ON THE p-ADIC BIRCH AND SWINNERTON-DYER CONJECTURE FOR ELLIPTIC CURVES OVER NUMBER FIELDS

by

Daniel Disegni

Abstract. — We formulate a multi-variable p-adic Birch and Swinnerton-Dyer conjecture for p-ordinary elliptic curves A over number fields K. It generalises the one-variable conjecture of Mazur–Tate–Teitelbaum, who studied the case $K = \mathbf{Q}$ and the phenomenon of exceptional zeros. We discuss old and new theoretical evidence towards our conjecture and in particular we fully prove it, under mild conditions, in the following situation: K is imaginary quadratic, $A = E_K$ is the base-change to K of an elliptic curve over the rationals, and the rank of A is either 0 or 1.

The proof is naturally divided into a few cases. Some of them are deduced from the purely cyclotomic case of elliptic curves over $\mathbf{Q}$, which we obtain from a refinement of recent work of Venerucci alongside the results of Greenberg–Stevens, Perrin-Riou, and the author. The only genuinely multi-variable case (rank one, two exceptional zeros, three partial derivatives) is newly established here. Its proof generalises to show that the 'almost-anticyclotomic' case of our conjecture is a consequence of conjectures of Bertolini–Darmon on families of Heegner points, and of (partly conjectural) p-adic Gross–Zagier and Waldspurger formulas in families.

Contents

1. Introduction

Let $A/\mathbf{Q}$ be an elliptic curve, p be a prime. Mazur–Tate–Teitelbaum [29] observed long ago that if A has split multiplicative reduction at p, the p-adic L-function $L_p(A)$ of A vanishes at its central argument even when the complex L-function $L(A,s)$ does not (due to the vanishing of the interpolation factor relating their two values). They went on to conjecture that $L_p(A)$ has order of vanishing equal to exactly one more than that of $L(A,s)$, and to give a precise conjectural formula for its leading term.

The purpose of this work is to formulate a generalisation of their conjecture valid for elliptic curves over number fields, and to provide evidence in its favour. A salient feature of this generalisation is the presence of several variables.

Evidence and motivation for a conjecture are two sides of the same mathematical coin, with the expository difference that the latter is presented before rather than after. Readers eager to look at the side of motivation may prefer to start by looking at the various formulas at the end of §5.2.

1.1. The conjecture. — Fix a rational prime p and assume throughout this paper that A/K is an elliptic curve with ordinary (good or multiplicative) reduction at all primes $\mathfrak{p}|p$ of K. The first point of difference to [29] is that in general the existence of a p-adic L-function for A is far from being known. It will therefore be a preliminary hypotheses; we formulate it after introducing some notation.

p-adic L-function. — Let Γ be a $\mathbf{Z}_p$-free quotient of the Galois group of the maximal abelian extension of K. Via the reciprocity law of class field theory, it is equipped with a surjective homomorphism

$$\ell : K^\times \backslash K_{\mathbf{A}^\infty}^\times \to \Gamma. \tag{1.1.1}$$

Fix a finite extension L of $\mathbf{Q}_p$ containing, for all primes $\mathfrak{p}|p$ of good reduction, a splitting field for the polynomial $P_\mathfrak{p}(X) = X^2 - a_\mathfrak{p} X + \mathrm{N}(\mathfrak{p})$, where $a_\mathfrak{p} = \mathrm{N}(\mathfrak{p}) + 1 - |A(k_\mathfrak{p})|$ (here $k_\mathfrak{p}$ is the residue field, $N(\mathfrak{p}) = |k_\mathfrak{p}|$). We let $\alpha_\mathfrak{p} \in L$ be the unique root of $P_\mathfrak{p}(X)$ which is a unit in $\mathscr{O}_L$ if $\mathfrak{p}$ is a prime of good reduction, and $\alpha_\mathfrak{p} = +1$ (respectively, $\alpha_\mathfrak{p} = -1$) if $\mathfrak{p}$ is a prime of split (respectively, non-split) multiplicative reduction. Finally, we let $\mathbf{Q}(\alpha) := \mathbf{Q}((\alpha_\mathfrak{p})_{\mathfrak{p}|p}) \subset L$.

The (hypothetic) p-adic L-function $L_p^{(\Gamma)}(A)$ will be an element of $\mathscr{O}_L[\![\Gamma]\!] \otimes L$, which we also view as the ring $\mathscr{O}(\mathscr{Y}_\Gamma)^\mathrm{b}$ of bounded regular functions on the Cartier dual of Γ over L: this is a rigid space $\mathscr{Y}_\Gamma/L$ whose R-valued points, for any affinoid L-algebra R, parametrise continuous characters $\chi : \Gamma \to R^\times$; accordingly, we will write $L_p^{(\Gamma)}(A,\chi) = \chi(L_p^{(\Gamma)}(A)) \in L(\chi)$ for a character $\chi \in \mathscr{Y}_\Gamma(L(\chi))$.

***Hypothesis* (L_p). —** *The complex L-function of A and its twists $L(A,\chi,s)$ by finite characters of Γ have analytic continuation to the entire complex plane, and there exists an element*

$$L_p^{(\Gamma)}(A) \in \mathscr{O}_L[\![\Gamma]\!] \otimes L$$

satsifying the following property: for each finite extension $\mathbf{Q}(\alpha,\chi)$ of $\mathbf{Q}(\alpha)$, each finite order character $\chi : \Gamma \to \mathbf{Q}(\alpha,\chi)^\times$, and each pair (ι_∞, ι_p) of an embedding $\iota_\infty : \mathbf{Q}(\alpha,\chi) \hookrightarrow \mathbf{C}$ and a $\mathbf{Q}(\alpha)$-embedding $\iota_p : \mathbf{Q}(\alpha,\chi) \hookrightarrow \overline{L}$, we have

$$\iota_\infty \iota_p^{-1} L_p^{(\Gamma)}(A)(\chi) = \prod_{\mathfrak{p}|p} \iota_\infty e_\mathfrak{p}(\chi_\mathfrak{p}) \cdot \frac{L(A, \iota_\infty\chi, 1)}{|D_K|^{-1/2}\Omega_A} \qquad \text{in } \iota_\infty \mathbf{Q}(\alpha,\chi),$$

where Ω_A is the Néron period appearing in the Birch and Swinnerton-Dyer conjecture for A [47], D_K is the discriminant of K, and the local factors $e_\mathfrak{p}(\chi_\mathfrak{p})$ are given as follows:

$$e_\mathfrak{p}(\chi_\mathfrak{p}) = \begin{cases} (1 - \alpha_\mathfrak{p}^{-1}\chi(\mathfrak{p})^{-1})(1 - \alpha'_\mathfrak{p}\chi(\mathfrak{p})) & \text{if } \chi_\mathfrak{p} \text{ is unramified,} \\ \alpha_\mathfrak{p}^{-\mathfrak{f}_\mathfrak{p}} \tau(\chi_\mathfrak{p}) & \text{if } \chi_\mathfrak{p} \text{ is ramified of conductor } \mathfrak{f}_\mathfrak{p}. \end{cases}$$

Here $\alpha'_\mathfrak{p} := \alpha_\mathfrak{p}^{-1}$ if E has good reduction and $\alpha'_\mathfrak{p} := 0$ if E has multiplicative reduction, and $\tau(\chi_\mathfrak{p})$ is the Gauß sum

$$\tau(\chi_\mathfrak{p}, \psi_\mathfrak{p}) := \sum_{x \in \mathscr{O}_K/\mathfrak{p}^{\mathfrak{f}_\mathfrak{p}}} \chi_\mathfrak{p}(x)\psi_\mathfrak{p}(x),$$

for some choice[1] *of an additive character* $\psi_{\mathfrak{p}}$ *of* $K_{\mathfrak{p}}$ *of level* 0.

Note that the interpolation property determines $L_p^{(\Gamma)}(A)$ uniquely if it exists. When Γ is the Galois group Γ_K of the maximal $\mathbf{Z}_p$-extension of K (or when Γ is understood from context), it will be omitted from the notation.

Remark 1.1.1. — If A/K is a (p-ordinary) elliptic curve over a number field, a generalisation of the Shimura–Taniyama–Weil conjecture predicts the existence of a (p-ordinary, cohomological) automorphic representation π for $\mathbf{GL}_2/K$ such that $L(s,\pi) = L(A, s+1/2)$. The construction of p-adic L-functions as in Hypothesis 1.1 (with the period Ω_A replaced by an a priori different period Ω_π) attached to such ordinary representations π was recently obtained by Deppe [15] for all number fields.

Let $\mathscr{I}_\Gamma \subset \mathscr{O}_L[\![\Gamma]\!]_L$ be the augmentation ideal (which is also the ideal of functions on $\mathscr{Y}_\Gamma$ vanishing at the trivial character $\chi = \mathbf{1}$), and define the *order of vanishing* $\mathrm{ord}_{\chi=1} L_p^{(\Gamma)}(A)$ to be the largest integer $\tilde{r} \geq 0$ such that $L_p^{\Gamma}(A) \in \mathscr{I}_\Gamma^{\tilde{r}}$. Note that if $\Gamma \to \Gamma'$ is a quotient, then

$$\mathrm{ord}_{\chi=1} L_p^{(\Gamma)}(A) \leq \mathrm{ord}_{\chi=1} L_p^{(\Gamma')}(A). \tag{1.1.2}$$

For any $\tilde{r} \geq \mathrm{ord}_{\chi=1} L_p(A)$, we define

$$\mathrm{d}^{\tilde{r}} L_p(A, \mathbf{1}) \quad \in \mathrm{Sym}^{\tilde{r}} \Gamma \otimes L,$$

as the image of $L_p(A)$ in $\mathscr{I}_\Gamma^{\tilde{r}}/\mathscr{I}_\Gamma^{\tilde{r}+1} \cong \mathrm{Sym}^{\tilde{r}}\Gamma \otimes L$, the last isomorphism being given by $\prod_{i=1}^{\tilde{r}}(\gamma_i - 1) \mapsto [\gamma_1 \otimes \cdots \otimes \gamma_{\tilde{r}}]$. When $\tilde{r} = \mathrm{ord}_{\chi=1} L_p(A)$, it can be thought of as the Γ-leading term of $L_p(A)$ at $\chi = \mathbf{1}$.[2]

Arithmetic side: the extended Mordell–Weil and Selmer groups. — The Birch and Swinnerton-Dyer conjecture relates $\mathrm{ord}_{s=1} L(A,s)$ to the rank

$$r := \mathrm{rk}\, A(K).$$

For our modified case, let $S_p^{\mathrm{exc}} = S_p^{\mathrm{exc}}(A)$ be the set of places above p over which A has split multiplicative reduction, and let $r^{\mathrm{exc}} = |S_p^{\mathrm{exc}}|$. We conjecture that, if Hypothesis (L_p) is satisfied for (A,Γ) and if the natural surjection $\Gamma_K \to \Gamma_{\mathbf{Q}}$ factors through Γ,[3]

$$\mathrm{ord}_{\chi=1} L_p^{(\Gamma)}(A) = \tilde{r} := r + r^{\mathrm{exc}}. \tag{1.1.3}$$

The integer $\tilde{r}$ is interpreted as the rank of the *extended Mordell–Weil group* $A^\dagger(K)$. In order to define it, recall first that Tate proved that if A'/F is an elliptic curve with split multiplicative reduction over a non-archimedean local field F, there is a rigid analytic isomorphism $\mathbf{G}_{m,F}^{\mathrm{an}}/q^{\mathbf{Z}} \to A'^{\mathrm{an}}$ for some $q \in F^\times$ (called the *Tate period* of A'/F and chosen to satisfy $\mathrm{ord}_{\mathfrak{p}}(q) > 0$). Then, letting $q_{A,\mathfrak{p}}$ be the Tate period of $A/K_{\mathfrak{p}}$ for $\mathfrak{p} \in S_p^{\mathrm{exc}}$,

$$A^\dagger(K) := A(K) \oplus \bigoplus_{\mathfrak{p} \in S_p^{\mathrm{exc}}} \mathbf{Z}\, q_{A,\mathfrak{p}},$$

and $\tilde{r} = \mathrm{rk}\, A^\dagger(K)$.

---

[1] The function $L_p^{(\Gamma)}(A) = L_p^{(\Gamma)}(A, \psi_p)$ then has a mild dependence on the choice of $\psi_p = (\psi_{\mathfrak{p}})_{\mathfrak{p}|p}$: if $a \in \mathscr{O}_{K,p}^\times$ and $a.\psi_p = (a_{\mathfrak{p}}.\psi_{\mathfrak{p}})$ with $a_{\mathfrak{p}}.\psi_{\mathfrak{p}}(x) := \psi_{\mathfrak{p}}(ax)$, then $L_p^{(\Gamma)}(A, a.\psi_p)(\chi) = \chi_p(a) L_p^{(\Gamma)}(A,\psi_p)(\chi)$. For a careful discussion of this point and formalisation of the 'space of additive characters of level 0', see [17, Theorem A]. In this paper we will be interested in the leading term at $\chi = \mathbf{1}$, which is independent of choices.

[2] We should remark, to clear any possible confusion which might be generated by our notation, that $\mathrm{d}^{\tilde{r}} L_p(A, \mathbf{1})$ is the analogue of the usual Taylor coefficient $\frac{1}{\tilde{r}!} L^{(\tilde{r})}(A,1)$ (and *not* of the r^{th} derivative $L^{(\tilde{r})}(A,1)$).

[3] If this last condition is not satisfied, there are examples in which the order of vanishing can be higher; in fact we may even have $L_p^{(\Gamma)}(A) = 0$ identically, see Proposition 2.2.3 below.

The work of Nekovář (see [33, §7.14], [34, §9.6.7]) introduces an extended Selmer group $\widetilde{H}^1_f(K, V_pA)$,[4], a $\mathbf{Q}_p$-vector space containing $A^\dagger(K)\otimes\mathbf{Q}_p$ and explicitly described as

$$\widetilde{H}^1_f(K, V_pA) \cong H^1_f(K, V_pA) \oplus \bigoplus_{\mathfrak{p}\in S_p^{\mathrm{exc}}} \mathbf{Q}_p q_{A,\mathfrak{p}}, \tag{1.1.4}$$

where $H^1_f(K, V_pA)$ is the (Bloch–Kato) Selmer group of A. We have $A^\dagger(K)_{\mathbf{Q}_p} = \widetilde{H}^1_f(K, V_pA)$, provided that $Ш(A)[p^\infty]$ is finite. Our conjectures will implicitly assume this to be the case, in the sense that they would likely need to be modified if $Ш(A)[p^\infty]$ were to be infinite.[5]

Arithmetic side: the regulator. — We now turn to describing the various arithmetic ingredients which will combine into the conjectural value of the leading term. For the complex L-function, the leading term is conjecturally given by the product of a rational number and of the Néron–Tate regulator on $A(\mathbf{Q})$. In our case, the Néron–Tate height pairing

$$h_{\mathrm{NT}}\colon A(K)\times A(K)\to \mathbf{R}, \tag{1.1.5}$$

whose *discriminant* (see Definition 2.1.2 below: it also accounts for $|A(K)_{\mathrm{tors}}|^2$) on $A(K)$ is denoted by $R_{\mathrm{NT}}(A)$, is replaced by the extended height pairing

$$\widetilde{h}_\ell\colon \widetilde{H}^1_f(K, V_pA)\times\widetilde{H}^1_f(K, V_pA)\to \Gamma\otimes L; \tag{1.1.6}$$

defined by Nekovář (*locc. citt.*). (More precisely, Nekovář defines a pairing $\widetilde{h}$ with values in $K^\times\backslash K^\times_{\mathbf{A}^\infty}\hat{\otimes}L = \Gamma_K\hat{\otimes}L$. The pairing $\widetilde{h}_\ell$ is its image under (1.1.1).) The regulator term

$$\widetilde{R}_\ell(A)\in \mathrm{Sym}^{\widetilde{r}}\Gamma\otimes L$$

is defined as the discriminant of (1.1.6) on $A^\dagger(K)$. A concrete description of the height pairing (1.1.6) will be given in §2.1. For now we will just say that (a) it extends the "canonical" height pairing

$$h_\ell = h_\ell^{\mathrm{can}}\colon A(K)\times A(K)\to\Gamma\otimes L \tag{1.1.7}$$

also defined in [33, §7.14]; (b) in the case $K=\mathbf{Q}$ considered in [29], our regulator $\widetilde{R}_\ell(A)$ differs from the regulator of [29] by a factor $\mathrm{ord}_p(q_{A,p})$ if $S_p^{\mathrm{exc}}=\{p\}$ (whereas the two coincide if $S_p^{\mathrm{exc}}=\emptyset$).

The conjecture. — We first recall the classical Birch and Swinnerton-Dyer (BSD_∞) conjecture for elliptic curves over number fields. We present it as a "hypothesis", as we will prefer to formulate its p-adic analogue based on the hypothesis that the first two predictions of (BSD_∞) hold.

***Hypothesis* ($\mathbf{BSD}_\infty$).** — *Let A be an elliptic curve over a number field K.*

1. *The integer $r_{\mathrm{an}}(A) := \mathrm{ord}_{s=1}L(A,s)$ equals $r(A) := \mathrm{rk}A(K)$;*
2. *Letting $c_v(A)$ denote the local Tamagawa number of A at a prime v of K and $R_{\mathrm{NT}}(A)$ be the regulator of* (1.1.5) *on $A(K)$, the number*

$$|Ш(A)|_{\mathrm{an}} := \frac{L^{(r)}(A,1)}{r!|D_K|^{-1/2}R_{\mathrm{NT}}(A)\Omega_A\prod_v c_v(A)}$$

   belongs to $\mathbf{Q}^\times$.
3. *The Tate–Shafarevich group $Ш(A)$ is finite, and its order equals $|Ш(A)|_{\mathrm{an}}$.*

We may now state the p-adic Birch and Swinnerton–Dyer conjecture (BSD_p).

***Conjecture* ($\mathbf{BSD}_p$).** — *Let A be an elliptic curve over a number field K, p a rational prime such that A has ordinary reduction at all the primes $\mathfrak{p}|p$ of K. Let Γ be a $\mathbf{Z}_p$-free quotient of $\mathrm{Gal}(K^{\mathrm{ab}}/L)$. Suppose that Hypotheses (L_p) and (BSD_∞)–1-2 are satisfied and that $\mathrm{ord}_{s=1}L(A,s)=r$. Let S_p be the set of primes of K above p, $S_p^{\mathrm{exc}}\subset S_p$ its subset of primes of split multiplicative reduction for A, and let*

$$\widetilde{r} := r + |S_p^{\mathrm{exc}}|.$$

[4] In the case at hand this was also defined *ad hoc* in [29].

[5] Cf. the remark *On the rational part in the arithmetic side* in §1.3.

Let $\widetilde{e}_{\mathfrak{p}}(\mathbf{1}) := e_{\mathfrak{p}}(\mathbf{1})$ *if* $\mathfrak{p} \in S_p - S_p^{\mathrm{exc}}$, *and* $\widetilde{e}_{\mathfrak{p}}(\mathbf{1}) := \mathrm{ord}_{\mathfrak{p}}(q_{A,\mathfrak{p}})^{-1}$ *if* $\mathfrak{p} \in S_p^{\mathrm{exc}}$.

Then $L_p^{(\Gamma)}(A)$ *vanishes at* $\chi = \mathbf{1}$ *to order at least* $\widetilde{r}$, *we have*[6] $A^\dagger(K)_{\mathbf{Q}_p} \cong \widetilde{H}^1_f(K, V_pA)$ *and their dimension is* $\widetilde{r}$, *and*

$$\mathrm{d}^{\widetilde{r}} L_p^{(\Gamma)}(A, \mathbf{1}) = \prod_{\mathfrak{p}|p} \widetilde{e}_{\mathfrak{p}}(\mathbf{1}) \cdot \widetilde{R}_\ell(A) \cdot |Ш(A)|_{\mathrm{an}} \cdot \prod_v c_v(A) \quad \textit{in } \mathrm{Sym}^{\widetilde{r}}\Gamma \otimes L. \tag{1.1.8}$$

Remark 1.1.2. — The formulation chosen for Conjecture (BSD_p) is slightly spurious in that the term $|Ш(A)|_{\mathrm{an}}$ appearing in its right-hand side should ideally be replaced by its conjectural value $|Ш(A)|$ (let us refer to the resulting conjecture as (BSD_p°) for the purposes of this remark). The reason behind our choice is that in this paper we are mostly concerned with (i) the multivariable aspects, (ii) the comparison of the rational parts of the leading terms of $L(A,s)$ and $L_p(A)$; whereas we leave out the comparison between $|Ш(A)|$ and $|Ш(A)|_{\mathrm{an}}$. We should raise, however, two points. First, Conjecture (BSD_p°) would probably have the advantage of admitting a rephrasing, *up to* p*-units*, solely in terms of invariants of the Nekovář–Selmer complex underlying the extended Selmer group[7] (concretely, in terms of the discriminant of $\widetilde{h}$ on $\widetilde{H}^1_f(K, T_pA)$ and of the sizes of other cohomology groups $\widetilde{H}^i_f(K, T_pA)_{\mathrm{tors}}$, cf. [34, §0.16.2]). Secondly, results on $|Ш(A)|$ can in fact be obtained by comparing Conjecture (BSD_p) with (BSD_p°) and the latter with Iwasawa main conjectures, see e.g. [37].

Remark 1.1.3. — If the conjecture holds, the order of vanishing at $\mathbf{1}$ of $L_p^{(\Gamma)}(A)$ is $\widetilde{r}$ if and only if $\widetilde{R}_\ell(A) \neq 0$, i.e. if the extended height pairing (1.1.6) is non-degenerate. This is conjectured to hold under the assumptions stated before the conjectured equality (1.1.3) (which is thus recovered). It can fail in other cases, where one can go on to define *derived* p-adic heights: see [3, 21].

Remark 1.1.4. — The rank of Γ_K is $1 + s + \delta$, where s is the number of complex places of K and $\delta = \delta_{K,p}$ is the Leopoldt defect of K at p (conjectured, and known if K is abelian, to be 0). Therefore

$$\mathrm{rank}\,\mathrm{Sym}^{\widetilde{r}}\Gamma_K = \binom{s + \delta + \widetilde{r}}{\widetilde{r}}.$$

Remark 1.1.5. — It is easy to see that if the conjecture holds for Γ, then it holds for any quotient Γ' of Γ. One further important case of (BSD_p) was considered before, namely when $A = E_K$ is the base-change of an elliptic curve over $\mathbf{Q}$ to an imaginary quadratic field K and $\Gamma = \Gamma^-$ is the rank-1 quotient of Γ_K on which the complex conjugation $c \in \mathrm{Gal}(K/\mathbf{Q})$ acts by -1. This *anticyclotomic* single-variable conjecture was stated and studied by Bertolini–Darmon in a series of works beginning with [4].

1.2. Evidence. — The rest of this paper presents the evidence for Conjecture (BSD_p), whose compatibility with the conjecture of [29] is recalled in Proposition 3.1.1.

The results are of course concentrated in the cases where something is known for the classical conjecture (BSD_∞), namely when A is an elliptic curve over $\mathbf{Q}$ (or a totally real field F) or its base-change to an imaginary quadratic field (or a quadratic CM extension of F), and the archimedean analytic rank is at most 1. The cases of higher-degree totally real and CM fields are largely analogous to the cases of $\mathbf{Q}$ and imaginary quadratic fields, but the results there a little more fragmentary and a little less clean. We will therefore limit our discussion of them to various remarks (3.2.3, 3.2.4, 4.2.6) throughout the main body of the text.

Theorem A. — *Let* $E/\mathbf{Q}$ *be an elliptic curve of conductor* N *with ordinary reduction at the prime* p. *Suppose that* $r_{\mathrm{an}} := \mathrm{ord}_{s=1}L(E,s) \leq 1$ *and that*

(∗) *if* $r_{\mathrm{an}} = 1$ *and* $S_p^{\mathrm{exc}}(E) \neq \emptyset$, *then* $p \geq 5$ *and there exists another prime* $m \neq p$ *of multiplicative reduction for* E.

(6) This isomorphism is equivalent to the finiteness of the p-part $Ш(A)[p^\infty]$ of the Tate–Shafarevich group of A.

(7) This last formulation would not, even implicitly, depend on the finiteness of the Tate–Shafarevich group $Ш(A)$.

Then Hypotheses (L_p) *and* (BSD_∞)*-1-2 are satisfied, and Conjecture* (BSD_p) *holds.*

Theorem B. — *Let $E/\mathbf{Q}$ be an elliptic curve of conductor N with ordinary reduction at the prime p. Let K be an imaginary quadratic field of discriminant prime to Np and let $A = E_K$ be the base-change. Suppose that $r_{\mathrm{an}} := \mathrm{ord}_{s=1} L(A,s) \leq 1$ and that*

($*'$) *if $r_{\mathrm{an}} = 1$ and $S_p^{\mathrm{exc}}(A) \neq \emptyset$, then $p \geq 5$ and there exists another prime $m \neq p$ of multiplicative reduction for E, and moreover:*
   (a) if p is inert in K, then the prime m can be chosen to be also inert in K;
   (b) if p splits in K, then every $v|N$ splits in K.

Then Hypotheses (L_p) *and* (BSD_∞)*-1-2 are satisfied, and Conjecture* (BSD_p) *holds.*

A new exceptional zero height formula. — We highlight the main new case of Theorem B, thereby also exemplifying the type of formulas predicted by our conjecture. Let us introduce some notation. Given A, ℓ, $\mathfrak{p} \in S_p^{\mathrm{exc}}$ as above, the *$\mathscr{L}$-invariant* (as introduced in [29]) is

$$\mathscr{L}_{\mathfrak{p},\ell}(A) := \frac{\ell_{\mathfrak{p}}(q_{A,\mathfrak{p}})}{\mathrm{ord}_{\mathfrak{p}}(q_{A,\mathfrak{p}})} \in \Gamma \otimes \mathbf{Q}_p. \tag{1.2.1}$$

We place ourselves in the setup of Theorem B. The dihedral action of $\mathrm{Gal}(K/\mathbf{Q})$ induces an eigenspace decomposition $\Gamma_K = \Gamma^+ \times \Gamma^-$, with Γ^+ identified with $\Gamma_{\mathbf{Q}}$ via the adèlic norm and each of the factors free of rank 1 over $\mathbf{Z}_p$; we obtain a corresponding decomposition $\mathscr{Y} = \mathscr{Y}^+ \times \mathscr{Y}^-$. We denote by

$$(\mathrm{d}^-)^i(\mathrm{d}^+)^j : \mathscr{I}_{\Gamma_K}^{i+j} \to (\mathrm{Sym}^i \Gamma^- \otimes \mathrm{Sym}^j \Gamma^+) \otimes L$$

the projection, and by

$$\mathscr{L}_{\mathfrak{p}}^{\pm}(A) := \mathscr{L}_{\mathfrak{p},\ell^\pm}(A),$$

where $\ell^\pm : \Gamma \to \Gamma^\pm$ is the projection. Finally, there is another pairing h_ℓ^{norm} on $H^1_f(K, V_pA)$, which is defined by means of universal norms and whose relation with h^{can} will be recalled in (2.1.1) below: we let

$$R^{\mathrm{norm},+}(A)$$

be the discriminant of $h^{\mathrm{norm},+} = h_{\ell^+}^{\mathrm{norm}}$ on $A(K)$.

Theorem C. — *Let $E/\mathbf{Q}$ be an elliptic curve with conductor N and split multiplicative reduction at the prime $p \geq 5$. Let K be an imaginary quadratic field such that all primes dividing N split in K and let $A := E_K$; then $S_p^{\mathrm{exc}}(A) = S_p = \{\mathfrak{p}, \mathfrak{p}^*\}$. Suppose that $\mathrm{ord}_{s=1} L(A,s) = 1$. We have $\mathrm{d}^i L_p(A) = 0$ for all $i \leq 2$, and*

$$(\mathrm{d}^-)^2 \mathrm{d}^+ L_p(A, \mathbf{1}) = \mathscr{L}_{\mathfrak{p}}^-(A)\mathscr{L}_{\mathfrak{p}^*}^-(A) \cdot R^{\mathrm{norm},+}(A) \cdot |Ш(A)|_{\mathrm{an}} \prod_v c_v(A)$$

in $(\Gamma^-)^{\otimes 2} \otimes \Gamma^+ \otimes \mathbf{Q}_p$.

Outline of proofs. — The proof of Theorem A in §3 is reduced, according to the value of r_{an} and the reduction type of E at p, to various formulas of Perrin-Riou [37], Greenberg–Stevens [18], Venerucci [48], and the author [17]. The present work claims no originality for it (save perhaps for the precise determination of constants in Venerucci's formula for the case of $r = 1$ and split multiplicative reduction).

Theorem B is also separated into several cases, according as above to the value of r_{an}, the reduction type of E at p, *and* the behaviour of p in K. Moreover each case is broken down into several formulas according to the natural rank one quotients $\mathrm{Sym}^{\widetilde{r}} \Gamma_K \to \mathrm{Sym}^i \Gamma^+ \otimes \mathrm{Sym}^{\widetilde{r}-i} \Gamma^-$. (The results in each individual case sometimes hold under weaker assumptions than those of Theorem B.)

We single out two cases: the *purely cyclotomic case* of $i = \widetilde{r}$, which reduces to Theorem A for E and the twist $E^{(K)}$, and the *almost-anticylotomic case* of $i = 0$ or $i = 1$ (depending on the sign $\widetilde{\varepsilon}$ of the functional equation for $L_p(A)$). Our range of $\widetilde{r}$ is low enough that those two cases, together with some identities $0 = 0$ deduced from parity considerations, will suffice to cover Theorem B.

In §4, we first review the construction of $\mathscr{Y}^-$-families of Heegner points on A in the case of $\widetilde{\varepsilon}=-1$, as well as analogous functions on $\mathscr{Y}^-$ if $\widetilde{\varepsilon}=+1$ (*theta elements*). Then we (re)formulate conjectures of Bertolini–Darmon [4] on their leading terms at $\mathbf{1}\in\mathscr{Y}^-$, and describe the evidence: they are known under mild conditions if the rank of A is at most 1. Several cases are due to Bertolini–Darmon themselves [5–7]; we deduce one further case from a recent formula independently proven by Castella [12] and Molina Blanco [31]. Finally, we state (partly conjectural) explicit versions of the p-adic Gross–Zagier and Waldspurger formula in anticyclotomic families, based on recent works of Chida–Hsieh [13] and the author [17].

The key observation made in §5 is that, granted the anticyclotomic versions of the p-adic Gross–Zagier and Waldspurger formulas, the almost-anticyclotomic case of (BSD_p) for A is essentially equivalent to the Bertolini–Darmon conjecture for A. This allows to complete the proof of Theorem B, of which Theorem C is shown to be a special case.

1.3. Miscellaneous remarks. — We conclude this introduction with some comments on Conjecture (BSD_p).

Supersingular primes. — The presence of primes $\mathfrak{p}|p$ of good supersingular reduction could also be allowed; the associated variations, however, would be orthogonal to the situation of exceptional zeros, which is the most interesting phenomenon investigated in this paper. We therefore prefer to leave the extension to the interested reader, who may consult e.g. [2] for the case of elliptic curves over $\mathbf{Q}$, [40] for the most general case (but restricted to the cyclotomic variable), and [45] and references therein for alternative formulations.

Generalisations. — It is easy to imagine (and there is a fair amount of theoretical evidence showing) that the conjecture can be extended, with appropriate variations, to the case of abelian varieties, or to twisted cases, or to modular forms of higher weight. In fact, we regard it as a special case of a very general multi-variable conjecture on the leading terms of p-adic L-functions for deformations of (symplectic) motives, to which we hope to return in future work.

Invitation to numerical investigations. — In this paper, we have strived not for generality but for keeping the conjecture as concrete and elementary as possible: we hope this will encourage some of our readers to try and test it numerically in new cases.

Relation to Iwasawa main conjectures. — We expect the Birch and Swinnerton-Dyer conjecture for the extended Selmer group alluded to in Remark 1.1.2 to be a consequence of a suitable version of the Iwasawa main conjecture and the hypothetic non-degeneracy of $\widetilde{h}$, via the formulas of [34, §0.16.2]. In the situation of Theorem B, the relevant main conjecture is the two-variable main conjecture for $A=E_K$, which is proved in [43] when the root number of A is $+1$. It is also to be expected that Theorem C up to p-units should follow from the Birch and Swinnerton-Dyer conjecture in anticyclotomic family for A; in the complementary case of good reduction, this conjecture was recently proved by X. Wan [50]

On the work of Venerucci. — Theorem A, in the case of exceptional zeros and rank one, refines the recent result of Venerucci [48, Theorem D] on the original conjecture of [29]; a version of his result is also independently proved by Büyükboduk [10] under some assumptions. Venerucci also obtains a a two-variable exceptional zero formula [48, Theorem C], which can be regarded as an instance of the general multi-variable conjecture alluded to above, and which was for us a source of inspiration alongside the works of Bertolini–Darmon and Castella.

Exceptional p-adic heights formulas. — The formula of Theorem C stands alongside Venerucci's [48, Theorem D] (see also Proposition 3.2.5 below) as a second example of exceptional zero formulas for p-adic heights of points on rank one curves. Its proof only uses Heegner points through the author's formula of [17, Theorem C] (also valid over totally real fields) and the work of Castella [12] (for $\mathbf{Q}$, but in principle generalisable) and Molina Blanco [31] (also valid for totally real fields, with an a priori different notion of $\mathscr{L}$-invariants). Therefore a variant of Theorem C can also be proved for totally real fields.

On the other hand, the proof of [48, Theorem D] makes essential use of Beilinson–Kato classes, whose analogue in the case of totally real fields has yet to be constructed (cf. [35]).

1.4. Acknowledgements. — I would like to thank Lennart Gehrmann and Eric Urban for conversations, and Francesc Castella, Shinichi Kobayashi and Santiago Molina Blanco for correspondence on their respective works [12, 25, 31].

The author is supported by a public grant from the Fondation Mathématique Jacques Hadamard. This article was written while the author held a fellowship at the CRM, Montréal.

2. Foundations

We start this section with a brief review of the various p-adic height pairings we will need in this paper. Then we give some explicit versions of the Waldspurger, Gross–Zagier, and p-adic Gross–Zagier formulas. In the first two cases these are directly taken from recent works of Cai–Shu–Tian [11] and Chida–Hsieh [13] based on the general formulas of Waldspurger and Yuan–Zhang–Zhang [51]; in the latter p-adic case we apply the results of [11, 13] to deduce them from [17].

2.1. p-adic height pairings. — Let A/K be an elliptic curve over a number field, with ordinary reduction at all $\mathfrak{p} \in S_p$. We will consider three height pairings associated to a "p-adic logarithm" ℓ as in (1.1.1). (The material of this subsection is entirely taken from [29] and [33], to which we refer for more details; our notation and conventions are fixed as in [33, especially §7].) They are analogous to the classical Néron–Tate height pairing

$$h_{\mathrm{NT}} \colon A(K) \times A(K) \to \mathbf{R}$$

(which, for an elliptic curve over K, we always take to be normalised over K). The first p-adic pairing is the "canonical" height pairing $h_\ell = h_\ell^{\mathrm{can}}$ on the Bloch–Kato Selmer group $H^1_f(K, V_pA)$, valued in $\Gamma \otimes L$ where Γ and L are introduced before Hypothesis (L_p) in §1.1. We will not recall its definition. The second one is the extended pairing $\widetilde{h}_\ell$ of (1.1.6) on $\widetilde{H}^1_f(K, V_pA) \cong H^1_f(K, V_pA) \oplus \bigoplus_{\mathfrak{p} \in S_p^{\mathrm{exc}}} \mathbf{Q}_p q_{A,\mathfrak{p}}$. It extends h_ℓ, and a concrete description is given in [33, §7.14]; let us recall it. For $\mathfrak{p} \in S_p^{\mathrm{exc}}$, let

$$\log_{A,\mathfrak{p},\ell} \colon A(K_\mathfrak{p}) \otimes \mathbf{Q}_p \cong H^1_f(K_\mathfrak{p}, V_pA) \to \Gamma \otimes \mathbf{Q}_p$$

be the map induced from $\ell_\mathfrak{p}|_{\mathscr{O}^\times_{K,\mathfrak{p}}}$ via $\mathscr{O}^\times_{K,\mathfrak{p}} \hat{\otimes} \mathbf{Q}_p \cong K^\times_\mathfrak{p} / q^{\mathbf{Z}}_{A,\mathfrak{p}} \hat{\otimes} \mathbf{Q}_p \cong A(K_\mathfrak{p}) \otimes \mathbf{Q}_p$. Then $\widetilde{h}_\ell$ is the symmetric bilinear pairing on $\widetilde{H}^1_f(K, V_pA) \cong H^1_f(K, V_pA) \oplus \bigoplus_{\mathfrak{p} \in S_p^{\mathrm{exc}}} \mathbf{Q}_p q_{A,\mathfrak{p}}$ given by

$$\begin{aligned}
\widetilde{h}_\ell(x, y) &= h_\ell(x, y) \\
\widetilde{h}_\ell(x, q_{A,\mathfrak{p}}) &= \log_{A,\mathfrak{p},\ell}(x) \\
\widetilde{h}_\ell(q_{A,\mathfrak{p}}, q_{A,\mathfrak{p}'}) &= \begin{cases} \ell(q_{A,\mathfrak{p}}) & \text{if } \mathfrak{p} = \mathfrak{p}' \\ 0 & \text{otherwise} \end{cases}
\end{aligned}$$

for all $x, y \in H^1_f(K, V_pA)$.

Lemma 2.1.1. — *Suppose that K/K_0 is a finite Galois extension and that $A = E_K$ for an elliptic curve E/K_0. Then the pairing*

$$\widetilde{h} \colon \widetilde{H}^1_f(K, V_pA) \otimes \widetilde{H}^1_f(K, V_pA) \to \Gamma_K \otimes L$$

is equivariant for the natural $\mathrm{Gal}(K/K_0)$*-action on all the terms.*

Proof. — This is a special case of a result which holds in general for an induced representation $V = \mathrm{Ind}_{K_0}^K V_0$, and which immediately follows, for example, from the cohomological construction of $\widetilde{h}$ summarised in [34, §0.16.0]. □

Finally, the third height pairing, the norm-adapted h_ℓ^{norm} (following Schneider [42]), is again defined on $H^1_f(K, V_pA)$; it is related to h_ℓ by

$$h_\ell^{\mathrm{norm}}(x,y) = h_\ell(x,y) - \sum_{\mathfrak{p}\in S_p^{\mathrm{exc}}} \frac{\log_{A,\mathfrak{p},\ell}(x)\log_{A,\mathfrak{p},\ell}(y)}{\ell(q_{A,\mathfrak{p}})}, \tag{2.1.1}$$

where each $\ell(q_{A,\mathfrak{p}}) \neq 0$ by [1], and for $\alpha_1, \alpha_2, \alpha_3 \in K_\mathfrak{p}^\times$ with $\ell(\alpha_3) \neq 0$, the ratio $\ell(\alpha_1)\ell(\alpha_2)/\ell(\alpha_3) \in \Gamma \otimes \mathbf{Q}$ is defined as follows. Let $\varpi \in K_\mathfrak{p}^\times$ be an element of valuation $n > 0$ in the kernel of ℓ; then we may uniquely write $\alpha_i^n = \varpi^{r_i} u_i \beta_i$ for some $r_i \in \mathbf{Z}$, roots of unity $u_i \in \mathscr{O}_{K,\mathfrak{p}}^\times$, and $\beta_i \in 1 + \mathfrak{p}\mathscr{O}_{K,\mathfrak{p}}^\times$. We can further write $\beta_i = \exp(b_i)$ for $b_i \in \mathfrak{p}\mathscr{O}_{K,\mathfrak{p}}$, and then define

$$\frac{\ell(\alpha_1)\ell(\alpha_2)}{\ell(\alpha_3)} := \frac{1}{np^m}\ell(\exp(p^m b_1 b_2/b_3)) \quad \text{in } \Gamma\otimes\mathbf{Q}$$

for any sufficiently large $m \in \mathbf{N}$.

Definition 2.1.2. — Let M be a finitely generated $\mathbf{Z}$-module, L a field of characteristic zero, Γ a finite-dimensional L-vector space, $h : M_L \otimes M_L \to \Gamma$ a symmetric L-bilinear form. The *regulator* of h on M is the discriminant

$$R(M,h) := [M : \sum_{i=1}^r \mathbf{Z}x_i]^{-2} \cdot \det h(x_i, x_j) \quad \in \mathrm{Sym}^r\Gamma,$$

where $r := \dim_L M_L$, the $x_i \in M$ are any r elements forming a basis of M_L, and the determinant of an $r \times r$ matrix with entries in Γ is computed via the usual alternating sum of products along generalised diagonals.

2.2. Gross–Zagier and Waldspurger formulas. — We give explicit versions of the Waldspurger, Gross–Zagier, and p-adic Gross–Zagier formulas.

Shimura curves and Shimura sets. — If N^- is a squarefree integer, we denote by B_{N^-} the quaternion algebra over $\mathbf{Q}$ of discriminant N^-; it is definite (resp. indefinite) if and only if N^- is the product of an odd (resp. even) number of primes. If $R \subset B$ is an Eichler order, we denote by $X^{N^-}(R)$ the Shimura set (resp. Shimura curve) of level R. Explicitly, in the definite case

$$X^{N^-}(R) := B^\times \backslash \widehat{B}^\times / \widehat{R}^\times.$$

In the indefinite case, X is a projective algebraic curve over $\mathbf{Q}$ such that

$$X(\mathbf{C}) = B^\times \backslash \mathfrak{H}^\pm \times \widehat{B}^\times / \widehat{R}^\times \cup \{\text{cusps}\},$$

where $\mathfrak{H}^\pm = \mathbf{C} - \mathbf{R}$ and $\{\text{cusps}\}$ is a finite set, non-empty only if $N^- = 1$.

If N^+ is an integer prime to N^- and R is an Eichler order of level N^+ which is either understood from context or whose specification is unimportant, we write $X_0^{N^-}(N^+)$ for $X^{N^-}(R)$.

The setup. — Let $E/\mathbf{Q}$ be an elliptic curve of conductor N with ordinary reduction at the prime p. Let K be an imaginary quadratic field of discriminant D prime to N, and let η be the associated quadratic Dirichlet character and $u := |\mathscr{O}_K^\times|/2$. We factor $N = N^+N^-$ where N^+ (respectively, N^-) is a product of primes which are split (respectively, inert) in K, and we assume that N^- *is squarefree*. We let

$$\varepsilon := -\eta(N).$$

Let $B = B_{N^-}$, fix an embedding $K \subset B$ and pick an Eichler order $R \subset B$ of level N^+ such that $R \cap K = \mathscr{O}_K$. Let $X := X^{N^-}(R)$.

Let I_E be the ideal, in the spherical Hecke algebra $\mathbf{T}_{Np}$ for the level Np, generated by the $T_v - a_v(E)$ for all $v \nmid Np$. (Note that, by the Jacquet–Langlands correspondence, the algebra $\mathbf{T}_N$ also acts on level-N automorphic forms on any quaternion algebra.)

Finally, let ϕ be the normalised newform of level $\Gamma_0(N)$ associated with the isogeny class of E, and let $(\phi,\phi)_{\Gamma_0(N)}$ be the Petersson norm with respect to the hyperbolic volume $dxdy$ on $\Gamma_0(N)\backslash\mathfrak{H}$. We

denote the ratio of the Néron period of $A = E_K$ with this Petersson norm by

$$c_\infty(A) := \frac{\Omega_A}{8\pi^2(\phi,\phi)_{\Gamma_0(N)}} \in \mathbf{Q}^\times.$$

Note that this does not depend on the specific imaginary quadratic field K.

***Theorem 2.2.1* (Waldspurger formula).** — *Suppose that $\varepsilon = +1$ (equivalently, that the squarefree integer N^- is the product of an odd number of primes). For each $x \in X = B^\times\backslash\widehat{B}^\times/\widehat{R}^\times$ represented by $b_x \in \widehat{B}^\times$, let $w_x := |B^\times \backslash g_x\widehat{R}^\times g_x^{-1}/\{\pm 1\}|$ and define a pairing on $\mathbf{Z}[X]$ by*

$$\langle f_1, f_2\rangle = \sum w_x f_1(x) f_2(x). \tag{2.2.1}$$

Let $\delta(f) := \langle f, f\rangle$ be the associated quadratic form.

Let $f \in \mathbf{Z}[X][I_E]$ be an integer-valued function on X annihilated by the Hecke operators in I_E, and let

$$p(f) = u^{-1} \cdot \sum_{t \in \mathrm{Pic}(\mathscr{O}_K)} f(t).$$

Then we have

$$\frac{L(A,1)}{|D_K|^{-1/2}\Omega_A} = c_\infty(A)^{-1} \cdot \frac{p(f)^2}{\delta(f)}.$$

Proof. — This is a special case of [11, Theorem 1.2]. The proof is based on the original Waldspurger formula ([49] or [17, (1.4.1)]), which is a more general if less explicit statement: namely f is not necessarily a newform, and the right-hand side contains some extra local terms (toric integrals, denoted by β_v in [11] and, for comparisons, by α_v in [51], by $\mathscr{P}_v$ in [13], by Q_v in [17]). Then the deduction essentially amounts to (i) a computation of the local integrals and (ii) a formula relating the Asai L-value to $8\pi^2(\phi,\phi)_{\Gamma_0(N)} = c_\infty(A)^{-1}\Omega_A$. □

***Theorem 2.2.2* (Gross–Zagier formula).** — *Suppose that $\varepsilon = -1$ (equivalently, that the squarefree integer N^- is the product of an even number of primes). Let J be the Albanese variety of the Shimura curve X, and embed $X \hookrightarrow J$ by sending the Hodge class [51] to 0. Let $f : J \to E$ be a nontrivial morphism, and let*

$$\delta(f) = \deg(f) := f \circ f^\vee \in \mathrm{End}(E) = \mathbf{Z}.$$

Let H be the Hilbert class field of K and let $P \in X(H)$ be a CM point for K of conductor 1. Consider the Heegner point

$$P(f) = u^{-1} \cdot \sum_{t \in \mathrm{Pic}(\mathscr{O}_K)} f(P)^{\sigma_t} \in E(K)$$

where $t \mapsto \sigma_t$ is the reciprocity map of class field theory. Then

$$\frac{L'(A,1)}{|D_K|^{-1/2}\Omega_A} = c_\infty(A)^{-1} \cdot \frac{h_{\mathrm{NT}}(P(f),P(f))}{\delta(f)}.$$

Proof. — This is a special case of [11, Theorem 1.1], which is deduced from the more general formula of [51, Theorem 1.2] by the argument and calculations recalled in the proof of Theorem 2.2.1. □

Before stating the p-adic analogue, we recall the existence of p-adic L-functions.

Proposition 2.2.3. — *Let E be an elliptic curve over $\mathbf{Q}$ of conductor N, let $K = \mathbf{Q}$ or an imaginary quadratic field of discriminant prime to Np, and $\Gamma = \Gamma_K$. Let $A := E_K$ and let c be the generator of* $\mathrm{Gal}(K/\mathbf{Q})$. *Then (A,Γ) satisfies Hypothesis (L_p) from §1.1, and the p-adic L-function $L_p(A)$ satisfies a functional equation relating χ to χ^{-c}. If $K = \mathbf{Q}$ and E has conductor N, the sign of the functional equation of $L_p(A)$ is*

$$\widetilde{\varepsilon} := -\eta(N^{(p)}) \quad \in \{\pm 1\}, \tag{2.2.2}$$

where $N^{(p)}$ is the prime-to-p part of N and η is the quadratic Dirichlet character associated with K.

Proof. — This is a theorem of Amice–Vélu and Vishik (see [29, Chapter I]) for E, and of Perrin-Riou [38] for E_K (for p odd, in general see [17, Theorem A]; the proof of the functional equation in [38] applies to the case $p=2$ given the existence of $L_p(A)$). □

***Theorem 2.2.4* (p-adic Gross–Zagier formula). —** *Under the assumptions of Theorem 2.2.2, suppose moreover that p splits in K, and that E has ordinary (good or multiplicative) reduction at p. Then*

$$\mathrm{d}^+ L_p(A,\mathbf{1}) = \prod_{\mathfrak{p}\mid p} e_{\mathfrak{p}}(\mathbf{1})\cdot c_\infty(A)^{-1}\cdot \frac{h^+(P(f),P(f))}{\delta(f)}$$

in $\Gamma^+\otimes L$.

Note that when E has split multiplicative reduction, the identity is the trivial $0=0$.

Proof. — This is a special case of the analogous result to [11, Theorem 1.5], which can be obtained by applying word for word the arguments of *op. cit.* to [17, Theorem B] instead of [51, Theorem 1.2]. When E has good reduction and all $v|N$ split in K, this formula was proved by Perrin-Riou [37]. □

The "Heegner index". — Let E be an elliptic curve of conductor N. Let N^- be a squarefree divisor of N and let $f\in \mathbf{Z}[X_0^{N^-}(N^+)][I_E]$ (if B_{N^-} is definite) or $f: J=\mathrm{Alb}(X_0^{N^-}(N^+))\to E$ (if B_{N^-} is indefinite). Let K be an imaginary quadratic field, and define

$$I(E_K,f) := |Ш(E_K)|_{\mathrm{an}}\cdot c_\infty(E_K)\prod_{w\mid N} c_w(E_K)\cdot\delta(f), \tag{2.2.3}$$

where w runs over the primes of K. Under Hypothesis (BSD_∞)–2 for E_K, we have $I(E_K,f)\in\mathbf{Q}^\times$.

***Corollary 2.2.5.* —** *Let $E/\mathbf{Q}$ be an elliptic curve of conductor N, let K be an imaginary quadratic field, $A=E_K$, and assume that $r_{\mathrm{an}} := \mathrm{ord}_{s=1}L(A,s)\le 1$. Let N^- and f be as in either Theorem 2.2.1 (case $r_{\mathrm{an}}=0$) or Theorem 2.2.2 (case $r_{\mathrm{an}}=1$). Then there is a positive integer $i(A,f)$ such that*

$$i(A,f)^2 = I(A,f),$$

and explicitly

$$i(A,f) = \begin{cases} |A(K)|\cdot|p(f)| & \text{if } r_{\mathrm{an}}=0\\ [A(K):\mathbf{Z}P(f)] & \text{if } r_{\mathrm{an}}=1,\end{cases}$$

where in both cases the right-hand is finite by the work of Kolyvagin [27].

Proof. — The result follows form the definitions and the Waldspurger and Gross–Zagier formulas (Theorems 2.2.1 and 2.2.2). □

3. Evidence over Q

In this section we prove Theorem A.

3.1. Preliminaries. — We first study some invariance properties of Conjecture (BSD_p).

We start by recording an alternative statement of our conjecture, closer to the original conjecture of Mazur–Tate–Teitelbaum [29] in its usual formulation. Recall the $\mathscr{L}$-invariant defined in (1.2.1), and let

$$L^*_{\mathrm{alg}}(A,1) := \frac{L^{(r)}(A,1)}{r!|D_K|^{-1/2}\Omega_A R_{\mathrm{NT}}(A)},$$

where $r=\mathrm{ord}_{s=1}L(A,s)$.

***Proposition 3.1.1.* —** *Let A/K be an elliptic curve with ordinary reduction at all the primes above p. Suppose (A,Γ) satisfies Hypotheses (L_p) and (BSD_∞)–1-2 from §1.1. Let $r=\mathrm{ord}_{s=1}L(A,s)$, $\widetilde{r} := r+|S_p^{\mathrm{exc}}|$. Then Conjecture (BSD_p) holds for (A,Γ) if and only if*

$$\mathrm{d}^{\widetilde{r}} L_p(A^{(\Gamma_{\mathbf{Q}})},\mathbf{1}) = \prod_{\mathfrak{p}\in S_p - S_p^{\mathrm{exc}}} e_{\mathfrak{p}}(\mathbf{1}) \prod_{\mathfrak{p}\in S_p^{\mathrm{exc}}} \mathscr{L}_{\mathfrak{p},\ell_\Gamma}(A)\cdot R^{\mathrm{norm}}_{\ell_\Gamma}(A)\cdot L^*_{\mathrm{alg}}(A,1)$$

in $\mathrm{Sym}^{\tilde{r}}\Gamma \otimes L$, *with* $\ell_\Gamma \colon K^\times \backslash K^\times_{\mathbf{A}^\infty} \to \Gamma_K \to \Gamma$.

The proof, by elementary linear algebra, is already given in [29, p. 35] in slightly different language.

Lemma 3.1.2. — *Suppose that $E/\mathbf{Q}$ has multiplicative reduction at p and let K be an imaginary quadratic field in which p is unramified. The twist $E^{(K)}$ has multiplicative reduction at p too, and the following are equivalent:*

1. *p splits in K (respectively, p is inert in K);*
2. *E and $E^{(K)}$ have the same reduction type at p, either both split or both non-split (respectively, E and $E^{(K)}$ have different reduction type at p);*
3. *the base-change E_K has zero or two (respectively, one) primes above p of split multiplicative reduction.*

If p splits in K, then more precisely $r^{\mathrm{exc}}(E_K) = 2$ (respectively, $r^{\mathrm{exc}}(E_K) = 0$) if E has split (respectively non-split) multiplicative reduction.

The proof is easy and left to the reader.

Proposition 3.1.3. — *Let E be an elliptic curve over a number field F and let Γ be a $\mathbf{Z}_p$-free quotient of Γ_F. Let "Conjecture X" be either of Hypotheses (L_p), (BSD_∞), or Conjecture (BSD_p).*

1. *If E' is isogenous to E, then Conjecture X holds for (E,Γ) if and only if it holds for (E',Γ).*
2. *Suppose that $F = \mathbf{Q}$ and let K be an imaginary quadratic field in which p is unramified, and $\Gamma = \Gamma_{\mathbf{Q}}$ (which we also view as a quotient of Γ_K); then Hypothesis (L_p) holds for E, the twist $E^{(K)}$, and the base-change E_K.*
   Hypothesis (BSD_∞)–1-2 holds for (E,Γ) and $(E^{(K)},\Gamma)$ if and only if it holds for (E_K,Γ). If this is the case, then:
   (a) if Conjecture (BSD_p) holds for (E,Γ) and $(E^{(K)},\Gamma)$, then it holds for (E_K,Γ).
   (b) if Conjecture (BSD_p) holds for (E_K,Γ) and $(E^{(K)},\Gamma)$ and the two sides of (1.1.8) for $(E^{(K)},\Gamma)$ are nonzero, then Conjecture (BSD_p) holds for (E,Γ).

Proof. — Part 1 is obvious for (L_p), and classical for (BSD_∞), see [47]. It is already observed in [29] that the proof can be adapted to the case of (BSD_p) by noting that, for any $\mathfrak{p} \in S_p^{\mathrm{exc}}(E) = S_p^{\mathrm{exc}}(E')$, the $\mathbf{Q}$-lines generated by $q_{E,\mathfrak{p}}$ and $q_{E',\mathfrak{p}}$ in $F_\mathfrak{p}^\times$ are the same, and the right-hand side of (1.1.8) for E only depends on $\mathbf{Q}q_{E,\mathfrak{p}}$ and not on $q_{E,\mathfrak{p}}$. (In the formulation of Proposition 3.1.1, this is simply the observation that $\mathscr{L}_\mathfrak{p}(E) = \mathscr{L}_\mathfrak{p}(E')$.)

The assertions on (L_p) in part 2 are contained in Proposition 2.2.3. The equivalence statement for (BSD_∞) is also classical. To adapt its proof to the case of (BSD_p), note that by Lemma 3.1.2, the sets $S_p^{\mathrm{exc}}(E_K)$ and $S_p^{\mathrm{exc}}(E) \coprod S_p^{\mathrm{exc}}(E^{(K)})$ are (non-canonically) in bijection, and if $\mathfrak{p} \in S_p^{\mathrm{exc}}(E_K)$ then $q_{E_K,\mathfrak{p}} = q_{E_0,p}$ for some $E_0 \in \{E, E^{(K)}\}$. □

3.2. Proof of Theorem A. — We prove Theorem A, whose statement we recall in the following slightly more general form.

Theorem 3.2.1. — *Let $E/\mathbf{Q}$ be an elliptic curve with ordinary reduction at the prime p. Suppose that $r := \mathrm{ord}_{s=1} L(E,s) \leq 1$. Then:*

1. *If the reduction of E at p is* not *split multiplicative or $r = 0$, then Conjecture (BSD_p) holds.*
2. *If $r = 1$ and the reduction of E at p is split multiplicative, suppose that $p \geq 5$. Then Conjecture (BSD_p) holds up to a nonzero rational number; if moreover there is at least another prime $m \neq p$ of multiplicative reduction for E, then Conjecture (BSD_p) holds exactly, that is*

$$\mathrm{d}^2 L_p(E,\mathbf{1}) = \mathscr{L}_p(E) \cdot R^{\mathrm{norm}}(E) \cdot L'_{\mathrm{alg}}(E,1)$$

in $\Gamma_{\mathbf{Q}}^{\otimes 2} \otimes \mathbf{Q}$.

Remark 3.2.2. — If $E/\mathbf{Q}$ has good supersingular reduction at p and $r = 1$, then the analogue of Conjecture (BSD_p) is proved by Kobayashi [26].

Proof in case 1. — If $r = 0$, then the result is trivial unless the reduction is split multiplicative; in that case, it is due to Greenberg–Stevens [18] if $p \geq 5$. A different proof, based on ideas of Kato–Kurihara–Tsuji (unpublished), is given by Kobayashi in [25] (see also [14]); as written there it applies directly to any $p \geq 3$, and it extends to cover the case of $p = 2$ after inserting the appropriate modifications of the theory of the Coleman map described in [26, §3] and [36].

Suppose that $r = 1$ and the reduction is not split multiplicative. By Lemma 3.1.3 we may in fact prove the formula for E_K, where we choose K to be an imaginary quadratic field in which all primes dividing N split, and such that $L(E^{(K)}, 1) \neq 0$. (The existence of such K is guaranteed by [32].) Let $A = E_K$, and use the '$\pm$' notation introduced before Theorem C. Then by Corollary 2.2.5 we may rewrite the p-adic Gross–Zagier formula of Theorem 2.2.4 as

$$\mathrm{d}^+ L_p(A, \mathbf{1}) = \prod_{\mathfrak{p}|p} e_{\mathfrak{p}}(\mathbf{1}) \cdot R^+(A) \cdot L^*_{\mathrm{alg}}(A, 1),$$

as desired.[8]

Remark 3.2.3. — If E/F is a modular elliptic curve over a totally real field, whose reduction at every $\mathfrak{p}|p$ is ordinary but not split multiplicative, and if we have $\mathrm{ord}_{s=1} L(E, s) \leq 1$, then by the same argument (comparing the main results of [17] and [51]), Conjecture (BSD_p) holds for E up to a conjecture on the commensurability of Ω_E with a certain automorphic period (this last point is discussed in [16, §9]).

Remark 3.2.4. — The result of Greenberg–Stevens is generalised to modular elliptic curves over totally real fields by Mok [30] and Spiess [44]. In particular this proves Conjecture (BSD_p) over totally real fields in the case of analytic rank 0, up to the conjecture on periods mentioned in the previous remark.

Proof in case 2. — The rest of this section is dedicated to the proof of Theorem 3.2.1 in the case in which E has split multiplicative reduction at $p \geq 5$ and $r := \mathrm{ord}_{s=1} L(E, s) = 1$. The result is proven by Venerucci [48] up to a rational constant. We remove the ambiguity assuming the condition that E has a prime $m \neq p$ of multiplicative reduction; we fix such an m. We will in fact prove Conjecture (BSD_p) for the base-change of E to a suitable auxiliary imaginary quadratic field K. More precisely, denoting by N the conductor of E, let K be an imaginary quadratic field of discriminant D such that (a) p and m are inert in K, (b) every prime divisor of N/pm splits in K, (c) $L(E^{(K)}, 1) \neq 0$, (d) $\mathscr{O}_K^\times = \{\pm 1\}$. (The existence of such K is again guaranteed by [32].) By Proposition 3.1.3 and the (trivial) validity of Conjecture (BSD_p) for $E^{(K)}$, the statements of Conjecture (BSD_p) for E and for E_K are equivalent.

We need some more notation. Let J be the Jacobian of the Shimura curve $X = X_0^{mp}(N/mp)$. Let I_E be the ideal in the spherical Hecke algebra generated by the operators $T_v - a_v(E)$ for $v \nmid N$, and let $f' \colon X' = X_0^m(N/m) \to \mathbf{Z}$ be a generator of the space of integer-valued functions annihilated by I_E.

***Proposition 3.2.5* (Venerucci).** — *With notation as above, suppose that E is an optimal quotient $f : J \to E$ of J, that is, that $f^\vee$ is injective.*[9] *Let $P(f) \in E(K)$ be the corresponding Heegner point.*

Then

$$(\mathrm{d}^+)^2 L_p(E_K, \mathbf{1}) = c_\infty(E_K)^{-1} \mathscr{L}^+_{p\mathscr{O}_K}(E_K) \frac{h^{\mathrm{norm},+}(P(f), P(f))}{\delta(f')} \cdot c_p(E),$$

where $h^{\mathrm{norm},+} = h^{\mathrm{norm}}_{\ell^+}$ (with the notation of Theorem C), and c_p is the Tamagawa number of E at p.

Proof. — This is [48, Theorem D], whose **P** is our $P(f)$, taking into account the value of the constant ℓ_3 of *loc. cit.*, which is explicitly given in terms of previously defined constants ℓ_2 and ℓ in [48, §6.5, §6.4, Remark 2.2]. Note that in fact $\ell_3 = 2\ell_2 \cdot \mathrm{ord}_p(q_{E,p})$ (there is a typo in [48]), and that by Tate's p-adic uniformisation, we have $c_p(E) = \mathrm{ord}_p(q_{E,p})$.

[8] This argument was of course already made by Perrin-Riou [37] when E has good reduction.

[9] Note that this can always be achieved up to replacing E by an isogenous curve.

We explain the different normalisations accounting for apparent discrepancies in the powers of 2 between [48] and our statement. As the composition $\Gamma_{\mathbf{Q}} \hookrightarrow \Gamma_K \xrightarrow{\ell^+} \Gamma^+ \cong \Gamma_{\mathbf{Q}}$ is multiplication by 2, we have $h^{\mathrm{norm},+}(P(f),P(f)) = 2h^{\mathrm{norm}}_{\ell_{\mathbf{Q}}}(P(f),P(f))$, where in the second expression we view $P(f) \in E(\mathbf{Q})_{\mathbf{Q}}$; similarly, $\mathscr{L}^+_{p\mathscr{O}_K}(E_K) = 2\mathscr{L}_p(E)$.[10] Secondly, our $(\mathrm{d}^+)^2$ equals 1/2 times the operator $\frac{d^2}{ds^2}$ of [48, Theorem D] (after fixing $\Gamma^+ \cong \Gamma_{\mathbf{Q}} \cong \mathbf{Z}_p$). Finally, the Petersson product on $\mathbf{GL}_2$ used in [48, Remark 2.2], is $(1/2)\cdot 8\pi^2$ times our Petersson product; and the quaternionic inner product of *loc. cit.* is 1/2 times our inner product. Indeed both of the normalisations in *loc. cit.* are inherited from [9]: see [9] for the first assertion, whereas it is easiest to see the second assertion by comparing the Waldspurger formulas of [9, Proposition 3.4] and Theorem 2.2.1. □

Comparing Proposition 3.2.5 with Corollary 2.2.5, Conjecture (BSD_p) for $(E_K,\Gamma_{\mathbf{Q}})$ is reduced to the following statement.

Proposition 3.2.6. — *With the notation of Proposition 3.2.5, we have*

$$\delta(f) = \frac{\delta(f')}{c_p(E)}.$$

For future reference, we remark that the result and its proof remain valid if m is replaced by any squarefree product N^- of an odd number of primes different from p.

Proof. — Let $\mathscr{X}_p(J)$ be the character group of the toric part of the reduction of J. The asserted result is proved by Takahashi [46, Corollary 2.6] (see also [41, §2]) with $\delta(f') = \langle f', f'\rangle$ replaced by $u_J(g,g)$, where g is a generator of the free rank 1 saturated $\mathbf{Z}$-submodule $\mathscr{X}_p(J)[I_E] \subset \mathscr{X}_p(J)$ annihilated by I_E, and $u_J\colon \mathscr{X}_p(J)\times\mathscr{X}_p(J) \to \mathbf{Z}$ is Grothendieck's monodromy pairing.

To complete the proof, we then need to compare $\langle f', f'\rangle$ and $u_J(g,g)$. In fact by the Cerednik–Drinfeld uniformisation, $\mathscr{X}_p(J)$ is a saturated submodule of $\mathbf{Z}[\mathscr{E}]$ where $\mathscr{E} = B^\times_{m\cdot\infty}\backslash\widehat{B}^\times_{m\cdot\infty}/\widehat{R}^\times$ is the set of edges in the dual graph of the reduction of the Shimura curve X at p, so that g may be identified with f' up to a sign. Moreover by the Picard–Lefschetz formula, the pairing u_J is the restriction of the pairing $\langle\,,\,\rangle$ on $\mathscr{E}$ of (2.2.1). We conclude that $u_J(g,g) = \langle f', f'\rangle = \delta(f)$ as desired. □

This completes the proof of Conjecture (BSD_p) for $(E_K,\Gamma_{\mathbf{Q}})$. By Proposition 3.1.3 and the trivial validity of (BSD_p) for $E^{(K)}$, we deduce (BSD_p) for E, completing the proof of Theorem 3.2.1.

4. Anticyclotomic theory

The following framework and notation will be adopted for the rest of the paper (unless otherwise noted). We let $E/\mathbf{Q}$ be an elliptic curve of conductor N with ordinary reduction at p, and K an imaginary quadratic field of discriminant D prime to Np. We factor $N = N^+N^-$ where N^+ (respectively N^-) is a product of primes which are split (respectively inert) in K, and we assume that N^- is squarefree. For $N^? = N, N^+, N^-$ we denote by $N^{?,(p)}$ the prime-to-p part of $N^?$. Recall also the sign $\widetilde{\varepsilon} := -\eta(N^{(p)})$ from (2.2.2).

For primes $v \nmid N$, we let $a_v := v+1-|E(\mathbf{F}_v)|$, and we let $\alpha \in \mathbf{Z}_p$ be the unit root of $X^2 - a_pX + p$ if $p \nmid N$, and $\alpha = +1$ (resp. $\alpha = -1$) if E has split (resp. nonsplit) multiplicative reduction at v. We denote by $I_E \subset \mathbf{T}^{Np}$ the ideal generated by $T_v - a_v(E)$ for $v \nmid Np$.

We will use the notation $\Gamma^\pm$, $\ell^\pm$, $\mathscr{L}^\pm_{\mathfrak{p}}(A)$, $R^\pm(A)$ introduced before the statement of Theorem C, as well as $\widetilde{R}^\pm(A) := \widetilde{R}_{\ell^\pm}(A)$. We also write $\Gamma = \Gamma_K$ and $\mathscr{Y} = \mathscr{Y}_\Gamma = \mathscr{Y}^+ \times \mathscr{Y}^-$ where the ring of bounded functions on $\mathscr{Y}^\pm$ is $\mathbf{Z}_p[\![\Gamma^\pm]\!]_{\mathbf{Q}_p}$.

[10] This factor of 2 can also be viewed as the interpolation factor for $L_p(E^{(K)})$.

4.1. Theta elements. — We recall the construction of *theta elements*, certain functions on $\mathscr{Y}^-$ interpolating toric periods (case $\widetilde{\varepsilon}=+1$) and Heegner points (case $\widetilde{\varepsilon}=-1$); the reader is referred to the original works of Bertolini–Darmon [4, §2] or [8, §4] for more details.

Let $B=B_{N^{-,(p)}}$ be the quaternion algebra of discriminant $N^{-,(p)}$. Let $R\subset R_0\subset B$ be Eichler orders of respective conductors $pN^{+,(p)}$ and $N^{+,(p)}$. We may choose an isomorphism $B_p\cong M_2(\mathbf{Q}_p)$ identifying $R^\times$ with the usual congruence subgroup $\Gamma_0(p)$, and identifying $R_0^\times$ with $\Gamma_0(1)$ (resp. $\Gamma_0(p)$) if $p\nmid N$ (resp. $p|N$). Let $X:=X^{N^{-,(p)}}(R)$, $X_0:=X^{N^{-,(p)}}(R_0)$ be the associated Shimura sets (case $\widetilde{e}=+1$) or Shimura curves (case $\widetilde{e}=+-1$). Fix an embedding $K\subset B$ such that $R\cap K=\mathscr{O}_K$.

For $n\geq 0$, let $\mathscr{O}_{K,n}:=\mathbf{Z}_p+p^n\mathscr{O}_K$ and let $G_n:=\mathrm{Pic}(\mathscr{O}_{K,n})$; let $G_\infty:=\varprojlim_n G_n$ (then Γ^- is the $\mathbf{Z}_p$-free quotient of G_∞). Let $H_n\subset K^{\mathrm{ab}}$ be the ring class field of K of conductor n, $H_\infty:=\bigcup_n H_n$. By class field theory, we have a canonical identification $G_n\cong\mathrm{Gal}(H_n/K)$ for all $n=0,1,\dots,\infty$.

For $n\geq 1$, let

$$g_n:=\left(\begin{smallmatrix}p^n & 1\\ & 1\end{smallmatrix}\right)\in\mathbf{GL}_2(\mathbf{Q}_p)=B_p^\times. \tag{4.1.1}$$

Case $\widetilde{\varepsilon}=+1$. — Let $z_0\in X$ be the image of $1\in K^\times\subset B^\times\subset\widehat{B}^\times$ and, recalling that $B_p^\times\subset\widehat{B}^\times$ acts on X, let $z_n:=z_0\cdot g_n\in X$. Let $f:X_0\to\mathbf{Z}$ be a nontrivial function annihilated by the Hecke operators in I_E. Denote still by $f:X\to X_0\xrightarrow{f}\mathbf{Z}$ the composition, and let $f^\dagger\in\mathbf{Z}_p[X]$ be $f^\dagger:=f$ if $p|N$, and $f^\dagger:=f-\alpha^{-1}\cdot\left(\begin{smallmatrix}1 & \\ & p\end{smallmatrix}\right)f$ if $p\nmid N$, where $\left(\begin{smallmatrix}1 & \\ & p\end{smallmatrix}\right)\in B_p^\times$ acts on $\mathbf{Z}[X]$ via its right action on X.

For $n\geq 0$, let

$$\Theta_n=\Theta_n(f):=u_n^{-1}\cdot\sum_{t\in G_n}\alpha^{-n}f^\dagger(tz_n)\otimes[t]\quad\in\mathbf{Z}_p[G_n],$$

where $u_0=u=|\mathscr{O}_K^\times|/2$ and $u_n=1$ if $n\geq 1$. The elements Θ_n satisfy the compatibility relation $\Theta_n\mapsto\Theta_{n-1}$ for all $n\geq 1$ under the natural quotient maps. Hence we may form their limit in $\mathbf{Z}_p[\![G_\infty]\!]$ and consider its projection to $\mathbf{Z}_p[\![\Gamma^-]\!]$:

$$\Theta=\Theta(f):=\varprojlim_n\Theta_n\in\mathbf{Z}_p[\![\Gamma^-]\!]\subset\mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}}.$$

(Note that taking the image of z_n under $\alpha^{-n}f^\dagger$ is the same as taking the image under f of the 'regularised' versions of z_n defined in [4, §2.5].)

***Remark 4.1.1.* —** The construction of Θ presented in [8, §4] depends on the choice of an 'admissible' (one or two choices have to be excluded) half-line $\{v_0g_n\}_n$ in the Bruhat–Tits tree $\mathscr{T}$ of $\mathbf{GL}_2(\mathbf{Q}_p)=B_p^\times$, originating from a vertex v_0 corresponding to z_0. Here we have made the specific choice $g_n=\left(\begin{smallmatrix}p^n & 1\\ & 1\end{smallmatrix}\right)$. It is explained in *loc. cit.* that the group $K_p^\times/\mathbf{Q}_p^\times$ acts transitively on the set of admissible half-lines, so that another choice – such as the one made in [13] – would yield the element $\Theta'=[t_p]\Theta$ for some $t_p\in K_p^\times/\mathbf{Q}_p^\times$ with image $[t_p]\in\Gamma^-$. It follows that the following are independent of the choice of half-line in $\mathscr{T}$: (i) the 'leading term' of $\Theta\in\mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}}$ at $\chi^-=1$ (and more generally its image in $\mathscr{I}^r_{\mathscr{Y}^-}/\mathscr{I}^{r+1}_{\mathscr{Y}^-}$, for any r such that $\Theta\in\mathscr{I}^r_{\mathscr{Y}^-}$); (ii) letting $*:\mathbf{Z}_p[\![\Gamma^-]\!]\to\mathbf{Z}_p[\![\Gamma^-]\!]$ be the involution induced by inversion on Γ^-, the element $\Theta\cdot\Theta^*$.

Case $\widetilde{\varepsilon}=-1$. — Let J (resp. J_0) denote the Albanese variety of X (resp. X_0). Let $f:J_0\to E$ be a nontrivial morphism and denote still by f the composition $J\to J_0\xrightarrow{f}E$. Let $f^\dagger\in\mathrm{Hom}(J,E)\otimes\mathbf{Z}_p$ be $f^\dagger:=f$ if $p|N$ and $f^\dagger:=f-\alpha^{-1}\cdot\left(\begin{smallmatrix}1 & \\ & p\end{smallmatrix}\right)f$, where $\left(\begin{smallmatrix}1 & \\ & p\end{smallmatrix}\right)\in B_p^\times$ acts on $\mathrm{Hom}(J,E)$ via its action on J.

Let $z_0\in X(H_0)$ be a CM point of conductor 1 and, recalling that $\mathbf{GL}_2(\mathbf{Q}_p)\cong B_p^\times\subset\widehat{B}^\times$ acts on X, let

$$z_n:=z_0\cdot g_n\in X(H_n),$$

a CM point of conductor p^n in X.

For $\chi:G_\infty\to\Lambda^\times$ a character valued in the units of some ring Λ, let $\Lambda(\chi)$ denote the Galois-module Λ with action by χ, and let

$$A(\chi):=(A(H_\infty)\otimes\Lambda(\chi))^{G_\infty}.$$

If G is any quotient of G_∞ and $\Lambda = \Lambda_G = \mathbf{Z}_p[\![G]\!]$, denote by $\chi_{\mathrm{univ},G}\colon \mathrm{Gal}(H_\infty/K) \to \Lambda_G^\times$ the universal character; when $G = G_n$ we set $\chi_{\mathrm{univ},n} = \chi_{\mathrm{univ},G}$; when $G = \Gamma^-$ we set $\chi^-_{\mathrm{univ}} := \chi_{\mathrm{univ},\Gamma^-}$

For $n \geq 0$, let

$$\mathscr{P}_n = \mathscr{P}_n(f) := u_n^{-1} \cdot \sum_{\sigma \in G_n} \alpha^{-n} f^\dagger(z_n^\sigma) \otimes [\sigma] \quad \in A(\chi_{\mathrm{univ},n}),$$

where again $u_0 = u = |\mathscr{O}_K^\times|/2$ and $u_n = 1$ if $n \geq 1$. The elements $\mathscr{P}_n$ satisfy the compatibility relation $\mathscr{P}_n \mapsto \mathscr{P}_{n-1}$ for all $n \geq 1$ under the natural quotient maps $A(\chi_{\mathrm{univ},n}) \to A(\chi_{\mathrm{univ},n-1})$. Hence we may form their limit in $A(\chi_{\mathrm{univ},G_\infty})$ and consider its projection to $A(\chi^-_{\mathrm{univ}})$:

$$\mathscr{P} = \mathscr{P}(f) := \lim_n \mathscr{P}_n \in A(\chi^-_{\mathrm{univ}}).$$

We still denote by $\mathscr{P}$ the image of $\mathscr{P}$ in the Selmer group $H^1_f(K, V_pA \otimes \mathbf{Z}_p[\![\Gamma^-]\!])$ (where $\mathbf{Z}_p[\![\Gamma^-]\!]$ is a G_K-module with action by χ^-_{univ}). As A is ordinary, for each $\mathfrak{p}|p$ there is a short exact sequence of $G_{K_\mathfrak{p}}$-modules

$$0 \to V_\mathfrak{p}^+ \to V_pA \to V_\mathfrak{p}^- \to 0,$$

where $V_\mathfrak{p}^\pm$ have rank one. Then by the work of Nekovář, there is a big extended Selmer group $\widetilde{H}^1_f(K, V_pA \otimes \mathbf{Z}_p[\![\Gamma^-]\!])$ sitting in an exact sequence [34, (6.1.32)]

$$0 \to \bigoplus_{\mathfrak{p}|p} H^0(K_\mathfrak{p}, V_\mathfrak{p}^- \otimes \mathbf{Z}_p[\![\Gamma^-]\!]) \to \widetilde{H}^1_f(K, V_pA \otimes \mathbf{Z}_p[\![\Gamma^-]\!]) \to H^1_f(K, V_pA \otimes \mathbf{Z}_p[\![\Gamma^-]\!])) \to 0. \tag{4.1.2}$$

The specialisation of $\widetilde{H}^1_f(K, V_pA \otimes \mathbf{Z}_p[\![\Gamma^-]\!])$ under the augmentation $\mathbf{Z}_p[\![\Gamma^-]\!] \to \mathbf{Z}_p$ is $\widetilde{H}^1_f(K, V_pA)$ (and in fact a similarly good behaviour holds under all specialisations at finite characters of Γ^-).

As χ^-_{univ} is infinitely ramified, each $H^0(K_\mathfrak{p}, V_\mathfrak{p}^- \otimes \mathbf{Z}_p[\![\Gamma^-]\!]) = 0$ and the map (4.1.2) is an isomorphism; hence we can identify $\mathscr{P}$ with a unique element still denoted

$$\mathscr{P} \in \widetilde{H}^1_f(K, V_pA \otimes \mathbf{Z}_p[\![\Gamma^-]\!]).$$

Remark 4.1.2. — A more explicit but equivalent construction of the lifting of $\mathscr{P}$ from $A(\chi^-_{\mathrm{univ}})$ to $\widetilde{H}^1_f(K, V_pA \otimes \mathbf{Z}_p[\![\Gamma^-]\!])$ (or rather, in the framework adopted there, to a certain extended big Mordell–Weil group) is given in [4, §2.6].

The observations of Remark 4.1.1 also apply to the present case.

4.2. Bertolini–Darmon conjectures. — We review (and slightly reformulate) conjectures of Bertolini and Darmon [4, 8] on the 'leading terms' of Θ and $\mathscr{P}$.

Pfaffian regulators. — Let M be a finitely generated $\mathbf{Z}$ module equipped with an involution c. Let L be a field of characteristic zero, Γ a finite-dimensional vector space over L, and $h\colon M_L \otimes M_L \to \Gamma$ a symmetric bilinear form satisfying

$$h(cx, cy) = -h(x, y) \tag{4.2.1}$$

for all $x, y \in M$. Denote by $M_L^\pm$ the $\pm$-eigenspaces for the action of c on M_L and, for $? = +, -, \emptyset$, let $r^? := \dim M_L^?$.

Suppose first that r is even. We define the *Pfaffian-regulator* of h on M to be

$$\mathrm{pf}(M, h) := [M : \sum \mathbf{Z}x_i]^{-1} \cdot \mathrm{pf}((h(x_i, cx_j))_{i,j=1}^r) \quad \in \mathrm{Sym}^{r/2}\Gamma$$

where $x_1, \ldots, x_r$ are elements of M forming a basis of M_L, and in the right-hand side 'pf' denotes the Pfaffian of an antisymmetric matrix. Note that $\mathrm{pf}(M)$ is well-defined only up to a sign, depending on the orientation of the chosen basis. Comparing with Definition 2.1.2, we find $\mathrm{pf}(M)^2 = \mathrm{sgn}(c)R(M)$, where $R(M, h)$ is the regulator of h on M and $\mathrm{sgn}(c)$ is the determinant of c on M_L. In fact h is degenerate unless $r^+ = r^-$; therefore in all cases

$$\mathrm{pf}(M, h)^2 = (-1)^{r/2} R(M, h). \tag{4.2.2}$$

If $r = \dim M_L$ is odd, then $R(M,h) = 0$. In this case we can define a 'higher' Pfaffian regulator $\mathrm{Pf}(M,h) \in M \otimes \mathrm{Sym}^{(r-1)/2}\Gamma$. Suppose first that there is a non-torsion element $x \in M$ in the radical of h whose image in M_L belongs to the larger of $M_L^{\pm}$. Then

$$\mathrm{Pf}(M,h) := x \otimes \mathrm{pf}(M/\mathbf{Z}x) \quad \in M_L \otimes \mathrm{Sym}^{(r-1)/2}\Gamma.$$

This is well-defined up to sign: it is apparent that the definition only depends on the line generated by x in M_L; if this is not unique, then $|r^+ - r^-| \geq 2$, which implies $R(M) = 0$, and $\mathrm{Pf}(M) = 0$ regardless of the choice of x in the definition.

In general, denote by $\overline{M}$ the image of M in M_L, and let $\gamma \in \mathbf{GL}(M_L)$ be an element such that $\gamma\overline{M} \subset M_L$ contains an element x' in the radical of h; let $M' := \gamma\overline{M} \oplus M_{\mathrm{tors}}$. Then we define

$$\mathrm{Pf}(M,h) := \det(\gamma)^{-1}\mathrm{Pf}(M',h). \tag{4.2.3}$$

Going back to our situation, consider the $\mathbf{Z}$-module $A^\dagger(K)$ equipped with the pairing $\widetilde{h}^-$. If $\dim A^\dagger(K)_{\mathbf{Q}}$ is even, we let

$$\mathrm{pf}^-(A) := \mathrm{pf}(A^\dagger(K), \widetilde{h}^-).$$

If $\dim A^\dagger(K)_{\mathbf{Q}}$ is odd, we let

$$\mathrm{Pf}^-(A) := \mathrm{Pf}(A^\dagger(K), \widetilde{h}^-).$$

Recall the number $I(A,f)$ from (2.2.3), and under the same assumptions define

$$\widetilde{I}(A,f) := \prod_{\mathfrak{p}|p} \widetilde{e}_{\mathfrak{p}}(\mathbf{1}) \cdot I(A,f), \tag{4.2.4}$$

where $\mathfrak{p}$ runs over the primes of K above p and $\widetilde{e}_{\mathfrak{p}}(\mathbf{1})$ is as in Conjecture (BSD_p).

Conjecture 4.2.1. — *Consider the setup of §4.1. Let $\widetilde{r} := \dim A^\dagger(K)_{\mathbf{Q}}$.*

1. *Suppose that $\widetilde{\varepsilon} = +1$. Then $\widetilde{r}$ is even, $\Theta = \Theta(f) \in \mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}}$ vanishes at $\chi^- = \mathbf{1}$ to order at least $\widetilde{r}/2$, the number $\widetilde{I}(A,f)$ is the square of an integer $\widetilde{i}(A,f)$, and up to a sign*
$$(\mathrm{d}^-)^{\widetilde{r}/2}\Theta(\mathbf{1}) = \widetilde{i}(A,f) \cdot \mathrm{pf}^-(A)$$
in $\mathrm{Sym}^{\widetilde{r}/2}\Gamma^- \otimes \mathbf{Q}$.
2. *Suppose that $\widetilde{\varepsilon} = -1$. Then $\widetilde{r}$ is odd, $\mathscr{P} = \mathscr{P}(f) \in \widetilde{H}^1_f(K, V_pA \otimes \mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}})$ vanishes at $\chi^- = \mathbf{1}$ to order at least $(\widetilde{r}-1)/2$, the number $\widetilde{I}(A,f)$ is the square of an integer $\widetilde{i}(A,f)$, and up to a sign*
$$(\mathrm{d}^-)^{(\widetilde{r}-1)/2}\mathscr{P}(\mathbf{1}) = \widetilde{i}(A,f) \cdot \mathrm{Pf}^-(A)$$
in $A^\dagger(K)_{\mathbf{Q}} \otimes \mathrm{Sym}^{(\widetilde{r}-1)/2}\Gamma^-$.

Remark 4.2.2. — Suppose that f is *optimal*, i.e. either surjective onto $\mathbf{Z}$ (case $\widetilde{\varepsilon} = +1$) or with connected kernel (case $\widetilde{\varepsilon} = -1$), and moreover that the following identities hold: (i) $|Ш(A)| = |Ш(A)|_{\mathrm{an}}$; (ii) $\prod_{v|N^-} c_v(E) = c_\infty(E_K)^{-1}\delta(f)^{-1}$. Then Conjecture 4.2.1 is equivalent to the original conjecture formulated by Bertolini–Darmon in [4]. Assume that E is isolated in its isogeny class, let $f_0 : J_0(N) \to E$ be the optimal modular parametrisation, and let $c = c_E \in \mathbf{N}$ be the Manin constant of E [28, p. 6]; it satisfies $c_\infty(E_K)^{-1} = c^2\delta(f_0)$. The identity (ii) is then implied by the conjecture that $c = 1$ together with the main results of Ribet and Takahashi in [41, 46], asserting that $\delta(f_0)/\delta(f) = \prod_{v|N^-} c_v(E)$; cf. [7, Remark 6.6, Theorem 6.7]. It is not clear to us whether (ii) should hold in general.

The conjecture is only made up to sign, since the right-hand side is insensitive to changing f into $-f$ whereas the left-hand side is not. However we have the following elementary observation about signs.

Lemma 4.2.3. — *Let $*$ be the $\mathbf{Z}_p$-algebra involution on $\mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}} = \mathbf{Z}_p[\![\Gamma^-]\!]_{\mathbf{Q}_p}$ induced by inversion on Γ^-, and denote the image under $*$ of an element s of some $\mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}}$-module by s^*. Suppose that Θ (resp. $\mathscr{P}$) vanishes at $\mathbf{1}$ to order $\geq s$ (resp. $\geq s'$). Then*

$$(\mathrm{d}^-)^s\Theta^*(\mathbf{1}) = (-1)^s\Theta(\mathbf{1}), \qquad (\mathrm{d}^-)^{s'}\mathscr{P}^*(\mathbf{1}) = (-1)^{s'}\mathscr{P}(\mathbf{1}).$$

Proof. — The differential of $*$ at $\mathbf{1} \in \mathscr{Y}^-$ is $\mathrm{d}^- * (\mathbf{1}) = -1$. □

Remark 4.2.4. — Suppose that $r^{\mathrm{exc}}(A) = 0$ and $r_{\mathrm{an}}(A) \leq 1$. Then Conjecture 4.2.1 follows immediately from the construction of Θ and $\mathscr{P}$ and Corollary 2.2.5. An elaboration of this observation will result in Proposition 5.1.1 below.

Evidence. — We next summarise the available evidence towards the Bertolini–Darmon conjecture in cases where $r^{\mathrm{exc}}(A) \neq 0$. By the Lemma 3.1.2, up to switching E and $E^{(K)}$ we may then suppose that E has split multiplicative reduction.

Theorem 4.2.5. — *Suppose that E has split multiplicative reduction, and let $r_{\mathrm{an}} := \mathrm{ord}_{s=1} L(A,s)$. Conjecture 4.2.1 holds in the following cases.*

1. *$r_{\mathrm{an}} = 0$ and p is inert in K, as an exact identity when E is isolated in its isogeny class, and up to a nonzero multiplicative constant otherwise.*
2. *$r_{\mathrm{an}} = 0$ and p splits in K.*
3. *$r_{\mathrm{an}} = 1$ and p is inert in K.*
4. *$r_{\mathrm{an}} = 1$, $p \geq 5$ splits in K, and $N^- = 1$.*

Proof. — Parts 1–3 are essentially due to Bertolini–Darmon; we shall recall their results, then deduce Part 4 from a recent result of Castella and Molina Blanco.

When p splits in K we write $p\mathscr{O}_K = \mathfrak{p}\mathfrak{p}^*$. The choice of $\mathfrak{p}$ or $\mathfrak{p}^*$ will only affect the formulas which follow up to a sign, therefore it won't be specified.

1. This is essentially the main result of [5]. In its reformulation in [8, Theorem 5.4, §5.2], we have
$$\mathscr{P}(\mathbf{1}) = q_{A,p\mathscr{O}_K} \cdot \widetilde{i}(A,f)$$
for some $\widetilde{i}(A,f) \in \mathbf{Z}_p$, which is denoted there by $\varkappa$, and equals $c_p^{-1} \cdot \lambda_{q_E}((y_n))$ in the notation of [5, Theorem 5.1], with $c_p = c_p(E) = \mathrm{ord}_p(q_{E,p})$. (Namely, $y = \lim_n y_n \in q_{E,p}^{\times} \hat{\otimes} \mathbf{Q}_p$ is identified with $\mathscr{P}(\mathbf{1})$; and λ_{q_E}, which also has a geometric interpretation, is simply the homomorphism to $\mathbf{Q}_p$ deduced from ord_p.) It is proved in *loc. cit.* that $\lambda_{q_E}((y_n)) = I(A,f)c_p$, hence
$$\widetilde{i}(A,f)^2 = c_p^{-1} \cdot I(A,f) = \widetilde{I}(A,f).$$
That $\widetilde{I}(A,f)$ is in fact a square in $\mathbf{Z}$, under the additional assumption stated, follows from the results of Ribet and Takahashi mentioned in Remark 4.2.2, together with Corollary 2.2.5.
2. This is the main result of [7]. In this case $\widetilde{r} = 2$ and
$$\mathrm{d}^-\Theta(\mathbf{1}) = \mathscr{L}_{\mathfrak{p}}^-(A) \cdot p(f) = \mathrm{ord}_p(q_{E,p})^{-1} \cdot \widetilde{h}^-(q_{A,\mathfrak{p}}, q_{A,\mathfrak{p}}) \cdot i(A,f) = \widetilde{i}(A,f) \cdot \mathrm{pf}^-(A),$$
where the second equality is by Corollary 2.2.5.
3. We deduce this from the main result of [6]. In this case $\widetilde{r} = 2$; we introduce some notation. Let $X = X_0^{N^-}(N^+)$ and $X' := X_0^{N^-,(p)}(N^+p)$. Let J' be the Albanese variety of X'. Let $f : X \to \mathbf{Z}$ (resp., $f' : J' \to E$) be the unique-up-to-sign surjective map annihilated by the Hecke operators in I_E (resp., the morphism with connected kernel, which exists after possibly replacing E by an isogenous curve). We may and do assume that $\Theta = \Theta(f)$ is constructed starting from f. Then
$$\mathrm{d}^-\Theta(\mathbf{1}) = \log^-_{A,p\mathscr{O}_K}(P(f')) = \widetilde{h}^-(P', q_{A,p\mathscr{O}_K}) \cdot [A : \mathbf{Z}P(f')] = \mathrm{pf}^-(A) \cdot i(A,f'),$$
where $P' \in A(K) \otimes \mathbf{Q}$ is such that the (generalised) index $[A(K) : \mathbf{Z}P'] = 1$. By Proposition 3.2.6, we have $\delta(f') = c_p^{-1}\delta(f')$; hence with $\widetilde{i}(A,f) := i(A,f')$,
$$\widetilde{i}(A,f)^2 = I(A,f') = c_p^{-1} I(A,f) = \widetilde{I}(A,f).$$

4. We deduce this from a theorem proved independently by Castella [12] and Molina Blanco [31]:[(11)] the equality

$$\mathrm{d}^-\mathscr{P}(\mathbf{1}) = \mathscr{L}_{\mathfrak{p}}^-(A)\cdot P(f) \tag{4.2.5}$$

holds *in the quotient* $H^1_f(K,V_pA)$ *of* $\widetilde{H}^1_f(K,V_pA)$. (In fact in [12] the identity is proved after applying $\mathrm{loc}_{\mathfrak{p}}\colon A(K)\to H^1_f(K_{\mathfrak{p}},V_pA)$; under our assumption that $\mathrm{ord}_{s=1}L(A,1)=1$, by the work of Gross–Zagier and Kolyvagin the $\mathbf{Q}_p$-vector space $H^1_f(K,V_pA)=A(K)_{\mathbf{Q}_p}$ is generated by the image of P and the map $\mathrm{loc}_{\mathfrak{p}}$ is then injective.)

We lift (4.2.5) to the desired identity in $\widetilde{H}^1_f(K,V_pA)=A^\dagger(K)_{\mathbf{Q}_p}$. We abbreviate $P=P(f)$ and assume that the rank of E is 1 (otherwise, we switch E with its twist $E^{(K)}$). We make use of two observations.

(i) $\mathscr{P}$ is invariant under the conjugation c, hence so is $\mathrm{d}^-\mathscr{P}(\mathbf{1})$.

(ii) Letting $g\in\Gamma^-$ be a generator, the vanishing of $\mathscr{P}(\mathbf{1})$ implies that $\mathscr{P}$ is divisible by $[g]-1$ in $\mathbf{Z}_p[\![\Gamma^-]\!]$, and $\mathrm{d}^-\mathscr{P}(\mathbf{1})$ is precisely the image of $([g]-1)^{-1}\mathscr{P}\in\widetilde{H}^1_f(K,V_pA\otimes\mathbf{Z}_p[\![\Gamma^-]\!])$ in $\widetilde{H}^1_f(K,V_pA)$. As such, it is a 'universal norm' for the anticyclotomic extension of K and hence (see [34, (0.16.1)(iii)]) it belongs to the radical of $\widetilde{h}^-$.

Noting that $c_p:=c_p(E)=\mathrm{ord}_p(q_{E,p})=\widetilde{e}_{\mathfrak{p}}(\mathbf{1})^{-1}=\widetilde{e}_{\mathfrak{p}^*}(\mathbf{1})^{-1}$, write

$$\mathrm{d}^-\mathscr{P}(\mathbf{1}) = c_p^{-1}\cdot(aP(f)+bq_{A,\mathfrak{p}}+q_{A,\mathfrak{p}^*})$$

in terms of the natural basis of $A^\dagger(K)$. It follows from (4.2.5) that $a=\ell^-(q_{A,\mathfrak{p}})$, from (i) that $b=c$, and the common value can be fixed by (ii):

$$0 = c_p\cdot\widetilde{h}^-(\mathrm{d}^-\mathscr{P}(\mathbf{1}),q_{A,\mathfrak{p}}) = \ell^-(q_{A,\mathfrak{p}})\log^-_{A,\mathfrak{p}}(P)+b\cdot\ell^-(q_{A,\mathfrak{p}}),$$

hence the unique (by the non-vanishing [1] of $\ell^-(q)$) solution is $b=-\log^-_{A,\mathfrak{p}}(P)=\log^-_{A,\mathfrak{p}^*}(P)$.

We verify that this implies the desired formula for $\mathrm{d}^-\mathscr{P}(\mathbf{1})$, according to the definition of $\mathrm{Pf}^-(A)$ in (4.2.3). Let

$$\gamma=\begin{pmatrix}\ell^-(q_{A,\mathfrak{p}}) & \log^-_{A,\mathfrak{p}^*}(P) & \log^-_{A,\mathfrak{p}^*}(P)\\ & 1 & \\ & & 1\end{pmatrix}\in\mathbf{GL}_3(\mathbf{Q}_p),$$

identified with an element of $\mathbf{GL}(A^\dagger(K)_{\mathbf{Q}_p})$ by means of the ordered basis $(P,q_{A,\mathfrak{p}},q_{A,\mathfrak{p}^*})$. Let $M':=\gamma A^\dagger(K)\oplus A(K)_{\mathrm{tors}}$, and let

$$x':=c_p\cdot\mathrm{d}^-\mathscr{P}(\mathbf{1})=\ell^-(q_{A,\mathfrak{p}})\cdot P+\log^-_{A,\mathfrak{p}^*}(P)\cdot q_{A,\mathfrak{p}}+\log^-_{A,\mathfrak{p}^*}(P)\cdot q_{A,\mathfrak{p}^*}\quad\in M'.$$

Then $M'/\mathbf{Z}x'$ is freely generated by $q_{A,\mathfrak{p}}$ and $q_{A,\mathfrak{p}^*}$, and

$$[A(K):\mathbf{Z}P]\cdot\mathrm{Pf}^-(A)=\det(\gamma)^{-1}\cdot x'\otimes\mathrm{pf}(M'/\mathbf{Z}x')=\ell^-(q_{A,\mathfrak{p}})^{-1}\cdot x'\otimes\ell^-(q_{A,\mathfrak{p}})=x'.$$

As the last term is $\widetilde{e}_{\mathfrak{p}}(\mathbf{1})^{-1}\cdot\mathrm{d}^-\mathscr{P}(\mathbf{1})$ by definition, it follows that

$$\mathrm{d}^-\mathscr{P}(\mathbf{1})=\widetilde{e}_{\mathfrak{p}}(\mathbf{1})\cdot[A(K):\mathbf{Z}P]\cdot\mathrm{Pf}^-(A),$$

and we conclude by Corollary 2.2.5.

□

Remark 4.2.6. — The work of Molina Blanco [31] also provides a generalisation to totally real fields of the results of [7]. A similar generalisation has been independently obtained by Pin-Chi Hung [24].

4.3. p-adic Gross–Zagier and Waldspurger formulas in anticyclotomic families. — Retaining the setup and notation of §4.1, we state formulas relating Θ and $\mathscr{P}$ to $L_p(A)$.

(11) The results of Molina Blanco hold without the assumption $N^-=1$ (and more generally for Shimura curves over totally real fields), but in those additional cases they are formulated in terms of an $\mathscr{L}$-invariant which is not currently known to coincide with the one of our conjectures.

***Theorem 4.3.1* (Waldspurger formula in anticyclotomic family).** — *Suppose that $\widetilde{\varepsilon}=+1$. Then we have*

$$L_p(A)|_{\mathscr{Y}^-} = c_\infty(A)^{-1}\cdot\frac{\Theta\cdot\Theta^*}{\delta(f)} \tag{4.3.1}$$

in $\mathbf{Z}_p[\![\Gamma^-]\!]_{\mathbf{Q}_p}$.

Proof. — This is essentially a special case of [13, Theorem A]: more precisely, that result combined with Theorem B *ibid.* implies that the following identity (or equivalently all of its specialisations at finite $\chi^-\in\mathscr{Y}^-$) holds:

$$L_p(A)|_{\mathscr{Y}^-} = \varepsilon(E)\cdot c_\infty(A)^{-1}\cdot\frac{\Theta'\cdot\Theta'^*}{\langle f,f\rangle_R}. \tag{4.3.2}$$

Here Θ' is the same as our Θ, except for a different choice of the sequence g_n; as noted in Remark 4.1.1, we then have $\Theta'\cdot\Theta'^*=\Theta\cdot\Theta^*$. The sign $\varepsilon(E):=\prod_v\varepsilon_v(E)$ (the product ranging over all places of $\mathbf{Q}$) is the global root number of E. Finally, by (3.9) *ibid.*, $\langle f,f\rangle_R:=\langle f,\tau f\rangle$ for the pairing (2.2.1) and an Atkin–Lehner element $\tau=\prod_{v|N}\tau_v\in\widehat{B}^\times$. By Atkin–Lehner theory combined with the Jacquet–Langlands correspondence (see [4, Theorem 1.2]), $\tau f=\prod_{v|N^+}\varepsilon_v(E)\prod_{v|N^-}(-\varepsilon_v(E))\cdot f$. As N^- is the squarefree product of an odd number of factors and $\varepsilon_\infty(E)=-1$, we deduce $\tau f=\varepsilon(E)f$. Inserting this into (4.3.2) yields (4.3.1).

We recall the steps of proof of [13, Theorem A], in order to show that the previous argument can be unwound and then carried over to the proof of the next theorem. The starting point is the original representation-theoretic Waldspurger formula [49] or [51, (1.4.1)], which in the form used in [13, proof of Proposition 3.5] reads (with slightly different notation)

$$\frac{p_T(f_1,\chi)p_T(f_2,\overline{\chi})}{\langle f_3,f_4\rangle_{\mathrm{Pet}}}=\frac{\zeta(2)L(1/2,\pi_K\otimes\chi)}{2L(1,\pi,\mathrm{ad})}\cdot\prod_v\int^*_{K_v^\times/\mathbf{Q}_v^\times}\frac{\langle\pi(t)f_{1,v},f_{2,v}\rangle_v}{\langle f_{3,v},f_{4,v}\rangle_v}\chi(t_v)dt_v, \tag{4.3.3}$$

where $\pi=\otimes_v\pi_v$ is the automorphic representation with trivial central character of $B_{\mathbf{A}}^\times$ associated with E; χ is a finite order character of $\mathbf{A}^\times\backslash K_{\mathbf{A}}^\times$; the terms p_T are integrals on the torus $\mathbf{A}^\times\backslash K_{\mathbf{A}}^\times\subset\mathbf{A}^\times\backslash B_{\mathbf{A}}^\times$; the pairing $\langle,\rangle_{\mathrm{Pet}}$ (resp. $\langle,\rangle_v$) is the bilinear Petersson pairing on $\pi\otimes\widetilde{\pi}$ with respect to the Tamagawa measure (resp. an arbitrary pairing on $\pi_v\otimes\widetilde{\pi}_v$); the $f_i=\otimes_v f_{i,v}$ are arbitrary elements of π (if $i=1,3$) or $\widetilde{\pi}$ (if $i=2,4$) such that $\langle f_3,f_4\rangle_{\mathrm{Pet}}\neq 0$; and finally the notation $\int^*$ denotes an integral (for certain local measures dt_v) normalised by dividing by an appropriate product of L-values.

Then in [13], the formula (4.3.2) is deduced from (4.3.3) by specific choices of the f_i which are images of newforms under certain Atkin–Lehner elements (and elements g_n) and the following steps: (i) formula for the Asai L-value $L(1,\pi,\mathrm{ad})$; (ii) computation of the Petersson pairing; (iii) computation of local integrals at places $v\nmid p$; (iv) computation of local integrals at p. For convenience of reference, in the first paragraph of this proof we have deduced (4.3.1) from (4.3.3) via (4.3.2) and some Atkin–Lehner functional equations. This is equivalent to directly deducing (4.3.1) from (4.3.3) with the following choices: $f_3=f_4:=f=\overline{f}$ is the $\mathbf{Z}$-valued newform in $\pi=\overline{\widetilde{\pi}}$; $f_1=f_2:=f^{(n)}=g_nf^\dagger$. The local computations corresponding to such choices are the same as those in [13, §3] except for the addition (or subtraction) of the ingredient of Atkin–Lehner functional equations. Steps (i)–(iii) (for our choices of f_i) are also in [11]. □

Let

$$\underline{\widetilde{h}}^+:\widetilde{H}^1_f(K,V_pA\otimes\mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}})\otimes\widetilde{H}^1_f(K,V_pA\otimes\mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}})^*\to\mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}}\otimes\Gamma^+$$

be the 'big height pairing' constructed by Nekovář[34, §11]. It specialises to the pairing $\widetilde{h}^+$ at $\chi^-=\mathbf{1}\in\mathscr{Y}^-$ (and an equally good specialisation property holds for all finite order $\chi^-\in\mathscr{Y}^-$).

***Conjecture 4.3.2* (p-adic Gross–Zagier formula in anticyclotomic family)**

Suppose that E is ordinary at p and that $\widetilde{\varepsilon}=-1$, so that $L_p(A)$ vanishes identically along $\mathscr{Y}^-$. Let $\mathrm{d}^+L_p(A)|_{\mathscr{Y}^-}$ denote the image of $L_p(A)$ in $\mathscr{I}_{\mathscr{Y}^-}/\mathscr{I}^2_{\mathscr{Y}^-}\cong\mathbf{Z}_p[\![\Gamma^-]\!]_{\mathbf{Q}_p}\otimes_{\mathbf{Z}_p}\Gamma^+$.

Then we have

$$\mathrm{d}^+ L_p(A)|_{\mathscr{Y}^-} = c_\infty(A)^{-1} \cdot \frac{\widetilde{\underline{h}}^+(\mathscr{P}, \mathscr{P}^*)}{\delta(f)} \tag{4.3.4}$$

in $\mathbf{Z}_p[\![\Gamma^-]\!]_{\mathbf{Q}_p} \otimes_{\mathbf{Z}_p} \Gamma^+$.

Theorem 4.3.3. — *Suppose that p splits in K. Then Conjecture 4.3.2 holds.*

Proof. — This is a consequence of the representation-theoretic version of the same formula from [17, Theorem C.4], in turn based on Theorem B *ibid.*[12] For a definition of the relevant representation π of $B_{\mathbf{A}}^\times$, and a careful discussion of the various pairings involved and their relation or analogy to the ones appearing in versions of Waldspurger's formula, we refer to [11].[13]

More precisely, one can choose a pairing $\langle , \rangle$ on $\pi \otimes \widetilde{\pi}$ analogous to the Petersson pairing in (4.3.3) (see [11, §2.2], local pairings $\langle , \rangle_v$ such that $\langle , \rangle = \prod_v \langle , \rangle_v$, and obtain a version of the p-adic Gross–Zagier formula entirely analogous to (4.3.3) by dividing both sides of [17, Theorem B] by $\langle f_3, f_4 \rangle$. Then the deduction of (4.3.4) from such formula is obtained by inserting the *same* choices of $\{f_i\}_{i=1,2,3,4}$ and the *same* algebraic computations of steps (i)-(iv) from the proof of Theorem 4.3.1.[14] □

5. Evidence over imaginary quadratic fields

5.1. Conjecture (BSD_p) and the Bertolini–Darmon conjectures. — We observe a precise relation between the Bertolini–Darmon conjecture and the p-adic Birch and Swinnerton-Dyer conjecture, via the Waldspurger and p-adic Gross–Zagier formulas in anticyclotomic families. (In the original work of Bertolini–Darmon [4], the other terms of comparison were not available in general; besides the purely anticyclotomic single-variable case of (BSD_p) which they conjectured, there was rather a relation of analogy with the archimedean Birch and Swinnerton-Dyer conjecture, via the archimedean Waldspurger and Gross–Zagier formulas.)

We retain the setup and notation of §4.1. Let $\widetilde{r}_{\mathrm{an}} := \mathrm{ord}_{s=1} L(A,s) + |S_p^{\mathrm{exc}}(A)|$, $\widetilde{r} := \dim A^\dagger(K)_{\mathbf{Q}}$, and

$$\epsilon := \begin{cases} 0 & \text{if } \widetilde{\varepsilon} = +1 \\ 1 & \text{if } \widetilde{\varepsilon} = -1. \end{cases}$$

By the *anticyclotomic Waldspurger/Gross–Zagier formula*, we shall mean either Theorem 4.3.1 (case $\widetilde{\varepsilon} = +1$) or Conjecture 4.3.2 (case $\widetilde{\varepsilon} = -1$).

By the *Bertolini–Darmon Conjecture*, we shall mean Conjecture 4.2.1, *except* for the assertion that the p-adic number $\widetilde{I}(A,f)^{1/2}$ is an integer.

By the *almost-anticyclotomic case* of Conjecture (BSD_p), we shall mean the following statement: $(\mathrm{d}^+)^\epsilon L_p(A)|_{\mathscr{Y}^-} \in \mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}} \otimes (\Gamma^+)^\epsilon$ vanishes to order $\geq \widetilde{r}_{\mathrm{an}} - \epsilon$ at $\chi^- = \mathbf{1}$, $A^\dagger(K)$ has rank $\widetilde{r} = \widetilde{r}_{\mathrm{an}}$, and

$$(\mathrm{d}^-)^{\widetilde{r}-\epsilon} (\mathrm{d}^+)^\epsilon L_p(A, \mathbf{1})$$

equals the projection of the right hand side of (1.1.8) under

$$\pi_\epsilon : \mathrm{Sym}^{\widetilde{r}} \Gamma_K \to \mathrm{Sym}^{\widetilde{r}-\epsilon} \Gamma^- \otimes (\Gamma^+)^\epsilon.$$

(Note that, if $\widetilde{\varepsilon} = -1$, the restriction $L_p(A)|_{\mathscr{Y}^-}$ is identically zero by the functional equation; correspondingly $\widetilde{R}^-(A) = 0$ by the property (4.2.1) of $\widetilde{h}^-$, provided that the rank of $A^\dagger(K)$ is odd as expected.)

[12] When E has good reduction and all $v|N$ split in K the result was proved by Howard [22].

[13] The discussion in [11] is based on [51] rather than [17], but those two works adopt exactly the same framework. The constants appearing in the archimedean and p-adic Gross–Zagier formula exactly match: compare [17, (1.1.3) and Theorem B].

[14] Step (iv) is also carried out in [17, Lemma 10.1.2].

Proposition 5.1.1. — *Suppose that Hypothesis* (BSD_∞)*-1-2 and the anticyclotomic Waldspurger/Gross–Zagier formula hold for A. Then the Bertolini–Darmon Conjecture for A implies the almost-anticyclotomic case of Conjecture* (BSD_p) *for A. Conversely, the almost-anticyclotomic case of Conjecture* (BSD_p) *implies the Bertolini–Darmon Conjecture provided that, in case* $\widetilde{\varepsilon}=-1$*, the term* $\pi_1\left(\widetilde{R}(A)\right)\neq 0$.

Proof. — In case $\widetilde{\varepsilon}=+1$, note that the orders of vanishing of Θ and Θ^* are the same. Then by the anticyclotomic Waldspurger formula, $L_p(A)|_{\mathscr{Y}^-}$ vanishes to order $\geq\widetilde{r}$ if and only if Θ vanishes to order $\geq\widetilde{r}/2$. By Lemma 4.2.3, the 'leading terms' $(\mathrm{d}^-)^{\widetilde{r}/2}\Theta$ and $(\mathrm{d}^-)^{\widetilde{r}/2}\Theta^*$ differ by the sign $(-1)^{\widetilde{r}/2}$. Then the desired equivalence is reduced to the identity

$$\widetilde{R}^-(A)=(-1)^{\widetilde{r}/2}\cdot\mathrm{pf}^-(A)^2,$$

which is (4.2.2).

We now turn to the case $\widetilde{\varepsilon}=-1$. Let $A^\dagger(K)^\pm_{\mathbf{Q}_p}$ be the larger of the eigenspaces under the complex conjugation c, and let $x\in A^\dagger(K)^\pm_{\mathbf{Q}_p}$ be an element in the radical of $\widetilde{h}^-$. Complete $x=x_1$ to an ordered basis $\mathscr{B}=\{x_1,\dots,x_{\widetilde{r}}\}$ of $A(K)^\dagger_{\mathbf{Q}_p}$, which we may take to be the image of an integral basis of $A^\dagger(K)/A(K)_{\mathrm{tors}}$ under an element $\gamma\in\mathbf{SL}(A^\dagger(K)_{\mathbf{Q}_p})$. Denote $M_1:=\bigoplus_{i\neq j}^n\mathbf{Z}x_i\oplus A(K)_{\mathrm{tors}}$. We may compute $\pi_1\left(\widetilde{R}(A)\right)$ in the basis $\mathscr{B}$, evaluating $\pi_1\left(\det(\widetilde{h}(x_i,x_j)_{i,j=1}^{\widetilde{r}})\right)$ by expansion along the first row. As $x=x_1$ is in the radical of $\widetilde{h}^-$, the j^{th} term in the expansion is $\pi_1\left(\widetilde{h}(x,x_j)R_j\right)=\widetilde{h}^+(x,x_j)R_j^-$, where R_j is $(-1)^{1+j}$ times the $(1,j)^{\mathrm{th}}$ minor and $R_j^-=\pi_0(R_j)$. If $j\neq 1$ this minor in fact vanishes as the first column of the corresponding matrix is zero. We conclude that

$$\pi_1\left(\widetilde{R}(A)\right)=\widetilde{h}^+(x,x)R(M_2,\widetilde{h}^-)=(-1)^{(\widetilde{r}-1)/2}\cdot\widetilde{h}^+\left(\mathrm{Pf}^-(A),\mathrm{Pf}^-(A)\right),$$

where the last equality uses (4.2.2) applied to M_2. By this identity, the anticyclotomic Gross–Zagier formula, and again Lemma 4.2.3, we see that the Bertolini–Darmon Conjecture implies the almost-anticyclotomic case of Conjecture (BSD_p). The implication can be reversed if $\widetilde{h}^+$ is non-vanishing on $\mathrm{Pf}^-(A)$. □

5.2. Proof of Theorems B and C. — We proceed to prove our main theorems, after some preliminaries which allow to settle 'trivial' cases.

Proposition 5.2.1. — *1. We have*

$$\widetilde{\varepsilon}=(-1)^{\widetilde{r}_{\mathrm{an}}}.$$

2. Suppose that $L_p(A)$ *vanishes to order* $\geq i+j$ *at* $\chi=\mathbf{1}$*. Then if* $i\not\equiv\widetilde{r}\pmod 2$*, we have*

$$(\mathrm{d}^+)^i(\mathrm{d}^-)^jL_p(A,\mathbf{1})=0$$

in $(\mathrm{Sym}^i\Gamma^+\otimes\mathrm{Sym}^j\Gamma^-)\otimes L$.

3. Suppose that $L_p(A)$ *vanishes to order* $\geq\widetilde{r}_{\mathrm{an}}$ *at* $\chi=\mathbf{1}$*. Then*

$$\mathrm{d}^{\widetilde{r}_{\mathrm{an}}}L_p(A,\mathbf{1})\in(\mathrm{Sym}^{\widetilde{r}}\Gamma)^+_L,$$

the $+1$*-eigenspace for the action of the complex conjugation* $c\in\mathrm{Gal}(K/\mathbf{Q})$ *on* $(\mathrm{Sym}^{\widetilde{r}}\Gamma)\otimes L$*; that is,* $(\mathrm{d}^+)^{\widetilde{r}_{\mathrm{an}}-j}(\mathrm{d}^-)^jL_p(A,\mathbf{1})=0$ *in* $(\mathrm{Sym}^{\widetilde{r}_{\mathrm{an}}-j}\Gamma^+\otimes\mathrm{Sym}^j\Gamma^-)\otimes L$ *for every odd* j.

Proof. — The sign of the functional equation for $L(A,s)$ is $-\eta(N)=(-1)^{r_{\mathrm{an}}}$; then part 1 is equivalent to the statement that r^{exc} is odd if and only if $p|N$ and p is inert in K, which follows from Lemma 3.1.2. Part 2 follows from part 1 and the functional equation for $L_p(A)$, and part 3 from part 2. □

The following is the counterpart of the previous proposition on the arithmetic side.

Proposition 5.2.2. — *Let* $\widetilde{r}$ *be the rank of* $A^\dagger(K)_{\mathbf{Q}_p}$*. Then*

$$\widetilde{R}(A)\in(\mathrm{Sym}^{\widetilde{r}}\Gamma)^+_L;$$

that is, the image of $\widetilde{R}(A)$ *in* $(\mathrm{Sym}^{\widetilde{r}-j}\Gamma^+ \otimes \mathrm{Sym}^j\Gamma^-)\otimes L$ *vanishes for every odd* j.

Proof. — By Lemma 2.1.1, the map

$$\det\widetilde{h}\colon \det A^\dagger(K)_{\mathbf{Q}_p}\otimes\det A^\dagger(K)_{\mathbf{Q}_p}\to(\mathrm{Sym}^{\widetilde{r}}\Gamma)\otimes L$$

is c-equivariant. As $c^2=1$, c acts by ±1 on $\det A^\dagger(K)_{\mathbf{Q}_p}$ and by $(\pm1)^2=+1$ on $\det A^\dagger(K)^{\otimes 2}_{\mathbf{Q}_p}$. The result follows. □

The proof of Theorem B for is naturally subdivided into several cases corresponding to the projections $\pi_i\colon \mathrm{Sym}^{\widetilde{r}}\Gamma\to(\mathrm{Sym}^i\Gamma^+\otimes\mathrm{Sym}^{\widetilde{r}-i}\Gamma^-)$. The identity between the images of both sides of (1.1.8) under the above projection will be referred to as the *purely cyclotomic case* if $i=\widetilde{r}$, as the *purely anticyclotomic case* if $i=0$, and as a *mixed case* if $0<i<\widetilde{r}$.

By Proposition 3.1.3, the purely cyclotomic case is always reduced to the case $K=\mathbf{Q}$ treated before.

Case $r=0$, *p inert.* — This is trivial unless A has (necessarily split, by Lemma 3.1.2) multiplicative reduction, in which case we have $\widetilde{r}=1$ for A. The cyclotomic case is reduced to Theorem 3.2.1 as remarked before. By Propositions 5.2.1.3 and 5.2.2, the anticyclotomic case is reduced to the equality $0=0$.

Remark 5.2.3. — In this context, the purely cyclotomic and the almost-anticyclotomic case of (BSD_p) coincide. A proof using Proposition 5.1.1 would presently only be conditional, as the p-adic Gross–Zagier formula is not available when p is inert K. Nevertheless it seems worth highlighting that such a formula, combined with Bertolini–Darmon's

$$\mathscr{P}(\mathbf{1})\doteq q_{A,p\mathscr{O}_K}$$

(Theorem 4.2.5.1) would yield an intriguing (and difficult) proof of the result of Greenberg–Stevens.

Case $r=0$, *p split.* — Again the only non-trivial case is the one of split multiplicative reduction with $\widetilde{r}=2$ and $A^\dagger(K)_{\mathbf{Q}_p}$ generated by $q_{A,\mathfrak{p}}\in K_{\mathfrak{p}}^\times$ and $q_{A,\mathfrak{p}^*}\in K_{\mathfrak{p}^*}^\times$ for $S_p=\{\mathfrak{p},\mathfrak{p}^*\}$. First we show the assertion on the order of vanishing, i.e. that $\mathrm{d}L_p(A,\mathbf{1})=0$: the component $\mathrm{d}^+L_p(A,\mathbf{1})=0$ by the factorisation

$$L_p(A)|_{\mathscr{Y}^+}=\frac{\Omega_E^+\Omega_E^-}{|D_K|^{-1/2}\Omega_A}L_p(E)L_p(E^{(K)}), \tag{5.2.1}$$

and the component $\mathrm{d}^-L_p(A,\mathbf{1})=0$ by the anticyclotomic Waldspurger formula (Theorem 4.3.1), since both $\Theta,\Theta^*\in\mathbf{Z}_p[\![\Gamma^-]\!]$ vanish at $\chi^-=\mathbf{1}$.

We can now deal prove the identity (1.1.8). The purely cyclotomic case is as usual reduced to Theorem 3.2.1. The mixed case is again trivial, i.e. reduced to $0=0$, by Propositions 5.2.1 and 5.2.2. The purely anticyclotomic case follows from Proposition 5.1.1 and Theorem 4.2.5.2: explicitly, it is the identity

$$(\mathrm{d}^-)^2L_p(A,\mathbf{1})=\mathscr{L}_{\mathfrak{p}}^-(A)\mathscr{L}_{\mathfrak{p}^*}^-(A)\cdot L_{\mathrm{alg}}(A,1)\qquad\text{in }(\Gamma^-)^{\otimes 2}_{\mathbf{Q}_p}.$$

Case $r=1$, *p inert.* — The purely cyclotomic case is reduced to Theorem 3.2.1. If A has good reduction at p, then $\widetilde{r}=r=1$ and the purely anticyclotomic case is trivial by Propositions 5.2.1, 5.2.2. Suppose that A has (necessarily split) multiplicative reduction. Then $\widetilde{r}=2$. For the order of vanishing, we have $\mathrm{d}^+L_p(A,\mathbf{1})=0$ by (5.2.1), and Theorem 4.3.1 again implies $\mathrm{d}^-L_p(A,\mathbf{1})=0$.

The mixed case is again trivial. Finally, the purely anticyclotomic case follows from Proposition 5.1.1 and Theorem 4.2.5.3: explicitly, it is the identity

$$(\mathrm{d}^-)^2L_p(A,\mathbf{1})=-\frac{\log^-_{A,p\mathscr{O}_K}(P)^2}{\mathrm{ord}_p(q_{A,p})}\cdot L'_{\mathrm{alg}}(A,1)$$

in $(\Gamma^-)^{\otimes 2}\otimes\mathbf{Q}_p$, where $P\in A(K)_{\mathbf{Q}}$ is such that the generalised index $[A(K):\mathbf{Z}P]=1$.

Case $r=1$, *p split.* — The purely cyclotomic case is reduced to Theorem 3.2.1. If E does not have split multiplicative reduction, then $\widetilde{r}(A)=r(A)=1$, and the anticyclotomic case is trivial by Propositions

5.2.1, 5.2.2. If E has split multiplicative reduction, then $\widetilde{r}(A) = r+2 = 3$. We first prove the assertion on the order of vanishing. By the functional equation we have $(\mathrm{d}^+)^i L_p(A)|_{\mathscr{Y}^-} = 0$ for every even i. Then we only need to show $(\mathrm{d}^-)^j \mathrm{d}^+ L_p(A, \mathbf{1}) = 0$ for $j = 0, 1$. For $j = 0$ this follows from the factorisation (5.2.1) and Theorem 3.2.1. Consider the case $j = 1$. By the p-adic Gross–Zagier formula in anticyclotomic families (Theorem 4.3.3), $\mathrm{d}^+ L_p(A)|_{\mathscr{Y}^-}$ is a multiple of the image of $\mathscr{P} \otimes \mathscr{P}^*$ under $\underline{\widetilde{h}}^+$ on $\mathscr{Y}^-$. As both $\mathscr{P}, \mathscr{P}^*$ have a trivial zero at $\chi^- = \mathbf{1}$. We conclude that $\mathrm{d}^-\mathrm{d}^+ L_p(A, \mathbf{1}) = 0$ and so $L_p(A)$ vanishes to order at least $\widetilde{r} = 3$ at $\chi = \mathbf{1}$.

We now turn to the main identity (1.1.8). By Propositions 5.2.1, 5.2.2, the only nontrivial cases are the purely cyclotomic and the almost-anticyclotomic ones. The latter follows from Proposition 5.1.1 and Theorems 4.3.3 and 4.2.5.4.

The almost-anticyclotomic case is equivalent to the following, which is precisely Theorem C in the Introduction.

Theorem 5.2.4. — *Let $E/\mathbf{Q}$ be an elliptic curve with conductor N and split multiplicative reduction at the prime $p \geq 5$. Let K be an imaginary quadratic field such that all primes dividing N split in K and let $A := E_K$; then $S_p^{\mathrm{exc}}(A) = S_p = \{\mathfrak{p}, \mathfrak{p}^*\}$. Suppose that $\mathrm{ord}_{s=1} L(A, s) = 1$. We have $\mathrm{d}^i L_p(A) = 0$ for all $i \leq 2$, and*

$$(\mathrm{d}^-)^2 \mathrm{d}^+ L_p(A, \mathbf{1}) = \mathscr{L}_{\mathfrak{p}}^-(A) \mathscr{L}_{\mathfrak{p}^*}^-(A) \cdot R^{\mathrm{norm},+}(A) \cdot L'_{\mathrm{alg}}(A, 1) \tag{5.2.2}$$

in $(\mathrm{Sym}^2 \Gamma^- \otimes \Gamma^+)_{\mathbf{Q}_p}$.

Proof. — We give two proofs.

1. Observe first that $R^{\mathrm{norm},-}(A) = 0$ as $A(K)_{\mathbf{Q}_p}$ is a c-eigenspace and $h^{\mathrm{norm},-}$ satisfies (4.2.1). Then by Proposition 3.1.1, the right-hand side of (5.2.2) equals the image under π_1 of the right-hand side of (1.1.8). Since under our assumption we have just proved that (1.1.8) holds, so does (5.2.2).
2. We can unwind the previous argument to give a more self-contained (but not essentially different) proof. Let $\overline{\mathscr{P}}$ be $\mathscr{P}$ viewed as an element of $H^1_f(K, V_p A, \mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}})$ rather than $\widetilde{H}^1_f(K, V_p A, \mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}})$, and consider the pairing

$$\underline{h}^{\mathrm{norm},+} \colon H^1_f(K, V_p A, \mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}}) \otimes H^1_f(K, V_p A, \mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}})^* \to \mathscr{O}(\mathscr{Y}^-)^{\mathrm{b}} \otimes \Gamma^+$$

constructed in [39]: its specialisations coincide with those of $\underline{\widetilde{h}}^+$ at all finite order $\chi^- \in \mathscr{Y}^- - \{\mathbf{1}\}$, whereas at $\chi^- = \mathbf{1}$ it specialises to $h^{\mathrm{norm},+}$. We may then rewrite (4.3.4) in the form

$$\mathrm{d}^+ L_p(A)|_{\mathscr{Y}^-} = c_\infty(A)^{-1} \cdot \frac{\underline{h}^{\mathrm{norm},+}\left(\overline{\mathscr{P}}, \overline{\mathscr{P}}^*\right)}{\delta(f)}$$

(since the specialisations of both formulas at all finite order $\chi^- \in \mathscr{Y}^-$ coincide: at $\chi^- = \mathbf{1}$ both reduce to $0 = 0$). We can then directly obtain Theorem 5.2.4 by applying $(\mathrm{d}^-)^2$, inserting the formula $\mathrm{d}^- \mathscr{P}(\mathbf{1}) = \mathscr{L}_{\mathfrak{p}}^-(A) \cdot P(f)$ of (4.2.5), and fixing constants via Corollary 2.2.5.

□

References

[1] Katia Barré-Sirieix, Guy Diaz, François Gramain, and Georges Philibert, *Une preuve de la conjecture de Mahler-Manin*, Invent. Math. **124** (1996), no. 1-3, 1–9, DOI 10.1007/s002220050044 (French). MR1369409 (96j:11103) ↑9, 19

[2] Dominique Bernardi and Bernadette Perrin-Riou, *Variante p-adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier)*, C. R. Acad. Sci. Paris Sér. I Math. **317** (1993), no. 3, 227–232 (French, with English and French summaries). MR1233417 (94k:11071) ↑7

[3] Massimo Bertolini and Henri Darmon, *Derived p-adic heights*, Amer. J. Math. **117** (1995), no. 6, 1517–1554. MR1363078 ↑5

[4] M. Bertolini and H. Darmon, *Heegner points on Mumford-Tate curves*, Invent. Math. **126** (1996), no. 3, 413–456, DOI 10.1007/s002220050105. MR1419003 (97k:11100) ↑5, 7, 15, 17, 18, 20, 21

[5] Massimo Bertolini and Henri Darmon, *A rigid analytic Gross-Zagier formula and arithmetic applications*, Ann. of Math. (2) **146** (1997), no. 1, 111–147, DOI 10.2307/2951833. With an appendix by Bas Edixhoven. MR1469318 (99f:11079) ↑7, 18

[6] ———, *Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization*, Invent. Math. **131** (1998), no. 3, 453–491, DOI 10.1007/s002220050211. MR1614543 (99f:11080) ↑7, 19

[7] ———, *p-adic periods, p-adic L-functions, and the p-adic uniformization of Shimura curves*, Duke Math. J. **98** (1999), no. 2, 305–334, DOI 10.1215/S0012-7094-99-09809-5. MR1695201 (2000f:11075) ↑7, 18, 19, 20

[8] ———, *The p-adic L-functions of modular elliptic curves*, Mathematics unlimited—2001 and beyond, Springer, Berlin, 2001, pp. 109–170. MR1852156 (2002i:11061) ↑15, 16, 17, 18

[9] ———, *Hida families and rational points on elliptic curves*, Invent. Math. **168** (2007), no. 2, 371–431, DOI 10.1007/s00222-007-0035-4. MR2289868 (2008c:11076) ↑14

[10] Kâzım Büyükboduk, *On Nekovář's heights, exceptional zeros and a conjecture of Mazur-Tate-Teitelbaum*, Int. Math. Res. Not. IMRN **7** (2016), 2197–2237, DOI 10.1093/imrn/rnv205. MR3509952 ↑7

[11] Li Cai, Jie Shu, and Ye Tian, *Explicit Gross-Zagier and Waldspurger formulae*, Algebra Number Theory **8** (2014), no. 10, 2523–2572, DOI 10.2140/ant.2014.8.2523. MR3298547 ↑8, 10, 11, 21

[12] Francesc Castella, *On the exceptional specializations of big Heegner points*, J. Inst. Math. Jussieu, to appear. ↑7, 8, 19

[13] Masataka Chida and Ming-Lun Hsieh, *Special values of anticyclotomic L-functions for modular forms*, J. Reine Angew. Math., to appear. ↑7, 8, 10, 16, 20, 21

[14] Pierre Colmez, *La conjecture de Birch et Swinnerton-Dyer p-adique*, Astérisque **294** (2004), ix, 251–319 (French, with French summary). MR2111647 ↑13

[15] Holger Deppe, *p-adic L-functions of automorphic forms and exceptional zeros*, Doc. Math. **21** (2016), 689–734. MR3522253 ↑3

[16] Daniel Disegni, *p-adic Heights of Heegner points on Shimura curves*, to appear in Algebra & Number Theory. ↑13

[17] ———, *The p-adic Gross–Zagier formula on Shimura curves*, preprint. ↑3, 6, 7, 8, 10, 11, 13, 21

[18] Ralph Greenberg and Glenn Stevens, *p-adic L-functions and p-adic periods of modular forms*, Invent. Math. **111** (1993), no. 2, 407–447, DOI 10.1007/BF01231294. MR1198816 (93m:11054) ↑6, 13

[19] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320, DOI 10.1007/BF01388809. MR833192 (87j:11057) ↑

[20] Benedict H. Gross, *L-functions at the central critical point*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 527–535. MR1265543 (95a:11060) ↑

[21] Benjamin Howard, *Derived p-adic heights and p-adic L-functions*, Amer. J. Math. **126** (2004), no. 6, 1315–1340. MR2102397 ↑5

[22] ———, *The Iwasawa theoretic Gross-Zagier theorem*, Compos. Math. **141** (2005), no. 4, 811–846, DOI 10.1112/S0010437X0500134X. MR2148200 (2006f:11074) ↑21

[23] ———, *Variation of Heegner points in Hida families*, Invent. Math. **167** (2007), no. 1, 91–128, DOI 10.1007/s00222-006-0007-0. MR2264805 (2007h:11067) ↑

[24] Pin-Chi Hung, *On the derivative of anticyclotomic p-adic L-functions for Hilbert modular forms*, preprint. ↑20

[25] Shinichi Kobayashi, *An elementary proof of the Mazur-Tate-Teitelbaum conjecture for elliptic curves*, Doc. Math. **Extra Vol.** (2006), 567–575. MR2290598 ↑8, 13

[26] ———, *The p-adic Gross-Zagier formula for elliptic curves at supersingular primes*, Invent. Math. **191** (2013), no. 3, 527–629, DOI 10.1007/s00222-012-0400-9. MR3020170 ↑13

[27] V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and $SH(E,\mathbf{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671 (Russian); English transl., Math. USSR-Izv. **32** (1989), no. 3, 523–541. MR954295 (89m:11056) ↑11

[28] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61. MR0354674 ↑18

[29] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48, DOI 10.1007/BF01388731. MR830037 (87e:11076) ↑2, 4, 5, 6, 7, 8, 11, 12

[30] Chung Pang Mok, *The exceptional zero conjecture for Hilbert modular forms*, Compos. Math. **145** (2009), no. 1, 1–55, DOI 10.1112/S0010437X08003813. MR2480494 ↑13

[31] Santiago Molina Blanco, *Anticyclotomic p-adic L-functions and the exceptional zero phenomenon*, preprint. ↑7, 8, 19, 20

[32] M. Ram Murty and V. Kumar Murty, *Non-vanishing of L-functions and applications*, Progress in Mathematics, vol. 157, Birkhäuser Verlag, Basel, 1997. MR1482805 (98h:11106) ↑13, 14

[33] Jan Nekovář, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. 108, Birkhäuser Boston, Boston, MA, 1993, pp. 127–202. MR1263527 (95j:11050) ↑4, 8

[34] ———, *Selmer complexes*, Astérisque **310** (2006), viii+559 (English, with English and French summaries). MR2333680 (2009c:11176) ↑4, 5, 7, 9, 16, 19, 21

[35] Jan Nekovář and Anthony Scholl, *Introduction to plectic cohomology*, preprint. ↑8

[36] Kazuto Ota, *A generalization of the theory of Coleman power series*, Tohoku Math. J. (2) **66** (2014), no. 3, 309–320, DOI 10.2748/tmj/1412783201. MR3266735 ↑13

[37] Bernadette Perrin-Riou, *Points de Heegner et dérivées de fonctions L p-adiques*, Invent. Math. **89** (1987), no. 3, 455–510, DOI 10.1007/BF01388982 (French). MR903381 (89d:11034) ↑5, 6, 11, 13

[38] ———, *Fonctions L p-adiques associées à une forme modulaire et à un corps quadratique imaginaire*, J. London Math. Soc. (2) **38** (1988), no. 1, 1–32, DOI 10.1112/jlms/s2-38.1.1 (French). MR949078 (89m:11043) ↑11

[39] ———, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), no. 4, 399–456 (French, with English summary). MR928018 (89d:11094) ↑25

[40] ———, *Fonctions L p-adiques des représentations p-adiques*, 1995 (French, with English and French summaries). MR1327803 (96e:11062) ↑7
[41] Kenneth A. Ribet and Shuzo Takahashi, *Parametrizations of elliptic curves by Shimura curves and by classical modular curves*, Proc. Nat. Acad. Sci. U.S.A. **94** (1997), no. 21, 11110–11114, DOI 10.1073/pnas.94.21.11110. Elliptic curves and modular forms (Washington, DC, 1996). MR1491967 (99e:11080) ↑14, 18
[42] Peter Schneider, *p-adic height pairings. I*, Invent. Math. **69** (1982), no. 3, 401–409, DOI 10.1007/BF01389362. MR679765 (84e:14034) ↑9
[43] Christopher Skinner and Eric Urban, *The Iwasawa Main Conjectures for GL_2*, Invent. Math. **195** (2014), no. 1, 1–277, DOI 10.1007/s00222-013-0448-1. MR3148103 ↑7
[44] Michael Spieß, *On special zeros of p-adic L-functions of Hilbert modular forms*, Invent. Math. **196** (2014), no. 1, 69–138, DOI 10.1007/s00222-013-0465-0. MR3179573 ↑13
[45] Florian Sprung, *A formulation for p-adic versions of the Birch and Swinnerton-Dyer conjectures in the supersingular case*, preprint. ↑7
[46] Shuzo Takahashi, *Degrees of parametrizations of elliptic curves by Shimura curves*, J. Number Theory **90** (2001), no. 1, 74–88, DOI 10.1006/jnth.2000.2614. MR1850874 (2002h:11052) ↑14, 18
[47] John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 306, 415–440. MR1610977 ↑2, 12
[48] Rodolfo Venerucci, *Exceptional zero formulae and a conjecture of Perrin-Riou*, Invent. Math. **203** (2016), no. 3, 923–972, DOI 10.1007/s00222-015-0606-8. MR3461369 ↑6, 7, 8, 13, 14
[49] J.-L. Waldspurger, *Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie*, Compositio Math. **54** (1985), no. 2, 173–242 (French). MR783511 (87g:11061b) ↑10, 20
[50] Xin Wan, *Heegner Point Kolyvagin System and Iwasawa Main Conjecture*, preprint. ↑7
[51] Xinyi Yuan, Shou-Wu Zhang, and Wei Zhang, *The Gross-Zagier Formula on Shimura Curves*, Annals of Mathematics Studies, vol. 184, Princeton University Press, Princeton, NJ, 2012. ↑8, 10, 11, 13, 20, 21

DANIEL DISEGNI, Laboratoire de Mathématiques d'Orsay, Université Paris-Sud, CNRS, Université Paris-Saclay, 91405 Orsay, France. • *E-mail :* daniel.disegni@gmail.com