Università degli Studi di Milano

Dipartimento di Matematica F. Enriques

Scuola di Dottorato in Scienze Matematiche
Corso di Dottorato di Ricerca in Matematica
XXVI Ciclo

Tesi di Dottorato di Ricerca

On the Birch and Swinnerton-Dyer conjecture for elliptic curves of analytic rank one

Candidato
Andrea Berti
Matricola
R08961

Relatore
Prof. Massimo Bertolini
Coordinatore del Dottorato
Prof. Lambertus Van Geemen

Anno Accademico 2013/2014

to my family

L'essenziale è invisibile agli occhi.

Contents

Introduction

The main result of this Thesis is to prove the p-part of the Birch and Swinnerton-Dyer conjecture for semistable elliptic curve of analytic rank one. Our main result is the following arithmetic relation:

Theorem A *Let $E/\mathbb{Q}$ be a semistable elliptic curve of analytic rank one (i.e. the Hasse-Weil L-series $L(E/\mathbb{Q},s)$ has a simple zero at $s=1$). Then there exists a* finite *set of primes $\Sigma_E \supset \{2,3,5,7\}$ such that: for every prime $p \notin \Sigma_E$ of good ordinary reduction for $E/\mathbb{Q}$*

$$\text{“ } p \text{ divides } \frac{L'(E/\mathbb{Q},1)}{\Omega_E \cdot h_E(P_E)} \text{ ”} \quad \Longleftrightarrow \quad \text{“ } p \text{ divides } \#Ш(E/\mathbb{Q}) \cdot C_N \text{ ”},$$

where the notations are as follows: P_E is a generator of the Mordell-Weil group $E(\mathbb{Q})$ modulo torsion, Ω_E is the real period of $E/\mathbb{Q}$, and $h_E(P_E)$ is the Néron-tate height of P_E −so that the ratio $L'(E/\mathbb{Q})/\Omega_E \cdot h_E(P_E)$ is a non-zero integer. Moreover, $Ш(E/\mathbb{Q})$ is the Tate-Shafaravivh group of $E/\mathbb{Q}$, and $C_N := \prod_{\ell|\mathrm{cond}(E/\mathbb{Q})} c_\ell$, with $c_\ell := c_\ell(E/\mathbb{Q})$ the ℓ-th Tamagawa factor of E for every prime ℓ dividing the conductor $\mathrm{cond}(E/\mathbb{Q})$ *of $E/\mathbb{Q}$.*

In [SU] Skinner and Urban proved (under some hypotheses verified in our setting), the validity of the p-part of the Birch and Swinnerton-Dyer conjecture for semistable elliptic curves of analytic rank zero. Their result is a consequence of the Iwasawa Main Conjecture for GL_2. Our strategy adapts the techiniques of the work of Bertolini and Darmon and deduces the result for elliptic curves of analytic rank one from the result of [SU]. The idea is to explicitely construct a modular form g by rasing the level of the modular form f attached by Wiles result [Wi] to the elliptic curve E, and to relate the special value of the L-function attached to g to the the index in $E(K)$ of a Heegner point P_K, where K is a suitable imaginary quadratic field. Assuming the existence of a lift to characteristic zero of an eigenform obtained by raising the level from a p-isolated eigenform (see the Lifting Hypothesis 2.3.2) we prove the following result:

Theorem B *Let $E/\mathbb{Q}$ be an elliptic curve of squarefree conductor N. Assume that E has analytic rank one. Let P_E be a generator of the Mordell-Weil group modulo torsion and denote by $h_E(P_E)$ its canonical Néron-Tate height. Let $p \geq 11$ be a prime of good ordinary reduction for E and suppose that p does not divide the minimal degree d_E of a modular parametrization $\varphi_E : X_0(N) \to E$. Assume furthermore the Lifting Hypothesis 2.3.2. The equality*

$$\mathrm{ord}_p\left(\frac{L'(E/\mathbb{Q},1)}{\Omega_E \cdot h_E(P_E)}\right) = \mathrm{ord}_p(\#Ш(E/\mathbb{Q}) \cdot C_N)$$

holds (i.e. the p-part of the Birch and Swinnerton-Dyer formula holds for $L(E/\mathbb{Q},s)$).

This Thesis is divided into two parts. The first part is essentially expository: we introduce the definitions of the objects we use in this work and state the Birch and Swinnerton-Dyer conjecture. We discuss in detail the evidence and the known partial results. We discuss in particular the work of Skinner and Urban [SU], and the equivalence between classical and quaterinionic modular forms, via the Jacquet-Langlands correspondence.

The second part is devoted to the proof of Theorem A. We start giving the main steps of the proof, then first we give a simplification of the statement, that, after our reduction,

is equivalent to a relation between the p-orders of the Shafarevich-Tate group of $E/\mathbb{Q}$ and the index of the above-mentioned Heegner point. Then we give the explicit construction of an eigenform obtained by raising the level from the modular form attached to E, borrowing techniques from [BD].

All the constructions work modulo p^n, and one is left with the technical problem to show the existence of a lift to characteristic zero of the mod-p^n modular form obtained. This is known in the case $n = 1$ and gives Theorem A. Following Vatsal [Va] we state a special value formula, which combined with the result of Skinner and Urban [SU] on the validity of the p-part of the Birch and Swinnerton-Dyer conjecture for elliptic curves of analytic rank zero, allows us to conclude our proof. Theorem B follows from a similar argument, assuming the Lifting Hypothesis 2.3.2.

Chapter 1

Elliptic curves: results and open problems

In this first Chapter we introduce the definitions and the results we use in Chapters II.

1.1 The Mordell-Weil theorem

Main Reference: [B]

Let E be an elliptic curve defined over a number field K. One important result, and in some sense, the starting point for the study of the arithmetic of the K-rational points of E is the Mordell-Weil theorem.

Theorem 1.1.1 (Mordell-Weil)**.** *The Mordell-Weil group $E(K)$ is finitely generated, i.e. it is of the form*

$$E(K) = \mathbb{Z}^r \oplus E(K)_{\text{tors}},$$

where $r \geq 0$ and $E(K)_{\text{tors}}$ is the finite torsion subgroup of $E(K)$.

Remark 1.1.2. The torsion subgroup $E(K)_{\text{tors}}$ can be easily calculated for a given E, and its order is bounded in terms of the degree $[K : \mathbb{Q}]$, thanks to the works of Mazur [Ma1] and Merel [Me].
The integer $r := \text{rnk}_{\mathbb{Z}}(E)$ is called the *algebraic rank* of E. The proof of the Mordell-Weil theorem does not provide an effective algorithm to determine r and no algorithm in general is known.

We omit a complete proof of this fact, that is very common in literature, see for example [Si]. We just give the outline of the main steps for fixing the notations.

The proof is divided into two steps. The first step provides the existence of a function $h : E(K) \to \mathbb{R}$, called *height*, such that:

- fixed one point $Q \in E(K)$ there exists a constant C depending on Q (and on E) and a constant C' depending only on the curve E, giving the following bounds

  $$h(P+Q) \leq 2h(P) + C, \quad h(mP) \geq m^2 h(P) + C',$$

  for an arbitrary $P \in E(K)$ and any positive integer m.

- for each $x > 0$ we have that

$$\#\{P \in E(K) : h(P) < x\} < \infty.$$

The second step is known as the weak Mordell-Weil theorem and states the finiteness of the quotient $E(K)/nE(K)$ for every n.

The link between the two steps is given by the so-called descent lemma of Fermat, that ensures that every abelian group G with a finite quotient G/nG and equipped with an height function as above is finitely generated.

If we take $K = \mathbb{Q}$, then we can define a height function of a point $P \in E(\mathbb{Q})$ as

$$h(P) = \begin{cases} 0 & \text{if } P = O_E \\ \log(\max\{|r|, |s|\}) & \text{if } P = (r/s, y) \text{ with } (r, s) = 1. \end{cases}$$

The height function h can be turned into a quadratic function, called the canonical Néron-Tate height, by the formula

$$\hat{h}_{NT}(P) := \frac{1}{2} \lim_{n\to\infty} 4^{-n} h(2^n P),$$

that satisfies the following properties:

i $2\hat{h}_{NT}(P) - h(P) = O(1)$,

ii $\hat{h}_{NT}(P) \geq 0$ for all P, and the equality holds if and only if P is a torsion point,

iii $\hat{h}_{NT}(mP) = m^2 \hat{h}_{NT}(P)$.

We fix the notation for the associated bilinear symmetric pairing:

$$\langle P, Q \rangle_{NT} = \hat{h}_{NT}(P + Q) - \hat{h}_{NT}(P) - \hat{h}_{NT}(Q).$$

Remark 1.1.3. The above discussion generalises to any number field K, and gives rise to a canonical Néron-Tate non-degenerate pairing

$$\langle , \rangle_{NT} : E(K)/E(K)_{\text{tors}} \times E(K)/E(K)_{\text{tors}} \to \mathbb{R}$$

To simplify notations, if it does not generate confusion, we denote $\hat{h}_{NT}$ by h_E.

The point of the proof which is more relevant for our argument is the second step, i.e. the weak Mordell-Weil theorem.

The result is trivial on an algebraic closure $\bar{K}$ of K. Denoting by $[n]$ the multiplication-by-n map, we have an exact sequence

$$0 \to E[n] \to E\left(\bar{K}\right) \xrightarrow{[n]} E\left(\bar{K}\right) \to 0$$

of modules with a natural continuous action of the absolute Galois group $G_K = \text{Gal}\left(\bar{K}/K\right)$. Taking Galois cohomology on the sequence, we get a new exact sequence

$$\begin{aligned} 0 \to E[n] \to E\left(\bar{K}\right) \xrightarrow{[n]} E\left(\bar{K}\right) \to \\ \to \text{H}^1\left(G_K, E[n]\right) \to \text{H}^1\left(G_K, E\right) \xrightarrow{[n]} \text{H}^1\left(G_K, E\right) \end{aligned}$$

from which we can extract the so called Kummer sequence

$$0 \to E(K)/nE(K) \xrightarrow{\delta} \mathrm{H}^1(G_K, E[n]) \to \mathrm{H}^1(G_K, E)[n] \to 0.$$

Actually nothing changes if we take an arbitrary isogeny $\phi : E \to E$ instead of $[n]$, so we have, more in general, a sequence of G_K-modules

$$0 \to E[\phi] \to E\left(\bar{K}\right) \xrightarrow{[\phi]} E\left(\bar{K}\right) \to 0$$

that again gives the Kummer sequence

$$0 \to E(K)/\phi(E(K)) \xrightarrow{\delta} \mathrm{H}^1(G_K, E[\phi]) \to \mathrm{H}^1(G_K, E)[\phi] \to 0. \tag{1.1}$$

We are interested in $\operatorname{Im}\delta$, therefore we look for local informations.

Let v be any place of K and denote by K_v the completion of K at v. We fix the embeddings

$$\begin{array}{ccc} K & \hookrightarrow & \bar{K} \\ \downarrow & & \downarrow \\ K_v & \hookrightarrow & \bar{K}_v \end{array}$$

and obtain an inclusion on absolute Galois groups

$$G_{K_v} \subset G_K.$$

Turning back to the exact sequence (1.1) we have the diagram

$$\begin{array}{ccccccccc} 0 & \to & \frac{E(K)}{\phi(E(K))} & \xrightarrow{\delta} & \mathrm{H}^1(G_K, E[\phi]) & \to & \mathrm{H}^1(G_K, E)[\phi] & \to & 0 \\ & & \downarrow & & \downarrow & \searrow & \downarrow & & \\ 0 & \to & \prod_v \frac{E(K_v)}{\phi(E(K_v))} & \xrightarrow{\delta} & \prod_v \mathrm{H}^1(G_{K_v}, E[\phi]) & \to & \prod_v \mathrm{H}^1(G_{K_v}, E)[\phi] & \to & 0. \end{array}$$

Computing

$$\ker\left\{\mathrm{H}^1(G_K, E[\phi]) \to \mathrm{H}^1(G_K, E)[\phi]\right\}$$

is again a hard problem, but in the local case

$$\ker\left\{\mathrm{H}^1(G_{K_v}, E[\phi]) \to \mathrm{H}^1(G_{K_v}, E)[\phi]\right\}$$

the computation is straightforward thanks to Hensel's Lemma.

This leads to the following definitions.

Definition 1.1.4. Let $\phi : E \to E$ be a K-rational isogeny.

The *ϕ-Selmer group* of E/K is

$$\mathrm{Sel}_\phi(E/K) = \ker\left\{\mathrm{H}^1(G_K, E[\phi]) \to \prod_v \mathrm{H}^1(G_{K_v}, E)[\phi]\right\}$$

and the *Shafarevich-Tate group* of E/K is

$$\underline{\mathrm{III}}(E/K) = \ker\left\{\mathrm{H}^1(G_K, E) \to \prod_v \mathrm{H}^1(G_{K_v}, E)\right\}.$$

The conclusion of the proof of the theorem is given by the following result (for details see [Si], X, 4.2).

Theorem 1.1.5. *There is an exact sequence*

$$0 \to E(K)/\phi(E(K)) \to \mathrm{Sel}_\phi(E/K) \to Ш(E/K)[\phi] \to 0.$$

Furthermore the Selmer group is finite.

The last assertion in particular implies the weak Mordell-Weil theorem.

Remark 1.1.6. The group $\mathrm{Sel}_\phi(E/K)$ is effectively calculable, hence it is natural to investigate how good it is as an approximation of $E(K)/\phi(E(K))$, in other words, how large $Ш(E/K)_\phi$ can be.

1.1.1 Selmer groups of abelian varieties

Following [GP] we define the Selmer group of an abelian variety as follows. Let $A/\mathbb{Q}$ be an abelian variety. Assume that A has multiplication by a totally real field F i.e. there is a morphism from the ring of integers of F and the ring of rational endomorphisms of A. Let $\mathfrak{p}$ be an ideal of $\mathcal{O}_F$. There is an exact sequence

$$0 \to A[\mathfrak{p}^n] \to A \to \mathfrak{p}^{-n} \otimes_{\mathcal{O}_F} A \to 0.$$

Taking Galois cohomology, we define the Kummer map as the morphims

$$\mathfrak{p}^{-n} \otimes_{\mathcal{O}_F} A(F) \to \mathrm{H}^1(F, A[\mathfrak{p}^n]).$$

The kernel of the Kummer map is the ideal

$$(\mathcal{O}_F/\mathfrak{p}^n) \otimes_{\mathcal{O}_F} A(\mathbb{Q}),$$

and so the image of the Kummer map is

$$(\mathfrak{p}^{-n}) \otimes_{\mathcal{O}_F} ((\mathcal{O}_F/\mathfrak{p}^n) \otimes_{\mathcal{O}_F} A(\mathbb{Q})).$$

The $\mathfrak{p}^n$-*Selmer group* of A is the group

$$\mathrm{Sel}_{\mathfrak{p}^n}(A/F) \subset \mathrm{H}^1(F, A[\mathfrak{p}^n])$$

of classes $x \in \mathrm{H}^1(F, A[\mathfrak{p}^n])$ such that the restrictions $x_v \in \mathrm{H}^1(F_v, A[\mathfrak{p}^n])$ lie in the image of $\mathrm{Hom}_{\mathcal{O}_F}(\mathfrak{p}^n, A(F_v))$, under the local Kummer map for all the places v of K.

1.2 The L-series of an elliptic curve

Let E be an elliptic curve definite over $\mathbb{Q}$ and let N be the arithmetic conductor of E. Let p be a rational prime, and denote by $\mathcal{E}_p$ the minimal model of E over $\mathbb{Z}_p$, write $\bar{\mathcal{E}}_p$ for the special fiber of $\mathcal{E}_p$. By the definition of the conductor we have:

1. $\bar{\mathcal{E}}_p$ is smooth if and only if p does not divide N and we say that E has good reduction at p
2. if p divides N exactly then $\bar{\mathcal{E}}_p$ has a unique singular point that is a node, in this case we say that E has multiplicative reduction. If the tangent lines have rational slopes over $\mathbb{F}_p$ we say that the reduction is split multiplicative, if they are only definite over a quadratic extension of $\mathbb{F}_p$ we say that the reduction is non-split multiplicative

3. if p^2 divides N then the singular point of $\bar{\mathcal{E}}_p$ is a cusp, and in this case we say that the reduction of E at p is additive.

Let

$$a_p = \begin{cases} p+1-\#\bar{\mathcal{E}}_p(\mathbb{F}_p) & \text{if } p \text{ is a prime of good reduction,} \\ 0 & \text{if the reduction of } E \text{ at } p \text{ is additive,} \\ 1 & \text{if the reduction of } E \text{ at } p \text{ is split multiplicative,} \\ -1 & \text{if the reduction of } E \text{ at } p \text{ is non-split multiplicative.} \end{cases}$$

Definition 1.2.1. The L-series of E is the function of the complex variable s defined by

$$L(E/\mathbb{Q},s) = \prod_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}} \prod_{p|N} \frac{1}{1-a_p p^{-s}}.$$

The above definition generalises to the case of an elliptic curve E defined over a number field K. Let v be a non-archimedean prime of K and denote by $\mathbf{N}_{K/\mathbb{Q}}v$ the norm of v. Let $\mathfrak{N}$ denotes the arithmetic conductor of E over K, that is an ideal of the ring of integer $\mathcal{O}_K$ of K. Define

$$a_v = \begin{cases} \mathbf{N}_{K/\mathbb{Q}}v+1-\#\bar{\mathcal{E}}_p(\mathbb{F}_v) & \text{if } v \text{ is a prime of good reduction,} \\ 0 & \text{if the reduction of } E \text{ at } v \text{ is additive,} \\ 1 & \text{if the reduction of } E \text{ at } v \text{ is split multiplicative,} \\ -1 & \text{if the reduction of } E \text{ at } v \text{ is non-split multiplicative.} \end{cases}$$

In this case the L-series of E over K is defined by the formula

$$L(E/K,s) = \prod_{v\nmid \mathfrak{N}} \frac{1}{1-a_v\mathbf{N}_{K/\mathbb{Q}}v^{-s}+\mathbf{N}_{K/\mathbb{Q}}v^{1-2s}} \prod_{v|\mathfrak{N}} \frac{1}{1-a_v\mathbf{N}_{K/\mathbb{Q}}v^{-s}}.$$

We give an example relating the values of the L-series of E over $\mathbb{Q}$ and its quadratic twist over a quadratic number field K and the value of the L-series of E over K.

Example 1.2.2. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and let write its Weirstrass equation $E : y^2 = x^3 + ax + b$ for some $a, b \in \mathbb{Z}$. Let K be a quadratic extension of $\mathbb{Q}$ of squarefree discriminant D. Assume that all the primes dividing N are split in K. Denote by E^K the quadratic twist of E, and recall that E^K is defined by the equation $Dy^2 = x^3+ax+b$. The arithmetic conductor of E^K is D^2N. Write ε_K for the quadratic Dirichlet character. It can be checked that the L-series of $L(E^K/\mathbb{Q},s)$ is given by the formula

$$L(E^K/\mathbb{Q},s) = \prod_{p\nmid N} \frac{1}{1-a_p\varepsilon_K(p)p^{-s}+\varepsilon_K(p)p^{1-2s}} \prod_{p|N} \frac{1}{1-a_p\varepsilon_K(p)p^{-s}}.$$

Now, write the product:

$$
\begin{aligned}
& L(E/\mathbb{Q},s)L(E^K/\mathbb{Q},s) = \\
= & \prod_{p\nmid N} \frac{1}{(1-a_p p^{-s}+p^{1-2s})(1-a_p\varepsilon_K(p)p^{-s}+\varepsilon_K(p)p^{1-2s})} \prod_{p|N} \frac{1}{(1-a_p\varepsilon_K(p)p^{-s})(1-a_p p^{-s})} \\
= & \prod_{v\nmid ND} \frac{1}{1-a_v \mathbf{N}_{K/\mathbb{Q}} v^{-s}+\mathbf{N}_{K/\mathbb{Q}} v^{1-2s}} \prod_{v|ND} \frac{1}{1-a_v \mathbf{N}_{K/\mathbb{Q}} v^{-s}} \\
= & L(E/K,s).
\end{aligned}
$$

i.e. we have a factorization

$$L(E/\mathbb{Q},s)L(E^K/\mathbb{Q},s) = L(E/K,s). \tag{1.2}$$

The following property of the L-series of an elliptic curve definite over $\mathbb{Q}$ was proved by Wiles [Wi] and Taylor-Wiles [TW] for semistable elliptic curves; the full result is contained in [BCDT].

Theorem 1.2.3 ([Wi], [TW],[BCDT])**.** *The L-series $L(E/\mathbb{Q},s)$ extends to an entire function over $\mathbb{C}$ and has a functional equation of the form*

$$\Lambda(E/\mathbb{Q},s) = (-1)^{\mathrm{sgn}E/\mathbb{Q}}\Lambda(E/\mathbb{Q},2-s)$$

where

$$\Lambda(E/\mathbb{Q},s) = (2\pi)^{-s}\Gamma(s)N^{s/2}L(E/\mathbb{Q},s).$$

Remark 1.2.4. Note that for the twisted elliptic curve E^K we have:

$$\Lambda(E^K/\mathbb{Q},s) = (2\pi)^{-s}\Gamma(s)N^{s/2}D^s L(E^K/\mathbb{Q},s).$$

The sign of the functional equation for E^K is given by

$$\mathrm{sgn}(E^K/\mathbb{Q}) = \mathrm{sgn}(E/\mathbb{Q})\varepsilon_K(-N). \tag{1.3}$$

In this way we can define also the sign of the L-function of E/K by using equation (1.2)

$$
\begin{aligned}
\mathrm{sgn}(E/K) &= \mathrm{sgn}(E/\mathbb{Q})\mathrm{sgn}(E^K/\mathbb{Q}) \\
&= \mathrm{sgn}(E/\mathbb{Q})^2\varepsilon_K(-N) \\
&= \varepsilon_K(-N) \\
&= \varepsilon_K(N)\varepsilon_K(-1) \\
&= -1.
\end{aligned}
$$

1.3 The Birch and Swinnerton-Dyer conjecture

The (conjectural) link between the Mordell-Weil group and the L-series associated to an elliptic curve is given by the Birch and Swinnerton-Dyer conjecture. In this section we define the invariants we need to state the conjecture. We start by stating the conjecture for elliptic curves defined over the rationals. Given an elliptic curve $E/\mathbb{Q}$ we associate to it the following invariants.

- The *real period* of E is defined as

$$\Omega_E := \int_{E(\mathbb{R})} |\omega_E|.$$

where ω_E is an invariant differential on a global minimal Weierstrass equation for E.

- The *Tamagawa number* at p is

$$c_p(E) := \#\left(E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)\right),$$

where $E_0(\mathbb{Q}_p)$ is the subgroup of $E(\mathbb{Q}_p)$ consisting of points which reduces to nonsingular points of $\bar{\mathcal{E}}_p$. Note in particular that $c_p(E) = 1$ if p is a prime of good reduction for E. Denote by $C_N(E)$ the product of all the Tamagawa numbers

$$C_N(E) = \prod_{p|N} c_p(E).$$

In our work, we also need the definition of the Tamagawa numbers of an abelian variety A. Let A be an abelian variety over a local field K with residue class field k. Let $\mathcal{A}$ be the Néron model of A over the ring of integer of K. Denote by $\mathcal{A}_k$ the closed special fiber of $\mathcal{A}$ that, in general, is not connected. Let $\mathcal{A}_k^0$ denote the geometric component of $\mathcal{A}$ containing the identity. The group $\Phi_{\mathcal{A}}(k) := \mathcal{A}_k/\mathcal{A}_k^0$ of connected components, is a finite group scheme over k. The Tamagawa number of $\mathcal{A}$ is $c_A = \#\Phi_{\mathcal{A}}(k)$. If A is defined over a global field K, define the local Tamagawa number at a place v of K as $c_v(A) := \#\Phi_{\mathcal{A}}(K_v)$ where K_v denotes the completion of K at v. Note that for an elliptic curve E the two definitions agree.

- The *regulator* $\mathrm{Reg}(E/\mathbb{Q})$ is the discriminant of the canonical Néron-Tate height pairing. To be more precise, Let $P_1, \ldots, P_r$ be a $\mathbb{Z}$-basis for $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$, then

$$\mathrm{Reg}(E/\mathbb{Q}) := \det(\langle P_i, P_j\rangle_{NT}). \tag{1.4}$$

We are now ready to state the following conjecture.

Conjecture 1.3.1 (Birch and Swinnerton-Dyer)**.** *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N.*

i) The equality

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = \mathrm{rnk}_{\mathbb{Z}}(E)$$

holds.

ii) Let

$$\mathrm{BSD}_r(E/\mathbb{Q}) := \frac{\mathrm{Reg}(E/\mathbb{Q}) \cdot \Omega_E \cdot C_N(E) \cdot \#\text{Ш}(E/\mathbb{Q})}{\#E(\mathbb{Q})^2_{\mathrm{tors}}}$$

and note that the dependence by r of the right side of the equation is hidden in the regulator. If $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = r$ then

$$\lim_{s\to 1} \frac{L(E/\mathbb{Q}, s)}{(s-1)^r} = \mathrm{BSD}_r(E/\mathbb{Q}).$$

For our work, it is interesting to give a version of the Birch and Swinnerton-Dyer conjecture for elliptic curves defined over a quadratic imaginary number field K. In this case we need to extend some definitions. First the period $\Omega_{E/K}$ is defined as follows: let ω be a Néron differential on E, then

$$\Omega_{E/K} := \int_{E(\mathbb{C})} \omega \wedge \bar{\omega}.$$

The regulator $\mathrm{Reg}(E/K)$ is defined again by the equation (1.4), with clear meaning of notations, in light of Remark 1.1.3.

Conjecture 1.3.2 (Birch and Swinnerton-Dyer over a quadratic number field.)**.** *Let E/K be an elliptic curve defined over a quadratic number field K of discriminant* $\mathrm{disc}\, K$*. Then:*

1. *the equality*
$$\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{rnk}_{\mathbb{Z}}(E)$$
holds

2. *Define*
$$\mathrm{BSD}_r(E/K) := \frac{\mathrm{Reg}(E/K) \cdot \Omega_{E/K} \cdot C_N(E)^2 \cdot \#Ш(E/K)}{\sqrt{|\,\mathrm{disc}\, K|} \cdot \#E(K)^2_{\mathrm{tors}}}. \tag{1.5}$$
If $\mathrm{ord}_{s=1} L(E/K, s) = r$ *then*
$$\lim_{s \to 1} \frac{L(E/K, s)}{(s-1)^r} = \mathrm{BSD}_r(E/K).$$

1.4 Modularity

Let $\mathcal{H}$ denotes the Poincarè complex upper plane, i.e. $\mathcal{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$. Let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N \text{ divides } c \right\}$$

be the Hecke congruence subgroup. $\Gamma_0(N)$ acts on $\mathcal{H}$ by Moebius transformations, i.e. according to the rule

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

To the quotient $\Gamma_0(N)\backslash\mathcal{H}$ it is possible to give a natual structure of Riemann surface.

Definition 1.4.1. A cusp form of weight k on $\Gamma_0(N)$ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that

- $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$
- for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ there exists an integer h such that f admit a so-called Fourier expansion
$$(c\tau + d)^{-k} f(\gamma\tau) = \sum_{n \geq 0} a_n e^{2\pi i \tau (n/h)} = \sum_{n \geq 0} a_n q^{n/h}$$

Denote by $S_k(\Gamma_0(N))$ the (finite-dimensional) $\mathbb{C}$-vector space of modular forms. We refer to N as the level of f.

The only case we are interested in is the case of $k = 2$.
Let $Y_0(N)$ denotes the moduli space of pairs (E, C) where E is an elliptic curve and C is a cyclic subgroup of E of order N.

It holds that $Y_0(N)(\mathbb{C})$ is isomorphic to $\mathcal{H}/\Gamma_0(N)$.

Definition 1.4.2. The modular curve $X_0(N)$ is the algebraic curve over $\mathbb{Q}$ obtained as compactification of $Y_0(N)$. In other words

$$X_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash\mathcal{H}^*$$

where $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$, and the action of $\Gamma_0(N)$ on $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \infty$ is given by:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{s}{r} = \frac{as + br}{cs + dr}$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \frac{a}{c}$$

It is possible to show that $X_0(N)(\mathbb{C})$ is a compact Riemann surface.

The vector space $S_2(\Gamma_0(N))$ is equipped with a nondegenerate Hermitian inner product known as Petersson scalar product defined as

$$(f_1, f_2) = \int_{\Gamma_0(N)\backslash\mathcal{H}} f_1(\tau)\overline{f_2(\tau)}dxdy. \tag{1.6}$$

It is also equipped with the action of the Hecke operators T_p indexed by the rational primes and defined by the formula

$$T_p f = \begin{cases} \frac{1}{p}\sum_{i=0}^{p-1} f\left(\frac{\tau+i}{p}\right) + pf(p\tau) & \text{if } p \nmid N \\ \\ \frac{1}{p}\sum_{i=0}^{p-1} f\left(\frac{\tau+i}{p}\right) & \text{if } p \mid N. \end{cases}$$

The Hecke operators act linearly on $S_2(\Gamma_0(N))$ and their effect on a q-expansion of a modular form $f = \sum_{n\geq 1} a_n q^n$ is given by

$$T_p f = \begin{cases} \sum_{p|n} a_n q^{n/p} + p\sum a_n q^{pn} & \text{if } p \nmid N \\ \\ \sum_{p|n} a_n q^{n/p} & \text{if } p \mid N. \end{cases}$$

It is useful to define the Hecke operators T_n for all the integers n, by equating the coefficients in the following formal identity:

$$\sum_{n\geq 1} T_n n^{-s} := \prod_{p\nmid N}(1 - T_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N}(1 - T_p p^{-s})^{-1}.$$

We denote by $\mathbb{T}$ the algebra generated over $\mathbb{Z}$ by the Hecke operators, and write $\mathbb{T}^0$ for the subalgebra generated by Hecke operators T_n with n prime to N.

Proposition 1.4.3. *The Hecke algebras $\mathbb{T}$ and $\mathbb{T}^0$ are finitely generated $\mathbb{Z}-$modules. Furthermore the rank of $\mathbb{T}$ is exactly the genus of $X_0(N)$.*

The operators in $\mathbb{T}^0$ are self-adjoint with respect to the Petersson scalar product. The space $S_2(\Gamma_0(N))$ decomposes as an orthogonal direct sum

$$S_2(\Gamma_0(N)) = \bigoplus_{\lambda} S_\lambda^0$$

taken over all $\mathbb{C}$-algebra homomorphisms $\lambda : \mathbb{T}^0 \to \mathbb{C}$ where S_λ^0 denotes the corresponding eigenspace in $S_2(\Gamma_0(N))$. Now, given a ring homomorphism $\lambda : \mathbb{T} \to \mathbb{C}$ defined on the full Hecke algebra $\mathbb{T}$ denote by S_λ its associate eigenspace. It holds the following.

Theorem 1.4.4 (Multiplicity one)**.** *The eigenspace S_λ attached to $\lambda : \mathbb{T} \to \mathbb{C}$ is one-dimensional.*

A modular form in $S_2(\Gamma_0(N))$ is said to be an *oldform* if it is a linear combination of functions of the form $f(d'z)$ with $f \in S_2(\Gamma_0(N/d))$ and d divides $d' > 1$. The *newspace* $S_2(\Gamma_0(N))^{\text{new}}$ if it is in the orthogonal complement of the space of oldforms, with respect to Petersson scalar product.

Theorem 1.4.5 (Atkin-Lehner)**.** *The Hecke algebra $\mathbb{T}$ acts semi-simply on $S_2(\Gamma_0(N))^{\text{new}}$ with one-dimensional eigenspaces. We have the decomposition*

$$S_2(\Gamma_0(N)) = S_2^{\text{old}}(\Gamma_0(N)) \bigoplus_{\lambda} f_\lambda.$$

Here the sum is taken over all algebra homomorphisms $\lambda : \mathbb{T} \to \mathbb{C}$ corresponding to eigenvectors in $S_2(\Gamma_0(N))^{\text{new}}$ and $f_\lambda(\tau) = \sum_{n\geq 1} \lambda(T_n) e^{2\pi\tau i n}$.

A simultaneous eigenvector f_λ is is called a *normalized eigenform* or simply a *newform* of level N.

To a newform of level N is attached the L-series

$$L(f, s) = \sum_{n\geq 1} a_n n^{-s},$$

where $a_n = a_n(f) = T_n f$. Note that by definition of the Hecke operators the L-series of f enjoys properties similar to those of the L-series attached to an elliptic curve.

Definition 1.4.6. An elliptic curve E defined over $\mathbb{Q}$ is modular if there is a nonconstant morphism defined over $\mathbb{Q}$, from $X_0(N)$ to E for some N.

The following results provide a link between elliptic curves and modular forms.

Theorem 1.4.7 (Faltings)**.** *Let E and E' be elliptic curves over $\mathbb{Q}$. Then the L-series $L(E/\mathbb{Q}, s)$ and $L(E'/\mathbb{Q})$ are equal if and only if E and E' are isogenous over $\mathbb{Q}$.*

Theorem 1.4.8 (Eichler-Shimura)**.** *Let f be a normalized eigenform of weight 2 for $\Gamma_0(N)$ with rational Fourier coefficients. There exists an elliptic curve E_f defined over $\mathbb{Q}$ such that:*

- *there is a nonconstant morphism $X_0(N) \to E_f$ defined over $\mathbb{Q}$*

- $L(E_f/\mathbb{Q}, s) = L(f, s)$ *up to finitely many Euler factors.*

Conversely, given a modular elliptic curve over $\mathbb{Q}$ *such that for some* N *there is a nonconstant morphism* $X_0(N) \to E$ *defined over* $\mathbb{Q}$*, then there is a weight 2 newform* f *as above and* E *is isogenous to* E_f *over* $\mathbb{Q}$*.*

Theorem 1.4.9 (Carayol)**.** *If* f *satysfies the hypotheses of the first part of Theorem 1.4.8, then thet L-series* $L(E_f/\mathbb{Q}, s)$ *and* $L(f, s)$ *are equal. Furthermore* N *is equal to* N_{E_f}*, the conductor of the curve* E_f*.*

Corollary 1.4.10. *If* E *is an elliptic curve over* $\mathbb{Q}$*, of conductor* N_E*. Then the following are equivalent:*

i. E *is modular;*

ii. for some N *there exists a newform* f *of weight 2 and level* N*, with rational Fourier coefficients, such that* E_f *is isogenous to* E *over* $\mathbb{Q}$*.*

iii. for some N *there exists a newform* f *of weight 2 and level* N *such that*

$$L(E/\mathbb{Q}, s) = L(f, s);$$

Furthermore, in any of the above statement, N *can be choosen to be the conductor* N_E*.*

Theorem 1.4.11 (Wiles [Wi], Taylor-Wiles [TW], Breuil-Conrad-Diamond-Taylor [BCDT])**.** *Every elliptic curve* E *defined over* $\mathbb{Q}$ *is modular.*

Remark 1.4.12. The map $\varphi_E : X_0(N) \to E$ is called modular parametrization. The proof of the modularity theorem is quite involved. The main step consists in constructing a morphism

$$f : \mathbb{T} \to \mathbb{Z}$$

with kernel $\mathcal{I}_f$ such that the elliptic curve E is isogenous to the quotient $J_0(N)/\mathcal{I}_f J_0(N)$, where $J_0(N)$ is the Jacobian variety of $X_0(N)$. The relations between the L-series follows from the existence of integral models for $X_0(N)$, combined with the Eichler-Shimura relations, stating that over the Jacobian $J_0(N)_{/\mathbb{F}_p}$

$$T_p = \mathrm{Frob}_p + \mathrm{Frob}_p^\vee$$

where Frob_p is the Frobenius morphism in characteristic p and $\mathrm{Frob}_p^\vee$ its transpose.

We briefly recall the construction of Eichler and Shimura in a more general setting. Given an eigenform f the Fourier coefficients of f are not in general rational numbers, but it can be shown that they are algebraic integers.

The proof of this fact relies ont the fact that the Hecke algebra $\mathbb{T}$ can be viewed as a subset of the endomorphisms of the Jacobian of $X_0(N)$. Let K_f be the totally real field $\mathbb{Q}(a_n(f))$ generated by the Fourier coefficients of f. Since the Hecke algebra $\mathbb{T}$ is a finitely generated $\mathbb{Z}$-module, it is a finite extension of $\mathbb{Q}$. Consider the map associating to each Hecke operator T_n the eigenvalue of a_n of T_n acting on f. Denote by $\mathcal{I}_f$ the kernel of the map induced by f on the Hecke algebra, i.e.

$$\mathcal{I}_f := \{T_n \in \mathbb{T} : T_n f = 0\}.$$

The kernel $\mathcal{I}_f$ is a $\mathbb{Z}$-module and we have the isomorphism

$$\mathbb{T}/\mathcal{I}_f \cong \mathbb{Z}[a_n(f)].$$

It is possible to associate to a cuspidal eigenform f the abelian variety $A_f := J_0(N)/\mathcal{I}_f J_0(N)$. Note that the definition makes sense since the Hecke algebra acts on the Jacobian of the modular curve. This construction furthermore holds on every number field K. It is not in general true that A_f is an elliptic curve, although it is true if we take $K = \mathbb{Q}$. Indeed the dimension of A_f is exactly the index of K_f in $\mathbb{Q}$. We summarize the results in the following theorem.

Theorem 1.4.13. *Let f be an eigenform of level N. Let K_f be as above. There exists a pair (A, ψ) that satisfies the following properties.*

i. The abelian variety A is defined over $\mathbb{Q}$ and has dimension $[K_f : \mathbb{Q}]$. Furthermore the map

$$J_0(N) \to A$$

is a surjective morphism defined over $\mathbb{Q}$.

ii. the map ψ is an isomorphism of K_f into $\mathrm{End}(A) \otimes \mathbb{Q}$. For every n the Hecke operator T_n act on A as multiplication by a_n, in other words, $\psi(a_n)$ is the restriction to A of the Hecke operator acting on the Jacobian $J_0(N)$.

iii. There is an equality between the L functions

$$L(A/\mathbb{Q}, s) = L(f, s).$$

1.5 Heegner points

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and let $K = \mathbb{Q}(\sqrt{-D})$ for where $D > 0$ Assume for semplicity that $D \neq 3, 4$. We choose K such that all prime factors of N are split in K. Let $\mathcal{O}_K$ be the ring of integers of K. It follows that $N\mathcal{O}_K = \mathcal{N}\bar{\mathcal{N}}$ for an ideal $\mathcal{N}$ of $\mathcal{O}_K$ with $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$.

By the modularity theorem, there exists a modular parameterization $\varphi_E : X_0(N) \to E$ of minimal degree. Let $\mathcal{N}^{-1}$ be the fractional ideal of $\mathcal{O}_K$ for which $\mathcal{N}\mathcal{N}^{-1} = \mathcal{O}_K$. $\mathcal{O}_K$ and $\mathcal{N}$ can be viewed as $\mathbb{Z}$-lattices of rank two in $\mathbb{C}$. The map

$$\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}^{-1}$$

is a cyclic isogeny of degree N between the elliptic curves $\mathbb{C}/\mathcal{O}_K$ and $\mathbb{C}/\mathcal{N}^{-1}$. This isogeny corresponds to a complex point $x_1 \in X_0(N)(\mathbb{C})$. According to the theory of complex multiplication, the point x_1 is defined over the Hilbert class field H of K.

More generally, for an integer c prime to N, let $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ be the order of conductor c in $\mathcal{O}_K$ and let $\mathcal{N}_c = \mathcal{N} \cap \mathcal{O}_c$, which is an invertible ideal of $\mathcal{O}_c$. Then $\mathcal{O}_c/\mathcal{N}_c \simeq \mathbb{Z}/N\mathbb{Z}$ and the map $\mathbb{C}/\mathcal{O}_c \to \mathbb{C}/\mathcal{N}_c^{-1}$ is a cyclic isogeny of degree N. Thus, it defines a point $x_c \in X_0(N)(\mathbb{C})$. By the theory of complex multiplication, this point is defined over the ring class field $K[c]$ of conductor c over K. Note in particular that if we take $c = 1$ then $K[1] = H$.

The modular parametrization $\varphi_E : X_0(N) \to E$ allows us to obtain points on the elliptic curve as follows: let

$$P_c = \varphi_E(x_c) \in E(K[c]).$$

Let $P_K = \mathrm{Tr}_{H/K}(x_1)$. P_K is called the Heegner point for the discriminant D. The Heegner point P_K is only well defined up to sign and torsion, namely if $\mathcal{N}'$ is another ideal with $\mathcal{O}/\mathcal{N}' \simeq \mathbb{Z}/N\mathbb{Z}$ then the new Heegner point differs from P_K by a sign change and a rational torsion point.

1.6 The Gross-Zagier formula

Let E be an elliptic curve of conductor N, associated via the Eichler-Shimura construction to a newform of weight 2 of level N. Let $\varphi_E : X_0(N) \to E$ be a modular parametrization of minimal degree. Let ω be a Néron differential. Its pullback has the form

$$\varphi^*(\omega) = \tilde{m} \cdot \pi i f(\tau) d\tau. \tag{1.7}$$

The *Manin constant* m is the absolute value of the constant $\tilde{m}$ appearing in equation (1.7). The Manin constant satisfies the properties stated in the next proposition

Proposition 1.6.1. *Let m be the Manin constant of an elliptic curve E of conductor N, and let p denotes a prime Then:*

- *the Manin constant is an integer (Edixhoven, [Ed], Prop.2);*
- *if p divides the Manin constant, then p^2 divides $4N$ (Mazur, [Ma1], Cor. 4.1);*
- *if the Manin constant is a multiple of 4, then 4 divides N (Raynaud, see [AU], Prop. 3.1);*
- *if p divides the Manin constan, then p also divide N (Abbes-Ullmo [AU], Theorem A).*

Let K be a quadratic imaginary field as above. Let x_1 be a Heegner point of discriminant D on $X_0(N)$. The point

$$P_K := \sum_{\sigma \in \mathrm{Gal}(H/K)} \varphi(x_1^\sigma) = \sum_{\sigma \in \mathrm{Gal}(H/K)} \varphi(x_1)^\sigma$$

belongs to $E(K)$.

Theorem 1.6.2 (Gross-Zagier)**.** *The equality*

$$L'(E/K, 1) = \frac{\Omega_{E/K} \cdot h_E(P_K)}{m^2 \cdot \sqrt{\mathrm{disc}\, K}}$$

holds. In particular $L'(E/K, s)$ is zero if and only if P_K is a torsion point in $E(K)$.

Remark 1.6.3. The result of Gross-Zagier has been generalized by Zhang [Zh] to the case of Shimura curves.

1.7 The result of Kolyvagin

An evidence in the direction of the validity of the Birch and Swinnerton-Dyer conjecture is due to Kolyvagin [Ko]. Let K be a quadratic imaginary field, and E as above an elliptic curve defined over $\mathbb{Q}$ of discriminant N.

Hypothesis 1.7.1. We say that the field K satisfies the *Heegner hypothesis* if all primes ℓ dividing N are split in the extension $K/\mathbb{Q}$.

Theorem 1.7.2 (Kolyvagin)**.** *If the Heegner point P_K has infinite order in $E(K)$ then*

i. the group $E(K)$ has rank 1;

ii. the group $\text{Ш}(E/K)$ is finite and its order divides $t[E(K) : \mathbb{Z}P_K]^2$ for some integer $t \geq 1$.

Combining the results of Gross-Zagier and Kolyvagin we obtain the following result.

Theorem 1.7.3 (Gross-Zagier-Kolyvagin)**.** *Let $E/\mathbb{Q}$ be an elliptic curve definite over $\mathbb{Q}$ and such that $\text{ord}_{s=1}L(E/\mathbb{Q}, s) \leq 1$. Then the Shafarevich group $\text{Ш}(E/\mathbb{Q})$ is finite and the rank of the elliptic curve coincide with the order of vanishing of the associated L-function, i.e. the equality*

$$\text{rnk}(E(\mathbb{Q})) = \text{ord}_{s=1}L(E/\mathbb{Q}, s)$$

holds.

Sketch of the proof. Recall that $\text{sgn}(E/\mathbb{Q})$ denotes the sign in the functional equation of $L(E/\mathbb{Q}, s)$, given in Theorem 1.4.11. We have two different cases to consider: the first is when $\text{sgn}(E/\mathbb{Q})$ is 1 while in the second case it is equal to 1.

Case 1. Assume that $\text{sgn}(E/\mathbb{Q}) = -1$ By a result of Waldspurger [Wa] (but see also Murty-Murty [MM]) there exist infinitely many quadratic imaginary fields K having Dirichlet character ϵ such that:

(a) $\epsilon(\ell) = 1$ if ℓ divides N;

(b) $\epsilon(-1) = -1$;

(c) $L(E^K/\mathbb{Q}, 1)$ is nonzero.

The first two properties in particular implies that $L(E^K/\mathbb{Q}, s)$ vanishes at to even order at $s = 1$. Indeed, the existence of the factorisation given in equation (1.2)

$$L(E/K, 1) = L(E/\mathbb{Q}, 1)L(E^K/\mathbb{Q}, 1)$$

combined with the Heegner hypothesis, together imply that $L(E/K, s)$ vanishes at odd order at $s = 1$.

Case 2. Assume that $\text{sgn}(E/\mathbb{Q}) = 1$. For all quadratic extensions having Dirichlet character satisfying conditions (a) and (b), $L(E^K/\mathbb{Q}, 1)$ vanishes, for parity reasons. In this case by the results of Murty-Murty [MM], there exists a quadratic imaginary field we denote again by K (with a little abuse of notations), such that

$$L'(E^K/\mathbb{Q}, 1) = 0.$$

In both cases, we have that

- K satisfies the Heegner hypothesis with respect to E;
- the order of $L(E/K, s)$ at $s = 1$ is 1, so by definition the derivative of the L-function, $L'(E/K, 1)$ is nonzero.

Theorem 1.6.2 implies the existence of a non-torsion Heegner point P_K. By the result of Kolyvagin (Theorem 1.7.2) $E(K)$ has rank one, hence the index $[E(K) : \mathbb{Z}P_K]$ and the Shafarevich group $\text{Ш}(E/K)$ are finite. It is possible to show that, up to torsion, P_K belongs to $E(\mathbb{Q})$ if and only if $\text{sgn}(E/\mathbb{Q}) = -1$ (For details see [Gr]). It follows that the rank of $E(\mathbb{Q})$ is equal to the order of vanishing of $L(E/\mathbb{Q}, s)$ at $s = 1$. By a general fact of cohomology, the natural map from $\text{Ш}(E/\mathbb{Q})$ to $\text{Ш}(E/K)$ induced by restriction has finite kernel (See [Ko], Corollary B). Thus the finiteness of $\text{Ш}(E/K)$ implies the finiteness of $\text{Ш}(E/\mathbb{Q})$. □

Remark 1.7.4. The proof of the above-mentioned Corollary B of [Ko] is based the following general fact of cohomology. The kernels of the maps sending

$$\text{Ш}(E/\mathbb{Q}) \to \text{Ш}(E/K)$$

and

$$\text{Ш}(E^K/\mathbb{Q}) \to \text{Ш}(E/K)$$

are contained respectively in $\text{H}^1(K/\mathbb{Q}, E(\mathbb{Q}))$ and $\text{H}^1(K/\mathbb{Q}, E^K(\mathbb{Q}))$, that are 2-torsion groups. In particular note that

$$\frac{\#\text{Ш}(E/K)}{\#\text{Ш}(E/\mathbb{Q}) \cdot \#\text{Ш}(E^K/\mathbb{Q})} = 2^\alpha$$

for some $\alpha \in \mathbb{Z}$.

1.8 An equivalent statement of the Birch and Swinnerton-Dyer for analytic rank one

The following result, stated in [MC] provides an equivalent version of the Birch and Swinnerton-Dyer conjecture for elliptic curves with analityc rank one. We write a detailed proof for completeness. Let $E/\mathbb{Q}$ be an elliptic curve of squarefree conductor N. Assume that E has analytic rank one, and let P_E be a generator for its Mordell-Weil group modulo torsion. Let K be a quadratic imaginary field satisfying the Heegner hypothesis. From the factorization (1.2):

$$L(E/K, s) = L(E/\mathbb{Q}, s)L(E^K/\mathbb{Q}, s)$$

we have that:

- $L(E^K/\mathbb{Q}, s)$ does not vanish at $s = 1$;
- the equality

  $$L'(E/K, 1) = L'(E/\mathbb{Q}, 1)L(E^K/\mathbb{Q}, 1) \tag{1.8}$$

  holds.

In particular, combining the Birch and Swinnerton-Dyer conjecture for $E/\mathbb{Q}$ and $E^K/\mathbb{Q}$, we have:

$$\mathrm{BSD}_1(E/K) := \mathrm{BSD}_1(E/\mathbb{Q})\,\mathrm{BSD}_0(E^K/\mathbb{Q}). \tag{1.9}$$

Writing explicitely the right hand side of the equation we have the conjectural equality:

$$\mathrm{BSD}_1(E/K) = \frac{h_E(P_E)\cdot\Omega_E\cdot\#\text{Ш}(E/\mathbb{Q})\cdot C_N(E)}{\#E(\mathbb{Q})^2_{\mathrm{tors}}}\cdot\frac{\Omega_{E^K}\cdot\#\text{Ш}(E^K/\mathbb{Q})\cdot C_N(E^K)}{\#E^K(\mathbb{Q})^2_{\mathrm{tors}}}. \tag{1.10}$$

The Heegner hypothesis implies that $C_N(E/K)=C_N(E)^2$, since all primes dividing N are split in K. Furthermore, it is possible to show that:

$$\Omega_{E/K} = \frac{\Omega_E\cdot\Omega_{E^K}}{\sqrt{|\operatorname{disc} K|}}.$$

Remark 1.8.1. Comparing equation (1.10) with the formula (1.11) (that we write again for ease of the reader)

$$\mathrm{BSD}_1(E/K) = \frac{\mathrm{Reg}(E/K)\cdot\Omega_{E/K}\cdot C_N(E)^2\cdot\#\text{Ш}(E/K)}{\sqrt{|\operatorname{disc} K|}\cdot\#E(K)^2_{\mathrm{tors}}} \tag{1.11}$$

one can observe that the statement is compatible with the equation (1.8) and the properties of all the invariants.

See [GZ] pages 310-311 for details.

Theorem 1.8.2. *Let $E/\mathbb{Q}$ be an elliptic curve of analytic rank one, and let K be an imaginary quadratic field as above. Then the Birch and Swinnerton-Dyer conjecture for E/K is equivalent to the conjectural equality*

$$\#\text{Ш}(E/K)\cdot C_N(E)^2\cdot m^2 = [E(K):\mathbb{Z}P_K]^2.$$

Proof. Let P_i's be a basis for $E(K)$ modulo torsion. The following equality

$$\frac{\mathrm{Reg}(E/K)}{\#E(K)^2_{\mathrm{tors}}} = \frac{\mathrm{disc}\langle P_i,P_j\rangle_{NT}}{\#E(K)^2_{\mathrm{tors}}} = \frac{\det\langle P_i,P_j\rangle_{NT}}{[E(K):\sum\mathbb{Z}P_i]^2}$$

holds. Since the analytic rank of E is equal to one, by definition

$$\langle P_K,P_K\rangle_{NT} = h_E(P_K).$$

Hence the equality (1.11) can be written as:

$$\mathrm{BSD}_1(E/K) = \frac{h_E(P_K)\cdot\Omega_{E/K}\cdot C_N(E)^2\cdot m^2\cdot\#\text{Ш}(E/K)}{\sqrt{|\operatorname{disc} K|}\cdot[E(K):\mathbb{Z}P_K]^2}.$$

The Gross-Zagier formula for elliptic curves of analytic rank one, implies that

$$L'(E/K,1) = \frac{h_E(P_K)\cdot\Omega_{E/K}}{m^2\sqrt{|\operatorname{disc} K|}}.$$

The Birch and Swinnerton-Dyer conjecture predicts the equality

$$\mathrm{BSD}_1(E/K) = L'(E/K, 1),$$

that reduces to

$$\#\text{Ш}(E/K) \cdot C_N(E)^2 \cdot m^2 = [E(K) : \mathbb{Z}P_K]^2. \tag{1.12}$$

□

Remark 1.8.3. As can be easily seen by writing equation (1.17) in the form

$$\#\text{Ш}(E/K) = \left(\frac{[E(K) : \mathbb{Z}P_K]}{C_N(E) \cdot m} \right)^2,$$

the order of $\text{Ш}(E/K)$ is a square. This fact is known in general under the hypotesis of fineness of the Shafarevich-Tate group, by a result of Cassels [Ca]. In our setting $\text{Ш}(E/K)$ is finite by the above-mentioned result of Kolyvagin. The comparison of these assertions provides an evidence of the validity of the Birch and Swinnerton-Dyer conjecture.

Kolyavagin in [Ko] has proved the validity of the following result.

Theorem 1.8.4. *Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ an imaginary quadratic field satisfying the Heegner hypothesis for E. Let P_K be an Heegner point in $E(K)$. If P_K has finite order, or equivalently $L'(E/K, 1)$ does not vanish, then the following quality*

$$\#\text{Ш}(E/K) \mid t \cdot [E(K) : \mathbb{Z}P_K]^2$$

holds, where t is an integer such that a prime p divides t if and only if one of the following condition holds:

- *$p = 2$;*
- *the representation $\bar{\rho}_{E,p}$ of the absolute Galois group $G_{\mathbb{Q}}$ attached to $E[p]$ is not surjective.*

1.9 A theorem of Skinner and Urban

In their recent paper [SU] Skinner and Urban have proved, under suitable hypotheses, the validity of the p-part of the Birch and Swinnerton-Dyer formula for elliptic curves. In this section we briefly recall their results. The result of [SU] is consequence of a result of Morel and Shin asserting the existence of four-dimensional p-adic representations associated with certain cuspidal automorphic representations of the unitary group $U(2, 2)$, for details see [SU] page 99.

The result we need is a consequence of the so-called Iwasawa main Conjecture. We start fixing notations and recalling definitions, that are given in details in [SU]. The first object we need to define is the characteristic ideal.

Definition 1.9.1. A *divisorial ideal* is an ideal that is equal to the intersection of all principal ideals containing it.

For example, any principal ideal is divisorial. Let A be a noetherial normal domain. Of $Q \subset A$ is a prime ideal of height one, denote by $\mathrm{ord}_Q(A)$ the essential valuation attached to Q. Any divisorial ideal is hence of the form

$$I = \{x \in A : \mathrm{ord}_Q(x) \geq m_Q, \text{for all } Q \text{ ideal of height one}\},$$

where m_Q are non-negative integer and only finitely many of them are positive. T he integers m_Q are well defined and uniquely determined. Let $\mathrm{ord}_Q(I) := m_Q$. In this case, we observe that A_Q is a discrete valuation ring and that $\mathrm{ord}_Q(I)$ is exactly the valuation of any generator of IA_Q. If I and J are two divisorial ideal, then $\mathrm{ord}_Q(J)$ is greater of equal to $\mathrm{ord}_Q(J)$ for all primes ideal Q of height one if and only if I contains J. In particular if I is divisorial an x belongs to A, then the ideal (x) generated by x contains I if and only if $\mathrm{ord}_Q(I) \geq \mathrm{ord}_Q(I)$ for all prime ideals Q of heigth one.

Definition 1.9.2. Let A be a Noetherian normal domain and X a finite A-module. The *characteristic ideal* of X is

$$\mathrm{Ch}_A(X) = \{x \in A : \mathrm{ord}_Q(x) \geq \mathrm{lenght}_{A_Q}(X_Q), \text{for all prime ideals } Q \text{ of height one}\}$$

Note that it possible that $\mathrm{lenght}_{A_Q}(X_Q)$ is infinite.

In what follows:

- p is an odd prime;
- $\iota : \mathbb{C} \cong \mathbb{C}_p$ is a fixed isomorphism;
- $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$;
- $\mathbb{Q}_\infty \subset \mathbb{Q}(\mu_{p^\infty})$ is the cyclotomic $\mathbb{Z}p$-extension of $\mathbb{Q}$;
- $\Gamma_{\mathbb{Q}} = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$;
- $\Lambda_{\mathbb{Q}} = \mathbb{Z}_p[[\Gamma_{\mathbb{Q}}]]$ is the Iwasawa algebra;
- for any $\mathbb{Z}_p$- algebra A define $\Lambda_A = \Lambda_{A,\mathbb{Q}} = \Lambda_{\mathbb{Q}} \otimes_{Z_p} A$;
- $\Psi = \Psi_{\mathbb{Q}} : G_{\mathbb{Q}} \to \Lambda_{\mathbb{Q}}^\times$ is the composition $G_{\mathbb{Q}} \to \Gamma_{\mathbb{Q}} \to \Lambda_{\mathbb{Q}}^\times$ (where the first map is surjective and the second is injective);
- $\varepsilon_{\mathbb{Q}}$ is a character of $\mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times$ that is the normalization, using the (geometric) Frobenius elements, of the compositum of $\Psi_{\mathbb{Q}}$ with the reciprocity map of class field theory (see page 15 of [SU] for details);
- ε is the cyclotomic character giving the (canonical) isomorphism $\mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \cong \mathbb{Z}_p^\times$;
- $\gamma \in \Gamma$ is the topological generator such that $\varepsilon(\gamma) = 1 + p$;
- for any $\zeta \in \mu_{p^\infty}$ and integer k, $\psi_{k,\zeta}$ is the finite order character of $\mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times$ that is the composition of $\Psi_{\mathbb{Q}}$ with the map $\Lambda_{\mathbb{Q}}^\times \to \mathbb{C}_p^\times$, mapping γ to $\zeta(p+1)$;
- ω is the Teichmuller character;

- $f = \sum_{n\geq 1} a_n q^n \in S_k(N, \psi_0)$ for $k \geq 2$ is a cuspidal eigenform with character ψ_0 of $(\mathbb{Z}/N\mathbb{Z})^\times$;
- L is a finite extension of $\mathbb{Q}_p$ containing all the Fourier coefficients of f and $\mathcal{O}_L$ is its ring of integers.

Assume that f is ordinary at p, i.e. a_p is invertible in the ring of integer of L. Denote by $\rho_f : G_\mathbb{Q} \to \mathrm{Aut}_L V_f$ the two dimensional Galois representation attached to f. There exists a L-line $V_f^+ \subset V_f$, stable under the action of the Galois group $G_{\mathbb{Q}_p}$ and such that V_f/V_f^+ is unramified. Let $T_f \subset V_f$ be a $\mathcal{O}_L$ lattice, stable for the action of $\Gamma_\mathbb{Q}$ and denote by T_f^+ the intersection of T_f with V_f^+. We define the Selmer group and the associated characteristic ideal.

Definition 1.9.3. Denote by $\Lambda^*_{\mathcal{O}_L} = \mathrm{Hom}_{\mathbb{Z}_p}(\Lambda_{\mathcal{O}_L}, \mathbb{Q}_p/\mathbb{Z}_p)$ the Pontryagin dual and use the notation $\Lambda^*_{\mathcal{O}_L}(\Psi^{-1})$ to mean that the Galois action is given by the character Ψ^{-1}.

$$\begin{aligned} \text{(1.13)}\ \mathrm{Sel}_L(T_f) &= \ker\{\mathrm{H}^1(\mathbb{Q}, T_f \otimes_{\mathcal{O}_L} \Lambda^*_{\mathcal{O}_L}(\Psi^{-1})) \to \\ \text{(1.14)} &\to \mathrm{H}^1(I_p, (T_f/T_f^+) \otimes_{\mathcal{O}_L} \Lambda^*_{\mathcal{O}_L}(\Psi^{-1})) \times \prod_{\ell\neq p} \mathrm{H}^1(I_\ell, T_f \otimes_{\mathcal{O}_L} \Lambda^*_{\mathcal{O}_L}(\Psi^{-1})\}. \end{aligned}$$

Let

$$X_L(T_f) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_L(T_f), \mathbb{Q}_p/\mathbb{Z}_p)$$

and

$$\mathrm{Ch}_{f,\mathbb{Q}} = \mathrm{Ch}_{\Lambda_\mathbb{Q},\mathcal{O}_L}(X_L(T_f)).$$

Let $0 < p < k-2$ be an integer, fix a p^{t-1}-th root of unity. We assume, to simplify our exposition, that ζ is different from 1, but the result stated in [SU] holds also in that case. Define the *algebraic part of a special value* for f as:

$$L_{\mathrm{alg}}(f, \psi_\zeta^{-1}\omega^n, n+1) := a_p(f)^{-1} \frac{p^{t(n-1)} n! L(f, \psi_\zeta^{-1}, \omega^n, n+1)}{(-2\pi i)^n \tau(\psi_\zeta^{-1}\omega^n)\Omega_f^{(\mathrm{sgn}(-1)^m)}}$$

where:

- $a_p(f)$ is the p-adic root of the polynomial $x^2 - a_p x + p^{k+1}\psi_0$;
- $\tau(\psi)$ is the Gauss sum for ψ;
- $\Omega^\pm$ are Hida canonical periods.

The p-adic L-function is an element $\mathcal{L}_{f,\mathbb{Q}}$ of $\Lambda_{\mathbb{Q},\mathcal{O}_L}$ defined by the following interpolation property. If

$$\phi_{n,\zeta} : \Lambda_{\mathcal{O}_L} \to \mathcal{O}_L(\zeta),$$

is the $\mathcal{O}_L$ homomorphism sending γ to $\zeta(p+1)$ then

$$\phi_{n,\zeta}(\mathcal{L}_{f,\mathbb{Q}}) = L_{\mathrm{alg}}(f, \psi_\zeta^{-1}\omega^n, n+1)$$

for $0 < n < k-2$.

We can state the Iwasawa Main Conjecture for f.

Conjecture 1.9.4 (Iwasawa Main Conjecture)**.** *The module $X_L(T_f)$ is a finite $\Lambda_{\mathbb{Q},\mathcal{O}_L}$-module and $\mathrm{Ch}_{f,\mathbb{Q}}$ is generated by $\mathcal{L}_{f,\mathbb{Q}}$.*

Skinner and Urban in [SU], using a previuos result of Kato [Ka] proved the following result.

Theorem 1.9.5 (Skinner-Urban)**.** *Let f be a newform of level N. Suppose that*

i. f has weight 2 and trivial character;

ii. f has good ordinary reduction at p;

iii. the residual representation $\bar{\rho}_f$ is irreducible;

iv. for some ℓ different from p and dividing N exactly $\bar{\rho}_f$ is ramified at ℓ.

Then the Iwasawa Main Conjecture holds in $\Lambda_{\mathbb{Q},\mathcal{O}_L} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Suppose furthermore that T_f admits an $\mathcal{O}_L$ basis such that the image of ρ_f contains $\mathrm{SL}_2(\mathbb{Z}_p)$. Then the Iwasawa Main Conjecture is true in $\Lambda_{\mathbb{Q}_{\mathcal{O}_L}}$.

This result has interesting application to the Birch and Swinnerton-Dyer Conjecture, in particular Skinner and Urban, following an idea of Mazur, proved the following result:

Theorem 1.9.6 (Skinner-Urban)**.** *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Denote by $\bar{\rho}_{E,p}$ the representation of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $E[p]$. Suppose that*

1. E has good ordinary reduction at $p > 7$;

2. there exists a prime $q \neq p$ such that $q \,||\, N$ and $\bar{\rho}_{E,p}$ is ramified at q;

3. the image of the representation $\bar{\rho}_{E,p}$ contains $\mathrm{SL}_2(\mathbb{F}_p)$;

4. $L(E/\mathbb{Q}, 1) \neq 0$;

then the equality

$$\mathrm{ord}_p\left(\frac{L(E/\mathbb{Q},1)}{\Omega_E}\right) = \mathrm{ord}_p(\#Ш(E/\mathbb{Q}) \cdot C_N)$$

holds.

The assumption on f are satisfied, for example, by semistable elliptic curves $E/\mathbb{Q}$, for any prime $p \geq 11$ of good ordinary reduction for E.

The result of Skinner and Urban is actually stronger. Let g be a modular form of level N, and suppose that there is a maximal ideal $\mathfrak{p}$ of the ring $\mathcal{O}_g$ of Fourier coefficients of g such that the completion of $\mathcal{O}_g$ at $\mathfrak{p}$ is isomorphic to $\mathbb{Z}_p$. Let K be an imaginary quadratic number field of of discriminant prime to N such that all the prime divisors of N are split in K.

Let A_g/K be the abelian variety attached to g by the Eichler-Shimura construction. Fix an integer n and consider the Selmer group $\mathrm{Sel}_{\mathfrak{p}^n}(A_g/K)$ defined in Section 1.1.1. Let

$$\mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K) = \varinjlim_k \mathrm{Sel}_{\mathfrak{p}^k}(A_g/K).$$

As discussed by Skinner in [Sk] the definition of the Selmer groups $\mathrm{Sel}_{\mathfrak{p}^n}(A_g/K)$ and the definition given by equation (1.13) coincides, since both coincide with the Bloch-Kato definition of the Selmer groups.

Theorem 1.9.7. *Let $g \in S_2(\Gamma_0(N))$ be a weight-two newform. Assume that g satisfies all the assumption of Theorem 1.9.5 and that there is a maximal ideal $\mathfrak{p}$ of the ring $\mathcal{O}_g$ of Fourier coefficients of g such that the completion of $\mathcal{O}_g$ at $\mathfrak{p}$ is isomorphic to $\mathbb{Z}_p$. If $L(g/K,1)$ is different from zero, then*

$$\mathrm{ord}_p\left(L(g/K,1)/\Omega_g\right) = \mathrm{lenght}_{\mathcal{O}_\mathfrak{p}} \mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K) + \prod_{\ell|N} t_g(\ell)$$

where $t_g(\ell)$ is an integer called Tamagawa exponent *at ℓ attached to g.*[1]

1.10 Reduction of the Birch and Swinnerton-Dyer conjecture for elliptic curves of analytic rank one

Let $E/\mathbb{Q}$ be an elliptic curve of squarefree conductor N. Let $p \geq 11$ be a prime of ordinary good reduction for E. Assume that E has analytic rank one.

Theorem 1.10.1 (Mazur, [Ma2], Theorem 4)**.** *Let $E/\mathbb{Q}$ be a semi-stable elliptic curve and $p \geq 11$ be a prime number. Then the representation $\bar{\rho}_{E,p} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is surjective.*

The following result is a reformulation of Lemma 2.2 of [BD], the second part of the statement, as pointed out by Bertolini and Darmon, is a consequence of Ribet level-lowering theorem [Ri2].

Lemma 1.10.2. *Assume that p does not divide the minimal degree of a modular parametrization $\varphi_E : X_0(N) \to E$. The cuspform associated with E is not congruent modulo p to modular forms of lower level. Furthermore p does not divide the Tamagawa numbers of E.*

Theorem 1.10.3. *Let $E/\mathbb{Q}$ be an elliptic curve of squarefree conductor N. Assume that E has analytic rank one, and write P_E for a generator of the Mordell-Weil group of E modulo torsion. Let $p \geq 11$ a prime of good ordinary reduction for E and assume that p does not divide the minimal degree of a modular parametrization $\varphi_E : X_0(N) \to E$. Let K be a quadratic imaginary field satisfying the Heegner hypothesis, and let P_K be a generator of $E(K)$ modulo torsion. Assume the following equality:*

$$2\mathrm{ord}_p[E(K) : \mathbb{Z}P_K] = \mathrm{ord}_p \#\text{Ш}(E/K). \tag{1.15}$$

Then the equality

$$\mathrm{ord}_p\left(\frac{L'(E/\mathbb{Q},1)}{\Omega_E \cdot h_E(P_E)}\right) = \mathrm{ord}_p\left(\text{Ш}(E/\mathbb{Q}) \cdot C_N(E)\right) \tag{1.16}$$

holds.

Proof. In Theorem 1.8.2 we showed that the Birch and Swinnerton-Dyer conjecture for E/K is equivalent to the equality:

$$\#\text{Ш}(E/K) \cdot C_N(E)^2 \cdot m^2 = [E(K) : \mathbb{Z}P_K]^2. \tag{1.17}$$

[1] We postpone a detailed definition of the Tamagawa exponent to the Section 2.5.4

By equation (1.8)

$$L'(E/K,1) = L'(E/\mathbb{Q},1)L(E^K/\mathbb{Q},1).$$

the validity of the p-part of the Birch and Swinnerton-Dyer conjecture for $E/\mathbb{Q}$ follows from the validity of the p-part of equation (1.17) combined with the p-part of the Birch and Swinnerton-Dyer conjecture for $E^K/\mathbb{Q}$. First, note that $E^K/\mathbb{Q}$, in light of Theorem 1.10.1 statisfies the assumption of Theorem [SU], in particular the p-part of the Birch and Swinnerton-Dyer conjectrure holds for $E^K/\mathbb{Q}$. By Lemma 1.10.2 p does not divide $C_N(E)$. Furthermore by Proposition 1.6.1 p does not divide the Manin constant m. Hence our assumptions implies the p-part of the Birch and Swinnerton-Dyer conjecture for $E/\mathbb{Q}$. □

Remark 1.10.4. Theorem 1.8.4 combined with the Theorem 1.10.1 imply that we only have to show that

$$2\mathrm{ord}_p([E(K) : \mathbb{Z}P_K]) \leq \mathrm{ord}_p(\#Ш(E/K)).$$

1.11 Modular forms on quaternion algebras and the Jacquet-Langlands correspondence

1.11.1 Quaternion algebras and Eichler orders

A quaternion algebra B over a field F is a 4-dimensional central simple algebra over F. Assuming that the characteristic of F is not 2, then any quaterion algebra is isomorphic to

$$\left(\frac{a,b}{F}\right) := F \oplus Fi \oplus Fj \oplus Fk, \quad \text{where } i^2 = a, j^2 = b, ij = -ji = k,$$

for some $a, b \in F^\times$. B is split over F is said to be *split* if it is isomorphic to $M_2(F)$. Similarly if K is an extension field of F then B is split over K if $B \otimes_F K$ is a split quaternion algebra over K.

Over the reals and $\mathbb{Q}_p$ or more in general any local field L, there are (up to isomorphism) exactly two quaterion algebras: $M_2(L)$ and the algebra of Hamilton quaternions.

More interesting is the classification of quaternions algebras over number fields. For any place v of F let F_v denote the completion of F at v and define $B_v := B \otimes_F F_v$. Again if B_v is a split quaternion algebra we say that B splits at v, otherwise we say it is *ramified*.

Consider a finite set S of places of $\mathbb{Q}$. It can be proved that there exists a unique (up to isomorphism) quaternion algebra ramified only at the places of S if and only if the cardinality of S is even.

Let Z be a finitely generated subring of F.

Definition 1.11.1. A *Z-order in B* is a subring of B that is a free Z-module of rank 4. It is *maximal* if it is not contained in any larger Z-order. An *Eichler Z-order* R is the intersection of two maximal Z orders. Writing $R := R_1 \cap R_2$, the *level* of R is the index of R as Z-module in either R_1 or R_2.

It is possibile to show that the above notion of level does not depend to the choice of the orders R_1 and R_2 defining R. Any conjugate of a maximal order is also a maximal order, hence the best situation is when a maximal order is unique up to conjugation by elements of $B^\times$.

Definition 1.11.2. We say that B and Z satisfy the *Eichler condition* if there is at least one archimedean prime or one prime invertible in Z at which Z is split.

Proposition 1.11.3. *If B and Z satisfy the Eichler condition then any two maximal Z-orders of B are conjugate, and similarly any two Eichler Z-orders of the same level are conjugate.*

A good reference for an explaination of the proof is [Vi]. We recall the main steps in order to fix the notation for the following sections. Denote by $\hat{\mathbb{Z}}$ the profinite completion of $\mathbb{Z}$ and by $\hat{\mathbb{Q}} := \hat{\mathbb{Z}} \otimes \mathbb{Q}$ the ring of finite rational adèles. If R is an Eichler order of level N in B denote by

$$\hat{R} := R \otimes \hat{\mathbb{Z}}; \qquad \hat{B} := B \otimes \hat{\mathbb{Q}} = \hat{R} \otimes \mathbb{Q};$$

the adelizations of R and B respectively. There is a natural correspondence

$$\{\text{Eichler } Z\text{-orders of level } N \text{ in } B\} \longleftrightarrow \hat{B}^\times / \hat{\mathbb{Q}}^\times \hat{\mathbb{R}}^\times \qquad ,$$

given by sending the coset definite by an idèle (b_ℓ) indexed by the rational prime ℓ to the order

$$(b_\ell)\hat{R}(b_\ell^{-1}) \cap B.$$

It can be proved that this is an Eichler Z-order of level N, that the map is well defined and that all Eichler Z-orders of level N can be obtained in this way. In other words we have the bijection:

$$\{\text{conjugacy classes of Eichler } Z\text{-orders of level } N \text{ in } B\} \longleftrightarrow B^\times \backslash \hat{B}^\times / \hat{R}^\times.$$

If p is a rational prime, let $B_p := B \otimes \mathbb{Q}_p$ and $R_p := R \otimes \mathbb{Z}_p$. Strong approximation yields a p-adic description of the above double coset space.

Theorem 1.11.4. *Let p be a prime such that B is split at p. Then the natural map*

$$R[1/p]^\times \backslash B_p^\times / R_p^\times \to B^\times \backslash \hat{B}^\times / \hat{R}^\times$$

sending the class represented by b_p to the class of the idèle $(\dots, 1, b_p, 1, \dots)$ is a bijection.

If B is a quaterion algebra over $\mathbb{Q}$ we say that B is an *indefinite* quaternion algebra if it is split at ∞. Otherwise we say it is *definite*.

1.11.2 Modular forms on quaterion algebras

In the remaining part of the exposition of this section we follow closely Section 1 of [BD]. The setting of this section is slightly different from the setting of the other parts of this thesis. To simplify our armuments we assume that p is in the level, hence we look at forms defined of the edges of the so-called *Bruhat-Tits tree* (cf definition below). We are actually interested in working on vertices, but up to p-stabilize our forms, it makes not difference to work on vertices or on edges.

Let N^- be an arbitrary squarefree integer which is the product of an even number of primes, and let N^+ be an arbitrary integer prime to N^-. Let p be a prime that does not divide the product $N_0 = N^+N^-$. Let N be the product $N = pN_0 = pN^+N^-$.

Let B be the definite quaternion algebra ramified at all the primes dividing N^- and let R be an Eichler $\mathbb{Z}[1/p]$-order of level N^+ in B.

We start by defining the *Bruhat-Tits tree* of a local field.

Let K be a local field, complete with respect to a valuation v, and denote by $|\cdot|_v$ the associated absolute value . Let $\mathcal{O}_K$ be its ring of integer, and recall that

$$\mathcal{O}_K = \{x \in K : v(x) \geq 0\}.$$

Denote by $\mathfrak{m}$ its maximal ideal and by π an uniformizer. Let $k = \mathcal{O}_K/\pi\mathcal{O}_K$ be the residue field of K. Define $V := K^2$. Let L and L' be two complete $\mathcal{O}_K$-lattices in V. By the invariant factor theorem, there exists an $\mathcal{O}_K$ basis $\{e_1, e_2\}$ of L and twi integers a, b such that $\{\pi^a e_1, \pi^b e_2\}$ is an $\mathcal{O}_K$-basis for L'

Remark 1.11.5.
1. It is possibile to show that the integers a and b are independent of the choiche of bases for L and L'.
2. L is a sublattice of L' if and only if both a and b are non-negative. In this case:

$$L/L' \cong \left(\mathcal{O}_K/\pi^a\ \mathcal{O}_K\right) \oplus \left(\mathcal{O}_K/\pi^b\mathcal{O}_K\right).$$

Let x and y be nonzero elements of K, and denote by $c := v(y/x)$. Replacing L (resp. L') by xL (resp. yL'), has the effect of replacing a and b by $a + c$ and $b + c$. Then $|\ a - b\ |_v$ depends only in the homothety classes Λ and Λ' of resp. L and L'. We refer to $|\ a - b\ |_v$ as the *distance* betweem Λ and Λ' and write

$$|\ a - b\ |_v = d(\Lambda, \Lambda').$$

The homothety classes of complete $\mathcal{O}_K$-lattices of V corresponds bijectively to the maximal orders of $\mathrm{M}_2(K)$. From now on we adopt this point of view. The distance $d(\Lambda, \Lambda')$ can be calculated as follows. Fix a representative L of Λ. Then define L' to be the unique representative of Λ' such that $L' \subset L$ and L is not contained in πL. For such L' it holds:

$$L/L' \cong \mathcal{O}_K/\pi^{d(\Lambda,\Lambda')\mathcal{O}_K}.$$

Note that:

1. $d(\Lambda, \Lambda') = 0$ if and only if $\Lambda = \Lambda'$;
2. $d(\Lambda, \Lambda') = 1$ if and only if there exists L and L' such that $L/L' \cong k$.

By this notion of distance, we can endow the set of classes of lattices in V with the structure of a combinatorial graph $\mathcal{T}$ where two homothety classes of lattices are adjacent if they have distance equal to one. It is known that, furthermore, $\mathcal{T}_K$ have the structure of a tree.

Definition 1.11.6. The tree $\mathcal{T}_K$ is called the *Bruhat-Tits tree* of $\mathrm{PGL}_2(K)$, and we use the notation $\mathcal{V}(\mathcal{T}_K)$ for the set of its vertices and $\mathcal{E}(\mathcal{T}_K)$ for the set of its edges.

Let us turn our attention to the case of $K = \mathbb{Q}_p$. Denote simply by $\mathcal{T}$ the Bruhat-Tits tree of $B_p^\times/\mathbb{Q}_p^\times$, keeping the notation of the previous section. The set $\mathcal{V}(T)$ of vertices of $\mathcal{T}$ is indexed by the maximal $\mathbb{Z}_p$-orders in B_p.

Two vertices are adjacent if their intersection is an Eichler order of level p. Let $\overrightarrow{\mathcal{E}}(\mathcal{T})$ denotes the set of ordered edges of $\mathcal{T}$, i.e. the set of ordered pairs (s, t) of adjacent vertex of $\mathcal{T}$. Any vertex e can be written as

$$e = (s = \mathrm{source}(e), t = \mathrm{target}(e)).$$

The tree $\mathcal{T}$ is endowed by a natural left transitive action of $B_p^\times/\mathbb{Q}_p^\times$ by isometries that corresponds to conjugation of maximal orders by elements of $B_p^\times$. The group $\Gamma := R^\times/\mathbb{Z}[1/p]^\times$ is a discrete subgroup of $B_p^\times/\mathbb{Q}_p^\times$ with respect to the p-adic topology and it acts naturally on $\mathcal{T}$. In particular the quotient $\mathcal{T}/\Gamma$ is a finite graph.

Definition 1.11.7. A modular form of weight two on $\mathcal{T}/\Gamma$ is a $\mathbb{Z}_p$-value function f on $\overrightarrow{\mathcal{E}}(\mathcal{T})$ invariant under the action of Γ. Denote by $S_2(\mathcal{T}/\Gamma)$ the space of such modular functions, that is a free $\mathbb{Z}_p$-module .

For any ring Z denote by $S_2(\mathcal{T}/\Gamma, Z)$ the space of Γ-invariant functions on $\overrightarrow{\mathcal{E}}(\mathcal{T})$ with values in Z.

Similarly define the space $S_2(\mathcal{V}/\Gamma, Z)$ of Γ-invariant Z-valued functions on $\mathcal{V}(\mathcal{T})$.

The space $S_2(\mathcal{T}/\Gamma)$ is endowed with a nondegenerate $\mathbb{Z}_p$ bilinear pairing that identifies $S_2(\mathcal{T}/\Gamma)$ with its $\mathbb{Q}_p$-dual. It is defined as

$$\langle f_1, f_2\rangle = \sum_{i=1}^{s} \#\operatorname{Stab}_\Gamma(e_i) f_1(e_i) f_2(e_i) \tag{1.18}$$

where e_i for $i = 1...s$ are representatives of the orbits of the action of Γ on the edges of the Bruhat-Tits tree $\mathcal{T}$. Replacing the edges with the vertex we have a similar pairing on $S_2(\mathcal{V}/\Gamma)$.

1.11.3 Hecke operators

Let ℓ be a prime that does not divide p. An element M_ℓ of reduced norm ℓ in the $\mathbb{Z}[1/p]$ order R admit a decomposition as

$$\Gamma M_\ell \Gamma = \gamma_1 \Gamma \cup \dots \gamma_t \Gamma.$$

The integer t depends on the prime ℓ and is given by

$$t = \begin{cases} \ell + 1 & \text{if } \ell \nmid N_0 \\ \ell & \text{if } \ell \mid N^+ \\ 1 & \text{if } \ell \mid N^-. \end{cases}$$

The Hecke operators are then defined as the linear endomorphism of $S_2(\mathcal{T}/\Gamma)$ given by the rule

$$f_\ell \mapsto \sum_{i=1}^{t} f(\gamma^{-1} e).$$

They are well defined since the above assignment does not depend on the choice of M_ℓ and the representatives γ_i. If ℓ does not divides N_0 we denote by T_ℓ the so called Hecke operators, otherwise we use the notation U_ℓ We can also define a Hecke operator at p, denoted by U_p, as

$$(U_p f)(e) = \sum_{s(e')=t(e)} f(e')$$

where the sum is taken over the p edges e' with source equal to the target of e, not including the edge obtained from e by reversing orientation. The good Hecke operator are self-adjoint for the pairing defined in (1.18), i.e.

$$\langle T_\ell f_1, f_2\rangle = \langle f_1, T_\ell f_2\rangle.$$

We will denote by $\mathbb{T}$ the Hecke algebra acting on the space $S_2(\mathcal{T}/\Gamma)$.

The classical notions of oldform and newform have a counterpart in these settings. As explained in the previous section the modular curves $X_0(N)$ and $X_0(Nq)$ for a prime q not dividing N are related by the two degeneracy maps. Similarly, we can define the degeneracy maps

$$s^*, t^* : S_2(\mathcal{V}/\Gamma) \to S_2(\mathcal{T}/\Gamma)$$

defined as

$$s^*(f)(e) = f(s(e)), \;\; t^*(f)(e) = f(t(e))$$

A form f in $S_2(\mathcal{T}/\Gamma, Z)$ is p-old if it is can be written as

$$f = s^*(f_1) + t^*(f_2)$$

for $f_1, f_2 \in S_2(\mathcal{V}/\Gamma)$ and it is p-new if it is orthogonal to the oldform.

Definition 1.11.8. A form $f \in S_2(\mathcal{T}/\Gamma)$ is an eigenform if it is a simultaneous eigenvector for all the Hecke operators, to be more precise, and clarify the notation:

$$\begin{array}{c} T_\ell(f) = a_\ell(f) f, \quad \text{for all } \; l \nmid N, \\ U_\ell(f) = \alpha_\ell(f) f, \quad \text{for all } \ell \mid N, \end{array}$$

with $a_\ell, \alpha_\ell \in \mathbb{Z}_p$.

An eigenform detemines a maximal ideal

$$\mathfrak{m}_f := \langle p, T_\ell - a_\ell(f), U_\ell - \alpha_\ell(f) \rangle.$$

The following property of some modular forms will be crucial in Chapter II.

Definition 1.11.9. A modular form is p-isolated if the completion of $S_2(\mathcal{T}/\Gamma)$ at $\mathfrak{m}_f$ is a free $\mathbb{Z}_p$ module of rank one.

Remark 1.11.10.

1. The previous definition is equivalent to say that, avoiding the trivial cases, the form f is not congruent to any other form in $S_2(\mathcal{T}/\Gamma)$.
2. Being p-isolated is actually a property of the mod p eigenform in $S_2(\mathcal{T}/\Gamma, \mathbb{F}_p)$ associated to f or of the maximal ideal $\mathfrak{m}_f$ itself.
3. As observed in Lemma 2.2 of [BD], in the settings of Chapter II we can deduce that if a modular form f is attached to an elliptic curve $E/\mathbb{Q}$, under some technical hypotesis, the form is p isolated. We will explain in details how this can be used to obtain some divibility relations between a prime p, the degree of the modular parametrization and the Tamagawa numbers of E.

1.11.4 The Jacquet-Langlands correspondence

Denote by $S_2(\Gamma_0(N)$ the complex vector space of classical modular forms of weight 2 on $\mathcal{H}/\Gamma_0(N)$. It is endowed with an action of Hecke operators that we denote, by abuse of notation as T_ℓ, U_ℓ, U_p. We say that ϕ is an eigenform on $\Gamma_0(N)$ that arises from a newform ϕ_0 of level N_0, if it is a simultaneous eigenfunction for the good Hecke operator, and let denote by a_ℓ the eigenvalue of T_ℓ. Assume that ϕ is also an eigenfunction for U_p, and denote by α_p

the eigenvalue of U_p. As remarked in [BD] it is possible to give an explicit description of α_p. Indeed if p does not divide N_0 then α_p is a root of the polynomial $x^2 - a_p x + p$ where a_p is the eigenvalue of T_p acting on ϕ_0. Conversely if p divides N_0 i.e. $\phi_0 = \phi$, denote by A_ϕ the abelian variety attached to ϕ by the Eichler-Shimura construction, then

$$\alpha_p = \begin{cases} 1 & \text{if } A_\phi \text{ has split multiplicative reduction at } p \\ -1 & \text{if } A_\phi \text{ has nonsplit multiplicative reduction at } p \end{cases}$$

The following proposition that is Proposition 1.3 in [BD] relates, via the Jacquet-Langlands correspondence, classical and quaternionic modular forms.

Proposition 1.11.11. *Let ϕ as above. Then there exists an eigenform f in $S_2(\mathcal{T}/\Gamma)$ satisfying:*

$$\begin{array}{ll} T_\ell f = a_\ell(\phi) f & \text{for all } \ell \nmid N, \\ U_\ell f = \alpha_\ell(\phi) f & \text{for all } \ell \mid N^+, \\ U_p f = \alpha_p(\phi) f & \end{array} \tag{1.19}$$

Furthermore the form f defined by above properties is unique up to multiplication by a nonzero complex number. Conversely, given an eigenform $f \in S_2(\mathcal{T}/\Gamma, \mathbb{C})$ there exists an eigenform $\phi \in S_2(\Gamma_0(N))$ satisfying (1.19)

The above proposition has the following corollary concerning the case of elliptic curves.

Corollary 1.11.12. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and p a prime of good ordinary reduction for E. If ℓ is a prime that does not divide N, set*

$$a_\ell = \ell + 1 - \#E(\mathbb{F}_\ell).$$

Let $\alpha_p \in \mathbb{Z}_p^\times$ be the unique root of the polynomial $x^2 - a_p x + p$. Then there exists an eigenform $f \in S_2(\mathcal{T}/\Gamma)$ satisfying:

$$\begin{array}{ll} T_\ell f = a_\ell f & \text{for all } \ell \nmid N, \\ U_p f = \alpha_p(\phi) f & \\ f \notin p S_2(\mathcal{T}/\Gamma) & \end{array}$$

Remark 1.11.13. The previous corollary also works without the assumption that p is a prime of good ordinary reduction. In this case, set

$$\alpha_p = \begin{cases} 1 & \text{if } E \text{ has split multiplicative reduction at } p \\ -1 & \text{if } E \text{ has nonsplit multiplicative reduction at } p \end{cases}$$

according with the description of α_p above.

Chapter 2

On the Birch and Swinnerton-Dyer conjecture for elliptic curves of analytic rank one

2.1 Statement of the main results

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let $\varphi_E : X_0(N) \to E$ be a modular parametrisation of minimal degree $d_E := \deg(\varphi_E)$, and let p be a rational prime. We will assume from now that the following hypothesis is satisfied.

Hypothesis 2.1.1. 1. $E/\mathbb{Q}$ has analytic rank one, i.e. $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 1$.

2. $E/\mathbb{Q}$ is semistable, i.e. N is square-free.

Thanks to part 1 of our Hypothesis, the theorem of Gross-Zagier and Kolyvagin tells us that $E(\mathbb{Q})$ has rank one, and that the Tate-Shafarevich group $\text{Ш}(E/\mathbb{Q})$ is finite. Let P_E be a generator of $E(\mathbb{Q})$ modulo torsion. Our goal in this chapter is to prove the following result (cf. Chapter I for the relevant definitions).

Theorem 2.1.2. *There exists a finite set of primes $\Sigma_E \supset \{2, 3, 5, 7\}$ (depending only on $E/\mathbb{Q}$) with the following property. For every prime $p \notin \Sigma_E$ of good ordinary reduction for $E/\mathbb{Q}$: p divides $L'(E/\mathbb{Q}, 1)/\big(\Omega_E \cdot h_E(P_E)\big)$ if and only if p divides $\#\text{Ш}(E/\mathbb{Q}) \cdot C_N$. (We note that, under our assumptions, the ratio $L'(E/\mathbb{Q}, 1)/\big(\Omega_E \cdot h_E(P_E)\big)$ is an integer.)*

Under a suitable additional *Lifting Hypothesis* 2.3.2, we also prove the following theorem.

Theorem 2.1.3. *Let $p > 7$ be a prime of good ordinary reduction for $E/\mathbb{Q}$, which does not divide d_E. Assume moreover that the Lifting Hypothesis* 2.3.2 *is satisfied. Then the equality:*

$$\mathrm{ord}_p\left(\frac{L'(E/\mathbb{Q}, 1)}{\Omega_E \cdot h_E(P_E)}\right) = \mathrm{ord}_p(\#\text{Ш}(E/\mathbb{Q}) \cdot C_N)$$

holds. In other words, the p-part of the Birch and Swinnerton-Dyer formula for $E/\mathbb{Q}$ holds.

Remark 2.1.4. We would like to make a few comments about the hypotheses of our results.

Regarding Hypothesis 2.1.1: the assumption that $E/\mathbb{Q}$ has analytic rank one is of course crucial in all that follows, and the fact that p is a prime of *ordinary reduction* for $E/\mathbb{Q}$ is also

fundamental for our method, which relies crucially on the work Bertolini-Darmon [BD] and Skinner-Urban [SU]. The other assumptions, namely the semistability of $E/\mathbb{Q}$ and the fact that p does not divides the minimal degree of a modular parametrisation, can be considerably weakened (cf. hypothesis CR in [PW]). They are assumed in order to avoid some technical complications that could have shaded the presentation of the main ideas of our method.

Regarding the Lifting Hypothesis mentioned in the statement of Theorem 2.1.3: referring to the following Sections for more details, we remark here that we believe it is always satisfied (and should be possible to verify it following some ideas appearing in [BD]).

2.2 First reduction

Fix an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$, where d is a square-free positive integer greater then 3 (so that $\mathcal{O}_K^* = \{\pm 1\}$), satisfying the following assumptions:

- (Heegner Hypothesis) every prime divisor of N splits in K.
- (Non-vanishing Hypothesis) $\mathrm{ord}_{s=1} L(E/K, s) = 1$.

Since $E/\mathbb{Q}$ has analytic rank one by Hypothesis 2.1.1, the existence of infinitely many quadratic imaginary fields $K/\mathbb{Q}$ satisfying these assumptions follows by a well-known result of Waldspurger [Wa] (cf. proof of Theorem 1.7.3). Let

$$P_K \in E(K)$$

be the Heegner point attached in Section 1.5 to K and φ_E. The theorem of Gross-Zagier-Kolyvagin then tells us: $E(K) \otimes \mathbb{Q}$ is a 1-dimensional vector space generated by P_K, and the Tate-Shafarevich group $\text{Ш}(E/K)$ is finite. Let us write for simplicity:

$$I(P_K) := [E(K) : \mathbb{Z}P_K].$$

What we will actually prove in this Chapter are the following results.

Theorem 2.2.1. *Let $p > 7$ be a prime of good ordinary reduction for $E/\mathbb{Q}$, which does not divide d_E. Then: p divides the cardinality of $\text{Ш}(E/K)$ if and only if it divides $I(P_K)$.*

Theorem 2.2.2. *Let $p > 7$ be a prime of good ordinary reduction for $E/\mathbb{Q}$, which does not divide d_E. Assume that the Lifting Hypothesis 2.3.2 is satisfied. Then*

$$2\mathrm{ord}_p\big(I(P_K)\big) = \mathrm{ord}_p\Big(\#\text{Ш}(E/K)\Big).$$

In the rest of this Section, we will show how Theorem 2.2.1 (resp., 2.2.2) imply Theorem 2.1.2 (resp., Theorem 2.1.3). More precisely, we have the results.

Theorem 2.2.3. *Theorem 2.2.1 implies Theorem 2.1.2.*

Proof. Let $p > 7$ be a prime of good ordinary reduction, which does not divides the degree d_E. Let $K/\mathbb{Q}$ be a quadratic imaginary field of discriminant coprime with $2Np$. Let us consider the following rational quantities:

$$L'(E/K, 1)^{\mathrm{alg}} := \frac{L'(E/K, 1)}{\Omega_{E/K} \cdot h_E(P_E)};$$

$$L'(E/\mathbb{Q},1)^{\mathrm{alg}} := \frac{L'(E/\mathbb{Q},1)}{\Omega_E \cdot h_E(P_E)};$$

$$L(E^K/\mathbb{Q},1)^{\mathrm{alg}} := \frac{L(E^K/\mathbb{Q})}{\Omega_{E^K}},$$

where $E^K/\mathbb{Q}$ is the quadratic twist of $E/\mathbb{Q}$ by K. With these notations, we have the equality (under our assumptions):

$$L'(E/K,1)^{\mathrm{alg}} = L'(E/\mathbb{Q},1)^{\mathrm{alg}} \cdot L(E^K/\mathbb{Q},1)^{\mathrm{alg}}. \tag{2.1}$$

Given two rational numbers α and β, we will write $\alpha \sim_p \beta$ if $\alpha = u\cdot\beta$, where u is a p-adic unit. As explained in Lemma 2.2 of [BD], the fact that $p \nmid d_E$ implies that $C_N(E/\mathbb{Q}) \sim_p 1$ (where we write more precisely $C_N(E/\mathbb{Q})$ for the product of the Tamagawa numbers of $E/\mathbb{Q}$), i.e. that $E[p]$ is ramified at every prime $q|N$. Since the conductor of $E^K/\mathbb{Q}$ is ND_K^2 (where D_K is the absolute discriminant of K), since the Tamagawa factor of an elliptic curve at a prime of additive reduction is coprime with p (since $p > 7$), and since $E^K[p]$ is the twist of $E[p]$ by the quadratic character attached to $K/\mathbb{Q}$ and the latter is unramified at p (so $E^K[p]$ is ramified if $E[p]$ is), this also implies $C_{ND_K^2}(E^K/\mathbb{Q}) \sim_p 1$. Moreover, by a theorem of Mazur, the mod-p representation $\overline{\rho}_E$ of $G_{\mathbb{Q}}$ on $E[p]$ is surjective (since $p > 7$ and $E/\mathbb{Q}$ is semistable), so that $E/\mathbb{Q}$ satisfies the assumptions of Theorem 1.9.6. This implies that $E^K/\mathbb{Q}$ also satisfies the hypothesis of *loc. cit.*, and applying Skinner-Urban Theorem we obtain the formula:

$$L(E^K/\mathbb{Q},1)^{\mathrm{alg}} \sim_p \#Ш(E^K/\mathbb{Q}). \tag{2.2}$$

By Corollary 2 of [OS], there exists a finite of primes Σ_E, depending only on $E/\mathbb{Q}$, with the following property: let $q \notin S_E$ be a prime. Then there exists infinitely many quadratic imaginary fields $K/\mathbb{Q}$ of discriminant coprime with $2qN$, such that every prime divisor of N splits in $K/\mathbb{Q}$, and such that

$$\mathrm{ord}_q\Big(L(E^K/\mathbb{Q},1)^{\mathrm{alg}}\Big) = 0.$$

With this result at hand: let $\Sigma_E := S_E \cup \{q|d_E\}$, assume from now on that $p := q \notin \Sigma_E$, and assume that $K/\mathbb{Q}$ is chosen satisfying the properties above. In particular, p and K satisfy the assumptions of Theorem 2.2.1, and we have:

$$L(E^K/\mathbb{Q},1)^{\mathrm{alg}} \sim_p 1; \quad \#Ш(E^K/\mathbb{Q}) \sim_p 1, \tag{2.3}$$

the second equation coming from (2.2). Moreover, by the Gross-Zagier Theorem:

$$L'(E/K,1)^{\mathrm{alg}} \doteq I(P_K).$$

This follows combining Theorem 1.6.2 with Proposition 1.6.1. Appealing now to Theorem 2.2.1 (which is assumed here to hold), we deduce from the preceding equation:

$$p|L'(E/K,1)^{\mathrm{alg}} \quad \Longleftrightarrow \quad p|\#Ш(E/K). \tag{2.4}$$

Since $\#Ш(E/K) \doteq \#Ш(E/\mathbb{Q})\cdot\#Ш(E^K/\mathbb{Q})$ (as $p \neq 2$), we then obtain:

$$p|L'(E/\mathbb{Q},1)^{\mathrm{alg}} \overset{(2.1)\text{ and }(2.3)}{\Longleftrightarrow} p|L'(E/K,1)^{\mathrm{alg}} \overset{(2.4)}{\Longleftrightarrow} p|\#Ш(E/K) \overset{(2.3)}{\Longleftrightarrow} p|\#Ш(E/\mathbb{Q}).$$

Since (as noted above) $C_N \sim_p 1$ under our assumption, this conclude the proof. □

Theorem 2.2.4. *Theorem* 2.2.2 *implies Theorem* 2.1.3.

Proof. The proof proceeds as in the preceding Theorem, but is much simpler, since we need not appeal to the results of Ono-Skinner mentioned above. The details were already given in Theorem 1.10.3. □

Thanks to the preceding two results, we will concentrate in the rest of this Thesis to the proofs of Theorem 2.2.1 and Theorem 2.2.2. In the rest of this Section we give a sketch of the proofs, referring to the rest of the chapter for more details.

2.3 Outline of the proof

In this Section we outline the proof of Theorem 2.2.1 and Theorem 2.2.2, referring to the following Sections for more details and missing definitions.

The main idea behind the proofs is to use the theory of congruences between modular forms in order to reduce the p-part of the BSD conjecture in analytic rank one to the p-part of the BSD conjecture in analytic rank zero, the latter being now a consequence of the work of Skinner-Urban and Kato on the cyclotomic Iwasawa main conjecture.

Let $f = \sum_{k=1}^{\infty} a_k(E)q^k \in S_2(\Gamma_0(N), \mathbb{Z})$ be the weight-two newform attached to $E/\mathbb{Q}$ by the Modularity Theorem 1.4.11. According to [BD], we give the following:

Definition 2.3.1. Let n be a positive integer, and let ℓ be a rational prime. We say that ℓ is *n-admissible relative to* (f, K, p) if it satisfies the following properties:

1. ℓ does not divide $2Np$.
2. ℓ is *inert* in K.
3. p does not divide $\ell^2 - 1$.
4. $a_\ell(E)^2 \equiv (\ell + 1)^2 \bmod p^n$.

Roughly speaking, our method goes as follows. Fix, once and for all, an embedding of $\overline{\mathbb{Q}}$ inside $\overline{\mathbb{Q}}_p$. Assume that we can produce, for $n \gg 0$, an n-admissible prime ℓ, together with a weight-two newform $g = \sum_{k=1}^{\infty} a_k(g)q^k \in S_2(\Gamma_0(N\ell), \mathbb{Z}_p)$ [1] congruent to f modulo p^n:

$$a_m(g) \equiv a_m(f) \bmod p^n$$

for every positive integer m coprime with ℓ. We note that condition 4 above is necessary in order that such an *ℓ-level raising* g of f exists. Let $L(g/K, s)$ be the Hecke L-series of g/K, and let $\mathrm{sgn}(g/K)$ be the sign in its functional equation. As ℓ is inert in K by assumption 2:

$$\mathrm{sgn}(g/K) = +1,$$

so that $L(g/K, s)$ is not forced to vanish at $s = 1$ by parity conditions. Indeed, as explained in [BD1], [BD], a suitable *Jochnowitz congruence* would give in this setting a precise relation

[1] By this notation we mean that g is a weight-two newform of level $N\ell$, such that $a_k(g) \in \mathbb{Z}_p$ for every integer k, under our fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

between the p-adic order of the algebraic part $L^{\mathrm{alg}}(g/K,1) \in \mathbb{Z}_p$ of the special value $L(g/K,1)$, and the p-adic order of the index $I(P_K)$ of the Heegner point P_K in $E(K)$:

$$\mathrm{ord}_p\big(I(P_K)\big) \overset{\text{Jochnowitz congruence}}{\longleftrightarrow} \mathrm{ord}_p\Big(L^{\mathrm{alg}}(g/K,1)\Big). \tag{2.5}$$

In this way, we can recover the p-part of $I(P_K)$ from the p-part of $L^{\mathrm{alg}}(g/K,1)$. Using the p-part of the BSD formula in rank zero, the latter is related to the cardinality of a suitable p-primary Selmer group attached to g/K, which in turn can be related to the cardinality of the p-primary part of the Tate-Shafarevich group of E/K.

The technical problem with the above strategy comes from the fact that, given $n \gg 0$ and an n-admissible prime ℓ, a newform $g \in S_2(\Gamma_0(N\ell),\mathbb{Z}_p)$ congruent to f modulo p^n does not necessarily exist. More precisely: following the approach of Bertolini and Darmon in [BD], we can use the work of Ribet on raising the level to construct an *ℓ-new, mod-p^n modular form* $\overline{g}$ of level $\Gamma_0(N\ell)$ which is congruent to f modulo p^n (see Section 2.4.4 for the details), but in general $\overline{g}$ cannot be lifted to a true modular from (in characteristic zero). For this reason, we will make use in our argument of the following hypothesis, which we will refer to as the *Lifting Hypothesis*.

Hypothesis 2.3.2 (Lifting hypothesis)**.** There exists a triple (n,ℓ,g), where n is a positive integer, ℓ is an n-admissible prime relative to (f,K,p), and $g \in S_2(\Gamma_0(N\ell),\mathbb{Z}_p)$ is a weight-two newform, satisfying the following properties:

1. $n > \max\Big(2\mathrm{ord}_p\big(I(P_K)\big), \#\text{Ш}(E/K)[p^\infty]\Big)$.
2. g is congruent to f modulo p^n, i.e.
$$a_m(g) \equiv a_m(f) \bmod p^n$$
for every positive integer m coprime with ℓ.
3. The natural inclusion $E(K) \subset E(K_\ell)$ induces an injective map: $E(K)/p^n \hookrightarrow E(K_\ell)/p^n$.

Remark 2.3.3. 1. Let n be a 'large' positive integer. As mentioned above (cf. Section 2.4.4), for every n-admissible prime ℓ, the work of Ribet attaches to (n,ℓ) a mod-p^n modular form $\overline{g} = \overline{g}_\ell$ of level $N\ell$, which is congruent to f mod p^n. The crucial part of the preceding hypothesis is 2, asserting that we can choose ℓ such that $\overline{g}$ can be lifted to a weight-two newform $g \in S_2(\Gamma_0(N\ell),\mathbb{Z}_p)$, congruent to f modulo p^n. The 'auxiliary request' 3 is of a more technical nature, albeit it will be needed in our method.

2. We remark that Ribet's raising the level result asserts that, for every 1-admissible prime ℓ, there exists a weight-two newform $g \in S_2(\Gamma_0(N\ell),\mathbb{Z}_p)$ which is congruence to f modulo p. In other words, with the notations of the preceding remark: if $n=1$, we can *always* lift $\overline{g}$ to a true modular form.

Notations and assumptions. We fix for the rest of this Section a positive integer n, and a n-admissible prime ℓ, such that the natural 'mod-p^n localisation at ℓ':

$$\iota_\ell : E(K)\otimes\mathbb{Z}/p^n\mathbb{Z} \hookrightarrow E(K_\ell)\otimes\mathbb{Z}/p^n\mathbb{Z} \tag{2.6}$$

is injective. We note that, under our assumptions, $E(K)\otimes\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}/p^n\mathbb{Z}$, generated by the reduction modulo p^n of a generator $\mathbf{P}$ of $E(K)/E(K)_{\mathrm{tors}} \cong \mathbb{Z}$ (since $E(K)[p]=0$ under

our hypotheses). As explained in Theorem 3.2 of [BD], we can then use the Chebotarev density theorem to show that there exist infinitely many pairs (n, ℓ) satisfying these properties. Moreover, in order to simplify the exposition, we will ***assume*** for the rest of this Section ***that*** $K/\mathbb{Q}$ ***has class number one***.

Step 1: Raising the level in the quaternionic setting

By a slight abuse of notation, let us write again

$$f : \mathbb{T} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$$

for the morphism modulo p^n attached to f, where $\mathbb{T}$ is the Hecke algebra of level N introduced in Section 1.4. Let $\mathcal{I}_f \subset \mathbb{T}$ denotes the kernel of f.

Recall our fixed n-admissible prime ℓ. Working on results and ideas of Ribet and Bertolini-Darmon (cf. Sections 5 and 9 of [BD], and Section 2.4 below), we will prove in Section 2.4.4 that there exists a mod-p^n modular form $\overline{g} = \overline{g}_\ell$ of level $N\ell$ which is congruent to f modulo p^n. More precisely: let $\mathbb{T}_\ell \subset \mathrm{End}(S_2(\Gamma_0(N\ell), \mathbb{C}))$ be the Hecke ring generated over $\mathbb{Z}$ by the Hecke operators T_q, for primes $q \nmid N\ell$, and U_q, for primes $q|N\ell$, acting on the space of cusp forms $S_2(\Gamma_0(N\ell), \mathbb{C})$. Write $\mathbf{T}_\ell$ for the *ℓ-new quotient of* $\mathbb{T}_\ell$, i.e. for the quotient of $\mathbb{T}_\ell$ acting on the subspace $S_2^{\ell\text{-new}}(\Gamma_0(N\ell), \mathbb{C})$ of $S_2(\Gamma_0(N\ell), \mathbb{C})$ made of cusp-forms which are new at ℓ. Then there exists a surjective morphism:

$$\overline{g} : \mathbf{T}_\ell \to \mathbb{Z}/p^n\mathbb{Z},$$

such that $\overline{g}(T_q^{N\ell}) = f(T_q^N)$ for every prime $q \nmid N$ and $\overline{g}(U_q^{N\ell}) = f(U_q^N)$ for every prime $q|N$, where we write for clarity here T_q^M for the q-th Hecke operator of level M acting on $S_2(\Gamma_0(M), \mathbb{C})$, and similarly for U_q^M.

The Jacquet-Langlands correspondence allows us to view $\overline{g}$ as a mod-p^n modular form on the *definite* quaternion algebra $B = B(\ell\infty)$ ramified at ℓ and ∞. Precisely: fix an Eichler $\mathbb{Z}$-order R of level N in B, and consider the adelic double coset space

$$\mathcal{X}_{N,\ell} := \widehat{R}^\times \backslash \widehat{B}^\times / B^\times,$$

where we write $\widehat{M} := M \otimes \widehat{\mathbb{Z}}$, with $\widehat{\mathbb{Z}} = \prod_{q \text{ prime}} \mathbb{Z}_q$ the profinite completion of $\mathbb{Z}$. As explained in [BD3], $\mathcal{X}_{N,\ell}$ is a finite set, and its divisor group $\mathrm{Pic}(\mathcal{X}_{N,\ell})$ is equipped with an action of the Hecke algebra $\mathbf{T}_\ell$. The modular form $\overline{g}$ alluded to above then corresponds, by Jacquet-Langlands, to a surjective morphism

$$\overline{\phi}_\ell : \mathrm{Pic}(\mathcal{X}_{N,\ell}) \longrightarrow \mathbb{Z}/p^n\mathbb{Z},$$

which is a common eigenfunction for the Hecke operators in $\mathbf{T}_\ell$, with associated system of Hecke eigenvalues given by $\overline{g}$. Moreover, $\overline{\phi}_\ell$ is characterised by these properties up to multiplication by a unit modulo p^n.

Let $\mathcal{V} = \mathcal{V}_p := \mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p)$ be the set of vertices of the Bruhat-Tits tree of $\mathrm{PGL}_2(\mathbb{Q}_p)$. Let us fix an isomorphism $\iota_p : B_p := B \otimes_{\mathbb{Z}} \mathbb{Q}_p \cong \mathrm{M}_2(\mathbb{Q}_p)$, and let us write $\Gamma := \iota_p\left(R[1/p]^\times\right)$. Strong approximation [Vi] provides us with a natural identification:

$$\mathcal{V}/\Gamma = \mathcal{X}_{N,\ell},$$

defined sending the class of $\iota_p(b)$ in $\mathcal{V}/\Gamma$ to the class of the idéle $(\dots, 1, b, 1, \dots)$ in $\mathcal{X}_{N,\ell}$. We can then view $\overline{\phi}_\ell$ as an element of the space of quaternionic modular forms $S_2(\mathcal{V}/\Gamma, \mathbb{Z}/p^n\mathbb{Z})$ introduced in Section 1.11.4, i.e. as a function

$$\overline{\phi}_\ell : \mathcal{V}/\Gamma \longrightarrow \mathbb{Z}/p^n\mathbb{Z},$$

such that $\overline{\phi}_\ell \notin p \cdot S_2(\mathcal{V}/\Gamma, \mathbb{Z}/p^n\mathbb{Z})$.

It is crucial for our method to give an explicit, geometric description of $\overline{\phi}_\ell : \mathcal{V}/\Gamma \to \mathbb{Z}/p^n\mathbb{Z}$. This is possible thanks to Ribet's description of $\mathcal{X}_{N,\ell} = \mathcal{V}/\Gamma$ in term of enhanced supersingular elliptic curves in characteristic ℓ [Ri], generalising Deuring's classification of endomorphism algebras of elliptic curves over finite fields. Precisely: recall that a point in the reduction $X_0(N)_{/\mathbb{F}_\ell}$ of $X_0(N)$ modulo ℓ is represented by a pair $(\mathcal{E}, \mathcal{C})$, where $\mathcal{E}$ is an elliptic curve defined over $\overline{\mathbb{F}}_\ell$, "enhanced by" a cyclic subgroup $\mathcal{C} \subset \mathcal{E}$ of order N. Write $\mathcal{S}_\ell$ for the subset of points of $X_0(N)_{/\mathbb{F}_\ell}$ which are represented by a pair as above, with $\mathcal{E}$ a *supersingular* elliptic curve. Proposition 3.3 of [Ri] shows that there exists a bijection

$$\mathcal{V}/\Gamma = \mathcal{X}_{N,\ell} \cong \mathcal{S}_\ell, \tag{2.7}$$

which is compatible, 'outside ℓ', with the actions of the Hecke algebras $\mathbb{T}$ and $\mathbf{T}_\ell$ on $\mathcal{S}_\ell$ and $\mathcal{X}_{N,\ell}$ respectively (see Proposition 2.4.11 for a precise statement).

Since the j-invariant of a supersingular elliptic curve defined over $\overline{\mathbb{F}}_\ell$ lives in the quadratic extension $\mathbb{F}_{\ell^2}/\mathbb{F}_\ell$, it follows that $\mathcal{S}_\ell \subset X_0(N)(\mathbb{F}_{\ell^2})$. Write $J := J_0(N)$ for the Jacobian of $X_0(N)_{/\mathbb{Q}}$. In Section 2.4 below we will prove that, under the identification (2.7), the mod-p^n modular form $\overline{\phi}_\ell$ corresponds to a composition:

$$\gamma : \mathcal{S}_\ell \to J(\mathbb{F}_{\ell^2})/\mathcal{I}_f \overset{\mathrm{red}_\ell^{-1}}{\cong} J(K_\ell)/\mathcal{I}_f \overset{\kappa_\ell}{\to} \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z}, \tag{2.8}$$

where the notations are as follows. Write $\mathrm{Div}(\mathcal{S}_\ell) := \mathbb{Z}[\mathcal{S}_\ell]$ and $\mathrm{Div}^0(\mathcal{S}) \subset J(\mathbb{F}_{\ell^2})$ for the subgroup of degree zero divisors. Since $\mathcal{I}_f$ is not an Eisenstein ideal, we have a natural isomorphism $\mathrm{Div}^0(\mathcal{S})/\mathcal{I}_f \cong \mathrm{Div}(\mathcal{S})/\mathcal{I}_f$. This allows us to define the first arrow above as the composition $\mathcal{S}_\ell \subset \mathrm{Div}(\mathcal{S}_\ell) \twoheadrightarrow \mathrm{Div}(\mathcal{S}_\ell)/\mathcal{I}_f \cong \mathrm{Div}^0(\mathcal{S}_\ell)/\mathcal{I}_f \to J(\mathbb{F}_{\ell^2})/\mathcal{I}_f$. Writing K_ℓ for the completion of K at the unique prime above ℓ, the reduction map $J(K_\ell) \to J(\mathbb{F}_{\ell^2})$ induces the isomorphism denoted red_ℓ^{-1} above (recall that ℓ is inert in K). Writing $\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n])$ for the unramified cohomology of the G_{K_ℓ}-module $E(\overline{K}_\ell)[p^n]$, the map κ_ℓ is induced by the local Kummer map for $J_{/K_\ell}$, using the isomorphism $\mathrm{Ta}_p(J)/\mathcal{I}_f \cong E[p^n]$ arising from the modular parametrisation $\varphi_E : X_0(N) \to E$. Finally: we will prove below that for every n-admissible prime ℓ, the finite cohomology $\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n])$ is free of rank one over $\mathbb{Z}/p^n\mathbb{Z}$, and the last map in the composition above refers to a fixed choice of an isomorphism. (We remark once more that the modular form $\overline{g}$, and then its Jacquet-Langlands lift $\overline{\phi}_\ell$, is uniquely determined only up to multiplication by a unit in $\mathbb{Z}/p^n\mathbb{Z}$.)

Step 2: Heegner points and a special value formula

As explained in Section 1.5, the Heegner point $P_K \in E(K)$ is the image under the modular parametrisation $\varphi_E : X_0(N) \to E$ of a CM point $\mathbb{P} \in X_0(N)(K)$ (recall that we are assuming for simplicity that K has class number 1 in this Section). More precisely: $\mathbb{P}$ can be represented by an enhanced elliptic curve (A, C), where A is an elliptic curve defined over K, with CM by $\mathcal{O}_K$, and having good reduction at (the unique prime of K) above ℓ. It follows that the

reduction $\overline{A}/\mathbb{F}_{\ell^2}$ of A modulo ℓ is a supersingular elliptic curve, so that $(\overline{A}, \overline{C})$ represents a point in $\mathcal{S}_\ell$ (with the notations of the preceding Section). In other words, writing $\mathrm{red}_\ell : J(K) \to J(\mathbb{F}_{\ell^2})$ for the natural reduction map: $\overline{\mathbb{P}} := \mathrm{red}_\ell(\mathbb{P}) \in \mathcal{S}_\ell$. Under the isomorphism (2.7), $\mathbb{P}$ then corresponds to an element

$$\mathfrak{v}(\mathbb{P}) \in \mathcal{V}/\Gamma$$

(i.e. to a vertex of the finite graph $\mathcal{T}/\Gamma$, where $\mathcal{T} = \mathcal{T}_p$ is the Bruhat-Tits tree of $\mathrm{PGL}_2(\mathbb{Q}_p)$).

Recall the mod-p^n modular form $\overline{g} = \overline{g}_\ell$ of level $N\ell$, and congruent to f modulo p^n, mentioned in the preceding Step. We ***assume*** here that $\overline{g}$ can be lifted to a weight-two newform $g = g_\ell \in S_2(\Gamma_0(N\ell), \mathbb{Z}_p)$ (i.e. g is a weight-two newform of level $\Gamma_0(N\ell)$, with Fourier coefficients in $\mathbb{Z}_p$, and such that the reduction modulo p^n of the corresponding morphism $g : \mathbb{T}_\ell \to \mathbb{Z}_p$ equals $\overline{g}$). As in the preceding Section, the Jacquet-Langlands correspondence attaches to g an eigenform $\phi_\ell : \mathrm{Pic}(\mathcal{X}_{N,\ell}) \to \mathbb{Z}_p$, with the same Hecke eigenvalues as g, and uniquely characterised by these properties up to multiplication by a p-adic unit. Using the identification $\mathcal{X}_{N,\ell} = \mathcal{V}/\Gamma$, we can consider ϕ as a function

$$\phi_\ell \in S_2(\mathcal{V}/\Gamma, \mathbb{Z}_p),$$

whose reduction modulo p^n equals the mod-p^n modular form $\overline{\phi}_\ell$.

The seminal *Gross formula* expresses the special value of the Hecke L-function of g/K in terms of the value of ϕ_ℓ at $\mathfrak{v}(\mathbb{P})$. Precisely, let $L(g/K, s)$ be the Hecke complex L-series of g/K, and define the *algebraic part* of $L(g/K, 1)$ by:

$$L^{\mathrm{alg}}(g/K, 1) := \frac{L(g/K, 1)}{\Omega_g^{\mathrm{can}}} \in \mathbb{Z}_p,$$

where Ω_g^{can} is the *canonical Shimura period* of g/K, as defined in Section 2.2 of [PW] (where it is denoted simply Ω_g). Then we have:

$$L^{\mathrm{alg}}(g/K, 1) \doteq \phi_\ell\big(\mathfrak{v}(\mathbb{P})\big)^2 \cdot p^{t_g(\ell)}. \tag{2.9}$$

Here $\doteq$ denotes equality up to multiplication by a p-adic unit, and $t_g(\ell)$ is a certain *Tamagawa exponent* at ℓ attached to g (see Section 2.5.4 for detailed definitions).

Let $\infty \in X_0(N)(\mathbb{Q})$ be a fixed rational point such that $\varphi_E(\infty) = O_E$. Using the explicit description (2.8) of $\overline{\phi}_\ell = \phi_\ell \bmod p^n$ explained in the Step I, we will easily deduce the formula:

$$\overline{\phi}_\ell(\mathfrak{v}(\mathbb{P})) \doteq \gamma\big(\mathrm{red}_\ell(\mathbb{P})\big) = \kappa_\ell\big(\mathbb{P} - \{\infty\}\big) = P_K(\ell) \bmod p^n,$$

where $\doteq$ denotes equality in $\mathbb{Z}/p^n\mathbb{Z}$ up to multiplication by a unit modulo p^n, and κ_ℓ is as in (2.8). Recall that we fixed above an isomorphism $\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z}$. Then we write $P_K(\ell) \in \mathbb{Z}/p^n\mathbb{Z}$ for the image of P_K under the composition of the local Kummer map on $E(K_\ell)/p^n$ with the natural restriction map $\iota_\ell : E(K)/p^n \to E(K_\ell)/p^n$. Since ι_ℓ is injective by assumption (2.6) (and since $E(K)[p] = 0$), restriction at ℓ induces an isomorphism $\mathbb{Z}/p^n\mathbb{Z}\cdot\widetilde{\mathbf{P}} = E(K)\otimes\mathbb{Z}/p^n\mathbb{Z} \cong \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z}$, sending the reduction $\widetilde{\mathbf{P}}$ of a generator $\mathbf{P} \in E(K)/E(K)_{\mathrm{tors}}$ modulo p^n to 1. As $P_K = I(P_K)\cdot\mathbf{P}$, we then obtain the identity $P_K(\ell) \doteq I(P_K) \bmod p^n$, and the last equation can be reformulated as:

$$\phi_\ell(\mathfrak{v}(\mathbb{P})) \doteq I(P_K) \bmod p^n. \tag{2.10}$$

(Here $\dot{\equiv}$ denotes equality in $\mathbb{Z}/p^n\mathbb{Z}$ up to multiplication by units.)

In particular: ***assume*** further that

$$n > \mathrm{ord}_p\big(I(P_K)\big).$$

Then equation (2.10) and equation (2.9) combine to give the identity:

$$\mathrm{ord}_p\Big(L^{\mathrm{alg}}(g/K,1)\Big) = 2\mathrm{ord}_p\big(I(P_K)\big) + t_g(\ell). \tag{2.11}$$

This is the Jochnowitz congruence mentioned in equation (2.5) (cf. [BD1], Section 6 of [Va], and Section 9 of [BD] for closely related results).

Step 3: Shafarevich-Tate groups

In this Step, we continue to ***assume***, as in Step II, that there exists a weight-two newform $g = g_\ell \in S_2(\Gamma_0(N\ell), \mathbb{Z}_p)$ lifting the mod-p^n modular form $\overline{g} = \overline{g}_\ell$ appearing in Step I.

Let A_g be the abelian variety over $\mathbb{Q}$ attached to the newform $g \in S_2(\Gamma_0(N\ell), \mathbb{Z}_p)$ by the Eichler-Shimura construction, so that A_g is a quotient of the modular Jacobian $J_0(N\ell)$ of level $N\ell$ (see Theorem 1.4.13 for more details). Let $K_g = \mathbb{Q}(\{a_n(g) : n \in \mathbb{N}\})$ be the totally real field generated over $\mathbb{Q}$ by the Fourier coefficients of g, and let $\mathcal{O}_g = \mathcal{O}_{K_g}$ be its ring of integers. Then $\mathcal{O}_g$ acts as a ring of $\mathbb{Q}$-rational endomorphisms on $A_g/\mathbb{Q}$, i.e. there exists a morphism $\mathcal{O}_g \to \mathrm{End}(A_g/\mathbb{Q})$. In particular, for every field extension $L/\mathbb{Q}$, the group $A_g(L)$ is an $\mathcal{O}_g$-module. Since the Fourier coefficients of g live in $\mathbb{Z}_p$, there exists a prime ideal $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_g)$ such that the completion $K_{g,\mathfrak{p}}$ of K_g at $\mathfrak{p}$ is isomorphic to $\mathbb{Q}_p$. Write $\mathcal{O}_\mathfrak{p} \cong \mathbb{Z}_p$ for the completion of $\mathcal{O}_g$ at $\mathfrak{p}$. We then have an isomorphism of $\mathbb{Z}/p^n\mathbb{Z}[G_\mathbb{Q}]$-modules:

$$A_g[\mathfrak{p}^n] \cong E[p^n].$$

Fixing such an isomorphism, we can consider both the p^n-Selmer group $\mathrm{Sel}_{p^n}(E/K)$ attached to E/K, and the $\mathfrak{p}^n$-Selmer group $\mathrm{Sel}_{\mathfrak{p}^n}(A_g/K)$ attached to A_g/K (cf. Section 1.1) as submodules of $\mathrm{H}^1(K, E[p^n])$. By the results of [GP], we know that the local conditions defining $\mathrm{Sel}_{p^n}(E/K)$ and $\mathrm{Sel}_{\mathfrak{p}^n}(A_g/K)$ as subgroups of $\mathrm{H}^1(K, E[p^n])$ match at all primes of K different from ℓ, while they are 'complementary' at ℓ [2]. Since $\iota_\ell : E(K)/p^n \hookrightarrow E(K_\ell)/p^n$ is injective by assumption (2.6), a simple argument based on Poitou-Tate duality allows us to show that there is an exact sequence

$$0 \to \mathrm{Sel}_{\mathfrak{p}^n}(A_g/K) \to \mathrm{Sel}_{p^n}(E/K) \xrightarrow{\kappa_\ell} \mathbb{Z}/p^n\mathbb{Z} \to 0,$$

where we write here κ_ℓ to denote the composition of restriction at ℓ with the local Kummer map $E(K_\ell)/p^n \to \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z}$ (see Step I for the last isomorphism). Since $E(K)$ is a semistable elliptic curve of analytic rank one and $p > 7$, we have $E(K)/p^n \cong \mathbb{Z}/p^n\mathbb{Z}$, so that Kummer theory and the preceding equation give the equality:

$$\#\mathrm{Sel}_{\mathfrak{p}^n}(A_g/K) = \#\text{Ш}(E/K)[p^n]. \tag{2.12}$$

[2] More precisely: the local cohomology $\mathrm{H}^1(K_\ell, E[p^n])$ at an n-admissible prime ℓ decomposes as a direct sum of its *finite part* $\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z}$ and its *ordinary part* $\mathrm{H}^1_{\mathrm{ord}}(K_\ell, E[p^n])$. Moreover, $\mathrm{H}^1_{\mathrm{fin}}$ is in perfect duality with $\mathrm{H}^1_{\mathrm{ord}}$ under the local Tate duality attached to the Weil pairing on $E[p^n]$. Since E has good reduction at ℓ, the local condition at ℓ defining $\mathrm{Sel}_{p^n}(E/K)$ is the finite one $\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n])$. On the other hand, A_g has purely toric reduction at ℓ, and Tate's theory tells us that the local condition at ℓ defining $\mathrm{Sel}_{\mathfrak{p}^n}(A_g/K)$ is the ordinary one $\mathrm{H}^1_{\mathrm{ord}}(K_\ell, E[p^n])$.

Step 4: End of the proofs

Thanks to the work of Kato and Skinner-Urban on the cyclotomic Iwasawa main conjecture for GL_2, we have the equality (cf. Theorem 1.9.7):

$$\mathrm{ord}_p\Big(L^{\mathrm{alg}}(g/K,1)\Big) = \mathrm{ord}_p\Big(\#\mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K)\Big) + t_g(\ell). \tag{2.13}$$

With this last equation at our disposal, we are now ready to conclude our proofs.

Proof of Theorem 2.2.1. Let us take $n = 1$. As recalled in Remark 2.3.3, Ribet's raising the level theorem guarantees the existence of a weigth-two newform $g \in S_2(\Gamma_0(N\ell), \mathbb{Z}_p)$ congruent to f modulo p. In particular, with the exception of equation (2.11), the results outlined in Step II and Step III hold (unconditionally) for $n = 1$. Then

$$\underline{\mathrm{III}}(E/K)[p] = 0 \quad \Longleftrightarrow \quad \mathrm{Sel}_{\mathfrak{p}}(A_g/K) = 0$$

by equation (2.12), while equation (2.13) gives us the equivalence:

$$\mathrm{Sel}_{\mathfrak{p}}(A_g/K) = 0 \quad \Longleftrightarrow \quad \mathrm{ord}_p\Big(L^{\mathrm{alg}}(g/K,1)\Big) = t_g(\ell) \quad {}^{3}.$$

Appealing now to Gross's formula (2.9) we have (cf. Step II):

$$\mathrm{ord}_p\Big(L^{\mathrm{alg}}(g/K,1)\Big) = t_g(\ell) \quad \Longleftrightarrow \quad \mathrm{ord}_p\Big(\phi_\ell\big(\mathfrak{v}(\mathbb{P})\big)\Big) = 0.$$

Finally: equation (2.10) gives the equivalence:

$$\mathrm{ord}_p\Big(\phi_\ell\big(\mathfrak{v}(\mathbb{P})\big)\Big) = 0 \quad \Longleftrightarrow \quad \mathrm{ord}_p\big(I(P_K)\big) = 0.$$

Putting everything together, we conclude our outline of the proof of Theorem 2.2.1.

Proof of Theorem 2.2.2 Assume that the Lifting Hypothesis 2.3.2 is satisfied. Then we can complete our fixed pair (n, ℓ) to a triple (n, ℓ, g) satisfying the conclusion of the Lifting Hypothesis. Then $n > \mathrm{ord}_p\big(I(P_K)\big)$ (by 1 of the Lifting Hypothesis), and all the formulas appearing in Step II are true. We then have:

$$\mathrm{ord}_p\Big(\#\mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K)\Big) + t_g(\ell) \overset{\text{Eq. (2.30)}}{=} \mathrm{ord}_p\Big(L^{\mathrm{alg}}(g/K,1)\Big) \overset{\text{Eq. (2.11)}}{=} \mathrm{ord}_p\big(I(P_K)\big) + t_g(\ell),$$

giving us in particular:

$$\mathrm{ord}_p\Big(\#\mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K)\Big) = \mathrm{ord}_p\big(I(P_K)\big). \tag{2.14}$$

Since $n > 2\mathrm{ord}_p\big(I(P_K)\big)$ by part 1 of Hypothesis 2.3.2, we deduce in particular that p^n kills the $\mathfrak{p}^\infty$-Selmer group of A_g/K, which implies: $\mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K) = \mathrm{Sel}_{\mathfrak{p}^n}(A_g/K)$ [4]. On the other hand, equation (2.12) tells us that the latter has the same cardinality as $\underline{\mathrm{III}}(E/K)[p^n]$, which in turn equals $\underline{\mathrm{III}}(E/K)[p^\infty]$, again by part 1 of the Lifting Hypothesis 2.3.2. Then equation (2.14) can be finally translated as:

$$\mathrm{ord}_p\Big(\#\underline{\mathrm{III}}(E/K)[p^\infty]\Big) = \mathrm{ord}_p\big(I(P_K)\big).$$

[3] To derive this from equation (2.13), we note that the natural surjection $\mathrm{Sel}_{\mathfrak{p}}(A_g/K) \twoheadrightarrow \mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K)[p]$ is an isomorphism. Indeed its kernel is $A_g(K)[\mathfrak{p}] \cong E(K)[p]$, which is zero (e.g. by Mazur's Theorem, since $p > 7$). In particular, we have: $\mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K) = 0$ if and only if $\mathrm{Sel}_{\mathfrak{p}}(A_g/K) = 0$, as desired.

[4] The natural map $\mathrm{Sel}_{\mathfrak{p}^n}(A_g/K) \to \mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K)[\mathfrak{p}^n] = \mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K)[p^n]$ is always surjective, and since $0 = E(K)[p^n] = A_g(K)[\mathfrak{p}^n]$ in our case (as $p > 7$ and $E[p]$ is irreducible by assumption), it is also injective.

2.4 Raising the level in the quaternionic setting

2.4.1 n-admissible primes and finite cohomology

Let us fix for the rest of this Section a positive integer n, and an n-admissible prime ℓ relative to (f, K, n); see Definition 2.3.1. Let K_ℓ denotes the completion of K at the unique prime dividing ℓ. Define the *finite/singular cohomology at* ℓ as:

$$\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) := \ker(\mathrm{H}^1(K_\ell, E[p^n]) \to \mathrm{H}^1(K_\ell^{\mathrm{unr}}, E[p^n]));$$

$$\mathrm{H}^1_{\mathrm{sing}}(K_\ell, E[p^n]) := \frac{\mathrm{H}^1(K_\ell, E[p^n])}{\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n])},$$

where $K_\ell^{\mathrm{unr}}/K_\ell$ is the maximal unramified extension of K_ℓ. The following result is essentially Lemma 2.6 of [BD]. We recall its proof in order to fix notations and for later reference.

Lemma 2.4.1. *We have a decomposition of $\mathbb{Z}/p^n\mathbb{Z}[G_{K_\ell}]$-modules*

$$E[p^n] \cong \mu_{p^n} \oplus \mathbb{Z}/p^n\mathbb{Z},$$

where $\mu_{p^n} := \mu_{p^n}(\overline{K}_\ell)$ (and $\mathbb{Z}/p^n\mathbb{Z}$ is considered as a G_{K_ℓ}-module with trivial action). Moreover, under this decomposition, we have isomorphisms:

$$\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathrm{H}^1(K_\ell, \mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}/p^n\mathbb{Z}; \quad \mathrm{H}^1_{\mathrm{sing}}(K_\ell, E[p^n]) \cong \mathrm{H}^1(K_\ell, \mu_{p^n}) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Proof. Since ℓ does not divides the conductor of $E/\mathbb{Q}$, the Galois representation $E[p^n]$ is unramified at ℓ, i.e. the action of G_{K_ℓ} on $E[p^n]$ factors through an action of the quotient group G_{K_ℓ}/I_{K_ℓ}, where I_{K_ℓ} is the inertia subgroup ([Si, Chapter VII]). By condition 2 in the Definition 2.3.1, the latter quotient is isomorphic to $\mathrm{Gal}(K_\ell^{\mathrm{unr}}/K_\ell) \cong G_{\mathbb{F}_{\ell^2}} := \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_{\ell^2}) \cong \hat{\mathbb{Z}}$ (with $\mathbb{F}_{\ell^k}$ denoting the field with ℓ^k elements), and is topologically generated by Frob_ℓ^2 (where $\mathrm{Frob}_\ell \in G_{\mathbb{F}_\ell}$ is the usual Frobenius). As explained in Chapter V and Chapter VII of [Si], the trace (resp., determinant) of the Frobenius Frob_ℓ acting on $E[p^n]$ is $a_\ell(E)$ (resp., ℓ). By condition 4 in Definition 2.3.1, we then obtain: the characteristic polynomial of Frob_ℓ acting on $E[p^n]$ is

$$X^2 \mp (\ell + 1) \cdot X + \ell \in \mathbb{Z}/p^n\mathbb{Z}[X].$$

In other words: Frob_ℓ acts on $E[p^n]$ with eigenvalues ± 1 and $\pm\ell$, so that Frob_ℓ^2 acts on $E[p^n]$ with eigenvalues 1 and ℓ^2. In addiction: by condition 3 in Definition 2.3.1, ℓ^2 is different from 1 (in $\mathbb{Z}/p^n\mathbb{Z}$). Since Frob_ℓ^2 acts on the unramified G_{K_ℓ}-module μ_{p^n} with eigenvalue ℓ^2, this gives us the claimed decomposition of $\mathbb{Z}/p^n\mathbb{Z}[G_{K_\ell}]$-modules:

$$E[p^n] \cong \mu_{p^n} \oplus \mathbb{Z}/p^n\mathbb{Z}.$$

In particular, applying cohomology to this decomposition, we deduce the decomposition:

$$\mathrm{H}^1(K_\ell, E[p^n]) \cong \mathrm{H}^1(K_\ell, \mu_{p^n}) \oplus \mathrm{H}^1(K_\ell, \mathbb{Z}/p^n\mathbb{Z}). \tag{2.15}$$

Using Hensel's Lemma and the ℓ-adic logarithm, we have

$$K_\ell^* = \ell^{\mathbb{Z}} \times \mu_{\ell^2-1} \times 1 + \ell\mathcal{O}_\ell \cong \mathbb{Z} \times \mu_{\ell^2-1} \times \mathbb{Z}_\ell^2$$

where $\mathcal{O}_\ell$ is the ring of integers of K_ℓ. By Kummer theory, we then deduce

$$\mathrm{H}^1(K_\ell, \mu_{p^n}) \cong K_\ell^* \otimes \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}/p^n\mathbb{Z},$$

since by property 3 in Definition 2.3.1, $p \nmid \ell^2 - 1$. By Tate local duality [Da, Theorem 10.9]:

$$H^1(K_\ell, \mathbb{Z}/p^n\mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}\Big(H^1(K_\ell, \mu_{p^n}), \mathbb{Z}/p^n\mathbb{Z}\Big) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

In order to conclude the proof of the Lemma, it remains to prove:

$$\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) = \mathrm{H}^1(K_\ell, \mathbb{Z}/p^n\mathbb{Z}) \tag{2.16}$$

(under the decomposition (2.15)). By [Se, Proposition 1, Chapter XIII], we have

$$\rho_\ell : \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong E[p^n]/(\mathrm{Frob}_\ell^2 - 1)E[p^n].$$

More precisely: let $\xi \in \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n])$, and let $\xi_o : G_{K_\ell} \to E[p^n]$ be 1-cocycle representing ξ. By definition, there exists $P \in E[p^n]$ such that $\xi_o(h) = P^h - P$ for every $h \in I_{K_\ell}$. Subtracting to ξ_o the 1-coboundary $G_K \to E[p^n]; g \mapsto P^g - P$, we see that $\xi = [\xi^o]$ is represented by a 1-cocycle ξ^o which factors through a 1-cocycle $\xi^o : G_{K_\ell}/I_{K_\ell} \cong G_{\mathbb{F}_{\ell^2}} \to E[p^n]$. With these notations:

$$\rho_\ell(\xi) := \xi^o\big(\mathrm{Frob}_\ell^2\big) \bmod \big(\mathrm{Frob}_\ell^2 - 1\big) \cdot E[p^n].$$

Using the decomposition $E[p^n] \cong \mu_{p^n} \oplus \mathbb{Z}/p^n\mathbb{Z}$, let $\mathbf{P} \in E[p^n]$ (resp., $\mathbf{Q} \in E[p^n]$) be a basis for the 1-eigenspace (resp., ℓ^2-eigenspace) for the action of Frob_ℓ^2 on $E[p^n]$. Then

$$E[p^n]/(\mathrm{Frob}_\ell^2 - 1)E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z} \cdot \mathbf{P} \cong \mathbb{Z}/p^n\mathbb{Z}$$

as Frob_ℓ^2-modules (using again that $p \nmid \ell^2 - 1$). Moreover, with the notations above, write $\xi^o = \xi^o_{\mathbf{P}} \oplus \xi^o_{\mathbf{Q}}$, for 1-cocycles $\xi^o_\star : G_{\mathbb{F}_{\ell^2}} \to \mathbb{Z}/p^n\mathbb{Z} \cdot \star$, and accordingly $\xi = \xi_{\mathbf{P}} \oplus \xi_{\mathbf{Q}}$. By the preceding discussion, we then obtain an isomorphism:

$$\theta_\ell : \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z} \cdot \mathbf{P}; \quad \theta_\ell(\xi) = \xi^o\big(\mathrm{Frob}_\ell^2\big) = \xi^o_{\mathbf{P}}\big(\mathrm{Frob}_\ell^2\big) = \theta_\ell(\xi_{\mathbf{P}}).$$

Since θ_ℓ is an isomorphism, this shows in particular that $\xi_{\mathbf{Q}} = 0$, i.e. $\xi = \xi_{\mathbf{P}}$. In other words: $\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \subset H^1(K_\ell, \mathbb{Z}/p^n\mathbb{Z} \cdot \mathbf{P})$, and the latter cohomology module is identified by construction with $H^1(K_\ell, \mathbb{Z}/p^n\mathbb{Z})$ under the decomposition (2.15). Since both cohomology groups have the same cardinality p^n, they have to be equal, thus proving the claim (2.16), and with it the Lemma. □

2.4.2 The map γ

Recall that $f = \sum_{n \geq 1} a_n q^n$ denotes the newform attached to $E/\mathbb{Q}$ by the result of [Wi] and [TW], and $\mathbb{T}$ denotes be the Hecke algebra of level N acting on the Jacobian of $X_0(N)$. More precisely: write $J := J_0(N)_{/\mathbb{Q}}$ for the Jacobian variety of $X_0(N)_{/\mathbb{Q}}$. There are indeed two natural actions of $\mathbb{T}$ on J, the Albanese and the Picard one (arising from viewing J as an Albanese of Picard variety respectively). Equip the Jacobian with the action of $\mathbb{T}$ induced by Picard (contravariant) functoriality. The form f determines an algebra homomorphism

$$f : \mathbb{T} \to \mathbb{Z}/p^n\mathbb{Z}, \qquad T_n \mapsto a_n \pmod{p^n},$$

denoted in the same way by an abuse of notation. Write $\mathcal{I}_f$ for its kernel. We are now interested in constructing a modular form of level $N\ell$ congruent to f modulo p^n. As discussed in Chapter I, the existence of a similar form in a result due to Ribet. We are moreover giving an explicit description of the form we are constructing. Most of the ideas and the techiniques are borrowed from Bertolini and Darmon work [BD], in particular section 9. There are some difference in between their work and the present. The first is that Bertolini and Darmon results are written in the setting of Shimura curves, while we are working only with modular curve. The second difference is in the fact that the raising the level result of [BD] is in two n-admissible primes. In our setting we are raising the level just in one prime.

The assumption that p does not divide the degree d_E of the modular parametrization implies that f is p-isolated, as remarked in Lemma 2.2 of [BD](but see also Theorem 2.2 of [ARS2] for details). Since $E[p]$ is an irreducible $\mathbb{F}_p[G_{\mathbb{Q}}]$-module, the modular parametrisation φ_E induces an isomorphism

$$\mathrm{Ta}_p(J)/\mathcal{I}_f \cong E[p^n].$$

Let us fix, once an and for all, such an isomorphism, under which we identify the modules involved. Then, the map

$$J(K_\ell)/\mathcal{I}_f \to \mathrm{H}^1(K_\ell, \mathrm{Ta}_p(J)/\mathcal{I}_f)$$

arising form Kummer theory yields a map

$$J(K_\ell)/\mathcal{I}_f \to \mathrm{H}^1(K_\ell, E[p^n]). \tag{2.17}$$

The image of (2.17) is equal to the group of unramified classes, since $E[p^n]$ is unramified at ℓ and ℓ is a prime of good reduction for J.

Since $\ell \nmid Np$ (so in particular the modular Jacobian J has good reduction at ℓ), and since ℓ is inert in K, we have a natural reduction map $\mathrm{red}_\ell : J(K_\ell) \to J(\mathbb{F}_\ell)$, inducing an isomorphism

$$J(K_\ell)/\mathcal{I}_f \to J(\mathbb{F}_{\ell^2})/\mathcal{I}_f. \tag{2.18}$$

By composing the inverse of (2.18) with (2.17), and fixing an identification of $\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n])$ and $\mathbb{Z}/p^n\mathbb{Z}$ as in the Lemma (2.4.1), we then get a surjective map

$$J(\mathbb{F}_{\ell^2})/\mathcal{I}_f \to \mathbb{Z}/p^n\mathbb{Z}. \tag{2.19}$$

Let $\mathcal{S}_\ell \subset X_0(N)(\mathbb{F}_{\ell^2})$ denotes the set of supersingular points of $X_0(N)$ in characteristic ℓ, and let $\mathrm{Div}(\mathcal{S}_\ell)$, resp. $\mathrm{Div}^0(\mathcal{S}_\ell)$ be the module of formal divisor, resp. degree zero divisors with $\mathbb{Z}$-coefficients supported on $\mathcal{S}_\ell$.

We make convention that $\mathbb{T}$ acts on the supersingular points by Albanese (covariant) functoriality instead of Picard's one, since it makes no difference in establishing the Hecke equivariance of the maps defined below. In fact a Hecke correspondence induces two different morphisms T and ξ via Picard and Albanese functoriality. The reader is referred to [Ri] for details of definitions. Denoting by w_N the Fricke involution, the relation

$$w_N T w_N = \xi$$

holds. In particular the Hecke operators induce the same endomorphism via Picard and Albanese functiorality. This is clear for Hecke operators corresponding to the primes not dividing the level. For the other primes, observe that the corresponding Hecke operators are

involutions and then, by a general property of curves, the two functoriality induces the same endomorphism. A complete exposition is contained in [Ri].

We note that the ideal $\mathcal{I}_f$ is *not* eisenstain (since by assumption $E[p]$ is irreducible, so that f cannot by cannot be congruent to an Eisenstein series modulo p^n). This implies easily that the natural inclusion of $\mathrm{Div}^0(\mathcal{S}_\ell)$ in $\mathrm{Div}(\mathcal{S}_\ell)$ induces an identification of the quotients $\mathrm{Div}^0(\mathcal{S}_\ell)/\mathcal{I}_f$ and $\mathrm{Div}(\mathcal{S}_\ell)/\mathcal{I}_f$. One then obtains a natural map

$$\mathrm{Div}(\mathcal{S}_\ell) \to J(\mathbb{F}_{\ell^2})/\mathcal{I}_f \tag{2.20}$$

that composed with the map (2.19) yields a map

$$\gamma : \mathrm{Div}(\mathcal{S}_\ell) \to \mathbb{Z}/p^n\mathbb{Z}.$$

As above denote by $\mathbb{T}$ be the Hecke algebra acting on $X_0(N)$. Write T_q $(q \nmid N)$ and U_q $(q \mid N)$ for the q-th Hecke operator in $\mathbb{T}$ and $\bar{T}_q$ and $\bar{U}_q$ for the natural image of T_q and U_q resp. in $\mathbb{T}/\mathcal{I}_f = \mathbb{Z}/p^n\mathbb{Z}$. Thus the following equalities modulo p^n hold: $\bar{T}_q \equiv a_q$ for $q \nmid N$ $\bar{U}_q \equiv a_q$ for $q|N$, and, since the prime ℓ is n-admissible $\bar{T}_\ell \equiv \epsilon(\ell+1)$.

The following proposition states the Hecke equivariance of the maps.

Proposition 2.4.2. *Let $x \in \mathrm{Div}(\mathcal{S}_\ell)$, the relations*

i. $\gamma(T_q x) = \bar{T}_q \gamma(x) \quad (q \nmid N)$

ii. $\gamma(U_q x) = \bar{U}_q \gamma(x) \quad (q \mid N)$

iii. $\gamma(\mathrm{Frob}_\ell\, x) = \epsilon\gamma(x)$

holds.

Proof. The proof follows quite closely the proof of Proposition 9.1 of [BD]. In Lemma 2.4.1 we obtained an identification

$$\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \frac{E[p^n]}{(\mathrm{Frob}_\ell^2 - 1)E[p^n]}.$$

This provides an explicit description of γ sending a point x to the image of $(\mathrm{Frob}_\ell^2 - 1)/p^n)x$ in $E[p^n]/(\mathrm{Frob}_\ell^2 - 1)E[p^n]$. It follows the equivariance of γ for the action of the operators T_q and U_q. As for *iii.* and *iv.*, recall that by the Eichler-Shimura relations the operator T_ℓ acts the correspondence $\mathrm{Frob}_\ell + \mathrm{Frob}_\ell^\vee$, $\mathrm{Frob}_\ell^\vee$ being the transpose of the Frobenius at ℓ. For points x defined over $\mathbb{F}_{\ell^2}$ we have the relation $\mathrm{Frob}_\ell^\vee\, x = \ell\, \mathrm{Frob}_\ell\, x$ and hence

$$T_\ell x = (\mathrm{Frob}_\ell + \mathrm{Frob}_\ell^\vee)x = (\ell+1)\, \mathrm{Frob}_\ell\, x.$$

By definition of n-admissible prime, note that $(\ell+1)$ is invertible in $\mathbb{Z}/p^n\mathbb{Z}$. The Frobenius at ℓ acts on the module $E[p^n]$ with eigenvalues ϵ and $\epsilon\ell$ hence it acts on the quotient $E[p^n]/(\mathrm{Frob}_\ell^2 - 1)E[p^n]$ by ϵ. □

2.4.3 The surjectivity of γ

In order to give an explicit description of a modular form obtained from f by raising the level, we need to show the surjectivity of the map γ that, up to some identifications, coincide with the sought-for modular form. In order to estabilish the surjectivity of the map γ defined above we need to fix notations and recall some results. First, let F be a field, we will denote by G_F the absolute Galois group $\mathrm{Gal}(\bar{F}/F)$. Let us begin with a general fact of cohomology, whose proof is contained in Chapter VI of [Se].

Theorem 2.4.3 (Lang triviality lemma)**.** *Let A be a connected algebraic group over a finite field k. Then*

$$\mathrm{H}^1(k, A) = 0.$$

Consider the covering $X_1(N) \to X_0(N)$. By Picard functoriality on the Jacobians, we have a map

$$\pi^* : J_0(N) \to J_1(N)$$

whose kernel $\mathrm{Sh}_N := \ker \pi^*$ is called the Shimura subgroup. Similarly, using Albanese functoriality we have

$$\pi_* : J_1(N) \to J_0(N)$$

and denote $\Sigma_N := \ker \pi_*$.

Definition 2.4.4. A μ-type group is a finite flat group scheme whose Cartier dual is a constant group.

Proposition 2.4.5 (Mazur, [Ma1], Prop.11.6)**.** *There is a natural isomorphism between the group of connected components of Σ_N and the Cartier dual of the Shimura subgroup Sh_N^D. Furthermore the Shimura subgroup is a μ-type group and in partirular it is finite and flat over $\mathbb{F}_\ell$.*

Proposition 2.4.6. *The map γ defined above is surjective.*

Proof. The map

$$J_0(\mathbb{F}_{\ell^2})/\mathcal{I}_f \to \mathbb{Z}/p^n\mathbb{Z}$$

is surjective, so it suffices to show the surjectivity of the natural map

$$J_0(\mathbb{F}_{\ell^2})^{ss} \to J_0(\mathbb{F}_{\ell^2})/\mathcal{I}_f.$$

The group Σ_N is defined by the exact sequence

$$0 \to \Sigma_N \to J_1(N) \to J_0(N);$$

taking Galois cohomology over $\mathbb{F}_{\ell^2}$ and using Lang's triviality lemma, we have the following exact sequence

$$J_1(N)(\mathbb{F}_{\ell^2}) \to J_0(N)(\mathbb{F}_{\ell^2}) \to \mathrm{H}^1(G_{\mathbb{F}_{\ell^2}}, \Sigma_N) \to 0. \tag{2.21}$$

Applying the result of Mazur stated in Proposition2.4.5, with another application of Lang's result, we have the isomorphism

$$\mathrm{H}^1(G_{\mathbb{F}_{l^2}}, \Sigma_N) \cong \mathrm{Sh}_N^D(\mathbb{F}_{\ell^2}).$$

The sequence (2.21) is equivariant under the action of the Galois group $\mathrm{Gal}(\mathbb{F}_{\ell^2}/\mathbb{F}_\ell)$. Since the action of $\mathrm{Gal}(\mathbb{F}_{\ell^2}/\mathbb{F}_\ell)$ on $\mathrm{H}^1(G_{\mathbb{F}_{l^2}}, \Sigma_N)$ is trivial, we have the following isomorphism of group schemes

$$J_0(N)(\mathbb{F}_{\ell^2})/\pi_*(J_1(N)(\mathbb{F}_{\ell^2})) \cong \mathrm{Sh}_N^D(\mathbb{F}_{\ell^2}).$$

All the supersingular points of $X_1(N)$ in characteristic ℓ are defined over $\mathbb{F}_{\ell^2}$ hence the image of $J_1(N)(\mathbb{F}_{\ell^2})$ in $J_0(N)(\mathbb{F}_{\ell^2})$ contains $J_1(N)(\mathbb{F}_{\ell^2})^{ss}$.

We claim, that

$$J_0(N)(\mathbb{F}_{\ell^2})/J_0(N)(\mathbb{F}_{\ell^2})^{ss} \cong \mathrm{Sh}_N^D(\mathbb{F}_{\ell^2}). \tag{2.22}$$

Assume the claim, and denote by $\mathfrak{m}_f$ the maximal ideal of $\mathbb{T}$ containing $\mathcal{I}_f$. By a result of Ribet, more precisely Theorem 1 of [Ri5] the group Sh_N is Eisenstein. As a consequence:

$$\mathrm{Sh}_N^D(\mathbb{F}_{\ell^2})[\mathfrak{m}_f] = \mathrm{Hom}_{\mathbb{F}_{\ell^2}}(\mathrm{Sh}_N, \mathbb{F}_{\ell^2})[\mathfrak{m}_f] = 0.$$

By duality, also the quotient $\mathrm{Sh}_N/\mathfrak{m}_f = 0$. Nakayama's lemma implies the triviality of $\mathrm{Sh}_N/\mathcal{I}_f$ that combined with the isomorphism (2.22) yields the surjectivity of γ. For the proof of the claim see the lemma below. □

Lemma 2.4.7. *Using the same notation of Proposition 2.4.6, there is an isomorphism*

$$J_0(N)(\mathbb{F}_{\ell^2})/J_0(N)(\mathbb{F}_{\ell^2})^{ss} \cong \mathrm{Sh}_N^D(\mathbb{F}_{\ell^2}).$$

Proof. First note that it is enough to show that

$$\#(J_0(N)(\mathbb{F}_{\ell^2})/J_0(N)(\mathbb{F}_{\ell^2})^{ss} \leq \#(\mathrm{Sh}_N^D(\mathbb{F}_{\ell^2}))$$

Indeed, all the supersingular points of $X_1(N)$ are defined over $\mathbb{F}_{\ell^2}$ and the image of $J_1(N)(\mathbb{F}_{\ell^2})$ in $J_0(N)(\mathbb{F}_{\ell^2})$ contains the subgroup $J_0(N)(\mathbb{F}_{\ell^2})^{ss}$. We will show that $J_0(N)(\mathbb{F}_{\ell^2})/J_0(N)(\mathbb{F}_{\ell^2})^{ss}$ is a quotient of Sh_N^D. This combined with the isomorphism

$$J_0(N)(\mathbb{F}_{\ell^2})/\pi_*(J_1(N)(\mathbb{F}_{\ell^2})) \cong \mathrm{Sh}_N^D(\mathbb{F}_{\ell^2}),$$

proves our claim. We need some results on coverings of modular curve, most of them are borrowed from Ihara's work [Ih]. First, the modular curve $X(N)$ corresponding to the full congruence subgroup $\Gamma(N)$ has no unramified coverings over $\mathbb{F}_{\ell^2}$ which are completely split at supersingular points of $X(N)$. By base change, all the unramified coverings of $X_0(N)$ that are completely split at supersingular points, are contained in $X(N)$ over $\mathbb{F}_{\ell^2}$. In particular there is an identification between $X_1(N)$ and the maximal abelian cover of $X_0(N)$ in $X(N)$. Furthermore, the Galois group of the maximal unramified covering of $X_0(N)$ which is contained in $X_1(N)$ is identified with $J_0(N)(\mathbb{F}_{\ell^2})^{ss}$.

Now, let G be a subgroup of $J_0(N)(\mathbb{F}_{\ell^2})$. G gives rise to an unramified abelian cover of $X_0(N)$ over $\mathbb{F}_{\ell^2}$ with Galois group $J_0(N)(\mathbb{F}_{\ell^2})/G$. Taking $G = J_0(N)(\mathbb{F}_{\ell^2})^{ss}$, we get a covering of $J_0(N)(\mathbb{F}_{\ell^2})/J_0(N)(\mathbb{F}_{\ell^2})^{ss}$ in which all supersingular points of $X_0(N)$ are split. □

2.4.4 Modular forms on quaternion algebras

Our aim in this section is to obtain an explicit raising the level. In particular we will show that γ can be identified with a certain quaternionic modular form.

Recall the algebras $\mathbb{T}_\ell \twoheadrightarrow \mathbf{T}_\ell$ introduced in Section 2.3, Step I. Then $\mathbf{T}_\ell$ is the $\mathbb{Z}$-module generated by all the Hecke operators of level $N\ell$ acting on the space $S_2^{\ell\text{-new}}(\Gamma_0(N\ell), \mathbb{C})$ of cusp forms of level $\Gamma_0(N\ell)$ which are new at ℓ. To avoid any confusions between the generators of $\mathbb{T}$ and $\mathbf{T}_\ell$, we denote by T_q, for primes $q \nmid N$ (resp., t_q, for primes $q \nmid N\ell$), and U_q, for primes $q|N$ (resp., u_q, for primes $q|N\ell$) the generators of the $\mathbb{Z}$-algebra $\mathbb{T}$ (resp., $\mathbf{T}_\ell$). We will prove the following Theorem, analogue in our setting to Theorem 5.18 of [BD].

Theorem 2.4.8. *There exists a surjective homomorphism*

$$\overline{g} := \overline{g}_\ell : \mathbf{T}_\ell \to \mathbb{Z}/p^n\mathbb{Z},$$

satisfying $\overline{g}(t_q) = f(T_q)$ for primes $q \nmid N\ell$, $\overline{g}(u_q) = f(U_q)$ for primes $q \mid N$, and $\overline{g}(u_\ell) = \epsilon$.

Using the Jacquet-Langlands correspondence, we can rephrase this Theorem in terms of modular forms on a suitable quaternion algebra. More precisely: let $B = B(\ell\infty)$ be the definite quaternion algebra ramified precisely at ℓ and ∞, and let R be an Eichler $\mathbb{Z}$-order of level N in B. In Section 2.3, Step I, we have associated to this data the double coset space

$$\mathcal{X}_{N,\ell} := \widehat{R}^\times \backslash \widehat{B}^\times / B^\times = \mathcal{V}/\Gamma,$$

where $\mathcal{V}$ is the set of vertices of the Bruhat-Tits tree of $\mathrm{PGL}_2(\mathbb{Q}_p)$ and $\Gamma \cong R[1/p]^\times$ (and the last identification comes from strong approximation). The group $\mathrm{Pic}(\mathcal{X}_{N,\ell}) = \mathrm{Pic}(\mathcal{V}/\Gamma)$ of divisors on $\mathcal{X}_{N,\ell} = \mathcal{V}/\Gamma$ is equipped with a natural action of the Hecke algebra $\mathbf{T}_\ell$ (see [BD3] for more details) [5]. For every ring A, this induces an action of $\mathbf{T}_\ell$ on the A-module $S_2(\mathcal{V}/\Gamma, A)$ of A-valued modular forms on $\mathcal{V}/\Gamma$. The Jacquet-Langlands correspondence gives us the following result.

Proposition 2.4.9 (Jacquet-Langlands correspondence)**.** *Let A be a ring. Write $S_2^\ell(N\ell, A)$ for the set of surjective ring morphisms $\psi : \mathbf{T}_\ell \to A$, and write $\mathcal{S}_2(\mathcal{V}/\Gamma; A)$ for the set of A-valued $\mathbf{T}_\ell$-eigenforms ϕ such that $\phi \notin pS_2(\mathcal{V}/\Gamma; A)$. Then there is a bijection:*

$$S_2^\ell(N\ell; A) \cong \mathcal{S}_2(\mathcal{V}/\Gamma; A).$$

If $\psi \in S_2^\ell(N\ell; A)$ corresponds to $\phi \in \mathcal{S}_2(\mathcal{V}/\Gamma; A)$ under this bijection, then $t_q(\phi) = \psi(t_q) \cdot \phi$ for every prime $q \nmid N\ell$, and $u_q(\phi) = \psi(u_q) \cdot \phi$ for every prime $q|N\ell$.

Thanks to the preceding Proposition, Theorem 2.4.8 is then equivalent to the following:

Theorem 2.4.10. *There exists a $\mathbf{T}_\ell$-eigenform $\overline{\phi}_\ell \in S_2(\mathcal{V}/\Gamma, \mathbb{Z}/p^n\mathbb{Z})$ such that:*

$$t_q(\overline{\phi}_\ell) = a_q \cdot \overline{\phi}_\ell; \quad u_{q'}(\overline{\phi}_\ell) = a_{q'} \cdot \overline{\phi}_\ell; \quad u_\ell(\overline{\phi}_\ell) = \epsilon \cdot \overline{\phi}_\ell$$

for every prime $q \nmid N\ell$ and every prime $q'|N$, and such that $\overline{\phi}_\ell \notin p \cdot S_2(\mathcal{V}/\Gamma, \mathbb{Z}/p^n\mathbb{Z})$.

[5] The notation $\mathrm{Pic}(\mathcal{X}_{N,\ell})$ for the group of divisors on the finite set $\mathcal{X}_{N,\ell}$ comes from the work of Gross. Indeed, Gross showed that $\mathrm{Pic}(\mathcal{X}_{N,\ell})$ can be naturally described as the Picard group of a certain finite union of genus-zero curves defined over $\mathbb{Q}$.

We will indeed construct the searched modular form $\overline{\phi}_\ell$ by using our map γ discussed in the preceding Sections. In order to do this, we need the following result of Ribet [Ri]. Recall that $\mathcal{S}_\ell \subset X_0(N)(\mathbb{F}_{\ell^2})$ denotes the set of supersingular points in the modular curve $X_0(N)_{/\mathbb{F}_\ell}$ in characteristic ℓ. In particular, by general principles, the group of divisors $\mathrm{Div}(\mathcal{S}_\ell)$ is equipped with an action of the level-N Hecke algebra $\mathbb{T}$.

Proposition 2.4.11. *There exists an isomorphism*

$$\xi_\ell : \mathrm{Pic}(\mathcal{X}_{N,\ell}) \cong \mathrm{Div}(\mathcal{S}_\ell),$$

satisfying the following properties: let $x \in \mathcal{X}_{N,\ell}$. Then

1. $\xi_\ell\big(t_q(x)\big) = T_q\big(\xi_\ell(x)\big)$, *for every prime $q \nmid N\ell$;*
2. $\xi_\ell\big(u_q(x)\big) = U_q\big(\xi_\ell(x)\big)$, *for every prime $q \nmid N$;*
3. $\xi_\ell\big(u_\ell(x)\big) = \mathrm{Frob}_\ell\big(\xi_\ell(x)\big)$.

Identifying $\mathcal{V}/\Gamma$ with $\mathcal{X}_{N,\ell}$ as above, we write again

$$\xi_\ell : \mathcal{V}/\Gamma \cong \mathcal{S}_\ell$$

for a bijection induced by an isomorphism ξ_ℓ as in the preceding Proposition.

Proof of Theorem 2.4.10. Let $\gamma : \mathrm{Div}(\mathcal{S}_\ell) \to \mathbb{Z}/p^n\mathbb{Z}$ be the map constructed in the Section 2.4.2. Combining Proposition 2.4.2 with Proposition 2.4.11, we deduce that

$$\overline{\phi}_\ell := \gamma \circ \xi_\ell$$

is a common eigenform for all the Hecke operators in $\mathbf{T}_\ell$, with Hecke eigenvalues as in the statement of the Theorem. By the surjectivity of γ established in Proposition 2.4.6, $\overline{\phi}_\ell$ is not contained in $p \cdot S_2(\mathcal{V}/\Gamma, \mathbb{Z}/p^n\mathbb{Z})$. □

The following is a Corollary of our method of proof.

Corollary 2.4.12. *Under the bijection $\xi_\ell : \mathcal{V}/\Gamma \cong \mathcal{S}_\ell$, the map $\gamma : \mathcal{V}/\Gamma \to \mathbb{Z}/p^n\mathbb{Z}$ defines an eigenform $\overline{\phi}_\ell \in S_2(\mathcal{V}/\Gamma, \mathbb{Z}/p^n\mathbb{Z})$ satisfying the conclusions of Theorem* 2.4.10.

2.5 Heegner points and a special value formula

We now exploit the computations of the preceding Section to prove a Jochnowitz congruence in the spirit of the work of Bertolini-Darmon [BD1] and [Va].

2.5.1 Gross points on definite quaternion algebras

In this Section we briefly recall the notion of Heegner, or Gross, points on our definite quaternion algebra $B = B(\ell\infty)$ ramified at ℓ and ∞. We refer to [BD3], [BD4] and [Va] for a much more detailed and general discussion.

Let R be an Eichler order of level N in B. An *orientation* on R is the choice of a collection of morphisms $v_q : R \otimes_{\mathbb{Z}} \mathbb{F}_q \to \mathbf{F}_q$, for every $q | N\ell$, where $\mathbf{F}_q := \mathbb{F}_q$ for $q | N$ and $\mathbf{F}_\ell := \mathbb{F}_{\ell^2}$. An *oriented Eichler order of level N* is a pair $(R, \{v_q\}_{q|N\ell})$, where R is an Eichler order of level

N, and $\{v_q\}_{q|N\ell}$ is an orientation. In the notations, we will often omit the reference to the orientation $\{v_q\}_{q|N\ell}$. Given $b \in B^*$, the order $R_b := bRb^{-1}$ is again an Eichler order of level N, and an orientation on R induces naturally an orientation of R_b. We can thus consider the finite set $\mathscr{C}_N(B)$ of conjugacy classes of oriented Eichler orders of level N in B. This is indeed an object we already know, thanks to the following:

Lemma 2.5.1. *There is a natural bijection: $\mathcal{X}_{N,\ell} \cong \mathscr{C}_N$.*

Proof. Let us fix an oriented Eichelr order R of level N. Given $\sigma \in \widehat{B}^\times$, it is easily verified that $R^\sigma := B \cap \sigma \cdot \widehat{R} \cdot \sigma^{-1}$ is again an Eichler order of level N, with a natural orientation (induced by that on R). It is also not difficult to show that the association $\sigma \mapsto R^\sigma$ induces the claimed bijection. We refer to [Vi] for details. □

Let us fix an orientation on $\mathcal{O} := \mathcal{O}_K$, i.e. the choice, for every prime $q|N\ell$, of a morphism $\mathcal{O} \to \mathbf{F}_q$. Given an oriented Eichler order R of level N, this gives us a natural notion of *oriented embedding* $f : \mathcal{O} \to R$.

Definition 2.5.2. A *Gross point of level N* (and conductor 1) is a pair (f, R), where R is an oriented Eichler order of level N in B, and where $f : K \to B$ is an embedding such that $f(K) \cap R = f(\mathcal{O})$, taken up to conjugation by $B^\times$. We write

$$\mathscr{G}_N := \mathscr{G}_N(1)$$

for the set of Gross points of level N.

Let $\mathrm{Pic}(\mathcal{O})$ be the class group of K, described in terms of finite ideles by:

$$\mathrm{Pic}(\mathcal{O}) = \widehat{\mathcal{O}}^\times \backslash \widehat{K}^\times / K^\times,$$

where we write again $\widehat{M} = M \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$. This allows us to define an action of $\mathrm{Pic}(\mathcal{O})$ on $\mathscr{G}_N$ as follows. Let $P \in \mathscr{G}_N$ be represented by a pair (f, R), and let $\sigma \in \widehat{K}^\times$. The embedding $f : K \to B$ induces a morphism $\hat{f} : \widehat{K} \to \widehat{B}$. Let

$$P^\sigma = (f, R^\sigma),$$

where $R^\sigma := B \cap \hat{f}(\sigma)\widehat{R}\hat{f}(\sigma)^{-1}$. It is easily verified that P^σ is again a Gross point of level N, and that we defined in this way an action of $\mathrm{Pic}(\mathcal{O})$ on $\mathscr{G}_N$. We have the following:

Proposition 2.5.3. *The action of $\mathrm{Pic}(\mathcal{O})$ on $\mathscr{G}_N$ already defined is simply transitive. In particular: there are exactly $h_K := \#\mathrm{Pic}(\mathcal{O})$ Gross points of level N.*

Proof. See [BD3] and the references listed there. □

We close this Section by pointing out that every M-valued form $\psi \in S_2(\mathcal{V}/\Gamma, M)$ gives rise to a map (denoted by the same symbol with a slight abuse of notation)

$$\psi : \mathscr{G}_N \longrightarrow M.$$

Indeed, as recalled in Section 2.4.4, strong approximation provides us with a canonical identification $\mathcal{V}/\Gamma = \mathcal{X}_{N,\ell}$, and by Lemma 2.5.1 we have a natural identification of $\mathcal{X}_{N,\ell}$ with the set $\mathscr{C}_N$ of conjugacy classes of oriented Eichler orders of level N in B. We can then view ψ as an M-valued function on $\mathscr{C}_N$. Finally, we have a natural 'forgetful map' $\mathscr{G}_N \to \mathscr{C}_N$, sending the Gross points represented by a pair (f, R) to the class in $\mathscr{C}_N$ of the oriented Eichler order R. Summing up, we define the map above as the composition:

$$\psi : \mathscr{G}_N \to \mathscr{C}_N \cong \mathcal{X}_{N,\ell} \cong \mathcal{V}/\Gamma \xrightarrow{\psi} M.$$

2.5.2 Reduction of Heegner points

Let H/K be the Hilbert class field of K. We recall that a point $x \in X_0(N)(\mathbb{C})$ is an *Heegner point of conductor* 1 if x is represented by an enhanced elliptic curve (A, C), where $A/\mathbb{C}$ is an elliptic curve with CM by the maximal order $\mathcal{O}$ of K, and $C \subset A$ is a cyclic subgroup of order N, stable under the action of $\mathcal{O}$. By the theory of complex multiplication, any such x is indeed rational over the Hilbert class field H/K of K, i.e. $x \in X_0(N)(H)$. Let us write $\mathscr{H}_N := \mathscr{H}_N(1) \subset X_0(N)(H)$ for the set of such Heegner points and conductor 1. The set $\mathscr{H}_N$ is equipped with a natural simply transitive action of $\mathrm{Gal}(H/K)$, and the latter group is identified by class field theory with the class group $\mathrm{Pic}(\mathcal{O})$ of K. Our aim in this Section is to explain how reduction modulo ℓ establishes a $\mathrm{Pic}(\mathcal{O})$-equivariant map from the set of Heegner points $\mathscr{H}_N$ to the set of Gross points $\mathscr{G}_N$.

Let is fix an ideal $\mathfrak{N} \subset \mathcal{O}$ such that $\mathcal{O}/\mathfrak{N} \cong \mathbb{Z}/N\mathbb{Z}$, which exists since we are assuming the Heegner hypothesis (i.e. every prime $q|N$ splits in K). We also fix a Heegner point $\mathbb{P} \in \mathscr{H}_N$, represented by a pair (A, C), where A/H is an elliptic curve defined over H with CM by $\mathcal{O}$, and $C := A[\mathfrak{N}]$ is its $\mathfrak{N}$-torsion submodule. Since ℓ is inert in K (by the definition of admissible prime), the elliptic curve A has *good supersingular* reduction modulo every prime of H dividing ℓ. More precisely: note that ℓ splits completely in H (as it is principal in K), and fix a prime $\mathfrak{l}|\ell$ of H. We will denote by $\bar{\cdot}$ every operations of reduction modulo $\mathfrak{l}$. Then the pair $(\overline{A}, \overline{C})$ is a supersingular enhanced elliptic curve over $\mathbb{F}_{\ell^2}$, and its endomorphism ring $\mathrm{End}(\overline{A})$ is a *maximal* order in the quaternion algebra

$$\mathrm{End}(\overline{A})_{\mathbb{Q}} := \mathrm{End}(\overline{A}) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B.$$

Let us fix such an isomorphism, which we consider as an equality. Let $\pi : \overline{A} \to \overline{A}/\overline{C} := \mathcal{A}$ be the natural isogeny. Then $\mathcal{A}/\mathbb{F}_{\ell^2}$ is again a supersingular elliptic curve, and its endomorphism ring $\mathrm{End}(\mathcal{A})$ is again isomorphic to a maximal order in B. The isogeny π induces an embedding $\mathrm{End}(\mathcal{A}) \hookrightarrow \mathrm{End}(\overline{A})_{\mathbb{Q}} = B$, defined by $\alpha \mapsto \pi^{-1} \circ \alpha \circ \pi$. It can be checked that

$$R_A := \mathrm{End}(\overline{A}) \cap \mathrm{End}(\mathcal{A})$$

is an Eichler order of level N in B. We have moreover a natural embedding

$$f_A : \mathcal{O} \longrightarrow R_A,$$

arising from the reduction modulo $\mathfrak{l}$ of endomorphisms: $\mathcal{O} \cong \mathrm{End}(A) \to \mathrm{End}(\overline{A})$. (Note that f_A indeed maps $\mathcal{O} \cong \mathrm{End}(A)$ into R_A, as follows easily by considering the embedding $\mathrm{End}(A/C) \hookrightarrow \mathrm{End}(A)_{\mathbb{Q}}$ arising as above by the natural isogeny $A \to A/C$.) After fixing an orientations of $\mathcal{O}$, we can put on R_A the orientation required to make f_A an oriented embedding. Then the pair (f_A, R_A) represents a Gross point $\mathfrak{g}(\mathbb{P}) \in \mathscr{G}_N$ of level N on B, which is easily seen to depend only on $\mathbb{P} \in \mathscr{H}_K$. In other words, we have defined a map

$$\mathscr{H}_N \to \mathscr{G}_N; \quad \mathbb{P} \mapsto \mathfrak{g}(\mathbb{P}).$$

We have the following Proposition; for a proof see [BD3] or [BD4].

Proposition 2.5.4. *Let $\mathbb{P} \in \mathscr{H}_N$ be a Heegner point, and let $\mathfrak{g}(\mathbb{P}) \in \mathscr{G}_N$ the corresponding Gross point. For every $\sigma \in \mathrm{Pic}(\mathcal{O})$ we have*

$$\mathfrak{g}\big(\mathbb{P}^{\sigma}\big) = \mathfrak{g}(\mathbb{P})^{\sigma},$$

where σ acts on $\mathbb{P} \in X_0(N)(H)$ via the reciprocity isomorphism $\mathrm{Pic}(\mathcal{O}) \cong \mathrm{Gal}(H/K)$, while it acts on $\mathfrak{g}(\mathbb{P})$ via the isomorphism $\mathrm{Pic}(\mathcal{O}) \cong \widehat{\mathcal{O}}^{\times} \backslash \widehat{K}^{\times} / K^{\times}$ (cf. Section 2.5.1).

2.5.3 Special values of quaternionic modular forms

Let $\overline{\phi}_\ell \in S_2(\mathcal{V}/\Gamma, \mathbb{Z}/p^n\mathbb{Z})$ be a mod-p^n eigenform satisfying then conclusions of Corollary 2.4.10. As in Section 2.5.1, we write again

$$\overline{\phi}_\ell : \mathscr{G}_N \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$$

for the associated 'restriction to Gross points'. Recall our Heegner point

$$P_K := \mathrm{Trace}_{H/K}\big(\varphi_E(\mathbb{P})\big),$$

where $\mathbb{P} \in \mathscr{H}_N$ is a fixed Heegner point of conductor one in $X_0(N)(H)$. Let us fix an isomorphism $\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z}$, and let us write

$$P_K(\ell) \in \mathbb{Z}/p^n\mathbb{Z}$$

for the image of P_K under the composition $E(K)/p^n \to E(K_\ell)/p^n \to \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n])$ arising from the local Kummer map. Thanks to the explicit description of $\overline{\phi}_\ell$ provided by Theorem 2.4.12, we can now prove the following:

Theorem 2.5.5. *Let $\mathbb{P} \in \mathscr{H}_N$ be a Heegner point of conductor one in $X_0(N)(H)$, and let $\mathfrak{g}(\mathbb{P}) \in \mathscr{G}_N$ be the corresponding Gross point of level N on B (cf. Section 2.5.1). Then*

$$\sum_{\sigma \in \mathrm{Pic}(\mathcal{O}_K)} \overline{\phi}_\ell\Big(\mathfrak{g}(\mathbb{P})^\sigma\Big) \doteq P_K(\ell),$$

where $\doteq$ denotes equality in $\mathbb{Z}/p^n\mathbb{Z}$ up to multiplication by a unit.

Proof. Write for simplicity $J := J_0(N)$ for the modular Jacobian of level N, and let

$$\kappa_\ell^J : J(K_\ell)/\mathcal{I}_f \longrightarrow \mathrm{H}^1_{\mathrm{fin}}(K_\ell, \mathrm{Ta}_p(J)/\mathcal{I}_f) \cong \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z}$$

be the morphism arising from the local Kummer map on $J(K_\ell)$, recalling that the modular parametrisation φ_E induces an isomorphism $\mathrm{Ta}_p(J)/\mathcal{I}_f \cong E[p^n]$. Similarly write

$$\kappa_\ell^E : E(K_\ell) \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z}$$

for the morphism induced by the local Kummer map on $E(K_\ell)$. As we will prove in Lemma 2.5.6 below, (multiplying eventually the fixed isomorphism $\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z}$ by a p-adic unit) we have: $\kappa_\ell^E \circ \varphi_E = \kappa_\ell^J$, where we write again $\varphi_E : J(K_\ell)/\mathcal{I}_f \to E(K_\ell)/p^n$. Letting $P := \varphi_E(\mathbb{P})$, and letting $\infty \in X_0(N)(\mathbb{Q})$ be a point such that $\varphi_E(\infty) = 0$, this implies:

$$P_K(\ell) = \sum_{\sigma \in \mathrm{Gal}(H/K)} \kappa_\ell^E\big(P^\sigma\big) = \sum_{\sigma \in \mathrm{Gal}(H/K)} \kappa_\ell^J\big(\mathbb{P}^\sigma - \{\infty\}\big) \tag{2.23}$$

On the other hand: let $\mathfrak{P}$ denotes any one of the Heegner points $\mathbb{P}^\sigma$, for $\sigma \in \mathrm{Gal}(H/K)$, and let $\overline{\mathfrak{P}} := \mathrm{red}_\ell(\mathfrak{P}) \in X_0(N)(\mathbb{F}_{\ell^2})$ be the image of $\mathfrak{P}$ under the reduction at ℓ map. As explained in the preceding Section, $\overline{\mathfrak{P}} \in \mathcal{S}_\ell$ is a supersingular point. By the very definition of the morphism γ (see Section 2.3, Step I), we have

$$\gamma\big(\overline{\mathfrak{P}}\big) = \kappa_\ell^J\big(\mathfrak{P} - \{\infty\}\big). \tag{2.24}$$

After identifying $\mathcal{V}/\Gamma = \mathcal{X}_{N,\ell}$ with $\mathcal{S}_\ell$ under Proposition 2.4.11, Theorem (2.4.12) tells us that $\gamma(\overline{\mathfrak{P}}) = \overline{\phi}_\ell(\overline{\mathfrak{P}})$, so that (with a slight abuse of notations), equation (2.24) becomes:

$$\overline{\phi}_\ell(\overline{\mathfrak{P}}) = \kappa_\ell^J\big(\mathfrak{P} - \{\infty\}\big). \tag{2.25}$$

Recall now that we consider $\overline{\phi}_\ell : \mathcal{X}_{N,\ell} = \mathcal{S}_\ell \to \mathbb{Z}/p^n\mathbb{Z}$ as a function on Gross points via the following composition: $\mathscr{G}_N \to \mathscr{C}_N \cong \mathcal{X}_{N,\ell}$, the first map being the 'forgetful (the oriented embedding) map'. Since the Gross point $\mathfrak{g}(\mathfrak{P})$ maps to the reduction $\overline{\mathfrak{P}}$ under this last map (by definition!), we have (again by construction) $\overline{\phi}_\ell\big(\mathfrak{g}(\mathfrak{P})\big) = \overline{\phi}_\ell(\overline{\mathfrak{P}})$. Turning back to our old notations $\mathfrak{P} = \mathbb{P}^\sigma$, equation (2.25) then becomes: $\overline{\phi}_\ell\Big(\mathfrak{g}\big(\mathbb{P}^\sigma\big)\Big) = \kappa_\ell^J\big(\mathbb{P}^\sigma - \{\infty\}\big)$. Identifying now $\mathrm{Pic}(\mathcal{O}_K)$ with $\mathrm{Gal}(H/K)$ under the reciprocity map of class field theory, we can now appeal to Proposition 2.5.4 to obtain the identity:

$$\overline{\phi}_\ell\Big(\mathfrak{g}(\mathbb{P})^\sigma\Big) = \overline{\phi}_\ell\Big(\mathfrak{g}\big(\mathbb{P}^\sigma\big)\Big) = \kappa_\ell^J\big(\mathbb{P}^\sigma - \{\infty\}\big).$$

In tandem with equation (2.23), this equation allows to finally compute:

$$P_K(\ell) = \sum_{\sigma\in\mathrm{Gal}(H/K)} \kappa_\ell^J\big(\mathbb{P}^\sigma - \{\infty\}\big) = \sum_{\sigma\in\mathrm{Pic}(\mathcal{O}_K)} \overline{\phi}_\ell\Big(\mathfrak{g}(\mathbb{P})^\sigma\Big),$$

thus concluding the proof of the Theorem. □

Lemma 2.5.6. *We have a commutative diagram*

$$\begin{array}{ccc} J(K)/\mathcal{I}_f & \xrightarrow{\delta_J} & \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z} \\ \downarrow{\scriptstyle \varphi_E} & & \downarrow{\scriptstyle d} \\ E(K)/p^nE(K) & \xrightarrow{\delta_E} & \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z} \end{array}$$

where the vertical arrow is given by a p-adic unit d.

Proof. The modular parametrization induces by functoriality the maps:

$$\varphi^* : E(K) \to J(K)$$

$$\varphi_* : J(K) \to E(K).$$

By ptoperties of degree we have:

$$\begin{array}{ccc} E(K) & \xrightarrow{\deg(\varphi_E)} & E(K) \\ & {\scriptstyle\varphi^*}\searrow \quad \nearrow{\scriptstyle\varphi_*} & \\ & J(K). & \end{array}$$

The composition $\varphi_* \circ \varphi^*$ is a bijection, since p does not divide the degree of the modular parametrization. In particular φ^* is injective and φ_* is surjective.

We have the following diagram

$$\begin{array}{ccccc} E(K) & \longrightarrow & E(K)/p^nE(K) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi^*} & & \downarrow & & \\ J(K) & \longrightarrow & J(K)/\mathcal{I}_f & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi_*} & & \downarrow & & \\ E(K) & \longrightarrow & E(K)/p^nE(K) & \longrightarrow & 0. \end{array}$$

Now taking cohomology, we have

$$\begin{array}{ccc} E(K)/p^nE(K) & \longrightarrow & \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z} \\ \downarrow & & \downarrow{\scriptstyle \psi^*} \\ J(K)/\mathcal{I}_f & \longrightarrow & \mathrm{H}^1_{\mathrm{fin}}(K_\ell, \mathrm{Ta}_p(J)/\mathcal{I}_f) \cong \mathbb{Z}/p^n\mathbb{Z} \\ \downarrow & & \downarrow{\scriptstyle \psi_*} \\ E(K)/p^nE(K) & \longrightarrow & \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z}. \end{array}$$

The map φ^* commutes with Kummer map, hence provides an identification between $E[p^n]$ and $\mathrm{Ta}_p(J)/\mathcal{I}_f$ induced this time by contravariant functoriality. Since the composition $\psi_* \circ \psi^*$ is bijective the diagram commutes. □

2.5.4 Gross special value formula

In this Section we state Gross's special value formula, using in an essential a certain 'lifting assumption' and the results proved in [PW].

Notations and the 'lifting assumption'

Let n be a positive integer, and let ℓ be an n-admissible prime. Recall the $f : \mathbb{T} \to \mathbb{Z}_p$ is the morphism associated to $E/\mathbb{Q}$ by the Modularity Theorem. The results recalled in Section 2.4.4 attached to f and ℓ a surjective morphism $\overline{g} := \overline{g}_\ell : \mathbb{T}_\ell \twoheadrightarrow \mathbf{T}_\ell \to \mathbb{Z}/p^n\mathbb{Z}$ congruent to f modulo p^n. Moreover, via the Jacquet-Langlands correspondence, the mod-p^n form $\overline{g}$ corresponds to an eigenform $\overline{\phi}_\ell \in S_2(\mathcal{V}/\Gamma, \mathbb{Z}/p^n\mathbb{Z})$ (see Section 2.4.4). In this Section we will assume that $\overline{g}$ can be lifted to a true weight-two newform $g \in S_2(\Gamma_0(N\ell), \mathbb{Z}_p)$. More precisely, we will work under the following assumption: fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{Q}_p$, under which we will view algebraic numbers inside $\overline{\mathbb{Q}}_p$.

> (**Lift**) There exists a morphism $g : \mathbf{T}_\ell \to \mathbb{Z}_p$, arising from a weight-two newfrom $g \in S_2(\Gamma_0(N\ell), \mathbb{C})$ of level $\Gamma_0(N\ell)$, s.t.: for every prime $q \nmid N\ell$ and every prime $q'|N$
>
> $$g(t_q) = f(T_q); \quad g(u_{q'}) = f(U_{q'}).$$
>
> (Recall that t_q and u_q denotes the Hecke operators of level $N\ell$ in $\mathbf{T}_\ell$.)

As briefly explained in Section 2.4.4: via the Jacquet-Langlands correspondence, the form g corresponds to an eigenform

$$\phi_\ell \in S_2(\mathcal{V}/\Gamma, \mathbb{Z}_p),$$

uniquely determined up to p-adic units, and whose reduction modulo p^n satisfies the conclusions of Corollary 2.4.10.

Statement (cf. [PW])

Before stating Gross formula we still need a couple of definitions.

Definition 2.5.7. Let $L(g/K, s) := L(g, s) \cdot L(g, \epsilon_K, s)$ be the Hecke L-series of g/K, where $\epsilon_K : (\mathbb{Z}/D_K\mathbb{Z})^* \to \{\pm 1\}$ is the quadratic character attached to $K/\mathbb{Q}$. The *algebraic part* of the special value $L(g/K, 1)$ is defined as:

$$L^{\mathrm{alg}}(g/K, 1) := \frac{L(g/K, 1)}{\Omega_g^{\mathrm{can}}},$$

where the *canonical Shimura period* Ω_g^{can} is defined by

$$\Omega_g^{\mathrm{can}} := \frac{\langle g, g\rangle}{\eta_g(N\ell)}.$$

Here $\langle g, g\rangle$ is the Petersson norm of g, and $\eta_g(N\ell)$ is the *congruence number* associated to g (see Section 2.2 of [PW] for a precise definition). Thanks to a result of Shimura, we know that $L^{\mathrm{alg}}(g/K, 1)$ lives both in K_g and (under our fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$) in $\mathbb{Z}_p$.

We now defined the *Tamagawa exponent* of g at ℓ, following [PW]. As discussed in Section 2.3, Step III, attached to g we have an abelian variety $A_g/\mathbb{Q}$ with real multiplication by the maximal order $\mathcal{O}_g$ of $K_g/\mathbb{Q}$, and a prime $\mathfrak{p}$ of K_g such that the completion $\mathcal{O}_\mathfrak{p} \cong \mathbb{Z}_p$, and such that $A_g[\mathfrak{p}^n] \cong E[p^n]$ as $G_\mathbb{Q}$-modules.

Definition 2.5.8. (cf. Definition 3.3 of [PW]) The *Tamagawa exponent* $t_g(\ell)$ of g at ℓ is greatest integer m such that the $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$-representation $A_g[\mathfrak{p}^m]$ is unramified.

We are now ready to state the version of Gross formula we will need in what follows. We note that the Theorem below makes use of some of the results proved in the article [PW], to which we refer for more details and precise references. As in Section 2.5.1, we write again

$$\phi_\ell : \mathscr{G}_N \longrightarrow \mathbb{Z}_p$$

for the map on Gross points attached to the eigenform $\phi_\ell \in S_2(\mathcal{V}/\Gamma, \mathbb{Z}_p)$.

Theorem 2.5.9. *Let $\mathbb{P} \in \mathscr{H}_N$ be a Heegner point of conductor one in $X_0(N)(H)$, and let $\mathfrak{g}(\mathbb{P}) \in \mathscr{G}_N$ be the associated Gross points of level N on B (cf. Section 2.5.2). Then*

$$L^{\mathrm{alg}}(g/K, 1) \doteq p^{t_g(\ell)} \cdot \left(\sum_{\sigma \in \mathrm{Pic}(\mathcal{O}_K)} \phi_\ell\Big(\mathfrak{g}(\mathbb{P})^\sigma\Big) \right)^2,$$

where $\doteq$ denotes equality in $\mathbb{Z}_p$ up to multiplication by p-adic units.

Proof. This follows combining Lemma 2.2 and Theorem 6.8 of [PW]. □

2.5.5 Jochnowitz congruence

We continue to assume in this Section that hypothesis (**Lift**) holds. Moreover, consider the following assumptions: recall that $I(P_K) := [E(K) : P_K]$ denotes the index of the Heegner point P_K in $E(K)$.

(**Big**) $n > \mathrm{ord}_p\big(I(P_K)\big)$.

(**Loc**) The natural map $\iota_\ell : E(K) \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z} \to E(K_\ell) \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z}$ is injective.

We can now state the Jochnowitz congruence alluded to at the beginning of this Section.

Theorem 2.5.10. *Assume that Hypotheses* (**Lift**)*,* (**Big**) *and* (**Loc**) *are satisfied. Then:*

$$\mathrm{ord}_p\Big(L^{\mathrm{alg}}(g/K, 1)\Big) = \mathrm{ord}_p\big(I(P_K)\big) + t_g(\ell).$$

Proof. Note that $E(K)/p^n \cong \mathbb{Z}/p^n\mathbb{Z}$, since $E(K)$ has rank one and $E(K)[p] = 0$. It follows by Hypotheses (**Big**) and (**Loc**) that $0 \neq P_K(\ell) = I(P_K) \bmod p^n$, up to multiplication by units modulo p^n. The result then follows combining Theorem 2.5.5 and Theorem 2.5.9. □

2.6 Shafarevich-Tate groups

We assume in this Section that Hypothesis (**Lift**), and we retain the notations introduced in Section 2.3, Step III.

Proposition 2.6.1. *Assume that Hypotheses* (**Lift**) *and* (**Loc**) *are satisfied. Then we have the equality:*

$$\#\,\mathrm{Sel}_{\mathfrak{p}^n}(A_g/K) = \#\underline{\mathrm{III}}(E/K)[p^n].$$

Proof. By Lemma 2.4.1 we have:

$$\mathrm{H}^1(K_\ell, E[p^m]) = \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \oplus \mathrm{H}^1_{\mathrm{ord}}(K_\ell, E[p^n]),$$

and each of the direct summand is free of rank one over $\mathbb{Z}/p^n\mathbb{Z}$. Define $v_* : \mathrm{H}^1(K_\ell, E[p^n]) \to \mathrm{H}^1_*(K_\ell, E[p^n])$ by composing the restriction map at ℓ with the projection to H^1_*.

By Lemma 5 of [GP], the local conditions defining $\mathrm{Sel}_{p^n}(E/K)$ and $\mathrm{Sel}_{\mathfrak{p}^n}(A_g/K)$ as subgroups of $\mathrm{H}^1(K, E[p^n])$ match at all primes of K different from ℓ. In other words both the Selmer group live inside the Selmer group $\mathrm{Sel}^{(\ell)}_{p^n}(E/K)$ of E/K relaxed at ℓ. Moreover, Lemma 8 of *loc. cit.* tells us that the local condition defining $\mathrm{Sel}_{p^n}(E/K)$ (resp., $\mathrm{Sel}_{\mathfrak{p}}(A_g/K)$) at ℓ is the unramified (resp., singular, or ordinary) one, i.e. $\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n])$ (resp., $\mathrm{H}^1_{\mathrm{ord}}(K_\ell, E[p^n]) := \mathrm{H}^1_{\mathrm{sing}}(K_\ell, E[p^n])$). This is a consequence of the fact that E (resp., A_g) has good reduction (resp., purely toric reduction) at ℓ. [6] In particular, we have an exact sequence:

$$0 \to \mathrm{Sel}_{\mathfrak{p}^n}(A_g/K) \to \mathrm{Sel}^{(\ell)}_{p^n}(E/K) \xrightarrow{v_{\mathrm{fin}}} \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

By Hypothesis (**Loc**), $E(K)/p^nE(K)$ injects into $\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n])$. Since $E(K)/E(K)_{\mathrm{tors}} = \mathbb{Z} \cdot \widetilde{\mathbf{P}} \cong \mathbb{Z}$ and $E(K)[p] = 0$ under our assumptions (as $E[p]$ is irreducible and $p > 7$),

[6] Note that in [GP] the authors works 'modulo p', i.e. they consider the case $n = 1$. On the other hand, their proof of Lemma 5 and Lemma 8 works (as written) in our more general situation, taking $I = \mathfrak{p}^n$ instead of $I = \mathfrak{p}$ with the notations of *loc. cit.*

$E(K)/p^n \cong \mathbb{Z}/p^n\mathbb{Z}\cdot\widetilde{\mathbf{P}}$ is a free $\mathbb{Z}/p^n\mathbb{Z}$-module, generated by the reduction $\widetilde{\mathbf{P}}$ of $\mathbf{P}$. Moreover, $v_{\mathrm{ord}}(\widetilde{\mathbf{P}}) = 0$ (where we write again $\widetilde{\mathbf{P}} \in \mathrm{Sel}_{p^n}(E/K)$ for the image of $\widetilde{\mathbf{P}} \in E(K)/p^n$ under the injective Kummer map $E(K)/p^n \hookrightarrow \mathrm{H}^1(K, E[p^n])$). This allows us to conclude that the map v_{fin} in the last equation is surjective, giving us the exact sequence:

$$0 \to \mathrm{Sel}_{\mathfrak{p}^n}(A_g/K) \to \mathrm{Sel}^{(\ell)}_{p^n}(E/K) \overset{v_{\mathrm{fin}}}{\to} \mathbb{Z}/p^n\mathbb{Z} \to 0. \tag{2.26}$$

In particular this gives

$$\#(\mathrm{Sel}_{\mathfrak{p}^n}(A_g/K)) \cdot p^n = \#(\mathrm{Sel}^{(\ell)}_{p^n}(E/K)). \tag{2.27}$$

We claim that

$$\mathrm{Sel}_{p^n}(E/K) = \mathrm{Sel}^{(\ell)}_{p^n}(E/K). \tag{2.28}$$

Assume the claim: by Kummer theory we have and exact sequence:

$$0 \to E(K)/p^nE(K) \to \mathrm{Sel}_{p^n}(E/K) \to \underline{\mathrm{III}}(E/K)_{p^n} \to 0.$$

Recalling that (by assumption) $E(K)/E(K)_{\mathrm{tors}}$ is isomorphic to $\mathbb{Z}$, and that $E(K)$ has trivial p-torsion (as already noted above): combining the last equation with (2.27) we finally obtain:

$$\#(\underline{\mathrm{III}}(E/K)_{p^n}) = p^{-n}\#(\mathrm{Sel}_{p^n}(E/K)) = \#(\mathrm{Sel}_{\mathfrak{p}^n}(A_g/K)).$$

We are then left to prove the validity of (2.28). By the discussion above, this amount to show that for every $x \in \mathrm{Sel}^{(\ell)}_{p^n}(E/K)$ we have $v_{\mathrm{ord}}(x) = 0$ (or equivalently $\mathrm{res}_\ell(x) \in \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n])$). Let x and let y be an arbitrary element of $\mathrm{Sel}^{(\ell)}_{p^n}(E/K)$. By Poitou-Tate duality we have

$$\sum_v \langle \mathrm{res}_v(x), \mathrm{res}_v(y)\rangle_v = 0, \tag{2.29}$$

where

$$\langle -, -\rangle_v : \mathrm{H}^1(K_v, E[p^n]) \times \mathrm{H}^1(K_v, E[p^n]) \to \mathrm{H}^2(K_v, \mu_{p^n}) \cong \mathbb{Z}/p^n\mathbb{Z}$$

is the local Tate pairing induced by the Weil pairing on $E[p^n] \times E[p^n] \to \mu_{p^n}$ (see, e.g. Chapter 10 of [Da]). This is a perfect, symmetric pairing, such that $\mathrm{H}^1_{\mathrm{fin}}(K_v, E[p^n])$ and $\mathrm{H}^1_{\mathrm{sing}}(K_v, E[p^n])$ are maximal isotropic subspaces. Since $\mathrm{res}_v(\xi) \in \mathrm{H}^1_{\mathrm{fin}}(K_v, E[p^n])$ for every $v \neq \ell$ and every $\xi \in \mathrm{Sel}^{(\ell)}_{p^n}(E/K)$, equation (2.29) then reduce to the equality:

$$\langle \mathrm{res}_\ell(x), \mathrm{res}_\ell(y)\rangle_\ell = 0,$$

valid for every $x, y \in \mathrm{Sel}^{(\ell)}_{p^n}(E/K)$. Take now $y = \widetilde{\mathbf{P}}$ (with the notations introduced above), so that $\mathrm{res}_\ell(\widetilde{\mathbf{P}}) = v_{\mathrm{fin}}(\widetilde{\mathbf{P}}) \in \mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n]) \cong \mathbb{Z}/p^n\mathbb{Z}$ is a unit modulo p^n. Then the last equation becomes: $\langle \mathrm{res}_\ell(x), v_{\mathrm{fin}}(\widetilde{\mathbf{P}})\rangle_\ell = 0$, and recalling the properties of the Tate pairing mentioned above, this gives:

$$\langle v_{\mathrm{ord}}(x), v_{\mathrm{fin}}(\widetilde{\mathbf{P}})\rangle_\ell = 0.$$

Since $v_{\mathrm{fin}}(\widetilde{\mathbf{P}})$ is a unit (i.e. generates $\mathrm{H}^1_{\mathrm{fin}}(K_\ell, E[p^n])$) and the local Tate pairing is perfect, this implies that $v_{\mathrm{ord}}(x) = 0$, as was to be shown. This proves the claim (2.28), and with it the Proposition. □

2.7 End of the proof

We state Skinner and Urban result in our settings.

Theorem 2.7.1 (Skinner-Urban)**.** *Assume that Hypothesis* (**Lift**) *holds. Then the equality*

$$\mathrm{ord}_p\Big(L^{\mathrm{alg}}(g/K,1)\Big) = \mathrm{ord}_p\Big(\#\mathrm{Sel}_{\mathfrak{p}^\infty}(A_g/K)\Big) + t_g(\ell). \tag{2.30}$$

holds.

Proof. Note first that the weight-two newform $g \in S_2(\Gamma_0(N\ell),\mathbb{Z}_p)$ satisfies all the assumptions of Theorem 1.9.7 (cf. Theorem 1.9.5). Indeed, we have $\overline{\rho}_g \cong \overline{\rho}_f$: by assumption $\overline{\rho}_f$ (i.e. $E[p]$) is irreducible, $p \nmid N\ell$, and as explained in the proof of [BD, Lemma 2.2], $\overline{\rho}_f$ is ramified at every prime divisor of N (under the assumption that p does not divide the minimal degree of a modular parametrisation). Finally, by the very definition of the Tamagawa exponents, $t_q(g) = 0$ for every prime such that $\overline{\rho}_g \cong \overline{\rho}_f$ is ramified, so that $t_q(g) = 0$ for every prime divisor of N. (On the other hand, again by the definition, $t_\ell(g) \geq 1$.) The statement then follows by Theorem 1.9.7. □

With this result at our disposal, we can then conclude the proof of Theorem 2.2.1 and Theorem 2.2.2 exactly as explained in the last paragraph of Section 2.3. To be completely precise, let us state explicitly Ribet's 'lifting result' in the case $n = 1$, which was needed in our proof in Section 2.3.

Proposition 2.7.2. *Let $\overline{g} : \mathbf{T}_\ell \to \mathbb{F}_p$ be the mod-p modular form appearing in the statement of Theorem* 2.4.8*. Then $\overline{g}$ can be lifted to a weight-two newform $g \in S_2(\Gamma_0(N\ell),\mathbb{Z})$, i.e. such that $\overline{g}$ is the reduction modulo p of the morphism $g : \mathbb{T}_\ell \twoheadrightarrow \mathbf{T}_\ell \to \mathbb{Z}_p$ attached to g.*

Proof. Ribet proved in [Ri3] that $\overline{g}$ can be lifted to weight-two eigenform $g \in S_2(\Gamma_0(N\ell),\mathbb{Z}_p)$ which is new at ℓ. On the other hand, let q be a prime divisor of N. As we already observed, under our assumptions, the residual representation $\overline{\rho}_f$ is ramified at every prime $q|N$. Since $\overline{\rho}_f \cong \overline{\rho}_g$, this implies that q divides the conductor of g, i.e. that g is q-new. In other words: g is a weight-two newform in $S_2(\Gamma_0(N\ell),\mathbb{Z}_p)$, as claimed. □

2.7.1 Lifting modular forms to characteristic zero

In this final Section we discuss the possibility of lifting p^n-modular forms to characteristic zero, and describe the method used by Bertolini-Darmon in [BD] to prove 'lifting results' in their setting.

Let ℓ be an n-admissible prime, for some positive integer n. The main result of the Section 2.4 provides an explicit characterization of a mod p^n modular form $\bar{g} \in S_2(\mathcal{V}/\Gamma,\mathbb{Z}/p^n\mathbb{Z})$, see for details Theorem 2.4.8 and the subsequent Corollary. We expect that it is often possibile to obtain a lift of $\bar{g}$ to a p-isolated eigenform with coefficients in $\mathbb{Z}_p$. More precisely, we propose the following conjecture.

Conjecture 2.7.3. *Let n be a positive integer. Then there exist infinitely many n-admissible primes such that $\bar{g}$ lifts to a p-isolated modular form $g \in S_2(\mathcal{V}/\Gamma,\mathbb{Z}_p)$.*

More precisely, there is a maximal ideal $\mathfrak{p}$ of the ring $\mathcal{O}_g$ of Fourier coefficients of g such that:

1. the completion of $\mathcal{O}_g$ at $\mathfrak{p}$ is isomorphic to $\mathbb{Z}_p$;
2. g is determined by a form $g \in S_2(\mathcal{T}/\Gamma, \mathcal{O}_g)$ (denoted in the same way by an abuse of notation) via the inclusion $\mathcal{O}_g \subset (\mathcal{O}_g)_{\mathfrak{p}} = \mathbb{Z}_p$.

Remark 2.7.4. It is in general not possible to lift an arbitrary mod p^n form to a true modular form. If we assume $n = 1$ the previous result is well known by a works of Ribet [Ri2]. In this case we obtain an arithmetic relation, that is weaker than Theorem 2.1.3. We are giving the exact statement at the end of this Chapter. All the other statements are, instead, proved directly with n arbitrary, so the possibility of the lifting will be enough to conclude.

We summarize the previous remak in the following proposition.

Proposition 2.7.5. *Assume $n = 1$. Then the form $\bar{g} \in S_2(\mathcal{V}/\Gamma, \mathbb{Z}/p^n\mathbb{Z})$ can be lifted to a form $g \in S_2(\mathcal{V}/\Gamma)$.*

Remark 2.7.6. It is not in general true that the form g obtaine is p-isolated.

The above conjecture is the analogue of Proposition 3.12 of [BD]. Their setting is a little bit different here.

Let ℓ_1 and ℓ_2 be two n-admissible prime relative to f such that p^n divides $a_{\ell_1} + 1 - \epsilon_1$ and $a_{\ell_2}(f)\ \ell_2 + \epsilon_1 - a_{\ell_2}(f)$. Let B be the definite quaterion algebra of discriminant $-D\ell_1\ell_2$, R be an Eichler $\mathbb{Z}[1/p]$-order of level N in B, and set $\Gamma := R^\times/\mathbb{Z}[1/p]^\times$.

Theorem 2.7.7 (Bertolini-Darmon)**.** *With the notations as above, there exists an eigenform $g \in S_2(\mathcal{T}/\Gamma, \mathbb{Z}/p^n\mathbb{Z})$ such that the following equality modulo p^n holds*

i $T_q g \equiv a_q(f)g$ *for* $q \nmid N\ell_1\ell_2$;

ii $U_q g \equiv a_q(f)g$ *for* $q \mid N$;

iii $U_{\ell_1} \equiv \epsilon_1 g$;

iv $U_{\ell_2} \equiv \epsilon_2 g$.

Furthermore, fixed an n-admissible prime ℓ_1, there are infinitely many n-admissible primes ℓ_2 such that g can be lifted to an eigenform with coefficients in $\mathbb{Z}_p$ satysfing the above congruences. The form obtained in this way is p-isolated.

Outline of the proof. There are several steps in the proof.

Step 1: Theorem 9.3 of [BD] gives the existence of the p^n modular form g that corresponds to a surjective algebra homomorphism

$$f_{\ell_1\ell_2} : \mathbb{T}_{\ell_1\ell_2} \to \mathbb{Z}/p^n\mathbb{Z}$$

where $\mathbb{T}_{\ell_1\ell_2}$ is the Hecke algebra acting on a certain Shimura curves, defined by a factorization $N\ell_1\ell_2 = N^+\ell_1 \cdot N^-\ell_2$ in Theorem 9.3 loc. cit.

Step 2: By Proposition 3.6 of [BD] the property of being p-isolated can be translated as a condition of triviality the so-called S-Selmer group attached to the adjoint W_f of the Galois p-adic representation of f (here S is a squarefree product of n-admissible primes). The precise

definition of this Selmer group, that we denote by $\mathrm{Sel}_S(\mathbb{Q}, W_f)$ is given in Definition 3.5 of [BD].

Let $\mathfrak{R}$ denote the universal ring attached to deformations ρ of the Galois representation having the following properties:

- The determinant of ρ is the cyclotomic character describing the action of $\mathrm{G}_{\mathbb{Q}}$ on the p-powers roots of unity;
- ρ is ordinary at p;
- for q dividing NS the restriction of ρ to I_p is ordinary;
- ρ is unramified outside NS.

The ring $\mathfrak{R}$ is a complete local Noetherian $\mathbb{Z}_p$-algebra with residue field $\mathbb{F}_p$. Let $\mathfrak{m}$ denote the maximal ideal of $\mathfrak{R}$. Deformation theory provides an identification between

$$\mathfrak{m}/(p, \mathfrak{m}^2) = \mathrm{Sel}_S(\mathbb{Q}, W_f)^*,$$

where $\mathrm{Sel}_S(\mathbb{Q}, W_f)^*$ is the Pontrjagin dual of $\mathrm{Sel}_S(\mathbb{Q}, W_f)$. As a clear consequence $\mathfrak{R} = \mathbb{Z}_p$ if and only if $\mathrm{Sel}_S(\mathbb{Q}, W_f)$ is trivial. For $S = 1$ a well known result of Wiles , [Wi] Section 3 shows the existence of an isomorphism between $\mathfrak{R}$ and the ring $\mathbb{T}_f$ of Hecke operators acting on $S_2(\mathcal{T}/\Gamma)$ completed at the maximal ideal attached to f. Hence since $\mathfrak{R} = \mathbb{Z}_p = \mathbb{T}_f$ the form f is p-isolated.

Step 3: a pair of primes (ℓ_1, ℓ_2) is a rigid pair if $\mathrm{Sel}_{\ell_1,\ell_2}(\mathbb{Q}, W_f)$ is trivial. By Theorem 3.10 and Theorem 3.11 of [BD] for every ℓ_1 admissible prime, there exist infinitely many n-admissible primes ℓ_2 such that (ℓ_1, ℓ_2) is a rigid pair

Step 4: since (ℓ_1, ℓ_2) is a rigid pair then the algebra $\mathbb{T}_{\ell_1\ell_2}$ is isomorphic to $\mathbb{Z}_p$ therefore the morphism f_{ℓ_1,ℓ_2} lifts to characteristic zero, hence also g can be lifted to a true modular form in $S_2(\mathcal{T}/\Gamma)$. Finally, the fact that g is p-isolated follows from the observations in *Step 2*.

□

Remark 2.7.8. The goal of [BD] is to obtain a version of the so called Iwasawa Main Conjecture in the antyciclotomic settings. Their argument is inductive and consists in the explicit construction of an Euler system (to be more precise, a Kolyvagin system) controlling some Selmer groups in the anticyclotomic tower. For this fact, Bertolini and Darmon needed to produce a large supply of rigid pairs. For our interests we need just to show the existence of a single auxiliary n-admissible prime ℓ.

Remark 2.7.9. There is another possibility for concluding our argument, circumventing the need of a lift of the modular form. As pointed out by Pollack-Weston in [PW] one could work directly with mod p^n modular forms, their Selmer groups and their p-adic L-functions. All the arguments of [BD] go through in this more general settings, so we expect that also the results of Skinner-Urban admit a mod p^n-version.

Aknowledgements

I wish to express my deepest gratitude to my supervisor prof. Massimo Bertolini, without his invaluable insight, guidance, patience and support, this thesis would not have been possible. In May 2010 Prof. Bertolini gave me the draft [Be], containing the ideas on which this work is based. The author has been informed that recently Zhang has proved a generalization of the results of this thesis. We remark that this work is totally independent from Zhang's one.

I also would like to thank Rodolfo Venerucci for carefully reading this pages, for his suggestions, and for the fruitful discussions through these months.

I would also express my gratitude to my family. I think I cannot find all the proper words to tell them what their inspiring and loving education and support meant to me. My special "thanks" to them is full of love and gratitude for everything I owe them. Thanks also to my four-pawed family, though I am (quite) sure they cannot read these lines, I have the feeling that sometimes only one thing can help more than one dog's wagging tail and that is, two dogs' wagging tails.

Bibliography

[AU] Abbes and E. Ullmo, *A propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math. 103 (1996), no. 3, 269–286.

[ARS] A., Ribet K.A., Stein,W.A. *The Manin Constant*, JPAM Coates Volume (2006),

[ARS2] Agashe A., Ribet K.A., Stein,W.A. *The Modular Degree, Congruence Primes and Multiplicity one* preprint (2006),
available a t:http://www.math.fsu.edu/~agashe/math.html

[Be] M. Bertolini, Private note

[B] Bertolini M., *Report on the Birch and Swinnerton-Dyer Conjecture*, to appear on the proceedings of the symposium "Advances in Number Theory and Geometry", International School and Workshop on "150 years of Riemann Hypothesis" (director E. Bombieri), Milan Journal of Mathematics.

[BD] Bertolini M., Darmon H., *Iwasawa's Main Conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions*, Annals of Math. (2) 162 (2005), no. 1, 1-64.

[BD1] Bertolini M., Darmon H., *Euler systems and Jochnowitz congruences*, American Journal Math. 121, n. 2 (1999) 259-281

[BD2] Bertolini M. , Darmon H., *The p-adic L-functions of modular elliptic curves*, "Mathematics Unlimited – 2001 and Beyond", Springer Verlag (2001) 109-170.

[BD3] Bertolini M., Darmon H.*Heegner points on Mumford-Tate curves* Inventiones Math 126 (1996) 413-456.

[BD4] Bertolini M., Darmon H.*Heegner points, p-adic L-functions and the Cerednik-Drinfeld uniformization* Inventiones Math 131 (1998) 453-491.

[BCDT] Breuil, C., Conrad, B., Diamond, F., and Taylor, R., *On the modularity of elliptic curves over Q: wild 3-adic exercises.* J. Amer. Math. Soc. 14 (2001), no. 4, 843-939.

[Ca] Cassels, J. W. S. , *Arithmetic on curves of genus 1. III. The Tate–Shafarevich and Selmer groups*, Proceedings of the London Mathematical Society. (1962) Third Series 12: 259–296

[Da] Darmon, H. *Rational points on modular elliptic curves.* CBMS Regional Conference Series in Mathematics, 101. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004. xii+129 pp.

[DT] Diamond F., Taylor R., *Non-optimal levels for* mod l *modular representations of* $\mathrm{Gal}(\bar{Q}/Q)$, Invent. Math 115

[DDT] Darmon H., Diamond F. and Taylor R. *Fermat's Last Theorem* Current Developments in Mathematics 1, 1995, International Press, pp. 1-157.

[Ed] Edixhoven B., On the Manin constants of modular elliptic curves, Arithmetic algebraic geometry (Texel, 1989), Birkhauser Boston, Boston, MA, 1991, pp. 25–39

[Gr] Gross, B.H. *Kolyvagin's work on modular elliptic curves. L-functions and arithmetic* (Durham, 1989), 235–256, London Math. Soc. Lecture Note Ser., 153, Cambridge Univ. Press, Cambridge, 1991.

[GP] B. H. Gross and J. A. Parson, *On the local divisibility of Heegner points* in Number Theory, Analysis and Geometry – in memory of Serge Lang, D. Goldfeld, J. Jorgenson, P. Jones, D. Ramakrishnan, K. A. Ribet and J. Tate (eds.), Springer, New York, 2012, 215–241

[GZ] Gross, B. H.; Zagier, Don B. *Heegner points and derivatives of L-series.* Invent. Math. 84 (1986), no. 2, 225–320

[Ih] Ihara, Y. *Shimura curves over finite fields and their rational points* Contemporary Math. 245 (1999) 15-2

[Ih2] Ihara, Y. *On congruence monodromy problem.* Reproduction of the Lecture Notes: Volume 1 (1968) [MR0289518], Volume 2 (1969) [MR0289519] (University of Tokyo), with author's notes (2008). MSJ Memoirs, 18. Mathematical Society of Japan, Tokyo, 2008. xviii+230 pp

[Ih3] Ihara,Y. *On modular curves over finite fields* in Discrete subgroups of Lie type and applications to moduli in Baily, Walter L., Discrete subgroups of Lie groups and applications to moduli (Internat. Colloq., Bombay, 1973), Tata Institute of Fundamental Research Studies in Mathematics 7, Oxford University Press, pp. 161–202

[Ka] Kato, K, *p-adic Hodge theory and values of zeta functions of modular curves*, Asterisque 295 (2004), 117–290.

[Ko] Kolyvagin, V. A. *Euler systems* The Grothendieck Festschrift, Vol. II, 435–483, Progr. Math., 87, Birkhäuser Boston, Boston, MA, 1990.

[Ma1] Mazur, B. *Modular curves and the Eisenstein ideal.* Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33–186 (1978).

[Ma2] Mazur, B. *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162

[Me] Merel, L. *Bornes pour la torsion des courbes elliptique sur le corps de nombres.* Invent. Math. 124 (1996), no 1-3, 447-475

[MR] Mazur, B.; Ribet, K. A. *Two-dimensional representations in the arithmetic of modular curves.* (French summary) Courbes modulaires et courbes de Shimura (Orsay, 1987/1988). Astérisque No. 196-197 (1991), 6, 215–255 (1992).

[MC] Mac Callum W.G. *Kolyvagin's work on Shafarevich-tate groups* L-functions and arithmetic; Cambridge University Press, Cambridge 1991 pp 295-316

[MM] Murty M. R., MurtyV. K., *Mean values of derivatives of modular L-series*, Annals of Math. 133 (1991), 447–475

[OS] Ono, K. and Skinner, C., *Fourier coefficients of half-integral weight modular forms modulo* l, Annals of Math. (2), 147 (1998), no.2, 453–470.

[PW] Pollack R.; Weston T., *On the anicyclotomic* μ*-invariants of modular forms*, Compos. Math. 147 (2011) n. 5 , 1353-1381

[Ri] Ribet, K. A. *On modular representations of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms.* Invent. Math. 100 (1990), no. 2,

[Ri2] Ribet K. *Raising the levels of modular representations.* In Sèminaire de Theòrie des Nombres,Paris 1987?88, volume 81 of Progr. Math., pages 259?271. Birkhauser Boston, Boston, MA, 1990

[Ri3] Ribet, K. A. *Congruence relations between modular forms.* Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983), 503–514, PWN, Warsaw, 1984.

[Ri4] Ribet, K. A. *Bimodules and abelian surfaces.* Algebraic number theory, 359–407, Adv. Stud. Pure Math., 17, Academic Press, Boston, MA, 198

[Ri5] Ribet, K. *On the component groups and the Shimura subgroup of* $J(N)$Séminaire de Théorie des Nombres, 1987–1988 (Talence, 1987–1988), Exp. No. 6, 10 pp., Univ. Bordeaux I, Talence, 19

[Se] Serre J.P; *Local fields.* Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979. viii+241

[Se2] Serre J.P.; *Algebraic groups and Class Fields* Translated from the French. Graduate Texts in Mathematics, 117. Springer-Verlag, New York, 1988. x+207 pp.

[Si] Silverman, J. H. *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht.

[Sk] Skinner, C. *Multiplicative reduction and the cyclotomic main conjecture for GL2* arXiv:1407.1093

[SU] Skinner, C.; Urban, E. *The Iwasawa main conjectures for GL2.* Invent. Math. 195 (2014), no. 1, 1–277

[Va] Vatsal,V. *Special values of anticyclotimic L-functions.* Duke Math. J. 116 (2003) n.2 219-261.

[TW] Taylor, R.; Wiles, A. *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) 141 (1995), no. 3, 553-572.

[Wa] Waldspurger, J.-L. *Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie.* (French) Compositio Math. 54 (1985), no. 2,

[Wi] Wiles, A., *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) 141 (1995), no. 3, 443-551.

[Zh] Zhang,S.-W.; *Gross-Zagier formula for GL(2). II.* Heegner points and Rankin L-series, 191–214, Math. Sci. Res. Inst. Publ., 49, Cambridge Univ. Press, Cambridge, 2004. (Reviewer: Douglas L. Ulmer)

[Vi] Vignéras M.-F.;*Arithmétique des algèbres de quaternions.* Lecture Notes in Math., vol. 800 Springer, Berlin (1980)