}$$

Let $\mathcal{M} = \mathrm{Ker}\,(\pi_k)$. Since (17) shows that, for all primes $l \neq p$, we have

$$\pi_k(T_l) \equiv a_l(h) \equiv 1 + \omega^{k-1}(l) \bmod p, \tag{19}$$

we see immediately that, for all $l \neq p$,

$$T_l - 1 - \omega^{k-1}(l) \in \mathcal{M}. \tag{20}$$

Take $\mathfrak{p}$ to be any minimal prime of $\mathbb{T}_{k,p}$ which is contained in $\mathcal{M}$. Since $\mathbb{T}_{k,p}/\mathfrak{p}$ is a commutative ring that is free of finite rank as a $\mathbb{Z}_p$-module, it has Krull dimension 1. We can therefore find an injective ring homomorphisn

$$\psi : \mathbb{T}_{k,p}/\mathfrak{p} \hookrightarrow \bar{\mathbb{Q}}_p.$$

Write $\mathcal{O}$ for the ring of integers of the field of fractions of the image of ψ. Clearly $\mathcal{O}$ has Krull dimension one as $\mathfrak{p}$ is minimal. By the duality between Hecke algebras and modular forms (see for example, [1, 6.5]), it is a classical result (see [6, pp. 325–328]) that the element $\psi \in \mathrm{Hom}_{\mathcal{O}}(\mathbb{T}_{k,p}/\mathfrak{p}, \mathcal{O})$ corresponds to a primitive eigenform $f \in S_k^{\mathrm{ord}}(p, \mathcal{O})$ such that

$$T_l(f) = a_l(f) \cdot f$$

where $a_l(f) = \psi(T_l)$ for all primes l. On the other hand, if π is a uniformiser of $\mathcal{O}$, then

$$a_l(f) \equiv 1 + \omega^{k-1}(l) \bmod \pi, \ l \neq p, \quad \text{and} \quad a_p(f) \equiv 1 \bmod \pi. \tag{21}$$

Since f is a primitive eigenform, there is an associated irreducible Galois representation (see [1, §6])

$$\rho = \rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(K)$$

where K is the fraction field of $\mathcal{O}$. Choosing a lattice stable under $G_{\mathbb{Q}}$, we may assume that

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}).$$

Let D_p denote the decomposition group at p. By the hypothesis that f is ordinary, we have (see [11])

$$\rho_{|D_p} \simeq \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}.$$

where ψ_2 is an unramified character with $\psi_2(\mathrm{Frob}_p) = a_p(f)$, and Frob_p is the Frobenius at p. By conjugating with the element $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we may write

$$\rho_{|D_p} = \begin{pmatrix} \psi_2 & 0 \\ * & \psi_1 \end{pmatrix}. \tag{22}$$

Further, as ρ is unramified outside p, we have

$$\det(\rho(\mathrm{Frob}_l)) = l^{k-1}, \ \ l \neq p,$$

and hence

$$\det(\rho) = \chi^{k-1},$$

where, as before, $\chi = \chi_{\mathbb{Q}}$ is the cyclotomic character. Thus, as $\psi_{2_{|I_p}} = 1$, we have

$$\psi_{1_{|I_p}} = \det \rho_{|I_p} = \chi_{|I_p}^{k-1}.$$

But $\omega = \chi \bmod \pi$, and hence

$$\psi_{1_{|I_p}} \equiv \omega^{k-1} \bmod \pi, \ \text{ and } \omega^{k-1} \not\equiv 1 \bmod \pi \text{ as } k \text{ is even.}$$

We therefore conclude that there exists an element $\sigma_0 \in I_p$ such that $\psi_2(\sigma_0) = 1$ and $\psi_1(\sigma_0) = \alpha$, with $\alpha \in \mathcal{O}^\times$ and $\alpha \not\equiv 1 \bmod \pi$. As $\rho(\sigma_0)$ has distinct eigenvalues 1 and α, we can choose a new $\mathcal{O}$-basis for the representation ρ such that (22) remains valid and we have

$$\rho(\sigma_0) = \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}, \tag{23}$$

For σ in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, write

$$\rho(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}.$$

By (22), we have $b_\sigma = 0$ for σ in I_p, and as ρ is unramified outside p, $b_\sigma = 0$ for σ in I_l ($l \neq p$). Further, as ρ is irreducible, there exists an element τ in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$

such that $b_\tau \neq 0$. Let τ_0 be an element in $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ with the property that $\text{ord}_\pi(b_{\tau_0})$ is minimal among all such choices of τ, and put $n = \text{ord}_\pi(b_{\tau_0})$. Replacing ρ by

$$\begin{pmatrix} 1 & 0 \\ 0 & \pi^n \end{pmatrix} \rho \begin{pmatrix} 1 & 0 \\ 0 & \pi^{-n} \end{pmatrix},$$

we may assume that $n = 0$, in other words, that b_{τ_0} belongs to $\mathcal{O}^\times$. Put $\mathbb{F} = \mathcal{O}/\pi\mathcal{O}$ and let

$$\bar{\rho} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{F})$$

be the residual representation of $\rho \bmod \pi$. By (21), we have

$$\text{Trace}(\bar{\rho}) = 1 + \omega^{k-1}; \quad \det(\bar{\rho}) = \omega^{k-1}. \tag{24}$$

Let $\bar{\rho}^{\text{ss}}$ be the semi-simplification of the residual representation $\bar{\rho}$. Since $\bar{\rho}^{\text{ss}}$ and $\mathbf{1} \oplus \omega^{k-1}$ are two semi-simple representations over $\mathbb{F}$ with the same characteristic polynomials, thanks to (24), we conclude from the Brauer-Nesbitt theorem, that

$$\bar{\rho}^{\text{ss}} = \mathbf{1} \oplus \omega^{k-1}.$$

From (22) and (23), and the fact that ω^{k-1} is ramified at p, we conclude that $\bar{\rho}$ is of the form

$$\begin{pmatrix} 1 & 0 \\ 0 & \omega^{k-1} \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ * & \omega^{k-1} \end{pmatrix}, \quad \text{or} \quad \begin{pmatrix} 1 & * \\ 0 & \omega^{k-1} \end{pmatrix}, \tag{25}$$

with the second two possibilities non-split. From the non-vanishing of $\bar{b}_{\tau_0}$, we see that it must be the third possibility. In other words, we have

$$\bar{\rho}(\sigma) = \begin{pmatrix} 1 & \bar{b}_\sigma \\ 0 & \omega^i(\sigma) \end{pmatrix}$$

for all σ in $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Let $\mathbb{F}(\omega^{1-k})$ denote the $\mathbb{F}$-vector space of dimension one on which $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts via the character ω^{1-k}. Define a map h in $H^1(G_\mathbb{Q}, \mathbb{F}(\omega^{1-k}))$ by

$$h : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}(\omega^{1-k})$$

$$\sigma \mapsto \omega^{1-k}(\sigma)\bar{b}_\sigma.$$

As

$$b_{\sigma\tau} = b_\tau + b_\sigma \omega^{k-1}(\tau),$$

it follows that h is a 1-cocycle on $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ with values in $\mathbb{F}(\omega^{1-k})$. Moreover, h is an unramified cocycle because $b_\sigma = 0$ for all σ in I_p, and also in I_l, for all $l \neq p$ any prime, because the representation ρ is unramified outside p. Thus we obtain an unramified 1-cocycle in $\bar{h}$ in $H^1(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}, \mathbb{F}(\omega^{1-k}))$. On the other hand, as $\Delta = \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ has order prime to p, we see that

$$H^1(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}, \mathbb{F}(\omega^{1-k})) = \text{Hom}_\Delta(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\mu_p)), \mathbb{F}(\omega^{1-k})).$$

Moreover, as $\bar{b}_{\tau_0}$ is not zero, it is plain that $\bar{h}$ is non-zero. Hence, by class field theory, we must have $\text{Hom}_\Delta(\mathcal{C}^{(1-k)}, \mathbb{F}(\omega^{1-k}))$ is not equal to zero. Thus $\mathcal{C}^{(1-k)} \neq 0$, thereby proving Ribet's theorem. □

7. Λ-adic setting for the main conjecture

The aim of this section is to prove Theorem 4.4, and thus we fix for the rest of this section an odd integer i with $i \not\equiv -1 \bmod (p-1)$.

Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$, and $\Lambda_{\mathcal{O}}$ the ring of formal power series in T with coefficients in $\mathcal{O}$. We can then consider the spaces $\mathrm{M}^{\mathrm{ord}}(1, \omega^i, \Lambda_{\mathcal{O}}) \supseteq \mathrm{S}^{\mathrm{ord}}(1, \omega^i, \Lambda_{\mathcal{O}})$, and define the objects $\mathbb{H}_i$, $\mathbb{T}_i$, $\mathbb{I}_i$ made with Λ replaced by $\Lambda_{\mathcal{O}}$. It is then very easy to see that it suffices to prove the assertion in Theorem 4.4 with Λ replaced by $\Lambda_{\mathcal{O}}$. Thus, from now on, we shall work with the objects formed with $\Lambda_{\mathcal{O}}$, with $\mathcal{O}$ sufficiently large.

We must invoke the Ferrero-Washington theorem, which asserts that p does not divide the power series $A_0^{(i)}(T)$. Thus, taking $\mathcal{O}$ sufficiently large, we can write

$$A_0^{(i)}(T) = \prod_{r=1}^{n_i} (T - \alpha_j^{(i)}) B_0^{(i)}(T),$$

where all of the roots $\alpha_j^{(i)}$ belong to $\mathcal{O}$, and $B_0^{(i)}(T)$ is a unit in $\Lambda_{\mathcal{O}}$. Choose an integer $m > 0$ with $m \equiv 0 \bmod (p-1)$ such that

$$\{\alpha_j^{(i)} : j = 1, \ldots, n_i\} \cap \{(\alpha_j^{(i)} + 1)(1+p)^m - 1 : j = 1, \ldots, n_i\} = \emptyset. \qquad (26)$$

We now define

$$H = \mathcal{E}^{(i)}((1+T)(1+p)^{-m} - 1) \cdot E_m.$$

Put

$$H = \sum_{n=0}^{\infty} a_0(H) q^n.$$

Lemma 7.1. *H belongs to* $\mathrm{M}(1, \omega^i, \Lambda_{\mathcal{O}})$. *Moreover, the formal power series* $a_0(H)$ *has no zero in common with* $A_0^{(i)}(T)$.

Proof. We deduce from (9) with $i = 1$ that

$$a_0(H) = A_0^{(i)}((1+T)(1+p)^{-m} - 1) \cdot \zeta(\mathbb{Q}, 1 - m)/2,$$

and conclude from (26) that $a_0(H)$ has no zero in common with $A_0^{(i)}(T)$.

Since $\omega^m = 1$, we see immediately that $\phi_k(H)$ belongs to $\mathrm{M}_k(p, \omega^{i+1-k}, \mathbb{Z}_p)$ for all sufficiently large integers k. Thus H belongs to $\mathrm{M}(1, \omega^i, \Lambda_{\mathcal{O}})$ and the proof of the lemma is complete. $\qquad \square$

Recall the Hida operator $\mathfrak{e}$ on $\mathrm{M}(1, \omega^i, \Lambda_{\mathcal{O}})$ defined by the formula

$$\mathfrak{e} = \lim_{n \to \infty} \mathrm{T}_p^{n!}. \qquad (27)$$

where T_p is now the Hecke operator of p on $\mathrm{M}(1, \omega^i, \Lambda_{\mathcal{O}})$. We have [7]

$$\mathrm{M}^{\mathrm{ord}}(1, \omega^i, \Lambda_{\mathcal{O}}) = \mathfrak{e}\mathrm{M}(1, \omega^i, \Lambda_{\mathcal{O}}), \quad \mathrm{S}^{\mathrm{ord}}(1, \omega^i, \Lambda_{\mathcal{O}}) = \mathfrak{e}\mathrm{S}(1, \omega^i, \Lambda_{\mathcal{O}}).$$

We then make the crucial definition

$$H' = \mathfrak{e}\,(a_0(H)\mathcal{E}^{(i)} - A_0^{(i)}H), \qquad (28)$$

so that H' belongs to $\mathrm{M}^{\mathrm{ord}}(1, \omega^i, \Lambda_{\mathcal{O}})$.

Lemma 7.2. *In fact, H' belongs to $\mathrm{S}^{\mathrm{ord}}(1, \omega^i, \Lambda_{\mathcal{O}})$.*

Proof. By construction $a_0(H') = 0$. The assertion then follows from a general theorem of Wiles (see [16] and [1, §7]). $\qquad\square$

Now let $\mathfrak{p} = (T - \alpha_j^{(i)})\Lambda_{\mathcal{O}}$ for some j, and put $m = \mathrm{ord}_{\mathfrak{p}}(A_0^{(i)}(T))$. It follows from Lemma 7.1 that $\mathrm{ord}_{\mathfrak{p}}(a_0(H)) = 0$, or equivalently that $a_0(H)^{-1}$ belongs to $\Lambda_{\mathcal{O},\mathfrak{p}}$, the localisation of $\Lambda_{\mathcal{O}}$ at $\mathfrak{p}$. The Hecke algebra

$$\mathbb{T}_{i,\mathfrak{p}} = \mathbb{T}_i \otimes_{\Lambda_{\mathcal{O}}} \Lambda_{\mathcal{O},\mathfrak{p}}$$

acts on

$$\mathrm{S}^{\mathrm{ord}}(1, \omega^i, \Lambda_{\mathcal{O}}) \otimes_{\Lambda_{\mathcal{O}}} \Lambda_{\mathcal{O},\mathfrak{p}},$$

and we define the $\Lambda_{\mathcal{O},\mathfrak{p}}$-homomorphism

$$\Pi_i : \mathbb{T}_{i,\mathfrak{p}} \to \Lambda_{\mathcal{O},\mathfrak{p}}/\mathfrak{p}^m$$

by

$$\Pi_i(t) = a_0(H)^{-1} \cdot a_1(H'|t) \bmod \mathfrak{p}^m.$$

Lemma 7.3. *We have $\Pi_i(t) = a_1(\mathcal{E}^{(i)}|t) \bmod \mathfrak{p}^m$. In particular $\mathbb{I}_i$ is contained in the kernel of Π_i. Also, Π_i is surjective.*

Proof. We have $\mathfrak{e}\,\mathcal{E}^{(i)} = \mathcal{E}^{(i)}$, and so

$$H' = a_0(H)\mathcal{E}^{(i)} - A_0^{(i)}\,\mathfrak{e}\,H.$$

Thus

$$H'|t = a_0(H)(\mathcal{E}^{(i)}|t) - A_0^{(i)}(\mathfrak{e}\,H|t).$$

Since $A_0^{(i)} \cdot \Lambda_{\mathcal{O}} = \mathfrak{p}^m$, the first assertion of the lemma follows. The second assertion is then clear because $\mathbb{I}_i$ annihilates $\mathcal{E}^{(i)}$. Finally, the surjectivity of Π_i is plain because $\mathbb{T}_i$ contains the identity endomorphism. $\qquad\square$

In view of the above lemma, we see that there is a surjective homomorphism

$$\mathbb{T}_{i,\mathfrak{p}}/\mathbb{I}_i\mathbb{T}_{i,\mathfrak{p}} \to \Lambda_{\mathcal{O},\mathfrak{p}}/\mathfrak{p}^m.$$

As this is true for every root of $A_0^{(i)}(T)$, it follows that

$$\mathrm{char}_{\Lambda_{\mathcal{O}}}(\mathbb{T}_i/\mathbb{I}_i\mathbb{T}_i) \subseteq A_0^{(i)}(T)\Lambda_{\mathcal{O}}.$$

This completes the proof of Theorem 4.4. $\qquad\square$

8. First part of the proof of the main conjecture

We continue to assume that i is an odd integer with $i \not\equiv -1 \bmod (p-1)$. Recall that our goal is to prove that

$$\mathrm{char}_\Lambda(X_\infty^{(-i)}) \subset A_0^{(i)}((1+T)^{-1} - 1)\Lambda, \tag{29}$$

since, as remarked earlier (see Lemma 4.1, (8) and (10)), this implies the main conjecture (Theorem 3.5) by a classical argument due to Iwasawa [9].

In order to carry out our subsequent arguments, we have to enlarge the ring $\Lambda_\mathcal{O}$. The reason for this is the following. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ be the minimal prime ideals of the Hecke algebra $\mathbb{T}_i$ defined using $\Lambda_\mathcal{O}$. By a theorem of Hida [7, Theorem 7, Chap. 7, p. 221], all of the quotient rings $\mathbb{T}_1/\mathfrak{q}_j$ $(j = 1, \ldots, s)$ are contained in the integral closure R of $\Lambda_\mathcal{O}$ in a suitable finite extension of the quotient field of $\Lambda_\mathcal{O}$. We shall henceforth consider the spaces

$$\mathrm{M}^{\mathrm{ord}}(1, \omega^i, R) \supseteq \mathrm{S}^{\mathrm{ord}}(1, \omega^i, R),$$

and the endomorphism algebras $\mathbb{H}_i$, $\mathbb{T}_i$, and the Eisenstein ideal $\mathbb{I}_i$, made by replacing $\Lambda_\mathcal{O}$ by the ring R. It follows that for this new Hecke algebra $\mathbb{T}_i$ with respect to the ring R, we have ring isomorphisms

$$\eta_j : \mathbb{T}_i/\mathfrak{q}_j \simeq R \quad (1 \leq j \leq s) \tag{30}$$

for every minimal prime ideal $\mathfrak{q}_j$ of $\mathbb{T}_i$. By the usual duality (see [7, Theorem 5, Chap. 7]), there then exists unique normalized ordinary eigenforms

$$f_j = \sum_{k=1}^{\infty} c_k(f_j)\, q^k \ (1 \leq j \leq s),$$

whose Fourier coefficients $c_k(f_j)$ $(k \geq 1)$ are in R, such that

$$\eta_j(\mathrm{T}_l) = c_l(f_j) \tag{31}$$

for all prime numbers l. We remark that each homomorphism ϕ_k on $\Lambda_\mathcal{O}$ has a finite number of extensions to the ring R, and each of the f_j's can be specialised under all these extensions to classical modular forms [7].

It is clear from the definition of the Eisenstein ideal that there is a natural surjection as R-algebras from R onto $\mathbb{T}_i/\mathbb{I}_i\mathbb{T}_i$, giving rise to an isomorphism

$$\lambda_i : R/J_i \simeq \mathbb{T}_i/\mathbb{I}_i\mathbb{T}_i \tag{32}$$

for some ideal J_i of R. We now fix for the rest of this section a prime ideal $\mathcal{P}$ of height one in R. Exactly the same arguments as those used to prove Theorem 4.4 show that again we have

$$\mathrm{ord}_\mathcal{P}(\mathrm{char}_R(\mathbb{T}_i/\mathbb{I}_i\mathbb{T}_i)) \geq \mathrm{ord}_\mathcal{P}(A_0^{(i)}(T)); \tag{33}$$

here for any finitely generated torsion R-module M, $\mathrm{char}_R(M)$ denotes its characteristic ideal.

The next important step in the proof of the main conjecture is to relate

$$\mathrm{ord}_{\mathcal{P}}(\mathrm{char}_R(R/J_i)) = \mathrm{ord}_{\mathcal{P}}(\mathrm{char}_R(\mathbb{T}_i/\mathbb{I}_i\mathbb{T}_i)) \tag{34}$$

to $\mathrm{char}_R(X_\infty^{(-i)} \otimes_\Lambda R)$ by an elaboration to the R-adic setting of Ribet's arguments, as set out in §6. First, we note that we may assume from now on that

$$\mathrm{ord}_{\mathcal{P}}(A_0^{(i)}) > 0,$$

since otherwise there is nothing to prove in (29). In view of (32), it follows that $\mathcal{P} \supset J_i$.

Put

$$\mathbb{T}_{i,\mathcal{P}} = \mathbb{T}_i \otimes_R R_{\mathcal{P}},$$

where $R_{\mathcal{P}}$ is the localization of R at $\mathcal{P}$. Write $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ for the minimal prime ideals of the localized Hecke algebra $\mathbb{T}_{i,\mathcal{P}}$. By a result of Hida [7, Theorem 4, Chap. 7], the algebra $\mathbb{T}_i$, and therefore also its localization $\mathbb{T}_{i,\mathcal{P}}$ has no nilpotent elements. Thus the natural R-algebra map

$$\mathbb{T}_{i,\mathcal{P}} \to \prod_{j=1}^{n} \mathbb{T}_{i,\mathcal{P}}/\mathfrak{q}_j \simeq \prod_{j=1}^{n} R_{\mathcal{P}} \tag{35}$$

is injective. Note also that $R_{\mathcal{P}}$ is an integrally closed, local, Noetherian domain of Krull dimension one, and hence is a discrete valuation ring.

Let us suppose that the indices are chosen so that the normalized ordinary eigenforms $f_1, \ldots, f_n$ correspond via (31) to those minimal prime ideals of $\mathbb{T}_i$ which, via localization give $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ in $\mathbb{T}_{i,\mathcal{P}}$. Thanks to Hida (see [7, §7.5, Chap. 7]), there exist irreducible Galois representations

$$\rho_j : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(V_j), \ (j \leq 1 \leq n) \tag{36}$$

where the V_j are vector spaces of dimension two over the fraction field of R, such that ρ_j is unramified outside of p and

$$\mathrm{Trace}\, \rho_j(\mathrm{Frob}_l) = c_l(f_j) \quad (l \neq p). \tag{37}$$

Moreover, we have

$$\det \rho_j = \theta_i,$$

where

$$\theta_i : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to R^\times$$

is the unique homomorphism which factors through the quotient $\Delta \times \Gamma$, and is defined on this quotient by

$$\theta_{i|_\Delta} = \omega^i, \quad \theta_i(\gamma) = 1 + T, \tag{38}$$

where, as before, γ is our fixed topological generator of Γ.

Let D_p denote the decomposition group of a fixed prime of $\bar{\mathbb{Q}}$ above p and I_p its inertial subgroup. Since $f_1, \ldots, f_n$ are ordinary eigenforms, a theorem of Wiles [16]

asserts that we can find an $R_{\mathcal{P}}$-basis of M_j such that the restriction of ρ_j to D_p relative to this basis is of the form

$$\rho_{j|D_p} = \begin{pmatrix} \Psi_1^{(j)} & * \\ 0 & \Psi_2^{(j)} \end{pmatrix}$$

where $\Psi_i^{(j)}$ and $\Psi_2^{(j)}$ are homomorphisms from D_p to $R_{\mathcal{P}}^{\times}$, with $\Psi_2^{(j)}|_{I_p} = \mathbf{1}$. Conjugating by the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we may assume that

$$\rho_{j|D_p} = \begin{pmatrix} \Psi_2^{(j)} & 0 \\ * & \Psi_1^{(j)} \end{pmatrix}. \tag{39}$$

We make one further modification of our $R_{\mathcal{P}}$-basis of M_j. Since p is totally ramified in $\mathbb{Q}(\mu_{p^\infty})$, we can fix a lifting $\tilde{\gamma}$ of γ to I_p whose image in Δ is trivial. As $\Psi_2^{(j)}(\tilde{\gamma}) = 1$, and

$$\Psi_2^{(j)}\Psi_1^{(j)} = \det \rho_{j|D_p} = \theta_{i|D_p},$$

we obtain $\Psi_1^{(j)}(\tilde{\gamma}) = 1 + T$. Since $\rho_j(\tilde{\gamma})$ has the distinct eigenvalues 1 and $1 + T$, it is easy to see that we can choose a new basis of M_j such that (39) still remains true and, in addition,

$$\rho_j(\tilde{\gamma}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 + T \end{pmatrix}. \tag{40}$$

Let w_j be the basis element of M_j, such that

$$\rho_j(\tilde{\gamma})w_j = (1 + T)w_j. \tag{41}$$

Define

$$V = \bigoplus_{j=1}^{n} V_j, \quad M = \bigoplus_{j=1}^{n} M_j, \tag{42}$$

and

$$\rho = \bigoplus_{j=1}^{n} \rho_j : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \bigoplus_{j=1}^{n} \mathrm{Aut}_{R_{\mathcal{P}}}(M_j), \tag{43}$$

and consider the element w in M defined as

$$w = w_1 + w_2 \cdots + w_n. \tag{44}$$

We now consider the image, which we denote by $\Phi_{\mathcal{P}}$, of the localized Hecke algebra $\mathbb{T}_{i,\mathcal{P}}$ in $\prod_{j=1}^{n} R_{\mathcal{P}}$ under the injective map (35). Note that the image of the Hecke operator T_p is a unit under (35) because the f_j are ordinary eigenforms. Hence, by (37) and (31), we conclude that $\Phi_{\mathcal{P}}$ is the $R_{\mathcal{P}}$-subalgebra generated by the identity and all the

$$\left\{ \bigoplus_{j=1}^{n} \mathrm{Trace}(\rho_j(\mathrm{Frob}_l)), \ l \neq p \right\}. \tag{45}$$

Similarly, we define

$$\Phi \subseteq \bigoplus_{j=1}^{n} R \tag{46}$$

to be the R-subalgebra generated by the identity and the elements (45).

Definition 8.1. $\mathfrak{R}_{\mathcal{P}} = \Phi_{\mathcal{P}}[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$, $\mathfrak{R} = \Phi[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$.

Of course, $\mathfrak{R}_{\mathcal{P}}$ is a $\Phi_{\mathcal{P}}$-algebra, and V and M (cf. (42)) have natural structures as $\mathfrak{R}_{\mathcal{P}}$-modules with $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acting via ρ. Clearly, the homomorphism ρ of (43) can be extended by $\Phi_{\mathcal{P}}$-linearity to a map

$$\rho : \mathfrak{R}_{\mathcal{P}} \to \bigoplus_{j=1}^{n} \mathrm{End}_{R_{\mathcal{P}}}(M_j). \tag{47}$$

Obviously $\mathfrak{R}_{\mathcal{P}}$ is non-commutative.

Definition 8.2. $\mathcal{L} = \mathfrak{R}w$ and $\mathcal{L}_{\mathcal{P}} = \mathfrak{R}_{\mathcal{P}}w$.

Recalling that $R_{\mathcal{P}}$ is a discrete valuation ring, it is clear that $\mathcal{L}_{\mathcal{P}}$ is a free $R_{\mathcal{P}}$-module of finite rank, since it is a submodule of the free $R_{\mathcal{P}}$-module M.

Lemma 8.3. *The element T does not lie in the ideal $\mathcal{P}$ of R.*

Proof. Assume T lies in $\mathcal{P}$. As $\mathcal{P}$ is a prime ideal, its intersection with $\Lambda_{\mathcal{O}}$ would then be $T\Lambda_{\mathcal{O}}$. Thus as we have assumed that $\mathrm{ord}_{\mathcal{P}}(A_0^{(i)}(T)) > 0$, it would follow that $A_0^{(i)}(0) = 0$, and hence $L(0, \omega^i) = 0$. But by (10),

$$A_0^{(i)}(0) = L(\mathbb{Q}, 0, \omega^i),$$

and the complex L-value on the right hand side is well-known to be non-zero. This contradiction completes the proof of the lemma. □

Definition 8.4. *The elements ε_1 and ε_2 in $\mathfrak{R}_{\mathcal{P}}$ are defined as*

$$\varepsilon_1 = \frac{-1}{T}(\tilde{\gamma} - (1 + T)), \quad \varepsilon_2 = \frac{1}{T}(\tilde{\gamma} - 1).$$

Obviously, we have

$$\varepsilon_1 + \varepsilon_2 = 1. \tag{48}$$

Also,

$$\rho(\varepsilon_1) = \bigoplus_{j} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \rho(\varepsilon_2) = \bigoplus_{j} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{49}$$

The following lemma is then obvious:

Lemma 8.5. *For all v in $\mathcal{L}_{\mathcal{P}}$, we have*

$$\varepsilon_i^2 v = \varepsilon_i v \ (i = 1, 2), \quad \varepsilon_1\varepsilon_2 v = \varepsilon_2\varepsilon_1 v = 0. \tag{50}$$

□

Definition 8.6. $\mathcal{L}_{1,\mathcal{P}} = \varepsilon_1 \mathcal{L}_{\mathcal{P}}$, $\mathcal{L}_{2,\mathcal{P}} = \varepsilon_2 \mathcal{L}_{\mathcal{P}}$.

Plainly $\mathcal{L}_{1,\mathcal{P}}$ and $\mathcal{L}_{2,\mathcal{P}}$ are $\Phi_{\mathcal{P}}$-modules such that $\mathcal{L}_{\mathcal{P}} = \mathcal{L}_{1,\mathcal{P}} \oplus \mathcal{L}_{2,\mathcal{P}}$. As $\Phi_{\mathcal{P}}$ is commutative, the $\Phi_{\mathcal{P}}$-Fitting ideals of both $\mathcal{L}_{1,\mathcal{P}}$ and $\mathcal{L}_{2,\mathcal{P}}$ are defined (see [12]).

Lemma 8.7. *The $\Phi_{\mathcal{P}}$-module $\mathcal{L}_{2,\mathcal{P}}$ is free of rank one, generated by w. In particular, the $\Phi_{\mathcal{P}}$-Fitting ideal of $\mathcal{L}_{2,\mathcal{P}}$ is zero.*

Proof. First note that $\Phi_{\mathcal{P}} w = \Phi_{\mathcal{P}} \varepsilon_2 w$, since $\varepsilon_2 w = w$. Hence $\Phi_{\mathcal{P}} w \subseteq \mathcal{L}_{2,\mathcal{P}} = \varepsilon_2 \mathcal{L}_{\mathcal{P}}$. To prove the converse, for r in $\mathfrak{R}$, we write

$$\rho(r) = \bigoplus_j \begin{pmatrix} a_{r,j} & b_{r,j} \\ c_{r,j} & d_{r,j} \end{pmatrix} \in \bigoplus_j M_2(R_{\mathcal{P}}),$$

whence

$$\rho(\varepsilon_2 r) w = \sum_{j=1}^{n} d_{r,j} w_j.$$

But $d_{r,j} = \operatorname{Trace} \rho_j(\varepsilon_2 r)$, so that $\oplus_j d_{r,j}$ is in $\Phi_{\mathcal{P}}$. Thus $\varepsilon_2 \mathfrak{R}_{\mathcal{P}} w$ is contained in $\Phi_{\mathcal{P}} w$, proving that $\mathcal{L}_{2,\mathcal{P}} = \Phi_{\mathcal{P}} w$.

To show that $\mathcal{L}_{2,\mathcal{P}}$ is free as a $\Phi_{\mathcal{P}}$-module, suppose $t \neq 0$ is an element of $\Phi_{\mathcal{P}}$ such that $t\mathcal{L}_{2,\mathcal{P}} = 0$. Then $\rho_j(t\varepsilon_2 r) w_j = 0$ for all r in $\mathfrak{R}_{\mathcal{P}}$ and $1 \leq j \leq n$. Let j be such that the j-th component of t is non-zero. Then we must have $\rho_j(t\varepsilon_2 r) w_j = 0$ for all r in $\mathfrak{R}_{\mathcal{P}}$. But then $\rho_j(\varepsilon_2 r)$ annihilates the whole of M_j. By (49), this clearly implies that ρ_j is reducible as a representation of $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, which contradicts the irreducibility of the ρ_j's. Finally, as the $\Phi_{\mathcal{P}}$-annihilator if $\mathcal{L}_{2,\mathcal{P}}$ is zero, its $\Phi_{\mathcal{P}}$-Fitting ideal is also zero (see [12]). This completes the proof. $\qquad\square$

Recall that we have extended ρ to a $\Phi_{\mathcal{P}}$-linear homomorphism from $\mathfrak{R}_{\mathcal{P}}$ to $\oplus \operatorname{End}_{R_{\mathcal{P}}}(M_j)$ (47). For each r in $\mathfrak{R}_{\mathcal{P}}$, we can restrict $\rho(r)$ to obtain a $\Phi_{\mathcal{P}}$-linear endomorphism of $\mathcal{L}_{\mathcal{P}} = \mathfrak{R}_{\mathcal{P}} w$, which we denote by $\tilde{\rho}(r)$. Since $\mathcal{L}_{1,\mathcal{P}}$ and $\mathcal{L}_{2,\mathcal{P}}$ are $\Phi_{\mathcal{P}}$-modules with $\mathcal{L}_{\mathcal{P}} = \mathcal{L}_{1,\mathcal{P}} \oplus \mathcal{L}_{2,\mathcal{P}}$, we can therefore write

$$\tilde{\rho}(r) = \begin{pmatrix} \mathcal{A}_r & \mathcal{B}_r \\ \mathcal{C}_r & \mathcal{D}_r \end{pmatrix}, \tag{51}$$

where $\mathcal{A}_r$ belongs to $\operatorname{Hom}_{\Phi_{\mathcal{P}}}(\mathcal{L}_{1,\mathcal{P}}, \mathcal{L}_{1,\mathcal{P}})$, $\mathcal{B}_r \in \operatorname{Hom}_{\Phi_{\mathcal{P}}}(\mathcal{L}_{2,\mathcal{P}}, \mathcal{L}_{1,\mathcal{P}})$, $\mathcal{C}_r \in \operatorname{Hom}_{\Phi_{\mathcal{P}}}(\mathcal{L}_{1,\mathcal{P}}, \mathcal{L}_{2,\mathcal{P}})$, $\mathcal{D}_r \in \operatorname{Hom}_{\Phi_{\mathcal{P}}}(\mathcal{L}_{2,\mathcal{P}}, \mathcal{L}_{2,\mathcal{P}})$. Note that by the previous lemma, $\operatorname{Hom}_{\Phi_{\mathcal{P}}}(\mathcal{L}_{2,\mathcal{P}}, \mathcal{L}_{2,\mathcal{P}}) \simeq \Phi_{\mathcal{P}}$.

We define $\mathcal{I}_{i,\mathcal{P}}$ to be the ideal of $\Phi_{\mathcal{P}}$ which is the image of $\mathbb{I}_i \mathbb{T}_{i,\mathcal{P}}$ under the injection (35). Note that $\mathcal{I}_{i,\mathcal{P}}$ is the ideal of $\Phi_{\mathcal{P}}$ generated by all elements of the form

$$\bigoplus_j (\operatorname{Trace} \rho_j(\operatorname{Frob}_l) - 1 - \theta_i(\operatorname{Frob}_l)). \tag{52}$$

Here we recall that

$$\theta_i(\operatorname{Frob}_l) = \omega^i(l)(1 + T)^{e_l}.$$

Lemma 8.8. *The following assertions hold:*

(i) $\mathcal{B}_\sigma = 0$ *for all σ in the decomposition group D_p.*

(ii) *The $\Phi_{\mathcal{P}}$-submodule of M generated by the images of all the maps $\mathcal{B}_r$, with r ranging over $\mathfrak{R}$ is equal to $\mathcal{L}_{1,\mathcal{P}}$.*

(iii) *For σ in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, $\mathcal{D}_\sigma \equiv \theta_i(\sigma) \bmod \mathcal{I}_{i,\mathcal{P}}$, where θ_i is given by (38), and we view $\mathcal{D}_\sigma$ as an element of $\Phi_{\mathcal{P}}$.*

(iv) *For each r in $\mathfrak{R}$, the image of $\mathcal{C}_r$ is contained in $\mathcal{I}_{i,\mathcal{P}}w$.*

(v) *For σ in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, we have*

$$\tilde{\rho}(\sigma) \equiv \begin{pmatrix} 1 & \mathcal{B}_\sigma \\ 0 & \theta_i(\sigma) \end{pmatrix} \bmod \mathcal{I}_{i,\mathcal{P}}. \tag{53}$$

(vi) *$\mathcal{L}_{1,\mathcal{P}}/\mathcal{I}_{i,\mathcal{P}}\mathcal{L}_{1,\mathcal{P}}$ is stable under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and this action is trivial.*

Proof. Assertion (i) is clear from (39). Turning to (ii), we note that for each r in $\mathfrak{R}$, we have

$$rw \in \mathrm{Im}\,\mathcal{B}_r \oplus \mathrm{Im}\,\mathcal{D}_r \subseteq \mathcal{L}_{1,\mathcal{P}} \oplus \mathcal{L}_{2,\mathcal{P}}.$$

Indeed, this is clear if r belongs to $\Phi_{\mathcal{P}}$, and it is also plain for r in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, since the component w_j of w is an element of our fixed $R_{\mathcal{P}}$-basis of M_j. Also, since $\mathcal{D}_r$ is isomorphic to $\Phi_{\mathcal{P}}$ by the previous lemma, we conclude that the image of $\mathcal{D}_r = \mathcal{L}_{2,\mathcal{P}}$ for any r in $\mathfrak{R}_{\mathcal{P}}$. Assertion (ii) now follows from the fact that $\mathcal{L}_{\mathcal{P}} = \mathfrak{R}_{\mathcal{P}}.w$.

We next prove (iii). For each r in $\mathfrak{R}_{\mathcal{P}}$, we have by (52),

$$\bigoplus_j (\mathrm{Trace}\,\rho_j(\varepsilon_2 r)) \equiv (\mathbf{1} \oplus \theta_1)(\varepsilon_2 r) \bmod \mathcal{I}_{i,\mathcal{P}}, \tag{54}$$

where $\mathbf{1}$ denotes the trivial character. The left hand side of (54) is easily seen to be $\mathcal{D}_r$, which we continue to view as an element of $\Phi_{\mathcal{P}}$. On the other hand, we have

$$\mathbf{1}(\varepsilon_2) = 0, \quad \theta_i(\varepsilon_2) = 1.$$

Hence the right hand side of (54) is equal to $\theta_i(r)$, establishing (iii).

Turning to (iv), note that we have the identity

$$\mathcal{D}_{rr'} = \mathcal{D}_r \mathcal{D}_{r'} + \mathcal{C}_r \mathcal{B}_{r'}$$

for all elements r, r' in $\mathfrak{R}_{\mathcal{P}}$. Since θ_i is a character, it follows from (iii) that

$$\mathrm{Im}\,\mathcal{C}_r \mathcal{B}_{r'} \subseteq \mathcal{I}_{i,\mathcal{P}}\mathcal{L}_{2,\mathcal{P}}.$$

As the image of the $\mathcal{B}_{r'}$ fills up the whole of $\mathcal{L}_{1,\mathcal{P}}$ as r' varies, we conclude that $\mathrm{Im}\,\mathcal{C}_r \subset \mathcal{I}_{i,\mathcal{P}}\mathcal{L}_{2,\mathcal{P}}$, proving (iv).

To establish (v) and (vi), we must show that $A_\sigma \bmod \mathcal{I}_{i,\mathcal{P}}$ is the identity map for any σ in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Suppose

$$\rho(\sigma) = \oplus \begin{pmatrix} a_{\sigma,j} & b_{\sigma,j} \\ c_{\sigma,j} & d_{\sigma,j} \end{pmatrix} \text{ in } \bigoplus_{j=1}^n \mathrm{GL}_2(R_{\mathcal{P}}).$$

The action of $\mathcal{A}_\sigma$ on the element $\varepsilon_1 r w$ in $\mathcal{L}_{1,\mathcal{P}}$ is given by multiplication by $a_\sigma = \oplus a_{\sigma,j}$. But $a_{\sigma,j} = \operatorname{Trace}(\rho_j(\varepsilon_1\sigma))$ as

$$\rho_j(\varepsilon_1\sigma) = \begin{pmatrix} a_{\sigma,j} & b_{\sigma,j} \\ 0 & 0 \end{pmatrix}.$$

On the other hand, by (52), we have

$$a_{\sigma,j} \equiv \operatorname{Trace}(\mathbf{1} + \theta_i)(\varepsilon_1\sigma) = 1 \bmod \mathcal{I}_{i,\mathcal{P}},$$

because

$$\theta_i(\varepsilon_1) = 0, \quad \mathbf{1}(\varepsilon_1) = 1.$$

This completes the proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

9. Completion of the proof

We continue to assume that i is an odd integer with $i \not\equiv -1 \bmod p - 1$. We now give an equivalent form of (29) which fits in better with our present arguments. Define R_i to be R endowed with the following action of $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$:

$$\sigma(r) = \theta_i(\sigma)r,$$

where θ_i is the character (38). The Pontryagin dual

$$\overset{\vee}{R}_i = \operatorname{Hom}(R_i, \mathbb{Q}_p/\mathbb{Z}_p)$$

is therefore a discrete p-primary abelian group on which $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts via θ_i^{-1}. For each subfield $\mathcal{K}$ of $\bar{\mathbb{Q}}$, define the subgroup of unramified cocycles by

$$H^1_{\mathrm{nr}}(\mathcal{K}, \overset{\vee}{R}_i) = \operatorname{Ker}\left(H^1(\operatorname{Gal}(\bar{\mathbb{Q}}/\mathcal{K}), \overset{\vee}{R}_i) \to \prod_v H^1(I_v, \overset{\vee}{R}_i) \right),$$

where the product is taken over all non-archimedean primes v of $\mathcal{K}$, and I_v denotes the inertial subgroup of some fixed prime of $\bar{\mathbb{Q}}$ above v. We recall that $X_\infty = \operatorname{Gal}(\mathcal{L}_\infty/\mathcal{F}_\infty)$, where $\mathcal{L}_\infty$ is the maximal unramifed abelian p-extension of $\mathcal{F}_\infty$. As is explained at the beginning of §3, there is a natural action of $\mathcal{G} = \Delta \times \Gamma$ on X_∞. We define

$$V_\infty = X_\infty^\bullet,$$

where as in §3, the dot means that the $\mathcal{G}$-action on X_∞ has been inverted. Define

$$\operatorname{Sel}_i(R) = H^1_{\mathrm{nr}}(\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \overset{\vee}{R}_i), \quad Z_i(R) = \operatorname{Hom}(\operatorname{Sel}_i(R), \mathbb{Q}_p/\mathbb{Z}_p). \qquad (55)$$

Lemma 9.1.

$$Z_i(R) = V_\infty^{(i)} \otimes_{\Lambda(\Gamma)} R.$$

Proof. Note that $(\overset{\vee}{R}_i)^\Delta = 0$ since i is not congruent to zero modulo $p - 1$. Hence

$$H^j(\mathcal{G}, \overset{\vee}{R}_i) = H^j(\Gamma, (\overset{\vee}{R}_i)^\Delta) = 0 \quad (j \geq 0). \qquad (56)$$

Thus

$$H^1(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \overset{\vee}{R}_i) \simeq H^1(\text{Gal}(\bar{\mathbb{Q}}/\mathcal{F}_\infty), \overset{\vee}{R}_i)^{\mathcal{G}}.$$

As p is totally ramified in $\mathbb{Q}(\mu_{p^\infty})$, one sees easily that this induces an isomorphism

$$\text{Sel}_i(R) \simeq H^1_{\text{nr}}(\text{Gal}(\bar{\mathbb{Q}}/\mathcal{F}_\infty), \overset{\vee}{R}_i)^{\mathcal{G}} = \text{Hom}_{\mathcal{G}}(X_\infty, \overset{\vee}{R}_i).$$

But recalling that $\mathcal{G}$ acts on $\overset{\vee}{R}_i$ by θ_i^{-1}, we see that

$$\text{Hom}_{\mathcal{G}}(X_\infty, \overset{\vee}{R}_i) = \text{Hom}_{\Lambda(\Gamma)}(V_\infty^{(i)}, \overset{\vee}{R}_i).$$

But

$$\text{Hom}_{\Lambda(\Gamma)}(V_\infty^{(i)}, \overset{\vee}{R}_i) = \text{Hom}_{\Lambda(\Gamma)}(V_\infty^{(i)},$$

$$\text{Hom}(R, \mathbb{Q}_p/\mathbb{Z}_p)) = \text{Hom}(V_\infty^{(i)} \otimes_{\Lambda(\Gamma)} R, \mathbb{Q}_p/\mathbb{Z}_p),$$

and this completes the proof.   □

Since $V_\infty^{(i)}$ is $X_\infty^{(-i)}$ with its Γ-action inverted, we conclude that, in order to prove (29), it suffices to show that for every prime ideal $\mathcal{P}$ of R of height one, we have

$$\text{ord}_{\mathcal{P}}(\text{char}_R Z_i(R)) \geq \text{ord}_{\mathcal{P}}(A_0^{(i)}(T)). \tag{57}$$

Define

$$\mathcal{N} = \text{Im}(\mathcal{L} \to \mathcal{L}_{\mathcal{P}}/\mathcal{I}_{i,\mathcal{P}}\mathcal{L}_{\mathcal{P}}),$$

$$\mathcal{N}_1 = \mathcal{N} \cap \mathcal{L}_{1,\mathcal{P}}/\mathcal{I}_{i,\mathcal{P}}\mathcal{L}_{1,\mathcal{P}} \quad \text{and} \quad \mathcal{N}_2 = \mathcal{N} \cap \mathcal{L}_{2,\mathcal{P}}/\mathcal{I}_{i,\mathcal{P}}\mathcal{L}_{2,\mathcal{P}}. \tag{58}$$

If V is any $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module, which is also an R-module, we write $V(\theta_i^{-1})$ for V with the new Galois action defined by

$$\sigma \circ v = \theta_i^1(\sigma) \cdot \sigma v,$$

where the action σv on the right is the old Galois action. Put

$$\mathfrak{X} = \text{Hom}_R(\mathcal{N}_1(\theta_i^{-1}), \overset{\vee}{R}_i).$$

Since $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts trivially on $\mathcal{N}_1$, it is clear that each β in $\mathfrak{X}$ is a $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-homomorphism. Given any β in $\mathfrak{X}$, we define a map

$$c_\beta : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \overset{\vee}{R}_i$$

by the formula

$$c_\beta(\sigma) = \beta(\mathcal{B}_\sigma(w).\theta_i(\sigma)^{-1} \bmod \mathcal{I}_{i,\mathcal{P}}), \tag{59}$$

where $\mathcal{B}_\sigma$ is the homomorphism given in (51), and hence the right hand side of (59) does indeed lie in $\beta(\mathcal{N}_1)$. For σ, τ in $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, we conclude from (53) that

$$\mathcal{B}_{\sigma\tau}(w) = (\mathcal{B}_\tau(w) + \mathcal{B}_\sigma(w)\theta_i(\tau)) \bmod \mathcal{I}_{i,\mathcal{P}}.$$

Recalling that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $\overset{\vee}{R}_i$ via θ_i^{-1}, it follows immediately that c_β is in fact a 1-cocycle, and we denote its class in $H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \overset{\vee}{R}_i)$ by $\mathfrak{c}_\beta$. We can therefore define a homomorphism

$$\Omega : \mathfrak{X} \to H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \overset{\vee}{R}_i) \tag{60}$$

by $\Omega(\beta) = \mathfrak{c}_\beta$.

Lemma 9.2. *The image of Ω is contained in $H^1_{\mathrm{nr}}(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}, \overset{\vee}{R}_i) = \mathrm{Sel}_i(R)$.*

Proof. Since the Galois representations ρ_j (see (36)) are unramified outside p, and $\mathcal{B}_\sigma = 0$ for all σ in the decomposition group D_p by Lemma (8.8), assertion (i) is clear. $\qquad\square$

Proposition 9.3. *The map Ω is injective after tensoring with the localisation $R_{\mathcal{P}}$ of R.*

Proof. If β is any element of $\mathfrak{X}$, we have the extension of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules

$$0 \to \mathcal{N}_1(\theta_i^{-1}) \to \mathcal{N}(\theta_i^{-1}) \to \mathcal{N}_2(\theta_i^{-1}) \to 0,$$

which clearly further gives rise to the extension

$$0 \to \mathcal{N}_1(\theta_i^{-1})/\mathrm{Ker}\,\beta \to \mathcal{N}(\theta_i^{-1})/\mathrm{Ker}\,\beta \to \mathcal{N}_2(\theta_i^{-1}) \to 0. \tag{61}$$

Since $\mathcal{N}_2$ can be identified with the module $(R/J_i) \cdot w$, the cohomology class of the extension (61) in $H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \mathcal{N}_1(\theta_i^{-1})/\mathrm{Ker}\,\beta)$ is given by the class of the cocycle

$$d(\sigma) = \theta_i(\sigma)^{-1}\sigma w - w \bmod (\mathrm{Ker}\,\beta). \tag{62}$$

Obviously, we have

$$\beta(d(\sigma)) = c_\beta(\sigma). \tag{63}$$

Assume now that β in $\mathfrak{X}$ is such that c_β is a coboundary, i.e. there exists t in $\overset{\vee}{R}_i$ such that
$$c_\beta(\sigma) = (\theta_i(\sigma)^{-1} - 1)t \quad \text{for all } \sigma \text{ in } \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}).$$

Since i is odd, we can choose σ_0 in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ such that $(\theta_i(\sigma_0)^{-1} - 1)$ is a unit in R. Hence
$$\beta(s) = t, \quad \text{where} \quad s = (\theta_i(\sigma_0)^{-1} - 1)^{-1}d(\sigma_0).$$

It follows easily that d itself is a coboundary. Hence the extension (61) is split, and so there exists a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-surjection

$$\mathcal{N}(\theta_i^{-1})/\mathrm{Ker}\,\beta \to \mathcal{N}_1(\theta_i^{-1})/\mathrm{Ker}\,\beta. \tag{64}$$

Recalling that $\mathcal{N}$ is cyclic and generated by w, it follows that the module on the right of (64) is cyclic with generator x, say. By virtue of (41), it follows that the module on the left of (64) is annihilated by $(\tilde{\gamma} - 1)$, and so x is also annihilated by $(\tilde{\gamma} - 1)$.

As $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts trivially on $\mathcal{N}_1$, we conclude that x is annihilated by $((1+T)^{-1}-1)$ and so also $T \cdot x = 0$. Hence

$$T\mathcal{N}_1(\theta_i^{-1}) \subset \text{Ker } \beta. \tag{65}$$

We now define

$$\mathfrak{X}' = \{\beta \text{ in } \mathfrak{X} \text{ such that } c_\beta \text{ is a coboundary}\}.$$

Under the natural pairing

$$\mathcal{N}_1 \times \mathfrak{X} \to \overset{\vee}{R_i},$$

$\mathfrak{X}'$ is dual to $\mathcal{N}_1(\theta_i^{-1})/W$, where

$$W = \bigcap_{\beta \in \mathfrak{X}'} \text{Ker } \beta.$$

However by (65),

$$W \supset T\mathcal{N}_1(\theta_i^{-1}).$$

Thus $T \cdot \mathfrak{X}' = 0$, whence $\mathfrak{X}'_{\mathcal{P}} = 0$, since $T \notin \mathcal{P}$. This proves that the map Ω is injective after tensoring with $R_{\mathcal{P}}$ over R and the proof of the proposition is complete.   □

Note that as an R-module, we have

$$\mathfrak{X} = \text{Hom}_R(\mathcal{N}_1(\theta_i^{-1}), \overset{\vee}{R_i}) = \text{Hom}(\mathcal{N}_1, \mathbb{Q}_p/\mathbb{Z}_p),$$

and so, dualizing the map Ω, we obtain a homomorphism of R-modules

$$\overset{\vee}{\Omega} : Z_i(R) \twoheadrightarrow \mathcal{N}_1,$$

which is surjective after localisation at $\mathcal{P}$ by Proposition 9.3. Thus, for every prime ideal $\mathcal{P}$ of height one of R, we have

$$\text{ord}_{\mathcal{P}} \, \text{char}_{R_{\mathcal{P}}}(Z_i(R)_{\mathcal{P}}) \geq \text{ord}_{\mathcal{P}} \, \text{char}_{R_{\mathcal{P}}}((\mathcal{N}_1)_{\mathcal{P}}). \tag{66}$$

We recall that, by (32) and (35), we have the isomorphism of $R_{\mathcal{P}}$-algebras

$$R_{\mathcal{P}}/J_{i,\mathcal{P}} \simeq \Phi_{\mathcal{P}}/\mathcal{I}_{i,\mathcal{P}}\Phi_{\mathcal{P}}. \tag{67}$$

Using this isomorphism, we can view the $\Phi_{\mathcal{P}}$-module $\mathcal{L}_{1,\mathcal{P}}/\mathcal{I}_{\mathcal{P}}\mathcal{L}_{1,\mathcal{P}}$ as a module over $R_{\mathcal{P}}$ which is annihilated by $J_{i,\mathcal{P}}$. By arguments from commutative algebra, we shall then prove at the end of this section the following key lemma.

Lemma 9.4. *For every prime ideal $\mathcal{P}$ of height 1 of R, the $R_{\mathcal{P}}$-Fitting ideal of $\mathcal{L}_{1,\mathcal{P}}/\mathcal{I}_{i,\mathcal{P}} \mathcal{L}_{1,\mathcal{P}}$ is contained in $J_{i,\mathcal{P}}$.*

Assuming this lemma, we shall complete the proof of (57), and hence also the proof of the main conjecture. As the $R_{\mathcal{P}}$-Fitting ideal of $\mathcal{L}_{1,\mathcal{P}}/\mathcal{I}_{i,\mathcal{P}} \mathcal{L}_{1,\mathcal{P}}$ is contained in $J_{i,\mathcal{P}}$ Proposition 17 of [12] allows us to conclude that

$$\text{char}_{R_{\mathcal{P}}}(\mathcal{L}_{1,\mathcal{P}}/\mathcal{I}_{i,\mathcal{P}}\mathcal{L}_{1,\mathcal{P}}) \subseteq J_{i,\mathcal{P}}. \tag{68}$$

Combining this last inclusion with (66), and noting that

$$(\mathcal{N}_1)_{\mathcal{P}} = \mathcal{L}_{1,\mathcal{P}}/\mathcal{I}_{i,\mathcal{P}}, \mathcal{L}_{1,\mathcal{P}}$$

we have

$$\mathrm{ord}_{\mathcal{P}}\,(Z_i(R)_{\mathcal{P}}) \geq \mathrm{ord}_{\mathcal{P}}\,J_{i,\mathcal{P}}. \tag{69}$$

Recall that the Hecke algebra $\mathbb{T}_{i,\mathcal{P}}$ is isomorphic to $\Phi_{\mathcal{P}}$ and hence by (67) and Theorem 4.4, we have

$$\mathrm{ord}_{\mathcal{P}}\,J_{i,\mathcal{P}} := \mathrm{ord}_{\mathcal{P}}(\mathrm{char}(R_{\mathcal{P}}/J_{i,\mathcal{P}}) \geq \mathrm{ord}_{\mathcal{P}}\,A_0^{(i)}(T), \tag{70}$$

which proves (57) and therefore the main conjecture.

We are very grateful to F. Nuccio for providing us with the following proof of Lemma 9.4. Recall that there is a natural ring homomorphism from $R_{\mathcal{P}}$ to $\Phi_{\mathcal{P}}$ making $\Phi_{\mathcal{P}}$ an $R_{\mathcal{P}}$ algebra and note that $\Phi_{\mathcal{P}}$ is a flat $R_{\mathcal{P}}$-module as it is free of finite rank over $R_{\mathcal{P}}$. On the other hand, defining $L_1 \subset \mathcal{L}_1$ to be the R-submodule $L_1 = \varepsilon_1\,R.w$, so that

$$L_{1,\mathcal{P}} \otimes_{\Phi,\mathcal{P}} \Phi_{\mathcal{P}} = \mathcal{L}_{1,\mathcal{P}}.$$

Since $\Phi_{\mathcal{P}}$ is a flat $R_{\mathcal{P}}$-module, and $L_{1,\mathcal{P}}$ is $R_{\mathcal{P}}$-faithful, it follows from [2, Chap. 1, §2, Cor. 2], that

$$\mathrm{ann}_{\Phi,\mathcal{P}}(\mathcal{L}_{1,\mathcal{P}}) = 0.$$

Hence by Corollary 14 of [12], we have that the $\Phi_{\mathcal{P}}$-Fitting ideal satisfies

$$\mathrm{Fitt}_{\Phi_{\mathcal{P}}}(\mathcal{L}_{1,\mathcal{P}}/\mathcal{I}_{i,\mathcal{P}}\mathcal{L}_{1,\mathcal{P}}) \subset \mathcal{I}_{i,\mathcal{P}}.$$

Hence, by [12, Lemma 10], we obtain

$$\mathrm{Fitt}_{\Phi_{\mathcal{P}}/\mathcal{I}_{i,\mathcal{P}}}(\mathcal{L}_{1,\mathcal{P}}/\mathcal{I}_{i,\mathcal{P}}\mathcal{L}_{1,\mathcal{P}}) = 0.$$

Invoking the ring isomorphism (67), we conclude that

$$\mathrm{Fitt}_{R_{\mathcal{P}}/J_{i,\mathcal{P}}}(\mathcal{L}_{1,\mathcal{P}}/\mathcal{I}_{i,\mathcal{P}}\mathcal{L}_{1,\mathcal{P}}) = 0.$$

Since $\mathcal{L}_{1,\mathcal{P}}$ is a faithful $R_{\mathcal{P}}$-module, we can apply Lemma 10 of [12] once more to complete the proof of Lemma 9.4. $\qquad\square$

References

[1] D. Banerjee, E. Ghate and V. G. Narasimha Kumar, Λ-adic forms and the Iwasawa Main Conjecture (this volume).

[2] N. Bourbaki, Elements of Mathematics, Commutative Algebra, Chapters 1–7, Springer (1989).

[3] P. Cassou-Nogues, Valeurs aux entiers négatifs des fonctions zêta p-adiques, *Invent. Math.*, **51** (1979) 29–59.

[4] J. Coates and R. Sujatha, Cyclotomic fields and zeta values, Springer Monographs in Mathematics, Springer (2006).

[5] P. Deligne and K. Ribet, Values of abelian *L*-functions at negative integers over totally real fields, *Invent. Math.*, **59** (1980) 227–286.

[6] H. Hida, Modules of congruence of Hecke algebras and *L*-functions associated with cusp forms, *Amer. J. Math.*, **110** (1988) 323–382.

[7] H. Hida, Elementary theory of *L*-functions and Eisenstein series, London Mathematical Society Student Texts **26**, Cambridge University Press, Cambridge (1993).

[8] K. Iwasawa, On $\mathbb{Z}_l$-extensions of algebraic number fields, *Ann. Math.*, **98** (1973) 246–326.

[9] K. Iwasawa, Lectures on *p*-adic *L*-functions, *Ann. Math. Studies*, **74**, Princeton University Press (1972).

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

[11] B. Mazur and A. Wiles, On *p*-adic analytic families of Galois representations, *Comp. Math.*, **59** (1986) 231–264.

[12] F. Nuccio, Fitting Ideals (this volume).

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

[14] K. Rubin, The Main Conjecture Appendix in S. Lang Cyclotomic fields I and II, Combined second edition, Graduate Texts in Mathematics, 121, Springer-Verlag, New York (1990).

[15] C. Seigel, Berechnung von Zeta-funktionen an ganzzahligen Stellen, *Nach. Akad. Wiss. Göttingen*, (1969) 87–102.

[16] A. Wiles, On ordinary Λ-adic representations associated to modular foms, *Invent. Math.*, **94** (1988) 529–573.

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