



ANNALES

DE

L'INSTITUT FOURIER

Matteo LONGO

**On the Birch and Swinnerton-Dyer conjecture for modular elliptic curves
over totally real fields**

Tome 56, n° 3 (2006), p. 689-733.

http://aif.cedram.org/item?id=AIF_2006__56_3_689_0

© Association des Annales de l'institut Fourier, 2006, tous droits réservés.

L'accès aux articles de la revue « Annales de l'institut Fourier » (<http://aif.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://aif.cedram.org/legal/>). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

*Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>*

ON THE BIRCH AND SWINNERTON-DYER CONJECTURE FOR MODULAR ELLIPTIC CURVES OVER TOTALLY REAL FIELDS

by Matteo LONGO (*)

ABSTRACT. — Let E/F be a modular elliptic curve defined over a totally real number field F and let ϕ be its associated eigenform. This article presents a new method, inspired by a recent work of Bertolini and Darmon, to control the rank of E over suitable quadratic imaginary extensions K/F . In particular, this argument can also be applied to the cases not covered by the work of Kolyvagin and Logachëv, that is, when $[F : \mathbb{Q}]$ is even and ϕ not new at any prime.

RÉSUMÉ. — Soit E/F une courbe elliptique modulaire définie sur un corps de nombres totalement réel F et soit ϕ la forme propre associée. Cet article présente une nouvelle méthode, inspirée par un récent travail de Bertolini et Darmon, pour contrôler le rang de E sur des extensions convenables quadratiques imaginaires K/F . En particulier, ce résultat peut être appliqué aux cas qui ne sont pas considérés dans le travail de Kolyvagin et Logachëv, *i.e.*, quand $[F : \mathbb{Q}]$ est pair et ϕ n'est pas nouveau en aucun idéal premier.

Introduction

Let E be an elliptic curve of conductor \mathfrak{n} with no complex multiplication defined over a totally real number field F of finite degree d over \mathbb{Q} . Choose a totally imaginary quadratic extension K/F ; such an extension can be described as $K = F(\sqrt{\alpha})$, where α is a totally negative element of F . By the well-known theorem of Mordell-Weil, the rank of the groups $E(F)$ and $E(K)$ are finite. Denote by $L(E, s)$ the Hasse-Weil L -series attached

Keywords: Elliptic Curves, Birch and Swinnerton-Dyer Conjecture, Shimura Varieties, Congruences between Hilbert Modular Forms.

Math. classification: 11G05, 11G18, 11G40, 11F30.

(*) The author was partially supported by the research project COFIN PRIN 2002 *Geometria delle Varietà Algebriche* and by the Marie Curie Research Training Network *Arithmetic Algebraic Geometry*.

to E and by $L_K(E, s)$ its base change over K . These series converge for $\Re(s)$ greater than $3/2$. The following Birch and Swinnerton-Dyer conjecture **BSD** for E over F and K is well-known:

CONJECTURE (BSD). — *The series $L(E, s)$ and $L_K(E, s)$ have a continuation to entire functions whose order of vanishing at the central point $s = 1$ is equal to the rank of the groups, respectively, $E(F)$ and $E(K)$.*

This article presents some new cases of the **BSD** conjecture for modular elliptic curves E/F when the order of vanishing of $L_K(E, s)$ at $s = 1$ is zero. These new cases are those not covered by the well-known work of Kolyvagin and Logachëv [34]. In particular, the present work can be applied to modular elliptic curves E with everywhere good reduction over extensions F/\mathbb{Q} of even degree (and to all the twists of E by quadratic characters of F).

The notion of modularity can be made precise as follows. For any rational prime p , denote by $T_p(E)$ the p -adic Tate module of E and by

$$\rho_{E,p} : \text{Gal}(\overline{F}/F) \rightarrow \text{Aut}(T_p(E)) \simeq \text{GL}_2(\mathbb{Z}_p)$$

the associated Galois representation.

On the other hand, let $\phi \in \mathcal{S}_2(\mathfrak{n})$ be a Hilbert modular form of parallel weight 2 and $\Gamma_0(\mathfrak{n})$ -level structure (see Section 1.1 for precise definitions). Assume that ϕ is an eigenform for the action of the Hecke algebra $\mathbb{T}_{\mathfrak{n}}$ acting faithfully on $\mathcal{S}_2(\mathfrak{n})$ and denote by $\theta_{\phi}(\mathbb{T})$ the associated eigenvalues, where $\mathbb{T} \in \mathbb{T}_{\mathfrak{n}}$. For any prime ideal $\mathfrak{q} \nmid \mathfrak{n}$ (respectively, $\mathfrak{q} \mid \mathfrak{n}$) of \mathcal{O}_F , denote by $\mathbb{T}_{\mathfrak{q}}$ the Hecke operator at \mathfrak{q} and by $\mathbb{S}_{\mathfrak{q}}$ the spherical operator at \mathfrak{q} (respectively, by $\mathbb{U}_{\mathfrak{q}}$ the Hecke operator at \mathfrak{q}); see [42] for definitions. After a suitable normalization, it is possible to assume that the eigenvalues $\theta_{\phi}(\mathbb{T})$ belong to the ring of integers \mathcal{O}_{ϕ} of a finite extension K_{ϕ} of \mathbb{Q} . Fix finally a prime ideal \mathfrak{p} of \mathcal{O}_{ϕ} . Thanks to the work of Carayol [11], Wiles [50] and Taylor [45], there is a unique continuous representation:

$$\rho_{\phi,\mathfrak{p}} : \text{Gal}(\overline{F}/F) \rightarrow \text{GL}_2(\mathcal{O}_{\phi,\mathfrak{p}})$$

which is unramified at all the prime ideals $\mathfrak{q} \nmid \mathfrak{np}$ and so that the characteristic polynomial of a Frobenius element at these primes is $X^2 - \theta_{\phi}(\mathbb{T}_{\mathfrak{q}}) + |\mathfrak{q}|\theta_{\phi}(\mathbb{S}_{\mathfrak{q}})$, where $\mathcal{O}_{\phi,\mathfrak{p}}$ is the completion of \mathcal{O}_{ϕ} at \mathfrak{p} and $|\mathfrak{q}|$ is the norm of \mathfrak{q} , that is, the number of elements of the residue field of \mathcal{O}_F at \mathfrak{q} .

The following definition explains the notion of modularity.

DEFINITION 0.1. — *E is modular if there exists an eigenform ϕ of parallel weight 2 and level \mathfrak{n} so that $K_{\phi} = \mathbb{Q}$ and $\rho_{\phi,\mathfrak{p}}$ is equivalent to $\rho_{E,p}$, where p is a prime of \mathbb{Z} .*

If E is modular, then $L(E, s)$ (respectively, $L_K(E, s)$) coincides with the L -series $L(\phi, s)$ (respectively, $L_K(\phi, s)$) for $\Re(s) \gg 0$. Hence, $L(E, s)$ and $L_K(E, s)$ have continuations to entire functions. In the following, we prefer the notations $L(\phi, s)$ and $L_K(\phi, s)$ to denote $L(E, s)$ and $L_K(E, s)$.

For $F = \mathbb{Q}$ the **BSD** conjecture is known when the order of vanishing of $L(E, s) = L(\phi, s)$ at $s = 1$ is at most one. Thanks to the work of Wiles [51] and Taylor-Wiles [46], successively improved in a series of papers [17], [14] and [8], it is known that all elliptic curves over \mathbb{Q} are modular. Set $N := \mathfrak{n}$. For such curves, there is a parametrization over \mathbb{Q} :

$$\varphi : X_0(N) \rightarrow E,$$

where $X_0(N)$ is the modular curve of level N . Let ω be the unique invariant differential on E over \mathbb{Q} so that $\varphi^*(\omega)(z) = \phi(z)dz$ (z a complex variable). Suppose that all primes dividing N are split in $K := \mathbb{Q}(\sqrt{-D})$. In this case, the order of vanishing of $L_K(\phi, 1)$ is odd, hence $L_K(\phi, 1) = 0$. The **BSD** conjecture for elliptic curves over K should imply that the rank of $E(K)$ is at least one, and exactly one if $L'_K(\phi, 1) \neq 0$.

There is a theory of Heegner points on $X_0(N)$ coming from its interpretation as moduli space for elliptic curves with a cyclic subgroup of order N . More precisely, choose an ideal \mathcal{N} of \mathcal{O}_K , the ring of integers of K , so that $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$. The complex tori \mathbb{C}/\mathcal{O}_K and $\mathbb{C}/\mathcal{N}^{-1}$ define elliptic curves related by a cyclic N -isogeny, giving a complex point $x_1 \in X_0(N)(\mathbb{C})$. The theory of complex multiplication implies that this point is defined over the Hilbert class field K_1 of K . Define $y_1 := \varphi(x_1)$ and $y_K := \text{Tr}_{K_1/K}(y_1)$. The main result of [25] is:

$$L'_K(\phi, 1) = \frac{\int_{E(\mathbb{C})} \omega \wedge \overline{i\omega}}{\sqrt{D}} \hat{h}(y_K),$$

where \hat{h} is the Néron-Tate height. It follows that the point y_K has infinite order if and only if $L'_K(\phi, 1) \neq 0$.

In [33] Kolyvagin proved that, under the previous assumptions, the rank of $E(K)$ is one and that

$$y_K \in E(K)^v,$$

where $-v = \pm 1$ is the sign of the functional equation of $L(\phi, s)$ and $E(K)^v$ is the v -eigenspace for the complex conjugation. For more details and an exposition of this argument, see [24].

Kolyvagin's result proves the rank one case of the **BSD** conjecture for E over K and can be used to derive a proof of the Birch and Swinnerton-Dyer conjecture for E over \mathbb{Q} when the order of vanishing of $L(\phi, s)$ at $s = 1$ is at most one. More precisely, assume that the order of vanishing of

$L(\phi, 1)$ is 0 or 1. In this case, it is possible to choose an extension K/F so that all primes dividing N are split in K and $L'_K(\phi, 1) \neq 0$ (if $L(\phi, 1) \neq 0$ the existence of such a field K follows from the work of Bump-Friedberg-Hoffstein [9] and Murty-Murty [37], while for $L(\phi, 1) = 0$ this is a result of Waldspurger [48]). Then Kolyvagin's result on the rank of $E(K)$ imply the **BSD** conjecture over \mathbb{Q} .

Assume now that either $[F : \mathbb{Q}]$ is odd or $[F : \mathbb{Q}]$ is even and ϕ is new at least at one prime which divides \mathfrak{n} exactly. In this case the previous techniques can be generalized. The main idea is to replace, via the Jacquet-Langlands correspondence, the modular parametrization by a Shimura curve parametrization $\varphi : X \rightarrow E$ defined over F in the spirit of [11]. The analogue in this context of [25] and [33] are, respectively, [53] and [34]. See [53] for more details.

This article proposes a new approach to the **BSD** conjecture when $L_K(\phi, 1) \neq 0$. A similar strategy has been used by Bertolini and Darmon [4] in the context of Iwasawa's Main Conjecture. It is worth to point out that the totally real case introduces new problems which are not present in the rational case and must be treated by different tools. The main features of this approach are:

1. The analytic result on the non-vanishing of $L'_K(\phi, 1)$ is replaced by a more algebraic point of view such as the Gross formula [23] generalized by Zhang in [52].
2. Kolyvagin's method requires an imaginary quadratic K/F so that the rank of $E(K)$ is one, while in the setting of this work the rank of $E(K)$ is zero.
3. It is possible to treat the missing cases for F totally real, that is, $[F : \mathbb{Q}]$ even and ϕ not new at any prime. In particular, this method applies to elliptic curves with everywhere good reduction defined over totally real fields of even degree over \mathbb{Q} and to all their twists by quadratic characters of F . This case introduces arithmetic problems which are not present in the case $F = \mathbb{Q}$.

The main idea of this approach is parallel to the idea that [50] and [45] used to build the \mathfrak{p} -adic representation associated to a modular form ϕ when $[F : \mathbb{Q}]$ is even and ϕ is not new at any prime. Basically, by the theory of congruences between modular forms, it is possible to find a modular form $\phi_\ell \equiv \phi \pmod{p}$ of level $\mathfrak{n}\ell$ which is new at ℓ , where $\ell \subset \mathcal{O}_F$ is a congruence prime. Since ϕ is new at ℓ , there is a theory of Shimura curves associated to ϕ_ℓ and, by varying the prime ℓ , it is possible to obtain an Euler system and control the rank of $E(K)$.

The main result

Although the most intriguing aspects of this work concern elliptic curves over F with everywhere good reduction and $[F : \mathbb{Q}]$ even, the main result and the outline of the proof are now stated in a more general form.

If the relative discriminant of K/F is prime to \mathfrak{n} , there is a factorization $\mathfrak{n} = \mathfrak{n}^+ \mathfrak{n}^-$ induced by the extension K/F : \mathfrak{n}^+ (respectively, \mathfrak{n}^-) is divisible by the prime ideals dividing \mathfrak{n} which are split (respectively, inert) in K .

ASSUMPTION 0.2. — *The ideal \mathfrak{n} satisfies the following conditions:*

1. *The discriminant of K/F is prime to \mathfrak{n} ; let $\mathfrak{n} = \mathfrak{n}^+ \mathfrak{n}^-$ be the associated factorization as above;*
2. *\mathfrak{n}^- is square-free and the number of primes dividing it has the same parity as $d := [F : \mathbb{Q}]$;*
3. *ϕ is new at each prime dividing \mathfrak{n}^- .*

If E has everywhere good reduction and $[F : \mathbb{Q}]$ is even, Assumption 0.2 is verified for any K . This is true also for any twist of E by quadratic characters χ of F such that the corresponding quadratic extension of F is either CM or totally real. This assumption is equivalent to the requirement that the order of vanishing of $L_K(\phi, 1)$ is even, so it is compatible with the hypothesis $L_K(\phi, 1) \neq 0$. As already observed, the **BSD** conjecture precludes in this setting the existence of Heegner points with infinite order as in the original method of Kolyvagin. Moreover, the parity assumption is crucial for the use of Shimura curves.

The following Theorem A (respectively, Theorem B) states that the **BSD** conjecture holds when the order of vanishing of $L(\phi, s)$ (respectively, $L_K(\phi, s)$) at $s = 1$ is zero.

THEOREM A. — *If $L(\phi, 1) \neq 0$ then $E(F)$ is finite.*

THEOREM B. — *If $L_K(\phi, 1) \neq 0$ then $E(K)$ is finite.*

Theorem A follows from Theorem B by non-vanishing results for twists of L -series. Indeed, if $L(\phi, 1) \neq 0$ then by [49] it is possible to find K inducing a factorization $\mathfrak{n} = \mathfrak{n}^+ \mathfrak{n}^-$ as above and so that $L_K(\phi, 1) \neq 0$.

Theorem B follows by making a p -descent for a suitable rational prime p and bounding the p -Selmer group $\text{Sel}_p(E/K)$ (the definition of $\text{Sel}_p(E/K)$ can be found in [44, Ch. X, §4]). The next paragraphs explain the conditions which are required for the choice of p . Theorem B will be deduced from Theorem C in the following after the choice of a suitable prime p .

The *Gross-Zhang formula* [52] gives an arithmetic description of the special value at $s = 1$ of $L_K(\phi, s)$. Let B be a quaternion algebra over F

which is ramified at all the archimedean places of F and at all the prime ideals dividing \mathfrak{n}^- (by the previous assumption, such a quaternion algebra exists). Let $R \subseteq B$ be an Eichler order of level \mathfrak{n}^+ . Denote by \widehat{B} and \widehat{R} the finite adèle ring of, respectively, B and R . By the Jacquet-Langlands correspondence [27] there exists a weight 2 modular form

$$f : \widehat{R}^\times \backslash \widehat{B}^\times / B^\times \rightarrow \mathbb{Z}$$

on the quaternion algebra B with the same eigenvalues as ϕ under the action of the Hecke algebra $\mathbb{T}_\mathfrak{n}$. Since any prime dividing \mathfrak{n}^- is inert in K/F by Assumption 0.2, it follows from [47, Chapitre III, Théorème 3.8] that there exists an embedding $\Psi : K \hookrightarrow B$ so that $\Psi(\mathcal{O}_K) = R \cap \Psi(K)$, where \mathcal{O}_K is the ring of algebraic integers of K . Then there is a map:

$$\widehat{\Psi} : \widehat{\mathcal{O}}_K^\times \backslash \widehat{K}^\times / K^\times \rightarrow \widehat{R}^\times \backslash \widehat{B}^\times / B^\times.$$

Define the algebraic part of $L_K(\phi, s)$ to be: $\mathcal{L}_K(\phi) := \sum_{\mathfrak{a}} (f \circ \widehat{\Psi})(\mathfrak{a}) \in \mathbb{Z}$, where the sum is over a set of representatives of $\text{Pic}(\mathcal{O}_K) \simeq \widehat{\mathcal{O}}_K^\times \backslash \widehat{K}^\times / K^\times$. The Gross-Zhang formula states that:

$$(0.1) \quad L_K(\phi, 1) \doteq |\mathcal{L}_K(\phi)|^2,$$

where \doteq denotes an equality up to an explicitly computable non-zero factor.

For any group G denote by $G[p]$ its p -torsion. Define

$$\text{Sel}_p(\phi/K) := \{s \in \text{Sel}_p(E/K) : \text{res}_{\mathfrak{q}}(s) = 0, \forall \mathfrak{q} \mid \mathfrak{n}^+\},$$

where $\text{res}_{\mathfrak{q}}(s) : H^1(K, E[p]) \rightarrow H^1(K_{\mathfrak{q}}, E[p]) := \bigoplus_{v \mid \mathfrak{q}} H^1(K_v, E[p])$ is the direct sum of the restriction maps in Galois cohomology, the sum is over the set of primes v of \mathcal{O}_K dividing \mathfrak{q} and K_v is the completion of K at v (for more details on these definitions, see Section 1.3).

Say that a modular form ϕ to be p -isolated if there are no non-trivial congruences $\phi \equiv \psi \pmod{p}$ between ϕ and other forms ψ of level \mathfrak{n} which are new at \mathfrak{n}^- .

The following result provides the key ingredient to prove Theorem B above.

THEOREM C. — *Assume that the following conditions on the prime $p > 3$ are verified:*

1. p is prime to $\mathfrak{n}D$, where D is the absolute discriminant of K ;
2. $p \nmid \mathcal{L}_K(\phi)$;
3. ϕ is p -isolated;
4. The $\text{Gal}(\overline{F}/F)$ -module $E[p]$ is irreducible.

Then $\text{Sel}_p(\phi/K) = 0$.

Theorem B can be deduced by Theorem C as follows. Assume that $L_K(\phi, 1) \neq 0$. Choose a rational prime $p > 3$ verifying conditions 1, 2, 3 and 4 in Theorem C and the following displayed equation:

$$(0.2) \quad \text{Sel}_p(E/K) = \text{Sel}_p(\phi/K).$$

Note that there are infinitely many primes satisfying all these conditions: for 2, since $L_K(\phi, 1) \neq 0$, Equation (0.1) shows that $\mathcal{L}_K(\phi) \neq 0$; for 3, use the finiteness of the \mathbb{C} -vector space of Hilbert modular forms of fixed weight and level; for 4, use [41, Théorème 2] and the fact that E has no complex multiplication; for the displayed Equation (0.2), choose p such that E has good ordinary reduction at primes dividing p and use the theorem of Lutz as in [22, Section 2] (recall that p is prime to \mathfrak{n}^+ by 1). By the choice of p made above, it follows from Theorem C that $\text{Sel}_p(E/K) = 0$. Since there is an injective map

$$E(K)/pE(K) \hookrightarrow \text{Sel}_p(E/K)$$

arising from Kummer theory, Theorem B follows.

The proof of Theorem A and B is then reduced to the proof of Theorem C, which is outlined in the next subsection.

The outline of the proof of Theorem C

The general approach for obtaining results on the rank of $E(K)$ is to bound the p -Selmer group $\text{Sel}_p(E/K)$. The strategy for finding such bounds is to construct a collection of global cohomology classes (a so called *Euler system*) $\{\kappa_\ell \in H^1(K, E[p])\}_{\ell \in L}$ so that: (1) L is a sufficiently large set of primes of \mathcal{O}_F and (2) each class κ_ℓ satisfies prescribed local properties, that is, the restriction of κ_ℓ at any prime not dividing $\mathfrak{n}^+\ell$ belongs to the image of the local Kummer map. The existence of an Euler system combined with a standard argument based on the global reciprocity law of class field theory can then be used to obtain the desired bound.

The idea of the present paper, as in [4], is to produce an Euler system using the theory of congruences between modular forms. The set of primes L for the Euler system $\{\kappa_\ell\}_{\ell \in L}$ is given by the congruence primes ℓ , which, following the terminology introduced by Bertolini and Darmon, are called p -admissible. For any $\ell \in L$, the class κ_ℓ is obtained from Heegner points on the Shimura curve $X_{\mathfrak{n}^+, \mathfrak{n}^- \ell}$ of level \mathfrak{n}^+ attached to a quaternion algebra of discriminant $\mathfrak{n}^- \ell$ which is split at exactly one of the archimedean places of F . The sketch of the proof can be divided into five steps.

Step 1: The raising the level result.

Let $\theta_\phi : \mathbb{T}_n \rightarrow \mathbb{Z}/p\mathbb{Z}$ denote the morphism associated to ϕ . A modular form ϕ' of level \mathfrak{n}' is said to be *congruent to $\phi \pmod{p}$* (write: $\phi' \equiv \phi \pmod{p}$) if the Fourier coefficients of ϕ' belong to the ring of integer $\mathcal{O}_{\phi'}$ of a number field $K_{\phi'}$ and there is a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_{\phi'}$ dividing p so that: (1) $\mathcal{O}_{\phi'}/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z}$ and (2) $T_q(\phi') \equiv \theta_\phi(T_q)\phi' \pmod{\mathfrak{p}}$ for primes $q \nmid \mathfrak{nn}'$ and $T_q(\phi') \equiv \theta_\phi(U_q)\phi' \pmod{\mathfrak{p}}$ for primes $q \mid (\mathfrak{n}, \mathfrak{n}')$. Definition 0.3 introduces the congruence primes and Theorem 0.4 states the raising the level result.

DEFINITION 0.3. — *Define a prime $\ell \subset \mathcal{O}_F$ to be p -admissible if:*

1. $\ell \nmid \mathfrak{np}$;
2. ℓ is inert in K ;
3. $p \nmid |\ell|^2 - 1$;
4. $p \mid |\ell| + 1 - \epsilon\theta_\phi(T_\ell)$, where $\epsilon = \pm 1$.

THEOREM 0.4. — *Assume that ℓ is p -admissible and that the representation of $\text{Gal}(\overline{F}/F)$ on $E[p]$ is irreducible. Then there exists a modular form ϕ_ℓ of level $\mathfrak{n}\ell$ new at ℓ so that $\phi_\ell \equiv \phi \pmod{p}$.*

Step 2: The Jacquet-Langlands correspondence.

Denote by $\overline{\theta}_\phi : \mathbb{T}_n \rightarrow \mathbb{Z}/p\mathbb{Z}$ (respectively, $\overline{\theta}_{\phi_\ell} : \mathbb{T}_{\mathfrak{n}\ell} \rightarrow \mathbb{Z}/p\mathbb{Z}$) the morphism associated to ϕ (respectively, to ϕ_ℓ). Use the following notations: $\mathfrak{m}_f := \text{Ker}(\overline{\theta}_\phi)$ and $\mathfrak{m}_{f_\ell} := \text{Ker}(\overline{\theta}_{\phi_\ell})$. By the Jacquet-Langlands correspondence it is possible to associate to ϕ_ℓ a modular form f_ℓ on a quaternion algebra \mathcal{B} which is split at exactly one of the archimedean places of F and whose discriminant is $\mathfrak{n}^{-1}\ell$ (note that such a quaternion algebra exists by Assumption 0.2). Fix an Eichler order $\mathcal{R} \subseteq \mathcal{B}$ of level \mathfrak{n}^+ and consider the Shimura curve X defined over F whose complex points are

$$X(\mathbb{C}) := \widehat{\mathcal{R}}^\times \backslash (\widehat{\mathcal{B}}^\times \times \mathcal{H}^\pm) / \mathcal{B}^\times \simeq \prod_{j=1}^h \Gamma_j \backslash \mathcal{H},$$

where $\mathcal{H}^\pm = \mathbb{C} - \mathbb{R}$, the symbol \mathcal{H} denotes the complex upper half plane and $\Gamma_j \subseteq \mathcal{B}^\times$ are arithmetic subgroups related to the level structure \mathcal{R} . The modular form f_ℓ can be viewed as a holomorphic differential on $X(\mathbb{C})$. Denote by J the Jacobian variety of X and by $J[p]$ its p -torsion. The following theorem, due essentially to Boston-Lenstra-Ribet [6], gives the relation between the cohomology of $E[p]$ and that of $J[p]$.

THEOREM 0.5. — *There is an isomorphism of $\text{Gal}(\overline{F}/F)$ -modules $J[p]/\mathfrak{m}_{f_\ell} \simeq E[p]^k$, where k is a positive integer.*

Step 3: The construction of κ_ℓ .

Denote by μ the archimedean place of F where \mathcal{B} is split. By Assumption 0.2 there is an embedding

$$K^\times \hookrightarrow \mathcal{B}^\times \hookrightarrow (\mathcal{B} \otimes_{F,\mu} \mathbb{R})^\times \simeq \text{GL}_2(\mathbb{R})$$

inducing an action of K^\times on \mathcal{H}^\pm by fractional linear transformations. This action has only one fixed point $P \in \mathcal{H}$ which is rational over the Hilbert class field K_1 of K by the theory of complex multiplication (see [43, Theorem 9.6]). Define the Heegner divisor $D_K := \sum_{\sigma \in \text{Gal}(K_1/K)} \sigma(P) \in \text{Div}(X)(K_1)$. If the representation of $\text{Gal}(\overline{F}/F)$ on $E[p]$ is irreducible, the ideal \mathfrak{m}_{f_ℓ} is not Eisenstein and so D_K defines a point in $P_K \in J(K)/\mathfrak{m}_{f_\ell}$. The Kummer map:

$$(0.3) \quad J[p]/\mathfrak{m}_{f_\ell} \hookrightarrow H^1(K, J[p]/\mathfrak{m}_{f_\ell}) \simeq H^1(K, E[p])^k$$

yields k global classes $\kappa_j \in H^1(K, E[p])$ for $j = 1, \dots, k$ (the isomorphism in (0.3) is a consequence of Theorem 0.5). For any prime $\mathfrak{q} \subseteq \mathcal{O}_F$, denote by $\delta_{\mathfrak{q}}$ the local Kummer map and by $\text{res}_{\mathfrak{q}}$ the restriction map in cohomology. Since any κ_j comes from a class of $\text{Sel}_p(J/K)$ and the conductors of J and E differ only at ℓ , it is possible to show that $\text{res}_{\mathfrak{q}}(\kappa_\ell) \in \text{Im}(\delta_{\mathfrak{q}})$ for primes $\mathfrak{q} \nmid n^+\ell$ (see Theorem 5.5 for precise references). So there are two problems: (1) The choice of a suitable component $H^1(K, E[p]) \subseteq H^1(K, J[p]/\mathfrak{m}_{f_\ell})$: the class κ_ℓ is then defined to be the projection on it; (2) The description of $\text{res}_\ell(\kappa_\ell)$.

Remark 0.6. — The problem of finding a suitable copy of $H^1(K, E[p])$ in $H^1(K, J[p]/\mathfrak{m}_{f_\ell})$ appears only when $[F : \mathbb{Q}]$ is even and ϕ is not new at any prime dividing n^- . Indeed, in all other cases (so, in particular, when $F = \mathbb{Q}$) it is possible to show that $\Phi_\ell/\mathfrak{m}_{f_\ell} \simeq \mathbb{Z}/p\mathbb{Z}$ and, as a consequence, to prove that $J[p]/\mathfrak{m}_{f_\ell} \simeq E[p]$. The problems with the missing case are related to the geometry of Shimura curves and to the description of the action of Hecke operators via Brandt matrices. More precisely, assume from now to the end of this remark that $[F : \mathbb{Q}]$ is even and ϕ is not new at any prime dividing n^- . In this case, it is not possible prove that $\Phi_\ell/\mathfrak{m}_{f_\ell} \simeq \mathbb{Z}/p\mathbb{Z}$ using the the argument of [38, Proposition 5] based on the geometry of Shimura curves. On the other hand, it is possible, studying the action of Hecke operators via Brandt matrices, to give precise conditions on F and n

which imply $\Phi_\ell/\mathfrak{m}_{f_\ell} \simeq \mathbb{Z}/p\mathbb{Z}$. These conditions are collected in the notion of *Eisenstein pair* (see Definition 3.4). When no one of these conditions is verified, it is necessary to use a more complicate argument to find a suitable component $\mathcal{C}_\ell \simeq \mathbb{Z}/p\mathbb{Z} \subseteq \Phi_\ell/\mathfrak{m}_{f_\ell}$ playing the same role as $\Phi_\ell/\mathfrak{m}_{f_\ell}$ in the previous case.

Step 4: The component \mathcal{C}_ℓ and the Reciprocity Law.

Since X is a moduli space for suitable abelian varieties with level structure, there is a model \mathcal{X} of X over \mathcal{O}_F . Denote by \mathcal{X}_ℓ the fiber of \mathcal{X} at ℓ and define $\mathcal{X}_{\ell^2} := \mathcal{X}_\ell \otimes_{F_\ell} K_\ell$. Let \mathbb{C}_ℓ be the completion of the algebraic closure of F_ℓ and define $\mathcal{H}_\ell := \mathbb{C}_\ell - F_\ell$. By the Čerednik-Drinfeld theorem, there is an isomorphism of rigid analytic spaces over K_ℓ :

$$\mathcal{X}_{\ell^2}(\mathbb{C}_\ell) = \prod_{j=1}^h \Gamma_j \backslash \mathcal{H}_\ell,$$

where $\Gamma_j \subseteq \mathrm{PGL}_2(F_\ell)$ are arithmetic subgroups related to the fixed level structure $\mathcal{R} \subseteq \mathcal{B}$. Denote by $\mathcal{X}_{\mathbb{F}_{\ell^2}}$ the special fiber of \mathcal{X}_{ℓ^2} , where \mathbb{F}_{ℓ^2} is the residue field of K_ℓ . The Čerednik-Drinfeld theorem shows that the set of vertices \mathcal{V}_ℓ of the arithmetic graph \mathcal{G}_ℓ associated to $\mathcal{X}_{\mathbb{F}_{\ell^2}}$ has the following description: $\mathcal{V}_\ell = \widehat{R}^\times \backslash \widehat{B}^\times / B^\times \times \{0, 1\}$.

THEOREM 0.7. — *The Heegner point $P \in X(K_1)$ reduces to a non singular point of the special fiber $\mathcal{X}_{\mathbb{F}_{\ell^2}}$. In particular, P_K defines a divisor $v_K \in \mathbb{Z}^0[\widehat{R}^\times \backslash \widehat{B}^\times / B^\times] / \mathfrak{m}_{f_\ell}$.*

This result is proved in Section 5.2 using the ℓ -adic description of Heegner points obtained from the Čerednik-Drinfeld theorem.

Let Φ_ℓ denote the group of connected components of the Jacobian variety of \mathcal{X}_{ℓ^2} . Define $H_{\mathrm{sing}}^1(K_\ell, E[p]) := H^1(K_\ell^{\mathrm{unr}}, E[p])^{\mathrm{Gal}(K_\ell^{\mathrm{unr}}/K_\ell)}$. This group is the orthogonal complement of $\delta_\ell(E(K_\ell)/pE(K_\ell))$ under the local Tate pairing $\langle \cdot, \cdot \rangle_\ell$. The following Theorem 0.8 (proved in Propositions 4.10 and 4.11) characterizes the choice of the component $H^1(K, E[p])$ inside $H^1(K, J[p]/\mathfrak{m}_{f_\ell})$, while Theorem 0.9 (proved in Proposition 5.4) describes $\mathrm{res}_\ell(\kappa_\ell)$ by the Reciprocity Law.

THEOREM 0.8. — *There exists a component $\mathcal{C}_\ell \simeq \mathbb{Z}/p\mathbb{Z} \subset \Phi_\ell/\mathfrak{m}_{f_\ell}$ so that*

$$\mathcal{C}_\ell \simeq H_{\mathrm{sing}}^1(K_\ell, E[p]) \subset H^1(K_\ell, E[p]) \subset H^1(K_\ell, J[p]/\mathfrak{m}_{f_\ell})$$

and there is a canonical non-trivial isomorphism

$$\bar{\omega}_\ell : \text{Im}(\delta_*) / \langle \mathfrak{m}_f, U_\ell^2 - 1 \rangle \rightarrow \mathcal{C}_\ell \simeq \mathbb{Z}/p\mathbb{Z},$$

where $\text{Im}(\delta_*) \subseteq \mathbb{Z}^0[\widehat{R}^\times \setminus \widehat{B}^\times / B^\times]$ is the subgroup of elements having degree zero on each connected component of \mathcal{G}_ℓ .

THEOREM 0.9. — *There is an element $C \in (\mathbb{Z}/p\mathbb{Z})^\times$ so that $\bar{\omega}_\ell(v_K) \equiv C\mathcal{C}_K(\phi) \pmod{p}$ in \mathcal{C}_ℓ .*

Step 5: The Euler system argument.

This is the final step of the proof of Theorem C. We must show that $\text{Sel}_p(\phi/K)$ is zero. So, fix an element $s \in \text{Sel}_p(\phi/K)$ and assume that $s \neq 0$. For any primes \mathfrak{q} , let $\partial_\mathfrak{q} : H^1(K, E[p]) \rightarrow H^1_{\text{sing}}(K_\mathfrak{q}, E[p])$ be the composition of the map $\text{res}_\mathfrak{q}$ and the projection to $H^1_{\text{sing}}(K_\mathfrak{q}, E[p])$. Choose a p -admissible prime ℓ so that $\partial_\ell(s) = 0$ and $\text{res}_\ell(s) \neq 0$ (such a prime ℓ exists by Theorem 2.3). If ℓ is a p -admissible prime, then (see also Lemma 2.2)

$$(0.4) \quad \delta_\ell(E(K_\ell)/pE(K_\ell)) \simeq \mathbb{Z}/p\mathbb{Z} \quad \text{and} \quad H^1_{\text{sing}}(K_\ell, E[p]) \simeq \mathbb{Z}/p\mathbb{Z}.$$

The global Tate duality yields $\langle s, \kappa_\ell \rangle = \sum_\mathfrak{q} \langle \text{res}_\mathfrak{q}(s), \text{res}_\mathfrak{q}(\kappa_\ell) \rangle_\mathfrak{q} = 0$. Since $\text{res}_\mathfrak{q}(\kappa_\ell)$ is orthogonal to s with respect to the local Tate pairing $\langle \cdot, \cdot \rangle_\mathfrak{q}$ for $\mathfrak{q} \neq \ell$, it follows that $\langle \text{res}_\ell(s), \text{res}_\ell(\kappa_\ell) \rangle_\ell = 0$. Since $H^1_{\text{fin}}(K_\ell, E[p])$ and $H^1_{\text{sing}}(K_\ell, E[p])$ are orthogonal with respect to the local pairing $\langle \cdot, \cdot \rangle_\ell$, the isomorphisms (0.4) and the condition $\partial_\ell(\kappa_\ell) \neq 0$ (which follows from Theorem 0.9) imply that $\text{res}_\ell(s) = 0$, which is a contradiction. This completes the sketch of the proof.

Examples.

Assume that E is an elliptic curve with everywhere good reduction over a real quadratic field $F = \mathbb{Q}(\sqrt{D})$. If E is a \mathbb{Q} -curve, that is, E is isogenous to its Galois conjugate, then E appears as a quotient of the modular curve $J_1(N)$ over \mathbb{Q} for some N . In this case, the classical methods of Kolyvagin could perhaps be applied to E (see the brief discussion in [16, Section 3]). The author will study this variant of the classical method in a forthcoming work. The really new cases which can be treated by the present work are elliptic curves which are not \mathbb{Q} -curves. An example of such curves can be found in [16]: let $\omega := \frac{1+\sqrt{509}}{2}$ and $F = \mathbb{Q}(\omega)$; then the elliptic curve corresponding to the following Weierstrass equation

$$y^2 - xy - \omega y = x^3 + (2 + 2\omega)x^2 + (162 + 3\omega)x + (71 + 34\omega)$$

is not a \mathbb{Q} -curve. For this curve, and also for any of its twists by quadratic characters of F , the present result is really new and could not be obtained by other methods.

Acknowledgements. The results contained in this article are presented in the author's Ph.D. thesis [35]. It is a pleasure for the author to thank sincerely his Ph.D. advisor Professor Massimo Bertolini for having proposed this problem and for very helpful suggestions and improvements during the work. The author wishes also to thank Professor Frances Sullivan for reading the preliminary version of this paper and the anonymous referee for suggesting useful improvements in the exposition.

1. Selmer groups of modular elliptic curves

1.1. Hilbert modular forms

Let F be a totally real number field of finite degree d over \mathbb{Q} with ring of algebraic integers \mathcal{O}_F . For any open compact subgroup $U \subseteq \widehat{\mathrm{GL}}_2(F)$, denote by $\mathcal{S}_2(U)$ the finite dimensional \mathbb{C} -vector space of parallel weight 2 Hilbert cusp forms with respect to U (here $\widehat{\mathrm{GL}}_2(F)$ is the idele group of the ring $M_2(F)$ of 2×2 matrices with coefficients in F). For the definition and the main properties of this space, see [45] and [50]. Set $\mathcal{S}_2(\mathfrak{n}) := \mathcal{S}_2(\widehat{\Gamma}_0(\mathfrak{n}))$, where $\Gamma_0(\mathfrak{n})$ is the subgroup of $M_2(\mathcal{O}_F)$ consisting of $(\bmod \mathfrak{n})$ upper triangular matrices and $\widehat{\Gamma}_0(\mathfrak{n})$ denotes its idele group. Finally, for any divisor $\mathfrak{r} \mid \mathfrak{n}$, let $\mathcal{S}_2^{\mathrm{new}}(\mathfrak{n}/\mathfrak{r}, \mathfrak{r}) \subseteq \mathcal{S}_2(\mathfrak{n})$ be the subspace of those forms which are new at \mathfrak{r} and set: $\mathcal{S}_2^{\mathrm{new}}(\mathfrak{n}) := \mathcal{S}_2^{\mathrm{new}}(\mathcal{O}_F, \mathfrak{n})$.

Let $\mathbb{T}_{\mathfrak{n}}$ be the Hecke algebra of level \mathfrak{n} acting faithfully on $\mathcal{S}_2(\mathfrak{n})$. For prime ideals $\mathfrak{q} \nmid \mathfrak{n}$ (respectively, $\mathfrak{q} \mid \mathfrak{n}$) denote by $T_{\mathfrak{q}}$ (respectively, by $U_{\mathfrak{q}}$) the corresponding Hecke operator. Finally, for primes $\mathfrak{q} \nmid \mathfrak{n}$, denote by $S_{\mathfrak{q}} \in \mathbb{T}_{\mathfrak{n}}$ the spherical operator at \mathfrak{q} . For the definitions of these operators, see [42]. Denote by $\mathbb{T}_{\mathfrak{n}/\mathfrak{r}, \mathfrak{r}}^{\mathrm{new}}$ the quotient of $\mathbb{T}_{\mathfrak{n}}$ acting faithfully on $\mathcal{S}_2^{\mathrm{new}}(\mathfrak{n}/\mathfrak{r}, \mathfrak{r})$ and set $\mathbb{T}_{\mathfrak{n}}^{\mathrm{new}} := \mathbb{T}_{\mathcal{O}_F, \mathfrak{n}}^{\mathrm{new}}$.

Any $\phi \in \mathcal{S}_2(\mathfrak{n})$ which is a simultaneous eigenvector for all Hecke operators gives rise to a morphism

$$\theta_{\phi} : \mathbb{T}_{\mathfrak{n}} \rightarrow \mathbb{C}$$

so that, for any $T \in \mathbb{T}_{\mathfrak{n}}$, $T(\phi) = \theta_{\phi}(T)\phi$. An eigenvector ϕ as above can be normalized so that the image of θ_{ϕ} is an order in the ring of integers \mathcal{O}_{ϕ} of a finite extension K_{ϕ} of \mathbb{Q} ; such a ϕ is called a normalized eigenform or

simply an eigenform. For any prime \mathfrak{p} of \mathcal{O}_ϕ , denote by $\mathcal{O}_{\phi,\mathfrak{p}}$ the completion of \mathcal{O}_ϕ at \mathfrak{p} and by

$$\bar{\theta}_\phi : \mathbb{T}_n \rightarrow \mathcal{O}_{\phi,\mathfrak{p}}/\mathfrak{p}$$

the reduction of $\theta_\phi \pmod{\mathfrak{p}}$.

Let $\phi \in \mathcal{S}_2(\mathfrak{n})$ be a normalized eigenform and fix a prime ideal \mathfrak{p} of \mathcal{O}_ϕ . Denote by \bar{F} an algebraic closure of F and by $\mathcal{O}_{\phi,\mathfrak{p}}$ the completion of \mathcal{O}_ϕ at \mathfrak{p} . Recall from the Introduction that there is a unique continuous representation of the absolute Galois group of F :

$$\rho_{\phi,\mathfrak{p}} : \text{Gal}(\bar{F}/F) \rightarrow \text{GL}_2(\mathcal{O}_{\phi,\mathfrak{p}})$$

which is unramified at all the prime ideals $\mathfrak{q} \nmid \mathfrak{n}\mathfrak{p}$ and so that the characteristic polynomial of a Frobenius element at these primes is

$$X^2 - \theta_\phi(\text{T}_\mathfrak{q}) + |\mathfrak{q}|\theta_\phi(\text{S}_\mathfrak{q}).$$

Assume now that $K_\phi = \mathbb{Q}$; then $\mathfrak{p} = p$ is a rational prime and $\mathcal{O}_{\phi,\mathfrak{p}} = \mathbb{Z}_p$. In this case, say that ϕ has rational coefficients. Denote by $T_\phi[p^\infty] \simeq \mathbb{Z}_p^2$ the $\text{Gal}(\bar{F}/F)$ -module associated to the representation $\rho_{\phi,p}$ and define

$$V_\phi[p^\infty] := T_\phi[p^\infty] \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p^2.$$

Set: $T_\phi[p^n] := T_\phi[p^\infty]/p^n T_\phi[p^\infty] \simeq (\mathbb{Z}/p^n\mathbb{Z})^2$ so that the multiplication by $p: T_\phi[p^{n+1}] \rightarrow T_\phi[p^n]$ yields a projective system and: $T_\phi[p^\infty] = \varprojlim_n T_\phi[p^n]$. On the other hand, define:

$$A_\phi[p^\infty] := V_\phi[p^\infty]/T_\phi[p^\infty] \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^2$$

and denote by $A_\phi[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^2$ its p^n -torsion. The natural inclusion $A_\phi[p^n] \hookrightarrow A_\phi[p^{n+1}]$ yields an inductive system and: $A_\phi[p^\infty] = \varinjlim_n A_\phi[p^n]$. Note that the Galois modules $T_\phi[p^n]$ and $A_\phi[p^n]$ are isomorphic. Reduction modulo p of $\rho_{\phi,p}$ yields a representation:

$$\bar{\rho}_{\phi,p} : \text{Gal}(\bar{F}/F) \rightarrow \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

whose associated $\text{Gal}(\bar{F}/F)$ -module is $A_\phi[p]$ (or, that is the same, $T_\phi[p]$).

Let $\phi \in \mathcal{S}_2(\mathfrak{n})$ be a normalized eigenform and let $\bar{\theta}_\phi$ and $\bar{\rho}_{\phi,\mathfrak{p}}$ be as above. Denote by $\mathfrak{m}_{\phi,\mathfrak{p}}$ the kernel of $\bar{\theta}_\phi$. For any finite set S of prime ideals of \mathcal{O}_F , denote by $\mathbb{T}_n^{(S)}$ the subalgebra of \mathbb{T}_n generated by $\text{T}_\mathfrak{q}$ and $\text{S}_\mathfrak{q}$ for $\mathfrak{q} \nmid \mathfrak{n}$, $\mathfrak{q} \notin S$ and $\text{U}_\mathfrak{q}$ for $\mathfrak{q} \mid \mathfrak{n}$, $\mathfrak{q} \notin S$. Define $\mathfrak{m}_{\phi,\mathfrak{p}}^{(S)} := \mathfrak{m}_{\phi,\mathfrak{p}} \cap \mathbb{T}_n^{(S)}$.

DEFINITION 1.1. — A $\mathbb{T}_n^{(S)}$ -module \mathcal{E} is said to be Eisenstein if its completion $\mathcal{E}_{\mathfrak{m}_{\phi,\mathfrak{p}}^{(S)}}$ is zero for any maximal ideal $\mathfrak{m}_{\phi,\mathfrak{p}}^{(S)}$ defined as above and such that the residual representation $\bar{\rho}_{\phi,\mathfrak{p}}$ is irreducible.

Remark 1.2. — See also the characterization of Eisenstein modules introduced by [18] for $F = \mathbb{Q}$ and generalized by [28].

PROPOSITION 1.3. — *For any integral ideal $\mathfrak{q} \nmid \mathfrak{n}$ of \mathcal{O}_F , define $\eta_{\mathfrak{q}} := T_{\mathfrak{q}} - (|\mathfrak{q}| + 1)$. Let S be a finite set of prime ideals. If $\bar{\rho}_{\phi, \mathfrak{p}}$ is irreducible, then the ideal $\langle \eta_{\mathfrak{q}}, \mathfrak{q} \nmid \mathfrak{n}, \mathfrak{q} \notin S \rangle$ and the maximal ideal $\mathfrak{m}_{\phi, \mathfrak{p}}$ are prime to each other. It follows that, if $T_{\mathfrak{q}} \in \mathbb{T}_{\mathfrak{n}}^{(S)}$ acts on a $\mathbb{T}_{\mathfrak{n}}^{(S)}$ -module \mathcal{E} as multiplication by $|\mathfrak{q}| + 1$, then \mathcal{E} is Eisenstein.*

Proof. — The proof is a direct generalization of [39, Theorem 5.2, part c] □

1.2. Modular elliptic curves

Let E/F be an elliptic curve with no complex multiplication defined over the totally real number field F . Denote by \mathfrak{n} its arithmetic conductor, which is an integral ideal of \mathcal{O}_F . For any rational prime p , denote by $E[p]$ the p -torsion of E and by $T_p(E)$ its p -adic Tate module. Denote finally by

$$\rho_{E,p} : \text{Gal}(\bar{F}/F) \rightarrow \text{Aut}(T_p(E)) \simeq \text{GL}_2(\mathbb{Z}_p)$$

and by

$$\bar{\rho}_{E,p} : \text{Gal}(\bar{F}/F) \rightarrow \text{Aut}(E[p]) \simeq \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

the representation of the absolute Galois group of F , respectively, on $T_p(E)$ and $E[p]$.

DEFINITION 1.4. — *The elliptic curve E of conductor \mathfrak{n} is said to be modular if there exists an eigenform $\phi \in \mathcal{S}_2(\mathfrak{n})$ with rational coefficients so that the $\text{Gal}(\bar{F}/F)$ -modules $T_p(E)$ and $T_{\phi}[p^{\infty}]$ are isomorphic, where p is a rational prime.*

1.3. The Selmer group

Let E be a modular elliptic curve of conductor \mathfrak{n} and let ϕ be its associated eigenform. Assume that the prime p , appearing in the Definition 1.4, satisfies the following:

ASSUMPTION 1.5. — *E has good ordinary reduction at each prime $\mathfrak{p} \mid p$ of \mathcal{O}_F and the representation $T_{\phi}[p]$ is irreducible.*

Note that Assumption 1.5 implies in particular that \mathfrak{n}^- and p are relatively prime. Moreover, since E has no complex multiplication, Assumption 1.5 is verified for infinitely many primes by [41] and [5]. Choose a totally imaginary quadratic extension K/F with relative discriminant $D_{K/F}$ prime to $\mathfrak{n}p$. The extension K defines a factorization $\mathfrak{n} = \mathfrak{n}^+ \mathfrak{n}^-$ where \mathfrak{n}^+ (respectively, \mathfrak{n}^-) is divisible by the prime ideals of F which are split (respectively, inert) in K . The techniques which will be used in this work rely on the following:

ASSUMPTION 1.6. — \mathfrak{n}^- is square-free and the number of prime ideals of \mathcal{O}_F dividing \mathfrak{n}^- and $d := [F : \mathbb{Q}]$ have the same parity. Moreover, $\phi \in \mathcal{S}_2^{\text{new}}(\mathfrak{n}^+, \mathfrak{n}^-)$, that is, ϕ is new at the primes dividing \mathfrak{n}^- .

Remark 1.7. — The above conditions are obviously verified if $[F : \mathbb{Q}]$ is even and $\mathfrak{n}^- = \mathcal{O}_F$, which is the leading example and the most interesting application of this work.

For any field k and any $\text{Gal}(\bar{k}/k)$ -module M , denote by $H^1(k, M) = H^1(\text{Gal}(\bar{k}/k), M)$ the continuous cohomology groups (here \bar{k} is an algebraic closure of k and $i \geq 0$). If \mathfrak{q} is a prime ideal of \mathcal{O}_F , let $K_{\mathfrak{q}}$ be the sum of the completions of K at the primes $v \mid \mathfrak{q}$ of the ring of integers \mathcal{O}_K of K . Choose decomposition subgroups $G_{\mathfrak{q}} \subset \text{Gal}(\bar{F}/F)$ at \mathfrak{q} and $G_v \subset \text{Gal}(\bar{K}/K)$ at $v \mid \mathfrak{q}$ so that $G_v \subseteq G_{\mathfrak{q}}$. Let $I_{\mathfrak{q}} \subset G_{\mathfrak{q}}$ and $I_v \subset G_v$ be the inertia subgroups. Finally, let K_v^{unr} be the maximal unramified extension of K_v . For any $\text{Gal}(\bar{K}/K)$ -module M , set: $H^1(K_{\mathfrak{q}}, M) := \bigoplus_{v \mid \mathfrak{q}} H^1(K_v, M)$ and $H^1(I_{\mathfrak{q}}, M) := \bigoplus_{v \mid \mathfrak{q}} H^1(I_v, M)$, where the sum is extended over all the prime ideals v of K dividing \mathfrak{q} . For any positive integer n , denote by $M_{\phi}[p]$ either $A_{\phi}[p]$ or $T_{\phi}[p]$. In view of the definition of the p -Selmer group $\text{Sel}_p(\phi/K)$ associated to ϕ , p and K , the following notions of finite, singular and ordinary structures are introduced.

Good primes

For primes $\mathfrak{q} \nmid \mathfrak{n}p$ of \mathcal{O}_F , define the *singular part* of $H^1(K_{\mathfrak{q}}, E[p])$ to be:

$$H_{\text{sing}}^1(K_{\mathfrak{q}}, M_{\phi}[p]) := \bigoplus_{v \mid \mathfrak{q}} H^1(K_v^{\text{unr}}, M_{\phi}[p])^{\text{Gal}(K_v^{\text{unr}}/K_v)}.$$

The *finite part* is the kernel of the natural projection map:

$$H_{\text{fin}}^1(K_{\mathfrak{q}}, M_{\phi}[p]) := \text{Ker}(H^1(K_{\mathfrak{q}}, M_{\phi}[p]) \rightarrow H_{\text{sing}}^1(K_{\mathfrak{q}}, M_{\phi}[p])).$$

Primes dividing n^-

If $\mathfrak{q} \mid n^-$, assume that $p \nmid |\mathfrak{q}|^2 - 1$. By the Tate uniformization of elliptic curves, there exists an unique subspace $M_\phi^{(\mathfrak{q})}[p] \simeq \mathbb{Z}/p\mathbb{Z}$ of $M_\phi[p]$ so that $\text{Gal}(\overline{F}_\mathfrak{q}/F_\mathfrak{q})$ acts on it by $\pm\epsilon_p$, where $\epsilon_p : \text{Gal}(\overline{F}_\mathfrak{q}/F_\mathfrak{q}) \rightarrow \mathbb{Z}_p^\times$ is the cyclotomic character describing the action on the p -power roots of unity (if $M_\phi[p]$ is unramified at \mathfrak{q} , use that a Frobenius element at \mathfrak{q} acting on $M_\phi[p]$ has eigenvalues ± 1 and $\pm|\mathfrak{q}|$ and that $p \nmid |\mathfrak{q}|^2 - 1$: see [4, Remark after Assumption 2.1] for more details). In this case there is an exact sequence of $\text{Gal}(\overline{F}/F)$ -modules:

$$0 \rightarrow M_\phi^{(\mathfrak{q})}[p] \rightarrow M_\phi[p] \rightarrow M_\phi^{(1)}[p] := M_\phi[p]/M_\phi^{(\mathfrak{q})}[p] \rightarrow 0$$

and $I_\mathfrak{q}$ acts trivially on the last quotient. Define the *ordinary part* of $H^1(K_\mathfrak{q}, E[p])$ to be:

$$H_{\text{ord}}^1(K_\mathfrak{q}, M_\phi[p]) := \bigoplus_{v|\mathfrak{q}} H^1(K_v, M_\phi^{(\mathfrak{q})}[p]).$$

Primes dividing p

If $\mathfrak{p} \mid p$, by the good ordinary assumption on the reduction of E at \mathfrak{p} , there exists a unique quotient $M_\phi^{(1)}[p] \simeq \mathbb{Z}/p\mathbb{Z}$ of $M_\phi[p]$ so that the inertia subgroup $I_\mathfrak{p}$ at \mathfrak{p} acts trivially on it (see for example [15, Proposition 2.11]). Denote by $M_\phi^{(\mathfrak{p})}[p] \simeq \mathbb{Z}/p\mathbb{Z}$ the kernel of the natural projection map so that there is an exact sequence of $I_\mathfrak{p}$ -modules:

$$0 \rightarrow M_\phi^{(\mathfrak{p})}[p] \rightarrow M_\phi[p] \rightarrow M_\phi^{(1)}[p] \rightarrow 0$$

and $I_\mathfrak{p}$ acts on $M_\phi^{(\mathfrak{p})}[p]$ via the cyclotomic character. The *ordinary part* of $H^1(K_\mathfrak{p}, E[p])$ is defined to be:

$$H_{\text{ord}}^1(K_\mathfrak{p}, M_\phi[p]) := R_\mathfrak{p}^{-1}(H^1(I_v, M_\phi^{(\mathfrak{p})}[p])),$$

where $R_\mathfrak{p} : \bigoplus_{v|\mathfrak{p}} H^1(K_v, M_\phi[p]) \rightarrow \bigoplus_{v|\mathfrak{p}} H^1(I_v, M_\phi[p])$ is the restriction map.

The Tate duality

For any positive integer n , the Galois modules $A_\phi[p]$ and $T_\phi[p]$ are isomorphic to their own Kummer duals and there is a canonical $\text{Gal}(\overline{F}/F)$ -equivariant pairing $A_\phi[p] \times T_\phi[p] \rightarrow \mu_p$. Combining this with the cup product in cohomology yields, for each prime \mathfrak{q} of \mathcal{O}_F , a canonical local Tate pairing:

$$\langle \cdot, \cdot \rangle_\mathfrak{q} : H^1(K_\mathfrak{q}, A_\phi[p]) \times H^1(K_\mathfrak{q}, T_\phi[p]) \rightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

PROPOSITION 1.8. — *If $\mathfrak{q} \nmid \mathfrak{np}$ the groups*

$$H_{\text{fin}}^1(K_{\mathfrak{q}}, A_{\phi}[p]) \text{ and } H_{\text{fin}}^1(K_{\mathfrak{q}}, T_{\phi}[p])$$

are annihilators to each other under the local Tate pairing $\langle, \rangle_{\mathfrak{q}}$. The same is true for $H_{\text{ord}}^1(K_{\mathfrak{q}}, A_{\phi}[p])$ and $H_{\text{ord}}^1(K_{\mathfrak{q}}, T_{\phi}[p])$ for primes $\mathfrak{q} \mid \mathfrak{n}^-p$.

Proof. — This result follows from standard properties of the local Tate pairing: see for example [15, Section 2.3]. □

Selmer groups

For any prime ideal \mathfrak{q} of \mathcal{O}_F , denote by

$$\text{res}_{\mathfrak{q}} : \oplus_{v|\mathfrak{q}} H^1(K_v, M_{\phi}[p]) \rightarrow \oplus_{v|\mathfrak{q}} H^1(I_v, M_{\phi}[\mathfrak{p}])$$

the restriction map. For primes $\mathfrak{q} \nmid \mathfrak{np}$, let

$$\partial_{\mathfrak{q}} : H^1(K, M_{\phi}[p]) \rightarrow H_{\text{sing}}^1(K, M_{\phi}[p])$$

be the composition of the restriction with the projection. If $\partial_{\mathfrak{q}}(s) = 0$, then denote by $v_{\mathfrak{q}}(s)$ the image of s in $H_{\text{fin}}^1(K, M_{\phi}[p])$.

DEFINITION 1.9. — *The Selmer group $\text{Sel}_p(\phi/K)$ is the subgroup of the global cohomology group $H^1(K, A_{\phi}[p])$ consisting of those elements s so that:*

1. For $\mathfrak{q} \nmid \mathfrak{np}$, $\partial_{\mathfrak{q}}(s) = 0$.
2. For primes $\mathfrak{q} \mid \mathfrak{n}^-p$, $\text{res}_{\mathfrak{q}}(s) \in H_{\text{ord}}^1(K_{\mathfrak{q}}, A_{\phi}[p])$.
3. For primes $\mathfrak{q} \mid \mathfrak{n}^+$, $\text{res}_{\mathfrak{q}}(s) = 0$.

2. The Euler system argument

2.1. Admissible primes

Keep the same notations and assumptions as in Section 1: E is a modular elliptic curve and ϕ is its associated eigenform.

DEFINITION 2.1. — *A prime ideal ℓ of \mathcal{O}_F is said to be admissible (relatively to the prime p) if the following conditions hold:*

- (i) ℓ does not divide \mathfrak{np} ;
- (ii) ℓ is inert in K ;
- (iii) p does not divide $|\ell|^2 - 1$;
- (iv) p divides $|\ell| + 1 - \epsilon a_{\ell}$, where $\epsilon = \pm 1$ and $a_{\ell} = \theta_{\phi}(\mathbf{T}_{\ell})$.

Note that if ℓ is an admissible prime then $K_\ell := K \otimes_F F_\ell \simeq F_{\ell^2}$, where F_{ℓ^2} is the unique quadratic unramified extension of F_ℓ .

LEMMA 2.2. — *Let ℓ be an admissible prime. Then the local cohomology groups $H_{\text{fin}}^1(K_\ell, A_\phi[p])$ and $H_{\text{sing}}^1(K_\ell, T_\phi[p])$ are both isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

Proof. — A direct generalization of [4, Lemma 2.6]. □

THEOREM 2.3. — *Let s be a non-zero element of $H^1(K, A_\phi[p])$. Then there exist infinitely many admissible primes such that $\partial_\ell(s) = 0$ and $v_\ell(s) \neq 0$.*

Proof. — A direct generalization of [4, Theorem 3.2]. □

2.2. Controlling the Selmer group

DEFINITION 2.4. — *A collection of cohomology classes*

$$\{\kappa_\ell\}_\ell \subseteq H^1(K_\ell, T_\phi[p])$$

indexed by the set of admissible primes ℓ is said to be an Euler system for ϕ/K relative to p if each class κ_ℓ enjoys the following properties:

1. *For $\mathfrak{q} \nmid \mathfrak{n}p\ell$, $\partial_\mathfrak{q}(\kappa_\ell) = 0$.*
2. *For $\mathfrak{q} \mid \mathfrak{n}^-p$, $\text{res}_\mathfrak{q}(\kappa_\ell) \in H_{\text{ord}}^1(K_\mathfrak{q}, T_\phi[p])$.*

Note that in the previous definition no condition is required for the primes $\mathfrak{q} \mid \mathfrak{n}^+\ell$. The next standard argument reduces the proof of Theorem C in the Introduction to the problem of producing an Euler system.

LEMMA 2.5. — *Let $\{\kappa_\ell\}_\ell$ be an Euler system for ϕ/K relative to p and assume that for all but a finite number of primes $\partial_\ell(\kappa_\ell) \neq 0$. Then $\text{Sel}_p(\phi/K) = 0$.*

Proof. — Assume that there exists $s \in \text{Sel}_p(\phi/K)$ with $s \neq 0$ and, by Theorem 2.3, fix an admissible prime ℓ so that $\text{res}_\ell(s) \neq 0$ and $\partial_\ell(\kappa_\ell) \neq 0$. By the global reciprocity law of class field theory, $\sum_\mathfrak{q} \langle \text{res}_\mathfrak{q}(s), \text{res}_\mathfrak{q}(\kappa_\ell) \rangle_\mathfrak{q} = 0$, where the sum is over all the prime ideals of \mathcal{O}_F . Proposition 1.8 and Definition 2.4 imply that $\text{res}_\mathfrak{q}(s)$ and $\text{res}_\mathfrak{q}(\kappa_\ell)$ are orthogonal to each other with respect to the local Tate pairing $\langle \cdot, \cdot \rangle_\mathfrak{q}$ at primes $\mathfrak{q} \neq \ell$, so $\langle \text{res}_\ell(s), \text{res}_\ell(\kappa_\ell) \rangle_\ell = 0$. Then since $\partial_\ell(\kappa_\ell) \neq 0$, Lemma 2.2 yields $\text{res}_\ell(s) = 0$. This contradiction proves the lemma. □

Theorem C of the Introduction now follows from the existence of an Euler system satisfying prescribed local conditions at ℓ via Lemma 2.5. The rest of the work is devoted to the construction of an Euler system under the hypothesis that the order at $s = 1$ of the L -function $L_K(\phi, s)$ of ϕ over K is zero. The strategy will be to find the classes κ_ℓ for admissible primes ℓ in the cohomology of Shimura curves defined from quaternion algebras of discriminant $\mathfrak{n}^- \ell$. The theory of congruences between modular forms at the admissible prime ℓ will give the required properties. Before stating the result to be proved in the next sections, define S to be the set of all the primes $p > 3$ so that:

1. p divides the algebraic part $\mathcal{L}_K(\phi) \in \mathbb{Z}$ of $L_K(\phi, s)$ defined in Section 5.1;
2. There are non-trivial congruences (mod p) between ϕ and other eigenforms of level \mathfrak{n} (for more details, see Definition 4.7);
3. The representation $\bar{\rho}_{\phi,p}$ is reducible.

The result to be proved in the next sections is the following:

THEOREM 2.6. — *Assume that E is modular. If $p \notin S$, then there exists an Euler system $\{\kappa_\ell\}_\ell$ for ϕ relative to p .*

3. The Jacquet-Langlands correspondence

3.1. Modular forms on quaternion algebras

Fix a quaternion algebra B over F of discriminant \mathfrak{m}^- which is ramified at all the archimedean places of F . Fix a prime ideal \mathfrak{m}^+ prime to \mathfrak{m}^- and let $R \subseteq B$ be an Eichler order of level \mathfrak{m}^+ . (Hence, $\mathfrak{m}^- = \prod_{j=1}^s \mathfrak{q}_j$ is square-free and s has the same parity as $[F : \mathbb{Q}]$.) Denote by \widehat{B} (respectively, \widehat{R}) the finite adèle ring of B (respectively, R). Fix an open compact subgroup $U \subseteq \widehat{B}^\times$ and a ring C .

DEFINITION 3.1. — *The space of C -valued modular forms with respect to U on the quaternion algebra B is the C -module*

$$\mathcal{S}_2^B(U; C) := \mathcal{L}(U; C) / \mathcal{L}(U; C)^{\text{triv}}$$

where the elements of $\mathcal{L}(U; C)$ are functions $f : U \backslash \widehat{B}^\times / B^\times \rightarrow C$ and $\mathcal{L}(U; C)^{\text{triv}}$ is the C -submodule of $\mathcal{L}(U; C)$ consisting of those functions which factor through the adelization $\widehat{n}_B : \widehat{B} \rightarrow \widehat{F}$ of the norm map $n_B : B \rightarrow F$.

For a fixed Eichler order R , refer to $\mathcal{S}_2^B(\widehat{R}^\times; C)$ as the space of modular forms of level \mathfrak{m}^+ and denote it by $\mathcal{S}_2^B(\mathfrak{m}^+; C)$.

3.2. The Hecke algebra $\mathbb{T}_{\mathfrak{m}^+}^B$

The Hecke operator $T_{\mathfrak{q}}$

Let \mathfrak{q} be a prime ideal of \mathcal{O}_F not dividing \mathfrak{m}^+ and assume that $U_{\mathfrak{q}} \simeq \mathcal{R}_{\mathfrak{q}}^{\times}$. Define the Hecke operator

$$T_{\mathfrak{q}} : \mathbb{Z}[U \backslash \widehat{B}^{\times} / B^{\times}] \longrightarrow \mathbb{Z}[U \backslash \widehat{B}^{\times} / B^{\times}]$$

by the rule: $T_{\mathfrak{q}}(g) := \sum_{\alpha} \begin{pmatrix} 1 & \alpha \\ 0 & \pi_{\mathfrak{q}} \end{pmatrix} g + \begin{pmatrix} \pi_{\mathfrak{q}} & 0 \\ 0 & 1 \end{pmatrix} g$, where the sum is extended over a set of representatives $\{\alpha\}$ for the quotient $\mathcal{O}_{F,\mathfrak{q}}/\mathfrak{q}$, the element $\pi_{\mathfrak{q}} \in \mathcal{O}_{F,\mathfrak{q}}$ is chosen so that $\text{val}_{\mathfrak{q}}(\pi_{\mathfrak{q}}) = 1$ and the matrices are ideles whose \mathfrak{q} -component is the displayed one and the other components are all equal to 1. Now use strong approximation to describe $T_{\mathfrak{q}}$. Set: $\widehat{\mathcal{O}}_F \left[\frac{1}{\mathfrak{q}} \right] := \widehat{\mathcal{O}}_F^{(\mathfrak{q})} F_{\mathfrak{q}}$, and $U \left[\frac{1}{\mathfrak{q}} \right] := U^{(\mathfrak{q})} \text{GL}_2(F_{\mathfrak{q}})$, where the superscript (\mathfrak{q}) denotes the idele with the \mathfrak{q} -component removed. By the strong approximation theorem (see [47, page 60]): $\widehat{B}^{\times} \simeq \prod_{j=1}^h U \left[\frac{1}{\mathfrak{q}} \right] g_j B^{\times}$, where g_1, \dots, g_h are representatives of the double coset space $U^{(\mathfrak{q})} \backslash \widehat{B}^{(\mathfrak{q})\times} / B^{\times} = U \left[\frac{1}{\mathfrak{q}} \right] \backslash \widehat{B}^{\times} / B^{\times} \simeq \widehat{\mathfrak{n}}_B \left(U \left[\frac{1}{\mathfrak{q}} \right] \right) \backslash \widehat{F}^{\times} / F_+$ (the last isomorphism is induced by the adelization $\widehat{\mathfrak{n}}_B$ of the norm map and F_+ denotes the group of totally positive elements of F). Define now the following subgroups for each $j = 1, \dots, h$:

$$\begin{aligned} \widetilde{\Gamma}_{j,0,\mathfrak{q}} &:= g_j^{-1} U \left[\frac{1}{\mathfrak{q}} \right] g_j \cap B^{\times}; & \Gamma_{j,0,\mathfrak{q}} &:= \widetilde{\Gamma}_{j,0,\mathfrak{q}} / \mathcal{O}_F \left[\frac{1}{\mathfrak{q}} \right]^{\times}; \\ \widetilde{\Gamma}_{j,+, \mathfrak{q}} &:= (\widetilde{\Gamma}_{j,0,\mathfrak{q}})_e; & \Gamma_{j,+, \mathfrak{q}} &:= (\Gamma_{j,0,\mathfrak{q}})_e, \end{aligned}$$

where the subscript e means elements of even \mathfrak{q} -adic valuation. The strong approximation theorem yields:

$$U \backslash \widehat{B}^{\times} / B^{\times} \simeq \prod_{j=1}^h \text{PGL}_2(\mathcal{O}_{F,\mathfrak{q}}) \backslash \text{PGL}_2(F_{\mathfrak{q}})(g_j)_{\mathfrak{q}} / \Gamma_{j,0,\mathfrak{q}}$$

where $(g_j)_{\mathfrak{q}}$ denotes the projection of g_j on the \mathfrak{q} -component. Note that $g \in U \backslash \widehat{B}^{\times} / B^{\times}$ lies on the i -th component of the last product if and only if $\widehat{\mathfrak{n}}_B(g) = \widehat{\mathfrak{n}}_B(g_i)$, so $T_{\mathfrak{q}}$ acts componentwise. Denote by $\mathcal{T}_{\mathfrak{q}}$ the Bruhat-Tits tree of $\text{PGL}_2(F_{\mathfrak{q}})$ and by $\mathcal{V}(\mathcal{T}_{\mathfrak{q}})$ its vertexes. For each j there is a natural projection $\mathcal{V}(\mathcal{T}_{\mathfrak{q}}) \rightarrow \text{PGL}_2(\mathcal{O}_{F,\mathfrak{q}}) \backslash \text{PGL}_2(F_{\mathfrak{q}})(g_j)_{\mathfrak{q}} / \Gamma_{j,0,\mathfrak{q}}$. The operator $T_{\mathfrak{q}}$ is induced by the projection of the operator $\widetilde{T}_{\mathfrak{q}}$ of $\mathbb{Z}[\mathcal{V}(\mathcal{T}_{\mathfrak{q}})]$ which associates to each vertex v the sum of the vertices w whose distance from v is 1. Note that the degree of $T_{\mathfrak{q}}$ is $|\mathfrak{q}| + 1$.

The Hecke operator U_q

Let \mathfrak{q} be a prime ideal of \mathcal{O}_F dividing \mathfrak{m}^+ and assume that $U_q \simeq \mathcal{R}_q^\times$. Using the same conventions as above, define the Hecke operator

$$U_q : \mathbb{Z}[U \backslash \widehat{B}^\times / B^\times] \longrightarrow \mathbb{Z}[U \backslash \widehat{B}^\times / B^\times]$$

by the rule: $U_q(g) := \sum_{\alpha} \begin{pmatrix} 1 & \alpha \\ 0 & \pi_q \end{pmatrix} g$, where $\{\alpha\}$ is a set of representatives for $\mathcal{O}_{F,q}/\mathfrak{q}$. Suppose that \mathfrak{q} divides \mathfrak{m}^+ exactly. In this case it is possible to obtain a description for U_q as for T_q . Using the same notations and definitions as above, the strong approximation theorem yields:

$$U \backslash \widehat{B}^\times / B^\times = \prod_{j=1}^h \Gamma_0(\pi_q) \backslash \mathrm{PGL}_2(F_q) / \Gamma_{j,0,q},$$

where $\Gamma_0(\pi_q) \subseteq \mathrm{PGL}_2(\mathcal{O}_{F,q})$ is the subgroup of $(\bmod \mathfrak{q})$ upper triangular matrices. For each j there is a projection map $\vec{\mathcal{E}}(\mathcal{T}_q) = \Gamma_0(\pi_q) \backslash \mathrm{PGL}_2(F_q) \rightarrow \Gamma_0(\pi_q) \backslash \mathrm{PGL}_2(F_q) / \Gamma_{j,0,q}$. The operator U_q is induced by the projection of the operator \widetilde{U}_q of $\mathbb{Z}[\mathcal{E}(\mathcal{T}_q)]$ which associates to any oriented edge $e = (v, w)$ the sum of the edges e' emanating from its target (that is, of the form (w, z) for some vertex $z \neq v$). It is clear that the degree of U_q is $|\mathfrak{q}|$.

Hecke algebras

For a prime ideal $\mathfrak{q} \nmid \mathfrak{m}^+ \mathfrak{m}^-$ so that $U_q \simeq R_q^\times$, denote by

$$S_q : \mathbb{Z}[U \backslash \widehat{B}^\times / B^\times] \rightarrow \mathbb{Z}[U \backslash \widehat{B}^\times / B^\times]$$

the spherical operator defined by: $S_q(g) := \sum_{\alpha} \alpha g$, where $U \pi_q U = \sum_{\alpha} \alpha U$. Denote by $\mathbb{T}_{\mathfrak{m}^+}^B$ the free \mathbb{Z} -algebra generated by T_q and S_q for prime ideals $\mathfrak{q} \nmid \mathfrak{m}^+ \mathfrak{m}^-$ and U_q for prime ideals $\mathfrak{q} \mid \mathfrak{m}^+$. The space of modular forms $\mathcal{S}_2^B(\mathfrak{m}^+; \mathbb{Z})$ is naturally a $\mathbb{T}_{\mathfrak{m}^+}^B$ -module. Moreover, if $U_q \simeq \mathcal{R}_q$ for $\mathfrak{q} \notin S$, where S is a finite set of prime ideals, then $\mathcal{S}_2^B(U; \mathbb{Z})$ is naturally a $\mathbb{T}_{\mathfrak{m}^+}^{B,(S)}$ -module, where $\mathbb{T}_{\mathfrak{m}^+}^{B,(S)}$ is the subalgebra of $\mathbb{T}_{\mathfrak{m}^+}^B$ generated by Hecke operators corresponding to primes not in S .

Generalized Brandt matrices

It is possible to give another description of Hecke operators in terms of Brandt matrices. This is a classical subject and an example of the Jacquet-Langlands correspondence, established in this case by the Eichler trace

formula [20]. The exposition follows closely Jordan-Livné [31]; the aim of this section is to generalize the divisibility property of [39, Theorem 3.12] and [31, Proposition 1.10]. Let $U \subseteq \widehat{B}^\times$ be an open compact subgroup and let g_1, \dots, g_h be a set of representatives of the double coset space $U \backslash \widehat{B}^\times / B^\times$. Assume that $\mathcal{S}_2(U; \mathbb{Z})$ is a $\mathbb{T}_{\mathfrak{m}^+}^{B, (S)}$ -module for a finite set of primes S . Any operator $T \in \mathbb{T}_{\mathfrak{m}^+}^{B, (S)}$ induces a linear map

$$T : \mathbb{Z}[U \backslash \widehat{B}^\times / B^\times] \rightarrow \mathbb{Z}[U \backslash \widehat{B}^\times / B^\times].$$

Denote by $B(\mathfrak{q}) = (m_{i,j}(\mathfrak{q}))_{i,j=1,\dots,h}$ the matrix of T associated to the chosen basis g_1, \dots, g_h . For $j = 1, \dots, h$, define $U_j := g_j^{-1} U g_j$ and $\Gamma_j := g_j^{-1} U g_j \cap B^\times$ and set $w_j := [\Gamma_j : \mathcal{O}_F^\times]$. Let finally $\{n_1, \dots, n_s\}$ be the orders of the groups $(\Gamma_i^\times \cap \Gamma_j) / \mathcal{O}_F^\times$ for $i, j \in \{1, \dots, h\}$.

PROPOSITION 3.2. — *Assume that the class number of F is one and for any n_i , the norm map from the ideals of $F(\mu_{n_i})$ to the ideals of F is injective, where μ_{n_j} are the n_j -th roots of unity. Then for any ideal \mathfrak{q} not dividing $\mathfrak{m}^+ \mathfrak{m}^-$ such that $U_{\mathfrak{q}} \simeq R_{\mathfrak{q}}^\times$, the entries $m_{i,j}(\mathfrak{q})$ of the i -th row of the Brandt matrix $B(\mathfrak{q})$ are divisible by w_i unless $i = j$.*

Proof. — The proof is a direct generalization of [31, Proposition 1.10]. □

PROPOSITION 3.3. — *Assume that $n_j = 1$ for all $j = 1, \dots, s$. Then for any ideal \mathfrak{q} not dividing $\mathfrak{m}^+ \mathfrak{m}^-$ such that $U_{\mathfrak{q}} \simeq R_{\mathfrak{q}}^\times$, the entries $m_{i,j}(\mathfrak{q})$ of the i -th row of the Brandt matrix $B(\mathfrak{q})$ are divisible by w_i unless $i = j$.*

Proof. — Fix a prime ideal $\mathfrak{q} \nmid \mathfrak{m}^+ \mathfrak{m}^-$. From Section 3.2, the operator $T_{\mathfrak{q}}$ is induced by the projection of the operator $\widetilde{T}_{\mathfrak{q}}$ of $\mathbb{Z}[\mathcal{V}(\mathcal{T}_{\mathfrak{q}})]$ which associates to each vertex v the sum of the vertices w whose distance from v is 1. Fix the vertex v_i corresponding to g_i via strong approximation and let $v_j \neq v_i$ be a vertex belonging to the support of $T_{\mathfrak{q}}(v_i)$. Since any element in Γ_i induces a permutation of the vertexes joined to v_i , it is clear that the order of v_j in $T_{\mathfrak{q}}(v_i)$ is divisible by $\frac{w_i}{(\Gamma_i^\times \cap \Gamma_j) / \mathcal{O}_F^\times}$. The result follows. □

The canonical pairing

There is a pairing

$$\langle \ , \ \rangle : \mathbb{Z}[U \backslash \widehat{B}^\times / B^\times] \times \mathbb{Z}[U \backslash \widehat{B}^\times / B^\times] \rightarrow \mathbb{Z}$$

defined to be the extension by \mathbb{Z} -linearity of the following rule: for any pair $(x, y) \in U \backslash \widehat{B}^\times / B^\times \times U \backslash \widehat{B}^\times / B^\times$, $\langle x, y \rangle := w(x) \delta_{x,y}$, where $\delta_{x,y}$ is

the Kronecker symbol and $w(x) := [\Gamma_x : \mathcal{O}_F^\times]$ is the weight of x , where $\Gamma_x := x^{-1}Ux \cap B^\times$. Consider the embedding

$$j : \mathbb{Z}[U \backslash \widehat{B}^\times / B^\times] \rightarrow \mathbb{Z}[U \backslash \widehat{B}^\times / B^\times]^\vee$$

deduced from the pairing $\langle \cdot, \cdot \rangle$, where the superscript \vee denotes the \mathbb{Z} -dual. Define

$$\Phi = \Phi(U) := \frac{\mathbb{Z}^0[U \backslash \widehat{B}^\times / B^\times]^\vee}{j(\mathbb{Z}^0[U \backslash \widehat{B}^\times / B^\times])}.$$

Recall the integers w_j and n_i associated as above to a chosen basis of $U \backslash \widehat{B}^\times / B^\times$.

DEFINITION 3.4. — *The pair (F, U) is said to be Eisenstein if at least one of the following conditions is verified:*

- (i) *The assumption of Proposition 3.2 is verified: the class number of F is one and for any n_i , the norm map from the ideals of $F(\mu_{n_i})$ to the ideals of F is injective.*
- (ii) *The assumption of Proposition 3.3 is verified: $n_j = 1$ for all $j = 1, \dots, s$.*

PROPOSITION 3.5. — *If the pair (F, U) is Eisenstein, then for any integral ideal $\mathfrak{q} \nmid \mathfrak{m}^+ \mathfrak{m}^-$ such that $U_{\mathfrak{q}} \simeq R_{\mathfrak{q}}^\times$, the operator $\eta_{\mathfrak{q}} := T_{\mathfrak{q}} - (|\mathfrak{q}| + 1) \in \mathbb{T}_{\mathfrak{m}^+}^B$ annihilates Φ .*

Proof. — A direct generalization of [39, Proposition 3.12] which can be deduced from Propositions 3.2 and 3.3. □

COROLLARY 3.6. — *If the pair (F, U) is Eisenstein, then Φ is Eisenstein.*

Proof. — This is a direct consequence of Propositions 3.5 and 1.3. □

3.3. The Jacquet-Langlands correspondence

Set $\mathfrak{m} := \mathfrak{m}^+ \mathfrak{m}^-$. Recall from Section 1.1 that $\mathcal{S}_2^{\text{new}}(\mathfrak{m}^+, \mathfrak{m}^-)$ is the subspace of $\mathcal{S}_2(\mathfrak{m})$ consisting of those forms which are new at the primes dividing \mathfrak{m}^- and denote by $\mathbb{T}_{\mathfrak{m}^+, \mathfrak{m}^-}^{\text{new}}$ the quotient of $\mathbb{T}_{\mathfrak{m}}$ acting faithfully on $\mathcal{S}_2^{\text{new}}(\mathfrak{m}^+, \mathfrak{m}^-)$.

THEOREM 3.7 (Jacquet-Langlands). — *Let $\phi \in \mathcal{S}_2^{\text{new}}(\mathfrak{m}^+, \mathfrak{m}^-)$ be a normalized eigenform for $\mathbb{T}_{\mathfrak{m}}$ with rational coefficients. Then there exists a modular form $f \in \mathcal{S}_2^B(\mathfrak{m}^+; \mathbb{Z})$ such that, for $\mathfrak{q} \nmid \mathfrak{m}$, $T_{\mathfrak{q}}(f) = \theta_{\phi}(T_{\mathfrak{q}})f$, while for $\mathfrak{q} \mid \mathfrak{m}^+$: $U_{\mathfrak{q}}(f) = \theta_{\phi}(U_{\mathfrak{q}})f$. Moreover, the Hecke algebra $\mathbb{T}_{\mathfrak{m}^+}^B$ is isomorphic to the quotient $\mathbb{T}_{\mathfrak{m}^+, \mathfrak{m}^-}^{\text{new}}$ of $\mathbb{T}_{\mathfrak{m}}$.*

Proof. — This result is due to [27] and can be obtained using Eichler’s trace formula [20] generalized to totally real fields as in see [47, V.2.4]. See [1, Section 1.6] for a statement in this form. \square

If $\mathcal{S}_2(U; \mathbb{Z})$ is a $\mathbb{T}_{\mathfrak{m}^+}^{B, (S)}$ -module, then it is also a faithful $\mathbb{T}_U := \mathbb{T}_{\mathfrak{m}^+}^{B, (S)} \cap \mathbb{T}_{\mathfrak{m}^+, \mathfrak{m}^-}^{\text{new}}$ -module.

4. Shimura curves

4.1. Definition

Let F be a totally real number field of degree d over \mathbb{Q} . Fix integral ideals \mathfrak{c}^+ and \mathfrak{c}^- of \mathcal{O}_F prime to each other so that $\mathfrak{c}^- \neq \mathcal{O}_F$ is square-free and the number of primes dividing it have opposite parity with respect to d . Let \mathcal{B} be the quaternion algebra defined over F with discriminant \mathfrak{c}^- which is split in exactly one of the archimedean places of F , say μ . Choose an Eichler order $\mathcal{R} \subseteq \mathcal{B}$ of level \mathfrak{c}^+ and, for any prime $\mathfrak{q} \nmid \mathfrak{c}^-$, fix isomorphisms: $\varphi_{\mathfrak{q}} : \mathcal{B}_{\mathfrak{q}} := \mathcal{B} \otimes_F F_{\mathfrak{q}} \rightarrow M_2(F_{\mathfrak{q}})$ so that: $\varphi_{\mathfrak{q}}(\mathcal{R}_{\mathfrak{q}}) = M_2^{\text{val}_{\mathfrak{q}}(\mathfrak{c}^+)}(\mathcal{O}_{F, \mathfrak{q}})$, where the following notations are used: $\mathcal{O}_{F, \mathfrak{q}}$ is the completion of \mathcal{O}_F at \mathfrak{q} , the symbol $\text{val}_{\mathfrak{q}}(\mathfrak{c}^+)$ denotes the valuation of \mathfrak{c}^+ at \mathfrak{q} and $M_2^{\text{val}_{\mathfrak{q}}(\mathfrak{c}^+)}(\mathcal{O}_{F, \mathfrak{q}}) \subseteq M_2(\mathcal{O}_{F, \mathfrak{q}})$ is the subgroup of the $(\text{mod } \mathfrak{q}^{\text{val}_{\mathfrak{q}}(\mathfrak{c}^+)})$ upper triangular matrices. Denote by $\widehat{\mathcal{B}}$ and $\widehat{\mathcal{R}}$ the finite adèle rings of, respectively, \mathcal{B} and \mathcal{R} and set $\mathcal{H}^{\pm} := \mathbb{C} - \mathbb{R}$. Fix an open compact subgroup $\mathcal{U} \subseteq \widehat{\mathcal{B}}^{\times}$ and set:

$$X_{\mathcal{U}}(\mathbb{C}) := \mathcal{U} \backslash \widehat{\mathcal{B}}^{\times} \times \mathcal{H}^{\pm} / \mathcal{B}^{\times}.$$

By the strong approximation theorem, there are elements $g_j \in \widehat{\mathcal{B}}^{\times}$ so that $\widehat{\mathcal{B}}^{\times} := \coprod_{j=1}^h \mathcal{U} g_j \mathcal{B}^{\times}$. Define \mathcal{B}_+ to be the subgroup of \mathcal{B} consisting of elements b whose image in $\mathcal{B} \otimes_{\mu} \mathbb{R} \simeq \text{GL}_2(\mathbb{R})$ belongs to $\text{GL}_2^+(\mathbb{R})$, the subgroup of matrices with positive determinant (the tensor product is over the archimedean place μ where \mathcal{B} is split). Then $\Gamma_j := g_j^{-1} \mathcal{U} g_j \cap \mathcal{B}_+$ acts on $\mathcal{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$ by fractional linear transformation via the embedding $\mu : \mathcal{B}_+ \rightarrow \text{GL}_2^+(\mathbb{R})$. By [43, Proposition 9.2], \mathcal{H} / Γ_j has a structure of Riemann surface, and $X_{\mathcal{U}}(\mathbb{C}) \simeq \coprod_{j=1}^h \mathcal{H} / \Gamma_j$ has a rational model $X_{\mathcal{U}}$ over $\text{Spec}(F)$ which is connected but not geometrically connected; denote by $J_{\mathcal{U}}$ the connected component subgroup of $\text{Pic}(X_{\mathcal{U}})$ over F .

By [10, Section 2], $X_{\mathcal{U}}$ has a descriptions as moduli space for suitable abelian varieties with level structure. >From this description it follows that $X_{\mathcal{U}}$ has a model $\mathcal{X}_{\mathcal{U}}$ over $\text{Spec}(\mathcal{O}_F)$. For more details and for a complete exposition of this topic, see [53, Section 1]. If $\mathcal{U} = \widehat{\mathcal{R}}^{\times}$, denote $X_{\mathcal{U}}, \mathcal{X}_{\mathcal{U}}$

and $J_{\mathcal{U}}$ respectively by $X_{\mathfrak{c}^+, \mathfrak{c}^-}$, $\mathcal{X}_{\mathfrak{c}^+, \mathfrak{c}^-}$ and $J_{\mathfrak{c}^+, \mathfrak{c}^-}$. In this case, an object in $X_{\mathfrak{c}^+, \mathfrak{c}^-}$ can be identified with a pair $(\underline{A}, C) = ((A, \iota, \theta, \kappa), C)$ consisting of: an abelian scheme $A \rightarrow \text{Spec}(S)$, where S is an F' -scheme and F' a fixed imaginary quadratic extension of F ; an action $\iota : \mathcal{O}_{\mathcal{B}'} \rightarrow \text{End}(A)$ of a maximal order $\mathcal{O}_{\mathcal{B}'} \supseteq \mathcal{R}' := \mathcal{R} \otimes_{\mathcal{O}_F} \mathcal{O}_{F'}$ of $\mathcal{B}' := \mathcal{B} \otimes_F F'$ on $\text{End}(A)$, where $\mathcal{O}_{F'}$ is the ring of integers of F' ; a class $\theta : A \rightarrow A^\vee$ of polarizations; a \mathcal{B}' -linear isomorphism $\kappa : \widehat{\mathcal{O}}_{\mathcal{B}'} \rightarrow \prod_q T_q(A)$, where $\widehat{\mathcal{O}}_{\mathcal{B}'}$ is the finite adèle ring of $\mathcal{O}_{\mathcal{B}'}$ and for all rational primes q , $T_q(A)$ is the q -adic Tate module of A ; a cyclic submodule structure C of level \mathfrak{c}^+ defined in [53, 1.5.2].

Suppose that for $\mathfrak{q} \notin S$, $\mathcal{U}_{\mathfrak{q}} \simeq \mathcal{R}_{\mathfrak{q}}^\times$, where S is a finite set of primes of \mathcal{O}_F . Then $\mathcal{X}_{\mathcal{U}}$ has a natural structure of $\mathbb{T}_{\mathcal{U}} := \mathbb{T}_{\mathfrak{c}^+, \mathfrak{c}^-}^{\text{new}} \cap \mathbb{T}_{\mathfrak{c}^+}^{(S)}$ -module, where $\mathfrak{c} := \mathfrak{c}^+ \mathfrak{c}^-$. Define the *Hodge class* of $\mathcal{X}_{\mathcal{U}}$ to be the unique element $\xi \in \text{Pic}(\mathcal{X}_{\mathcal{U}})$ such that ξ has degree one on each connected component of $\mathcal{X}_{\mathcal{U}}$ and the action of $\mathbb{T}_{\mathcal{U}}$ on ξ is Eisenstein (that is, for any prime $\mathfrak{q} \notin S$, $\mathfrak{q} \nmid n\ell$, the action of $T_{\mathfrak{q}} \in \mathbb{T}_{\mathcal{U}}$ on ξ is given by multiplication by $|\mathfrak{q}| + 1$). For existence and uniqueness of this class, see [53, Section 4.1] and [52, Section 6.2]. Denote by $\text{Pic}^{\text{Eis}}(\mathcal{X}_{\mathcal{U}})$ the subgroup of $\text{Pic}(\mathcal{X}_{\mathcal{U}})$ consisting of those elements whose restriction to any connected component of $\mathcal{X}_{\mathcal{U}}$ is a multiple of ξ . By [52, Section 6.1], $\text{Pic}(\mathcal{X}_{\mathcal{U}}) = \text{Pic}^{\text{Eis}}(\mathcal{X}_{\mathcal{U}}) \oplus \text{Pic}^0(\mathcal{X}_{\mathcal{U}})$. If \mathcal{I} is an ideal of $\mathbb{T}_{\mathfrak{c}^+, \mathfrak{c}^-}^{\text{new}}$ so that the maximal ideal containing it comes from an irreducible representation, then the canonical inclusion induces an isomorphism:

$$(4.1) \quad \text{Pic}^0(\mathcal{X}_{\mathcal{U}})/\mathcal{I}^{(S)} \simeq \text{Pic}(\mathcal{X}_{\mathcal{U}})/\mathcal{I}^{(S)},$$

where $\mathcal{I}^{(S)} := \mathcal{I} \cap \mathbb{T}_{\mathcal{U}}$.

4.2. The Čerednik-Drinfeld theorem

Let $\mathcal{X} := \mathcal{X}_{\mathcal{U}}$ be the scheme over $\text{Spec}(\mathcal{O}_F)$ defined in Section 4.1. Let $\ell \mid \mathfrak{c}^-$ be a prime ideal and denote by \mathcal{X}_{ℓ} the special fiber of \mathcal{X} over $\text{Spec}(\mathcal{O}_{F, \ell})$. Define the formal group $\widehat{\mathcal{X}}_{\ell}$ over $\mathcal{O}_{F, \ell}$ to be the completion of \mathcal{X}_{ℓ} along its special fiber. Let B be the quaternion algebra over F of discriminant \mathfrak{c}^-/ℓ which is ramified at all the archimedean places of F (such an algebra exists by the assumption on \mathfrak{c}^-). The algebra B is said to be obtained from \mathcal{B} by interchanging the invariants at ℓ and μ , where μ is the only archimedean place where \mathcal{B} is split. For any \mathbb{Z} -algebra A , denote by $\widehat{A}^{(\ell)}$ the finite adèle ring \widehat{A} with the ℓ -component removed. Fix an isomorphism $\varphi : \widehat{B} \xrightarrow{\sim} \widehat{\mathcal{B}}^{(\ell)} M_2(F_{\ell})$ and choose Eichler orders R and R_{ℓ} of B of level, respectively, \mathfrak{c}^+ and $\mathfrak{c}^+ \ell$ so that $R \supseteq R_{\ell}$ and, under the above

isomorphism, $\widehat{\mathcal{R}}^{(\ell)}$ corresponds to $\widehat{R}^{(\ell)} = \widehat{R}_\ell^{(\ell)}$. Finally, set:

$$U := \varphi(\mathcal{U}^{(\ell)}) \cdot (R^\times \otimes_{\mathcal{O}_F} \mathcal{O}_{F,\ell}) \quad \text{and} \quad U_\ell := \varphi(\mathcal{U}^{(\ell)}) \cdot (R_\ell^\times \otimes_{\mathcal{O}_F} \mathcal{O}_{F,\ell}).$$

Denote by \mathbb{C}_ℓ the completion of an algebraic closure of F_ℓ and let $\widehat{\mathcal{H}}_\ell$ be the Deligne’s formal scheme over $\text{Spec}(\mathcal{O}_{F,\ell})$ obtained by blowing-up the projective line over $\text{Spec}(\mathcal{O}_{F,\ell})$ along its rational points in the special fiber over the residue field \mathbb{F}_ℓ of $\mathcal{O}_{F,\ell}$. The generic fiber of $\widehat{\mathcal{H}}_\ell$ is a rigid analytic space whose \mathbb{C}_ℓ -points are $\mathcal{H}_\ell := \mathbb{P}^1(\mathbb{C}_\ell) - \mathbb{P}^1(F_\ell)$. For more details, see [7, Chapitre I]. Finally, let Frob_ℓ be the Frobenius automorphism of $\text{Gal}(F_\ell^{\text{unr}}/F_\ell)$.

THEOREM 4.1 (Čerednik-Drinfeld). — *There exists an isomorphism of formal schemes over $\text{Spec}(\mathcal{O}_{F,\ell})$:*

$$\widehat{\mathcal{X}}_\ell \simeq U^{(\ell)} \backslash (\widehat{\mathcal{H}}_\ell \widehat{\otimes}_{\mathcal{O}_{F,\ell}} \mathcal{O}_{F,\ell}^{\text{unr}} \times \widehat{B}^{(\ell)\times}) / B^\times,$$

where $b \in \mathcal{B}^\times$ acts on $\mathcal{O}_{F,\ell}^{\text{unr}}$ by $\text{Frob}_\ell^{-\text{val}_\ell(b)}$.

Proof. — This result can be obtained by combining Čerednik’s description [12] of \mathcal{X}_ℓ as moduli space for certain formal groups with the Drinfeld’s description [19] of \mathcal{H}_ℓ . The main references for the theorem in this form are [7], especially for the case $F = \mathbb{Q}$ and [53], [52] for the general case. \square

The Jordan-Livné description [32, Section 4] of $\widehat{\mathcal{X}}_\ell$ can be used to derive a more simple form of Theorem 4.1. Since $\widehat{\mathcal{H}}_\ell$ is connected, the set of connected components of $\widehat{\mathcal{X}}_\ell$ is given by $U^{(\ell)} \backslash \widehat{B}^{(\ell)\times} / B^\times$. Note that

$$U^{(\ell)} \backslash \widehat{B}^{(\ell)\times} / B^\times = U^{(\ell)} \text{GL}_2(F_\ell) \backslash \widehat{B}^\times / B^\times \simeq \widehat{n}_B(U^{(\ell)}) F_\ell \backslash \widehat{F}^\times / F_+,$$

where F_+ are the totally positive elements in F and the last isomorphism is induced by the adelization \widehat{n}_B of the norm map $n_B : B \rightarrow F$. Fix representatives g_1, \dots, g_h of the double coset space $U^{(\ell)} \backslash \widehat{B}^{(\ell)\times} / B^\times$ (where $g_1 = 1$) and define the following subgroups for each $j = 1, \dots, h$:

$$\widetilde{\Gamma}_{j,0,\ell} := g_j^{-1} (U^{(\ell)} \text{GL}_2(F_\ell)) g_j \cap B^\times; \quad \Gamma_{j,0,\ell} := \widetilde{\Gamma}_{j,0,\ell} / (\widetilde{\Gamma}_{j,0,\ell} \cap F^\times);$$

$$\widetilde{\Gamma}_{j,+,\ell} := (\widetilde{\Gamma}_{j,0,\ell})_e; \quad \Gamma_{j,+,\ell} := (\Gamma_{j,0,\ell})_e,$$

where the subscript e means elements of even ℓ -adic valuation. There is an isomorphism of formal schemes over $\text{Spec}(\mathcal{O}_{F,\ell})$:

$$\widehat{\mathcal{X}}_\ell \simeq \prod_{j=1}^h \widehat{\mathcal{H}}_\ell \widehat{\otimes}_{\mathcal{O}_{F,\ell}} \mathcal{O}_{F,\ell}^{\text{unr}} / \widetilde{\Gamma}_{j,0,\ell}$$

(see [32, Lemma 4.3]). Following [32, page 243], let w_ℓ be a representative in $\Gamma_{j,0,\ell}$ for the non-trivial class in the quotient $\Gamma_{j,0,\ell} / \Gamma_{j,+,\ell}$. Denote by F_{ℓ^2}

the unique quadratic unramified extension of F_ℓ and by \mathcal{O}_{F,ℓ^2} its ring of integers. Then there is an isomorphism of formal schemes over $\text{Spec}(\mathcal{O}_{F,\ell})$:

$$\widehat{\mathcal{X}}_\ell \simeq \left(\prod_{j=1}^h \widehat{\mathcal{H}}_\ell / \Gamma_{j,+,\ell} \right)^{\times}$$

where

$$\chi \in H^1(\text{Gal}(F_{\ell^2}/F_\ell), \text{Aut}(\widehat{\mathcal{H}}_\ell \otimes \mathcal{O}_{F,\ell^2} / \Gamma_{j,+,\ell}))$$

is the cohomology class defined by $\tau \mapsto w_\ell \times \text{Id}$ (see [32, Theorem 4.3']). Denote by $\widehat{\mathcal{X}}_{\ell^2}$ the base-change: $\widehat{\mathcal{X}}_{\ell^2} := \widehat{\mathcal{X}}_\ell \otimes_{\mathcal{O}_{F,\ell}} \mathcal{O}_{F,\ell^2}$ and by \mathcal{X}_{ℓ^2} its generic fiber. The above discussion imply that there is an isomorphism $\widehat{\mathcal{X}}_{\ell^2} \simeq \prod_{j=1}^h \widehat{\mathcal{H}}_\ell / \Gamma_{j,+,\ell}$ of formal schemes over $\text{Spec}(\mathcal{O}_{F,\ell^2})$. In particular, there is an isomorphism of rigid analytic spaces over $\text{Spec}(\mathcal{O}_{F,\ell^2})$:

$$\mathcal{X}_{\ell^2}(\mathbb{C}_\ell) \simeq \prod_{j=1}^h \mathcal{H}_\ell / \Gamma_{j,+,\ell}.$$

It follows that \mathcal{X}_{ℓ^2} is a disjoint union of admissible curves in the sense of [32].

4.3. The dual graph of \mathcal{X}_{ℓ^2}

We keep the same notations as in Section 4.2. Let $\overline{\mathcal{G}}_\ell$ (respectively, \mathcal{G}_ℓ) be the dual graph of \mathcal{X}_ℓ (respectively, of \mathcal{X}_{ℓ^2}). Denote by $\mathcal{V}(\mathcal{G}_\ell)$ the set of vertices of \mathcal{G}_ℓ and by $\mathcal{E}(\mathcal{G}_\ell)$ the set of (unoriented) edges of \mathcal{G}_ℓ . Let Frob_ℓ be the automorphism of $\overline{\mathcal{G}}_\ell$ induced by the action of the Frobenius endomorphism on \mathcal{X}_ℓ . Denote by \mathcal{T}_ℓ the Bruhat-Tits tree of $\text{PGL}_2(F_\ell)$ with its natural action of $\text{GL}_2(F_\ell)$ by isometries, by $\mathcal{V}(\mathcal{T}_\ell)$ the set of its vertices, by $\mathcal{E}(\mathcal{T}_\ell)$ the set of its unoriented edges and by $\overrightarrow{\mathcal{E}}(\mathcal{T}_\ell)$ the set of its oriented edges. There is an isomorphism of graphs: $\overline{\mathcal{G}}_\ell \simeq \prod_{j=1}^h \mathcal{T}_\ell / \Gamma_{j,+,\ell}$. The action of Frob_ℓ on $\overline{\mathcal{G}}_\ell$ corresponds under this isomorphism to the action of w_ℓ (see [32, Section 3]). Then: $\mathcal{G}_\ell \simeq \prod_{j=1}^h \mathcal{T}_\ell / \Gamma_{j,+,\ell}$ and the action of Frob_ℓ on \mathcal{G}_ℓ corresponds to the identity map (see [32, Proposition 3.7]). Hence:

$$\mathcal{V}(\mathcal{G}_\ell) \simeq \prod_{j=1}^h \mathcal{V}(\mathcal{T}_\ell) / \Gamma_{j,+,\ell} \quad \text{and} \quad \mathcal{E}(\mathcal{G}_\ell) \simeq \prod_{j=1}^h \mathcal{E}(\mathcal{T}_\ell) / \Gamma_{j,+,\ell}.$$

For each $j = 1, \dots, h$, define the graph: $\mathcal{G}_j := \mathcal{T}_\ell / \Gamma_{j,+,\ell}$; denote by $\mathcal{V}(\mathcal{G}_j)$ and $\mathcal{E}(\mathcal{G}_j)$ the set, respectively, of its vertices and of its (unoriented) edges. Then: $\mathcal{G}_\ell \simeq \prod_{j=1}^h \mathcal{G}_j$, $\mathcal{V}(\mathcal{G}_\ell) = \prod_{j=1}^h \mathcal{V}(\mathcal{G}_j)$ and $\mathcal{E}(\mathcal{G}_\ell) = \prod_{j=1}^h \mathcal{E}(\mathcal{G}_j)$. Define

an *orientation* in each \mathcal{G}_j as follows. Let v_0 be the vertex of \mathcal{T}_ℓ corresponding to the maximal order $M_2(\mathcal{O}_\ell)$. A vertex $v \in \mathcal{V}(\mathcal{T}_\ell)$ is defined to be even or odd accordingly to the parity of its distance from v_0 . (By definition, the distance between two vertices v and w is n if and only if $v \cap w_0$ corresponds to an Eichler order of level n .) Since the determinant of each of the elements in $\Gamma_{j,+,\ell}$ is an even power of ℓ , the action of $\Gamma_{j,+,\ell}$ on \mathcal{T}_ℓ preserves the parity of the vertices; hence there is a well-defined notion of odd and even vertices in the quotient graph $\mathcal{T}_\ell/\Gamma_{j,+,\ell}$. Using this notion, define an orientation on \mathcal{G}_j , that is, a pair of maps $s : \mathcal{E}(\mathcal{G}_j) \rightarrow \mathcal{V}(\mathcal{G}_j)$ and $t : \mathcal{E}(\mathcal{G}_j) \rightarrow \mathcal{V}(\mathcal{G}_j)$ so that for any $e \in \mathcal{E}(\mathcal{G}_j)$, $e = s(e) \cap t(e)$, by requiring that $s(e)$ (respectively, $t(e)$) is the even (respectively, odd) vertex in e .

LEMMA 4.2. — $\mathcal{V}(\mathcal{G}_\ell) \simeq (U \backslash \widehat{B}^\times / B^\times) \times \{0, 1\}$ and $\mathcal{E}(\mathcal{G}_\ell) \simeq U_\ell \backslash \widehat{B}^\times / B^\times$.

Proof. — As in [3, Lemma 2.2], note that for each $j = 1, \dots, h$ there are isomorphisms: $\mathcal{V}(\mathcal{G}_j) \simeq (\text{PGL}_2(\mathcal{O}_\ell) \backslash \text{PGL}_2(F_\ell) / \Gamma_{j,0,\ell}) \times \{0, 1\}$ and $\mathcal{E}(\mathcal{G}_j) \simeq \Gamma_0(\ell) \backslash \text{PGL}_2(F_\ell) / \Gamma_{j,0,\ell}$, where $\Gamma_0(\ell)$ is the subgroup of matrices in $\text{PGL}_2(\mathcal{O}_\ell)$ congruent modulo ℓ to upper triangular matrices. The result is then a consequence of the strong approximation theorem (see Section 3.2). For more details, see [38, page 53]. □

Coboundary maps

Form the group rings $\mathbb{Z}[\mathcal{E}(\mathcal{G}_j)]$ and $\mathbb{Z}[\mathcal{V}(\mathcal{G}_j)]$ and denote by $\mathbb{Z}^0[\mathcal{E}(\mathcal{G}_j)]$ and by $\mathbb{Z}^0[\mathcal{V}(\mathcal{G}_j)]$ the degree zero elements. Define a coboundary map $\partial_{j,*} : \mathbb{Z}[\mathcal{E}(\mathcal{G}_j)] \rightarrow \mathbb{Z}^0[\mathcal{V}(\mathcal{G}_j)]$ to be the extension by \mathbb{Z} -linearity of the rule: for any $e \in \mathcal{E}(\mathcal{G}_j)$, $\partial_{j,*}(e) := t(s) - s(e)$. Denote by $\delta_{j,*}$ the restriction of $\partial_{j,*}$ to degree zero divisors: $\delta_{j,*} : \mathbb{Z}^0[\mathcal{E}(\mathcal{G}_j)] \rightarrow \mathbb{Z}^0[\mathcal{V}(\mathcal{G}_j)]$. For each $j = 1, \dots, h$, the map $\partial_{j,*}$ is surjective and its kernel is contained in $\mathbb{Z}^0[\mathcal{E}(\mathcal{G}_j)]$. It follows that $\text{Ker}(\partial_{j,*}) = \text{Ker}(\delta_{j,*})$ and that the following diagram is commutative, where the horizontal sequences are exact and the vertical arrows are inclusions:

$$\begin{array}{ccccccc}
 0 & \rightarrow & \text{Ker}(\partial_{j,*}) & \rightarrow & \mathbb{Z}[\mathcal{E}(\mathcal{G}_j)] & \xrightarrow{\partial_{j,*}} & \mathbb{Z}^0[\mathcal{V}(\mathcal{G}_j)] & \rightarrow & 0 \\
 (4.2) & & \parallel & & \uparrow & & \uparrow & & \\
 0 & \rightarrow & \text{Ker}(\partial_{j,*}) & \rightarrow & \mathbb{Z}^0[\mathcal{E}(\mathcal{G}_j)] & \xrightarrow{\delta_{j,*}} & \text{Im}(\delta_{j,*}) & \rightarrow & 0.
 \end{array}$$

Since $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)] = \prod_{j=1}^h \mathbb{Z}[\mathcal{E}(\mathcal{G}_j)]$ and $\mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)] = \prod_{j=1}^h \mathbb{Z}[\mathcal{V}(\mathcal{G}_j)]$, collecting the $\partial_{j,*}$ yields a map: $\partial_* : \mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)] \rightarrow \mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]$. By diagram (4.2), the image of ∂_* is $\prod_{j=1}^h \mathbb{Z}^0[\mathcal{V}(\mathcal{G}_j)]$ and, if δ_* denotes the restriction of ∂_* to $\prod_{j=1}^h \mathbb{Z}^0[\mathcal{E}(\mathcal{G}_j)]$, there is the following commutative diagram, where all

horizontal sequences are exact and the vertical arrows are inclusions:

$$\begin{array}{ccccccc}
 0 \rightarrow & \prod_{j=1}^h \text{Ker}(\partial_{j,*}) & \rightarrow & \mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)] & \xrightarrow{\partial_*} & \prod_{j=1}^h \mathbb{Z}^0[\mathcal{V}(\mathcal{G}_j)] & \rightarrow 0 \\
 & \parallel & & \uparrow & & \uparrow & \\
 0 \rightarrow & \prod_{j=1}^h \text{Ker}(\partial_{j,*}) & \rightarrow & \prod_{j=1}^h \mathbb{Z}^0[\mathcal{E}(\mathcal{G}_j)] & \xrightarrow{\delta_*} & \text{Im}(\delta_*) & \rightarrow 0.
 \end{array}$$

(4.3)

By Lemma 4.2, the orientation chosen induces two maps:

$$\alpha_*, \beta_* : \mathbb{Z}[U_\ell \backslash \widehat{B}^\times / B^\times] \rightarrow \mathbb{Z}[U \backslash \widehat{B}^\times / B^\times] \times \{0, 1\}$$

defined by the rules: $\alpha_*(e) := (s(e), 0)$ and $\beta_*(e) := (t(e), 1)$; hence there is a map:

$$(4.4) \quad \mathbb{Z}[U_\ell \backslash \widehat{B}^\times / B^\times] \xrightarrow{\alpha_* \times \beta_*} \mathbb{Z}[U \backslash \widehat{B}^\times / B^\times] \times \mathbb{Z}[U \backslash \widehat{B}^\times / B^\times].$$

Note that, under the above identifications, $\partial_* = \beta_* - \alpha_*$. On the image of the map (4.4) there is an action of both $T_\ell \in \mathbb{T}_{\mathfrak{c}^+}^B$ and $U_\ell \in \mathbb{T}_{\mathfrak{c}^+\ell}^B$. A simple computation shows that:

$$(4.5) \quad (\beta_* \times \alpha_*)(U_\ell(e)) = (T_\ell(\beta_*(e)) - \alpha_*(e), |\ell|\beta_*(e)).$$

4.4. The group of connected components

The map ω_ℓ

We keep the same notations as in Sections 4.2, 4.3. Recall the notation \mathbb{T}_U introduced in Section 4.1. Fix a prime ideal $\ell \mid \mathfrak{c}^-$ such that $T_\ell \in \mathbb{T}_U$. Recall that \mathcal{X}_{ℓ^2} is isomorphic over \mathcal{O}_{F,ℓ^2} to a disjoint union of admissible curves: $\mathcal{X}_{\ell^2} = \coprod_{j=1}^h \mathcal{X}_j$. For each $j = 1, \dots, h$, denote by \mathcal{J}_j the Néron model over \mathcal{O}_{F,ℓ^2} of \mathcal{X}_j , by Φ_j its group of connected components and by \mathbb{X}_j the character group of its maximal torus. Then define the analogous objects for \mathcal{X}_{ℓ^2} : $\mathcal{J}_\ell = \prod_{j=1}^h \mathcal{J}_j$, $\Phi_\ell := \prod_{j=1}^h \Phi_j$, $\mathbb{X}_\ell := \prod_{j=1}^h \mathbb{X}_j$ (note that these objects are defined over \mathcal{O}_{F,ℓ^2} and not over $\mathcal{O}_{F,\ell}$). After fixing orientations s and t as in Section 4.3, the diagram (4.3) corresponds to the following:

$$\begin{array}{ccccccc}
 0 \longrightarrow & \mathbb{X}_\ell & \xrightarrow{i} & \mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)] & \xrightarrow{\partial_*} & \prod_{j=1}^h \mathbb{Z}^0[\mathcal{V}(\mathcal{G}_j)] & \rightarrow 0 \\
 & \parallel & & \uparrow & & \uparrow & \\
 0 \longrightarrow & \mathbb{X}_\ell & \xrightarrow{i} & \prod_{j=1}^h \mathbb{Z}^0[\mathcal{E}(\mathcal{G}_j)] & \xrightarrow{\delta_*} & \text{Im}(\delta_*) & \rightarrow 0.
 \end{array}$$

Moreover, Grothendieck’s description [26, Theorems 11.5 and 12.5] of the group of connected components of an admissible curve yields the following exact sequence: $0 \rightarrow \mathbb{X}_\ell \xrightarrow{j} \mathbb{X}_\ell^\vee \xrightarrow{\tau_\ell} \Phi_\ell \rightarrow 0$.

For any edge $e \in \mathcal{E}(\mathcal{G}_\ell)$, let $g = g(e)$ be the element associated to e by the isomorphism of Lemma 4.2. The integer $w(g)$ defined in Section 3.2 is the weight of the singular point e . Use the same argument as in [4, Corollary 5.12] to define a natural Hecke-equivariant non trivial map

$$\omega_\ell : \prod_{j=1}^h \mathbb{Z}^0[\mathcal{V}(\mathcal{G}_j)] \rightarrow \Phi_\ell.$$

Geometric pairs

DEFINITION 4.3. — *Keep the same notations as in Section 3.2. The pair (F, U) is said to be geometric if at least one of the following conditions is verified:*

1. *Either $[F : \mathbb{Q}]$ is odd or $[F : \mathbb{Q}]$ is even and $\mathfrak{c}^-/\ell \neq \mathcal{O}_F$.*
2. *(F, U) is Eisenstein.*

PROPOSITION 4.4. — *The restriction of ω_ℓ to $\text{Im}(\delta_*)$ induces a \mathbb{T}_U -equivariant map*

$$\bar{\omega}_\ell : \text{Im}(\delta_*)/(\mathbb{U}_\ell^2 - 1) \rightarrow \Phi_\ell.$$

If (F, U) (respectively, (F, U_ℓ)) is geometric, the kernel (respectively, the cokernel) of $\bar{\omega}_\ell$ is Eisenstein.

Proof. — Define the pairing $\langle\langle, \rangle\rangle : \mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)] \times \mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)] \rightarrow \mathbb{Z}$ as follows: for any pair v, v' of vertices, put $\langle\langle v, v' \rangle\rangle := w(g)\delta_{v,v'}$, where $g = g(v)$ is the element in $U \setminus \widehat{B}^\times / B^\times$ associated to the vertex v by strong approximation and $w(g)$ is its weight. Consider the maps: $j_0 : \mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)] \hookrightarrow \mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^\vee$ and $j_1 : \text{Im}(\delta_*) \hookrightarrow \text{Im}(\delta_*)^\vee$ induced, respectively, by \langle, \rangle , and the natural restriction of $\langle\langle, \rangle\rangle$ to $\text{Im}(\delta_*)$. Set:

$$\Phi_0 := \frac{\prod_{j=1}^h \mathbb{Z}^0[\mathcal{E}(\mathcal{G}_j)]^\vee}{j_0(\prod_{j=1}^h \mathbb{Z}^0[\mathcal{E}(\mathcal{G}_j)])}, \quad \text{and} \quad \Phi_1 := \frac{\text{Im}(\delta_*)^\vee}{j_1(\text{Im}(\delta_*))}.$$

Equation (4.5) can be used as in [4, Proposition 5.13] to obtain the following commutative diagram:

$$\begin{array}{ccccccc}
 & & & 0 & & \text{Ker}(\gamma) & \\
 & & & \downarrow & & \downarrow & \\
 0 \longrightarrow & \text{Im}(\delta_*) & \xrightarrow{j_1} & \text{Im}(\delta_*)^\vee & \longrightarrow & \Phi_1 & \longrightarrow 0 \\
 & \downarrow \sigma & & \downarrow \delta_*^\vee & & \downarrow \gamma & \\
 0 \longrightarrow & \text{Im}(\delta_*) & \xrightarrow{j'_0} & \frac{\prod_{j=1}^h \mathbb{Z}^0[\mathcal{E}(\mathcal{G}_j)]^\vee}{j_0(i(\mathbb{X}_\ell))} & \longrightarrow & \Phi_0 & \longrightarrow 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & \text{Im}(\delta_*)/(\mathbb{U}_\ell^2 - 1) & \longrightarrow & \Phi_\ell & & \text{Coker}(\gamma) &
 \end{array}$$

Here $\sigma(x, y) = (|\ell| + 1)x + T_\ell(y), T_\ell(x) + (|\ell| + 1)y$. The first part of the proposition follows. For the second part, consider two cases, accordingly with the conditions satisfied by the geometric pair (F, U) (respectively, (F, U_ℓ)) in Definition 4.3.

Case I : The pair (F, U) (respectively, (F, U_ℓ)) satisfies 4.3 in Definition 4.3. In this case, Φ_1 (respectively, Φ_0) is Eisenstein by [38, Proposition 5].

Case II : The pair (F, U) (respectively, (F, U_ℓ)) satisfies 4.3 in Definition 4.3. In this case Φ_1 (respectively, Φ_0) is Eisenstein by Corollary 3.6 (use Lemma 4.2 to switch to quaternion algebras and note that the operators η_q of Proposition 1.3 restricts to Φ_0 and Φ_1).

The result follows from the snake lemma. □

Remark 4.5. — It is expected that the kernel and cokernel of $\bar{\omega}_\ell$ are always Eisenstein. Unfortunately, at the present there is no such a full result in the literature and the generalizations of the techniques from Case I and Case II above seem not obvious. For simplicity, assume that $\mathcal{U} = \widehat{\mathcal{R}}^\times$. If the geometric pair (F, U) is in the Case I above, then it is possible to choose a divisor $\ell_1 \mid \mathfrak{c}^-/\ell$. The groups Φ_0 and Φ_1 appearing in the proof of Proposition 4.4 can be interpreted as component groups of the special fiber over ℓ_1 of the Shimura curves, respectively, $X_{\mathfrak{c}^+ \ell_1 \ell, \mathfrak{c}^-/\ell_1 \ell}$ and $X_{\mathfrak{c}^+ \ell_1, \mathfrak{c}^-/\ell_1 \ell}$. The Eisenstein property comes in this case from this geometric approach, using results of [10]. For more details on this interpretation, see also [4, Section 5.6]. If there is not any ℓ_1 dividing \mathfrak{c}^-/ℓ , this approach does not seem to work. On the other hand, if F is not Eisenstein, no generalization of Proposition 3.2 is known, since its proof relies crucially on deep properties of certain cyclic extensions $F(\mu_k)/F$.

The reduction map to Φ_ℓ

Denote by $J := J_{c^+, c^-}$ the jacobian of the Shimura curve $X := X_{c^+, c^-}$ (see Section 4.1). Denote as in Section 4.2 by \mathcal{X}_{ℓ^2} the special fiber over \mathcal{O}_{F, ℓ^2} of the integral model \mathcal{X} of X . Let $\text{Div}(X)$ be the group of divisors of $X(\overline{F})$ with \mathbb{Z} coefficients and $\text{Div}^0(X)$ be the subgroup of $\text{Div}(X)$ consisting of divisors which have degree zero on each connected component of X . Suppose that $D = \sum n_P P \in \text{Div}^0(X)$ satisfies the following assumptions:

1. Each point $P \in \text{Supp}(D)$ is defined over F_{ℓ^2} ;
2. The image of each $P \in \text{Supp}(D)$ by the reduction map $r_\ell : \mathcal{X}_{\ell^2} \rightarrow \mathcal{E}(\mathcal{G}_\ell) \cup \mathcal{V}(\mathcal{G}_\ell)$ is an element $v_P \in \mathcal{V}(\mathcal{G}_\ell)$.

Under these assumptions, the reduction map r_ℓ applied to D provides an element $r_\ell(D) = \sum n_P r_\ell(P) \in \prod_{j=1}^h \mathbb{Z}^0[\mathcal{V}(\mathcal{G}_\ell)]$. Denote by ∂_ℓ the specialization map $\partial_\ell : J(F_{\ell^2}) \rightarrow \Phi_\ell$. The next proposition gives a relation between ω_ℓ , ∂_ℓ and r_ℓ .

PROPOSITION 4.6. — *Let $D \in \text{Div}^0(X)$ be a divisor satisfying the previous conditions and let $[D]$ be the class in J associated to D . Then in Φ_ℓ :*

$$\partial_\ell([D]) = \omega_\ell(r_\ell(D)).$$

Proof. — This result follows from Edixhoven’s description of the map ∂_ℓ which can be found in [2, Appendix, Section 2]. See also [4, Proposition 5.14]. □

4.5. Raising the level

Notations and assumptions as in Section 1 for the integral ideals \mathfrak{n}^+ and \mathfrak{n}^- , the rational prime p , the positive integer n and the eigenform ϕ with rational coefficients associated to the modular elliptic curve E . In particular, suppose that the Assumptions 1.5 and 1.6 are verified. Fix an admissible prime ℓ . Let B be the quaternion algebra over F of discriminant \mathfrak{n}^- which is ramified at all the archimedean places of F and choose Eichler orders R and R_ℓ of level, respectively, \mathfrak{n}^+ and $\mathfrak{n}^+ \ell$. Denote by \mathbb{T} the Hecke algebra $\mathbb{T}_{\mathfrak{n}^+}^B$, which, by the Jacquet-Langlands correspondence (Theorem 3.7) is isomorphic to $\mathbb{T}_{\mathfrak{n}^+, \mathfrak{n}^-}^{\text{new}}$, and by \mathbb{T}_ℓ the Hecke algebra $\mathbb{T}_{\mathfrak{n}^+, \mathfrak{n}^- \ell}^{\text{new}}$. Denote by T_ℓ and U_ℓ (respectively, by T'_ℓ and U'_ℓ) the Hecke operators in \mathbb{T} (respectively, in \mathbb{T}_ℓ). There is a morphism

$$f : \mathbb{T} \rightarrow \mathbb{Z}/p\mathbb{Z}$$

which, using the notations of Section 1.1, coincides with $\bar{\theta}_\phi$. Denote by \mathfrak{m}_f the kernel of f (it is a maximal ideal).

DEFINITION 4.7. — ϕ is said to be p -isolated if the completion at the maximal ideal \mathfrak{m}_f of $\mathbb{Z}[\widehat{R}^\times \setminus \widehat{B}^\times / B^\times]$ is isomorphic to \mathbb{Z}_p .

By the Jacquet-Langlands correspondence (Theorem 3.7), ϕ can be associated to a modular form in $\mathcal{S}_2^B(\mathfrak{n}^+; \mathbb{Z})$, hence it is clear that the completion of $\mathbb{Z}[\widehat{R}^\times \setminus \widehat{B}^\times / B^\times]$ at \mathfrak{m}_f has \mathbb{Z}_p -rank at least one. Since the maximal ideals in the support of $\mathcal{L}(\mathfrak{c}^+; \mathbb{Z})^{\text{triv}}$ are Eisenstein (see [28, Section 5]), the condition in the above definition simply asserts that there are no non-trivial congruences between ϕ and other forms of level \mathfrak{n} which are new at \mathfrak{n}^- . If ϕ is p -isolated, then the dimension of $\mathbb{Z}[\widehat{R}^\times \setminus \widehat{B}^\times / B^\times]^2 / \mathfrak{m}_f$ as $\mathbb{Z}/p\mathbb{Z}$ -vector space is two and, by the same argument as in [4, Theorem 5.15], it follows that the dimension of $\mathbb{Z}[\widehat{R}^\times \setminus \widehat{B}^\times / B^\times]^2 / \langle \mathfrak{m}_f, U_\ell^2 - 1 \rangle$ is one. Hence, the dimension of $\text{Im}(\delta_*) / \langle \mathfrak{m}_f, U_\ell^2 - 1 \rangle$ is always at most one. Since $(T_\ell - (|\ell| + 1))f$ is not trivial in $\mathbb{Z}^0[\widehat{R}^\times \setminus \widehat{B}^\times / B^\times]$, it follows that

$$\text{Im}(\delta_*) / \langle \mathfrak{m}_f, U_\ell^2 - 1 \rangle \simeq \mathbb{Z}/p\mathbb{Z}.$$

Congruences between modular forms

Define $\mathcal{S}_2^{\text{old}}(\mathfrak{n}, \ell)$ to be the ℓ -old subspace of $\mathcal{S}_2(\mathfrak{n}\ell)$ (that is, the orthogonal complement of $\mathcal{S}_2^{\text{new}}(\mathfrak{n}, \ell)$ with respect to the Petterson scalar product) and denote by

$$\begin{aligned} \mathcal{S}_2(\mathfrak{n}) \times \mathcal{S}_2(\mathfrak{n}) &\rightarrow \mathcal{S}_2^{\text{old}}(\mathfrak{n}, \ell) \\ (\phi_1, \phi_2) &\mapsto \phi_1 + \phi_2|_\ell \end{aligned}$$

the maps defining it (for more details, see [42]). Following Ribet [40], define a modular form $\psi \in \mathcal{S}_2^{\text{old}}(\mathfrak{n}, \ell)$ by: $\psi := \phi - \epsilon|\ell|\phi|_\ell$, where $p \mid \epsilon f(T_\ell) - (|\ell| + 1)$.

Remark 4.8. — $\psi \notin \mathcal{S}_2^{\text{new}}(\mathfrak{n}, \ell)$. The theory of congruences between modular forms will produce in this situation a form in $\mathcal{S}_2^{\text{new}}(\mathfrak{n}, \ell)$ with the same eigenvalues as ψ modulo p .

Using Equation (4.5) it is easy to show that ψ is an eigenform for the Hecke algebra $\mathbb{T}_{\mathfrak{n}\ell}$ and:

- (i) For $\mathfrak{q} \nmid \mathfrak{n}\ell$, $T'_\mathfrak{q}(\psi) = \theta_\phi(T_\mathfrak{q})\psi$;
- (ii) For $\mathfrak{q} \mid \mathfrak{n}$, $U'_\mathfrak{q}(\psi) = \theta_\phi(U_\mathfrak{q})\psi$;
- (iii) $U'_\ell(\psi) \equiv \epsilon\psi \pmod{p}$.

The following theorem collects various results concerning congruences between modular forms. Assume from now on that $p > 3$.

THEOREM 4.9 (Taylor, Ribet, Rajaei). — *There exists a surjective morphism*

$$f_\ell : \mathbb{T}_\ell \rightarrow \mathbb{Z}/p\mathbb{Z}$$

so that:

- (i) For $\mathfrak{q} \nmid \mathfrak{n}\ell$, $f_\ell(\mathbb{T}'_{\mathfrak{q}}) = f(\mathbb{T}_{\mathfrak{q}})$;
- (ii) For $\mathfrak{q} \mid \mathfrak{n}$, $f_\ell(\mathbb{U}'_{\mathfrak{q}}) = f(\mathbb{U}_{\mathfrak{q}})$;
- (iii) $f_\ell(\mathbb{U}'_\ell) = \epsilon$.

Proof. — If $\mathfrak{n}^- = \mathcal{O}_F$, this is the main result of [45, Theorem 1]. When $F = \mathbb{Q}$, see [39, Section 7]. This argument has been extended to Hilbert modular forms when $\mathfrak{n}^- \neq \mathcal{O}_F$ by [38, Corollary 4]. The same argument applies when the pairs (F, \widehat{R}^\times) and $(F, \widehat{R}_\ell^\times)$ are both geometric (note that this includes the case of $\mathfrak{n}^- \neq \mathcal{O}_F$). Here a short sketch of the proof follows. Denote by Φ_ℓ the group of connected components attached to the Shimura curve $\mathcal{X}_{\mathfrak{n}^+, \mathfrak{n}^- \ell}$. The action of $\mathbb{T}_{\mathfrak{n}\ell}$ on $\text{Im}(\delta_*)/\langle \mathfrak{m}_f, \mathbb{U}_\ell^2 - 1 \rangle$ is via a surjective homomorphism $f'_\ell : \mathbb{T}_{\mathfrak{n}^+, \mathfrak{n}^-}^{\text{new}} \rightarrow \mathbb{Z}/p\mathbb{Z}$. Since in this case the kernel and the cokernel of $\overline{\omega}_\ell$ are Eisenstein (see Proposition 4.4), there is an isomorphism (induced by $\overline{\omega}_\ell$):

$$\text{Im}(\delta_*)/\langle \mathfrak{m}_f, \mathbb{U}_\ell^2 - 1 \rangle \simeq \Phi_\ell/\langle \mathfrak{m}_f, \mathbb{U}_\ell^2 - 1 \rangle \simeq \Phi_\ell/\mathfrak{m}_{f'_\ell}.$$

The action of $\mathbb{T}_{\mathfrak{n}\ell}$ is via the ℓ -new part. It follows that f'_ℓ factors through \mathbb{T}_ℓ giving the sought for character $f_\ell : \mathbb{T}_{\mathfrak{n}^+, \mathfrak{n}^- \ell}^{\text{new}} \rightarrow \mathbb{Z}/p\mathbb{Z}$ and that there is an isomorphism:

$$(4.6) \quad \text{Im}(\delta_*)/\langle \mathfrak{m}_f, \mathbb{U}_\ell^2 - 1 \rangle \simeq \Phi_\ell/\mathfrak{m}_{f_\ell}.$$

□

Quotients of Φ_ℓ

Assume from now on that ϕ is p -isolated. Let $X := X_{\mathfrak{n}^+, \mathfrak{n}^- \ell} \rightarrow \text{Spec}(F)$ be the Shimura curve of level \mathfrak{n}^+ attached to the quaternion algebra \mathcal{B} which is ramified at the primes dividing $\mathfrak{n}^- \ell$ and is split at exactly one of the archimedean places of F . Denote by \mathcal{X} its integral model, by \mathcal{X}_{ℓ^2} the special fiber over K_ℓ , by J_ℓ its jacobian variety and by Φ_ℓ its group of connected components.

PROPOSITION 4.10. — *If the pairs (F, \widehat{R}^\times) and $(F, \widehat{R}_\ell^\times)$ are both geometric then*

$$\Phi_\ell/\mathfrak{m}_{f_\ell} \simeq \mathbb{Z}/p\mathbb{Z}.$$

Proof. — Since ϕ is p -isolated, this result is an immediate consequence of equation (4.6) in the proof of Theorem 4.9. \square

PROPOSITION 4.11. — *If $\mathfrak{n}^- = \mathcal{O}_F$ and $[F : \mathbb{Q}]$ is even, then there is a component*

$$\mathcal{C}_\ell \simeq \mathbb{Z}/p\mathbb{Z} \hookrightarrow \Phi_\ell/\mathfrak{m}_{f_\ell}$$

and an isomorphism:

$$\bar{\omega}_\ell : \text{Im}(\delta_*)/\langle \mathfrak{m}_f, U_\ell^2 - 1 \rangle \longrightarrow \mathcal{C}_\ell.$$

Proof. — For any prime ideal $\mathfrak{q}_0 \nmid \mathfrak{n}^+ \mathfrak{n}^- \ell$ denote by $\mathcal{U}(\mathfrak{q}_0)$ the subgroup of $\widehat{\mathcal{B}}^\times$: $\mathcal{U}(\mathfrak{q}_0) := \mathcal{U}^{(\mathfrak{q}_0)}\Gamma_1(\mathfrak{q}_0)$, where $\Gamma_1(\mathfrak{q}_0)$ is the subgroup of $A \in \text{GL}_2(\mathcal{O}_{F,\mathfrak{q}_0})$ so that $A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{\mathfrak{q}_0}$. Denote by $X(\mathfrak{q}_0) \rightarrow \text{Spec}(F)$ the Shimura curve of level $\mathcal{U}(\mathfrak{q}_0)$ and let $\mathcal{X}(\mathfrak{q}_0) \rightarrow \text{Spec}(\mathcal{O}_F)$ be its integral model (see [53, Section 1]). Choose \mathfrak{q}_0 so that:

- (i) There are no congruences between forms of level \mathfrak{n} and forms of level $\mathcal{U}(\mathfrak{q}_0)$ which are new at \mathfrak{q}_0 .
- (ii) The integral model $\mathcal{X}(\mathfrak{q}_0)$ is regular.

This is possible by [29, Section 12] (see also [30, Section 6]). Note that ϕ , viewed as a modular form of level $\mathcal{U}(\mathfrak{q}_0)$, is a $(\text{mod } p)$ eigenform for $\mathbb{T}^{(\mathfrak{q}_0)}$ with eigenvalues in $\mathbb{Z}/p\mathbb{Z}$; denote by $f^{(\mathfrak{q}_0)} : \mathbb{T}^{(\mathfrak{q}_0)} \rightarrow \mathbb{Z}/p\mathbb{Z}$ the associated morphism and by $\mathfrak{m}_f^{(\mathfrak{q}_0)}$ its kernel. Let $\mathcal{G}_\ell(\mathfrak{q}_0) = \coprod_{j=1}^h \mathcal{G}_j(\mathfrak{q}_0)$ be the dual graph of the special fiber at ℓ of $\mathcal{X}(\mathfrak{q}_0)$. Denote by $\mathcal{V}(\mathcal{G}_\ell(\mathfrak{q}_0)) = \coprod_{j=1}^h \mathcal{V}_j(\mathfrak{q}_0)$ and $\mathcal{E}(\mathcal{G}_\ell(\mathfrak{q}_0)) = \coprod_{j=1}^h \mathcal{E}_j(\mathfrak{q}_0)$, respectively, the vertexes and the edges of $\mathcal{G}_\ell(\mathfrak{q}_0)$. Denote by $\delta_*(\mathfrak{q}_0)$ the map in diagram (4.3):

$$\prod_{j=1}^h \mathbb{Z}^0[\mathcal{E}(\mathcal{G}_j(\mathfrak{q}_0))] \xrightarrow{\delta_*(\mathfrak{q}_0)} \prod_{j=1}^h \mathbb{Z}^0[\mathcal{V}(\mathcal{G}_j(\mathfrak{q}_0))]$$

and by $\bar{\omega}_\ell(\mathfrak{q}_0) : \text{Im}(\delta_*(\mathfrak{q}_0)) \rightarrow \Phi_\ell(\mathfrak{q}_0)$ the resulting map, where $\Phi_\ell(\mathfrak{q}_0)$ is the group of connected components of the Jacobian of $\mathcal{X}(\mathfrak{q}_0)$ at ℓ . Since $\mathcal{X}(\mathfrak{q}_0)$ is regular, the weights of the singular points are all equal to one, so by Proposition 4.4 there is an isomorphism:

$$(4.7) \quad \text{Im}(\delta_*(\mathfrak{q}_0))/\langle \mathfrak{m}_f^{(\mathfrak{q}_0)}, U_\ell^2 - 1 \rangle \longrightarrow \Phi_\ell(\mathfrak{q}_0)/\mathfrak{m}_{f_\ell}^{(\mathfrak{q}_0)}.$$

There are maps: $\text{Im}(\delta_*) \times \text{Im}(\delta_*) \rightarrow \text{Im}(\delta_*(\mathfrak{q}_0))$ and $\Phi_\ell \times \Phi_\ell \rightarrow \Phi_\ell(\mathfrak{q}_0)$; denote by $\text{Im}(\delta_*(\mathfrak{q}_0))^{\text{old}}$ and $\Phi_\ell(\mathfrak{q}_0)^{\text{old}}$ the respective images. Since there are no congruences between forms of level \mathfrak{n} and forms of level $U_1(\mathfrak{q}_0)$ which are new at \mathfrak{q}_0 , there are isomorphisms:

$$\text{Im}(\delta_*(\mathfrak{q}_0))^{\text{old}}/\langle \mathfrak{m}_f^{(\mathfrak{q}_0)}, U_\ell^2 - 1 \rangle \simeq \text{Im}(\delta_*(\mathfrak{q}_0))/\langle \mathfrak{m}_f^{(\mathfrak{q}_0)}, U_\ell^2 - 1 \rangle$$

and $\Phi_\ell(\mathfrak{q}_0)^{\text{old}}/\mathfrak{m}_f^{(\mathfrak{q}_0)} \simeq \Phi_\ell(\mathfrak{q}_0)/\mathfrak{m}_f^{(\mathfrak{q}_0)}$. It follows that the map (4.7) yields an isomorphism:

$$\text{Im}(\delta_*)(\mathfrak{q}_0)^{\text{old}}/\langle \mathfrak{m}_f^{(\mathfrak{q}_0)}, U_\ell^2 - 1 \rangle \xrightarrow{\bar{\omega}_\ell(\mathfrak{q}_0)} \Phi_\ell(\mathfrak{q}_0)^{\text{old}}/\mathfrak{m}_f^{(\mathfrak{q}_0)}.$$

For brevity, set: $\tilde{\mathfrak{m}}_f^{(\mathfrak{q}_0)} := \langle \mathfrak{m}_f^{(\mathfrak{q}_0)}, U_\ell^2 - 1 \rangle$. The following diagram, whose vertical arrows are surjections:

$$\begin{array}{ccc} \text{Im}(\delta_*)/\tilde{\mathfrak{m}}_f^{(\mathfrak{q}_0)} \times \text{Im}(\delta_*)/\tilde{\mathfrak{m}}_f^{(\mathfrak{q}_0)} & \xrightarrow{\bar{\omega}_\ell^2} & \Phi_\ell/\mathfrak{m}_f^{(\mathfrak{q}_0)} \times \Phi_\ell/\mathfrak{m}_f^{(\mathfrak{q}_0)} \\ \downarrow \pi_1 & & \downarrow \pi_2 \\ \text{Im}(\delta_*(\mathfrak{q}_0))^{\text{old}}/\tilde{\mathfrak{m}}_f^{(\mathfrak{q}_0)} & \xrightarrow{\bar{\omega}_\ell(\mathfrak{q}_0)} & \Phi_\ell(\mathfrak{q}_0)^{\text{old}}/\mathfrak{m}_f^{(\mathfrak{q}_0)} \end{array}$$

implies the result. Indeed, choose $P \in \Phi_\ell(\mathfrak{q}_0)^{\text{old}}/\mathfrak{m}_f^{(\mathfrak{q}_0)}$ so that $P \neq 0$ (the image of ϕ gives such an element). Then there is $(Q_1, Q_2) \in \text{Im}(\delta_*)/\tilde{\mathfrak{m}}_f^{(\mathfrak{q}_0)} \times \text{Im}(\delta_*)/\tilde{\mathfrak{m}}_f^{(\mathfrak{q}_0)}$ so that $[\bar{\omega}_\ell(\mathfrak{q}_0) \circ \pi_1](Q_1, Q_2) = P$. Then also $[\pi_2 \circ \bar{\omega}_\ell^2](Q_1, Q_2) = P$; since $P \neq 0$ it follows that at least one of the Q_j 's, say Q_1 , is non-zero. The desired component can be defined to be $\mathcal{C}_\ell := \langle \bar{\omega}_\ell(Q_1) \rangle$. \square

DEFINITION 4.12. — Define the component $\mathcal{C}_\ell \simeq \mathbb{Z}/p\mathbb{Z} \subseteq \Phi_\ell/\mathfrak{m}_{f_\ell}$ to be $\Phi_\ell/\mathfrak{m}_{f_\ell}$ if the pairs (F, U) and (F, U_ℓ) are geometric (see Proposition 4.10) and the component in Proposition 4.11 otherwise.

Galois representations

Let J be the jacobian of X and denote by $T_p(J)$ the p -adic Tate module of J . Since J is a \mathbb{T}_ℓ -module, the quotient $T_p(J)/\mathfrak{m}_{f_\ell}$ is a $\mathbb{T}_\ell/\mathfrak{m}_{f_\ell} \simeq \mathbb{Z}/p\mathbb{Z}$ -vector space. Since \mathcal{X}_{ℓ^2} is a disjoint union of admissible curves, it is possible to use the Mumford-Kurihara theory of ℓ -adic uniformization (see [21]) and produce an exact sequence:

$$(4.8) \quad 0 \longrightarrow \mathbb{X}_\ell \xrightarrow{j} \mathbb{X}_\ell^\vee \otimes_{F_\ell^2} \bar{F}_{\ell^2} \longrightarrow J_\ell(K_\ell) \longrightarrow 0,$$

where j is the injection $\mathbb{X}_\ell \hookrightarrow \mathbb{X}_\ell^\vee$ induced by the monodromy pairing. By the same argument as [4, Section 5.6], taking cohomology and tensoring by $\mathbb{T}_\ell/\mathfrak{m}_{f_\ell}$ yields an exact sequence:

$$(4.9) \quad \Phi_\ell/\mathfrak{m}_{f_\ell} \rightarrow H^1(F_{\ell^2}, T_p(J)/\mathfrak{m}_{f_\ell}) \rightarrow H_{\text{unr}}^1(F_{\ell^2}, \mathbb{X}_\ell/\mathfrak{m}_{f_\ell}).$$

THEOREM 4.13. — There exist an integer $k \geq 1$ so that there is an isomorphism of $\text{Gal}(\bar{F}/F)$ -modules:

$$T_p(J)/\mathfrak{m}_{f_\ell} \simeq T_\phi[p]^k.$$

Moreover, there is a component $\mathcal{D}_\ell \simeq T_\phi[p]$ in the above decomposition of $T_p(J)/\mathfrak{m}_{f_\ell}$ so that the image of \mathcal{C}_ℓ via the map (4.9) followed by the projection to $H^1(K_\ell, \mathcal{D}_\ell)$ is not trivial and corresponds to $H^1_{\text{sing}}(K_\ell, T_\phi[p])$. Finally, if both the pairs (F, \widehat{R}^\times) and $(F, \widehat{R}_\ell^\times)$ are geometric, then $T_p(J)/\mathfrak{m}_{f_\ell} \simeq T_\phi[p]$ and $\Phi_\ell/\mathfrak{m}_{f_\ell} \simeq H^1_{\text{sing}}(K, T_\phi[p])$.

Proof. — By Assumption 1.5, the representation $\bar{\rho}_{\phi,p}$ is irreducible. Then [6] shows that $T_p(J)/\mathfrak{m}_{f_\ell}$ is semisimple over $\mathbb{Z}/p\mathbb{Z}[\text{Gal}(\overline{F}/F)]$. Combining the Eichler-Shimura relations, the Chebotarev density and the Brauer-Nesbitt theorems, it follows that $T_p(J)/\mathfrak{m}_{f_\ell}$ is isomorphic to $k \geq 1$ copies of $T_\phi[p]$.

By the same argument as [4, Lemma 5.16], any generator of \mathcal{C}_ℓ can be lifted to a non-zero element $t \in T_p(J)/\mathfrak{m}_{f_\ell}$. Define $\mathcal{D}_\ell \simeq T_\phi[p]$ to be a component on the above decomposition containing t . The exact sequence (4.9) shows that the natural projection of \mathcal{C}_ℓ in $H^1(K_\ell, \mathcal{D}_\ell)$ corresponds to the ramified cohomology $H^1_{\text{sing}}(K_\ell, T_\phi[p])$.

The last part of the proposition is a direct generalization of [4, Theorem 5.17], since in this case $\Phi_\ell/\mathfrak{m}_{f_\ell}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and so $k = 1$. \square

Quotients of J

COROLLARY 4.14. — *Let $D = \sum n_P P \in \text{Div}(X)$ be a divisor so that each $P \in \text{Supp}(D)$ satisfies the conditions of Section 4.4. Let $[D]$ be the class in J/\mathfrak{m}_{f_ℓ} associated with D by the inclusion (4.1). Then $\partial_\ell([D]) = \omega_\ell(r_\ell(D))$ in \mathcal{C}_ℓ .*

Proof. — This is clear from Proposition 4.6 and Theorem 4.13. \square

5. The construction of the Euler system

5.1. The Gross-Zhang formula for the special value of L -series

Let ϕ be an eigenform of level \mathfrak{n} . Recall from Section 1 the factorization $\mathfrak{n} = \mathfrak{n}^+ \mathfrak{n}^-$ associated with the imaginary extension K/F and assume that ϕ is new at the primes dividing \mathfrak{n}^- . The L -series $L_K(\phi, s)$ attached to ϕ and K can be continued to an entire function and has a functional equation. More precisely, define

$$\Lambda_K(\phi, s) = (D_{F/\mathbb{Q}}^2 |D_{K/F} \cdot \mathfrak{n}|)^{s-1} \left(\frac{\Gamma(s)}{(2\pi)^{s-1}} \right)^{2d} L_K(\phi, s),$$

where $D_{F/\mathbb{Q}}$ (respectively, $D_{K/F}$) is the discriminant of F over \mathbb{Q} (respectively, of K over F), $\Gamma(s)$ is the usual complex Γ -function and $|\cdot|$ is the norm map on ideals. The functional equation is the following:

$$\Lambda_K(\phi, s) = (-1)^d \epsilon(\mathfrak{n}) \Lambda_K(\phi, 2 - s).$$

For more details, see [53, Sections 3 and 6]. The sign

$$\epsilon_{\mathfrak{n},K}(\phi) := (-1)^d \epsilon(\mathfrak{n}) = \pm 1$$

of the functional equation is related to the order of vanishing of $L_K(\phi, s)$ at its central point $s = 1$; more precisely, this order is even if $\epsilon_{\mathfrak{n},K}(\phi) = 1$ and is odd otherwise. Since, by Assumption 1.6, the number of primes dividing \mathfrak{n}^- and d have the same parity, then $\epsilon_{\mathfrak{n},K}(\phi) = 1$.

Let B be the quaternion algebra over F which is ramified at all archimedean places of F and at all the primes dividing \mathfrak{n}^- . Fix an Eichler order R of level \mathfrak{n}^+ in B . By the Jacquet-Langlands correspondence (Theorem 3.7), there exists (unique up to multiples) a modular form $f : \widehat{R}^\times \backslash \widehat{B}^\times / B^\times \rightarrow \mathbb{Z}$ with the same eigenvalues as ϕ . Since all primes dividing \mathfrak{n}^- are inert in K , it follows by [47, III.3.8], that there exists a monomorphism $\Psi : K \rightarrow B$. Assume that Ψ is an optimal embedding of the integers \mathcal{O}_K of K into the Eichler order R , that is, $\Psi(\mathcal{O}_K) = \Psi(K) \cap R$. Adelicization $\widehat{\Psi} : \widehat{K} \rightarrow \widehat{B}$ yields a map, denoted by the same symbol,

$$\widehat{\Psi} : \widehat{\mathcal{O}}_K^\times \backslash \widehat{K}^\times / K^\times \rightarrow \widehat{R}^\times \backslash \widehat{B}^\times / B^\times.$$

DEFINITION 5.1. — *The algebraic part $\mathcal{L}_K(\phi)$ of $L_K(\phi, s)$ is defined by:*

$$\mathcal{L}_K(\phi) := \sum_{\mathfrak{a}} (f \circ \widehat{\Psi})(\mathfrak{a}),$$

where the sum is extended over a set of representatives $\mathfrak{a} \in \text{Pic}(\mathcal{O}_K)$.

THEOREM 5.2 (Gross-Zhang). — $L_K(\phi, 1) \doteq |\mathcal{L}_K(\phi)|^2$, where \doteq denotes an equality up to an explicitly computable non-zero factor.

Proof. — See [52, Theorem 1.3.2] and [23, Proposition 7.7] for $F = \mathbb{Q}$. □

5.2. Heegner points on Shimura curves

We keep the same notations and assumptions as in Section 4.5: E is a modular elliptic curve of conductor \mathfrak{n} , its associated eigenform ϕ is p -isolated and ℓ is an admissible prime.

Complex analytic description

Recall the complex analytic description of the Shimura curve (Section 4.1):

$$X(\mathbb{C}) = \widehat{\mathcal{R}}^\times \backslash \widehat{\mathcal{B}}^\times \times \mathcal{H} / \mathcal{B}^\times,$$

where \mathcal{B} is a quaternion algebra over F of discriminant $\mathfrak{n}^{-\ell}$ which is split in precisely one of the archimedean places of F , say μ and \mathcal{R} is an Eichler order of level \mathfrak{n}^+ . By Assumption 1.6, the set of F -homomorphisms $\text{Hom}(K, \mathcal{B})$ is not empty. Each point $P = (g, \psi)$ of the double coset space

$$Y_{\mathcal{R}}(K) := \widehat{\mathcal{R}}^\times \backslash \widehat{\mathcal{B}}^\times \times \text{Hom}(K, \mathcal{B}) / \mathcal{B}^\times$$

defines naturally a point $P \in X(\mathbb{C})$ as follows. First note that $(\mathcal{B} \otimes_F \mathbb{R})^\times \simeq \text{GL}_2(\mathbb{R})$ (tensor product with respect to μ) acts on \mathcal{H}^\pm by fractional linear transformations; hence there is an induced action of $\psi(K^\times)$ which has exactly one fixed point $z_\psi \in \mathcal{H}$. Moreover, by class field theory, if ψ is an optimal embedding of \mathcal{O}_K into the Eichler order $\mathcal{R}_g := g^{-1}\widehat{\mathcal{R}}g \cap \mathcal{B}$, then z_ψ can be defined over K_1 , the Hilbert class field of K (see [43, Theorem 9.6]). It follows that (g, ψ) defines naturally a point $(g, z_\psi) \in X(K_1)$.

DEFINITION 5.3. — *A Heegner point by \mathcal{O}_K is a point $(g, z_\psi) \in X(K_1)$ defined by the previous construction from a pair $(g, \psi) \in Y_{\mathcal{R}}(K)$ where ψ is an optimal embedding of \mathcal{O}_K into $\mathcal{R}_g := g^{-1}\widehat{\mathcal{R}}g \cap \mathcal{B}$.*

By [47, II.3 and III.5], Heegner points by \mathcal{O}_K exist. Define the action of $\text{Pic}(\mathcal{O}_K)$ on $Y_{\mathcal{R}}(K)$ as follows: $\forall \mathfrak{a} \in \widehat{\mathcal{O}}_K^\times \backslash \widehat{K}^\times / K^\times \simeq \text{Pic}(\mathcal{O}_K)$ and $\forall (g, \psi) \in Y_{\mathcal{R}}(K)$, $\mathfrak{a}(g, \psi) := (g\psi(\mathfrak{a}), \psi)$. By [43, Section 9], the action of $\text{Pic}(\mathcal{O}_K)$ on Heegner points is free and corresponds via class field theory to the Galois action of $\text{Gal}(K_1/K)$.

For any Heegner point $P = ((A, \iota, \theta, \kappa), C)$ by \mathcal{O}_K , define the *endomorphism ring of P* to be $\text{End}(P) := \text{End}(A)$ (see also [53, Section 2.1]). Then $\text{End}(P) \simeq \mathcal{O}_K$ and $\text{End}(P)^0 := \text{End}(P) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq K$.

ℓ -adic analytic description

Let $P \in X(K_1)$ be an Heegner point by \mathcal{O}_K . Since ℓ is inert in K , the prime of K over ℓ splits completely in K_1 and, chosen a prime λ of K_1 above ℓ , the completion of K_1 at λ is isomorphic to $K_\ell \simeq F_{\ell^2}$, hence $P \in \mathcal{X}_{\ell^2}(K_\ell)$. Fix an isomorphism $\widehat{B} \simeq \widehat{\mathcal{B}}^{(\ell)}\text{M}_2(F_\ell)$ and choose an Eichler order R of B of level \mathfrak{n}^+ so that $\widehat{\mathcal{R}}^{(\ell)}$ corresponds to $\widehat{R}^{(\ell)}$ under the chosen isomorphism (the superscript $^{(\ell)}$ denotes as usual the corresponding adèle ring with the

ℓ -component removed). Set $R \left[\frac{1}{\ell} \right] := \widehat{R}^{(\ell)} M_2(F_\ell) \cap B$, and, for any $g \in \widehat{B}^\times$, $R_g \left[\frac{1}{\ell} \right] := g^{-1} \widehat{R} \left[\frac{1}{\ell} \right] g \cap B$. Denote by $\text{End}(\bar{P})$ the endomorphism ring of the reduced abelian variety A over \mathbb{F}_ℓ , the residue field of K_ℓ at ℓ . Define $\text{End}(\bar{P}) \left[\frac{1}{\ell} \right] := \text{End}(\bar{P}) \otimes \mathcal{O}_K \left[\frac{1}{\ell} \right]$, where $\mathcal{O}_K \left[\frac{1}{\ell} \right] = \widehat{\mathcal{O}}_K^{(\ell)} K_\ell \cap K$.

The Čerednik-Drinfeld theorem and the description of \mathcal{H}_ℓ as moduli space for special formal \mathcal{R}_ℓ -modules of height 4 (see [7, Chapitre I] and [53, Section 2.3]) imply that $\text{End}^0(\bar{P}) := \text{End}(\bar{P}) \otimes \mathbb{Q} \simeq B$ while, by [53, Proposition 2.3.2] (see also [52, Section 5.4]), $\text{End}(\bar{P}) \left[\frac{1}{\ell} \right]$ is isomorphic to $R_g \left[\frac{1}{\ell} \right]$ for some $g \in \widehat{B}^\times$. Since $\text{End}^0(P) := \text{End}(P) \otimes \mathbb{Q} \simeq K$, it follows that the map obtained by reduction of endomorphisms $\text{End}(P) \rightarrow \text{End}(\bar{P})$ gives rise to maps: $\Psi : K \rightarrow B$ and $\Psi^0 : \mathcal{O}_K \left[\frac{1}{\ell} \right] \rightarrow R_g \left[\frac{1}{\ell} \right]$. Hence P defines naturally an element

$$(g, \Psi) \in \widehat{R} \left[\frac{1}{\ell} \right]^\times \setminus (\widehat{B}^\times \times \text{Hom}(K, B)) / B^\times.$$

The extension of Ψ by K_ℓ yields a map:

$$\Psi_\ell : K_\ell \rightarrow B_\ell := B \otimes_F F_\ell \simeq M_2(F_\ell)$$

which induces an action of K_ℓ^\times on \mathcal{H}_ℓ by fractional linear transformations; this action has two distinct fixed points z and \bar{z} which belong to K_ℓ and are conjugate by the non-trivial element in $\text{Gal}(K_\ell/F_\ell)$. Choose z so that the action of Ψ_ℓ on the tangent space $t(P)$ at P is via the character $z \mapsto \frac{z}{\bar{z}}$, where $z \mapsto \bar{z}$ is the action of $\text{Gal}(K_\ell/F_\ell)$ (the other point has an action by $z \mapsto \frac{\bar{z}}{z}$). This construction provides a point

$$P_\Psi := (g, z) \in \widehat{R} \left[\frac{1}{\ell} \right]^\times \setminus (\widehat{B}^\times \times \mathcal{H}_\ell) / B^\times.$$

Then the image of P by the Cedernik-Drinfeld theorem is P_Ψ .

The Tate-Honda theorem implies that there exists a unique maximal order v_Ψ of $M_2(F_\ell)$ containing $\Psi(\mathcal{O}_K) \simeq \Psi(\text{End}(P))$: for details, see [53, Propositions 2.3.2 and 3.4.5] or [52, Sections 5.4 and 5.5]. Since the reduction map $r_\ell : \mathcal{X}_{\ell^2}(K_\ell) \rightarrow \mathcal{V}(\mathcal{G}_\ell) \cup \mathcal{E}(\mathcal{G}_\ell)$ is $\text{GL}_2(F_\ell)$ -equivariant and v_Ψ is the unique vertex of \mathcal{T}_ℓ fixed by the action of $\Psi_\ell(K_\ell^\times)$, it follows that the reduction of P_Ψ corresponds to the vertex v_Ψ , hence, in particular, it is not a singular point. Set: $r_\ell(P_\Psi) = v_\Psi \in \mathcal{V}(\mathcal{G}_\ell)$.

Let σ be the element associated with $\mathfrak{a} \in \text{Pic}(\mathcal{O}_K)$ via class field theory and denote by P^σ its action on P . Then $\text{Hom}(P^\sigma, P) \simeq \mathfrak{a}$ and it follows from the same argument as [25, Proposition 7.3] that $\text{Hom}(\bar{P}^\sigma, \bar{P}) \simeq \text{End}(\bar{P})\mathfrak{a}$ (see also [53, Proposition 2.4.5] and [52, Sections 5.4 and 5.5]). Since $\text{End}(\bar{P}^\sigma)$ is the right order of $\text{Hom}(\bar{P}^\sigma, \bar{P})$, reduction modulo the

fixed prime above ℓ gives a map

$$\Psi^\sigma : \mathcal{O}_K \left[\frac{1}{\ell} \right] \simeq \text{End}(P^\sigma) \left[\frac{1}{\ell} \right] \rightarrow \text{End}(\bar{P}^\sigma) \left[\frac{1}{\ell} \right] \simeq R_g^\sigma \left[\frac{1}{\ell} \right]$$

where $R_g^\sigma \left[\frac{1}{\ell} \right] := \mathfrak{a}^{-1} g^{-1} \widehat{R} \left[\frac{1}{\ell} \right] g \mathfrak{a} \cap B$. It follows that the action of σ on $P = (g, \Psi)$ is given by $P^\sigma = (g\mathfrak{a}, \Psi)$. Since, from Lemma 2.2, $\mathcal{V}(\mathcal{G}_\ell) \simeq \widehat{R}^\times \backslash \widehat{B}^\times / B^\times \times \{0, 1\}$, the action of σ on $\mathcal{V}(\mathcal{G}_\ell)$ corresponds to the multiplication by \mathfrak{a} on $\widehat{R}^\times \backslash \widehat{B}^\times / B^\times \times \{0, 1\}$.

5.3. The reciprocity law

Keep the same notations and assumptions as in Section 5.2. Let P be a Heegner point of conductor \mathcal{O}_K . Define the divisor

$$D_K := \sum_{\sigma} P^\sigma \in \text{Div}(X)(K_1),$$

where the sum is extended over all $\sigma \in \text{Gal}(K_1/K)$. Choose a prime λ of K_1 over ℓ ; hence D_K can be viewed as a divisor in $\text{Div}(\mathcal{X}(K_\ell))$ via the isomorphism between the completion of K_1 at λ and K_ℓ . Consider the component \mathcal{C}_ℓ in Definition 4.12; by Corollary 4.14, there is an equality $\partial_\ell(D_K) = \omega_\ell(r_\ell(D_K))$ in \mathcal{C}_ℓ . The following proposition is the *Reciprocity Law* connecting Heegner points and the special value of L -series.

PROPOSITION 5.4. — *There is an element $C \in (\mathbb{Z}/p\mathbb{Z})^\times$ so that $\partial_\ell(D_K) \equiv C \mathcal{L}_K(\phi)$ in $\mathcal{C}_\ell \simeq \mathbb{Z}/p\mathbb{Z}$.*

Proof. — Let $v_\Psi \in \widehat{R}^\times \backslash \widehat{B}^\times / B^\times$ be the vertex associated with P as in Section 5.2. The reduction map to \mathcal{C}_ℓ gives rise to a map $r_\ell : \widehat{R}^\times \backslash \widehat{B}^\times / B^\times \rightarrow \mathbb{Z}/p\mathbb{Z}$ having the same eigenvalues as the map f associated to ϕ by the Jacquet-Langlands correspondence; hence $r_\ell = Cf$ for an element $C \in (\mathbb{Z}/p\mathbb{Z})^\times$. From Section 5.2, the action of $\mathfrak{a} \in \text{Pic}(\mathcal{O}_c) \simeq \text{Gal}(K_1/K)$ on Heegner points corresponds to right multiplication by \mathfrak{a} on the vertex v_Ψ corresponding to P . The result follows from the definition of the algebraic part $\mathcal{L}_K(\phi)$ of ϕ . □

5.4. The Euler system

We keep the same notations and assumptions as in Section 5.3. The divisor D_K defines by projection a point $P_K \in J(K)/\mathfrak{m}_{f_\ell}$. The Kummer map $\delta : J(K)/pJ(K) \rightarrow H^1(K, J[p])$ yields a map:

$$d : J(K)/\mathfrak{m}_{f_\ell} \rightarrow H^1(K, T_p(J)/\mathfrak{m}_{f_\ell}) \simeq H^1(K, T_\phi[p])^k,$$

where the last isomorphism follows from Theorem 4.13. Let \mathcal{C}_ℓ be the component in Definition 4.12 and let

$$\pi_\ell : H^1(K_\ell, T_\phi[p])^k \rightarrow H^1(K_\ell, \mathcal{D}_\ell) \simeq H^1(K_\ell, T_\phi[p])$$

be the corresponding projection map (see also Theorem 4.13). Define

$$\kappa_\ell := \pi_\ell(d(P_K)).$$

THEOREM 5.5. — *Suppose that $\mathcal{L}_K(\phi) \not\equiv 0 \pmod{p}$ and that ϕ is p -isolated. Then the class $\kappa_\ell \in H^1(K, T_\phi[p])$ has the following properties.*

1. For $\mathfrak{q} \nmid n p \ell$, $\partial_{\mathfrak{q}}(\kappa_\ell) = 0$;
2. For $\mathfrak{q} \mid n^-$, $\text{res}_{\mathfrak{q}}(\kappa_\ell) \in H_{\text{ord}}^1(K_{\mathfrak{q}}, T_\phi[p])$;
3. For $\mathfrak{q} \mid p$, $\text{res}_{\mathfrak{q}}(\kappa_\ell) \in H_{\text{ord}}^1(K_{\mathfrak{q}}, T_\phi[p])$;
4. $\partial_\ell(\kappa_\ell) \neq 0$.

Proof. — First note that κ_ℓ comes from a global point of $J(K)/\mathfrak{m}_{f_\ell}$, so it belongs to the p -Selmer group of J/\mathfrak{m}_{f_ℓ} over K . Then 5.5 follows from [36, Chapter I, Section 3]. For 5.5, use that the Shimura curve \mathcal{X}_{ℓ^2} has a Mumford-Tate uniformization at primes $\mathfrak{q} \mid n^-$ (see [13] for details). For 5.5, use the description of the image of the Kummer map given by [5, Section 3]. Finally, 5.5 follows from Proposition 5.4. \square

COROLLARY 5.6. — *Theorem 2.6 holds.*

Proof. — Since $L_K(\phi, 1) \neq 0$, there exists only a finite number of primes p so that $p \mid \mathcal{L}_K(\phi)$. Choose p so that $p \nmid \mathcal{L}_K(\phi)$ and assume that ϕ is p -isolated. Then for each n , $\{\kappa_\ell\}_\ell$ is an Euler system by Theorem 5.5. \square

BIBLIOGRAPHY

- [1] M. BERTOLINI & H. DARMON, “Heegner points on Mumford-Tate curves”, *Invent. Math.* **126** (1996), no. 3, p. 413-456.
- [2] ———, “A rigid analytic Gross-Zagier formula and arithmetic applications”, *Ann. of Math. (2)* **146** (1997), no. 1, p. 111-147, With an appendix by Bas Edixhoven.
- [3] ———, “ p -adic periods, p -adic L -functions, and the p -adic uniformization of Shimura curves”, *Duke Math. J.* **98** (1999), no. 2, p. 305-334.
- [4] ———, “Iwasawa’s main conjecture for elliptic curves over anticyclotomic \mathbb{Z}_p -extensions”, *Ann. of Math. (2)* **162** (2005), no. 1, p. 1-64.
- [5] S. BLOCH & K. KATO, “ L -functions and Tamagawa numbers of motives”, in *The Grothendieck Festschrift, Vol. I*, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, p. 333-400.
- [6] N. BOSTON, L. HENDRIK W. JR. & K. A. RIBET, “Quotients of group rings arising from two-dimensional representations”, *C. R. Acad. Sci. Paris Sér. I Math.* **312** (1991), no. 4, p. 323-328.
- [7] J.-F. BOUTOT & H. CARAYOL, “Uniformisation p -adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld”, *Astérisque* (1991), no. 196-197, p. 7, 45-158, Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

- [8] C. BREUIL, B. CONRAD, F. DIAMOND & R. TAYLOR, “On the modularity of elliptic curves over \mathbf{Q} : wild 3-adic exercises”, *J. Amer. Math. Soc.* **14** (2001), no. 4, p. 843-939.
- [9] D. BUMP, S. FRIEDBERG & J. HOFFSTEIN, “Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L -functions and their derivatives”, *Ann. of Math. (2)* **131** (1990), no. 1, p. 53-127.
- [10] H. CARAYOL, “Sur la mauvaise réduction des courbes de Shimura”, *Compositio Math.* **59** (1986), no. 2, p. 151-230.
- [11] ———, “Sur les représentations galoisiennes modulo l attachées aux formes modulaires”, *Duke Math. J.* **59** (1989), no. 3, p. 785-801.
- [12] I. V. ČEREDNIK, “Uniformization of algebraic curves by discrete arithmetic subgroups of $\mathrm{PGL}_2(k_w)$ with compact quotient spaces”, *Mat. Sb. (N.S.)* **100(142)** (1976), no. 1, p. 59-88, 165.
- [13] J. COATES & R. GREENBERG, “Kummer theory for abelian varieties over local fields”, *Invent. Math.* **124** (1996), no. 1-3, p. 129-174.
- [14] B. CONRAD, F. DIAMOND & R. TAYLOR, “Modularity of certain potentially Barsotti-Tate Galois representations”, *J. Amer. Math. Soc.* **12** (1999), no. 2, p. 521-567.
- [15] H. DARMON, F. DIAMOND & R. TAYLOR, “Fermat’s last theorem”, in *Current developments in mathematics, 1995 (Cambridge, MA)*, Internat. Press, Cambridge, MA, 1994, p. 1-154.
- [16] H. DARMON & A. LOGAN, “Periods of Hilbert modular forms and rational points on elliptic curves”, *Int. Math. Res. Not.* (2003), no. 40, p. 2153-2180.
- [17] F. DIAMOND, “On deformation rings and Hecke rings”, *Ann. of Math. (2)* **144** (1996), no. 1, p. 137-166.
- [18] F. DIAMOND & R. TAYLOR, “Nonoptimal levels of mod l modular representations”, *Invent. Math.* **115** (1994), no. 3, p. 435-462.
- [19] V. G. DRINFEL’D, “Coverings of p -adic symmetric domains”, *Funkcional. Anal. i Priložen.* **10** (1976), no. 2, p. 29-40.
- [20] M. EICHLER, “The basis problem for modular forms and the traces of the Hecke operators”, in *Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Math., vol. 320, Springer, Berlin, 1973, p. 75-151.
- [21] L. GERRITZEN & M. VAN DER PUT, *Schottky groups and Mumford curves*, Lecture Notes in Mathematics, vol. 817, Springer, Berlin, 1980, viii+317 pages.
- [22] R. GREENBERG, “Iwasawa theory for elliptic curves”, in *Arithmetic theory of elliptic curves (Cetraro, 1997)*, Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, p. 51-144.
- [23] B. H. GROSS, “Heights and the special values of L -series”, in *Number theory (Montreal, Que., 1985)*, CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, p. 115-187.
- [24] ———, “Kolyvagin’s work on modular elliptic curves”, in *L -functions and arithmetic (Durham, 1989)*, London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, Cambridge, 1991, p. 235-256.
- [25] B. H. GROSS & D. B. ZAGIER, “Heegner points and derivatives of L -series”, *Invent. Math.* **84** (1986), no. 2, p. 225-320.
- [26] A. GROTHENDIECK, *Groupes de monodromie en géométrie algébrique. I*, Springer-Verlag, Berlin, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1967-1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim, Lecture Notes in Mathematics, Vol. 288, viii+523 pages.
- [27] H. JACQUET & R. P. LANGLANDS, *Automorphic forms on $\mathrm{GL}(2)$* , Springer-Verlag, Berlin, 1970, Lecture Notes in Mathematics, Vol. 114, vii+548 pages.

- [28] F. JARVIS, “Level lowering for modular mod l representations over totally real fields”, *Math. Ann.* **313** (1999), no. 1, p. 141-160.
- [29] ———, “Mazur’s principle for totally real fields of odd degree”, *Compositio Math.* **116** (1999), no. 1, p. 39-79.
- [30] ———, “Correspondences on Shimura curves and Mazur’s principle at p ”, *Pacific J. Math.* **213** (2004), no. 2, p. 267-280.
- [31] B. W. JORDAN & R. LIVNÉ, “Integral Hodge theory and congruences between modular forms”, *Duke Math. J.* **80** (1995), no. 2, p. 419-484.
- [32] B. W. JORDAN & R. A. LIVNÉ, “Local Diophantine properties of Shimura curves”, *Math. Ann.* **270** (1985), no. 2, p. 235-248.
- [33] V. A. KOLYVAGIN, “Finiteness of $E(\mathbf{Q})$ and $\text{SH}(E, \mathbf{Q})$ for a subclass of Weil curves”, *Izv. Akad. Nauk SSSR Ser. Mat.* **52** (1988), no. 3, p. 522-540, 670-671.
- [34] V. A. KOLYVAGIN & D. Y. LOGACHËV, “Finiteness of SH over totally real fields”, *Izv. Akad. Nauk SSSR Ser. Mat.* **55** (1991), no. 4, p. 851-876.
- [35] M. LONGO, “On the birch and swinnerton-dyer conjecture over totally real fields”, PhD Thesis, Dipartimento di Matematica P. e A., Padova, 2004.
- [36] J. S. MILNE, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press Inc., Boston, MA, 1986, x+421 pages.
- [37] M. R. MURTY & V. K. MURTY, “Mean values of derivatives of modular L -series”, *Ann. of Math. (2)* **133** (1991), no. 3, p. 447-475.
- [38] A. RAJAEI, “On the levels of mod l Hilbert modular forms”, *J. Reine Angew. Math.* **537** (2001), p. 33-65.
- [39] K. A. RIBET, “On modular representations of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms”, *Invent. Math.* **100** (1990), no. 2, p. 431-476.
- [40] K. A. RIBET, “Congruence relations between modular forms”, in *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983)* (Warsaw), PWN, 1984, p. 503-514.
- [41] J.-P. SERRE, “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques”, *Invent. Math.* **15** (1972), no. 4, p. 259-331.
- [42] G. SHIMURA, “The special values of the zeta functions associated with Hilbert modular forms”, *Duke Math. J.* **45** (1978), no. 3, p. 637-679.
- [43] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971, Kanô Memorial Lectures, No. 1, xiv+267 pages.
- [44] J. H. SILVERMAN, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986, xii+400 pages.
- [45] R. TAYLOR, “On Galois representations associated to Hilbert modular forms”, *Invent. Math.* **98** (1989), no. 2, p. 265-280.
- [46] R. TAYLOR & A. WILES, “Ring-theoretic properties of certain Hecke algebras”, *Ann. of Math. (2)* **141** (1995), no. 3, p. 553-572.
- [47] M.-F. VIGNÉRAS, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980, vii+169 pages.
- [48] J.-L. WALDSPURGER, “Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie”, *Compositio Math.* **54** (1985), no. 2, p. 173-242.
- [49] ———, “Correspondances de Shimura et quaternions”, *Forum Math.* **3** (1991), no. 3, p. 219-307.
- [50] A. WILES, “On ordinary λ -adic representations associated to modular forms”, *Invent. Math.* **94** (1988), no. 3, p. 529-573.
- [51] ———, “Modular elliptic curves and Fermat’s last theorem”, *Ann. of Math. (2)* **141** (1995), no. 3, p. 443-551.

- [52] S.-W. ZHANG, “Gross-Zagier formula for GL_2 ”, *Asian J. Math.* **5** (2001), no. 2, p. 183-290.
- [53] ———, “Heights of Heegner points on Shimura curves”, *Ann. of Math. (2)* **153** (2001), no. 1, p. 27-147.

Manuscrit reçu le 28 février 2005,
révisé le 3 août 2005,
accepté le 5 septembre 2005.

Matteo LONGO
Université Louis Pasteur
IRMA
7, rue René Descartes
67084 Strasbourg (France)
mlongo@math.unipd.it