Congruences between modular forms and the Birch and Swinnerton-Dyer conjecture

Andrea Berti, Massimo Bertolini, and Rodolfo Venerucci

Contents

Introduction

The theory of congruences between modular forms has turned out to be a crucial player in a number of momentous results in the theory of rational points on elliptic curves. To mention only a few instances, we recall here Mazur's theory of the Eisenstein ideal [**Maz78**], in which congruences between cusp forms and Eisenstein series on GL_2 are used to uniformly bound the torsion subgroups of elliptic curves over $\mathbf{Q}$. More germane to our setting, the recent work of Skinner–Urban [**SU14**] constructs classes in the p-primary Shafarevich–Tate group of an elliptic curve over $\mathbf{Q}$ (and more generally, over cyclotomic extensions) when p is ordinary and divides (the algebraic part of) the value of the associated Hasse–Weil L-series at $s=1$. This is achieved by exploiting p-power congruences between cusp forms on unitary groups and Eisenstein series whose constant term encodes the special value of the L-series of the elliptic curve. On the opposite side, when this special value is non-zero, Kato's Euler system [**Kat04**] arising from Steinberg symbols of modular units gives an upper bound on the p-primary Selmer group. The combination of these two results yields the validity of the p-part of the Birch and Swinnerton-Dyer conjecture for elliptic curves of analytic rank zero at almost all ordinary primes.

The goal of this paper is to present a direct proof of the p-part of the Birch and Swinnerton-Dyer conjecture for elliptic curves of analytic rank one for most ordinary primes, obtained by Wei Zhang in [**Zha14**] along a somewhat different path. More precisely, let $A/\mathbf{Q}$ be an elliptic curve of conductor N. Write $L(A/\mathbf{Q},s)$ for the Hasse–Weil L-function of A, and $Ш(A/\mathbf{Q})$ for its Shafarevich–Tate group. When $L(A/\mathbf{Q},s)$ has a simple zero at $s=1$, the theorem of Gross–Zagier–Kolyvagin [**GZ86**], [**Kol90**] states that $A(\mathbf{Q})$ has rank one and $Ш(A/\mathbf{Q})$ is finite. Fix a modular parametrisation

$$\pi_A : X_0(N) \longrightarrow A$$

of minimal degree $\deg(\pi_A)$. For every rational point $P \in A(\mathbf{Q})$, write $h^{\mathrm{NT}}(P) \in \mathbf{R}$ for the canonical Néron–Tate height of P, and let $\Omega_A \in \mathbf{R}^*$ be the real Néron period attached to $A/\mathbf{Q}$. Set $c_A := \prod_{q|N} c_q(A)$, where $c_q(A)$ is the Tamagawa number of $A/\mathbf{Q}_q$, and denote by $a_p(A)$ the coefficient $1+p-\bar{A}(\mathbf{F}_p)$ of A at p, and by $\mathrm{ord}_p : \mathbf{Q}^* \to \mathbf{Z}$ the p-adic valuation.

Theorem A. *Assume that $A/\mathbf{Q}$ is semistable. Let $p>7$ be a prime which does not divide $\deg(\pi_A)$, and is ordinary and non-anomalous for A (i.e., $a_p(A) \not\equiv 0,1 \pmod p$). If $L(A/\mathbf{Q},s)$ has a simple zero at $s=1$, then*

$$\mathrm{ord}_p\left(\frac{L'(A/\mathbf{Q},1)}{h^{\mathrm{NT}}(\mathbf{P})\cdot\Omega_A}\right) = \mathrm{ord}_p\Big(\#Ш(A/\mathbf{Q})\cdot c_A\Big),$$

where $\mathbf{P}$ is a generator of $A(\mathbf{Q})$ modulo torsion.

Note that the assumptions of Theorem A imply that the p-torsion of $A(\mathbf{Q})$ is trivial, and that the Tamagawa number c_A is a p-adic unit, so that it can be omitted in the statement.

By invoking the Kato–Skinner–Urban theorem mentioned above, Theorem A can be reduced (as explained in Section 5) to an analogous statement over an imaginary quadratic field K on which $L(A/K, s)$ has a simple zero. In light of the Gross–Zagier formula, this statement is in turn equivalent to the equality of the order of the p-primary part of the Shafarevich–Tate group of A/K and the p-part of the square of the index of a Heegner point in $A(K)$. Theorem 5.1 below proves this result by exploiting the theory of congruences between cusp forms on GL_2. In a nutshell, our strategy makes use of the explicit reciprocity laws of [**BD05**] combined with cohomological arguments and the theory of Euler systems to show that the existence of Selmer classes stated in Theorem 5.1 can be obtained from the constructive methods devised in [**SU14**] for elliptic curves of analytic rank zero.

Theorem 5.1 has been obtained independently by Wei Zhang [**Zha14**]. His method uses the reciprocity laws of loc. cit. together with [**SU14**] to prove Kolyvagin's conjecture on the non-vanishing of the cohomology classes defined in terms of Galois-theoretic derivatives of Heegner points over ring class fields. This conjecture is known to imply Theorem 5.1, thanks to prior work of Kolyvagin [**Kol91**]. The method explained in this paper (a weaker version of which appears in the first author's PhD thesis [**Ber14**]) is more direct, insofar as it consists in an explicit comparison of Selmer groups and of special values of L-series attached to congruent modular forms.

1. Modular forms and Selmer groups

Fix a squarefree positive integer N, a factorisation $N = N^+N^-$, and a rational prime $p > 3$ such that $p \nmid N$.

1.1. Eigenforms of level (N^+, N^-). Let $S_2(\Gamma_0(N))^{N^-\text{-new}}$ be the $\mathbf{C}$-vector space of weight-two cusp forms of level $\Gamma_0(N)$, which are new at every prime divisor of N^-. Write

$$\mathbb{T}_{N^+,N^-} \subset \mathrm{End}\left(S_2(\Gamma_0(N))^{N^-\text{-new}}\right)$$

for the Hecke algebra generated over $\mathbf{Z}$ by the Hecke operators T_q, for primes $q \nmid N$, and U_q for primes $q|N$.

Let R be a complete local Noetherian ring with finite residue field k_R of characteristic p. (In the following sections, R will often be chosen to be the finite ring $\mathbf{Z}/p^n\mathbf{Z}$.) An *R-valued (weight two) eigenform of level (N^+, N^-)* is a ring homomorphism

$$g : \mathbb{T}_{N^+,N^-} \longrightarrow R.$$

Denote by $S_2(N^+, N^-; R)$ the set of R-valued eigenforms of level (N^+, N^-). To every $g \in S_2(N^+, N^-; R)$ is associated – see for example [**Car94**], Section 2.2 – a Galois representation

$$\overline{\rho}_g : G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(k_R),$$

whose semi-simplification is characterised by the following properties. Let q be a prime which does not divide Np, and let $\mathrm{Frob}_q \in G_{\mathbf{Q}}$ be an arithmetic Frobenius at q. Then $\overline{\rho}_g$ is unramified at q, and the characteristic polynomial of $\overline{\rho}_g(\mathrm{Frob}_q)$ is $X^2 - \overline{g}(T_q)X + q \in k_R[X]$, where $\overline{g} : \mathbb{T}_{N^+,N^-} \to k_R$ is the composition of g with the projection $R \twoheadrightarrow k_R$. By Théorèm 3 of *loc. cit.*, if $\overline{\rho}_g$ is *(absolutely) irreducible*, one can lift it uniquely to a Galois representation

$$\rho_g : G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(R)$$

unramified at every prime $q \nmid Np$, and such that $\mathrm{trace}\big(\rho_g(\mathrm{Frob}_q)\big) = g(T_q)$ and $\det\big(\rho_g(\mathrm{Frob}_q)\big) = q$ for such a q. Assuming that $\overline{\rho}_g$ is irreducible, write

$$T_g \in {}_{R[G_{\mathbf{Q}}]}\mathrm{Mod}$$

for a R-module giving rise to the representation ρ_g. In other words, T_g is a free R-module of rank two, equipped with a continuous, linear action of $G_{\mathbf{Q}}$, which is unramified at every prime $q \nmid Np$, and such that Frob_q acts with characteristic polynomial $X^2 - g(T_q)X + q \in R[X]$ for every such q.

1.2. Selmer groups. Let $g \in S_2(N^+, N^-; R)$ be an eigenform satisfying the following assumption.

Assumption 1.1. 1. *$\overline{\rho}_g$ is absolutely irreducible.*

2. *ρ_g is* ordinary *at p, i.e., there exists a short exact sequence of $G_{\mathbf{Q}_p}$-modules*

$$0 \to T_g^{(p)} \to T_g \to T_g^{[p]} \to 0,$$

where $T_g^{(p)}$ (resp., $T_g^{[p]}$) is a free R-module of rank one, on which the inertia subgroup $I_{\mathbf{Q}_p} \subset G_{\mathbf{Q}_p}$ acts via the p-adic cyclotomic character $\varepsilon : G_{\mathbf{Q}_p} \twoheadrightarrow \mathrm{Gal}(\mathbf{Q}_p(\mu_{p^\infty})/\mathbf{Q}_p) \cong \mathbf{Z}_p^*$ (resp., acts via the trivial character).

3. *For every prime q dividing N, there exists a unique $G_{\mathbf{Q}_q}$-submodule $T_g^{(q)} \subset T_g$, free of rank one over R, such that $G_{\mathbf{Q}_{q^2}}$ acts on $T_g^{(q)}$ via the p-adic cyclotomic character $\varepsilon : G_{\mathbf{Q}_q} \twoheadrightarrow \mathrm{Gal}(\mathbf{Q}_q(\mu_{p^\infty})/\mathbf{Q}_q) \hookrightarrow \mathbf{Z}_p^*$. (Here $\mathbf{Q}_{q^2}/\mathbf{Q}_q$ denotes the quadratic unramified extension of $\mathbf{Q}_q$.)*

Let $K/\mathbf{Q}$ be an imaginary quadratic field of discriminant coprime with Np. For every (finite) prime v of K, define the *finite* and *singular* parts of the local cohomology group $H^1(K_v, T_g)$ as

$$H^1_{\mathrm{fin}}(K_v, T_g) := H^1(G_v/I_v, T_g^{I_v}); \quad H^1_{\mathrm{sing}}(K_v, T_g) := \frac{H^1(K_v, T_g)}{H^1_{\mathrm{fin}}(K_v, T_g)},$$

where I_v is the inertia subgroup of $G_v := \mathrm{Gal}(\overline{K}_v/K_v)$, and $H^1_{\mathrm{fin}}(K_v, T_g)$ is viewed as a submodule of $H^1(K_v, T_q)$ via the injective G_v/I_v-inflation map. For every prime v lying above a rational prime $q \mid Np$, define the *ordinary part* of the local cohomology $H^1(K_v, T_g)$ as

$$H^1_{\mathrm{ord}}(K_v, T_g) := \mathrm{Im}\left(H^1(K_v, T_g^{(q)}) \to H^1(K_v, T_g)\right).$$

Define the *Selmer group of* g/K as the submodule

$$\mathrm{Sel}(K, g) \subset H^1(K, T_g),$$

consisting of global cohomology classes $x \in H^1(K, T_g)$ satisfying the following conditions.

- x is *finite outside* Np: $\mathrm{res}_v(x) \in H^1_{\mathrm{fin}}(K_v, T_g)$ for every prime v of K not dividing Np.
- x is *ordinary* at every prime dividing Np: $\mathrm{res}_v(x) \in H^1_{\mathrm{ord}}(K_v, T_g)$ for every prime v of K dividing a rational prime $q|Np$.

Note that the Selmer group $\mathrm{Sel}(K, g)$ depends on g (since it depends on its level N), and not only on the representation T_g attached to it.

1.3. Admissible primes. In this section, R will denote the finite ring $\mathbf{Z}/p^n\mathbf{Z}$, where n is a positive integer and p is a rational prime. Let $g \in S_2(N^+, N^-; \mathbf{Z}/p^n\mathbf{Z})$ be a mod-p^n eigenform of level (N^+, N^-), and let $K/\mathbf{Q}$ be an imaginary quadratic field of discriminant coprime with Np.

Following [**BD05**], we say that a rational prime ℓ is an *n-admissible* prime relative to g if the following conditions are satisfied:

*A*1. ℓ does not divide Np.
*A*2. $\ell^2 - 1$ is a unit in $\mathbf{Z}/p^n\mathbf{Z}$ (i.e. $\ell \not\equiv \pm 1 \pmod{p}$).
*A*3. $g(T_\ell)^2 = (\ell+1)^2$ in $\mathbf{Z}/p^n\mathbf{Z}$.

If, in addition, ℓ is inert in K, we say that ℓ is n-admissible relative to (g, K).

For a rational prime ℓ, we say that an eigenform $g_\ell \in S_2(N^+, N^-\ell; \mathbf{Z}/p^n\mathbf{Z})$, i.e. a surjective morphism $g_\ell : \mathbb{T}_{N^+, N^-\ell} \to \mathbf{Z}/p^n\mathbf{Z}$, is an *$\ell$-level raising of g* if

$$g_\ell(T_q) = g(T_q), \qquad \text{resp. } g_\ell(U_q) = g(U_q)$$

for every prime $q \nmid N\ell$, resp. $q|N$. As recalled in loc. cit., if ℓ is n-admissible relative to g, then an ℓ-level raising g_ℓ exists.

Assume that g satisfies Assumption 1.1. Then $\overline{\rho}_g$ and $\overline{\rho}_{g_\ell}$ are isomorphic, absolutely irreducible representations of $G_{\mathbf{Q}}$ in $\mathrm{GL}_2(\mathbf{F}_p)$, and by the results recalled in Section 1.1, this implies that there is an isomorphism of $\mathbf{Z}/p^n\mathbf{Z}[G_{\mathbf{Q}}]$-modules

$$\mathscr{T} := T_g \cong T_{g_\ell} \in {}_{\mathbf{Z}/p^n\mathbf{Z}[G_{\mathbf{Q}}]}\mathrm{Mod}.$$

Fix such an isomorphism, that we regard as an equality from now on. The following lemma is proved by the same argument appearing in the proof of Lemma 2.6 of [**BD05**]. Write $K_\ell/\mathbf{Q}_\ell$ for the completion of K at the unique prime dividing ℓ (so $K_\ell = \mathbf{Q}_{\ell^2}$ is the quadratic unramified extension of $\mathbf{Q}_\ell$).

Lemma 1.2. *Let ℓ be an n-admissible prime relative to (g, K). Then there is a decomposition of $\mathbf{Z}/p^n\mathbf{Z}[G_{K_\ell}]$-modules*

$$\mathscr{T} = \mathbf{Z}/p^n\mathbf{Z}(\varepsilon) \oplus \mathbf{Z}/p^n\mathbf{Z},$$

where $\mathbf{Z}/p^n\mathbf{Z}(\varepsilon)$ (resp., $\mathbf{Z}/p^n\mathbf{Z}$) denotes a copy of $\mathbf{Z}/p^n\mathbf{Z}$ on which G_{K_ℓ} acts via the p-adic cyclotomic character ε (resp., acts trivially). Moreover, this decomposition induces isomorphisms

$$H^1_{\mathrm{fin}}(K_\ell, \mathscr{T}) \cong H^1(K_\ell, \mathbf{Z}/p^n\mathbf{Z}) \cong \mathbf{Z}/p^n\mathbf{Z}; \quad H^1_{\mathrm{sing}}(K_\ell, \mathscr{T}) \cong H^1(K_\ell, \mathbf{Z}/p^n\mathbf{Z}(\varepsilon)) \cong \mathbf{Z}/p^n\mathbf{Z}. \tag{1}$$

Let $g_\ell \in S_2(N^+, N^-\ell; \mathbf{Z}/p^n\mathbf{Z})$ be an ℓ-level raising of g. One deduces that $g_\ell \in S_2(N^+, N^-\ell; \mathbf{Z}/p^n\mathbf{Z})$ satisfies Assumption 1.1 too, and (with the notations above)

$$H^1_{\mathrm{ord}}(K_\ell, T_{g_\ell}) \cong H^1_{\mathrm{sing}}(K_\ell, T_g) \cong \mathbf{Z}/p^n\mathbf{Z}. \tag{2}$$

The preceding lemma allows us to define morphisms

$$v_\ell : H^1(K, \mathscr{T}) \longrightarrow H^1_{\mathrm{fin}}(K_\ell, \mathscr{T}) \cong \mathbf{Z}/p^n\mathbf{Z}; \quad \partial_\ell : H^1(K, \mathscr{T}) \longrightarrow H^1_{\mathrm{ord}}(K_\ell, \mathscr{T}) \cong \mathbf{Z}/p^n\mathbf{Z},$$

defined by composing the restriction map at ℓ with the projection onto the finite and ordinary (or singular) part respectively. Given a global class $x \in H^1(K, \mathscr{T})$, we call $v_\ell(x)$ its *finite part* at ℓ, and $\partial_\ell(x)$ its *residue* at ℓ.

1.4. Raising the level at admissible primes. As in the previous section, let $g \in S_2(N^+, N^-; \mathbf{Z}/p^n\mathbf{Z})$ be a mod-p^n eigenform of level (N^+, N^-).

ASSUMPTION 1.3. *The data $(\overline{\rho}_g, N^+, N^-, p)$ satisfy the following conditions:*
1. *$N = N^+N^-$ is squarefree;*
2. *p does not divide N;*
3. *$\overline{\rho}_g : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$ is surjective;*
4. *If $q \mid N^-$ and $q \equiv \pm 1 \pmod{p}$, then $\overline{\rho}_g$ is ramified at q.*

The following theorem, establishing the existence of a level raising at admissible primes, comes from the work of several people, including Ribet and Diamond–Taylor.

THEOREM 1.4. *Assume that Assumption 1.3 holds. Let $L = \ell_1 \cdots \ell_k$ be a product of (distinct) n-admissible primes ℓ_j relative to g. Then there exists a unique mod-p^n eigenform $g_L : \mathbb{T}_{N^+,N^-L} \longrightarrow \mathbf{Z}/p^n\mathbf{Z}$ of level (N^+, N^-L) such that*

$$g_L(T_q) = g(T_q) \quad (\textit{for all } q \nmid NL), \qquad g_L(U_q) = g(U_q) \quad (\textit{for all } q \mid N).$$

PROOF. We make some remarks about the references for the proof of this theorem. Assume that $N^- > 1$ and that N^- has an odd (resp., even) number of prime divisors. In this case the theorem is proved in Section 5 (resp., 9) of [**BD05**], working under slightly more restrictive assumptions on $(\overline{\rho}_g, N^+, N^-, p)$, subsequently removed in Section 4 of [**PW11**]. The method of [**BD05**] generalises previous work of Ribet (which considered the case $n = 1$), and uses Diamond–Taylor's generalisation of Ihara's Lemma (for modular curves) to Shimura curves. We refer to loc. cit. for more details and references.

Assume now that $N^- = 1$. If $n = 1$, the theorem has been proved by Ribet. If $n > 1$, the theorem can be proved by following the arguments appearing in Section 9 of [**BD05**] (see in particular Proposition 9.2 and Theorem 9.3), and invoking the classical Ihara Lemma (instead of Diamond–Taylor's generalisation) in the proof of Proposition 9.2. □

2. The explicit reciprocity laws

In this section we recall (special cases of) the explicit reciprocity laws proved in [**BD05**], which relate Heegner points on Shimura curves to special values of Rankin L-functions (described in terms of certain *Gross points* attached to modular forms on definite quaternion algebras). Together with the proof by Kato–Skinner–Urban of the (p-part of) the Birch and Swinnerton-Dyer formula in analytic rank zero (cf. Section 4 below), these reciprocity laws will be at the heart of our proof of Theorem A.

Fix throughout this section a factorisation $N = N^+N^-$ of a positive integer N, a rational prime p not dividing N, and a $\mathbf{Z}_p$-valued eigenform

$$f \in S_2(N^+, N^-; \mathbf{Z}_p)$$

of level (N^+, N^-). Fix also a quadratic imaginary field $K/\mathbf{Q}$ of discriminant coprime with Np. Assume that the following hypotheses are satisfied (cf. Hypothesis CR of [**PW11**]).

ASSUMPTION 2.1. 1. *N^- has an* even *number of prime factors.*
2. *A prime divisor q of N divides N^- precisely if q is inert in $K/\mathbf{Q}$.*
3. *$\overline{\rho}_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$ is surjective.*
4. *f is ordinary at p, i.e. $f(T_p) \in \mathbf{Z}_p^*$.*
5. *If $q \mid N^-$ and $q \equiv \pm 1 \pmod{p}$, then $\overline{\rho}_f$ is ramified at q.*

2.1. Special points on Shimura curves.

2.1.1. *Shimura curves (*[**BD05**, Section 5]*).* Let $\mathscr{B} := \mathscr{B}_{N^-}$ be a quaternion algebra of discriminant N^-, let $\mathscr{R} = \mathscr{R}_{N^+}$ be an Eichler order of level N^+ in $\mathscr{B}$, and let $\mathscr{R}_{\max}$ be a maximal order of $\mathscr{B}$ containing $\mathscr{R}$. (The indefinite quaternion algebra $\mathscr{B}$ is unique up to isomorphism, while $\mathscr{R}_{\max}$ and $\mathscr{R}$ are unique up to conjugation.) Let

$$\mathcal{F}_{N^+,N^-} : \mathrm{Sch}_{/\mathbf{Z}[1/N]} \longrightarrow \mathrm{Sets}$$

be the functor attaching to a $\mathbf{Z}[1/N]$-scheme T the set of isomorphism classes of triples (A, ι, C), where

- A is an abelian scheme over T of relative dimension 2;
- ι is a morphism $\mathscr{R}_{\max} \to \mathrm{End}(A/T)$, defining an action of $\mathscr{R}_{\max}$ on A;
- C is a subgroup scheme of A, locally isomorphic to $\mathbf{Z}/N^+\mathbf{Z}$, which is stable and locally cyclic over $\mathscr{R}$.

If $N^- > 1$, the moduli problem $\mathcal{F}_{N^+,N^-}$ is coarsely represented by a smooth projective scheme

$$X_{N^+,N^-} \to \mathrm{Spec}(\mathbf{Z}[1/N]),$$

called the *Shimura curve* attached to the factorisation $N = N^+N^-$. In particular

$$X_{N^+,N^-}(F) = \mathcal{F}_{N^+,N^-}(F)$$

for every algebraically closed field F of characteristic coprime with N.

If $N^- = 1$, then the functor $\mathcal{F}_{N,1}$ can be shown to be coarsely represented by the smooth, quasi-projective modular curve $X^o_{N,1} = Y_0(N)$ over $\mathbf{Z}[1/N]$ of level $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbf{Z})$. In this case we write

$$X_{N,1} = X_0(N) \to \mathrm{Spec}(\mathbf{Z}[1/N])$$

for the usual compactification obtained by adding to $X^o_{N,1}$ a finite set of cusps, which is again a smooth projective curve over $\mathbf{Z}[1/N]$.

2.1.2. *Heegner points.* Under Assumption 2.1(2) $X_{N^+,N^-}(\mathbf{C})$ contains points with CM by K. More precisely, let $\mathcal{O}_K$ be the maximal order of K. Then there exists a point $\mathbb{P} = (\mathcal{A}, \iota, \mathcal{C}) \in X_{N^+,N^-}(\mathbf{C})$ such that

$$\mathcal{O}_K \cong \mathrm{End}(\mathbb{P}), \tag{3}$$

where $\mathrm{End}(\mathbb{P}) \subset \mathrm{End}(\mathcal{A})$ denotes the ring of endomorphisms of $\mathcal{A}/\mathbf{C}$ which commute with the action of ι, and respect the level structure $\mathcal{C}$. By the theory of complex multiplication,

$$\mathbb{P} \in X_{N^+,N^-}(H),$$

where $H := H_K$ is the Hilbert class field of K. Call such a $\mathbb{P} \in X_{N^+,N^-}(H)$ a *Heegner point*, and write

$$\mathrm{Heeg}_{N^+,N^-}(K) \subset X_{N^+,N^-}(H)$$

for the set of Heegner points (of conductor one).

2.1.3. *Gross points.* Let $L = \ell_1 \cdots \ell_k$ be a squarefree product of an *odd* number of primes $\ell_j \nmid N$ which are *inert* in $K/\mathbf{Q}$. Let $B := B_{N^-L}$ be a definite quaternion algebra of discriminant N^-L (which is unique up to isomorphism), and let $R := R_{N^+}$ be a fixed Eichler order of level N^+ in B. The Eichler order R is not necessarily unique, even up to conjugation. Nonetheless, there are only finitely many conjugacy classes of Eichler orders of level N^+ in B, say $R_1, \ldots, R_h$. More precisely, consider the double coset space

$$\mathbb{X}_{N^+,N^-L} := \widehat{R}^* \backslash \widehat{B}^* / B^*, \tag{4}$$

where $\widehat{Z} := Z \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$ for every ring Z, with $\widehat{\mathbf{Z}} = \prod_{q \text{ prime}} \mathbf{Z}_q$. It is a finite set, in bijection with the set of conjugacy classes of *oriented* Eichler orders of level N^+ in B, via the rule $\widehat{B}^* \ni b \mapsto R_b := b\widehat{R}b^{-1} \cap B$ (cf. [**BD96**, Sec. 1]).

Define the set of *Gross points* of level N^+ and conductor p^∞ on B as

$$\mathrm{Gr}_{N^+,N^-L}(K, \infty) := \widehat{R}^* \backslash \big(\mathrm{Hom}(K, B) \times \widehat{B}^*\big) / B^*.$$

Here $\mathrm{Hom}(K, B)$ is the set of morphisms of algebras $f : K \to B$. (The group B^* acts on $\widehat{B}^*$ via the diagonal embedding $B^* \to \widehat{B}^*$, while it acts on $\mathrm{Hom}(K, B)$ via conjugation on B.) A Gross point $[f \times b] \in \mathrm{Gr}_{N^+,N^-L}(K, \infty)$ has *conductor one* if $f(K) \cap b\widehat{R}b^{-1} = f(\mathcal{O}_K)$. Denote by

$$\mathrm{Gr}_{N^+,N^-L}(K) \subset \mathrm{Gr}_{M^+,M^-L}(K, \infty)$$

the set of Gross points of conductor one. In what follows, a *Gross point (of level N^+ on B)* will always be a Gross point (of level N^+ on B) of conductor one.

2.1.4. *Gross points and reduction of Heegner points.* With the notations of the previous section, let $L = \ell$ be a rational prime which is inert in $K/\mathbf{Q}$ and such that $\ell \nmid N$. The reduction modulo ℓ map on the Shimura curve X_{N^+,N^-} allows us to define a map

$$r_\ell : \mathrm{Heeg}_{N^+,N^-}(K) \longrightarrow \mathrm{Gr}_{N^+,N^-\ell}(K)$$

from Heegner points to Gross points. More precisely, let $\mathbb{P} = (\mathcal{A}, \iota, \mathcal{C}) \in \mathrm{Heeg}_{N^+,N^-}(H)$. Fix a prime λ of H dividing ℓ. Since ℓ is inert in K, it is totally split in H, so that λ has associated residue field $\mathbf{F}_{\ell^2}$. The abelian variety $\mathcal{A}$ and the subgroup $\mathcal{C} \subset \mathcal{A}$ are defined over H, and $\mathcal{A}$ has good reduction at λ. Let

$$\overline{\mathbb{P}} := \mathrm{red}_\ell(\mathbb{P}) = (\overline{\mathcal{A}}, \bar{\iota}, \overline{C}) \in X_{N^+,N^-}(\mathbf{F}_{\ell^2})$$

be the reduction of $\mathbb{P}$ modulo λ, where $\overline{\mathcal{A}}/\mathbf{F}_{\ell^2}$ and $\overline{\mathcal{C}} \subset \overline{\mathcal{A}}$ denote the reductions of $\mathcal{A}$ and $\mathcal{C}$ modulo λ respectively, and $\bar{\iota}$ denotes the composition of ι with reduction of endomorphisms $\mathrm{End}(\mathcal{A}) \to \mathrm{End}(\overline{\mathcal{A}})$. Define (as above) $\mathrm{End}(\overline{\mathbb{P}}) \subset \mathrm{End}(\overline{\mathcal{A}})$ as the subring of endomorphisms of $\overline{\mathcal{A}}$ (defined over $\overline{\mathbf{F}}_\ell$) commuting with the action of ι and preserving $\overline{\mathcal{C}}$. It turns out that $\mathrm{End}(\overline{\mathbb{P}}) \cong R_{\mathbb{P}}$ is isomorphic to an Eichler order $R_{\mathbb{P}}$ of level N^+ in $B = B_{N^-\ell}$. In light of (3), reduction of endomorphisms on $\mathcal{A}$ induces then an embedding

$$f_{\mathbb{P},\ell} : \mathcal{O}_K \cong \mathrm{End}(\mathbb{P}) \longrightarrow \mathrm{End}(\overline{\mathbb{P}}) \cong R_{\mathbb{P}}.$$

Denote again by $f_{\mathbb{P},\ell} : K \to B$ the extension of scalars of $f_{\mathbb{P},\ell}$. By (4) there exists $b_{\mathbb{P}} \in \widehat{B}^*$ such that $R_{\mathbb{P}} = b_{\mathbb{P}}\widehat{R}b_{\mathbb{P}}^{-1} \cap B$. Define

$$r_\ell(\mathbb{P}) = \big[f_{\mathbb{P},\ell} \times b_{\mathbb{P}}\big] \in \mathrm{Gr}_{N^+,N^-\ell}(K).$$

2.1.5. *Action of* $\mathrm{Pic}(\mathcal{O}_K)$. The assumptions an notations are as in the preceding sections. Write $\mathrm{Pic}(\mathcal{O}_K)$ for the ideal class group of K, which admits the adelic description $\mathrm{Pic}(\mathcal{O}_K) = \widehat{\mathcal{O}}_K^*\backslash\widehat{K}^*/K^*$. Given an ideal class $\sigma \in \mathrm{Pic}(\mathcal{O}_K)$ and a Gross point $P = [f \times b] \in \mathrm{Gr}_{N^+,N^-\ell}(K)$, define

$$P^\sigma := \big[f \times \widehat{f}(\sigma) \cdot b\big] \in \mathrm{Gr}_{N^+,N^-\ell}(K),$$

where $\widehat{f} : \widehat{K} \to \widehat{B}$ is the morphism induced on adèles by the embedding $f : K \to B$. It is easily seen that the rule $P \mapsto P^\sigma$ defines an action of $\mathrm{Pic}(\mathcal{O}_K)$ on $\mathrm{Gr}_{N^+,N^-\ell}(K)$.

The Artin map of global class field theory gives a canonical isomorphism $\mathrm{Pic}(\mathcal{O}_K) \cong \mathrm{Gal}(H/K)$. The set of Heegner points $\mathrm{Heeg}_{N^+,N^-}(K)$ (of conductor one) is contained in $X_{N^+,N^-}(H)$, and one obtains a natural *geometric* action of $\mathrm{Pic}(\mathcal{O}_K)$ on $\mathrm{Heeg}_{N^+,N^-}(K)$.

With these definitions, the reduction map $r_\ell : \mathrm{Heeg}_{N^+,N^-}(K) \to \mathrm{Gr}_{N^+,N^-\ell}(K)$ defined in the preceding section is $\mathrm{Pic}(\mathcal{O}_K)$-equivariant [**BD96**], i.e.

$$r_\ell\big(\mathbb{P}^\sigma\big) = r_\ell(\mathbb{P})^\sigma \tag{5}$$

for every ideal class $\sigma \in \mathrm{Pic}(\mathcal{O}_K)$ and every Heegner point $\mathbb{P} \in \mathrm{Heeg}_{N^+,N^-}(K)$.

2.2. Modular forms on definite quaternion algebras. The notations and assumptions are as in Section 2.1.3. Let

$$\mathbb{J}_{N^+,N^-L} := \mathbf{Z}\big[\mathbb{X}_{N^+,N^-L}\big]$$

denote the group of formal divisors on the set $\mathbb{X}_{N^+,N^-L}$ defined in equation (4). As explained in Section 1.5 of [**BD96**], there is a Hecke algebra

$$\mathbf{T}_{N^+,N^-L} \subset \mathrm{End}(\mathbb{J}_{N^+,N^-L})$$

acting faithfully as a ring of endomorphisms of $\mathbb{J}_{N^+,N^-L}$, and generated over $\mathbf{Z}$ by Hecke operators t_q, for primes $q \nmid N$, and u_q, for primes $q|N$. By the Jacquet–Langlands correspondence [**BD96**, Section 1.6], there is an isomorphism $\mathbf{T}_{N^+,N^-L} \cong \mathbb{T}_{N^+,N^-L}$, defined by sending t_q (resp., u_q) to T_q (resp., U_q).

Let $n \in \mathbf{N} \cup \{\infty\}$, and let $g \in S_2(N^+, N^-L; \mathbf{Z}_p/p^n\mathbf{Z}_p)$ be a $\mathbf{Z}_p/p^n\mathbf{Z}_p$-valued eigenform of level (N^+, N^-L) (with the convention that $\mathbf{Z}_p/p^\infty\mathbf{Z}_p := \mathbf{Z}_p$). Then g induces a surjective morphism $g^{\mathrm{JL}} : \mathbf{T}_{N^+,N^-L} \twoheadrightarrow \mathbf{Z}_p/p^n\mathbf{Z}_p$. Let $\mathfrak{m}_g := \ker(g_{\{1\}})$ denote the maximal ideal of $\mathbf{T}_{N^+,N^-L}$ associated with (the reduction $g_{\{1\}}$ modulo p of) g, and let $\mathbb{J}_{\mathfrak{m}_g}$ and $\mathbf{T}_{\mathfrak{m}_g}$ denote the completions at $\mathfrak{m}_g$ of $\mathbb{J}_{N^+,N^-L}$ and $\mathbf{T}_{N^+,N^-L}$ respectively. According to Theorem 6.2 and Proposition 6.5 of [**PW11**], Assumption 2.1 implies that $\mathbb{J}_{\mathfrak{m}_g}$ is a free $\mathbf{T}_{\mathfrak{m}_g}$-module of rank one. As a consequence, g^{JL} induces a surjective morphism (denoted by the same symbol with a slight abuse of notation)

$$g^{\mathrm{JL}} : \mathbb{J}_{N^+,N^-L} \longrightarrow \mathbf{Z}_p/p^n\mathbf{Z}_p,$$

such that $g^{\mathrm{JL}}(h \cdot x) = g(h) \cdot g^{\mathrm{JL}}(x)$ for every $x \in \mathbb{J}_{N^+,N^-L}$ and every $h \in \mathbf{T}_{N^+,N^-L}$. Such a $\mathbf{T}_{N^+,N^-L}$-eigenform is unique up to p-adic units.

Remark 2.2. The above discussion establishes a correspondence between eigenforms in the sense of Section 1.1 and surjective $\mathbf{Z}_p/p^n\mathbf{Z}_p$-valued eigenforms on definite quaternion algebras. The latter is the point of view adopted in [**BD05**]; we refer the reader to Section 1.1 of *loc. cit.*, and in particular to equation (11) in the proof of Proposition 1.3, for more details.

2.2.1. *Special values attached to modular forms on definite quaternion algebras.* There is a natural forgetful map

$$\mathrm{Gr}_{N^+,N^-L}(K) \longrightarrow \mathbb{X}_{N^+,N^-L},$$

which maps the Gross point represented by the pair $f \times b \in \mathrm{Hom}(K,B) \times \widehat{B}^*$ to the class of the idèle b in $\mathbb{X}_{N^+,N^-L}$. Any function γ defined on $\mathbb{X}_{N^+,N^-L}$ then induces a function on the set of Gross points $\mathrm{Gr}_{N^+,N^-L}(K)$, denoted again γ. Let $g : \mathbb{T}_{N^+,N^-L} \to \mathbf{Z}_p/p^n\mathbf{Z}_p$ be as above. Thanks to the Jacquet–Langlands correspondence recalled in the preceding section, one can define the *special value attached to* (g, K) by

$$\mathscr{L}_p(g/K) := \sum_{\sigma \in \mathrm{Pic}(\mathcal{O}_K)} g^{\mathrm{JL}}\big(x^\sigma\big) \in \mathbf{Z}_p/p^n\mathbf{Z}_p, \tag{6}$$

where $x \in \mathrm{Gr}_{N^+,N^-L}(K)$ is any fixed Gross point of level N^+ on B. The special value $\mathscr{L}_p(g/K)$ is well defined up to multiplication by a p-adic unit. (Once g^{JL} is fixed, $\mathscr{L}_p(g/K)$ can be shown to be independent, up to sign, of the choice of the Gross point x fixed to define it. We refer to Section 3 of [**BD96**] for more details.)

When $n = \infty$, so that g arises from a classical modular form, $\mathscr{L}_p(g/K)$ is essentially equal to the square-root of the special value $L(g/K, 1)$, as explained in Section 3 below.

2.3. The reciprocity laws. Fix throughout this section a positive integer n, and denote by

$$f_{\{n\}} \in S_2(N^+, N^-; \mathbf{Z}/p^n\mathbf{Z})$$

the reduction of f modulo p^n (i.e. the composition of $f : \mathbb{T}_{N^+,N^-} \to \mathbf{Z}_p$ with the natural projection $\mathbf{Z}_p \twoheadrightarrow \mathbf{Z}/p^n\mathbf{Z}$). An n-admissible prime relative to $(f_{\{n\}}, K)$ is also said to be *n-admissible relative to* (f, K).

2.3.1. *The graph of modular forms.* Let $\mathcal{L} = \mathcal{L}_n$ denote the set of squarefree products $L = \ell_1 \cdots \ell_r$ of n-admissible primes ℓ_j relative to (f, K). One can decompose $\mathcal{L} = \mathcal{L}^{\mathrm{def}} \coprod \mathcal{L}^{\mathrm{indef}}$, where $L \in \mathcal{L}^{\mathrm{def}}$ is a *definite vertex* (resp., $L \in \mathcal{L}^{\mathrm{indef}}$ is an *indefinite vertex*) if the number r of primes dividing L is *odd* (resp., *even*).

According to Theorem 1.4 (and recalling Assumption 2.1), to every $L \in \mathcal{L}$ is associated a unique mod-p^n eigenform

$$f_L \in S_2(N^+, N^-L; \mathbf{Z}/p^n\mathbf{Z})$$

of level (N^+, N^-L), such that $f_L(T_q) = f_{\{n\}}(T_q)$ for every prime $q \nmid NL$ and $f_L(U_q) = f_{\{n\}}(U_q)$ for every prime $q|N$.

2.3.2. *Construction of cohomology classes.* Let $L \in \mathcal{L}^{\mathrm{indef}}$ be an indefinite vertex. Let $X_L := X_{N^+,N^-L}/\mathbf{Q}$ be the Shimura curve of level (N^+, N^-L), let $J_L/\mathbf{Q}$ be the Jacobian variety of X_L, and let $\mathrm{Ta}_p(J_L)$ be its p-adic Tate module. As explained e.g. in [**BD96**], the Hecke algebra $\mathbb{T}_{N^+,N^-L}$ acts faithfully as a ring of $\mathbf{Q}$-rational endomorphisms of J_L. Theorem 5.17 of [**BD05**], as generalised in Proposition 4.4 of [**PW11**], states that there is an isomorphism of $\mathbf{Z}/p^n\mathbf{Z}[G_{\mathbf{Q}}]$-modules

$$\pi_L : \mathrm{Ta}_p(J_L)/I_L \cong T_{f_L} \cong T_{f,n}, \tag{7}$$

where $I_L \subset \mathbb{T}_{N^+,N^-L}$ is the kernel of $f_L \in S_2(N^+, N^-L; \mathbf{Z}/p^n\mathbf{Z})$, $T_{f_L} \in {}_{\mathbf{Z}/p^n\mathbf{Z}[G_{\mathbf{Q}}]}\mathrm{Mod}$ is the Galois representation attached in Section 1.1 to the eigenform f_L, and $T_{f,n} := T_f \otimes_{\mathbf{Z}} \mathbf{Z}/p^n\mathbf{Z}$ (so that $T_{f,n} \cong T_{f_{\{n\}}}$). Let Pic_L denote the Picard variety of X_L. Since I_L is not an Eisenstein ideal, the natural map $J_L(K) \hookrightarrow \mathrm{Pic}_L(K)$ induces an isomorphism $J_L(K)/I_L \cong \mathrm{Pic}_L(K)/I_L$. One can then define the morphism

$$\mathtt{k}_L : \mathrm{Pic}_L(K)/I_L \cong J_L(K)/I_L \xrightarrow{\delta} H^1(K, \mathrm{Ta}_p(J_L)/I_L) \overset{\pi_L}{\cong} H^1(K, T_{f,n}),$$

where δ denotes the map induced by the global Kummer map $J_L(K)\widehat{\otimes}\mathbf{Z}_p \hookrightarrow H^1(K, \mathrm{Ta}_p(J_L))$ after taking the quotients by I_L. Fix now a Heegner point $\mathbb{P}(L) \in \mathrm{Heeg}_{N^+,N^-L}(K) \subset X_L(H)$, let

$$\mathbf{P}(L) := \sum_{\sigma \in \mathrm{Gal}(H/K)} \mathbb{P}(L)^\sigma \in \mathrm{Pic}_L(K),$$

and define the global cohomology class

$$\kappa(L) := \mathtt{k}_L\big(\mathbf{P}(L)\big) \in H^1(K, T_{f,n}).$$

The class $\kappa(L)$ is uniquely determined, up to sign, by the choice of the isomorphism π_L in (7) [**BD05**]. It is then naturally associated with the pair (f, L) up to multiplication by a p-adic unit.

2.3.3. *The special values.* The constructions of Sections 2.2.1 and 2.3.1 attach to a definite vertex $L \in \mathcal{L}^{\mathrm{def}}$ the quaternionic special value

$$\mathscr{L}_p(L) := \mathscr{L}_p(f_L/K) \in \mathbf{Z}/p^n\mathbf{Z}.$$

This is canonically attached to the pair (f, L) up to multiplication by a p-adic unit.

2.3.4. *The first reciprocity law.* Let $L \in \mathcal{L}^{\mathrm{def}}$, and let $\ell \in \mathcal{L}^{\mathrm{def}}$ be a n-admissible prime relative to (f, K) such that $\ell \nmid L$. Recall the residue map $\partial_\ell : H^1(K, T_{f,n}) \to H^1_{\mathrm{ord}}(K_\ell, T_{f,n}) \cong \mathbf{Z}/p^n\mathbf{Z}$ introduced in Section 1.3. The following theorem is a special case of [**BD05**, Theorem 4.1].

THEOREM 2.3. *The equality*

$$\partial_\ell\big(\kappa(L\ell)\big) = \mathscr{L}_p(L)$$

holds in $\mathbf{Z}/p^n\mathbf{Z}$*, up to multiplication by a p-adic unit.*

2.3.5. *The second reciprocity law.* Let $L \in \mathcal{L}^{\mathrm{indef}}$ be an indefinite vertex, and let $\ell \in \mathcal{L}^{\mathrm{def}}$ be a n-admissible prime which does not divide L. Recall the morphism $v_\ell : H^1(K, T_{f,n}) \to H^1_{\mathrm{fin}}(K_\ell, T_{f,n}) \cong \mathbf{Z}/p^n\mathbf{Z}$. The following theorem is a special case of [**BD05**, Theorem 4.2].

THEOREM 2.4. *The equality*

$$v_\ell\big(\kappa(L)\big) = \mathscr{L}_p(L\ell)$$

holds in $\mathbf{Z}/p^n\mathbf{Z}$*, up to multiplication by a p-adic unit.*

PROOF. This is proved in Section 9 of [**BD05**] when $N^- \neq 1$ (i.e. X_{N^+,N^-} is not the classical modular curve of level $\Gamma_0(N)$), using Diamond–Taylor's generalisation of Ihara's Lemma to Shimura curves. On the other hand, making use of the classical Ihara's Lemma, the argument of loc. cit. also applies to the case $N^- = 1$. To handle the case $N^- = 1$, one may alternately go through the argument of Vatsal in [**Vat03**, Section 6], where the case $N^- = 1$ and $n = 1$ of Theorem 2.4 is proved, and note that the proof applies also to the case $n > 1$. □

3. Gross' special value formula

In this section only, let $N = N^+N^-$ be a squarefree integer coprime with p, such that N^- is a product of an *odd* number of primes. Let $K/\mathbf{Q}$ be a quadratic imaginary field of discriminant coprime with Np. Let $g \in S_2(N^+, N^-; \mathbf{Z}_p)$ be a $\mathbf{Z}_p$-valued eigenform of level (N^+, N^-). We impose in this section the following hypotheses (cf. Assumption 2.1):

ASSUMPTION 3.1. *The data $(\overline{\rho}_g, K, N^+, N^-)$ satisfy the following conditions:*
1. *N^- has an* odd *number of prime factors.*
2. *A prime divisor q of N divides N^- precisely if q is inert in $K/\mathbf{Q}$.*
3. *$\overline{\rho}_g : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$ is surjective.*
4. *If $q \mid N^-$ and $q \equiv \pm 1 \pmod{p}$, then $\overline{\rho}_g$ is ramified at q.*

Section 2.2.1 (see equation (6) and the discussion following it) attached to g and K a special value

$$\mathscr{L}_p(g/K) \in \mathbf{Z}_p,$$

well defined up to multiplication by a p-adic unit. Gross' formula compares this *quaternionic special value* to the *algebraic part* of the *complex special value* of g/K, defined as

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

Here $L(g/K, s) := L(g, s) \cdot L(g, \epsilon_K, s)$ is the product of the Hecke complex L-series of g with that of the twist $g \otimes \epsilon_K$ of g by the quadratic character $\epsilon_K : (\mathbf{Z}/D\mathbf{Z})^* \to \{\pm 1\}$ of K. Moreover $\Omega_g \in \mathbf{C}^*$ is the *canonical Shimura period* of g. In order to define it, we briefly recall the definition of congruence numbers, referring to [**PW11**] for more details. Given a positive integer M and a factorisation $M = M^+ \cdot M^-$, write $\widehat{\mathbb{T}}_{M^+,M^-}$ for the p-adic completion of $\mathbb{T}_{M^+,M^-}$. For every eigenform $\phi \in S_2(M^+, M^-; \mathbf{Z}_p)$, define the *congruence ideal*

$$\eta_\phi(M^+, M^-) := \hat{\phi}\Big(\mathrm{Ann}_{\widehat{\mathbb{T}}_{M^+,M^-}}\big(\ker(\hat{\phi})\big)\Big) \subset \mathbf{Z}_p,$$

where $\hat{\phi} : \widehat{\mathbb{T}}_{M^+,M^-} \to \mathbf{Z}_p$ is the morphism induced by ϕ. One identifies $\eta_\phi(M^+, M^-)$ with the non-negative power of p that generates it, in other words we regard it as a positive integer. Then $\eta_\phi(M^+, M^-) = 1$ precisely if there is no non-trivial congruence modulo p between ϕ and eigenforms of level (L, M^-), for some divisor $L|M^+$. The canonical Shimura period mentioned above is defined as

$$\Omega_g := \frac{(g, g)}{\eta_g(N, 1)},$$

where (g, g) is the Petersson norm of $g \in S_2(\Gamma_0(N))$, and where we write again g to denote the composition of $g : \mathbb{T}_{N^+,N^-} \to \mathbf{Z}_p$ with the natural projection $\mathbb{T}_{N,1} \to \mathbb{T}_{N^+,N^-}$ in order to define $\eta_g(N, 1)$.

Before stating Gross' formula, we also need to introduce the Tamagawa exponents attached to g at primes dividing N. Let ϕ denote either g or its quadratic twist $g \otimes \epsilon_K$. Write as usual $T_\phi \in {}_{\mathbf{Z}_p[G_{\mathbf{Q}}]}\mathrm{Mod}$ for the p-adic representation attached to ϕ, and $A_\phi := T_\phi \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p$. Given a prime $q \mid N$, the *Tamagawa factor* $c_q(\phi)$ is defined to be the cardinality of (the finite group) $H^1(\mathrm{Frob}_q, A_\phi^{I_q})$, where I_q is the inertia subgroup of $G_{\mathbf{Q}_q}$. The *Tamagawa exponent* $t_q(g) = t_q(g/K)$ of g at q is the p-adic valuation of $c_q(g) \cdot c_q(g \otimes \epsilon_K)$. (If $q|N^-$ then $t_q(g)$ is the largest integer $n \geq 0$ such that the $G_{\mathbf{Q}}$-module $A_g[p^n]$ is unramified at q, cf. [**PW11**, Definition 3.3].)

The following result is due the the work many people, including Gross, Daghig, Hatcher, Hui Xue, Ribet–Takahashi, Pollack–Weston. We refer to [**PW11**] and Section 3.1 of [**BD07**] for more details and precise references.

THEOREM 3.2. *The equality*

$$L^{\mathrm{alg}}(g/K, 1) = \mathscr{L}_p(g/K)^2 \cdot \prod_{q|N^-} p^{t_q(g)}$$

holds in $\mathbf{Z}_p$, up to multiplication by a p-adic unit.

PROOF. Combine Lemma 2.2 and Theorem 6.8 of [**PW11**]. □

4. A theorem of Kato and Skinner–Urban

This section states the result of Kato–Skinner–Urban mentioned in the Introduction, proving the validity of the p-part of the Birch and Swinnerton-Dyer conjecture for weight-two newforms of analytic rank zero (under some technical conditions). Let $g \in S_2(1, N; \mathbf{Z}_p)$ be a weight-two newform with Fourier coefficients in $\mathbf{Z}_p$. Let $K/\mathbf{Q}$ be a quadratic imaginary field of discriminant coprime with Np. Consider as in the preceding section the algebraic part $L^{\mathrm{alg}}(g/K, 1) \in \mathbf{Z}_p$ of the complex special value of g/K. On the algebraic side, write as usual $A_g := T_g \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p \in {}_{\mathbf{Z}_p[G_{\mathbf{Q}}]}\mathrm{Mod}$ for the discrete representation attached to g. Assume that $p \nmid N$ is a prime

of *good ordinary reduction* for g, i.e. that $g(T_p) \in \mathbf{Z}_p^*$. This implies that A_g fits into a short exact sequence of $\mathbf{Z}_p[G_{\mathbf{Q}_p}]$-modules

$$0 \to A_g^+ \to A_g \to A_g^- \to 0,$$

where $A_g^\pm \cong \mathbf{Q}_p/\mathbf{Z}_p$ as $\mathbf{Z}_p$-modules, and $G_{\mathbf{Q}_p}$ acts on A_g^+ via $\varepsilon \cdot \gamma_{g,p}^{-1}$, where $\varepsilon : G_{\mathbf{Q}_p} \to \mathbf{Z}_p^*$ denotes the p-adic cyclotomic character, and $\gamma_{g,p} : G_{\mathbf{Q}} \twoheadrightarrow G_{\mathbf{Q}_p}/I_{\mathbf{Q}_p} \to \mathbf{Z}_p^*$ is the unramified character of $G_{\mathbf{Q}_p}$ sending an arithmetic Frobenius in $G_{\mathbf{Q}_p}/I_{\mathbf{Q}_p}$ to $g(U_p)$. Hence $A_g^- \cong \mathbf{Q}_p/\mathbf{Z}_p(\gamma_{g,p})$ is unramified, with $G_{\mathbf{Q}_p}$ acting via $\gamma_{g,p}$. Define the p-primary *Greenberg (strict) Selmer group* of g/K by

$$\mathrm{Sel}_{p^\infty}(K,g) := \ker\left(H^1(K_{Np}/K, A_g) \xrightarrow{\mathrm{res}_{Np}} \prod_{v|p} \frac{H^1(K_v, A_g)}{H^1_{\mathrm{ord}}(K_v, A_g)_{\mathrm{div}}} \times \prod_{v|N} H^1(K_v, A_g) \right),$$

where K_{Np}/K denotes the maximal algebraic extension of K which is unramified outside Np, and $H^1(K_{Np}/K, A_g)$ stands for $H^1(\mathrm{Gal}(K_{Np}/K), A_g)$. Moreover, the map res_{Np} denotes the direct sum of the restriction maps at v, running over the primes v of K which divide Np. Finally, for every prime $v|p$ of K, $H^1_{\mathrm{ord}}(K_v, A_g) \subset H^1(K_v, A_g)$ is the image of $H^1(K_v, A_g^+)$, and $H^1_{\mathrm{ord}}(K_v, A_g)_{\mathrm{div}}$ is its maximal p-divisible subgroup.

The following theorem combines the work of Kato [**Kat04**] and Skinner–Urban [**SU14**] on the Iwasawa main conjecture for GL_2. More precisely, it follows from Theorem 3.29 of [**SU14**], applied to g and its quadratic twist $g \otimes \epsilon_K$, taking into account the algebraic Birch and Swinnerton-Dyer formulae proved by Mazur. For the precise statement in the level of generality required here, we refer to Theorem B in Skinner's preprint [**Ski14**].

Recall the Tamagawa exponent $t_q(g) = t_q(g/K)$ attached to every prime $q|N$ in the preceding section.

THEOREM 4.1. *Assume that*
1. *$p \nmid N$ and g is p-ordinary,*
2. *the residual representation $\overline{\rho}_g : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$ is irreducible,*
3. *there exists a prime $q \mid N$ such that $\overline{\rho}_g$ is ramified at q.*

Then $L^{\mathrm{alg}}(g/K, 1) \neq 0$ if and only if $\mathrm{Sel}_{p^\infty}(K,g)$ is finite. In this case, the equality

$$L^{\mathrm{alg}}(g/K,1) = \#\mathrm{Sel}_{p^\infty}(K,g) \prod_{q|N} p^{t_q(g)}$$

holds in $\mathbf{Z}_p$, up to multiplication by p-adic units.

5. Heegner points and Shafarevich–Tate groups

Let $A/\mathbf{Q}$ be an elliptic curve of conductor N. Fix a modular parametrisation

$$\pi_A : X_0(N) \longrightarrow A$$

of minimal degree $\deg(\pi_A)$. Let $K/\mathbf{Q}$ be a quadratic imaginary field of discriminant coprime with Np, satisfying the Heegner hypothesis that every prime divisor of N *splits* in $K/\mathbf{Q}$. Fix a Heegner point $\mathbb{P} \in \mathrm{Heeg}_{N,1}(H) \subset X_0(N)(H)$ (see Section 2.1.2, recalling that $X_0(N) = X_{N,1}$ and H/K is the Hilbert class field of K). Define the Heegner point over K

$$P_K := \mathrm{Trace}_{H/K}\big(\pi_A(\mathbb{P})\big) \in A(K).$$

The theorem of Gross–Zagier [**GZ86**] states that P_K is a non-torsion point in $A(K)$ if and only the Hasse–Weil L-function $L(A/K, s)$ of A/K has a simple zero at $s = 1$. Moreover, according to the work of Kolyvagin [**Kol90**], if P_K is a non-torsion point, the Mordell–Weil group $A(K)$ has rank one and the Shafarevich–Tate group $Ш(A/K)$ is finite. In this case, denote by

$$I_p(P_K) := p^{\mathrm{ord}_p[A(K):\, \mathbf{Z}P_K]}$$

the p-part of the index of $\mathbf{Z}P_K$ in $A(K)$. Write, as customary, $Ш(A/K)_{p^\infty}$ for the p-primary part of the Shafarevich–Tate group of A/K. The following theorem is the main result of this note and will imply Theorem A of the Introduction.

THEOREM 5.1. *Assume that $A/\mathbf{Q}$ is semistable, and that $p > 7$ is a prime which does not divide $\deg(\pi_A)$. Assume furthermore that $a_p(A) \not\equiv 0, 1 \pmod p$, resp. $a_p(A) \not\equiv 0, \pm 1 \pmod p$ when p is split, resp. inert in K, and that all primes dividing N are split in K. If $L(A/K, s)$ has a simple zero at $s = 1$, then*

$$I_p(P_K)^2 = \#Ш(A/K)_{p^\infty}.$$

The proof of Theorem 5.1 is given in Section 5.5.

5.1. Setting and notations. Assume from now on that the assumptions of Theorem 5.1 are satisfied, and fix a positive integer n such that

$$n > 2 \cdot \max\Big\{\mathrm{ord}_p\big(I_p(P_K)\big),\ \mathrm{ord}_p\big(\#Ш(A/K)_{p^\infty}\big)\Big\}. \tag{8}$$

Let $f = f_A \in S_2(\Gamma_0(N), \mathbf{Z})$ be the weight-two newform of level N attached to $A/\mathbf{Q}$ by the modularity theorem. With the notations of Section 1.1, one considers

$$f \in S_2(N, 1; \mathbf{Z}_p); \quad N^+ := N; \quad N^- := 1.$$

Note that, since f is q-new at every prime $q \mid N$, one can consider $f \in S_2(N/m, m; \mathbf{Z}_p)$, for every positive divisor m of N. In other words, $f : \mathbb{T}_N := \mathbb{T}_{N,1} \to \mathbf{Z}_p$ factorises through the m-new quotient $\mathbb{T}_{N/m,m}$ of $\mathbb{T}_N$, for every positive divisor m of N. As in Section 2.3, for every $m \in \mathbf{N} \cup \{\infty\}$ let $f_{\{m\}} \in S_2(N, 1; \mathbf{Z}_p/p^m\mathbf{Z}_p)$ denote the reduction of f modulo p^m.

Lemma 5.2. 1. *The data (f, N^+, N^-, K, p) satisfy Assumption 2.1.*
2. *$f_{\{m\}}$ satisfies Assumption 1.1 for every $m \in \mathbf{N} \cup \{\infty\}$.*

Proof. Parts 1, 2, 4 and 5 of Assumption 2.1 are satisfied since A is ordinary at p and $N^- = 1$. As $A/\mathbf{Q}$ is semistable and $p > 7$, Assumption 2.1(3) holds by a result of Mazur [**Maz78**]. Moreover, the representation $T_{f,m} = T_f \otimes \mathbf{Z}_p/p^m\mathbf{Z}_p$ associated with $f_{\{m\}}$ is ordinary at p, hence Assumption 1.1(2) holds. Finally, since $p \nmid \deg(\pi_A)$, Assumption 1.1(3) holds by a result of Ribet [**Rib90**], as explained in Lemma 2.2 of [**BD05**]. □

With the notations of Section 2.3.1, write $\mathcal{L}_m$ for the graph associated to $f_{\{m\}}$, for $m \in \mathbf{N}$. Let $L \in \mathcal{L}_m$ and let $f_L \in S_2(N, L; \mathbf{Z}/p^m\mathbf{Z})$ be the L-level raising of $f_{\{m\}}$ (cf. Section 2.3.1). We say that f_L *can be lifted to a true modular form* if there exists a $\mathbf{Z}_p$-valued eigenform $g = g_L \in S_2(N, L; \mathbf{Z}_p)$ of level (N, L) whose reduction modulo p^m equals f_L (i.e. such that $f_L = g_{\{m\}}$).

5.2. Level raising at one prime. Let $\ell \in \mathcal{L}_n^{\mathrm{def}}$ be an n-admissible prime relative to (f, K). The next result shows that the conclusion of Theorem 5.1 holds under certain assumptions.

Proposition 5.3. *Assume that f_ℓ can be lifted to a true modular form. Moreover, assume that the map $A(K) \otimes \mathbf{Z}/p^n\mathbf{Z} \to A(K_\ell) \otimes \mathbf{Z}/p^n\mathbf{Z}$ (induced by the natural inclusion $A(K) \hookrightarrow A(K_\ell)$) is injective. Then*

$$I_p(P_K)^2 = \#Ш(A/K)_{p^\infty}.$$

The rest of this section will be devoted to the proof Proposition 5.3. Section 2.3.2 attaches to $f_{\{n\}}$ and $1 \in \mathcal{L}^{\mathrm{indef}}$ a global cohomology class $\kappa(1) \in H^1(K, T_{f,n})$. The representation $T_{f,n}$ attached to $f_{\{n\}}$ is nothing but the p^n-torsion submodule A_{p^n} of $A = A(\overline{\mathbf{Q}})$. Since $\overline{\rho}_f$ is irreducible, π_A induces isomorphisms of $\mathbf{Z}_p[G_{\mathbf{Q}}]$-modules $\pi_A : \mathrm{Ta}_p(J)/I_f \cong T_f$ and $\pi_{A,n} : \mathrm{Ta}_p(J)/I_{f,n} \cong T_{f,n}$, where $J/\mathbf{Q} = \mathrm{Jac}(X_0(N))$ is the Jacobian variety of $X_0(N)$, $I_f := \ker(f)$ and $I_{f,n} := \ker\big(f_{\{n\}}\big)$. One can then take $\pi_{A,n} = \pi_1$ in (7), and retracing definitions it follows that, up to multiplication by p-adic units,

$$\kappa(1) = \delta(P_K) \in \mathrm{Sel}(K, f_{\{n\}}), \tag{9}$$

where δ denotes the global Kummer map $A(K)/p^n \hookrightarrow H^1(K, A_{p^n})$. We observe that the class $\kappa(1)$ belongs to the Selmer group $\mathrm{Sel}(K, f_{\{n\}})$, defined in Section 1.2 by ordinary conditions (which can be imposed in the current context in light of Lemma 5.2), since this Selmer group coincides with the usual p^n-Selmer group of A in which the local conditions are described in terms of the local Kummer maps. Indeed, our assumption on $a_p(A)$ being $\not\equiv 1$ or $\not\equiv \pm 1 \pmod p$ implies that the local Selmer conditions at p agree (see for example [**Gre97**]). As for the primes dividing N, this is a direct consequence of the theory of non-archimedean uniformisation for A. This yields the equality up to units

$$I_p(P_K) = v_\ell\big(\kappa(1)\big) \in H^1_{\mathrm{fin}}(K_\ell, T_{f,n}) \cong \mathbf{Z}/p^n\mathbf{Z} \tag{10}$$

(see Section 1.3 for the last isomorphism). To see this, consider the composition

$$A(K) \otimes \mathbf{Z}/p^n\mathbf{Z} \to A(K_\ell) \otimes \mathbf{Z}/p^n\mathbf{Z} \overset{\delta}{\hookrightarrow} H^1_{\mathrm{fin}}(K_\ell, T_{f,n}) \cong \mathbf{Z}/p^n\mathbf{Z}. \tag{11}$$

Since $p > 7$, one has $A(K)_p = 0$ by Mazur's theorem. Moreover, as $\mathrm{ord}_{s=1}L(A/K, s) = 1$, the Gross–Zagier–Kolyvagin theorem gives that $A(K)$ has rank one. It follows that $A(K) \otimes \mathbf{Z}/p^n\mathbf{Z} \cong \mathbf{Z}/p^n\mathbf{Z}$. Since by assumption the first map in (11) is injective, the composition (11) is an isomorphism, and the claim (10) follows. Theorem 2.4 then yields the equality

$$I_p(P_K) = \mathscr{L}_p(\ell) \in \mathbf{Z}/p^n\mathbf{Z}, \tag{12}$$

up to multiplication by p-adic units. Let now $g \in S_2(N,\ell;\mathbf{Z}_p)$ be a $\mathbf{Z}_p$-valued eigenform of level (N,ℓ) lifting f_ℓ. Combining Theorem 3.2 with Theorem 4.1 yields (up to p-adic units)

$$\mathscr{L}_p(g/K)^2 \cdot p^{t_\ell(g)} \overset{\text{Theorem 3.2}}{=} L^{\mathrm{alg}}(g/K,1) \overset{\text{Theorem 4.1}}{=} \#\mathrm{Sel}_{p^\infty}(K,g) \cdot p^{t_\ell(g)}. \tag{13}$$

More precisely, note that g satisfies the assumptions of Theorem 3.2 and Theorem 4.1 by Lemma 5.2. Moreover, as explained in the proof of Lemma 2.2 of [**BD05**], the assumption $p \nmid \deg(\pi_A)$ and Ribet's lowering the level theorem [**Rib90**] imply that $A_p \cong A_{g,1}$ is ramified at every prime $q \mid N$. By the definition of $t_q(g)$, this gives $\prod_{q|N\ell} p^{t_q(g)} = p^{t_\ell(g)}$, and the first equality in (13). Since by construction $\mathscr{L}_p(g/K) \equiv \mathscr{L}_p(\ell) \pmod{p^n}$, and $I_p(P_K)$ is non-zero in $\mathbf{Z}/p^n\mathbf{Z}$ by (8), $\mathscr{L}_p(g/K) \neq 0$ by (12), hence $L^{\mathrm{alg}}(g/K,1) \neq 0$, and the second equality in (13) follows by Theorem 4.1. Combining equations (12) and (13) give the identity

$$I_p(P_K)^2 = \#\mathrm{Sel}_{p^\infty}(K,g). \tag{14}$$

It then remains to compare the cardinality of the p-primary Selmer group $\mathrm{Sel}_{p^\infty}(K,g)$ with that of the p-primary part of the Shafarevich–Tate group $Ш(A/K)$. In order to do that, one first notes that

$$\mathrm{Sel}(K,f_\ell) \cong \mathrm{Sel}_{p^\infty}(K,g), \tag{15}$$

where $\mathrm{Sel}(K,f_\ell)$ is the p^n-Selmer group attached in Section 1.1 to $f_\ell = g_{\{n\}}$. (Note that f_ℓ satisfies Assumption 1.1, thanks to Lemma 5.2.) By the irreducibility of A_p and our assumptions on $a_p(A)$, it is easily seen that the natural map $\mathrm{Sel}(K,f_\ell) \to \mathrm{Sel}_{p^\infty}(K,g)[p^n]$ is an isomorphism (cf. [**Gre97**]). On the other hand, equations (12), (13) and (8) imply that $p^n > \#\mathrm{Sel}_{p^\infty}(K,g)$, hence (15) follows. One is thus reduced to compare the cardinality of $\mathrm{Sel}(K,f_\ell)$ to that of $Ш(A/K)_{p^\infty}$. Kummer theory inserts $Ш(A/K)_{p^\infty}$ in a short exact sequence

$$0 \to A(K) \otimes \mathbf{Z}/p^n\mathbf{Z} \to \mathrm{Sel}(K,f_{\{n\}}) \to Ш(A/K)_{p^\infty} \to 0$$

(one uses again $p^n > \#Ш(A/K)_{p^\infty}$, which follows by (8)). By the discussion above this gives

$$\#Ш(A/K)_{p^\infty} = p^{-n} \cdot \#\mathrm{Sel}(K,f_{\{n\}}). \tag{16}$$

We claim that

$$\mathrm{Sel}^{(\ell)}(K,f_{\{n\}}) = \mathrm{Sel}(K,f_{\{n\}}). \tag{17}$$

where the suffix (ℓ) indicates condition at ℓ relaxed. To prove this, let $x \in \mathrm{Sel}^{(\ell)}(K,f_n)$ be a Selmer class relaxed at ℓ; we have to show that $x \in \mathrm{Sel}(K,f_{\{n\}})$, i.e. that its residue $\partial_\ell(x)$ at ℓ vanishes. Since (11) is an isomorphism, there exists a class $y \in A(K)/p^n \hookrightarrow \mathrm{Sel}(K,f_{\{n\}})$ such that $\mathrm{res}_\ell(y) = v_\ell(y) \in H^1_{\mathrm{fin}}(K_\ell,T_{f,n}) \cong \mathbf{Z}/p^n\mathbf{Z}$ is a unit modulo p^n. For every prime v of K, let $\langle -,-\rangle_v : H^1(K_v,T_{f,n}) \times H^1(K_v,T_{f,n}) \to H^2(K_v,\mu_{p^n}) \cong \mathbf{Z}/p^n\mathbf{Z}$ be the perfect local Tate pairing attached to the Weil pairing $T_{f,n} \times T_{f,n} \to \mu_{p^n}$. The subspace $H^1_{\mathrm{fin}}(K_v,T_{f,n})$ (resp., $H^1_{\mathrm{ord}}(K_v,T_{f,n})$ for $v|\ell Np$) is maximal isotropic for $\langle -,-\rangle_v$, i.e. it is equal to its own orthogonal complement under $\langle -,-\rangle_v$. By the reciprocity law of global class field theory and the definition of $\mathrm{Sel}^{(\ell)}(K,f_{\{n\}})$:

$$0 = \sum_v \langle \mathrm{res}_v(x), \mathrm{res}_v(y)\rangle_v = \langle \mathrm{res}_\ell(x), \mathrm{res}_\ell(y)\rangle_\ell = \langle \partial_\ell(x), v_\ell(y)\rangle_\ell,$$

where the first sum runs over all primes of K. Since $v_\ell(y)$ generates $H^1_{\mathrm{fin}}(K_\ell,T_{f,n})$ by assumption and the Tate local duality induces a perfect pairing between this finite part and the ordinary (or singular) part $H^1_{\mathrm{ord}}(K_\ell,T_{f,n})$, this implies $\partial_\ell(x) = 0$, as was to be shown.

Using again that (11) is an isomorphism, together with equation (2), one deduces the exact sequence

$$0 \to \mathrm{Sel}(K,f_\ell) \to \mathrm{Sel}^{(\ell)}(K,f_{\{n\}}) \xrightarrow{v_\ell} H^1_{\mathrm{fin}}(K_\ell,T_{f,n}) \cong \mathbf{Z}/p^n\mathbf{Z} \to 0. \tag{18}$$

This allows us to to conclude the proof of the proposition, as it gives

$$I_p(P_K)^2 \overset{(14)}{=} \#\mathrm{Sel}_{p^\infty}(K,g) \overset{(15)}{=} \#\mathrm{Sel}(K,f_\ell) \overset{(18)}{=} p^{-n} \cdot \#\mathrm{Sel}^{(\ell)}(K,f_{\{n\}}) \overset{(17)}{=} p^{-n} \cdot \#\mathrm{Sel}(K,f_{\{n\}}) \overset{(16)}{=} \#Ш(A/K)_{p^\infty}.$$

5.3. Level raising at three n-admissible primes. Write in this section $\mathcal{L} = \mathcal{L}_{2n}$. Fix three primes ℓ_1, ℓ_2 and ℓ_3 in $\mathcal{L}$ (so that ℓ_1, ℓ_2 and ℓ_3 are $2n$-admissible primes relative to (f,K)).

Since Assumption 2.1 is satisfied by Lemma 5.2, Section 2.3.2 attaches to $(f,1)$ and $(f,\ell_1\ell_2)$ Selmer classes

$$\kappa(1) = \delta(P_K) \in \mathrm{Sel}(K,f_{\{2n\}}); \quad \kappa(\ell_1\ell_2) \in \mathrm{Sel}(K,f_{\ell_1\ell_2}).$$

The fact that the first class belongs to $\mathrm{Sel}(K,f_{\{2n\}})$ was explained after equation (9). A similar argument applies to the second class, recalling that it arises as the Kummer image of a Heegner point on the Shimura curve $X_{N,\ell_1\ell_2}$ and invoking the Cerednik–Drinfeld theory of non-archimedean uniformisation for this curve at the primes ℓ_1 and ℓ_2 (see [**BD05**] for more details). If $\kappa(\ell_1\ell_1) \neq 0$, set

$$\widetilde{\kappa}(\ell_1\ell_2) := p^{t-1} \cdot \kappa(\ell_1\ell_2) \in H^1(K,T_{f,1}),$$

where $t \leq 2n$ is the smallest positive integer such that $p^t \cdot \kappa(\ell_1\ell_2) = 0$ (and we identify $H^1(K, T_{f,1})$ with $H^1(K, T_{f,2n})[p]$, which is possible since $T_{f,1}^{G_K} = 0$). If $\kappa(\ell_1\ell_2) = 0$, set $\widetilde{\kappa}(\ell_1\ell_2) := 0$ (in $H^1(K, T_{f,1})$). Recall the morphisms $v_{\ell_j} : H^1(K, T_{f,k}) \to H^1_{\mathrm{fin}}(K_{\ell_j}, T_{f,k}) \cong \mathbf{Z}/p^k\mathbf{Z}$ ($k \geq 1$). The aim of this section is to prove the following proposition.

PROPOSITION 5.4. *Assume that $f_{\ell_1\ell_2\ell_3}$ can be lifted to a true modular form of level $(N, \ell_1\ell_2\ell_3)$. Assume moreover that the restriction map $A(K)/p^n \to A(K_{\ell_1})/p^n$ at ℓ_1 is injective, and that $v_{\ell_3}\big(\widetilde{\kappa}(\ell_1\ell_2)\big) \neq 0$. Then*

$$I_p(P_K)^2 = \#Ш(A/K)_{p^\infty}.$$

The rest of this section will be devoted to the proof of Proposition 5.4. In particular, assume from now on that the assumptions of the proposition are satisfied.

Let $r \leq 2n$ be a positive integer. Since ℓ_1, ℓ_2 and ℓ_3 are $2n$-admissible primes, they are also r-admissible primes relative to (f, K, p). For every divisor m of $\ell_1\ell_2\ell_3$ write

$$\mathrm{Sel}_{p^r}(K, f_m) \subset H^1(K, T_{f,r}); \quad \mathrm{Sel}_{p^r}(K, f) := \mathrm{Sel}(K, f_{\{r\}})$$

to denote the Selmer group attached to the reduction modulo p^r of the mod-p^{2n} form f_m. For every $L \in \mathcal{L}$, let

$$\mathrm{Sel}^{(L)}_{p^r}(K, f_m) \subset H^1(K, T_{f,r})$$

be the relaxed Selmer group at L, i.e. the Selmer group defined by the same local conditions used to define $\mathrm{Sel}_{p^r}(K, f_m)$ at every prime of K which does not divide L, and by imposing *no* local condition at every prime of K dividing L. As explained in Section 3 of [**BD05**] (see in particular Proposition 3.3 and the references therein), we can enlarge $\ell_1\ell_2\ell_3$ to an integer $L \in \mathcal{L}$ which *controls* the Selmer group. More precisely, there exists $L \in \mathcal{L}$, divisible by $\ell_1\ell_2\ell_3$, such that the restriction map $\mathrm{Sel}_{p^{2n}}(K, f_{\{2n\}}) \to \bigoplus_{\ell|L} H^1(K_\ell, T_{f,2n})$ is injective and

$$\mathrm{Sel}^{(L)}_{p^{2n}}(K, f) \cong \big(\mathbf{Z}/p^{2n}\mathbf{Z}\big)^{\#L}$$

is free of rank $\#L$ over $\mathbf{Z}/p^{2n}\mathbf{Z}$, where $\#L := \#\{\ell : \ell \text{ prime and } \ell|L\}$. Fix from now on such an L. For every element $0 \neq x \in \mathrm{Sel}^{(L)}_{p^{2n}}(K, f)$, denote by $\mathrm{ord}_p(x)$ the largest integer such that $x \in p^{\mathrm{ord}_p(x)} \cdot \mathrm{Sel}^{(L)}_{p^{2n}}(K, f)$.

Theorem 2.3 and Theorem 2.4 yield the equality (up to multiplication by p-adic units)

$$I_p(P_K) = v_{\ell_1}\big(\kappa(1)\big) \overset{\text{Theorem 2.4}}{=} \mathscr{L}_p(\ell_1) \overset{\text{Theorem 2.3}}{=} \partial_{\ell_2}\big(\kappa(\ell_1\ell_2)\big) \in \mathbf{Z}/p^{2n}\mathbf{Z}, \tag{19}$$

the first equality being a consequence of the injectivity of the localisation map $A(K)/p^n \hookrightarrow A(K_{\ell_1})/p^n$, as explained in the proof Proposition 5.3 (see (10)). By (8) one deduces

$$\xi(\ell_1\ell_2) := \mathrm{ord}_p\big(\kappa(\ell_1\ell_2)\big) \leq \mathrm{ord}_p\big(\partial_{\ell_2}(\kappa(\ell_1\ell_2))\big) = \mathrm{ord}_p\left(I_p(P_K)\right) < n. \tag{20}$$

Let $\widehat{\kappa}(\ell_1\ell_2) \in \mathrm{Sel}^{(L)}_{p^{2n}}(K, f)$ be such that $p^{\xi(\ell_1\ell_2)} \cdot \widehat{\kappa}(\ell_1\ell_2) = \kappa(\ell_1\ell_2) \in \mathrm{Sel}^{(L)}_{p^{2n}}(K, f)$. Consider the natural map

$$\mathrm{Sel}^{(L)}_{p^{2n}}(K, f) \longrightarrow \mathrm{Sel}^{(L)}_{p^n}(K, f) \tag{21}$$

induced by the projection $T_{f,2n} \twoheadrightarrow T_{f,n}$, and write $\kappa'(\ell_1\ell_2) \in \mathrm{Sel}^{(L)}_{p^n}(K, f)$ for the image of $\widehat{\kappa}(\ell_1\ell_2)$. Note that, while $\widehat{\kappa}(\ell_1\ell_2)$ is well-defined only up to elements in $\mathrm{Sel}^{(L)}_{p^{2n}}(K, f)[p^{\xi(\ell_1\ell_2)}]$, $\kappa'(\ell_1\ell_2)$ depends only on $\kappa(\ell_1\ell_2)$.

LEMMA 5.5. *The class $\kappa'(\ell_1\ell_2)$ enjoys the following properties:*
1. *$\kappa'(\ell_1\ell_2) \in \mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2})$;*
2. *$\kappa'(\ell_1\ell_2)$ has exact order p^n;*
3. *$\partial_{\ell_2}\big(\kappa(\ell_1\ell_2)\big) \pmod{p^n} = p^{\xi(\ell_1\ell_2)} \cdot \partial_{\ell_2}\big(\kappa'(\ell_1\ell_2)\big) \in \mathbf{Z}/p^n\mathbf{Z}$, up to multiplication by units in $(\mathbf{Z}/p^n\mathbf{Z})^*$;*
4. *$v_{\ell_3}\big(\kappa'(\ell_1\ell_2)\big) \in (\mathbf{Z}/p^n\mathbf{Z})^*$ and $v_{\ell_3}\big(\kappa(\ell_1\ell_2)\big) \pmod{p^n} = p^{\xi(\ell_1\ell_2)}$, up to units in $(\mathbf{Z}/p^n\mathbf{Z})^*$.*

PROOF. Since $\mathrm{Sel}^{(L)}_{p^{2n}}(K, f)$ is free over $\mathbf{Z}/p^{2n}\mathbf{Z}$, $\widehat{\kappa}(\ell_1\ell_2)$ has order p^{2n}. If $x \in \mathrm{Sel}^{(L)}_{p^{2n}}(K, f) \subset H^1(K, T_{f,2n})$ belongs to the kernel of the map (21), then x comes from a class in $H^1(K, p^n \cdot T_{f,2n})$, hence is killed by p^n. It follows that $\kappa'(\ell_1\ell_2)$ has order p^n, thus proving part 2. To show part 1, i.e. that $\kappa'(\ell_1\ell_2)$ belongs to $\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2})$, one has to prove that $v_q\big(\kappa'(\ell_1\ell_2)\big) = 0$ for $q|\ell_1\ell_2$, and that $\partial_\ell\big(\kappa'(\ell_1\ell_2)\big) = 0$ for every ℓ dividing $L/\ell_1\ell_2$. This follows by the fact that $p^{\xi(\ell_1\ell_2)} \cdot \widehat{\kappa}(\ell_1\ell_2)$ already satisfies these properties, and by the fact that $\xi(\ell_1\ell_2) < n$ (see (20)). Indeed, for $? \in \{\mathrm{fin}, \mathrm{sing}\}$ and $k \in \{n, 2n\}$, there is an isomorphism $H^1_?(K, T_{f,k}) \cong \mathbf{Z}/p^k\mathbf{Z}$ (cf. Section 1.3), and the morphism $H^1_?(K_\ell, T_{f,2n}) \to H^1_?(K_\ell, T_{f,n})$ induced by $T_{f,2n} \twoheadrightarrow T_{f,n}$ corresponds to the canonical projection $\mathbf{Z}/p^{2n}\mathbf{Z} \to \mathbf{Z}/p^n\mathbf{Z}$. Part 3 also follows by the last argument. Finally, let t be the order of $\kappa(\ell_1\ell_2) \in \mathrm{Sel}^{(L)}_{p^{2n}}(K, f_{\ell_1\ell_2})$, so that $p^{\xi(\ell_1\ell_2)+t-1} \cdot \widehat{\kappa}(\ell_1\ell_2) = \widetilde{\kappa}(\ell_1\ell_2)$, and $\xi(\ell_1\ell_2) + t = 2n$. By assumption, $v_{\ell_3}\big(\widetilde{\kappa}(\ell_1\ell_2)\big) \neq 0$, which implies that $v_{\ell_3}\big(\widehat{\kappa}(\ell_1\ell_2)\big)$ has order p^{2n} in $\mathbf{Z}/p^{2n}\mathbf{Z}$, i.e. it is a unit modulo p^{2n}. Since, as remarked above, $v_{\ell_3}\big(\kappa'(\ell_1\ell_2)\big)$ is the image of $v_{\ell_3}\big(\widehat{\kappa}(\ell_1\ell_2)\big)$ under the projection $\mathbf{Z}/p^{2n}\mathbf{Z} \twoheadrightarrow \mathbf{Z}/p^n\mathbf{Z}$, Part 4 follows. □

Thanks to part 3 of the preceding lemma, (19) can be rewritten in term of the class $\kappa'(\ell_1\ell_2)$, i.e.

$$I_p(P_K) = p^{\xi(\ell_1\ell_2)} \cdot \partial_{\ell_2}\big(\kappa'(\ell_1\ell_2)\big) \in \mathbf{Z}/p^n\mathbf{Z}.$$

(The latter equality, valid up to multiplication by p-adic units, takes place now in $\mathbf{Z}/p^n\mathbf{Z}$, while (19) was an equality in $\mathbf{Z}/p^{2n}\mathbf{Z}$.) Moreover, Theorem 2.4 and Part 4 of the preceding lemma give

$$\mathscr{L}_p(\ell_1\ell_2\ell_3) \pmod{p^n} \overset{\text{Theorem 2.4}}{=} v_{\ell_3}\big(\kappa(\ell_1\ell_2)\big) \pmod{p^n} = p^{\xi(\ell_1\ell_2)} \in \mathbf{Z}/p^n\mathbf{Z}$$

(as usual up to p-adic units). We now make use of the assumption that $f_{\ell_1\ell_2\ell_3}$ can be lifted to a true modular form $g \in S_2(N, \ell_1\ell_2\ell_3; \mathbf{Z}_p)$. Using Theorem 3.2 and Theorem 4.1 one proves, by the same argument used in the proof of Proposition 5.3, that up to p-adic units

$$\mathscr{L}_p(g/K)^2 = \#\mathrm{Sel}_{p^\infty}(K, g) = \#\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2\ell_3}).$$

(To justify the second equality, note that $\mathscr{L}_p(\ell_1\ell_2\ell_3) \pmod{p^n} = p^{\xi(\ell_1\ell_2)}$ is non-zero in $\mathbf{Z}/p^n\mathbf{Z}$, as follows by (20), and proceed as in the proof of equation (15) in the proof of Proposition 5.3.) The preceding three equations combine to give

$$I_p(P_K)^2 = p^{2\cdot\mathrm{ord}_p\left(\partial_{\ell_2}\left(\kappa'(\ell_1\ell_2)\right)\right)} \cdot \#\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2\ell_3}). \tag{22}$$

(Here, given $0 \neq x \in \mathbf{Z}/p^n\mathbf{Z}$, $\mathrm{ord}_p(x)$ denotes the positive integer s.t. $\big(p^{\mathrm{ord}_p(x)}\big) = (x)$ as ideals of $\mathbf{Z}/p^n\mathbf{Z}$.) The proof of Proposition 5.4 will then result combining equation (22) with the following lemma.

Lemma 5.6.

$$\#Ш(A/K)_{p^\infty} = p^{2\cdot\mathrm{ord}_p\left(\partial_{\ell_2}\left(\kappa'(\ell_1\ell_2)\right)\right)} \cdot \#\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2\ell_3}).$$

Proof. Recall that by assumption the localisation map $A(K)/p^n \hookrightarrow A(K_{\ell_1})/p^n$ is injective. As in the proof of Proposition 5.3, this implies

$$\#\mathrm{Sel}_{p^n}(K, f_{\ell_1}) = \#Ш(A/K)_{p^\infty}. \tag{23}$$

Given this, the proof naturally breaks into two parts. One first compares the Selmer groups $\mathrm{Sel}_{p^n}(K, f_{\ell_1})$ and $\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2})$, and proves the equality

$$\#\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2}) = p^{n-2\cdot\mathrm{ord}_p\left(\partial_{\ell_2}\left(\kappa'(\ell_1\ell_2)\right)\right)} \cdot \#\mathrm{Sel}_{p^n}(K, f_{\ell_1}). \tag{24}$$

One then compares the Selmer groups $\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2})$ and $\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2\ell_3})$, and shows that

$$\#\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2}) = p^n \cdot \#\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2\ell_3}). \tag{25}$$

The lemma will then follow by combining the preceding three equations.

By Poitou–Tate duality, as formulated e.g. in [**Rub00**, Theorem 1.7.3] (see also [**Mil04**, Chapter I]), and the very definitions of the Selmer groups (see Section 1.2), there is an exact sequence

$$0 \to \mathrm{Sel}_{p^n}(K, f_{\ell_1}) \to \mathrm{Sel}_{p^n}^{(\ell_2)}(K, f_{\ell_1\ell_2}) \xrightarrow{\partial_{\ell_2}} H^1_{\mathrm{sing}}(K_{\ell_2}, T_{f,n}) \cong H^1_{\mathrm{fin}}(K_{\ell_2}, T_{f,n})^\vee \xrightarrow{v_{\ell_2}^\vee} \mathrm{Sel}_{p^n}(K, f_{\ell_1})^\vee,$$

where $(\cdot)^\vee := \mathrm{Hom}(\cdot, \mathbf{Z}/p^n\mathbf{Z})$, the isomorphism is induced by the local Tate pairing (cf. the proof of Proposition 5.3), and $v_{\ell_2}^\vee$ refers to the dual of the morphism $v_{\ell_2} = \mathrm{res}_{\ell_2} : \mathrm{Sel}_{p^n}(K, f_{\ell_1}) \to H^1_{\mathrm{fin}}(K, T_{f,n})$. Similarly, one has the exact sequence

$$0 \to \mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2}) \to \mathrm{Sel}_{p^n}^{(\ell_2)}(K, f_{\ell_1\ell_2}) \xrightarrow{v_{\ell_2}} H^1_{\mathrm{fin}}(K_{\ell_2}, T_{f,n}) \cong H^1_{\mathrm{sing}}(K_{\ell_2}, T_{f,n})^\vee \xrightarrow{\partial_{\ell_2}^\vee} \mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2})^\vee.$$

The existence of these exact sequences yields

$$\#\partial_{\ell_2}\big(\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2})\big) \cdot \#v_{\ell_2}\big(\mathrm{Sel}_{p^n}^{(\ell_2)}(K, f_{\ell_1\ell_2})\big) = p^n = \#\partial_{\ell_2}\big(\mathrm{Sel}_{p^n}^{(\ell_2)}(K, f_{\ell_1\ell_2})\big) \cdot \#v_{\ell_2}\big(\mathrm{Sel}_{p^n}(K, f_{\ell_1})\big). \tag{26}$$

We claim that

$$\partial_{\ell_2}\big(\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2})\big) = \partial_{\ell_2}\big(\kappa'(\ell_1\ell_2)\big) \cdot \mathbf{Z}/p^n\mathbf{Z} = \partial_{\ell_2}\big(\mathrm{Sel}_{p^n}^{(\ell_2)}(K, f_{\ell_1\ell_2})\big). \tag{27}$$

This would easily imply equation (24). Indeed, equations (26) and (27) would then give

$$\frac{\#\partial_{\ell_2}\big(\mathrm{Sel}_{p^n}^{(\ell_2)}(K, f_{\ell_1\ell_2})\big)}{\#v_{\ell_2}\big(\mathrm{Sel}_{p^n}^{(\ell_2)}(K, f_{\ell_1\ell_2})\big)} \overset{(27)}{=} \frac{\Big(\#\partial_{\ell_2}\big(\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2})\big)\Big)^2}{\#\partial_{\ell_2}\big(\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2})\big) \cdot \#v_{\ell_2}\big(\mathrm{Sel}_{p^n}^{(\ell_2)}(K, f_{\ell_1\ell_2})\big)} \overset{(26) \text{ and } (27)}{=} p^{n-2\mathrm{ord}_p\left(\partial_{\ell_2}\left(\kappa'(\ell_1\ell_2)\right)\right)}.$$

On the other hand, the (trivial part of the) exact sequences above show that the first term in the previous equation is equal to the ratio $\#\mathrm{Sel}_{p^n}(K, f_{\ell_1\ell_2})/\#\mathrm{Sel}_{p^n}(K, f_{\ell_1})$, and equation (24) would follow. In order to prove equation (27), note that

$$\mathrm{Sel}_{p^n}^{(\ell_2)}(K, f_{\ell_1\ell_2}) = \kappa'(\ell_1\ell_2) \cdot \mathbf{Z}/p^n\mathbf{Z} \oplus Ш_{\ell_1\ell_2}$$

for a certain direct summand $Ш_{\ell_1\ell_2}$. This follows by Parts 1 and 2 of Lemma 5.5. Assume *ad absurdum* that there is a class (β,α), with $\beta \in \kappa'(\ell_1\ell_2)\cdot \mathbf{Z}/p^n\mathbf{Z}$ and $0 \neq \alpha \in Ш_{\ell_1\ell_2}$, such that

$$\partial_{\ell_2}\big(\kappa'(\ell_1\ell_2)\big)\cdot \mathbf{Z}/p^n\mathbf{Z} \subsetneq \partial_{\ell_2}\big(\beta,\alpha\big)\cdot \mathbf{Z}/p^n\mathbf{Z} = \partial_{\ell_2}\big(\mathrm{Sel}_{p^n}^{(\ell_2)}(K,f_{\ell_1\ell_2})\big).$$

Without loss of generality, one can assume $\beta = 0$. Say $\partial_{\ell_2}(\alpha) = u_1\cdot p^t$ and $\partial_{\ell_2}\big(\kappa'(\ell_1\ell_2)\big) = u_2\cdot p^{t'}$, for units $u_j \in (\mathbf{Z}/p^n\mathbf{Z})^*$, and integers $t < t' < n$. Since the images of $p^{t'-t}\cdot\alpha$ and $\kappa'(\ell_1\ell_2)$ under ∂_{ℓ_2} generate the same ideal of $\mathbf{Z}/p^n\mathbf{Z}$, there exists a unit $u \in (\mathbf{Z}/p^n\mathbf{Z})^*$ such that $u\cdot p^{t'-t}\cdot\alpha - \kappa'(\ell_1\ell_2)$ belongs to the kernel of ∂_{ℓ_2}. In other words $u\cdot p^{t'-t}\cdot\alpha - \kappa'(\ell_1\ell_2) \in \mathrm{Sel}_{p^n}(K,f_{\ell_1})$. Let C be the smallest non-negative integer such that p^C kills $Ш(A/K)_{p^\infty}$. Equation (23) implies that p^C kills $u\cdot p^{t'-t}\cdot\alpha - \kappa'(\ell_1\ell_2)$, so that $p^C\cdot\kappa'(\ell_1\ell_2) = u\cdot p^{C+t'-t}\cdot\alpha = 0$. Since $\kappa'(\ell_1\ell_2)$ has order p^n by Lemma 5.5(2), this implies $C \geq n$, which is impossible by the choice (8) of n. This contradiction proves the second equality in (27), and since $\kappa'(\ell_1\ell_2) \in \mathrm{Sel}_{p^n}(K,f_{\ell_1\ell_2})$ by Lemma 5.5(1), the first equality follows too. As explained above, this also proves equation (24).

To conclude the proof of the proposition, one is left with the proof of equation (25). By Parts 1 and 4 of Lemma 5.5, $\kappa'(\ell_1\ell_2) \in \mathrm{Sel}_{p^n}(K,f_{\ell_1\ell_2})$, and $v_{\ell_3}\big(\kappa'(\ell_1\ell_2)\big)$ generates $\mathbf{Z}/p^n\mathbf{Z}$. In particular

$$v_{\ell_3}\big(\mathrm{Sel}_{p^n}^{(\ell_3)}(K,f_{\ell_1\ell_2\ell_3})\big) = \mathbf{Z}/p^n\mathbf{Z} = v_{\ell_3}\big(\mathrm{Sel}_{p^n}(K,f_{\ell_1\ell_2})\big).$$

As for equation (17) in the proof of Proposition 5.3, this implies (via Poitou–Tate duality)

$$\mathrm{Sel}_{p^n}^{(\ell_3)}(K,f_{\ell_1\ell_2\ell_3}) = \mathrm{Sel}_{p^n}(K,f_{\ell_1\ell_2}),$$

and then equation (25) follows from the short exact sequence

$$0 \to \mathrm{Sel}_{p^n}(K,f_{\ell_1\ell_2\ell_3}) \to \mathrm{Sel}_{p^n}^{(\ell_3)}(K,f_{\ell_1\ell_2\ell_3}) \xrightarrow{v_{\ell_3}} H^1_{\mathrm{fin}}(K,T_{f,n}) \cong \mathbf{Z}/p^n\mathbf{Z} \to 0.$$

□

5.4. A lifting theorem. In order to apply Proposition 5.3 and Proposition 5.4 to the proof of Theorem 5.1, we need the following *lifting theorem*, proved in Part 3 of [**BV15**]. The notations and assumptions are as in the previous sections; in particular $p \nmid \deg(\pi_A)$.

THEOREM 5.7. *Let ℓ_1 be a $2n$-admissible prime relative to (f,K,p). Assume that f_{ℓ_1}* cannot *be lifted to a true modular form. Then there exists infinitely many pairs (ℓ_2,ℓ_3) of $2n$-admissible primes such that:*

1. *$f_{\ell_1\ell_2\ell_3} \in S_2(N,\ell_1\ell_2\ell_3;\mathbf{Z}/p^{2n}\mathbf{Z})$ can be lifted to a true modular form $g := g_{\ell_1\ell_2\ell_3} \in S_2(N,\ell_1\ell_2\ell_3;\mathbf{Z}_p)$,*
2. *$v_{\ell_3}\big(\widetilde{\kappa}(\ell_1\ell_2)\big) \neq 0$ if and only if $\widetilde{\kappa}(\ell_1\ell_2) \neq 0$.*

5.5. Proof of Theorem 5.1. The following proposition is a consequence of Theorem 3.2 of [**BD05**].

PROPOSITION 5.8. *For every positive integer t, there exist infinitely many t-admissible primes ℓ relative to (f,K) such that the natural map $\iota_{\ell,t} : A(K)\otimes\mathbf{Z}/p^t\mathbf{Z} \to A(K_\ell)\otimes\mathbf{Z}/p^t\mathbf{Z}$ is an isomorphism.*

PROOF. As noted in the proof of Proposition 5.3, under our assumptions $A(K)\otimes\mathbf{Z}/p^t\mathbf{Z} \cong \mathbf{Z}/p^t\mathbf{Z}\cdot\mathbb{P}$, for every generator $\mathbb{P}$ of $A(K)$ modulo torsion. Similarly, for every t-admissible prime ℓ, the local Kummer map gives an isomorphism $A(K_\ell)\otimes\mathbf{Z}/p^t\mathbf{Z} \cong H^1_{\mathrm{fin}}(K_\ell,A_{p^t}) \cong \mathbf{Z}/p^t\mathbf{Z}$ (cf. Section 1.3). Let $\kappa_p \in H^1(K,A_p)$ be the image of $\mathbb{P} \pmod p \in A(K)\otimes\mathbf{F}_p$ under the global Kummer map $A(K)\otimes\mathbf{F}_p \hookrightarrow H^1(K,A_p)$. Theorem 3.2 of [**BD05**] shows that there exist infinitely many t-admissible primes ℓ relative to (f,K) such that $v_\ell(\kappa_p) \neq 0$ in $H^1_{\mathrm{fin}}(K_\ell,A_p)$. Since $v_\ell(\kappa_p)$ is the image of $\iota_{\ell,t}(\mathbb{P}) \pmod p \in A(K_\ell)\otimes\mathbf{F}_p$ under the local Kummer map $A(K_\ell)\otimes\mathbf{F}_p \cong H^1_{\mathrm{fin}}(K_\ell,A_p)$, this implies that $\iota_{\ell,t}(\mathbb{P})$ is not divisible by p in $A(K_\ell)\otimes\mathbf{Z}/p^t\mathbf{Z}$, i.e. that $\iota_{\ell,t}$ is an isomorphism, hence proving the proposition. □

We are now ready to prove Theorem 5.1. Thanks to the preceding proposition, one can fix a $2n$-admissible prime ℓ_1 relative to (f,K) such that $A(K)\otimes\mathbf{Z}/p^{2n}\mathbf{Z} \cong A(K_{\ell_1})\otimes\mathbf{Z}/p^{2n}\mathbf{Z}$. Let $f_{\ell_1} \in S_2(N,\ell_1;\mathbf{Z}/p^{2n}\mathbf{Z})$ be a level raising at ℓ_1 of the reduction of f modulo p^{2n}. If f_{ℓ_1} can be lifted to a true modular form of level (N,ℓ_1), apply Proposition 5.3 to conclude the proof of Theorem 5.1. Assume, on the contrary, that f_{ℓ_1} cannot be lifted to a true modular form. Then Theorem 5.7 guarantees the existence of infinitely many pairs (ℓ_2,ℓ_3) of $2n$-admissible primes such that: (i) the level raising $f_{\ell_1\ell_2\ell_3} \in S_2(N,\ell_1\ell_2\ell_3;\mathbf{Z}/p^{2n}\mathbf{Z})$ at $\ell_1\ell_2\ell_3$ of $f_{\{2n\}}$ can be lifted to a true modular form, and (ii) the image of $\widetilde{\kappa}(\ell_1\ell_2) \in H^1(K,A_p)$ under the map $v_{\ell_3} : H^1(K,A_p) \to H^1_{\mathrm{fin}}(K_{\ell_3},A_p)$ is non-zero. Indeed equation (20) implies that $\widetilde{\kappa}(\ell_1\ell_2) \neq 0$ for every $2n$-admissible prime ℓ_2, thanks to the injectivity of the localisation map $A(K)/p^n \hookrightarrow A(K_{\ell_1})/p^n$ at ℓ_1, so that (ii) holds true. In this case, Theorem 5.1 is a consequence of Proposition 5.4.

5.6. Generalisations. The statements of the results of the previous sections do not strive for a maximal degree of generality, but rather aim at keeping technicalities and notations as simple as possible. In this section, we briefly point at possible ways of generalising our results.

Semistability. Theorem 5.1 (and Theorem A of the Introduction) is stated under the assumption that the elliptic curve A is semistable. This makes it possible to consider in our arguments Selmer groups defined in terms of ordinary local conditions at the bad primes, and therefore to compare Selmer groups attached to different modular forms in a direct and elementary way. When N is not squarefree, the lack of natural ordinary conditions at the non-semistable primes may be obviated by imposing non-self dual local conditions. For example, one may view the cohomology classes $\kappa(1)$ and $\kappa(\ell_1\ell_2)$ as belonging to Selmer groups with relaxed local conditions at these primes, and keep track of the appearance of the restricted counterparts of these Selmer groups in the Poitou–Tate sequences of the proofs of Section 5.

The Heegner hypothesis. Section 6 below deduces Theorem A from Theorem 5.1 by choosing an auxiliary imaginary quadratic field K in which all prime divisors of the conductor of A are split, and hence the Heegner hypothesis of Section 5 is satisfied. A more general version of Theorem 5.1 can be proved along the same lines when K satisfies the generalised Heegner hypothesis Assumption 2.1(1,2). In this case, the Heegner point P_K arises on the Shimura curve X_{N^+,N^-} and the class $\kappa(\ell_1\ell_2)$ comes from a Heegner point on $X_{N^+,N^-\ell_1\ell_2}$. Since the results of the previous sections hold at this level of generality, and the Gross–Zagier formula has been generalised to Shimura curves by Zhang [**Zha01**], the proof of Theorem 5.1 goes through unchanged.

The non-anomalous condition. Our main results depend on the assumption that p is a non-anomalous ordinary prime for A/K. This implies that the local Selmer condition at p arising from the local Kummer map coincides with the ordinary condition. The latter condition is defined solely in terms of the Galois representation A_{p^n}. As a consequence, both classes $\kappa(1)$ and $\kappa(\ell_1\ell_2)$, which are defined as the Kummer images of Heegner points on *different* Shimura curves, satisfy the *same* local condition at p. When p is anomalous, one faces the need of directly comparing the images of the two different local Kummer maps. This requires a more sophisticated analysis of the models for A_{p^n} over the ring of integers of $K\otimes\mathbf{Z}_p$, as is carried out for example in Section 4 of [**GP12**].

The ordinary condition. The technical heart of our proof of Theorem 5.1 is represented by the explicit reciprocity laws of Section 2, which hold without the ordinary assumption. (Note that this hypothesis is imposed in [**BD05**] in order to obtain results over the anticyclotomic $\mathbf{Z}_p$-extension of K, and not just over the base.) In order to extend Theorem 5.1 (and its consequence Theorem A) to an elliptic curve having supersingular reduction at p, one considers Selmer groups where the local condition at p is defined to be the Kummer condition. As above, the comparison of Selmer conditions at p can be done following [**GP12**]. In order to complete the proofs, one needs an extension of Theorem 4.1 to the supersingular setting, similar to that announced in [**Wan14**].

6. Proof of Theorem A

In this section we prove Theorem A stated in the Introduction.

Thus, as in the Introduction and in Section 5, let $A/\mathbf{Q}$ be a semistable elliptic curve of conductor N, let $p>7$ be a non-anomalous prime of good ordinary reduction, and fix a modular parametrisation $\pi_A : X_0(N)\to A$ of minimal degree $\deg(\pi_A)$. Assume moreover that p does not divide $\deg(\pi_A)$ and that $L(A/\mathbf{Q},s)$ has a simple zero at $s=1$.

`Step I.` Thanks to the results of [**BFH90**], there exists a quadratic imaginary field $K/\mathbf{Q}$ such that

- (α) the discriminant of $K/\mathbf{Q}$ is coprime with $6Np$, and every prime divisor of Np splits in $K/\mathbf{Q}$;
- (β) the Hasse–Weil L-function $L(A/K,s)$ of A/K has a simple zero at $s=1$.

Writing $A^K/\mathbf{Q}$ for the K-quadratic twist of A, one has $L(A/K,s)=L(A/\mathbf{Q},s)\cdot L(A^K/\mathbf{Q},s)$, so that ($\beta$) is equivalent to $L(A^K/\mathbf{Q},1)\neq 0$. In particular

$$L'(A/K,1)=L'(A/\mathbf{Q},1)\cdot L(A^K/\mathbf{Q},1). \tag{28}$$

`Step II.` The Gross–Zagier formula [**GZ86**, Section V, Theorem 2.1] states that

$$\frac{D_K^{\frac{1}{2}}\cdot L'(A/K,1)}{c^2\cdot\Omega_{A/K}\cdot h^{\mathrm{NT}}(\mathbf{P}_K)}=[A(K):\mathbf{Z}P_K]^2.$$

Here c is the *Manin constant* associated with the strong Weil curve in the isogeny class of $A/\mathbf{Q}$, D_K is the absolute value of the discriminant of $K/\mathbf{Q}$, and $\Omega_{A/K}\in\mathbf{C}^*$ is the Néron period of A/K. Moreover, $\mathbf{P}_K$ denotes a generator of $A(K)/\text{torsion}$, $h^{\mathrm{NT}}(\mathbf{P}_K)\in\mathbf{R}$ its Néron–Tate canonical height, and $P_K\in A(K)$ the Heegner point attached to π_A (cf. Section 5). A result of Mazur [**Maz78**] states that $p^2|4N$ if $p|c$, hence c^2 is a p-adic unit in our setting. Moreover, $\Omega_{A/K}=D_K^{1/2}\cdot\Omega_A\cdot\Omega_{A^K}$, where Ω_* is the real Néron period of the elliptic curve $*/\mathbf{Q}$ [**GZ86**, Page

312]. Using (28), the preceding equation gives

$$\frac{L'(A/\mathbf{Q},1)}{\Omega_A\cdot h^{\mathrm{NT}}(\mathbf{P})}\cdot\frac{L(A^K/\mathbf{Q},1)}{\Omega_{A^K}}\doteq[A(K):\mathbf{Z}P_K]^2, \tag{29}$$

where $\doteq$ denotes equality up to multiplication by a p-adic unit, and $\mathbf{P}$ is a generator of $A(\mathbf{Q})/\text{torsion}$. (Note that in our setting $P_K\in A(\mathbf{Q})$, as the sign in the functional equation satisfied by $L(A/\mathbf{Q},s)$ is -1.)

`Step III.` As explained in the proof of Proposition 5.3 (see in particular the discussion following equation (13)), the residual representation $\overline{\rho}_{A,p}=\overline{\rho}_f$ is ramified at every prime $q|N$, hence $\overline{\rho}_{A^K,p}$ is also ramified at every prime $q|N$. Then the local Tamagawa number $c_q(A)=c_q(A^K)$ is a p-adic unit for every $q|N$, so that every local Tamagawa number of $A^K/\mathbf{Q}$ is a p-adic unit. (Indeed, if a prime $q\nmid N$ divides the conductor of $A^K/\mathbf{Q}$, then q divides the absolute discriminant of K, and $A^K/\mathbf{Q}$ has additive reduction at q and $c_q(A^K)\leq 4$). According to Theorem 2 of [**SU14**] (cf. Theorem 4.1) the p-part of the Birch and Swinnerton-Dyer formula holds for $A^K/\mathbf{Q}$:

$$\frac{L(A^K/\mathbf{Q},1)}{\Omega_{A^K}}\doteq\#Ш(A^K/\mathbf{Q})_{p^\infty}. \tag{30}$$

(Note that loc. cit. requires $\overline{\rho}_{A^K,p}$ to be surjective. On the other hand, as proved in [**Ski14**, Theorem B], the irreducibility of $\overline{\rho}_{A^K,p}$ is sufficient for the arguments of [**SU14**].)

`Step IV.` According to Theorem 5.1

$$[A(K):\mathbf{Z}P_K]^2\doteq\#Ш(A/K)_{p^\infty}\doteq\#Ш(A/\mathbf{Q})_{p^\infty}\cdot\#Ш(A^K/\mathbf{Q})_{p^\infty}.$$

Since $c_A:=\prod_{q|N}c_q(A)$ is a p-adic unit, combining the preceding equation with (29) and (30) yields

$$\frac{L'(A/\mathbf{Q},1)}{\Omega_A\cdot h^{\mathrm{NT}}(\mathbf{P})}\doteq\#Ш(A/\mathbf{Q})_{p^\infty}\cdot c_A,$$

concluding the proof of Theorem A.

References

[BD96] M. Bertolini and H. Darmon, *Heegner points on Mumford–Tate curves*, Invent. Math. **126** (1996), no. 3.
[BD05] ———, *Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions*, Annals of Mathematics **162** (2005).
[BD07] ———, *Hida families and rational points on elliptic curves*, Invent. Math. **168** (2007), no. 2.
[Ber14] A. Berti, *On the Birch and Swinnerton-Dyer conjecture for elliptic curves of analytic rank one*, Ph.D. Thesis, University of Milan (2014).
[BFH90] D. Bump, S. Friedberg, and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), no. 3.
[BV15] M. Bertolini and R. Venerucci, *The anticyclotomic Iwasawa main conjectures*, Preprint (2015).
[Car94] H. Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet*, P-adic monodromy and the Birch and Swinnerton-Dyer conjecture (B Mazur and G. Stevens, eds.), American Mathematical Society, 1994.
[GP12] B. Gross and J. Parson, *On the local divisibility of Heegner points*, Number theory, analysis and geometry, Springer, New York (2012).
[Gre97] R. Greenberg, *Iwasawa theory for elliptic curves*, Springer-Verlag New York, Inc., 1997.
[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **86** (1986), no. 2.
[Kat04] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004).
[Kol90] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., 87, Birkhäuser Boston, Boston, MA, 1990.
[Kol91] ———, *On the structure of Selmer groups*, Math. Ann. **291** (1991), no. 2.
[Maz78] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), no. 2, with an appendix by D. Goldfeld.
[Mil04] J.S. Milne, *Arithmetic duality theorems*, Kea Books, 2004.
[PW11] R. Pollack and T. Weston, *On anticyclotomic μ-invariants of modular forms*, Compositio Math. **147** (2011), no. 5.
[Rib90] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2.
[Rub00] K. Rubin, *Euler systems (Hermann Weyl Lectures)*, Annals of Mathematics Studies, vol. 147, Princeton University Press, 2000.
[Ski14] C. Skinner, *Multiplicative reduction and the cyclotomic main conjecture for* GL_2, Preprint (2014).
[SU14] C. Skinner and E. Urban, *The Iwasawa main conjecture for* GL_2, Invent. Math. **195** (2014), no. 1.
[Vat03] V. Vatsal, *Special values of anticyclotomic L-functions*, Duke Math. J. **116** (2003), no. 2.
[Wan14] X. Wan, *Iwasawa main conjecture for supersingular elliptic curves*, Preprint, arXiv:1411.6352 (2014).
[Zha01] S. Zhang, *Heights of Heegner points on Shimura curves*, Ann. Math. **153** (2001), no. 1.
[Zha14] W. Zhang, *Selmer groups and the indivisibility of Heegner points.*, Cambridge J. Math. **2** (2014), no. 2.