On the freeness of the integral cohomology groups of Hilbert-Blumenthal varieties as Hecke modules

Eknath Ghate

Dedicated to my parents, Anjali and Prabhu Ghate

1 Introduction

Let F be a totally real field of degree $d \geq 1$. Let f be a Hilbert modular cusp form defined over F of level $\mathfrak{N} \subset \mathcal{O}_F$ and parallel weight $(k, k, \ldots, k)$ with $k \geq 2$. Assume that f is a normalized newform and a common eigenform of all the Hecke operators. Such a Hilbert modular form will be called a primitive form. The purpose of this paper is to investigate the relationship between the primes of congruence of a primitive form f and the primes dividing a special value of the adjoint L-function of f.

In [9, Theorem 5] we defined a finite set of bad primes $\mathcal{S}$ in a sufficiently large number field K depending on f and proved the following result.

Theorem 1 *Let $\wp$ be a prime of K with $\wp \notin \mathcal{S}$. If*

$$\wp \mid \frac{W(f)\, \Gamma(1, \mathrm{Ad}(f))\, L(1, \mathrm{Ad}(f))}{\Omega(f, \epsilon)\Omega(f, -\epsilon)} \tag{1}$$

then $\wp$ is a congruence prime for f.

Here $W(f)$ is the complex constant occurring in the functional equation of the standard L-function of f, $L(s, \mathrm{Ad}(f))$ is the adjoint L-function of f and $\Gamma(s, \mathrm{Ad}(f))$ is an appropriate Γ-factor. Let $\mathcal{O}_{(\wp)}$ be the valuation ring of K at $\wp$. Then $\Omega(f, \pm\epsilon) \in \mathbb{C}^\times / \mathcal{O}_{(\wp)}{}^\times$ are Eichler-Shimura periods. It is implicit in the statement of the theorem that the quotient occurring in (1) is an element of $\mathcal{O}_{(\wp)}$.

Theorem 1 is a generalization to the Hilbert modular setting of a well known result of Hida [10] for elliptic modular forms (the case $d = 1$), connecting the special value at $s = 1$ of the adjoint L-function $L(s, \mathrm{Ad}(f))$ of f and the congruence primes of f. (In the elliptic modular setting the set $\mathcal{S}$ may be taken to consist of the primes of K dividing $6\mathfrak{N}$ as well as the primes dividing the primes of $\mathbb{Q}$ smaller than or equal to $k - 2$. In the general case $d \geq 1$ the set $\mathcal{S}$ depends on the weight and level of f, the field F, and the torsion in the boundary cohomology groups of the Borel-Serre compactification of the underlying

Hilbert-Blumenthal variety, among other things. The exact definition of $\mathcal{S}$ will be recalled shortly in equation (3) below.)

The field K in Theorem 1 is taken to contain the number field generated by the Fourier coefficients of f. Let us say that a prime $\wp$ of K of residue characteristic p is ordinary for f if the Fourier coefficient $c(p\mathcal{O}_F, f)$ of f is a $\wp$-adic unit. In [11] Hida established a converse to Theorem 1 for primes $\wp$ that are ordinary for f in the case $F = \mathbb{Q}$. Soon after Ribet [20] removed the assumption of ordinarity on $\wp$ obtaining the following unconditional converse to Theorem 1.

Theorem 2 ([11], [20]) *Let $F = \mathbb{Q}$. Let $\wp \mid p$ be a prime of K, with $p > k-2$ and $p \nmid 6\mathfrak{N}$. Then $\wp$ is a congruence prime for f if and only if*

$$\wp \mid \frac{W(f)\,\Gamma(1, \mathrm{Ad}(f))\,L(1, \mathrm{Ad}(f))}{\Omega(f, \epsilon)\Omega(f, -\epsilon)}.$$

The purpose of this paper is to prove a similar converse to Theorem 1 for Hilbert modular forms defined over totally real fields F of degree $d \geq 2$. As in [11] we will restrict our attention to primes $\wp$ which are ordinary for f.

Our strongest result is for certain Hilbert modular forms defined over real quadratic fields (the case $d = 2$). To state it assume that the residue characteristic p of $\wp$ is odd, let $p^* = (-1)^{(p-1)/2}p$ and let $F^* = F(\sqrt{p^*})$. Let ρ_f denote the $\wp$-adic Galois representation attached to f and let $\overline{\rho}_f$ denote its reduction. If f is ordinary at $\wp$ then by a result of Wiles [26] the restrictions of ρ_f to the decomposition groups at primes of F lying over p are 'upper-triangular'. Let $(p - \mathrm{dist})$ denote the condition that the reductions of the characters appearing on the diagonal are distinct (cf. Section 3.1). Let Assumption 1 denote the vanishing assumption on the boundary cohomology groups made in Section 4.5. Then we prove (cf. Theorem 10):

Theorem 3 *Let F be a real quadratic field of strict class number 1. Let f be a primitive Hilbert modular cusp form of level $\mathfrak{N} = 1$ and parallel weight (k, k) defined over F. Let $\wp \mid p$ be a prime of K such that $\wp \notin \mathcal{S}$ and assume that*

- *$\wp$ is ordinary for f and that $(p - \mathrm{dist})$ holds,*
- *$k \neq 2$, $p + 1$,*
- *$\overline{\rho}_f$ is absolutely irreducible when restricted to F^*,*
- Assumption 1 *holds.*

Then $\wp$ is a congruence prime for f if and only if

$$\wp \mid \frac{W(f)\,\Gamma(1, \mathrm{Ad}(f))\,L(1, \mathrm{Ad}(f))}{\Omega(f, \epsilon)\Omega(f, -\epsilon)}.$$

Here are a few comments about the proof and the hypotheses in Theorem 3. Let F be a totally real field of arbitrary degree $d \geq 1$ again and let f be a primitive cusp form defined over F (of arbitrary level and weight). In [9, Theorem 3] we showed that the set of bad primes $\mathcal{S}$ is essentially the set of primes for which duality for the integral parabolic cohomology groups of the underlying Hilbert-Blumenthal variety may fail. Outside $\mathcal{S}$ we used this duality to establish that the primes dividing the adjoint L-value are exactly the primes of support of a certain cohomological congruence module. We then showed that any such prime is actually a congruence prime for f obtaining Theorem 1 above.

Now assume that $\wp$ is ordinary for f and let $C_{\epsilon}^{\text{coh}}(f)$ denote the corresponding local cohomological congruence module (see (20) in Section 5 for its definition). Then $\wp$ divides the L-value in (1) if and only if $\wp$ occurs in the support of $C_{\epsilon}^{\text{coh}}(f)$. Moreover any such prime is a congruence prime for f. Thus to establish a converse to Theorem 1 one must prove that if $\wp$ is an (ordinary) congruence prime for f then $\wp$ occurs in the support of $C_{\epsilon}^{\text{coh}}(f)$.

To prove this last statement it would suffice to know that a suitable localization of the ordinary part of the middle dimensional integral parabolic cohomology groups of the underlying Hilbert-Blumenthal variety is free as a module over a localized Hecke algebra.

In this paper we give conditions under which this freeness holds. The basic tool that we use is an abstract commutative algebra criterion due to Diamond [3] and Fujiwara [7] for the freeness of certain modules over complete local algebras over p-adic rings (see Theorems 5 and 6 in the text). This result can be traced back to the work of Wiles [27], Taylor and Wiles [25], and Faltings [25, Appendix]. The main commutative algebra result of Faltings-Taylor-Wiles is an isomorphism criterion for a morphism between certain complete local rings in which a freeness assumption is used as a hypothesis. Subsequently Diamond [3] and Fujiwara [7] showed that it is possible to remove this freeness assumption, obtaining it instead as a byproduct of the isomorphism criterion.

The freeness criterion is formulated using what is now called a Taylor-Wiles system. One of the ingredients that go into such a system is a collection of modules M_Q indexed by certain finite sets of primes Q of F. In previous work (see for instance Diamond [2], Fujiwara [7], Skinner and Wiles [23], and Taylor [24]) the modules M_Q have played mostly a supporting role since the focus has been on establishing that certain universal deformation rings are Hecke algebras. Indeed previous authors have mostly used the zero or first dimensional cohomology groups of certain Shimura curves for the modules M_Q.

Since the main objective of the present work is to establish freeness results for the middle dimensional integral cohomology groups of Hilbert-Blumenthal varieties, we are naturally led to take the level-Q-augmented versions of such cohomology groups for the modules M_Q in our Taylor-Wiles system. This introduces some new problems in the verification of the axioms of the freeness criterion. The first three axioms, labelled (TW1), (TW2) and (TW3) in the text, can be established in the Hilbert modular setting in a more or less routine manner by extending the Galois cohomological arguments of Wiles in [27]. However we do need to make some simplifying assumptions here: we assume that the level $\mathfrak{N} = 1$, that the weight $k \neq 2, p+1$ (note that already $p > k-2$ since $\wp \notin \mathcal{S}$; see (3) below) and that $\overline{\rho}_f$ is absolutely irreducible when restricted to F^*.

The last two axioms of the freeness criterion, labelled (TW4) and (TW5) in the text, are more difficult to check. Roughly speaking these axioms require that the modules M_Q are well-controlled as Q varies. In Proposition 4 we show that if

($*$) the analogues of the modules M_Q with *divisible* coefficients vanish in all smaller degrees $0 \leq q < d$,

then (TW4) and (TW5) hold, at least under the technical simplifying assumptions that F has trivial strict class number, $k > 2$ and that certain boundary cohomology groups vanish (Assumption 1).

It is possible to prove ($*$) for $q = 1$ using a result of Serre [21] which says that the congruence subgroup property holds for $\mathrm{SL}_{2/F}$ for totally real fields F of degree $d \geq 2$ (see Theorem 7). Since ($*$) for $q = 0$ is not difficult to show, we obtain (TW4) and (TW5) in the case $d = 2$. The desired freeness result for the middle dimensional integral cohomology group follows, under the above mentioned assumptions (Theorem 8). With it in hand it is an easy consequence that the ordinary congruence prime $\wp$ is captured by the cohomological congruence module $C_\epsilon^{\mathrm{coh}}(f)$ and hence by the adjoint L-value (see Section 5). We thus obtain Theorem 3 in the case $d = 2$.

When $d > 2$ we are only able to prove a conditional analogue of Theorem 3 whose statement we leave to the main body of the paper (see Theorem 10). It would be interesting to investigate under what further conditions ($*$) holds in general.

We now quickly mention some connections with related results in the literature.

- M. Dimitrov's recent thesis [6] treats the case of general totally real fields. One key difference between our approach and his is that we make crucial use of the congruence subgroup property to prove ($*$) (when $d = 2$).

- Diamond, Flach and Guo [5] have recently established the Tamagawa number conjecture for the adjoint motives of elliptic modular forms ($d = 1$) outside a finite set of bad primes. This can be viewed as a refined version of Theorem 2. The Tamagawa number conjecture is still open in the Hilbert modular case ($d > 1$), and would be an interesting topic for future investigation.

- An alternative approach to the desired freeness result which avoids the use of Taylor-Wiles systems has been studied by Diamond [4] in the case $d = 2$ and trivial coefficients ($k = 2$). His approach is based on the original 'q-expansion principle' method used in the elliptic modular case by Mazur [16], Ribet, Tilouine, Edixhoven, Wiles, and others, to show that suitably localized Tate modules of Jacobians are free over localized Hecke algebras.

- Finally, Taylor-Wiles systems have been used to study the middle dimensional cohomology of other groups. In particular, Mokrane-Tilouine [19] and Genestier-Tilouine [8] have extensively studied the case of GSp_4.

In closing this introduction, we recall that previous arguments involving Taylor-Wiles systems in the Hilbert modular setting have mostly employed the zero or first dimensional cohomology groups of Shimura varieties associated to quaternion algebras over F for the auxiliary modules M_Q. The referee has suggested that it might be possible use such TW-systems to prove an analogue of, e.g., Theorem 3, but with quaternionic periods involved instead, and as a consequence, one may be able to obtain new integral period relations between our Eichler-Shimura periods and quaternionic periods.

2 Preliminaries

2.1 Some notation

Fix a totally real field F of degree $d \geq 2$. Let $\mathcal{O}_F$ denote the ring of integers of F. Let I_F denote the set of embeddings of F into $\mathbb{R}$.

Let $\mathrm{G} = \mathrm{Res}_{F/\mathbb{Q}}\mathrm{GL}_2$. Then let $\mathrm{G}_f = \mathrm{G}(\mathbb{A}_f)$ denote the finite part of $\mathrm{G}(\mathbb{A})$, where $\mathbb{A} = \mathbb{A}_f \times \mathbb{R}$ denotes the ring of adeles over $\mathbb{Q}$. Let $\mathrm{G}_\infty = \mathrm{G}(\mathbb{R})$, and let $\mathrm{G}_{\infty+}$ denote the set of those elements in G_∞ which have positive determinant at each place $\sigma \in I_F$. Let $\mathrm{G}(\mathbb{Q})_+ = \mathrm{G}(\mathbb{Q}) \cap \mathrm{G}_{\infty+}$.

Let K_f be an open, compact subgroup of $\mathrm{G}(\mathbb{A}_f)$, let $\mathrm{K}_\infty = \prod \mathrm{O}_2(\mathbb{R})$ denote the standard maximal compact subgroup of $G(\mathbb{R})$, and let $\mathrm{K}_{\infty+} = \prod \mathrm{SO}_2(\mathbb{R}) \subset \mathrm{G}_{\infty+}$ denote the connected component of K_∞ containing the identity element. Let $\mathrm{K} = \mathrm{K}_f\mathrm{K}_\infty$.

Let Z denote the center of G, and let Z_∞ denote the center of G_∞.

2.2 Hecke algebras

Let $\Delta \subset \mathrm{G}(\mathbb{A}_f)$ be a semigroup, such that $\Delta \supset K_f$. Let $\mathrm{K}_f\backslash\Delta/\mathrm{K}_f$ denote the space of double cosets of K_f in Δ. Define the Hecke algebra $h(\Delta, \mathrm{K}_f) = \mathbb{Z}[\mathrm{K}_f\backslash\Delta/\mathrm{K}_f]$ to be the free abelian group with basis the set of double cosets of K_f in Δ. For a double coset $\mathrm{K}_f g \mathrm{K}_f \in \mathrm{K}_f\backslash\Delta/\mathrm{K}_f$, we denote the corresponding basis element by $[\mathrm{K}_f g \mathrm{K}_f]$. The algebra structure on $h(\Delta, K_f)$ is given by the usual convolution product.

Now fix an ideal $\mathfrak{N}$ of $\mathcal{O}_F$. Let

$$\widehat{R}(\mathfrak{N}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\widehat{\mathcal{O}}_F) \,\middle|\, d_\mathfrak{p} \in \mathcal{O}_{F\mathfrak{p}}^\times,\ c_\mathfrak{p} \in \mathfrak{N}\mathcal{O}_{F\mathfrak{p}},\ \text{for all } \mathfrak{p} \mid \mathfrak{N} \right\},$$

and let $\Delta_0(\mathfrak{N}) = \widehat{R}(\mathfrak{N}) \cap \mathrm{G}(\mathbb{A}_f)$. Let $\mathrm{K}_0(\mathfrak{N})$ be the level $\mathfrak{N}$ congruence subgroup of $\mathrm{G}(\mathbb{A}_f)$ defined by

$$\mathrm{K}_0(\mathfrak{N}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\widehat{\mathcal{O}}_F) \,\middle|\, c \equiv 0 \pmod{\mathfrak{N}\widehat{\mathcal{O}}_F} \right\}.$$

The Hecke algebra $h(\Delta_0(\mathfrak{N}), \mathrm{K}_0(\mathfrak{N}))$ can be described explicitly as follows. For each ideal $\mathfrak{m} \subset \mathcal{O}_F$ let $T_\mathfrak{m} = \sum_g [\mathrm{K}_0(\mathfrak{N}) g \mathrm{K}_0(\mathfrak{N})]$, where the sum is taken over all $g \in \Delta_0(\mathfrak{N})$ with $\det(g)\mathcal{O}_F = \mathfrak{m}$. Note that

$$T_\mathfrak{p} = \mathrm{K}_0(\mathfrak{N}) \begin{pmatrix} \varpi_\mathfrak{p} & 0 \\ 0 & 1 \end{pmatrix} \mathrm{K}_0(\mathfrak{N}).$$

Also, for each $\mathfrak{p}$ with $\mathfrak{p} \nmid \mathfrak{N}$ let

$$S_\mathfrak{p} = \mathrm{K}_0(\mathfrak{N}) \begin{pmatrix} \varpi_\mathfrak{p} & 0 \\ 0 & \varpi_\mathfrak{p} \end{pmatrix} \mathrm{K}_0(\mathfrak{N}),$$

Then it is well known that $h(\Delta_0(\mathfrak{N}), \mathrm{K}_0(\mathfrak{N}))$ is a commutative algebra with 1. It is generated over $\mathbb{Z}$ by the Hecke operators $T_\mathfrak{p}$ as $\mathfrak{p}$ varies through all prime ideals of $\mathcal{O}_F$, and by $S_\mathfrak{p}$ for $\mathfrak{p} \nmid \mathfrak{N}$.

2.3 Cusp forms

Let $n = \sum_{\sigma \in I_F} n_\sigma \, \sigma \in \mathbb{Z}[I_F]$ with each $n_\sigma \geq 0$. Let $t = \sum_{\sigma \in I_F} \sigma \in \mathbb{Z}[I_F]$ and let $k = n + 2t$. The data n and k represent the weights of the cusp forms to be considered below. As in [9] we will assume in this paper that the weights are 'parallel', namely that $n_\sigma = n_\tau$ (and so $k_\sigma = k_\tau$), for any $\sigma, \tau \in I_F$. Thus n and k will also sometimes be used to denote this common value.

Let $\mathbb{A}_F = \mathbb{A} \otimes_\mathbb{Q} F$ denote the ring of adeles of F. Identify the center $\mathrm{Z}(\mathbb{A})$ of $\mathrm{G}(\mathbb{A})$ with the idele group $\mathbb{A}_F^\times$. Similarly identify $\mathrm{Z}(\mathbb{Q})$ with $F^\times$. Let $\chi : F^\times \backslash \mathbb{A}_F^\times \to \mathbb{C}^\times$ be a fixed Hecke character whose conductor divides $\mathfrak{N}$ and whose infinity type is $-n$.

Let $S_{k,J}(\mathfrak{N}, \chi)$ denote the space of Hilbert modular cusp form of weight n, level $\mathfrak{N}$, central character χ, and holomorphy type $J \subset I_F$. For a more precise description of these adelic cusp forms and their relation with (tuples of) classical cusp forms, see [9, Section 2].

There is a natural integral structure on $S_{k,J}(\mathfrak{N}, \chi)$ coming from Fourier expansion. Let $\chi_\mathfrak{N}$ denote the finite order character of $(\mathcal{O}_F/\mathfrak{N}\mathcal{O}_F)^\times = \widehat{\mathcal{O}}_F^\times/(1 + \mathfrak{N}\widehat{\mathcal{O}}_F)$ obtained by restricting χ to $\widehat{\mathcal{O}}_F^\times = \prod_\mathfrak{p} \mathcal{O}_{F\mathfrak{p}}$. For a subring A of $\mathbb{C}$ containing the values of $\chi_\mathfrak{N}$, let $S_{k,J}(\mathfrak{N}, \chi, A)$ be the set of elements of $S_{k,J}(\mathfrak{N}, \chi)$ whose Fourier coefficients lie in A.

The Hecke algebra $h(\Delta_0(\mathfrak{N}), \mathrm{K}_0(\mathfrak{N}))$ acts on the space $S_{k,J}(\mathfrak{N}, \chi, A)$ of cusp forms over A. Let $h_k(\mathfrak{N}, \chi, A)$ be the subalgebra of $\mathrm{End}_A(S_{k,J}(\mathfrak{N}, \chi, A))$ generated by $T_\mathfrak{p}$ (for all $\mathfrak{p}$) and $S_\mathfrak{p}$ (for $\mathfrak{p} \nmid \mathfrak{N}$). This algebra is independent of J. When A is not a subring of $\mathbb{C}$, for instance if A is the completion of (the ring of integers of) a number field B, then we can still define $h_k(\mathfrak{N}, \chi, A)$ as $h_k(\mathfrak{N}, \chi, B) \otimes A$.

2.4 Cohomology groups

Let

$$Y(\mathfrak{N}) = \mathrm{G}(\mathbb{Q}) \backslash \mathrm{G}(\mathbb{A}) / \mathrm{K}_0(\mathfrak{N}) \mathrm{K}_{\infty+} \mathrm{Z}_\infty.$$

be the Hilbert-Blumenthal variety of level $\mathfrak{N}$.

Let K be a sufficiently large number field: one that contains all the conjugates of the totally real field F, all the fields of Fourier coefficients of the normalized simultaneous eigenforms in $S_{k,I_F}(\mathfrak{N},\chi)$, as well as the values of $\chi_{\mathfrak{N}}$. We always think of K as a subfield of $\mathbb{C}$. Let $\mathcal{O}_K$ denote the ring of integers of K. The symbol $\wp$ will always denote a prime of K. We write $K_\wp$ for the completion of K and $\mathcal{O}_\wp$ for the ring of integers of $K_\wp$. Finally we write $\mathcal{O}_{(\wp)} = K \cap \mathcal{O}_\wp$ for the valuation ring of K at $\wp$. We will write A for any one of $\mathcal{O}_K$, $\mathcal{O}_{(\wp)}$, $\mathcal{O}_\wp$, K, $K_\wp$ or $K_\wp/\mathcal{O}_\wp$.

Let $L(n, A)$ denote the module of all polynomials with coefficients in A in the variables $\{X_\sigma, Y_\sigma \mid \sigma \in I_F\}$, which are homogeneous of degree $n_\sigma = n$ in each pair X_σ, Y_σ. Suitable variants $L_i(n,\chi,A)$ of this module come equipped with a natural action of certain subgroups of $\mathrm{G}(\mathbb{Q})_+$ (cf. [9, equation (6)]). Taking locally constant sections of the resulting covering maps defines in the usual manner a sheaf $\mathcal{L}(n,\chi,A)$ on $Y(\mathfrak{N})$. See [9, Section 3.1] for details. We let

$$\mathrm{H}^q_?(Y(\mathfrak{N}), \mathcal{L}(n,\chi,A))$$

denote the usual ($? = \emptyset$), compactly supported ($? = \mathrm{c}$), respectively parabolic ($? = \mathrm{p}$), cohomology groups of degree q of $Y(\mathfrak{N})$ with values in the sheaf $\mathcal{L}(n,\chi,A)$. Again, we refer the reader to Section 3.1 of [9] for precise definitions of these groups. Note that in particular the above cohomology groups are well defined for $A = \mathcal{O}_\wp$ and $A = K_\wp/\mathcal{O}_\wp$ if $\wp \notin \mathcal{S}$.

2.5 Ordinary idempotent

Let M be an $\mathcal{O}_\wp$-module of finite type and let $T \in \mathrm{End}(M)$. Let

$$e_T \quad = \quad \lim_{n\to\infty} T^{n!} \in \mathrm{End}(M)$$

be the idempotent attached to T. Then $M = e_T M \oplus (1 - e_T)M$ and T acts as an isomorphism on the first component and topologically nilpotently on the second component.

We apply the above construction to the case when M is one of the cohomology groups considered above and $T = T_p$ is the Hecke operator at the ideal $p\mathcal{O}_F$. Following Hida we shall call $e_{T_p}(M)$ the ordinary part of M. Thus we have the cohomology groups

$$\mathrm{H}^q_{?,\,\mathrm{ord}}(Y(\mathfrak{N}), \mathcal{L}(n,\chi,A))$$

for $? = \emptyset, \mathrm{c}, \mathrm{p}$ and $A = \mathcal{O}_\wp$ or $K_\wp/\mathcal{O}_\wp$ with $\wp \notin \mathcal{S}$.

A primitive cusp form $f \in S_{k,I_F}(\mathfrak{N},\chi)$ is said to be ordinary at a prime $\wp$ of $K \subset \mathbb{C}$ if the p^{th} Fourier coefficient $c(p\mathcal{O}_F, f) \in K$ of f is a $\wp$-adic unit. When p is unramified in F this is equivalent to requiring that $c(\mathfrak{p}, f)$ is a $\wp$-adic unit for each prime ideal $\mathfrak{p}$ of F lying over p. Eventually we shall assume that $\wp \notin \mathcal{S}_F \subset \mathcal{S}$ in which case p is unramified in F (see equation (3) below).

3 Deformations of Galois representations

3.1 Galois representations

Let $f \in S_{k,I_F}(\mathfrak{N}, \chi)$ be a primitive eigenform. We recall the following theorem due to Shimura, Ohta, Carayol, Wiles, Taylor and Blasius-Rogawski.

Theorem 4 *There is a Galois representation $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(K_\wp)$ which is unramified outside $\mathfrak{N}p$, with the properties that for each $\mathfrak{l} \nmid \mathfrak{N}p$, one has*

- $\mathrm{Tr}\,\rho_f(\mathrm{Frob}_\mathfrak{l}) = c(\mathfrak{l}, f)$,
- $\det \rho_f(\mathrm{Frob}_\mathfrak{l}) = \chi(\mathfrak{l})\mathrm{N}_{F|\mathbb{Q}}(\mathfrak{l})$.

Let $\mathfrak{p}$ denote a prime of F lying above a prime p of $\mathbb{Q}$. Let $D_\mathfrak{p}$, respectively $I_\mathfrak{p}$, denote the decomposition group, respectively inertia, subgroup at $\mathfrak{p}|p$. It is a theorem of Wiles [26] that if f is ordinary at $\wp$ then for each prime $\mathfrak{p}$ of F lying over p the representation ρ_f has the following upper-triangular shape:

$$\rho_f|_{D_\mathfrak{p}} \sim \begin{pmatrix} \delta_\mathfrak{p} & * \\ 0 & \epsilon_\mathfrak{p} \end{pmatrix}$$

where $\delta_\mathfrak{p}$ and $\epsilon_\mathfrak{p}$ are characters of $D_\mathfrak{p}$ with $\epsilon_\mathfrak{p}$ an unramified character.

Let $\mathbb{F}$ denote the residue field of $\mathcal{O}_\wp$, the ring of integers of $K_\wp$. Let $\overline{\rho}_f : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(\mathbb{F})$ denote the mod $\wp$ representation attached to f. It will be useful to impose two conditions on $\overline{\rho}_f$. To describe the first assume that f is ordinary at $\wp$. For the rest of this paper we shall assume that

$(p - \mathrm{dist})$ $\quad \overline{\delta}_\mathfrak{p} \neq \overline{\epsilon}_\mathfrak{p}$ for each prime $\mathfrak{p}$ of F lying over p.

If $(p - \mathrm{dist})$ holds we say that f is p-distinguished. This condition is imposed in order to have solutions to the deformation problems considered below.

We will eventually assume that f has level $\mathfrak{N} = 1$. In this case $(p - \mathrm{dist})$ is automatically satisfied if k is even and p is odd. Indeed if $(p - \mathrm{dist})$ fails then for some $\mathfrak{p}|p$ one has $\det(\overline{\rho}_f|_{D_\mathfrak{p}}) = \overline{\epsilon}_\mathfrak{p}^2 = \omega_p^{k-1}$ where ω_p is the mod p Teichmüller character. Since $\overline{\epsilon}_\mathfrak{p}$ is unramified the order of ω_p must divide $k-1$. But this order is $[F(\mu_p) : F]$ and so is even whereas $k - 1$ is odd, a contradiction. Presumably there are Hilbert modular forms of level one and odd parallel weight k defined over totally real fields of degree $d > 1$ (over $\mathbb{Q}$ there are none). So even when the level is one we will still need to impose the condition $(p - \mathrm{dist})$.

For the second condition on $\overline{\rho}_f$ let $p^* = (-1)^{(p-1)/2}p$ and let $F^* = F(\sqrt{p^*})$. Then from now on we shall assume that

$(\mathrm{ai}(F^*))$ $\quad$ The restriction of $\overline{\rho}_f$ to F^* is absolutely irreducible.

3.2 Deformation problems

Let A denote a complete, noetherian, local $\mathcal{O}_\wp$-algebra with residue field $\mathbb{F}$. A representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(A)$ is called a deformation of $\overline{\rho}_f$ if $\overline{\rho} \sim \overline{\rho}_f$ up to strict equivalence.

Let us assume that the prime p does not ramify in F. A deformation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(A)$ is said to be ordinary at p if for each prime $\mathfrak{p}$ of F lying over p there are characters $\psi_{\mathfrak{p}}$ and $\phi_{\mathfrak{p}}$ of $D_{\mathfrak{p}}$ lifting $\overline{\delta}_{\mathfrak{p}}$ and $\overline{\epsilon}_{\mathfrak{p}}$, with $\phi_{\mathfrak{p}}$ unramified, such that

$$\rho|_{D_{\mathfrak{p}}} \sim \begin{pmatrix} \psi_{\mathfrak{p}} & * \\ 0 & \phi_{\mathfrak{p}} \end{pmatrix}.$$

Let $\mathfrak{q}$ be a prime of F whose residue characteristic is not p. If the following condition holds:

($\mathrm{reg}_{\mathfrak{q}}$) $\overline{\rho}_f$ is unramified at $\mathfrak{q}$ and $\overline{\rho}_f(\mathrm{Frob}_{\mathfrak{q}})$ has two distinct eigenvalues

we say that $\overline{\rho}_f$ is regular at $\mathfrak{q}$.

Let $\nu_p : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathcal{O}_{\wp}{}^{\times}$ be the p-cyclotomic character. Fix a finite set of primes Q of F such that Q does not meet $\mathfrak{N}$ and such that $\overline{\rho}_f$ satisfies ($\mathrm{reg}_{\mathfrak{q}}$) for each $\mathfrak{q} \in Q$. A deformation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(A)$ of $\overline{\rho}_f$ is said to be of type Q if

- $\det \rho = \chi \nu_p = \det \rho_f$,
- ρ is ordinary at p, and,
- ρ is unramified outside $\mathfrak{N} \cup \{\mathfrak{p}|p\} \cup Q$.

Let R_Q denote the universal deformation ring corresponding to deformations of type Q. When $Q = \emptyset$ we simply write R for the universal deformation ring. For the existence of these universal deformation rings the reader is referred to the articles of Mazur [17] and [18].

4 Taylor-Wiles systems

In this section we shall use the method of Taylor-Wiles systems to show that under certain hypotheses a suitably localized middle dimensional integral cohomology group is free as a module over a localized Hecke algebra. In the next section (Section 5) we will draw the obvious conclusions concerning the connection between congruence primes and adjoint L-values.

4.1 Freeness criterion

We start by describing some abstract results in commutative algebra due to Wiles [27], Taylor and Wiles [25] and Faltings [25, Appendix] incorporating later simplifications due to Diamond [3] and Fujiwara [7]. In particular we recall an important freeness criterion for a certain module over a local complete noetherian algebra over a p-adic ring. Various expositions of the freeness criterion are now in the literature. Apart from the sources mentioned above see also [15] and [22].

The statements of the results below follow the formulation of Fujiwara [7]. We start with some notation. Let F denote an *arbitrary* number field (this convention is only for this section). Let $\mathcal{O}_F$ denote the ring of integers of F. Fix an odd prime p and let $\mathcal{O}$ be the ring of integers in a finite extension of $\mathbb{Q}_p$. Consider the set $\mathcal{Q}$ defined via

$$\mathcal{Q} = \{\mathfrak{q} \subset \mathcal{O}_F \bigm| \mathfrak{q} \text{ prime}, \ \mathrm{N}_{F|\mathbb{Q}}(\mathfrak{q}) \equiv 1 \ (\mathrm{mod}\ p)\}. \tag{2}$$

For each finite subset $Q \subset \mathcal{Q}$, let

- Δ_Q = the p-Sylow subgroup of $\prod_{\mathfrak{q} \in Q} (\mathcal{O}_F/\mathfrak{q})^\times$,
- $\mathcal{O}[\Delta_Q]$ = the corresponding group algebra over $\mathcal{O}$, and,
- $\mathfrak{a}_Q$ = the augmentation ideal of $\mathcal{O}[\Delta_Q]$.

Definition 1 (Taylor-Wiles system) *For each $m = 1, 2, \ldots$, fix a finite subset $Q_m \subset \mathcal{Q}$. A Taylor-Wiles system consists of a complete, noetherian, local $\mathcal{O}$-algebra R, and a collection of triples (R_m, T_m, M_m), indexed by $m = 1, 2, \ldots$, where*

- *R_m is a complete, noetherian, local $\mathcal{O}$-algebra, with a map $R_m \twoheadrightarrow R$,*
- *T_m is a complete, noetherian, local $\mathcal{O}$-algebra, with a map $R_m \twoheadrightarrow T_m$,*
- *M_m is a T_m-module,*

satisfying:

- *R_m (so also T_m) is an $\mathcal{O}[\Delta_{Q_m}]$-algebra, and,*
- *$R_m/\mathfrak{a}_{Q_m} R_m \xrightarrow{\sim} R$.*

Theorem 5 (Freeness Criterion) *Let R, (R_m, T_m, M_m) be a Taylor-Wiles system. Assume that the following conditions hold:*

(TW1) *If $\mathfrak{q} \in Q_m$ then $\mathrm{N}_{F|\mathbb{Q}}(\mathfrak{q}) \equiv 1 \pmod{p^m}$,*
(TW2) *The cardinality of Q_m is independent of m, say $|Q_m| = r$ for all m,*
(TW3) *R_m is generated by at most r elements as an $\mathcal{O}$-algebra,*
(TW4) *As an $\mathcal{O}[\Delta_{Q_m}]$-module, M_m is free of finite rank $s > 0$ independent of m,*
(TW5) *$\exists$ R-module M : $M_m/\mathfrak{a}_{Q_m} M_m = M$, $\forall m$, as R-modules.*

Then M is a free R-module.

Note that a Taylor-Wiles system yields a collection of diagrams

$$\begin{array}{ccc} R_m & \twoheadrightarrow & T_m \\ \downarrow\!\!\downarrow & & \downarrow \\ R & & \mathrm{End}(M_m), \end{array}$$

which modulo the augmentation ideals of the $\mathcal{O}[\Delta_{Q_m}]$ induce the diagrams

$$\begin{array}{ccc} R_m/\mathfrak{a}_{Q_m}R_m & \twoheadrightarrow & T_m/\mathfrak{a}_{Q_m}T_m \\ \| & & \downarrow \\ R & \xrightarrow{\pi_m} & \mathrm{End}(M_m/\mathfrak{a}_{Q_m}M_m), \end{array}$$

where π_m is defined so that the above diagram commutes. (TW5) implies that the kernel of $\pi_m : R \to \mathrm{End}_{\mathcal{O}}(M_m/\mathfrak{a}_{Q_m}M_m)$ is independent of m. Let $T = R/\ker(\pi_m)$ for any m.

Theorem 6 (Isomorphism criterion) *Under* (TW1-5) *R is a complete intersection ring which is free of finite rank over $\mathcal{O}$. Moreover, the natural map*

$$R \twoheadrightarrow T$$

is an isomorphism. In particular M is a free T-module.

Proof. Theorems 5 and 6 were proved independently by Diamond [3] and Fujiwara [7], building on the method of Taylor-Wiles-Faltings [25]. For Fujiwara's approach to the proofs of these theorems see [7] and [15]. Here we shall only indicate how the freeness of M as a T-module follows from a result of Diamond in [3].

Let A and B be power series rings over $\mathbb{F}$ in r variables and let $\mathfrak{n}$ denote the maximal ideal of A. Let S be an $\mathbb{F}$-algebra and let H be a non-zero S-module which is finite dimensional over $\mathbb{F}$. Suppose that for each $m = 1, 2, \ldots$, there exist $\mathbb{F}$-algebra homomorphisms $\phi_m : A \to B$ and $\psi_m : B \to S$, a B-module H_m and a B-linear homomorphism $\theta_m : H_m \to H$ such that the following hold

(a) ψ_m is surjective and $\psi_m\phi_m(\mathfrak{n}) = 0$,

(b) θ_m induces an isomorphism $H_m/\mathfrak{n}H_m \to H$,

(c) $\mathrm{Ann}_A(H_n) = \mathfrak{n}^m$ and H_m is free over $A/\mathfrak{n}^m$.

Then, by Theorem 2.1 of [3], S is a complete intersection of dimension zero and H is free over S.

To show how the freeness of M as a T-module follows from this result of Diamond let $\wp$ be the maximal ideal of $\mathcal{O}$. By (TW2) we get, for each $m = 1, 2, \ldots$, a surjection $A \twoheadrightarrow \mathbb{F}[\Delta_{Q_m}]$ which maps $\mathfrak{n}$ to the augmentation ideal of $\mathbb{F}[\Delta_{Q_m}]$ and which by (TW1) has kernel contained in $\mathfrak{n}^m$. Set $S = R/\wp$ and $S_m = R_m/\wp$. Then (TW3) gives a surjection $B \twoheadrightarrow S_m$ for each m. Let $\psi_m : B \twoheadrightarrow S$ be the composition of this map with the map $S_m \twoheadrightarrow S$ induced by $R_m \twoheadrightarrow R$. Define $\phi_m : A \to B$ so that the following diagram commutes

$$\begin{array}{ccc} A & \twoheadrightarrow & \mathbb{F}[\Delta_{Q_m}] \\ \downarrow & & \downarrow \\ B & \twoheadrightarrow & S_m, \end{array}$$

where the second vertical map is induced from the $\mathcal{O}[\Delta_{Q_m}]$-algebra structure on R_m. Finally set $H = M/\wp$ and $H_m = M_m/(\wp, \mathfrak{n}^m)$ and view these as B-modules. Then (TW5) gives a map $\theta_m : H_m \to H$ of B-modules. Now (a) above holds since $\mathfrak{n}$ maps to the augmentation ideal of $\mathbb{F}[\Delta_{Q_m}]$ and $\mathfrak{a}_{Q_m} \mapsto 0$ under $R_m \twoheadrightarrow R$. Condition (b) follows from (TW5) and (c) follows from (TW4). By Theorem 2.1 of [3] we deduce that H is free over S. Since M is a torsion free $\mathcal{O}$-module by (TW5) we see that M is a free R-module. It follows that $R \to \mathrm{End}(M)$ is injective and therefore the map $R \twoheadrightarrow T$ is an isomorphism. This shows that M is a free T-module. □

4.2 Construction of a Taylor-Wiles system

In this section we shall construct a Taylor-Wiles system. We shall keep the notation used in Sections 2 and 3. In particular F is a totally real field again of degree $d \geq 2$ and $f \in S_{k,I_F}(\mathfrak{N}, \chi)$ is a primitive Hilbert modular form over F of parallel weight $(k, k, \ldots, k)$.

Let $\mathcal{S}$ denote the finite set of primes of K fixed in [9]. More precisely

$$\mathcal{S} = \mathcal{S}_{\text{weight}} \cup \mathcal{S}_{\text{level}} \cup \mathcal{S}_{\text{elliptic}} \cup \mathcal{S}_F \cup \mathcal{S}_\partial \cup \mathcal{S}_{\text{invariant}}, \tag{3}$$

where

- $\mathcal{S}_{\text{weight}} = \big\{\wp \,\big|\, p \,:\, p \leq n = k-2\big\}$,
- $\mathcal{S}_{\text{level}} = \{\wp \,|\, p \,:\, p \,|\, \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{N})\}$,
- $\mathcal{S}_{\text{elliptic}} = \{\wp \,|\, p \,:\, \mathbb{Q}(\mu_p)^+ \subset F\}$, where $\mathbb{Q}(\mu_p)^+$ is the maximal totally real subfield of the p^{th} cyclotomic field $\mathbb{Q}(\mu_p)$,
- $\mathcal{S}_F = \{\wp \,|\, p \,:\, p \,|\, D_F \cdot h_F\}$, where D_F is the discriminant of F and h_F is the class number of F,
- $\mathcal{S}_\partial$ is the primes of torsion in the boundary cohomology groups (see [9, Section 3.3]), and,
- $\mathcal{S}_{\text{invariant}}$ is as in [9, Remark 6] when d is even and $n = 0$.

Let $\wp$ be a prime of K outside $\mathcal{S}$. Let p denote the residue characteristic of $\wp$. In particular since $\wp \notin \mathcal{S}_{\text{elliptic}}$ we have that $p \geq 5$.

Assume that f is ordinary at p and that the mod $\wp$ representation $\overline{\rho}_f$ attached to f satisfies $(p-\text{dist})$ and $(\text{ai}(F^*))$. Let us take the p-adic ring $\mathcal{O}$ fixed in the previous section to be $\mathcal{O} = \mathcal{O}_\wp$, the ring of integers in $K_\wp$. Let R be the universal deformation ring for deformations of $\overline{\rho}_f$ to complete noetherian local $\mathcal{O}_\wp$-algebras of type $Q = \emptyset$ described in Section 3.2.

Let $\mathcal{Q}$ denote the set of primes of F as in (2). Let $Q \subset \mathcal{Q}$ denote a finite non-empty subset of $\mathcal{Q}$ which does not meet $\mathfrak{N}$ and such that $(\text{reg}_\mathfrak{q})$ holds for each $\mathfrak{q} \in Q$. Let R_Q denote the universal deformation ring corresponding to deformations of $\overline{\rho}_f$ of type Q described in Section 3.2. By the universality of R_Q and the fact that R is a deformation of type Q we obtain a map

$$R_Q \to R.$$

Let $\mathfrak{q} \in Q$. Let $I_\mathfrak{q}$ denote the inertia subgroup at $\mathfrak{q}$. A theorem of Faltings (whose proof is analogous to Theorem 3.32 in [15]) says that there is a character $\delta_\mathfrak{q} : I_\mathfrak{q} \to R_Q^\times$ (depending on a choice of an eigenvalue of $\overline{\rho}_f(\mathrm{Frob}_q)$) such that the restriction of the universal deformation $\rho_Q : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(R_Q)$ of type Q to $I_\mathfrak{q}$ has the following shape:

$$\rho_Q|_{I_\mathfrak{q}} = \begin{pmatrix} \delta_\mathfrak{q}^{-1} & 0 \\ 0 & \delta_\mathfrak{q} \end{pmatrix}.$$

Since $\overline{\rho}_f$ is unramified at $\mathfrak{q}$ we have

$$\delta_\mathfrak{q}(I_\mathfrak{q}) \subset 1 + \mathfrak{m}_{R_Q}.$$

On the other hand since $1+\mathfrak{m}_{R_Q}$ is a pro-p group and $\overline{\rho}_f|_{D_\mathfrak{q}}$ is abelian (see page 124 of [15]) $\delta_\mathfrak{q}$ factors through the image of $I_\mathfrak{q}$ in the maximal pro-p quotient of $D_\mathfrak{q}^{\mathrm{ab}}$ which is isomorphic to $\Delta_\mathfrak{q}$, the p-Sylow subgroup of $(\mathcal{O}_F/\mathfrak{q})^\times$, by local class field theory. Via the map

$$\Delta_Q = \prod_{\mathfrak{q} \in Q} \Delta_\mathfrak{q} \xrightarrow{\prod \delta_\mathfrak{q}} R_Q^\times$$

R_Q is naturally an $\mathcal{O}_\wp[\Delta_Q]$-module. We now have the following easy proposition (see page 126 of [15] for the proof):

Proposition 1 *The natural map $R_Q \to R$ induces an isomorphism*

$$R_Q/\mathfrak{a}_Q R_Q \xrightarrow{\sim} R.$$

where $\mathfrak{a}_Q$ is the augmentation ideal of $\mathcal{O}_\wp[\Delta_Q]$.

Let $\mathrm{K}_Q = \mathrm{K}_0(\mathfrak{N}) \cap \mathrm{K}_1(Q)$. Let $S_{k,I_F}(\mathfrak{N} \cap Q, \chi)$ denote the set of holomorphic cusp forms with respect to K_Q. Then there is a natural inclusion map

$$S_{k,I_F}(\mathfrak{N}, \chi) \hookrightarrow S_{k,I_F}(\mathfrak{N} \cap Q, \chi). \tag{4}$$

Let $h_k(\mathfrak{N}, \chi, \mathcal{O}_\wp)$ denote the subalgebra of $\mathrm{End}(S_{k,I_F}(\mathfrak{N}, \chi))$ generated by all the Hecke operators. Similarly let $h_k(\mathfrak{N} \cap Q, \chi, \mathcal{O}_\wp)$ denote the subalgebra of $\mathrm{End}(S_{k,I_F}(\mathfrak{N} \cap Q, \chi))$ generated by all the Hecke operators. These algebras contain the diamond operators outside the level (see page 314 of [12] for the definition of these operators).

Let $\mathbb{F}$ denote the residue field of $\mathcal{O}_\wp$. The primitive form f considered as a mod $\wp$ modular form determines an algebra homomorphism

$$h_k(\mathfrak{N}, \chi, \mathcal{O}_\wp) \to \mathbb{F}$$

and therefore a maximal ideal $\mathfrak{m}$ of $h_k(\mathfrak{N}, \chi, \mathcal{O}_\wp)$. Let

$$T = h_k(\mathfrak{N}, \chi, \mathcal{O}_\wp)_\mathfrak{m}$$

denote the localization of $h_k(\mathfrak{N}, \chi, \mathcal{O}_\wp)$ at $\mathfrak{m}$.

Since the map (4) is not Hecke equivariant at the primes $\mathfrak{q} \in Q$ there is no natural map $h_k(\mathfrak{N} \cap Q, \chi, \mathcal{O}_\wp) \to h_k(\mathfrak{N}, \chi, \mathcal{O}_\wp)$. However a standard procedure allows one to choose a maximal ideal $\mathfrak{m}_Q$ of $h_k(\mathfrak{N} \cap Q, \chi, \mathcal{O}_\wp)$, the choice depending on that of the eigenvalues in the definition of the $\delta_\mathfrak{q}$ for $\mathfrak{q} \in Q$, such that for a prime $\wp'|\wp$ in a suitable finite extension of K the associated mod $\wp'$ eigenform in $S_{k,I_F}(\mathfrak{N} \cap Q, \chi)$ is congruent to f outside Q. Let T_Q be the localization of $h_k(\mathfrak{N} \cap Q, \chi, \mathcal{O}_\wp)$ at $\mathfrak{m}_Q$:

$$T_Q = h_k(\mathfrak{N} \cap Q, \chi, \mathcal{O}_\wp)_{\mathfrak{m}_Q}.$$

Hida theory combined with the theory of pseudo-deformations shows that T_Q (up to a possible twist to get the determinant right) is a solution to the deformation problem for $\overline{\rho}_f$ of type Q described in Section 3.2. By the universality of the deformation ring R_Q we obtain a map

$$R_Q \to T_Q.$$

Note that T_Q is naturally an $\mathcal{O}_\wp[\Delta_Q]$-module via the action of the diamond operators. One may check that the above map is actually a map of $\mathcal{O}_\wp[\Delta_Q]$-algebras.

We now define an $\mathcal{O}_\wp[\Delta_Q]$-module M_Q attached to Q. Let $\mathcal{C}$ denote the group of complex conjugations. The group $\mathcal{C}$ has cardinality 2^d with $d = [F : \mathbb{Q}]$ and has a natural action on cohomology. Let $\widehat{\mathcal{C}}$ denote the group of characters of $\mathcal{C}$ and fix $\epsilon \in \widehat{\mathcal{C}}$. When $n > 0$ or d is odd set

$$M_Q = \mathrm{H}^d_{\mathrm{p,ord}}(Y(\mathrm{K}_Q), \mathcal{L}(n, \chi, \mathcal{O}_\wp))[\chi, \epsilon]_{\mathfrak{m}_Q}.$$

Thus M_Q is a suitable localization of the ordinary part of the middle dimensional parabolic cohomology group of the Hilbert Blumenthal variety of level $\mathrm{K}_Q = \mathrm{K}_0(\mathfrak{N}) \cap \mathrm{K}_1(Q)$. Let us point out a small abuse of notation in the definition of M_Q. Since the Hecke algebra $h_k(\mathfrak{N} \cap Q, \chi, \mathcal{O}_\wp)$ does not necessarily act on the cohomology group used to define M_Q we should really localize at a pre-image $\tilde{\mathfrak{m}}_Q$ of $\mathfrak{m}_Q$ in an abstract Hecke algebra. However for notational convenience we do not do this. This abuse of notation will occur in the sequel frequently (for instance in the definition of M below). As for the notation in square brackets, we take the χ-eigenspace under the action of the strict class group of F (note $\wp$ is prime to the strict class number of F since $\wp \notin \mathcal{S}_F \subset \mathcal{S}$ and $\wp \nmid 2$). Similarly we take the direct sum of the ϵ and $-\epsilon$ eigenspaces under the action of $\mathcal{C}$ (note $\wp \nmid 2$). M_Q is well defined since $\wp \notin \mathcal{S}_{\text{elliptic}} \subset \mathcal{S}$ (cf. Section 3.1 [9]). When $n = 0$ and d is even we define M_Q as above except that we take the cuspidal cohomology instead of parabolic cohomology (cf. [9, Remark 6]). We remark that M_Q is naturally a T_Q-module and therefore also an $\mathcal{O}_\wp[\Delta_Q]$-module.

Finally if either $n > 0$ or d is odd set

$$M = \mathrm{H}^d_{\mathrm{p,ord}}(Y(\mathfrak{N}), \mathcal{L}(n, \chi, \mathcal{O}_\wp))[\chi, \epsilon]_{\mathfrak{m}}.$$

If $n = 0$ and d is even we define M as above except that again we take cuspidal cohomology instead of parabolic cohomology.

For each $m \in \mathbb{N}$ consider the subset $\mathcal{Q}(m) \subset \mathcal{Q}$ defined by

$$\mathcal{Q}(m) = \left\{ \mathfrak{q} \in \mathcal{Q} \;\middle|\; \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{q}) \equiv 1 \bmod p^m \text{ and } \overline{\rho}_f \text{ satisfies } (\mathrm{reg}_{\mathfrak{q}}) \right\}.$$

Let L be the splitting field of the projective image of $\overline{\rho}_f$. Then $\mathcal{Q}(m)$ consists of those primes $\mathfrak{q}$ of F such that $\mathrm{Frob}_{\mathfrak{q}} \in \mathrm{Gal}(L(\mu_{p^m})/F)$ fixes $F(\mu_{p^m})$ and has order dividing p. The Chebotarev density theorem shows that if $\overline{\rho}_f$ satisfies $(\mathrm{ai}(F^*))$ then there are infinitely many primes in $\mathcal{Q}(m)$. For each $m \in \mathbb{N}$ choose a non-empty finite subset $Q_m \subset \mathcal{Q}(m)$. Let R_m, respectively T_m, respectively M_m denote the objects R_Q, respectively T_Q, respectively M_Q defined above for $Q = Q_m$. Then $R, (R_m, T_m, M_m), m \in \mathbb{N}$ is a Taylor-Wiles system in the sense of Definition 1.

Note that Q_m satisfies (TW1) for all $m \in \mathbb{N}$. In the next subsection we shall show that the Q_m can be chosen to satisfy (TW2) and (TW3) as well under certain simplifying assumptions on the weight and level; that is we shall show that we may choose the sets Q_m to have a common cardinality r with the property that R_m is generated as an $\mathcal{O}_\wp$-algebra by at most r elements. When F is a real quadratic field (so $d = 2$) we will show that this Taylor-Wiles system satisfies (TW4) and (TW5) as well (under the additional assumption that the strict class number of F is one and a certain vanishing assumption on boundary cohomology groups). Theorems 5 and 6 will yield that

$$R \xrightarrow{\sim} T,$$

and that M is a free T-module.

4.3 (TW1), (TW2) and (TW3)

In this section we show that (TW1), (TW2) and (TW3) can be made to hold for the Taylor-Wiles system constructed in Section 4.2 when the level $\mathfrak{N} = 1$ and when the weight $k \neq 2$, $p + 1$ (see the condition (Sel) below). We borrow heavily from the original Galois cohomological arguments of Wiles [27] which continue to apply in the Hilbert modular setting with some minor modifications. We have also benefited greatly from the exposition of this part of Wiles' work in Chapter 3 of Hida [15].

Fix $m \in \mathbb{N}$ and let Q stand for the subset $Q_m \subset \mathcal{Q}(m)$ chosen at the end of Section 4.2. Denote by $F^{Q \cup \{p\}}$ the maximal extension of F unramified outside the primes of F dividing p and the primes in Q. Let $\mathfrak{G}_Q = \mathrm{Gal}(F^{Q \cup \{p\}}/F)$.

Let $W = \mathrm{Ad}^0(\overline{\rho}_f)$ be the three dimensional $\mathfrak{G}_Q$-module over $\mathbb{F}$, arising from the adjoint representation on the 2 by 2 matrices over $\mathbb{F}$ of trace 0.

For each $\mathfrak{q} \in Q \cup \{\mathfrak{p} \mid p\}$ let $B_{\mathfrak{q}}$ be an $\mathbb{F}$-subspace of $\mathrm{H}^1(D_{\mathfrak{q}}, W)$. We define the Selmer group attached to the $\mathfrak{G}_Q$-module W and the local conditions $B_{\mathfrak{q}}$, for $\mathfrak{q} \in Q \cup \{\mathfrak{p} \mid p\}$, as follows. Set

$$\mathrm{Sel}_Q(W) := \beta_Q^{-1}\left(\prod_{\mathfrak{q} \in Q \cup \{\mathfrak{p} \mid p\}} B_{\mathfrak{q}}\right),$$

where β_Q is the natural restriction map:

$$\beta_Q : \mathrm{H}^1(\mathfrak{G}_Q, W) \longrightarrow \prod_{\mathfrak{q} \in Q \cup \{\mathfrak{p} \mid p\}} \mathrm{H}^1(D_{\mathfrak{q}}, W).$$

Here $D_{\mathfrak{q}}$ is the decomposition group at $\mathfrak{q}$ inside $\mathrm{Gal}(\overline{F}/F)$.

Consider the following local conditions in the definition of the Selmer group:

- $B_{\mathfrak{q}} = \mathrm{H}^1(D_{\mathfrak{q}}, W)$, for each $\mathfrak{q} \in Q$, and,
- $B_{\mathfrak{p}}$ is given by

  $$B_{\mathfrak{p}} = \ker\left(\mathrm{H}^1(D_{\mathfrak{p}}, W) \to \mathrm{H}^1(I_{\mathfrak{p}}, W/W_0)\right),$$

  for each $\mathfrak{p} \mid p$, where W_0 is the sub-representation of W consisting of matrices of the form $\left(\begin{smallmatrix} 0 & \star \\ 0 & 0 \end{smallmatrix}\right)$ with respect to a basis such that $\overline{\rho}_f|_{D_{\mathfrak{p}}} = \left(\begin{smallmatrix} \overline{\delta}_{\mathfrak{p}} & * \\ 0 & \overline{\epsilon}_{\mathfrak{p}} \end{smallmatrix}\right)$ for $\mathfrak{p} \mid p$.

Lemma 1 *Let R_Q denote the universal deformation ring corresponding to $Q = Q_m$. Let $t_Q = \mathfrak{m}_{R_Q}/(\mathfrak{m}_{R_Q}^2 + \mathfrak{m}_{\mathcal{O}_\wp} R_Q)$ be the cotangent space of R_Q. Then with the choice of local conditions $B_{\mathfrak{q}}$ as above, we have*

$$t_Q \xrightarrow{\sim} \mathrm{Sel}_Q(W).$$

In particular the number of generators of R_Q as an $\mathcal{O}$-algebra $= \dim \mathrm{Sel}_Q(W)$*, the dimension of* $\mathrm{Sel}_Q(W)$ *over* $\mathbb{F}$*.*

Proof. This is well known (see, for instance, [15], Lemma 3.38). □

Consider the Selmer group attached to the dual representation of W defined as follows. Set $W^* = \mathrm{Hom}_{\mathbb{F}}(W, \mathbb{F})$ and set $W^*(1) = W^* \otimes_{\mathbb{F}} \mu_p$. (In our case since $W \subset \mathrm{M}_2(\mathbb{F})$, the non-degenerate pairing $(X, Y) \mapsto \mathrm{Tr}(XY)$ shows that $W^* \xrightarrow{\sim} W$. Thus we have $W^*(1) \xrightarrow{\sim} W(1)$). Here is the first of the well known facts in Galois cohomology that we shall need and that we simply state without proof:

Fact: Local Tate duality. (See [15], Theorem 4.43). There is a natural duality between

$$\mathrm{H}^{2-r}(D_{\mathfrak{q}}, W) \text{ and } \mathrm{H}^r(D_{\mathfrak{q}}, W^*(1)) = \mathrm{H}^r(D_{\mathfrak{q}}, W(1)) \tag{5}$$

for $r = 0, 1, 2$.

For an arbitrary subspace $B_{\mathfrak{q}} \subset \mathrm{H}^1(D_{\mathfrak{q}}, W)$, for $\mathfrak{q} \in Q \cup \{\mathfrak{p} \mid p\}$, let $B_{\mathfrak{q}}^{\perp} \subset \mathrm{H}^1(D_{\mathfrak{q}}, W^*(1))$ denote the orthogonal compliment of $B_{\mathfrak{q}}$ under the pairing of (5). Define the Selmer group $\mathrm{Sel}_Q(W^*(1))$ with respect to the subspaces $B_{\mathfrak{q}}^{\perp}$ as follows. For the restriction map

$$\beta_Q^* : \mathrm{H}^1(\mathfrak{G}_Q, W^*(1)) \longrightarrow \prod_{\mathfrak{q} \in Q \cup \{\mathfrak{p} \mid p\}} \mathrm{H}^1(D_{\mathfrak{q}}, W^*(1)),$$

let us set

$$\mathrm{Sel}_Q(W^*(1)) := {\beta_Q^*}^{-1} \left(\prod_{\mathfrak{q} \in Q \cup \{\mathfrak{p} \mid p\}} B_{\mathfrak{q}}^{\perp} \right).$$

Note that for the $B_{\mathfrak{q}}$ chosen as above we have $B_{\mathfrak{q}}^{\perp} = 0$ if $\mathfrak{q} \in Q$. We now quote the following fact:

Fact: Poitou-Tate exact sequence. (See [15], Theorem 4.50). For each $\mathfrak{q} \in Q \cup \{\mathfrak{p} \mid p\}$, let $B_{\mathfrak{q}}$ be an arbitrary subspace of $\mathrm{H}^1(D_{\mathfrak{q}}, W)$. Then, there is an exact sequence

$$0 \to \mathrm{Sel}_Q(W) \to \mathrm{H}^1(\mathfrak{G}_Q, W) \to \prod_{\mathfrak{q} \in Q \cup \{\mathfrak{p} \mid p\}} \frac{\mathrm{H}^1(D_{\mathfrak{q}}, W)}{B_{\mathfrak{q}}} \to \mathrm{Sel}_Q(W^*(1))^*$$
$$\to \mathrm{H}^2(\mathfrak{G}_Q, W) \to \prod_{\mathfrak{q} \in Q \cup \{\mathfrak{p} \mid p\}} \mathrm{H}^2(D_{\mathfrak{q}}, W) \to \mathrm{H}^0(\mathfrak{G}_Q, W^*(1))^* \to 0.$$

We now claim

$$\mathrm{H}^0(\mathfrak{G}_Q, W) = 0 = \mathrm{H}^0(\mathfrak{G}_Q, W^*(1))^*. \tag{6}$$

To see this suppose that W has a one dimensional subspace on which $\mathfrak{G}_Q$ acts by a character, say ϕ. Any non-zero element of this subspace may be viewed as an endomorphism of $V(\overline{\rho}_f) \cong \mathbb{F}^2$. This element cannot be a scalar since it has trace zero and $p > 2$. By Schur's lemma we deduce that $\overline{\rho}_f$ is not absolutely irreducible when restricted to $\ker(\phi)$. Thus either $\overline{\rho}_f$ is not absolutely irreducible over F or ϕ is a quadratic character. Now if ϕ is trivial then $\overline{\rho}_f$ is not absolutely irreducible over F, contradicting (ai(F^*)), and so the first equality in (6) must hold. On the other hand if ϕ is the restriction of ω_p^{-1} (the inverse of the Teichmüller character) to $\mathfrak{G}_Q$, then the fixed field of $\ker(\phi)$ is $F(\mu_p)$ so that $[F(\mu_p) : F] = 2$. This forces $\mathbb{Q}(\mu_p)^+ \subset F$ which is a contradiction since $\wp \notin \mathcal{S}_{\mathrm{elliptic}}$. Thus the second equality in (6) also holds.

We now need the following formula:

Fact: Global Euler characteristic formula. (See [15], Theorem 4.53).

$$\dim \mathrm{H}^0(\mathfrak{G}_Q, W) - \dim \mathrm{H}^1(\mathfrak{G}_Q, W) + \dim \mathrm{H}^2(\mathfrak{G}_Q, W) = \sum_{\nu \mid \infty} \left(\dim \mathrm{H}^0(\mathrm{Gal}(\overline{F}_\nu / F_\nu), W) - \dim W \right). \tag{7}$$

Let c_ν denote a complex conjugation at ν. Since $\det \overline{\rho}_f(c_\nu) = -1$, we have $\overline{\rho}_f(c_\nu) \sim \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, so that the eigenvalues of c_ν on W are $-1, +1, -1$. This means that the value of the expression on the RHS of (7) is d times $1 - 3 = -2$, where $d = [F : \mathbb{Q}]$ is the number of infinite places of F.

Now let us assume that we have made the choice of the local conditions at $\mathfrak{q} \in Q \cup \{\mathfrak{p} \mid p\}$, as mentioned above. Set

$$d_Q = \dim \mathrm{Sel}_Q(W) - \dim \mathrm{Sel}_Q(W^*(1)).$$

For $\mathfrak{p} \mid p$, let

$$h_\mathfrak{p} = \dim \mathrm{H}^0(D_\mathfrak{p}, W^*(1)) - \dim \frac{\mathrm{H}^1(D_\mathfrak{p}, W)}{B_\mathfrak{p}}.$$

and let $h_p = \sum_{\mathfrak{p}|p} h_\mathfrak{p}$. By the Poitou-Tate exact sequence, the global Euler characteristic formula, local Tate duality, and (6), we have:

$$d_Q = h_p + 2d + \sum_{\mathfrak{q} \in Q} \dim \mathrm{H}^0(D_\mathfrak{q}, W^*(1)). \tag{8}$$

Since $\wp \notin \mathcal{S}_F \subset \mathcal{S}$ the prime p is unramified in F. For each prime $\mathfrak{p}$ of F lying over p let $f_\mathfrak{p}$ denote the residue degree of $\mathfrak{p}$. We now impose an additional condition (recall we have already assumed that $\mathfrak{N} = 1$ so that the finite order character associated to χ is trivial):

(Sel) $\det \rho_f = \nu_p^{k-1}$ with $k \not\equiv 2 \pmod{p-1}$.

Since $\wp \notin \mathcal{S}_{\mathrm{weight}} = \{\wp | p : p \le k-2\} \subset \mathcal{S}$, the assumption (Sel) is equivalent to requiring that $k \neq 2$, $p+1$. We now have the following key proposition:

Proposition 2 *Assume that* (Sel) *holds. We have*

1. $h_\mathfrak{p} + 2f_\mathfrak{p} \le 0$, *for all* $\mathfrak{p}|p$.
2. $\dim \mathrm{H}^0(D_\mathfrak{q}, W^*(1)) = 1$, *for all* $\mathfrak{q} \in Q$.

Proof. Since $\mathrm{cd}(D_\mathfrak{p}) = 2$, the exact sequence

$$0 \to W_0 \to W \to W/W_0 \to 0,$$

yields the following long exact sequence in cohomology:

$$0 \to \mathrm{image}(u) \to \mathrm{H}^1(D_\mathfrak{p}, W/W_0) \to \mathrm{H}^2(D_\mathfrak{p}, W_0) \to \mathrm{H}^2(D_\mathfrak{p}, W) \to \mathrm{H}^2(D_\mathfrak{p}, W/W_0) \to 0,$$

where u is the map defined by

$$u : \mathrm{H}^1(D_\mathfrak{p}, W) \to \mathrm{H}^1(D_\mathfrak{p}, W/W_0).$$

Thus we have

$$\begin{aligned} \dim \mathrm{image}(u) &= \dim \mathrm{H}^1(D_\mathfrak{p}, W/W_0) - \dim \mathrm{H}^2(D_\mathfrak{p}, W_0) \\ &\quad + \dim \mathrm{H}^2(D_\mathfrak{p}, W) - \dim \mathrm{H}^2(D_\mathfrak{p}, W/W_0). \end{aligned}$$

Now consider the following commutative diagram

$$\begin{array}{ccccccccc} & & & & H^1(D_{\mathfrak{p}}, W) & & & & \\ & & & & \downarrow u & \searrow \delta & & & \\ 0 & \longrightarrow & H^1(D_{\mathfrak{p}}/I_{\mathfrak{p}}, (W/W_0)^{I_{\mathfrak{p}}}) & \longrightarrow & H^1(D_{\mathfrak{p}}, W/W_0) & \longrightarrow & H^1(I_{\mathfrak{p}}, W/W_0)^{D_{\mathfrak{p}}} & \longrightarrow & 0, \end{array}$$

where the bottom row comes from the inflation-restriction sequence, and the map δ is defined by the triangle above. By the definition of the Selmer group,

$$h_{\mathfrak{p}} = \dim H^0(D_{\mathfrak{p}}, W^*(1)) - \dim \mathrm{image}(\delta).$$

In any case we see that

$$\dim \mathrm{image}(\delta) \geq \dim \mathrm{image}(u) - \dim H^1(D_{\mathfrak{p}}/I_{\mathfrak{p}}, (W/W_0)^{I_{\mathfrak{p}}}).$$

But

$$H^1(D_{\mathfrak{p}}/I_{\mathfrak{p}}, (W/W_0)^{I_{\mathfrak{p}}}) \xrightarrow{\sim} (W/W_0)^{I_{\mathfrak{p}}}/(\mathrm{Frob}_{\mathfrak{p}} - 1)(W/W_0)^{I_{\mathfrak{p}}}.$$

Moreover there is an exact sequence

$$0 \to H^0(D_{\mathfrak{p}}/I_{\mathfrak{p}}, (W/W_0)^{I_{\mathfrak{p}}}) \to (W/W_0)^{I_{\mathfrak{p}}} \stackrel{\mathrm{Frob}_{\mathfrak{p}}-1}{\longrightarrow} (W/W_0)^{I_{\mathfrak{p}}} \to H^1(D_{\mathfrak{p}}/I_{\mathfrak{p}}, (W/W_0)^{I_{\mathfrak{p}}}) \to 0.$$

This shows that

$$\dim H^1(D_{\mathfrak{p}}/I_{\mathfrak{p}}, W/W_0)^{I_{\mathfrak{p}}} = \dim H^0(D_{\mathfrak{p}}/I_{\mathfrak{p}}, W/W_0)^{I_{\mathfrak{p}}} = \dim H^0(D_{\mathfrak{p}}, W/W_0).$$

Putting things together we get:

$$\begin{aligned} \dim \mathrm{image}(\delta) \quad \geq \quad & \dim H^1(D_{\mathfrak{p}}, W/W_0) - \dim H^2(D_{\mathfrak{p}}, W_0) + \dim H^2(D_{\mathfrak{p}}, W) \\ & - \dim H^2(D_{\mathfrak{p}}, W/W_0) - \dim H^0(D_{\mathfrak{p}}, W/W_0). \end{aligned}$$

One last formula we need is the following:

Fact: Local Euler characteristic formula. (See [15], Theorem 4.52).

$$\begin{aligned} -\dim H^0(D_{\mathfrak{p}}, W/W_0) + \dim H^1(D_{\mathfrak{p}}, W/W_0) - \dim H^2(D_{\mathfrak{p}}, W/W_0) \\ = \dim(W/W_0) \cdot f_{\mathfrak{p}} = 2f_{\mathfrak{p}}. \end{aligned}$$

Using it we see that:

$$\begin{aligned} h_{\mathfrak{p}} \quad &= \quad \dim H^0(D_{\mathfrak{p}}, W^*(1)) - \dim \mathrm{image}(\delta) \\ &\leq \quad \dim H^0(D_{\mathfrak{p}}, W^*(1)) - 2f_{\mathfrak{p}} + \dim H^2(D_{\mathfrak{p}}, W_0) - \dim H^2(D_{\mathfrak{p}}, W) \\ &= \quad -2f_{\mathfrak{p}} + \dim H^0(D_{\mathfrak{p}}, W_0^*(1)), \end{aligned}$$

where the last equality follows by local Tate-duality (applied twice: once for W and once for W_0).

We now claim that the condition (Sel) implies that $\mathrm{H}^0(D_{\mathfrak{p}}, W_0^*(1)) = 0$. Part 1) of the proposition then follows immediately. To see this note that by (Sel) we may write

$$\bar{\rho}_f|_{I_{\mathfrak{p}}} = \begin{pmatrix} \omega_p^{k-1} & * \\ 0 & 1 \end{pmatrix},$$

where ω_p is the Teichmüler character. Since

$$\begin{pmatrix} \omega_p^{k-1} & * \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \star \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \omega_p^{k-1} & * \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & \omega_p^{k-1}\star \\ 0 & 0 \end{pmatrix}$$

we see that $I_{\mathfrak{p}}$ acts on W_0 by ω_p^{k-1}, and therefore on $W_0^*(1)$ by ω_p^{2-k}. The condition (Sel) then shows that $\mathrm{H}^0(D_{\mathfrak{p}}, W_0^*(1)) = 0$.

As for part 2) note that $\mathfrak{q} \in Q$ implies that $\mathrm{N}_{F|\mathbb{Q}}(\mathfrak{q}) \equiv 1 \bmod p$, so $W^*(1) = W(1) = W$. Consequently since the eigenvalues of $\mathrm{Frob}_{\mathfrak{q}}$ on W are $\bar{\alpha}_{\mathfrak{q}}/\bar{\beta}_{\mathfrak{q}}$, 1, and $\bar{\beta}_{\mathfrak{q}}/\bar{\alpha}_{\mathfrak{q}}$, and $\bar{\alpha}_{\mathfrak{q}} \neq \bar{\beta}_{\mathfrak{q}}$ by $(\mathrm{reg}_{\mathfrak{q}})$, we see that $\dim \mathrm{H}^0(D_{\mathfrak{q}}, W^*(1)) = 1$. □

Corollary 1

$$d_Q \leq |Q|.$$

Proof. By Proposition 2 we have $h_p = \sum_{\mathfrak{p}|p} h_{\mathfrak{p}} \leq -2d$ since $\sum_{\mathfrak{p}|p} f_{\mathfrak{p}} = d$. The corollary then follows immediately from equation (8). □

Let

$$r := \dim \mathrm{Sel}_{\emptyset}(W^*(1))$$

be the dimension of the Selmer group when $Q = \emptyset$. Our next objective is to show that we may choose $Q = Q_m \subset \mathcal{Q}(m)$ such that $|Q| = r$ and so that $\mathrm{Sel}_Q(W^*(1)) = 0$. Lemma 1 and Corollary 1 will then show that this Q satisfies (TW1 - 3). Indeed, since $\mathrm{Sel}_Q(W^*(1)) = 0$, we see that $d_Q = \dim t_Q$, and so R_Q is generated by at most r elements as an $\mathcal{O}_\wp$-algebra.

Proposition 3 *There are infinitely many sets $Q \subset \mathcal{Q}(m)$ such that*

1. $|Q| = r = \dim \mathrm{Sel}_{\emptyset}(W^*(1))$, *and,*
2. $\mathrm{Sel}_Q(W^*(1)) = 0$.

Proof. Recall that $Q \subset \mathcal{Q}(m)$ was an arbitrarily chosen non-empty subset of $\mathcal{Q}(m)$. Since $B_{\mathfrak{q}}^{\perp} = 0$ for all $q \in Q$, we have

$$\mathrm{Sel}_Q(W^*(1)) \subset \ker \beta'_Q$$

where

$$\beta'_Q : \mathrm{H}^1(\mathfrak{G}_Q, W^*(1)) \longrightarrow \prod_{\mathfrak{q} \in Q} \mathrm{H}^1(D_{\mathfrak{q}}, W^*(1))$$

is the map obtained from β_Q^* by ignoring the restriction at all the primes $\mathfrak{p}|p$.

Let K_0 be the fixed field of $\ker \overline{\rho}_f$. Let $\mathfrak{h}_Q = \mathrm{Gal}(F^{Q\cup\{p\}}/K_0(\mu_p)) \subset \mathfrak{G}_Q$. When $Q = \emptyset$, we write $\mathfrak{G}$ (respectively $\mathfrak{h}$) for $\mathfrak{G}_Q$ (respectively $\mathfrak{h}_Q$). Let us also set $G = \mathrm{Gal}(K_0(\mu_p)/F)$.

We claim that $\ker \beta'_Q \subset \ker \beta_Q^\dagger$ where

$$\beta_Q^\dagger : \mathrm{H}^1(\mathfrak{G}_\emptyset, W^*(1)) \longrightarrow \prod_{\mathfrak{q}\in Q} \mathrm{H}^1(D_{\mathfrak{q}}, W^*(1)).$$

To see this suppose that $f \in \ker \beta'_Q$. Then the restriction of f to $\mathfrak{h}_Q$ is a homomorphism $\mathfrak{h}_Q \to W^*(1)$ which is locally trivial at all $\mathfrak{q} \in Q$. In particular this homomorphism factors through $\mathfrak{h}$. This shows that f itself is trivial on $\mathrm{Gal}(F^{Q\cup p}/F^p)$ so that $f \in \ker \beta_Q^\dagger$.

We now show that when the cardinality of $|Q|$ is sufficiently large, $\beta_Q^\dagger$ is injective. After what we have said above, we see that this will force $\mathrm{Sel}_Q(W^*(1))$ to vanish (when $|Q|$ is sufficiently large).

The following lemma is an easy modification of the corresponding lemma in [27]:

Lemma 2 *If $\wp \notin \mathcal{S}_{\mathrm{elliptic}}$ then*

$$\mathrm{H}^1(G, W(1)) = 0.$$

Proof. If $p \not| \, |\mathrm{image}(\overline{\rho}_f)|$, then $p \not| \, [K_0 : F]$, and so $p \not| \, |G|$ as well. Since $W(1)$ is a p-group, the lemma follows in this case.

So let us assume that $p \, \big| \, |\mathrm{image}(\overline{\rho}_f)|$. The inflation-restriction sequence yields

$$\begin{aligned} 0 \to \mathrm{H}^1(\mathrm{Gal}(K_0/F), W(1)^{\mathrm{Gal}(K_0(\mu_p)/K_0)}) &\to \mathrm{H}^1(G, W(1)) \\ &\to \mathrm{H}^1(\mathrm{Gal}(K_0(\mu_p)/K_0), W(1)) = 0, \end{aligned}$$

where the last group vanishes since $K_0(\mu_p)/K_0$ is a prime to p extension. Now $\mathrm{Gal}(K_0(\mu_p)/K_0)$ fixes W element wise, so if $\mathrm{Gal}(K_0(\mu_p)/K_0) \neq 1$ we see that $W(1)^{\mathrm{Gal}(K_0(\mu_p)/K_0)} = 0$, and the lemma follows again in this case. Thus we may assume that $K_0(\mu_p) = K_0$.

Let Z be the center of $G = \mathrm{Gal}(K_0/F)$. Again we have the inflation-restriction sequence

$$0 \to \mathrm{H}^1(G/Z, W(1)^Z) \to \mathrm{H}^1(G, W(1)) \to \mathrm{H}^1(Z, W(1)) = 0,$$

where, as before, the last group vanishes since $p \not| \, |Z|$. Since $\overline{\rho}_f$ is absolutely irreducible we see that Z, considered as a subgroup of $\mathrm{GL}_2(\mathbb{F})$, consists of scalar matrices. This means that Z acts trivially on W. If Z acts non-trivially on μ_p we have $W(1)^Z = 0$, and we get that $\mathrm{H}^1(G, W(1)) = 0$ and again the lemma follows. So we may assume that Z acts on μ_p trivially.

In this case we see that $\mathrm{Gal}(F(\mu_p)/F)$ is a quotient of G/Z. Now G/Z is not contained in a Borel subgroup by the absolute irreducibility hypothesis (ai(F^*)). By a general result about subgroups of $\mathrm{PGL}_2(\mathbb{F})$ we conclude that G/Z is isomorphic to $\mathrm{PGL}_2(k)$ or $\mathrm{PSL}_2(k)$ for some finite field $k \subset \overline{\mathbb{F}}$ (see [15], page 146). But this is a contradiction, since the latter group is simple since $p \geq 5$, and the former group has only one normal subgroup of index 2, and $[F(\mu_p) : F] > 2$ since $\wp \notin \mathcal{S}_{\text{elliptic}}$. □

Let us return to the proof of Proposition 3. By Lemma 2, the inflation-restriction sequence yields:

$$0 = \mathrm{H}^1(G, W(1)) \to \mathrm{H}^1(\mathfrak{G}, W(1)) \xrightarrow{\iota} \mathrm{H}^1(\mathfrak{h}, W(1))^G = \mathrm{Hom}_G(\mathfrak{h}, W(1)).$$

Now fix $0 \neq x \in \ker \beta_Q^\dagger$, and let $f_x : \mathfrak{h} \to W(1)$ be the image of x under ι. The image of $\overline{\rho}_f$ in $\mathrm{PGL}_2(\mathbb{F})$ either has cardinality divisible by p, or is dihedral, or is isomorphic to one of the groups A_4, S_4 or A_5. Suppose momentarily that this image is not dihedral.

Lemma 3 *Suppose that the image of $\overline{\rho}_f$ in $\mathrm{PGL}_2(\mathbb{F})$ is of order divisible by p or is isomorphic to one of the groups A_4, S_4 or A_5. Then there is an element $\sigma \in \mathfrak{G}$ such that*

(1) $\overline{\rho}_f(\sigma)$ has order ℓ, where $\ell \geq 3$ is prime to p, and,

(2) σ fixes $F(\mu_{p^m})$ (so $\det \overline{\rho}_f(\sigma) = 1$).

Proof. This is [27], Lemma 1.10; see also [15], Lemma 3.43. The proof uses results of Dickson. □

We claim that we may additionally assume that

(3) $f_x(\sigma^\ell) \neq 0$.

To see this let L be the fixed field of the kernel of f_x. Then the group $X = \mathrm{Gal}(L/K_0(\mu_p))$ is abelian of exponent p. We have the exact sequence

$$0 \to X \to \mathrm{Gal}(L/F) \to G \to 0.$$

Note that G acts on X via conjugation and $f_x : X \to W(1)$ is an injective morphism of G-modules. Now let σ' satisfy the conditions (1) and (2) above. Then $\mathrm{Ad}(\overline{\rho}_f)(\sigma')$ has three distinct eigenvalues on W and therefore on X and one of them is equal to 1. Write

$$X = X[1] \oplus X',$$

where $\sigma' = 1$ on $X[1]$ and $\sigma' - 1$ is an automorphism of X'. Arguing as on [27, page 523] we may assume that $f_x(X[1]) \neq 0$. Thus we may choose an element $\tau \in X[1]$ such that $f_x(\tau) \neq 0$.

By (6) we see that $W(1)^G = 0$ so that $X^G = 0$. On the other hand G acts trivially on $\mathrm{Gal}(K_0(\mu_{p^m})/K_0(\mu_p))$. Thus the fields L and $K_0(\mu_{p^m})$ are linearly disjoint over $K_0(\mu_p)$. Set

$$\tau' := 1 \times \tau \in \mathrm{Gal}(K_0(\mu_{p^m})/K_0(\mu_p)) \times \mathrm{Gal}(L/K_0(\mu_p)) = \mathrm{Gal}(L(\mu_{p^m})/K_0(\mu_p)).$$

Since $\tau \in X[1]$, τ' commutes with σ' in $\mathrm{Gal}(L(\mu_{p^m})/F)$. Then, noting that ${\sigma'}^{\ell} \in X$, we have

$$f_x((\tau'\sigma')^{\ell}) = f_x({\tau'}^{\ell}{\sigma'}^{\ell}) = \ell f_x(\tau') + f_x({\sigma'}^{\ell}).$$

Since ℓ is prime to p, $\ell f_x(\tau') \neq 0$, and so one of $\tau'\sigma'$ or σ' satisfies (1), (2) and (3) above. This proves the claim.

Now choose a prime $\mathfrak{q} \notin Q$ such that $\mathrm{Frob}_{\mathfrak{q}} = \sigma$ in $\mathrm{Gal}(L(\mu_{p^m})/F)$. Then the fact that $f_x(\mathrm{Frob}_{\mathfrak{q}}^{\ell}) \neq 0$ implies that $\beta^{\dagger}_{Q\cup\{\mathfrak{q}\}}(x) \neq 0$. By (2) we see that $\mathrm{N}_{F|\mathbb{Q}}(\mathfrak{q}) \equiv 1 \bmod p^m$. Further (1) and (2) imply that the characteristic roots $\overline{\alpha}$ and $\overline{\beta}$ of $\overline{\rho}_f(\sigma)$ satisfy $\overline{\alpha}\overline{\beta} = 1$ and hence are primitive ℓ^{th} roots of unity. Since $\ell \geq 3$ we have $\overline{\alpha} \neq \overline{\beta}$. This shows that

$$Q \cup \{\mathfrak{q}\} \subset \mathcal{Q}(m).$$

We have shown that for $0 \neq x \in \ker \beta^{\dagger}_Q$ there is a prime $\mathfrak{q} \notin Q$ such that $Q \cup \{\mathfrak{q}\} \subset \mathcal{Q}(m)$ and $\beta^{\dagger}_{Q\cup\{\mathfrak{q}\}}(x) \neq 0$. Iterating this statement we may enlarge Q sufficiently so that that $Q \subset \mathcal{Q}(m)$ and $\beta^{\dagger}_Q$ is injective. We now have

$$0 = \mathrm{Sel}_Q(W^*(1)) \subset \mathrm{Sel}_{\emptyset}(W^*(1)) \subset \mathrm{H}^1(\mathfrak{G}_{\emptyset}, W^*(1)) \xrightarrow{\beta^{\dagger}_Q} \prod_{\mathfrak{q}\in Q} \mathrm{H}^1(D_{\mathfrak{q}}, W^*(1)).$$

By the local Euler characteristic formula $\dim \mathrm{H}^1(D_{\mathfrak{q}}, W^*(1)) > 0$. In fact by this formula $\dim \mathrm{H}^1(D_{\mathfrak{q}}, W^*(1)) = \dim \mathrm{H}^0(D_{\mathfrak{q}}, W^*(1)) + \dim \mathrm{H}^2(D_{\mathfrak{q}}, W^*(1)) = 1 + 1 = 2$, where H^0 is computed using Proposition 2 and H^2 is computed using the same proposition by first using local Tate duality and the fact that as a $D_{\mathfrak{q}}$-module $W \xrightarrow{\sim} W^*(1)$. We may now remove primes from Q, one at a time, preserving the injectivity of $\beta^{\dagger}_Q$, until we reach $|Q| = r$. Thus we can find a Q as claimed in the statement of Proposition 3. The fact that we can find infinitely many such $Q's$ is not needed but it follows from the Chebotarev density theorem.

(We thank the referee for clarifying the following points which had confused us. The target of the map $\beta^{\dagger}_Q$ is slightly different from $\prod_{\mathfrak{q}\in Q} \mathrm{H}^1(D_{\mathfrak{q}}/I_{\mathfrak{q}}, W^*(1))$, which was the target of the map on [25, page 567, line 15] used in the original Taylor-Wiles argument. There, the dimension of each term $\mathrm{H}^1(D_{\mathfrak{q}}/I_{\mathfrak{q}}, W^*(1))$ was 1, and not 2. The first point to note here is that the argument goes through as long as the target has the form $\prod_{\mathfrak{q}\in Q} A_{\mathfrak{q}}$, with $\dim A_{\mathfrak{q}} > 0$. The second point is that the above target is not in fact substantially different from the one given in [25]. Indeed, since $\mathrm{N}_{F|\mathbb{Q}}(\mathfrak{q}) \equiv 1 \bmod p$, we see that $W^*(1) = W$ as a $D_{\mathfrak{q}}$-module, and then the first part of the inflation-restriction sequence

$$0 \to \mathrm{H}^1(D_{\mathfrak{q}}/I_{\mathfrak{q}}, W) \to \mathrm{H}^1(D_{\mathfrak{q}}, W) \to \mathrm{H}^1(I_{\mathfrak{q}}, W)^{D_{\mathfrak{q}}}$$

shows that we are simply working with a slightly larger space. Moreover, the first cohomology group is isomorphic to $W/(\mathrm{Frob}_{\mathfrak{q}} - 1)W$, which is indeed one-dimensional by $(\mathrm{reg}_{\mathfrak{q}})$, and the last cohomology group is just $\mathrm{Hom}_{D_{\mathfrak{q}}}(I_{\mathfrak{q}}^{\text{tame}}, W)$, easily seen to be $W^{\langle \mathrm{Frob}_{\mathfrak{q}} \rangle}$, and so is again one-dimensional by ($\mathrm{reg}_{\mathfrak{q}}$). All of this matches with our earlier computation showing that the middle cohomology group is two-dimensional.)

If the image of $\overline{\rho}_f$ in $\mathrm{PGL}_2(\mathbb{F})$ is dihedral then we can still proceed as follows.

Lemma 4 *Suppose that $\overline{\rho}_f$ satisfies $(\mathrm{ai}(F^*))$. If the image of $\overline{\rho}_f$ in $\mathrm{PGL}_2(\mathbb{F})$ is dihedral then for any irreducible Galois stable subspace Y of $W \otimes \bar{\mathbb{F}}$ there exists an element $\sigma \in \mathfrak{G}$ such that*

(1) the image of $\overline{\rho}_f(\sigma)$ in $\mathrm{PGL}_2(\mathbb{F})$ is non-trivial,

(2) σ fixes $F(\mu_{p^m})$, and,

(3) σ has an eigenvalue 1 on Y.

Proof. This is essentially Lemma 1.12 in [27], due to Taylor. □

One may now pick $\sigma \in \mathfrak{G}$ satisfying the first two conditions of the lemma, and by the third condition of the lemma, we may assume in addition that $f_x(\sigma^\ell) \neq 0$ where ℓ is the order of $\overline{\rho}_f(\sigma)$ (note ℓ is prime to p). The argument now proceeds as before finishing the proof of Proposition 3. □

4.4 A vanishing theorem

Let F be, as usual, a totally real field of degree $d > 1$ and $\mathcal{O}_F$ the ring of integers of F. Let $\Gamma \subset \mathrm{SL}_2(\mathcal{O}_F)$ be an arithmetic subgroup. In fact we shall assume that

$$\Gamma = \Gamma_0(\mathfrak{N}) \cap \Gamma_1(Q)$$

where $Q \subset \mathcal{Q}$ is a finite set of primes of F as in previous sections and $\Gamma_1(Q)$ denotes the obvious congruence subgroup (we are using Q to denote both the set and the ideal consisting of the product of primes in this set).

The aim of this section is to prove the following vanishing theorem for the ordinary part of the first degree parabolic cohomology group of Γ with divisible coefficients. The hypotheses imposed in the theorem are sufficient to treat the case of level $\mathfrak{N} = 1$. The proof uses the congruence subgroup property for Γ (see [21]) and was partly inspired by Buecker [1] where a similar theorem was proven in the case of $\mathrm{GSp}_{4/\mathbb{Q}}$.

Theorem 7 *Let F be a totally real field of degree $d > 1$ of strict class number 1. Let $p > 3$ and assume p is unramified in F. Assume that $\mathfrak{N}$ is square free and that $\mathfrak{N}Q$ is prime to 6. When $n = 0$ assume that p does not divide $|(\mathcal{O}_F/\mathfrak{N})^\times|$. If $n > 0$ assume that the finite order character $\chi_{\mathfrak{N}}$ associated to χ is trivial. Then*

$$\mathrm{H}^1_{\mathrm{p,ord}}(\Gamma, L(n, \chi, K_\wp/\mathcal{O}_\wp)) = 0.$$

Proof. First assume that $n = 0$. Then it suffices to show that

$$\mathrm{H}^1(\Gamma, K_\wp/\mathcal{O}_\wp) = 0.$$

Let $f : \Gamma \to K_\wp/\mathcal{O}_\wp \in \mathrm{H}^1(\Gamma, K_\wp/\mathcal{O}_\wp)$. Then f factors through Γ/Γ' where Γ' is the commutator subgroup of Γ. We claim that $\Gamma' \subset \Gamma_1(\mathfrak{N}) \cap \Gamma(Q)$ with finite index divisible only by primes dividing 6. Indeed locally for a place v of F an elementary computation using matrices shows that the commutator subgroup of $\Gamma_0(v)$ is $\Gamma_1(v)$ and similarly the commutator subgroup of $\Gamma_1(v)$ is the principal congruence subgroup $\Gamma(v)$. It is also well known that $\mathrm{SL}_2(\mathcal{O}_{F_v})$ is perfect for v prime to 6 and that for $v|6$ the index of the commutator subgroup is divisible at most by primes dividing 6. Using these facts along with the hypothesis that $\mathfrak{N}Q$ is square free and prime to 6 the claim follows using the congruence subgroup property due to Serre [21]. On the other hand $[\Gamma : \Gamma_1(\mathfrak{N}) \cap \Gamma(Q)]$ divides $[\Gamma_0(\mathfrak{N}) : \Gamma_1(\mathfrak{N})] \cdot [\Gamma_1(Q) : \Gamma(Q)]$. Thus $[\Gamma : \Gamma']$ is prime to p since p is prime to 6, p does not divide $[\Gamma_0(\mathfrak{N}) : \Gamma_1(\mathfrak{N})] = |(\mathcal{O}_F/\mathfrak{N})^\times|$ by hypothesis, and neither does it divide $[\Gamma_1(Q) : \Gamma(Q)] = \mathrm{N}_{F|\mathbb{Q}}(Q)$ since $\mathrm{N}_{F|\mathbb{Q}}(\mathfrak{q}) \equiv 1 \mod p$ for each $\mathfrak{q} \in Q$. We conclude that $f = 0$ proving the theorem in the case $n = 0$.

Now assume that $n > 0$. Since the finite order character $\chi_{\mathfrak{N}}$ associated to χ is trivial [14, Theorem 7.2] shows that

$$\mathrm{H}^1_{\mathrm{p,ord}}(\Gamma, L(n, \chi, K_\wp/\mathcal{O}_\wp)) \stackrel{\simeq}{=} \mathrm{H}^1_{\mathrm{p,ord}}(\Gamma \cap \Gamma_0(p), L(n, \chi, K_\wp/\mathcal{O}_\wp)).$$

Here and below we continue to write χ in the Γ-module $L(n, \chi, K_\wp/\mathcal{O}_\wp)$ even though $\chi_{\mathfrak{N}}$ is trivial. Let us change notation and replace $\mathfrak{N} \cdot p \cdot Q$ by $\mathfrak{N}$. Then it suffices to show that

$$\mathrm{H}^1_{\mathrm{p,ord}}(\Gamma, L(n, \chi, K_\wp/\mathcal{O}_\wp)) = 0 \tag{9}$$

where $\Gamma_1(\mathfrak{N}) \subset \Gamma \subset \Gamma_0(\mathfrak{N})$ with $\mathfrak{N}$ divisible by $p\mathcal{O}_F$. Note that the hypotheses made in the theorem imply that we may assume $\mathfrak{N}$ is square free and prime to 6.

Let π denote a uniformizer for $\mathcal{O}_\wp$. The exact sequence of Γ-modules

$$1 \to L(n, \chi, \frac{1}{\pi}\mathcal{O}_\wp/\mathcal{O}_\wp) \to L(n, \chi, K_\wp/\mathcal{O}_\wp) \xrightarrow{\pi} L(n, \chi, K_\wp/\mathcal{O}_\wp) \to 1$$

induces the following diagram with exact rows

$$\begin{array}{ccccc}
\mathrm{H}^1(\Gamma, L(n, \chi, \frac{1}{\pi}\mathcal{O}_\wp/\mathcal{O}_\wp)) & \longrightarrow & \mathrm{H}^1(\Gamma, L(n, \chi, K_\wp/\mathcal{O}_\wp)) & \xrightarrow{\pi} & \mathrm{H}^1(\Gamma, L(n, \chi, K_\wp/\mathcal{O}_\wp)) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{H}^1_\partial(\Gamma, L(n, \chi, \frac{1}{\pi}\mathcal{O}_\wp/\mathcal{O}_\wp)) & \longrightarrow & \mathrm{H}^1_\partial(\Gamma, L(n, \chi, K_\wp/\mathcal{O}_\wp)) & \xrightarrow{\pi} & \mathrm{H}^1_\partial(\Gamma, L(n, \chi, K_\wp/\mathcal{O}_\wp)).
\end{array}$$

Here the notation H^1_∂ means boundary cohomology group and the vertical maps are given by restriction. By considering the kernels of the vertical maps and noting that the above diagram is equivariant for the action of the Hecke operators (for which see [13, pages 288-89]) we obtain the following exact sequence:

$$\mathrm{H}^1_{\mathrm{p,ord}}(\Gamma, L(n, \chi, \frac{1}{\pi}\mathcal{O}_\wp/\mathcal{O}_\wp)) \to \mathrm{H}^1_{\mathrm{p,ord}}(\Gamma, L(n, \chi, K_\wp/\mathcal{O}_\wp)) \xrightarrow{\pi} \mathrm{H}^1_{\mathrm{p,ord}}(\Gamma, L(n, \chi, K_\wp/\mathcal{O}_\wp)).$$

Since every element of $\mathrm{H}^1_{\mathrm{p,ord}}(\Gamma, L(n, \chi, K_\wp/\mathcal{O}_\wp))$ is π^s-torsion for some s we see that to show (9) it suffices to show that

$$\mathrm{H}^1_{\mathrm{p,ord}}(\Gamma, L(n, \chi, \frac{1}{\pi}\mathcal{O}_\wp/\mathcal{O}_\wp)) = 0. \tag{10}$$

Recall that we have assumed that the strict class number of F is 1. Consider the Hecke operator

$$T_p = \left[\Gamma \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \Gamma\right].$$

It is well known that one can decompose

$$\Gamma \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \Gamma \quad = \quad \bigcup_u \alpha_u \Gamma$$

where u varies over a set of representatives of $\mathcal{O}_F/p$ and where

$$\alpha_u = \left(\begin{smallmatrix} p & u \\ 0 & 1 \end{smallmatrix}\right).$$

For each $\gamma \in \Gamma$ there is a unique $\gamma_u \in \Gamma$ such that $\gamma\alpha_u = \alpha_v\gamma_u$ where v depends on u. The action of T_p on a cocycle $f : \Gamma \to L$ is given by the following formula

$$T_p(f)(\gamma) = \sum_u \alpha_v \cdot f(\gamma_u). \tag{11}$$

Now consider the exact sequence

$$1 \to \Gamma_1(\mathfrak{N}) \to \Gamma \to \Gamma/\Gamma_1(\mathfrak{N}) \to 1.$$

The corresponding inflation-restriction sequence yields the following exact sequence in cohomology

$$0 \to \mathrm{H}^1(\Gamma/\Gamma_1(\mathfrak{N}), L^{\Gamma_1(\mathfrak{N})}) \to \mathrm{H}^1(\Gamma, L) \to \mathrm{H}^1(\Gamma_1(\mathfrak{N}), L) \tag{12}$$

where we have set $L = L(n, \chi, \frac{1}{\pi}\mathcal{O}_\wp/\mathcal{O}_\wp) = L(n, \chi, \mathbb{F})$ for $\mathbb{F}$ the residue field of $\mathcal{O}_\wp$. This allows us to break our analysis of the cohomology into two further parts namely the 'toral part' and the 'unipotent part'. We deal with the 'toral part' first. Below, for a group G, a normal subgroup N and a G-module A we sometimes identify $\mathrm{H}^1(G/N, A^N)$ with its image in $\mathrm{H}^1(G, A)$ under

$$\mathrm{Inf} : \mathrm{H}^1(G/N, A^N) \hookrightarrow \mathrm{H}^1(G, A).$$

Lemma 5 *We have*

$$\mathrm{H}^1_{\mathrm{ord}}(\Gamma/\Gamma_1(\mathfrak{N}), L^{\Gamma_1(\mathfrak{N})}) = 0.$$

Proof. Let $f : \Gamma/\Gamma_1(\mathfrak{N}) \to L^{\Gamma_1(\mathfrak{N})}$ be a cocycle. Then γ_u and γ have the same toral part so that $\gamma_u \equiv \gamma \mod \Gamma_1(\mathfrak{N})$. In particular $f(\gamma_u) = f(\gamma)$ for all u. So (11) shows

$$T_p(f)(\gamma) = \sum_u \alpha_v \cdot f(\gamma). \tag{13}$$

In particular the restriction of $T_p(f)$ to $\Gamma_1(\mathfrak{N})$ is trivial so that the class of $T_p(f)$ lies in $\mathrm{H}^1(\Gamma/\Gamma_1(\mathfrak{N}), L^{\Gamma_1(\mathfrak{N})})$. Thus T_p preserves this last space and it makes sense to speak of its ordinary part.

Recall that L consists of polynomials over $\mathbb{F}$ in the pairs of variables (X_σ, Y_σ) as σ varies through the embeddings of F into K which are homogeneous of degree n in each pair (X_σ, Y_σ). Further the action of a matrix $\delta \in \mathrm{M}_2(\mathcal{O}_F)$ on $P(X_\sigma, Y_\sigma)$ is given by replacing $(X_\sigma, Y_\sigma)^t$ by $(\delta^\sigma)^\iota \cdot (X_\sigma, Y_\sigma)^t$ where $(\delta^\sigma)^\iota = \det(\delta^\sigma)\cdot(\delta^\sigma)^{-1}$. Since f takes values in the $\Gamma_1(\mathfrak{N})$-invariants, $f(\gamma) = P(X_\sigma, Y_\sigma)$ has no terms that are pure monomials in the X_σ. It follows that α_v kills $f(\gamma)$ since for each σ, Y_σ get replaced by pY_σ, which vanishes since we are working in characteristic p. Thus the formula (13) shows that $T_p(f) = 0$. □

It remains to consider the 'unipotent part'. We have:

Lemma 6

$$\mathrm{H}^1_{\mathrm{p,ord}}(\Gamma_1(\mathfrak{N}), L) = 0.$$

Proof. Consider the map $i : L \to \mathbb{F}$ defined by picking out the coefficient of the monomial which is pure in the X_σ (equivalently by setting all $Y_\sigma = 0$). Putting the trivial action of $\Gamma_1(\mathfrak{N})$ on $\mathbb{F}$ one easily checks that the map i is $\Gamma_1(\mathfrak{N})$-equivariant. Hence one has an exact sequence

$$\mathrm{H}^1_{\mathrm{p}}(\Gamma_1(\mathfrak{N}), \ker(i)) \to \mathrm{H}^1_{\mathrm{p}}(\Gamma_1(\mathfrak{N}), L) \to \mathrm{H}^1_{\mathrm{p}}(\Gamma_1(\mathfrak{N}), \mathbb{F})$$

Clearly $\ker(i)$ is spanned by monomials that have at least one Y_σ in them. One sees therefore that the α_v preserve $\ker(i)$ so that T_p acts on $\mathrm{H}^1(\Gamma_1(\mathfrak{N}), \ker(i))$. In fact an argument identical to that in the proof of Lemma 5 shows that T_p kills this space. It follows that

$$\mathrm{H}^1_{\mathrm{p,ord}}(\Gamma_1(\mathfrak{N}), L) \hookrightarrow \mathrm{H}^1_{\mathrm{p,ord}}(\Gamma_1(\mathfrak{N}), \mathbb{F})$$

and so to prove the lemma it suffices to show that $\mathrm{H}^1_{\mathrm{p,ord}}(\Gamma_1(\mathfrak{N}), \mathbb{F}) = 0$.

In fact we show $\mathrm{H}^1_{\mathrm{p}}(\Gamma_1(\mathfrak{N}), \mathbb{F}) = 0$. We first claim that the commutator subgroup of $\Gamma_1(\mathfrak{N})$ is contained in the principal congruence subgroup $\Gamma(\mathfrak{N})$ with index divisible only by primes dividing 6. Indeed as we have already remarked locally the commutator subgroup of $\Gamma_1(v)$ is the principal congruence subgroup $\Gamma(v)$ for each place $v|\mathfrak{N}$ and $\mathrm{SL}_2(\mathcal{O}_{F_v})$ is perfect for v prime to 6 and has commutator subgroup of index divisible only by primes dividing 6 if $v|6$. Since $\mathfrak{N}$ is square free and prime to 6 the claim follows again by the congruence subgroup property due to Serre [21].

Now each element x in $\Gamma_1(\mathfrak{N})$ can be written as a product $x = \gamma u$ where $\gamma \in \Gamma(\mathfrak{N})$ and u is a unipotent element of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. By what we have said above there is a positive integer a divisible only by the primes 2 and 3 such that $\gamma^a = (xu^{-1})^a$ is in the commutator subgroup of $\Gamma_1(\mathfrak{N})$. Let $f : \Gamma_1(\mathfrak{N}) \to \mathbb{F}$ be a homomorphism in $\mathrm{H}^1_{\mathrm{p}}(\Gamma_1(\mathfrak{N}), \mathbb{F})$. Since $f(\gamma^a) = 0$ and a is prime to $p > 5$ we see that $f(\gamma) = 0$ Since f is 'parabolic' f vanishes on unipotent elements and $f(u) = 0$. We conclude that $f(x) = 0$. Thus $f = 0$ proving the lemma. □

Theorem 7 now follows in the case $n > 0$ from (12) and Lemmas 5 and 6 above. $\square$

4.5 (TW4) and (TW5)

In this section we reduce (TW4) and (TW5) to the vanishing of certain cohomology groups under the technical assumptions that $n > 0$, the strict class number of F is one, and a vanishing assumption on certain boundary cohomology groups. We then use Theorem 7 to verify that (TW4) and (TW5) hold when F is a real quadratic field under the above technical assumptions.

Fix m and let $Q = Q_m$. Recall that

$$M_Q = \mathrm{H}^d_{\mathrm{p,ord}}(Y(\mathrm{K}_Q), \mathcal{L}(n, \chi, \mathcal{O}_\wp))[\chi, \epsilon]_{\mathfrak{m}_Q}$$

where we take cuspidal cohomology instead of parabolic cohomology when $n = 0$ and d is even. (The second χ can in fact be dropped from the notation in view of the assumption that the strict class number of F is 1 but we maintain it). M_Q has a natural action of $\mathcal{O}_\wp[\Delta_Q]$ via the diamond Hecke operators. For (TW4) we must show that M_Q is a free $\mathcal{O}_\wp[\Delta_Q]$-module of rank independent of m.

To show this freeness we may assume that $\mathcal{O}_\wp$ contains the values of all the characters of Δ_Q since a finite extension of $\mathcal{O}_\wp$ is faithfully flat over $\mathcal{O}_\wp$. Let $\psi : \Delta_Q \to {\mathcal{O}_\wp}^\times$ be such a character. We also write ψ for the induced algebra homomorphism $\psi : \mathcal{O}_\wp[\Delta_Q] \to \mathcal{O}_\wp$. Let $\mathfrak{a}_{Q,\psi}$ denote the ideal of $\mathcal{O}_\wp[\Delta_Q]$ generated by elements of the form $g - \psi(g)$. Thus $\mathfrak{a}_{Q,\psi}$ is the kernel of $\psi : \mathcal{O}_\wp[\Delta_Q] \to \mathcal{O}_\wp$. When $\psi = 1$ we recover the usual augmentation ideal $\mathfrak{a}_Q$.

Lemma 7 *M_Q is $\mathcal{O}_\wp[\Delta_Q]$-free if and only if $M_Q \otimes_{\mathcal{O}[\Delta_Q],\psi} \mathcal{O}_\wp = M_Q/\mathfrak{a}_{Q,\psi} M_Q$ is $\mathcal{O}_\wp$-free for each character $\psi : \Delta_Q \to {\mathcal{O}_\wp}^\times$.*

Proof. One direction is clear. We prove the other. Suppose that

$$\frac{M_Q}{\mathfrak{a}_{Q,\psi} M_Q} \xrightarrow{\sim} {\mathcal{O}_\wp}^{s_\psi},$$

for some positive integer s_ψ. Let $\mathfrak{n}$ denote the maximal ideal and let $\mathbb{F}$ denote the residue field of the local ring $\mathcal{O}_\wp[\Delta_Q]$. Going modulo $\mathfrak{n}$ we get

$$\frac{M_Q}{\mathfrak{n} M_Q} \xrightarrow{\sim} \mathbb{F}^{s_\psi}.$$

In particular we see that s_ψ must be independent of ψ; call the common value s. By Nakayama's lemma we have a surjection

$$\mathcal{O}_\wp[\Delta_Q]^s \overset{\pi}{\twoheadrightarrow} M_Q.$$

Tensoring this with $\mathcal{O}_\wp[\Delta_Q]/\mathfrak{a}_{Q,\psi}$ we get a surjection

$${\mathcal{O}_\wp}^s \overset{\pi\otimes 1}{\twoheadrightarrow} {\mathcal{O}_\wp}^s$$

which must be an isomorphism. Thus $\ker(\pi) \subset \mathfrak{a}_{Q,\psi}^s$ for each ψ. We claim that $\cap_\psi \mathfrak{a}_{Q,\psi} = 0$. The claim implies π is injective showing that M_Q is $\mathcal{O}_\wp[\Delta_Q]$-free of rank s. To see the claim let $\sum a_g g \in \cap_\psi \mathfrak{a}_{Q,\psi}$ where the sum is over $g \in \Delta_Q$ and $a_g \in \mathcal{O}_\wp$. Then $\sum a_g \psi(g) = 0$ for all ψ. One can now check that the only solution to this system of equations is the trivial solution: $a_g = 0$ for all $g \in \Delta_Q$. □

Let us write $M_Q(\psi)$ for M_Q thought of as a module for $\mathcal{O}_\wp[\Delta_Q]$ with the action twisted by ψ. Let N_Q denote the Pontryagin dual of M_Q. We now make the following assumption. Recall that $\mathrm{K}_Q = \mathrm{K}_0(\mathfrak{N}) \cap \mathrm{K}_1(Q)$. Set $\mathrm{K}_{0,Q} = \mathrm{K}_0(\mathfrak{N}) \cap \mathrm{K}_0(Q)$.

Assumption 1 Let $\partial(Y(\mathrm{K})^*)$ denote the boundary of the Borel-Serre compactification $Y(\mathrm{K})^*$ of the Hilbert-Blumenthal variety $Y(\mathrm{K})$ attached to a compact open subgroup $\mathrm{K} \subset \mathrm{GL}_2(\hat{\mathcal{O}}_F)$. Then the following boundary cohomology groups vanish:

$$\begin{aligned} \mathrm{H}^q(\partial(Y(\mathrm{K}_Q)^*), \mathcal{L}(n, \chi, K_\wp/\mathcal{O}_\wp))_{\mathfrak{m}_Q} &= 0, \\ \mathrm{H}^q(\partial(Y(\mathrm{K}_{0,Q})^*), \mathcal{L}(n, \chi, K_\wp/\mathcal{O}_\wp)(\psi))_{\mathfrak{m}_Q} &= 0 \end{aligned}$$

for $0 \leq q \leq 2d$.

For the definition of the boundary cohomology groups and the Hecke action on them we refer the reader to [13, pages 288-89]. Assumption 1 may be thought of as the statement that the boundary cohomology groups are 'Eisenstein'.

An argument similar to the one used to prove the duality statement [9, Theorem 3] shows that

$$N_Q = \mathrm{H}^d_{\mathrm{p,ord}}(Y(\mathrm{K}_Q), \mathcal{L}(n, \chi, K_\wp/\mathcal{O}_\wp))[\chi, \epsilon]_{\mathfrak{m}_Q} \tag{14}$$

at least if $n > 0$. Indeed if $n > 0$ the obstruction to the perfectness of the pairing

$$M_Q \otimes \mathrm{H}^d_{\mathrm{p,ord}}(Y(\mathrm{K}_Q), \mathcal{L}(n, \chi, K_\wp/\mathcal{O}_\wp))[\chi, \epsilon]_{\mathfrak{m}_Q} \longrightarrow K_\wp/\mathcal{O}_\wp$$

is the torsion in the first cohomology group (of degree d) in Assumption 1 which vanishes by hypothesis. If $n = 0$ then we must take cuspidal cohomology everywhere instead of parabolic cohomology and then the analogue of (14) is true if we omit an additional finite set of primes $\wp$ which may depend on Q (this set of primes is similar to the set $\mathcal{S}_{\text{invariant}}$ that arose in [9, Remark 6]). For this reason we avoid the case $n = 0$. Note however that if the ordinary idempotent kills the invariant forms then the ordinary parts of the cuspidal and parabolic cohomology groups coincide (cf. [9, Remark 7]) in which case the proof given here works for $n = 0$ as well.

Write $N_Q(\psi)$ for N_Q with ψ-twisted Δ_Q-action. Also write $N_Q^q(\psi)$ for the cohomology group (14) but in degree q. Thus $N_Q^d(\psi) = N_Q(\psi)$. For $r \geq 0$ let

$$L_Q^r(\psi) = \mathrm{H}^r_{\mathrm{p,ord}}(Y(\mathrm{K}_{0,Q}), \mathcal{L}(n, \chi, K_\wp/\mathcal{O}_\wp)(\psi))[\chi, \epsilon]_{\mathfrak{m}_Q}.$$

We now wish to compute using group cohomology. We therefore make the simplifying assumption that the strict class number of F is one, the main advantage of this being that all the Hilbert-Blumenthal varieties we consider have only one connected component. In particular we have

$$Y(K_Q) = \Gamma_0(\mathfrak{N}) \cap \Gamma_1(Q) \backslash \mathcal{Z} \quad \text{and} \quad Y(K_{0,Q}) = \Gamma_0(\mathfrak{N}) \cap \Gamma_0(Q) \backslash \mathcal{Z}$$

where $\mathcal{Z} = H^d$ is the usual d-fold product of the upper half plane.

We also think of the above congruence subgroups as subgroups of $\mathrm{SL}_2(\mathcal{O}_F)$ rather than $\mathrm{PGL}_2(\mathcal{O}_F)_+$. Although this is not strictly correct it is of no matter since the exact sequence

$$1 \to \{\pm 1\} \to \mathrm{SL}_2(\mathcal{O}_F) \to \mathrm{PGL}_2(\mathcal{O}_F)_+ \to \mathcal{O}_{F+}^\times/(\mathcal{O}_F^\times)^2 = (\mathbb{Z}/2)^{d'} \to 1$$

for some $d' \leq d$ shows that the cohomology groups of congruence subgroups of $\mathrm{SL}_2(\mathcal{O}_F)$ and $\mathrm{PGL}_2(\mathcal{O}_F)_+$ are essentially the same when 2 is invertible in the coefficients.

Now Assumption 1 along with the boundary exact sequence shows that the cohomology groups

$$\begin{aligned} N_Q^q &= \mathrm{H}^q_{?,\mathrm{ord}}(Y(\mathrm{K}_Q), \mathcal{L}(n,\chi,K_\wp/\mathcal{O}_\wp))[\chi,\epsilon]_{\mathfrak{m}_Q}, \\ L_Q^q(\psi) &= \mathrm{H}^q_{?,\mathrm{ord}}(Y(\mathrm{K}_{0,Q}), \mathcal{L}(n,\chi,K_\wp/\mathcal{O}_\wp)(\psi))[\chi,\epsilon]_{\mathfrak{m}_Q}, \end{aligned}$$

are the same for $? = \mathrm{p}, \mathrm{c}, \emptyset$. In view of this the Hochschild-Serre spectral sequence reads:

$$E_2^{pq} = \mathrm{H}^p(\Delta_Q, N_Q^q(\psi)) \Longrightarrow L_Q^{p+q}(\psi). \tag{15}$$

Proposition 4 *Let $\wp$ be a prime of K with $\wp \notin \mathcal{S}$. Suppose that* Assumption 1 *holds and that $n > 0$. Assume also that*

$$N_Q^q(\psi) = 0 \tag{16}$$

for $0 \leq q \leq d-1$ and all characters $\psi : \Delta_Q \to \mathcal{O}_\wp$. Then (TW4) *and* (TW5) *hold.*

Proof. Since the Pontryagin dual of M_Q is N_Q, the Pontryagin dual of $M_Q/\mathfrak{a}_{Q,\psi}M_Q$ is $N_Q(\psi)^{\Delta_Q}$. By Lemma 7, M_Q is $\mathcal{O}_\wp[\Delta_Q]$-free if and only if $N_Q(\psi)^{\Delta_Q}$ is divisible for each character ψ. Now the spectral sequence (15) and the assumptions on the E_2 term, namely that $N_Q^q(\psi) = 0$ for $0 \leq q \leq d-1$, imply that $N_Q(\psi)^{\Delta_Q} = N_Q^d(\psi)^{\Delta_Q} = L_Q^d(\psi)$. Thus to show that M_Q is $\mathcal{O}_\wp[\Delta_Q]$-free it suffices to show that $L_Q^d(\psi)$ is divisible for each character ψ. Now the exact sequence

$$1 \to L(n,\chi,\mathcal{O}_\wp)(\psi) \to L(n,\chi,K_\wp)(\psi) \to L(n,\chi,K_\wp/\mathcal{O}_\wp)(\psi) \to 1$$

induces the obvious long exact sequence in cohomology. It follows that to show $L_Q^d(\psi)$ is divisible it is enough to show that

$$\mathrm{H}^{d+1}_{\mathrm{p,ord}}(Y(\mathrm{K}_{0,Q}), \mathcal{L}(n,\chi,\mathcal{O}_\wp)(\psi))[\chi,\epsilon]_{\mathfrak{m}_Q}$$

is torsion-free. The vanishing of the second boundary cohomology group (of degree d) in Assumption 1 and the fact that $n > 0$ imply that the Pontryagin dual of the above module is $L_Q^{d-1}(\psi)$. This is proved similarly to (14) above. Now an inspection of the spectral sequence (15) shows that $L_Q^{d-1}(\psi)$ vanishes proving that M_Q is $\mathcal{O}_\wp[\Delta_Q]$-free. This proves (TW4) except for the fact that the rank of M_Q as a free $\mathcal{O}_\wp[\Delta_Q]$-module is *a priori* dependent on Q. However once we prove (TW5) below, this rank will in fact be independent of Q.

To get (TW5) it is enough, by taking Pontryagin duals, to show that $N_Q^{\Delta_Q} = N$ where N is the Pontryagin dual of M. Let $\psi = 1$ be the trivial character. Then the hypotheses of the proposition and the spectral sequence (15) show that $N_Q^{\Delta_Q} = L$ where $L := L_Q^d(1)$. Consider the restriction map

$$\mathrm{H}^d_{\mathrm{p,ord}}(Y(\mathfrak{N}), \mathcal{L}(n,\chi,K_\wp/\mathcal{O}_\wp)(\psi))[\chi,\epsilon] \hookrightarrow \mathrm{H}^d_{\mathrm{p,ord}}(Y(\mathrm{K}_{0,Q}), \mathcal{L}(n,\chi,K_\wp/\mathcal{O}_\wp)(\psi))[\chi,\epsilon].$$

This is injective since the index of $\Gamma_0(Q)$ in $\mathrm{SL}_2(\mathcal{O}_F)$ is prime to p, the residue characteristic of $\wp$. Recall that $\mathfrak{m}$ is the maximal ideal of $h_k(\mathfrak{N},\chi,\mathcal{O}_\wp)$ corresponding to f mod $\wp$ and that $\mathfrak{m}_Q$ is a maximal ideal of $h_k(\mathfrak{N}\cap Q,\chi,\mathcal{O}_\wp)$ corresponding to an eigenform of augmented level Q that is Q-old and which takes the same Hecke eigenvalues mod $\wp$ as f outside Q. On localizing the restriction map above we obtain an isomorphism

$$\mathrm{H}^d_{\mathrm{p,ord}}(Y(\mathfrak{N}), \mathcal{L}(n,\chi,K_\wp/\mathcal{O}_\wp)(\psi))[\chi,\epsilon]_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{H}^d_{\mathrm{p,ord}}(Y(\mathrm{K}_{0,Q}), \mathcal{L}(n,\chi,K_\wp/\mathcal{O}_\wp)(\psi))[\chi,\epsilon]_{\mathfrak{m}_Q},$$

which in the notation above can be written as $L \xrightarrow{\sim} N$ when $\psi = 1$. This proves (TW5). As mentioned above the rank of M_Q as an $\mathcal{O}_\wp[\Delta_Q]$-module is consequently independent of Q. Thus (TW4) holds as well. $\square$

Checking the vanishing hypotheses of Proposition 4 seems to be a difficult task; in fact the vanishing may not even be true without further assumptions on the maximal ideal $\mathfrak{m}_Q$ at which one is localizing. Here we will be content with checking the vanishing hypothesis in the first non-trivial case $d = 2$, namely in the case that F is a real quadratic field. We must show that

$$N_Q^0(\psi) = 0 \quad \text{and} \quad N_Q^1(\psi) = 0. \tag{17}$$

The fact that $N_Q^1(\psi) = 0$ follows immediately from Theorem 7 as long as we assume that $\mathfrak{N}$ is square free, that $\mathfrak{N}Q$ is prime to 6 (arranging that Q is prime to 6 is easy: one just avoids the finitely many prime $\mathfrak{q} \in \mathcal{Q}$ lying over 6), that p is prime to $|(\mathcal{O}_F/\mathfrak{N})^\times|$ when $n = 0$ and that $\chi_\mathfrak{N} = 1$ when $n > 0$ (note $p \nmid 6$ since $\wp \notin \mathcal{S}_{\mathrm{elliptic}}$ and p is unramified in F since $\wp \notin \mathcal{S}_F$). On the other hand $N_Q^0(\psi) = 0$ follows trivially if either $n > 0$ or if $n = 0$ and $\chi_\mathfrak{N}$ is non-trivial, since in these cases the action of $\Gamma_0(\mathfrak{N}) \cap \Gamma_1(Q)$ is non-trivial. Even if $n = 0$ and $\chi_\mathfrak{N} = 1$ we still get that $\mathrm{H}^0_{\mathrm{p,ord}}(\Gamma_0(\mathfrak{N}) \cap \Gamma_1(Q), K_\wp/\mathcal{O}_\wp)_{\mathfrak{m}_Q} = 0$. This is because when the action is trivial the map from H^0 to the boundary cohomology group in degree 0 is just the diagonal map $a \mapsto (a, a, \ldots, a)$ for $a \in K_\wp/\mathcal{O}_\wp$ and so is injective. Thus (17) holds. As a result we obtain the following corollary to Proposition 4.

Corollary 2 *Suppose that $d = 2$ so that F is a real quadratic field (of strict class number 1). Assume that $\wp \notin \mathcal{S}$, that $\mathfrak{N}$ is square free and prime to 6, that $n > 0$, that $\chi_{\mathfrak{N}} = 1$, and that* Assumption 1 *holds. Then the Taylor-Wiles system constructed in Section 4.2 satisfies* (TW4) *and* (TW5).

We have now verified the axioms (TW1-5) for the Taylor-Wiles system constructed in Section 4.2 in the case $d = 2$ under the following assumptions: F has strict class number 1, $\mathfrak{N} = 1$, $k \neq 2, p+1$, and the boundary cohomology groups are 'Eisenstein' (Assumption 1). In the case $d > 2$ we have verified (TW1-5) under the additional general vanishing hypotheses (16). We can therefore state the central theorem of this paper:

Theorem 8 *Let F be a totally real field of degree $d \geq 2$ and strict class number 1. Let $\wp \notin \mathcal{S}$ and suppose that $k \neq 2$, $p+1$ and that $\mathfrak{N} = 1$. Let f mod $\wp$ correspond to the maximal ideal $\mathfrak{m} \subset h_k(\mathfrak{N}, \chi, \mathcal{O}_\wp)$. Assume that $\overline{\rho}_f$ satisfies* $(\mathrm{ai}(F^*))$ *and that* Assumption 1 holds. *Assume that $\wp$ is ordinary for f and that $\overline{\rho}_f$ satisfies* $(p - \mathrm{dist})$. *Let*

$$M = \mathrm{H}^d_{\mathrm{p,ord}}(Y(\mathfrak{N}), \mathcal{L}(n, \chi, \mathcal{O}_\wp))[\chi, \epsilon]_{\mathfrak{m}}$$

be the direct sum of the ϵ and $-\epsilon$ eigenspaces of the localization at $\mathfrak{m}$ of the ordinary part of the middle dimensional parabolic cohomology group of $Y(\mathfrak{N})$ with integral weight $n = k - 2$ coefficients. If

- *$d = 2$, or,*
- *$d > 2$ and the vanishing hypotheses* (16) *hold,*

then M is a free T-module of rank 2 where $T = h_k(\mathfrak{N}, \chi, \mathcal{O}_\wp)_{\mathfrak{m}}$.

Proof. The freeness is an immediate consequence of Theorems 5 and 6 for the Taylor-Wiles system constructed in this section. The rank statement follows by 'tensoring up to $\mathbb{C}$' and comparing dimensions using the Eichler-Shimura-Harder isomorphism (for which see Section 4.1 of [9]). □

5 Application to congruences

In this section we use Theorem 8 to obtain a converse to the main result proved in [9], namely Theorem 1 of the Introduction. Let us start by recalling this result. Let F be a totally real field, and let f be a primitive cusp form defined over F of parallel weight. Let $\wp \notin \mathcal{S}$. For each character $\epsilon \in \widehat{\mathcal{C}}$ there are periods $\Omega(f, \pm\epsilon) \in \mathbb{C}^\times/\mathcal{O}_{(\wp)}{}^\times$ (cf. [9, Section 4.2.1]) such that the quotient appearing in the statement of the theorem below is in $\mathcal{O}_{(\wp)}$.

Theorem 9 ([9], Theorem 5) *Let $\wp$ be a prime of K with $\wp \notin \mathcal{S}$. If*

$$\wp \Big| \frac{W(f)\,\Gamma(1,\mathrm{Ad}(f))\,L(1,\mathrm{Ad}(f))}{\Omega(f,\epsilon)\Omega(f,-\epsilon)}$$

then $\wp$ is a congruence prime for f.

We now state and prove a converse to Theorem 9. In the case that F is a real quadratic fields the following result was stated as Theorem 3 in the Introduction.

Theorem 10 *Let f be a primitive Hilbert modular cusp form of level one and parallel weight $(k, k, \cdots k)$ defined over a totally real field F of degree $d \geq 2$ and strict class number 1. Assume that*

- *$d = 2$, or,*
- *$d > 2$ and the vanishing hypotheses* (16) *hold.*

Say that $\wp \,\big|\, p$ is a prime of K with $\wp \notin \mathcal{S}$. Assume that $k \neq 2$, $p+1$. Assume that $\overline{\rho}_f$ satisfies (ai(F^*)) *and that* Assumption 1 *holds. Let $\wp$ be an ordinary prime for f for which $\overline{\rho}_f$ satisfies* ($p-$dist). *Then $\wp$ is a congruence prime for f if and only if*

$$\wp \Big| \frac{W(f)\,\Gamma(1,\mathrm{Ad}(f))L(1,\mathrm{Ad}(f))}{\Omega(f,\epsilon)\Omega(f,-\epsilon)}$$

for some (every) $\epsilon \in \widehat{\mathcal{C}}$.

Proof. Let A be either K and let $\mathcal{O}_A$ be a valuation ring $\mathcal{O}_{(\wp)}$ of K; or let A be a completion $K_\wp$ of K with $\mathcal{O}_A = \mathcal{O}_\wp$. Then $\mathcal{O}_A$ is a Dedekind domain whose quotient field contains K. For $\epsilon \in \widehat{\mathcal{C}}$, let $L_\epsilon(\mathcal{O}_A)$ denote the image of the ordinary parabolic cohomology group

$$\mathrm{H}^d_{\mathrm{p,ord}}(Y(\mathfrak{N}), \mathcal{L}(n,\chi,\mathcal{O}_A))[\chi,\epsilon]_{\mathfrak{m}}$$

in the vector space

$$V_\epsilon(A) := \mathrm{H}^d_{\mathrm{p,ord}}(Y(\mathfrak{N}), \mathcal{L}(n,\chi,A))[\chi,\epsilon]_{\mathfrak{m}}. \tag{18}$$

Recall that $V_\epsilon(A)$ decomposes as

$$V_\epsilon(A) \;=\; V_\epsilon(A)[f] \oplus W_\epsilon(A), \tag{19}$$

where $V_\epsilon(A)[f]$ is the eigenspace of the action of Hecke algebra corresponding to f, and $W(A)$ is the orthogonal compliment of $V(A)[f]$ with respect to the pairing [,] of [9].

Let us define

$$L_{f,\epsilon}(\mathcal{O}_A) := L_\epsilon(\mathcal{O}_A) \cap V_\epsilon(A)[f], \qquad L_{W,\epsilon}(\mathcal{O}_A) := L_\epsilon(\mathcal{O}_A) \cap W_\epsilon(A);$$
$$M_{f,\epsilon}(\mathcal{O}_A) := \pi_{V_\epsilon[f]}(L_\epsilon(\mathcal{O}_A)), \qquad M_{W,\epsilon}(\mathcal{O}_A) := \pi_W(L_\epsilon(\mathcal{O}_A)),$$

where $\pi_{V_\epsilon[f]} : V_\epsilon \to V_\epsilon[f]$ and $\pi_{W_\epsilon} : V_\epsilon \to W_\epsilon$ are the two projection maps. Define the cohomological congruence module of f to be

$$C_\epsilon^{\rm coh}(f) \quad = \quad \frac{L_\epsilon}{L_{f,\epsilon} \oplus L_{W,\epsilon}}. \tag{20}$$

Arguments similar to those used in the proof of Theorem 5 of [9] show that

$$\wp \,\big|\, C_\epsilon^{\rm coh}(f) \iff \wp \,\Big|\, \frac{W(f)\Gamma(1, \mathrm{Ad}(f))L(1, \mathrm{Ad}(f)}{\Omega(f,\epsilon)\,\Omega(f,-\epsilon)}.$$

Let T denote the $\mathfrak{m}$-localized Hecke algebra acting on the space $L_\epsilon(K_\wp)$. Note that T is independent of $\epsilon \in \widehat{\mathcal{C}}$. Let T^f respectively T^W denote the images of the Hecke algebra in the two factors corresponding to the decomposition (19) for $A = K_\wp$. Let

$$C(f) \quad = \quad \frac{T^f \oplus T^W}{T}.$$

be the usual congruence module for f. The freeness result (Theorem 8) shows that $L_\epsilon(\mathcal{O}_\wp)$ is a free T-module of rank 2. It is an easy consequence that

$$\wp \,\big|\, C_\epsilon^{\rm coh}(f) \iff \wp \,\big|\, C(f).$$

Thus $\wp$ is a congruence prime for f and the theorem follows. $\square$

Acknowledgements. I wish to thank H. Hida and J. Tilouine for several discussions during the time I worked on this paper. I also thank C. Khare, D. Prasad, M. S. Raghunathan, E. Urban, T. N. Venkataramana and the referee, for useful conversations and comments. I would also like to thank the University of Paris 13, and the Commission on Development and Exchanges of the IMU, for making possible visits to Paris in 1998 and 2000, during the first of which lectures by K. Fujiwara provided some inspiration for working on this project.

References

[1] K. Buecker. On the control theorem for the symplectic group. *Compositio Math.*, 113(1):91–115, 1998.

[2] F. Diamond. On deformation rings and Hecke rings. *Ann. of Math*, 144:137–166, 1996.

[3] F. Diamond. The Taylor-Wiles construction and multiplicity one. *Invent. Math*, 128(2):379–391, 1997.

[4] F. Diamond. On the Hecke action on the cohomology of Hilbert-Blumenthal surfaces. In *Number theory (Tiruchirapalli, 1996)*, volume 210 of *Contemp. Math*, pages 71–83. Amer. Math. Soc., Providence, RI, 1998.

[5] F. Diamond, M. Flach, and L. Guo. The Tamagawa number conjecture of adjoint motives of modular forms. *Ann. Sci. École Norm. Sup.*, 37(5):663–727, 2004.

[6] M. Dimitrov. Galois representations modulo p and cohomology of Hilbert modular varieties. *Ann. Sci. École Norm. Sup.*, 38(4):505–551, 2005.

[7] K. Fujiwara. Deformation rings and Hecke-algebras in the totally real case. *Preprint*, 1996.

[8] A. Genestier and J. Tilouine. Systèmes de Taylor-Wiles pour GSp(4). *Astérisque*, 302:177–290, 2005.

[9] E. Ghate. Adjoint L-values and primes of congruence for Hilbert modular forms. *Compositio Math.*, 132(3):243–281, 2002.

[10] H. Hida. Congruence of cusp forms and special values of their zeta functions. *Invent. Math.*, 63:225–261, 1981.

[11] H. Hida. On congruence divisors of cusp forms as factors of the special values of their zeta functions. *Invent. Math.*, 64:221–262, 1981.

[12] H. Hida. On p-adic Hecke algebras for GL_2 over totally real fields. *Ann. of Math.*, 128(2):295–384, 1988.

[13] H. Hida. p-Ordinary cohomology groups for $SL(2)$ over number fields. *Duke Math. J.*, 69:259–314, 1993.

[14] H. Hida. Control theorems of p-nearly ordinary cohomology groups for $SL(n)$. *Bull. Soc. Math. France*, 123(3):425–475, 1995.

[15] H. Hida. *Modular Forms and Galois Cohomology.* Cambridge University Press, Cambridge, 2000.

[16] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math*, 47:33–186, 1977.

[17] B. Mazur. Deforming Galois representations. In *Galois groups over* $\mathbb{Q}$ *(Berkeley, CA, 1987)*, Math. Sci. Res. Inst. Publ., 16, pages 385–437. Springer, New York, 1989.

[18] B. Mazur. An introduction to the deformation theory of Galois representations. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 243–311. Springer, New York, 1997.

[19] A. Mokrane and J. Tilouine. Cohomology of Siegel varieties with p-adic integral coefficients and applications. *Astérisque*, 280:1–95, 2002.

[20] K. Ribet. Mod p Hecke operators and congruences between modular forms. *Invent. Math.*, 71(1):193–205, 1983.

[21] J-P. Serre. Le problème des groupes de congruence pour SL2. *Ann. of Math*, 92:489–527, 1970.

[22] C. Skinner and A. Wiles. Residually reducible representations and modular forms. *Inst. Hautes Études Sci. Publ. Math.*, 89:5–126, 2000.

[23] C. Skinner and A. Wiles. Nearly ordinary deformations of irreducible residual representations. *Annales de la Faculté des Sciences de Toulouse*, X:185–215, 2001.

[24] R. Taylor. On the meromorphic continuation of degree two L-functions. *Doc. Math.*, pages 729–779, 2002.

[25] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.*, 141(3):553–572, 1995.

[26] A. Wiles. On ordinary λ-adic representations associated to modular forms. *Inv. Math.*, 94(3):529–573, 1988.

[27] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.*, 141(3):443–551, 1995.