



# Stark–Heegner points and the Shimura correspondence

Henri Darmon and Gonzalo Tornara

## ABSTRACT

Let  $g = \sum c(D)q^D$  and  $f = \sum a_nq^n$  be modular forms of half-integral weight  $k + 1/2$  and integral weight  $2k$  respectively that are associated to each other under the Shimura–Kohnen correspondence. For suitable fundamental discriminants  $D$ , a theorem of Waldspurger relates the coefficient  $c(D)$  to the central critical value  $L(f, D, k)$  of the Hecke  $L$ -series of  $f$  twisted by the quadratic Dirichlet character of conductor  $D$ . This paper establishes a similar kind of relationship for central critical *derivatives* in the special case  $k = 1$ , where  $f$  is of weight 2. The role of  $c(D)$  in our main theorem is played by the first derivative in the weight direction of the  $D$ th Fourier coefficient of a  $p$ -adic family of half-integral weight modular forms. This family arises naturally, and is related under the Shimura correspondence to the Hida family interpolating  $f$  in weight 2. The proof of our main theorem rests on a variant of the Gross–Kohnen–Zagier formula for Stark–Heegner points attached to real quadratic fields, which may be of some independent interest. We also formulate a more general conjectural formula of Gross–Kohnen–Zagier type for Stark–Heegner points, and present numerical evidence for it in settings that seem inaccessible to our methods of proof based on  $p$ -adic deformations of modular forms.

## 1. Introduction

Let  $N \geq 1$  be an odd square-free integer, and let  $S_{2k}(N)$  denote the space of cusp forms of even weight  $2k$  on the Hecke congruence group  $\Gamma_0(N)$ . Following the definitions in [Koh82], we denote by  $S_{k+1/2}^+(4N)$  the space of modular forms that transform like  $\theta(\tau)^{2k+1}$  under the action of  $\Gamma_0(4N)$ , and belong to the *plus space*: this means that they have a Fourier expansion of the form  $\sum_{D>0} c(D)q^D$ , where  $c(D) = 0$  unless

$$D^* := (-1)^k D \equiv 0, 1 \pmod{4}.$$

The spaces  $S_{2k}(N)$  and  $S_{k+1/2}^+(4N)$  are equipped with an action of Hecke operators and with a notion of newforms. (For forms of integral weight, this is classical Atkin–Lehner theory, while for forms of half-integral weight these notions are made precise in [Koh82].) The Hecke operators acting on  $S_{k+1/2}^+(4N)$  are indexed by squares of integers, and the operators  $T_{\ell^2}$ , for  $\ell$  a prime not dividing  $2N$ , preserve the subspace  $S_{k+1/2}^{\text{new}}(4N)$  of newforms.

A basic theorem of Shimura and Kohnen [Koh82, Theorem 2, § 5] states that the spaces  $S_{2k}^{\text{new}}(N)$  and  $S_{k+1/2}^{\text{new}}(4N)$  are isomorphic as Hecke modules. More precisely, if  $f = \sum a_nq^n$  is any normalised newform of weight  $2k$  on  $\Gamma_0(N)$ , there is a newform  $g \in S_{k+1/2}^{\text{new}}(4N)$  that is unique up to scaling and satisfies

$$T_{\ell^2}g = a_{\ell}g, \quad \text{for all primes } \ell \nmid 2N.$$

---

Received 3 December 2007, accepted in final form 20 February 2008.

*2000 Mathematics Subject Classification* 11F67, 11F37, 11F85, 11G40, 14G05.

*Keywords:* modular forms, elliptic curves,  $L$ -series,  $p$ -adic families, Gross–Kohnen–Zagier formula.

The first author was supported by an NSERC discovery grant and by CICMA, and the second author was supported by CICMA and a post-doctoral fellowship at the Centre de Recherches Mathematiques (CRM) in Montreal.

This journal is © [Foundation Compositio Mathematica](http://www.compositio-mathematica.org/) 2008.

The forms  $f$  and  $g$  are said to be in *Shimura correspondence*. We write

$$g = \sum_{D>0} c(D)q^D$$

for the Fourier expansion of  $g$ .

The Fourier coefficients  $a_\ell$  (for  $\ell$  a prime) of the integral weight eigenform  $f$  can be recovered from those of  $g$  by the rule

$$a_\ell = \begin{cases} \frac{c(D\ell^2)}{c(D)} + \left(\frac{D^*}{\ell}\right)\ell^{k-1} & \text{if } \ell \nmid N, \\ \frac{c(D\ell^2)}{c(D)} & \text{if } \ell \mid N, \end{cases}$$

where  $D$  is any integer for which  $c(D) \neq 0$  (cf. [Koh85, formula (11)]).

The arithmetic significance of the coefficients  $c(D)$  is revealed by the following fundamental formula of Kohlen and Waldspurger (cf. [Koh85, Corollary 1]):

$$|c(D)|^2 = \begin{cases} \lambda_g D^{k-1/2} L(f, D^*, k) & \text{if } (D^*/\ell) = w_\ell \text{ for all } \ell \mid N, \\ 0 & \text{otherwise,} \end{cases} \tag{1}$$

where

- (a) the complex number  $\lambda_g$  is a non-zero scalar that depends only on the choice of  $g$ ,
- (b) the function

$$L(f, D^*, s) = \sum_n a_n \chi_{D^*}(n) n^{-s}$$

is the twisted  $L$ -series attached to  $f$  and the quadratic Dirichlet character  $\chi_{D^*} := \left(\frac{D^*}{\cdot}\right)$  of conductor  $D^*$ , and

- (c) the integers  $w_\ell \in \{\pm 1\}$  are the eigenvalues of the Atkin–Lehner involutions  $W_\ell$  acting on  $f$ .

For example, suppose that  $f$  is of weight 2 and has rational Fourier coefficients, so that it corresponds to an elliptic curve  $E$  over  $\mathbb{Q}$  of conductor  $N$ . The Birch and Swinnerton-Dyer conjecture then predicts that, if  $c(D_1)$  and  $c(D_2)$  are non-zero, we have

$$\frac{c(D_1)}{c(D_2)} = \pm \sqrt{\frac{\#\text{III}(E^{-D_1})}{\#\text{III}(E^{-D_2})}},$$

where  $E^D$  denotes the twist of the elliptic curve  $E$  by the quadratic Dirichlet character attached to  $D$ . In this way, the coefficients of  $g$  package arithmetic information concerning the twists of  $E$ . In particular, once a sign for one of the non-vanishing coefficients  $c(D)$  has been fixed, the remaining coefficients pick out well-defined choices of square roots for  $\#\text{III}(E^{-D})$ . The law that governs the variation of their signs is not well understood.

We remark that the sign  $w(f, D^*) \in \{\pm 1\}$  that appears in the functional equation for  $L(f, D^*, s)$  is equal to

$$w(f, D^*) = (-1)^k \chi_{D^*}(-N) w_N, \quad \text{where } w_N := \prod_{\ell \mid N} w_\ell.$$

In particular,  $w(f, D^*) = 1$  whenever  $D$  satisfies  $\chi_{D^*}(\ell) = w_\ell$  for all  $\ell \mid N$ .

When  $w(f, D^*) = -1$ , the central critical value  $L(f, D^*, k)$  vanishes for parity reasons. It then becomes natural to study the central critical derivative  $L'(f, D^*, k)$ . One of the motivating questions behind the present paper is the following question.

*Question 1.1.* Can the data of  $L'(f, D^*, k)$  (at least for certain  $D$  satisfying  $w(f, D^*) = -1$ ) be packaged into the coefficients of a modular generating series?

Our main result (Theorem 1.5 below) provides an element of answer to this question by relating some of these central critical derivatives to the Fourier coefficients of  $p$ -adic families of modular forms of half-integral weight.

*p-adic families.* Denote by  $\mathbb{C}_p$  the completion of an algebraic closure  $\bar{\mathbb{Q}}_p$  of  $\mathbb{Q}_p$  and fix embeddings of  $\bar{\mathbb{Q}}$  into  $\mathbb{C}_p$  and  $\mathbb{C}$  once and for all. Fix a compact open region  $U \subset \mathbb{Z}_p$ , and let  $\mathcal{A}(U)$  denote the ring of  $\mathbb{C}_p$ -valued  $p$ -adic analytic functions on  $U$ . Given a formal  $q$  series

$$\underline{f} := \sum_{n \geq 0} \underline{a}_n q^n \tag{2}$$

whose coefficients  $\underline{a}_n$  belong to  $\mathcal{A}(U)$ , we will denote by

$$f_k := \underline{f}(k) = \sum_{n \geq 0} \underline{a}_n(k) q^n$$

its specialisation to  $k \in U$ , viewed as a formal power series with coefficients in  $\mathbb{C}_p$ . A point  $k \in U$  is said to be *classical* if

$$k \in \mathbb{Z}^{\geq 1} \quad \text{and} \quad k \equiv 1 \pmod{p-1},$$

and the set of all classical points in  $U$  is denoted by  $U_{\text{cl}}$ .

For the purposes of this paper, a  $p$ -adic family of modular forms on  $\Gamma_0(N)$  is a formal  $q$ -series  $\underline{f}$  as in (2) with the property that  $f_k$  is a classical normalised eigenform of weight  $2k$  on  $\Gamma_0(N)$ , for all  $k \in U_{\text{cl}}$ . This means that the Fourier coefficients of  $f_k$  belong to  $\bar{\mathbb{Q}}$  (and in fact generate a finite extension  $K_{f_k}$  of  $\mathbb{Q}$ ), and that the image of  $f_k$  in  $\mathbb{C}[[q]]$  under the chosen complex embedding  $K_{f_k} \hookrightarrow \mathbb{C}$  is a classical modular form of weight  $2k$  on  $\Gamma_0(N)$ .

Classical examples of  $p$ -adic families of modular forms include the following:

- (a) Eisenstein series of varying weights,

$$E_k := \zeta^*(1-2k) + 2 \sum_{n=1}^{\infty} \sigma_{2k-1}^*(n) q^n,$$

where  $\zeta^*(s) = (1-p^{-s})\zeta(s)$  is the Riemann zeta function with its Euler factor at  $p$  removed, and  $\sigma_{2k-1}^*(n) = \sum_{\substack{d|n \\ (p,d)=1}} d^{2k-1}$ .

- (b) The binary theta series associated to the powers of a fixed Hecke Grossencharacter  $\Psi$  of infinity type  $(1, 0)$  of an imaginary quadratic field  $K$ . These theta series are defined by letting, for all ideals  $a \triangleleft \mathcal{O}_K$  of the ring of integers of  $K$ ,

$$\Psi^*(a) = \begin{cases} \Psi(a) & \text{if } p \nmid a\bar{a}, \\ 0 & \text{otherwise,} \end{cases}$$

and setting

$$\theta_k := \sum_{a \triangleleft \mathcal{O}_K} \Psi^*(a)^{2k-1} q^{a\bar{a}}.$$

A third class of examples arises from a theorem of Hida, which we will now state in a special case.

Assume for this statement that  $f$  is a newform of weight 2 on  $\Gamma_0(N)$ , and fix a prime  $p$  that divides  $N$ . Note that  $p \neq 2$ , since we are assuming  $N$  to be odd.

**PROPOSITION 1.2 (Hida).** *There is a unique  $p$ -adic family  $\underline{f}$  (defined on a suitable neighbourhood  $U$  of  $k = 1$ ) satisfying  $f_1 = f$ .*

This proposition attaches to  $f$  an infinite collection of normalised eigenforms  $f_k$ , of varying weights, indexed by the  $k \in U_{\text{cl}}$ .

We mention in passing that Hida’s theorem is considerably more general than the special case given in Proposition 1.2. For instance,  $f$  could be an eigenform of arbitrary weight, and the condition  $p \mid N$  could have been relaxed to the assumption that  $f$  be *ordinary* at  $p$ . However, Proposition 1.2 is the only case that is germane to the concerns of this paper.

For classical points  $k > 1$ , the modular form  $f_k$  obtained from Proposition 1.2 is *not* new at  $p$ . This is because  $f_k$  is ordinary at  $p$ , i.e. of slope 0, while newforms of level  $N$  and weight  $2k$  have slope  $k - 1$ .

More precisely, writing  $N = pM$ , there is a unique normalised newform  $f_k^\sharp$  in  $S_{2k}(M)$  satisfying

$$T_\ell(f_k^\sharp) = \underline{a}_\ell(k)f_k^\sharp, \quad \text{for all primes } \ell \text{ with } (\ell, N) = 1.$$

Let

$$g_k = \sum_{D>0} c(D, k)q^D$$

denote the (unique, up to scaling) eigenform in  $S_{k+1/2}^+(4M)$  that is associated to  $f_k^\sharp$  by the Shimura–Kohnen correspondence, and let  $g = g_1$  be the newform in  $S_{3/2}^+(4N)$  associated to  $f$ .

It is crucial for our main result that the half-integral weight forms  $g_k$  have, *a priori*, ‘twice as many’ non-vanishing Fourier coefficients as the modular form  $g$ . The values of  $D$  for which  $c(D, k)$  need not vanish can be divided into two categories:

- (I) the  $D$  for which  $\chi_{-D}(\ell) = w_\ell$ , for all  $\ell$  dividing  $N$ ;
- (II) the  $D$  for which

$$\begin{cases} \chi_{-D}(\ell) = w_\ell & \text{for all } \ell \mid M, \\ \chi_{-D}(p) = -w_p; \end{cases}$$

for these  $D$ , we have  $c(D) = 0$ ; furthermore,  $L(f, -D, 1) = 0$ , because  $w(f, -D) = -1$ .

We will call discriminants  $-D$  of the first type *type I discriminants*, and those of the second type, *type II discriminants*.

Since the functions  $k \mapsto \underline{a}_n(k)$  on  $U_{\text{cl}}$  extend to analytic functions on  $U$ , it is natural to expect a similar principle for the functions  $k \mapsto c(D, k)$ . The fact that the individual forms  $g_k$  are only defined up to a non-zero scaling factor makes it necessary to introduce a normalisation. We do this by fixing a type I discriminant  $-\Delta_0$  for which  $c(\Delta_0) \neq 0$ . A theorem of Hida and Stevens (cf. [Ste94, Theorem 5.5 and Lemma 6.1]) then gives the following result.

**PROPOSITION 1.3.** *There is a  $p$ -adic neighbourhood of  $k = 1$  in  $U$  on which  $c(\Delta_0, k)$  is everywhere non-vanishing. After replacing  $U$  by such a neighbourhood, the normalised coefficient attached to  $k \in U_{\text{cl}} \cap \mathbb{Z}^{>1}$  by*

$$\tilde{c}(D, k) = \frac{(1 - (-D/p)\underline{a}_p(k)^{-1}p^{k-1})c(D, k)}{(1 - (-\Delta_0/p)\underline{a}_p(k)^{-1}p^{k-1})c(\Delta_0, k)} = \frac{c(p^2D, k)}{c(p^2\Delta_0, k)}$$

*extends to a  $p$ -adic analytic function on  $U$ , which satisfies*

$$\tilde{c}(D, 1) = \frac{c(p^2D)}{c(p^2\Delta_0)} = \frac{c(D)}{c(\Delta_0)}.$$

In particular, if  $-D$  is a type II discriminant, then  $c(D) = 0$  and hence  $\tilde{c}(D, 1) = 0$ . It then becomes natural to consider the derivative of  $\tilde{c}(D, k)$  with respect to  $k$  at  $k = 1$ .

We note in passing that the vanishing of the coefficient  $\tilde{c}(D, 1)$  when  $D$  is of type II can be traced to two different causes. Firstly, the Euler factor appearing in the numerator of  $\tilde{c}(D, k)$  vanishes at  $k = 1$ . Viewed in this light, the identity  $\tilde{c}(D, 1) = 0$  is an instance of the ‘exceptional zero phenomenon’ for  $p$ -adic  $L$ -functions that was first explored in [MTT86]. Secondly, it follows from the properties of the Shimura–Kohlen lift that the classical coefficients  $c(D, 1)$  also vanish. Theorem 1.5 leads to the conclusion that  $\tilde{c}(D, k)$  frequently vanishes to order 1 at  $k = 1$ . This is not in contradiction with the factorisation of  $\tilde{c}(D, k)$  appearing in Proposition 1.3, since the individual factors that appear there are not  $p$ -adic analytic functions of  $k$ .

Assume now, for simplicity, that the newform  $f \in S_2(N)$  has rational Fourier coefficients, so that it corresponds to an elliptic curve  $E$  of conductor  $N$ . Since  $p$  divides  $N$  exactly, the curve  $E$  has (split or non-split) multiplicative reduction at  $p$ . Let

$$\Phi_{\text{Tate}} : \mathbb{C}_p^\times / q^\mathbb{Z} \longrightarrow E(\mathbb{C}_p)$$

be Tate’s  $p$ -adic uniformisation of  $E$ , and let

$$\log_E : E(\mathbb{C}_p) \longrightarrow \mathbb{C}_p$$

be the  $p$ -adic formal group logarithm, which can be defined by

$$\log_E(P) = \log_q(\Phi_{\text{Tate}}^{-1}(P)),$$

where  $\log_q$  is the branch of the  $p$ -adic logarithm that vanishes on  $q^\mathbb{Z}$ . We extend this logarithm to  $E(\mathbb{C}_p) \otimes \mathbb{Q}$  by  $\mathbb{Q}$ -linearity.

Let  $E(\mathbb{Q}(\sqrt{-D}))^-$  denote the submodule of  $E(\mathbb{Q}(\sqrt{-D}))$  on which the non-trivial involution in  $\text{Gal}(\mathbb{Q}(\sqrt{-D})/\mathbb{Q})$  acts as  $-1$ . When  $-D$  is a type II discriminant, we have

$$\chi_{-D}(p) = -w_p = a_p,$$

and hence the quadratic twist  $E^{-D}$  of  $E$  over  $\mathbb{Q}(\sqrt{-D})$  has split multiplicative reduction at  $p$ .

LEMMA 1.4. *If  $P$  belongs to  $E(\mathbb{Q}(\sqrt{-D}))^-$ , then*

$$\log_E(P) \text{ belongs to } \mathbb{Q}_p.$$

*Proof.* The Tate uniformisation induces a homomorphism

$$\Phi_{\text{Tate}} : (\mathbb{Q}_p^{\text{nr}})^\times / q^\mathbb{Z} \longrightarrow E(\mathbb{Q}_p^{\text{nr}}),$$

where  $\mathbb{Q}_p^{\text{nr}}$  is the maximal unramified extension of  $\mathbb{Q}_p$ . Let  $\sigma$  be the Frobenius element in  $\text{Gal}(\mathbb{Q}_p^{\text{nr}}/\mathbb{Q}_p)$ . Then for all points  $P \in E(\mathbb{Q}(\sqrt{-D}))^-$ , we have:

- (i)  $P^\sigma = \chi_{-D}(p)P = a_pP$ , and
- (ii)  $\Phi_{\text{Tate}}^{-1}(P^\sigma) = a_p\Phi_{\text{Tate}}^{-1}(P)^\sigma$ .

It follows that  $\log_E(P)^\sigma = \log_E(P)$ , and the lemma follows. □

One of the main theorems of this paper is as follows.

THEOREM 1.5. *Let  $-D$  be a discriminant of type II. There is an element  $P_D \in E(\mathbb{Q}(\sqrt{-D}))^- \otimes \mathbb{Q}$  satisfying:*

- (i)  $\frac{d}{dk}\tilde{c}(D, k)_{k=1} = \log_E(P_D)$ ;
- (ii)  $P_D \neq 0$  if and only if  $L'(E, -D, 1) \neq 0$ .

Although the points  $P_D$  only belong to  $E(\mathbb{Q}(\sqrt{-D})) \otimes \mathbb{Q}$ , the proof of Theorem 1.5 will show that the collection  $\{P_D\}$  has bounded denominators: there exists an integer  $t_E$ , depending on  $E$  but

not on the type II discriminant  $-D$ , such that

$$t_E P_D \text{ belongs to } E(\mathbb{Q}(\sqrt{-D}))^-.$$

These global points, which are defined over a varying collection of quadratic fields, display an *a priori* unexpected coherence, which can be summarised by letting  $\epsilon$  be a first-order infinitesimal (satisfying  $\epsilon^2 = 0$ ) and considering the formal  $q$ -series with coefficients in  $\mathbb{Q}_p(\epsilon)$ :

$$g_{1+\epsilon} := \left( \sum_{-D \text{ of type I}} \tilde{c}(D)q^D \right) + \epsilon \left( \sum_{-D \text{ of type II}} \log_E(P_D)q^D \right).$$

Theorem 1.5 amounts to the statement that  $g_{1+\epsilon}$  is a ‘modular form of weight  $(3/2 + \epsilon)$ ’ associated to the Hida family  $\underline{f}$  (or rather, to its specialisation to a first-order neighbourhood of weight 2) under the Shimura correspondence.

The proof of Theorem 1.5 rests on two ingredients.

- (i) A formula of Kohnen expressing the products  $c(D_1, k)c(D_2, k)$  of Fourier coefficients of  $g_k$  in terms of certain *geodesic cycles integrals* associated to  $f_k^\sharp$  and to binary quadratic forms of discriminant  $D_1 D_2$ .
- (ii) The theory of *Stark–Heegner points*, which relates these period integrals to global points defined (conjecturally, in general) over ring class fields of real quadratic fields.

Sections 2 and 3 review these ingredients in turn. Section 4 describes the proof of Theorem 1.5. This proof suggests studying generating series whose coefficients are built out of Stark–Heegner points, in the spirit of the Gross–Kohnen–Zagier formula of [GKZ87] relating classical Heegner points to coefficients of modular forms of weight  $3/2$ . Several theorems of ‘Gross–Kohnen–Zagier type’ are formulated and proved in § 5. This section also formulates a more general Gross–Kohnen–Zagier conjecture for Stark–Heegner points which in some cases falls squarely outside the scope of the methods of this paper based on exploiting  $p$ -adic deformations of modular forms. Some of the cases of the Gross–Kohnen–Zagier conjecture for which a proof eludes us are discussed further in § 6, and some numerical evidence for them is provided.

## 2. Kohnen’s formula

In this section, and this section only, let  $f$  be a normalised newform of weight  $2k$  on  $\Gamma_0(M)$ , and let  $g = \sum_D c(D)q^D$  be the newform in  $S_{k+1/2}(4M)$  that is attached to it under the Shimura–Kohnen correspondence.

Our purpose is to briefly recall a theorem of Kohnen that expresses the product  $c(D_1)c(D_2)$  of two Fourier coefficients of  $g$  in terms of *Shintani cycles*, which we proceed to describe, following the treatment in [Koh85].

If  $c(D_1)$  and  $c(D_2)$  are non-zero, then  $D_1^*$  and  $D_2^*$  are discriminants of orders in a quadratic field, satisfying

$$\chi_{D_1^*}(\ell) = \chi_{D_2^*}(\ell) = w_\ell, \quad \text{for all } \ell \mid M, \tag{3}$$

by the definition of Kohnen’s plus space. Assume for simplicity that  $D_1^*$  and  $D_2^*$  are both fundamental and prime to  $2M$ . Then the product  $\Delta := D_1^* D_2^*$  is the discriminant of an order in a real quadratic field  $K$ , or of an order in the split quadratic algebra  $\mathbb{Q} \times \mathbb{Q}$  if  $D_1^* = D_2^*$ . Note that all the  $\ell \mid M$  are split in  $K$ . In particular, it is possible to choose an integer  $\delta$  such that

$$\delta^2 \equiv \Delta \pmod{4M}.$$

A primitive binary quadratic form  $Q(x, y) = Ax^2 + Bxy + Cy^2$  of discriminant  $\Delta$  is said to be a *Heegner form* (relative to the level  $M$ ) if

$$M \mid A, \quad B \equiv \delta \pmod{M}.$$

Let  $C_Q$  be the image in  $\Gamma_0(M) \backslash \mathcal{H}$  of the geodesic in the Poincaré upper half-plane consisting of the complex numbers  $z = x + iy$  satisfying

$$A|z|^2 + Bx + C = 0,$$

oriented from left to right if  $A > 0$ , from right to left if  $A < 0$ , and from  $-C/B$  to  $i\infty$  if  $A = 0$ . For example, if  $\Delta$  is not a perfect square, let

$$r + s\sqrt{\Delta} \tag{4}$$

be the fundamental unit of norm 1 in  $\mathcal{O}_\Delta := \mathbb{Z}[(\Delta + \sqrt{\Delta})/2]$ , normalised so that  $r, s > 0$ . Then the path  $C_Q$  is equivalent to the path from  $\tau$  to  $\gamma_Q\tau$ , where

$$\gamma_Q = \begin{pmatrix} r + sB & 2Cs \\ -2As & r - sB \end{pmatrix} \in \Gamma_0(M) \tag{5}$$

is a generator for the stabiliser subgroup of  $Q$  in  $\Gamma_0(M)$ , and  $\tau \in \mathcal{H}$  is any base point.

To each indefinite quadratic form  $Q$  is associated the Shintani cycle

$$r(f, Q) = \int_{C_Q} f(z)Q(z, 1)^{k-1} dz. \tag{6}$$

Note that  $r(f, Q)$  depends only on the  $\Gamma_0(M)$ -equivalence class of  $Q$ .

Let

$$\mathcal{F}_\Delta = \{\text{Heegner forms } Ax^2 + Bxy + Cy^2 \text{ of discriminant } \Delta\}.$$

This set of binary quadratic forms is preserved under the usual right action of  $\Gamma_0(M)$ . Define a function

$$\omega_{D_1^*, D_2^*} : \mathcal{F}_\Delta / \Gamma_0(M) \longrightarrow \pm 1$$

by the rule

$$\omega_{D_1^*, D_2^*}(Q) = \begin{cases} 0 & \text{if } \gcd(a, b, c, D_1) > 1, \\ (D_1^*/Q(m, n)) & \text{where } \gcd(Q(m, n), D_1) = 1, \text{ otherwise.} \end{cases}$$

Genus theory shows that  $\omega_{D_1^*, D_2^*}$  is well defined, and that it is a quadratic character on the class group of primitive binary quadratic forms of discriminant  $\Delta$ . This character cuts out the biquadratic field  $\mathbb{Q}(\sqrt{D_1^*}, \sqrt{D_2^*})$ , an unramified quadratic extension of  $\mathbb{Q}(\sqrt{\Delta})$ .

The Shintani cycle associated to the pair  $(D_1^*, D_2^*)$  is defined by the formula

$$r(f, D_1^*, D_2^*) = \sum_{Q \in (\mathcal{F}_\Delta / \Gamma_0(M))} \omega_{D_1^*, D_2^*}(Q) r(f, Q). \tag{7}$$

The following theorem of Kohlen (cf. [Koh85, Theorem 3]) plays a key role in this paper.

**THEOREM 2.1.** *For all  $D_1$  and  $D_2$  satisfying (3), we have*

$$\frac{c(D_1)\overline{c(D_2)}}{\langle g, g \rangle} = (-1)^{[k/2]} 2^k \times \frac{r(f, D_1^*, D_2^*)}{\langle f, f \rangle}.$$

### 3. Stark–Heegner points

For this section, we revert to the notation that was in use in the statement of Theorem 1.5 of the introduction. Thus, in particular,  $f$  is now a newform of weight 2 and level  $N = pM$  associated to an elliptic curve  $E$  of conductor  $N$ .



Let  $\Delta$  be a fundamental discriminant satisfying

$$\Delta > 0, \quad \chi_\Delta(p) = -1, \quad \chi_\Delta(\ell) = 1, \quad \text{for all } \ell \mid M. \tag{8}$$

The article [Dar01] (see also [BD08] and [Dar06]) introduces a conjectural  $p$ -adic variant of the Heegner point construction, associating to every equivalence class of binary quadratic forms of discriminant  $\Delta$  a  $p$ -adic point in  $E(\overline{\mathbb{Q}}_p)$ . These local points are called *Stark–Heegner points* in [Dar01], and are predicted to be defined over ring class fields of  $K = \mathbb{Q}(\sqrt{\Delta})$ .

We will have no need for the original definition given in [Dar01] based on the modular symbols attached to  $f$ . Rather, we will recall here an alternative description exploited in [BD08] that relies on the  $p$ -adic family  $\underline{f}_k$  and the classical newforms  $f_k^\sharp$  attached to  $f$  by Hida’s Proposition 1.2.

For each eigenform  $f_k$  with  $k \in U_{\text{cl}}$ , we begin by considering the complex period integrals

$$I_{\mathbb{C}}(f_k, P, r, s) := \int_r^s f_k(z)P(z) dz, \tag{9}$$

where  $P(z) \in \mathbb{Q}[z]^{[2k-2]}$  is a polynomial of degree at most  $2k - 2$ , and  $r, s$  are elements of  $\mathbb{P}_1(\mathbb{Q})$  viewed as subsets of the extended Poincaré upper half-plane  $\mathcal{H}^*$ . The integral (9) converges because  $f_k$  is a cusp form. Note that in order to define  $I_{\mathbb{C}}(f_k, P, r, s)$  we use the chosen complex embedding  $K_{f_k} \hookrightarrow \mathbb{C}$ , so that  $f_k$  can be viewed as a complex analytic function on  $\mathcal{H}^*$ .

Let

$$\begin{aligned} I_{\mathbb{C}}^+(f_k, P, r, s) &:= \text{Real}(I_{\mathbb{C}}(f_k, P, r, s)), \\ I_{\mathbb{C}}^-(f_k, P, r, s) &:= \text{Imag}(I_{\mathbb{C}}(f_k, P, r, s)). \end{aligned}$$

The following theorem of Shimura gives a rationality property for these complex numbers.

PROPOSITION 3.1 (Shimura). *There exist periods  $\Omega_k^+, \Omega_k^- \in \mathbb{C}^\times$  depending only on  $f_k$ , for which*

$$I^\pm(f_k, P, r, s) := \frac{1}{\Omega_k^\pm} I_{\mathbb{C}}^\pm(f_k, P, r, s)$$

*belongs to  $K_{f_k}$ , for all  $P \in \mathbb{Q}[z]^{[2k-2]}$ , and  $r, s \in \mathbb{P}_1(\mathbb{Q})$ .*

It will lighten the notation to fix a choice of sign  $\epsilon = \{1, -1\}$  and set

$$I(f_k, P, r, s) := I^\epsilon(f_k, P, r, s), \quad \Omega_k := \Omega_k^\epsilon. \tag{10}$$

For the proof of Theorem 1.5, it is only the value  $\epsilon = -1$  that is relevant, so the reader may assume throughout §§ 3 and 4 that  $\epsilon = -1$ . However, the possibility to choose  $\epsilon = 1$  allows a more general definition of Stark–Heegner points, which will be crucial in the theorems, conjectures and numerical experiments described in §§ 5 and 6.

The identification of the complex number  $I(f_k, P, r, s)$  with an element of  $K_{f_k}$  is made via the same complex embedding of  $K_{f_k}$  that was used to define  $I_{\mathbb{C}}(f_k, P, r, s)$ . Recall that we have fixed an embedding of  $\overline{\mathbb{Q}}$  into  $\mathbb{C}_p$ . Thanks to this embedding we can, and will, view the integrals  $I(f_k, P, r, s)$  as elements of  $\mathbb{C}_p$ . We can then extend their definition to  $P \in \mathbb{C}_p[z]^{[2k-2]}$  by  $\mathbb{C}_p$ -linearity.

Let  $\mathbb{Q}_{p^2} \subset \mathbb{C}_p$  be the quadratic unramified extension of  $\mathbb{Q}_p$ , let  $\mathcal{O}_{p^2}$  be its ring of integers, and let

$$\mathcal{H}_p^0 := \{\tau \in \mathcal{O}_{p^2} \text{ such that } \tau \not\equiv 0, 1, \dots, p-1 \pmod{p}\}.$$

We now invoke the following theorem of Stevens, which asserts that the quantities  $I(f_k, P, r, s)$  can in some sense be  $p$ -adically interpolated.

PROPOSITION 3.2 (Stevens). *After eventually replacing the region  $U$  by a smaller  $p$ -adic neighbourhood of 1, the complex periods  $\Omega_k$  can be chosen in such a way that:*



- (i) the function  $k \mapsto I(f_k, (z - \tau)^{2k-2}, r, s)$  extends to an analytic function of  $k \in U$ , for all  $\tau \in \mathcal{H}_p^0$ , and all  $r, s \in \mathbb{P}_1(\mathbb{Q})$ ;
- (ii) the function  $(r, s) \mapsto I(f_1, 1, r, s)$  takes its values in  $\mathbb{Q}$  and is not identically 0.

*Proof.* This theorem is stated in [BD08, Theorem 2.2.1]. In fact a more precise version is stated there, and since the statement will be used later, we recall it briefly here. Let  $(\mathbb{Z}_p^2)'$  denote the set of primitive vectors in  $\mathbb{Z}_p^2$ , i.e. the vectors that are not divisible by  $p$ . Given a polynomial  $P \in \mathbb{Q}[z]^{[2k-2]}$ , write  $\tilde{P}(x, y)$  for its homogenisation of degree  $2k - 2$ . (Note in particular that  $\tilde{P}(x, y)$  depends on  $k$ .) Theorem 2.2.1 of [BD08] asserts the existence, for each  $r, s \in \mathbb{P}_1(\mathbb{Q})$ , of a suitable  $p$ -adic distribution  $\mu_{r,s}$  on  $(\mathbb{Z}_p^2)'$  of total measure 0, satisfying

$$I(f_k, P, r, s) = \int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} \tilde{P}(x, y) d\mu_{r,s}(x, y), \quad \text{for all } k \in U_{\text{cl}}. \tag{11}$$

This completes the proof. □

For the most part, it is only the existence of the periods  $\Omega_k$  and the distributions  $\mu_{r,s}$  that will be used. Of course, the periods  $\Omega_k$  are far from unique, but if  $\{\Omega_k\}$  and  $\{\Omega'_k\}$  are any two choices, then

$$\Omega'_k = \lambda(k)\Omega_k,$$

where  $\lambda$  extends to an analytic function on  $U$  satisfying  $\lambda(1) \in \mathbb{Q}^\times$ . All the statements that will be made concerning the periods  $I(f_k, P, r, s)$  will be insensitive to a change in  $\lambda$ .

It is nonetheless useful to make a precise choice of periods  $\{\Omega_k\}_{k \in U_{\text{cl}}}$  satisfying the conclusion of Proposition 3.2. This can be done in terms of the periods of (7) thanks to the following lemma.

LEMMA 3.3. *Let  $\Delta_0$  be a fundamental discriminant satisfying*

$$\chi_{\Delta_0}(p) = w_p, \quad L(f, \Delta_0, 1) \neq 0.$$

*Assume that  $\Delta_0$  is positive if the sign  $\epsilon$  in (10) is 1, and that it is negative if  $\epsilon = -1$ . Then there exists a  $p$ -adic neighbourhood  $U$  of  $k = 1$  such that*

$$\Omega_k := r(f_k, \Delta_0, \Delta_0) = (1 - \chi_{\Delta_0}(p)\underline{a}_p(k)^{-1}p^{k-1})^2 r(f_k^\sharp, \Delta_0, \Delta_0) \tag{12}$$

*is non-zero for all  $k \in U_{\text{cl}}$ . Furthermore, this choice of  $\Omega_k$  satisfies the conclusion of Proposition 3.2.*

*Proof.* Proposition 3.2 implies that  $r(f_k, \Delta_0, \Delta_0)$  has all the required properties, provided that it is non-zero. A formula of Birch and Manin expresses  $r(f, \Delta_0, \Delta_0)$  as a non-zero multiple of  $L(f, \Delta_0, 1)$  (cf. for example the last equation on page 241 of [Koh85]). The result follows. □

We next define the periods  $I(f_k^\sharp, P, r, s) \in \mathbb{C}_p$  as in Proposition 3.1, but with  $f_k$  replaced by  $f_k^\sharp$ . (In particular, we use the same choice of complex periods  $\Omega_k$  that was made to define  $I^\pm(f_k, P, r, s)$ .)

Finally, we ‘regularize’ these periods by setting, for all  $k \in U_{\text{cl}}$ ,

$$J(f_k^\sharp, P, r, s) := (1 - \underline{a}_p(k)^{-2}p^{2k-2})I(f_k^\sharp, P, r, s). \tag{13}$$

PROPOSITION 3.4. *For all  $\tau \in \mathcal{H}_p^0$  and all  $r, s \in \mathbb{P}_1(\mathbb{Q})$ , the function*

$$k \mapsto J(f_k^\sharp, (z - \tau)^{2k-2}, r, s)$$

*extends to a  $p$ -adic analytic function of  $k$  that vanishes at  $k = 1$ .*

*Proof.* This follows from [BD08, Proposition 2.2.3]. This proposition also expresses  $J(f_k^\sharp, P, r, s)$  in terms of the distributions  $\mu_{r,s}$  alluded to in (11). More precisely,

$$J(f_k^\sharp, P, r, s) = \int_{(\mathbb{Z}_p^2)'} \tilde{P}(x, y) d\mu_{r,s}(x, y). \tag{14}$$

Proposition 3.4 then follows from the fact that  $P = (z - \tau)^{2k-2}$  is a continuous function on the compact space  $(\mathbb{Z}_p^2)'$  and is analytic as a function of  $k$ . The fact that  $\mu_{r,s}$  has total measure zero thus implies that the function  $k \mapsto J(f_k^\sharp, (z - \tau)^{2k-2}, r, s)$  vanishes at  $k = 1$ . Alternatively, note that the Euler factor in (13) vanishes at  $k = 1$  since  $\underline{a}_p(1)^2 = 1$ .  $\square$

Recall the set  $\mathcal{F}(\Delta)$  of Heegner forms of discriminant  $\Delta$  attached to the level  $M$ . In order to define this set, we had to choose a square root  $\delta$  of  $\Delta$  modulo  $M$ . We now choose a square root of  $\Delta$  in  $\mathbb{C}_p$ , which we will simply denote by  $\sqrt{\Delta}$ . For  $Q = [A, B, C] \in \mathcal{F}(\Delta)$ , let

$$\tau_Q := \frac{-B + \sqrt{\Delta}}{2A}$$

be a root of  $Q(z, 1) = 0$ . Assumption (8) implies that this element belongs to  $\mathcal{H}_p^0$ , for all  $Q \in \mathcal{F}(\Delta)$ . Recall the matrix  $\gamma_Q$  defined in (5). We now choose an arbitrary base point  $r \in \mathbb{P}_1(\mathbb{Q})$  and define

$$J(f, Q) = \frac{d}{dk}(J(f_k^\sharp, (z - \tau_Q)^{2k-2}, r, \gamma_Q r))_{k=1}. \tag{15}$$

The following lemma collects some of the basic properties of the invariants  $J(f, Q)$ .

LEMMA 3.5. (a) *The expression  $J(f, Q)$  does not depend on the  $r \in \mathbb{P}_1(\mathbb{Q})$  that was chosen to define it.*

(b) *The function  $Q \mapsto J(f, Q)$  depends only on the image of  $Q$  in the class group  $\mathcal{F}_\Delta/\Gamma_0(M)$ .*

(c) *The element  $J(f, Q)$  belongs to the quadratic unramified extension  $\mathbb{Q}_{p^2}$  of  $\mathbb{Q}_p$ . If  $x \mapsto \bar{x}$  denotes the non-trivial automorphism of this field, then*

$$J(f, Q) + \overline{J(f, Q)} = 2 \frac{d}{dk}(\tilde{r}(f_k^\sharp, Q)),$$

where

$$\tilde{r}(f_k^\sharp, Q) = \frac{1}{\Omega_k} \times (1 - \underline{a}_p(k)^{-2} p^{2k-2}) r(f_k^\sharp, Q),$$

and  $r(f_k^\sharp, Q)$  is the invariant defined in (6).

*Proof.* (a) A direct calculation shows that  $(az + b) - (cz + d)\tau_Q = \epsilon(z - \tau_Q)$ , where

$$\gamma_Q = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

and  $\epsilon$  is the fundamental unit of the order of discriminant  $\Delta$ , as in (4). It follows that

$$(\gamma_Q z - \tau_Q)^{2k-2} = \left(\frac{\epsilon}{cz + d}\right)^{2k-2} (z - \tau_Q)^{2k-2}.$$

Since we have  $\gamma_Q \in \Gamma_0(M)$ , and using the fact that  $f_k^\sharp$  is modular for  $\Gamma_0(M)$ , we get

$$\begin{aligned} I_{\mathbb{C}}(f_k^\sharp, (z - \tau_Q)^{2k-2}, \gamma_Q r, \gamma_Q s) &= \int_{\gamma_Q r}^{\gamma_Q s} f_k^\sharp(z) (z - \tau_Q)^{2k-2} dz \\ &= \int_r^s f_k^\sharp(\gamma_Q z) (\gamma_Q z - \tau_Q)^{2k-2} d\gamma_Q z \\ &= \int_r^s (cz + d)^{2k} f_k^\sharp(z) \left(\frac{\epsilon}{cz + d}\right)^{2k-2} (z - \tau_Q)^{2k-2} \frac{dz}{(cz + d)^2} \\ &= \epsilon^{2k-2} I_{\mathbb{C}}(f_k^\sharp, (z - \tau_Q)^{2k-2}, r, s). \end{aligned}$$

From this it follows immediately that

$$\begin{aligned} & J(f_k^\sharp, (z - \tau_Q)^{2k-2}, r, \gamma_Q r) - J(f_k^\sharp, (z - \tau_Q)^{2k-2}, s, \gamma_Q s) \\ &= J(f_k^\sharp, (z - \tau_Q)^{2k-2}, r, s) - J(f_k^\sharp, (z - \tau_Q)^{2k-2}, \gamma_Q r, \gamma_Q s) \\ &= (1 - \epsilon^{2k-2}) J(f_k^\sharp, (z - \tau_Q)^{2k-2}, r, s), \end{aligned}$$

where we can view  $\epsilon$  as an element of  $\mathbb{Q}_p^\times$ . The expression on the right is a product of two  $p$ -adic analytic functions that vanish at  $k = 1$ , and hence vanishes to order at least 2 at  $k = 1$ . Part (a) follows.

As for part (b), let  $Q' = Q\alpha$ , where

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

A direct calculation then shows that

$$J(f_k^\sharp, Q', \alpha^{-1}r, \gamma_{Q'}\alpha^{-1}r) = (c\tau_Q + d)^{2k-2} J(f_k^\sharp, Q, r, \gamma_Q r).$$

Part (b) now follows from the fact that  $(c\tau + d)^{2k-2}$  is a  $p$ -adic analytic function of  $k \in U$  that is equal to 1 at  $k = 1$ .

To prove part (c), we first remark that, by (15),

$$J(f, Q) + \overline{J(f, Q)} = \frac{d}{dk} (J(f_k^\sharp, (z - \tau_Q)^{2k-2}, r, \gamma_Q r) + J(f_k^\sharp, (z - \overline{\tau_Q})^{2k-2}, r, \gamma_Q r))_{k=1}.$$

By (14), the right-hand side of this equation can be rewritten as:

$$\begin{aligned} & \frac{d}{dk} \left( \int_{(\mathbb{Z}_p^2)'} (x - \tau_Q y)^{2k-2} + (x - \overline{\tau_Q} y)^{2k-2} d\mu_{r, \gamma_Q r}(x, y) \right)_{k=1} \\ &= 2 \left( \int_{(\mathbb{Z}_p^2)'} (\log_p(x - \tau_Q y) + \log_p(x - \overline{\tau_Q} y)) d\mu_{r, \gamma_Q r}(x, y) \right) \\ &= 2 \left( \int_{(\mathbb{Z}_p^2)'} (\log_p A + \log_p(x - \tau_Q y) + \log_p(x - \overline{\tau_Q} y)) d\mu_{r, \gamma_Q r} \right) \\ &= 2 \left( \int_{(\mathbb{Z}_p^2)'} \log_p \tilde{Q}(x, y) d\mu_{r, \gamma_Q r}(x, y) \right), \end{aligned}$$

where we have used the fact that  $\mu_{r,s}((\mathbb{Z}_p^2)') = 0$  in deriving the penultimate equality. We can rewrite this last expression as

$$\begin{aligned} J(f, Q) + \overline{J(f, Q)} &= 2 \frac{d}{dk} \left( \int_{(\mathbb{Z}_p^2)'} \tilde{Q}(x, y)^{k-1} d\mu_{r, \gamma_Q r}(x, y) \right)_{k=1} \\ &= 2 \frac{d}{dk} (J(f_k^\sharp, Q^{k-1}, r, \gamma_Q r))_{k=1} \\ &= 2 \frac{d}{dk} ((1 - \underline{a}_p(k)^{-2} p^{2k-2}) I(f_k^\sharp, Q^{k-1}, r, \gamma_Q r))_{k=1} \\ &= 2 \frac{d}{dk} \left( \frac{1}{\Omega_k} \times (1 - \underline{a}_p(k)^{-2} p^{2k-2}) r(f_k^\sharp, Q) \right)_{k=1}, \end{aligned}$$

where the third equality follows from (13). The result now follows from the definition of  $\tilde{r}(f_k^\sharp, Q)$ .  $\square$

Thanks to part (b) of Lemma 3.5, we can attach to any factorisation of  $\Delta$  as a product  $D_1D_2$  of two fundamental discriminants, the invariants

$$\begin{aligned} \tilde{r}(f_k^\sharp, D_1, D_2) &= \sum_{Q \in \mathcal{F}_\Delta/\Gamma_0(M)} \omega_{D_1, D_2}(Q) \tilde{r}(f_k^\sharp, Q), \\ J(f, D_1, D_2) &= \sum_{Q \in \mathcal{F}_\Delta/\Gamma_0(M)} \omega_{D_1, D_2}(Q) J(f, Q), \end{aligned}$$

where  $\omega_{D_1, D_2}$  is the genus character that was introduced in § 2. We assume in this definition that the sign  $\epsilon$  of (10) has been chosen to be 1 if  $D_1$  and  $D_2$  are positive, and  $-1$  if they are both negative.

Note that, for any pair  $(D_1, D_2)$  of fundamental discriminants occurring in a factorisation of  $\Delta$ , we necessarily have

$$D_1D_2 > 0, \quad \chi_{D_1}(p) = -\chi_{D_2}(p), \quad \chi_{D_1}(\ell) = \chi_{D_2}(\ell), \quad \text{for all } \ell \mid M.$$

In particular, the signs in the functional equations for the twisted  $L$ -series  $L(f, D_1, s)$  and  $L(f, D_2, s)$  are *opposite*. By interchanging  $D_1$  and  $D_2$  if necessary, assume that

$$w(f, D_1) = 1, \quad w(f, D_2) = -1.$$

It is not hard to see that  $J(f, D_1, D_2)$  is in an eigenspace for the non-trivial automorphism in  $\text{Gal}(\mathbb{Q}_{p^2}/\mathbb{Q}_p)$ . More precisely, we have

$$\overline{J(f, D_1, D_2)} = \begin{cases} J(f, D_1, D_2) & \text{if } \chi_{D_2}(p) = -w_p, \\ -J(f, D_1, D_2) & \text{if } \chi_{D_2}(p) = w_p. \end{cases} \tag{16}$$

We can now recall the following conjecture on ‘Stark–Heegner points’ that is formulated in [BD08].

CONJECTURE 3.6. *Let  $H$  be the ring class field associated to the order  $\mathbb{Z}[(\Delta + \sqrt{\Delta})/2]$  of  $K = \mathbb{Q}(\sqrt{\Delta})$ .*

- (a) *For each  $Q \in \mathcal{F}_\Delta/\Gamma_0(M)$ , there exists  $P_Q \in E(H) \otimes \mathbb{Q}$  such that  $J(f, Q) = \log_E(P_Q)$ .*
- (b) *There is a global point  $P(f, D_1, D_2) \in E(\mathbb{Q}(\sqrt{D_2}))^- \otimes \mathbb{Q}$  such that*

$$J(f, D_1, D_2) = \log_E(P(f, D_1, D_2)).$$

Furthermore,  $P(f, D_1, D_2)$  is of infinite order if and only if

$$L'(E/\mathbb{Q}(\sqrt{\Delta}), \omega_{D_1, D_2}, 1) = L(f, D_1, 1) L'(f, D_2, 1)$$

is non-zero.

While Conjecture 3.6 appears difficult, we have been able to prove the following special case, which will play a key role in the proof of Theorem 1.5.

THEOREM 3.7. *Assume that:*

- (a) *the level  $N$  is divisible by at least two primes;*
- (b) *we have  $\chi_{D_2}(p) = -w_p$  (so that in particular  $J(f, D_1, D_2)$  belongs to  $\mathbb{Q}_p$ ).*

Then:

- (i) *we have*

$$J(f, D_1, D_2) = \log_E(P(f, D_1, D_2)),$$

for some element  $P(f, D_1, D_2) \in E(\mathbb{Q}(\sqrt{D_2}))^- \otimes \mathbb{Q}$ ;

- (ii) *there exists an integer  $t_E$ , depending on  $E$  but not on  $(D_1, D_2)$ , such that  $t_E P(f, D_1, D_2)$  belongs to  $E(\mathbb{Q}(\sqrt{D_2}))^-$ ;*

(iii) the invariant  $P(f, D_1, D_2)$  corresponds to a point of infinite order if and only if

$$L'(E/\mathbb{Q}(\sqrt{\Delta}), \omega_{D_1, D_2}, 1) = L(f, D_1, 1) L'(f, D_2, 1)$$

is non-zero.

Theorem 3.7 is a special case, of [BD08, Theorem 1]. To recall the proof here would take us too far afield. (The key idea is to use the main theorem of [BD07] to express the periods  $J(f, D_1, D_2)$  in terms of actual Heegner points arising from parametrisations of  $E$  by Shimura curves associated to quaternion algebras that are ramified at  $p$ .) We will content ourselves with drawing attention to the important relationship between  $J(f, D_1, D_2)$  and the periods  $\tilde{r}(f_k^\sharp, D_1, D_2)$  that arise in Kohnen’s formula.

LEMMA 3.8. Under the assumptions of Theorem 3.7,

$$J(f, D_1, D_2) = \frac{d}{dk}(\tilde{r}(f_k^\sharp, D_1, D_2))_{k=1}.$$

Proof. Since  $J(f, D_1, D_2)$  belongs to  $\mathbb{Q}_p$ ,

$$2J(f, D_1, D_2) = J(f, D_1, D_2) + \overline{J(f, D_1, D_2)} = 2\frac{d}{dk}(\tilde{r}(f_k^\sharp, D_1, D_2))_{k=1},$$

where the last equality follows from part (c) of Lemma 3.5. □

#### 4. Proof of Theorem 1.5

Let  $-D_2$  be a discriminant of type II. Choose an auxiliary discriminant  $-D_1$  of type I satisfying:

- (a)  $\gcd(D_1, D_2) = 1$ ; and
- (b)  $c(D_1) \neq 0$ .

This implies that the product  $\Delta = D_1 D_2$  satisfies assumption (8). Note also that in this case

$$w(f, -D_1) = 1, \quad w(f, -D_2) = -1, \quad \chi_{-D_2}(p) = -w_p.$$

Hence all the conditions in the statement of Theorem 3.7 are satisfied.

By definition of the normalised coefficients, we have

$$\tilde{c}(D_1, k)\tilde{c}(D_2, k) = \frac{(1 - \underline{a}_p(k)^{-2}p^{2k-2})c(D_1, k)c(D_2, k)}{(1 - w_p \underline{a}_p(k)^{-1}p^{k-1})^2 c(\Delta_0, k)^2}.$$

Hence by Theorem 2.1,

$$\begin{aligned} \tilde{c}(D_1, k)\tilde{c}(D_2, k) &= \frac{(1 - \underline{a}_p(k)^{-2}p^{2k-2})r(f_k^\sharp, -D_1, -D_2)}{(1 - w_p \underline{a}_p(k)^{-1}p^{k-1})^2 r(f_k^\sharp, -\Delta_0, -\Delta_0)} \\ &= \frac{(1 - \underline{a}_p(k)^{-2}p^{2k-2})r(f_k^\sharp, -D_1, -D_2)}{\Omega_k}, \end{aligned}$$

where the last equality follows from the choice of  $\Omega_k$  that was made in (12), in light of the fact that  $\chi_{-\Delta_0}(p) = w_p$ . By the definition of the period  $\tilde{r}(f_k^\sharp, -D_1, -D_2)$  given in Lemma 3.5, it follows that

$$\tilde{c}(D_1, k)\tilde{c}(D_2, k) = \tilde{r}(f_k^\sharp, -D_1, -D_2).$$

Differentiating both sides with respect to  $k$ , evaluating at  $k = 1$  and applying Lemma 3.8, yields

$$\tilde{c}(D_1) \frac{d}{dk} \tilde{c}(D_2, k)_{k=1} = J(f, -D_1, -D_2). \tag{17}$$

The first part of Theorem 1.5 is now a consequence of Theorem 3.7 combined with the rationality of  $\tilde{c}(D_1)$ . The second part follows from the fact that  $\tilde{c}(D_1) \neq 0$  if and only if  $L(f, -D_1, 1) \neq 0$ .

**5. Gross–Kohnen–Zagier formulae for Stark–Heegner points**

The conjectures of [Dar01] predict that Stark–Heegner points should have many of the properties of their classical counterparts. It is therefore natural to look for analogues of the theorem of Gross, Kohnen and Zagier relating Stark–Heegner points to the Fourier coefficients of modular forms of weight 3/2. In fact, the method of proof of Theorem 1.5 yields some results in this direction.

For example, we have the next theorem.

**THEOREM 5.1.** *Let  $-D_2$  be a fixed discriminant of type II associated to  $f$ . Then the following hold.*

- (a) *The periods  $b(D_1) := J(f, -D_1, -D_2)$ , as  $-D_1$  varies over the type I discriminants attached to  $f$ , are (proportional to) the Fourier coefficients  $c(D_1)$  of a Shimura–Kohnen lift  $g \in S_{3/2}^+(4N)$  attached to  $f$ .*
- (b) *Assume further that  $N$  is the product of at least two primes. Then the function  $D_1 \mapsto b(D_1)$  is non-zero if and only if*

$$L'(f, -D_2, 1) \neq 0.$$

*Proof.* This follows directly from (17), which shows that the ratio between  $b(D_1)$  and  $c(D_1)$  is equal to the expression

$$\frac{d}{dk} \tilde{c}(D_2, k)_{k=1},$$

which does not depend on  $D_1$ . When  $N$  is divisible by at least two primes, Theorem 3.7 relates this expression to a global point on  $E(\mathbb{Q}(\sqrt{-D_2}))^- \otimes \mathbb{Q}$ , which is non-zero precisely when  $L'(f, -D_2, 1) \neq 0$ . □

Observe that Theorem 3.7 is not needed to prove part (a) of Theorem 5.1. In particular, when  $f$  is a form of prime conductor, the invariants  $J(f, -D_1, -D_2)$  (as  $D_1$  varies, and  $D_2$  is fixed) can still be related to the Fourier coefficients of a modular form of weight 3/2, even though the proof of Theorem 3.7 breaks down for such modular forms and we are unable to relate  $J(f, -D_1, -D_2)$  to a global point on  $E(\mathbb{Q}(\sqrt{-D_2}))^-$ . This remark leads to the following corollary, which gives further evidence for the general conjectures on Stark–Heegner points formulated in [Dar01].

**COROLLARY 5.2.** *Let  $-D_2$  be a fixed discriminant of type II. Assume that there exists a type I discriminant  $-D_1$  for which*

$$J(f, -D_1, -D_2) = \log_E(P(f, -D_1, -D_2)) \neq 0,$$

*with  $P(f, -D_1, -D_2) \in E(\mathbb{Q}(\sqrt{-D_2}))^- \otimes \mathbb{Q}$ . Then for all type I discriminants  $-D_1$ , the expressions  $J(f, -D_1, -D_2)$  are equal to the formal group logarithm of global points in  $E(\mathbb{Q}(\sqrt{-D_2}))^- \otimes \mathbb{Q}$ .*

In order to generalise this discussion, let  $D_2$  be any fixed discriminant (either positive or negative) satisfying

$$w(f, D_2) = -1,$$

but not necessarily of type II. Then the invariants  $J(D_1, D_2)$  are defined on all fundamental discriminants  $D_1$  satisfying

$$D_1 D_2 > 0, \quad \chi_{D_1}(p) = -\chi_{D_2}(p), \quad \chi_{D_1}(\ell) = \chi_{D_2}(\ell) \quad \text{for all } \ell \mid M. \tag{18}$$

The coefficients  $b(D_1) := J(f, D_1, D_2)$ , as  $D_1$  varies over fundamental discriminants satisfying (18), are really only defined up to sign, since they depend on the choice of a  $p$ -adic square root

of  $D_1D_2$ . But for discriminants  $D_1$  that are congruent to each other modulo  $p$ , it is possible to make a consistent choice of square root and remove the sign ambiguity in the definition of  $b(D_1)$  for  $D_1$  in a fixed residue class modulo  $p$ . Section 6.2 discusses this issue in more detail, and explains how in certain cases (for example, when  $p \equiv 3$  modulo 4) the coefficient  $b(D_1)$  can even be defined unambiguously for all  $D_1$ .

Theorem 5.1 suggests the following conjecture.

CONJECTURE 5.3. *The coefficients  $b(D)$  are proportional to the  $D$ th Fourier coefficients of a modular form of weight  $3/2$  on  $\Gamma_1(4N^2)$  associated to  $f$  by a (suitably generalised) Shimura–Kohnen correspondence. Furthermore, these coefficients vanish identically if and only if  $L'(f, D_2, 1) = 0$ .*

Conjecture 5.3 can be divided into two cases.

Case 1: The case where  $\chi_{D_2}(p) = -w_p$ . In that case the invariants  $J(f, D_1, D_2)$  belong to  $\mathbb{Q}_p$ , and the key Lemma 3.8 still holds. One therefore has a hope of proving Conjecture 5.3 by suitably generalising Kohnen’s formula. Some progress in this direction has been made by work of Mao, Rodriguez-Villegas and Tornara [MRVT07] and of Mao [Mao08]. See also [PT08] for more examples of the generalised Shimura–Kohnen correspondence in the case of composite levels.

Case 2: The case where  $\chi_{D_2}(p) = w_p$ . In that case one has

$$\overline{J(f, D_1, D_2)} = -J(f, D_1, D_2),$$

and the proof of Lemma 3.8 breaks down completely. In fact, the periods  $\tilde{r}(f_k^\#, D_1, D_2)$  vanish identically in this case, and there is therefore little hope of controlling the Stark–Heegner points  $J(f, D_1, D_2)$  by exploiting the  $p$ -adic variation of modular forms. In this setting, Conjecture 5.3 is more mysterious, and we can give little theoretical evidence for it. We have however gathered some numerical evidence in its support in the next section.

### 6. Numerical evidence

In this section we present some numerical evidence for Conjecture 5.3, in the case (which is the simplest and most natural for calculations) where:

- (i) the elliptic curve  $E$  has prime conductor  $p$  and odd analytic rank, so that  $w_p = 1$ ;
- (ii) the auxiliary discriminant  $D_2$  is equal to 1.

Under these hypotheses, we find ourselves in case 2 in the discussion of Conjecture 5.3. This setting is therefore the most interesting from a theoretical point of view because *both* hypotheses in Theorem 3.7 fail, and Lemma 3.8 does not hold.

For fundamental discriminants  $\Delta > 0$  satisfying  $\chi_\Delta(p) = -1$  (i.e. for real quadratic fields  $K$  in which  $p$  is inert), we can use the computer package `shp` of [DP08] to check and (conjecturally) compute the corresponding global point  $P(\Delta) \in E(\mathbb{Q})$  (the ‘trace’ of the Stark–Heegner points for  $K$ ).

On the other hand, a construction given in [MRVT07] associates to  $f$  a modular form  $g_+$  of weight  $3/2$  on  $\Gamma_1(4p^2)$  whose coefficients  $c(\Delta)$  are indexed by *real* quadratic discriminants  $\Delta > 0$  satisfying  $\chi_\Delta(p) = -1$ , and are related to a square root of the central values  $L(f, \Delta, 1)$ . This computation is done by a PARI/GP [PARI] package, which computes modular forms of half-integral weight as linear combinations of generalised theta series associated to positive definite ternary quadratic forms. The linear combinations are determined from Brandt matrices using the package `qalgmform` from [CNT].



TABLE 1. Traces of Stark–Heegner points in 37a.

$\Delta$	$h(\Delta)$	$P(\Delta)$	$m_\Delta$	$\Delta$	$h(\Delta)$	$P(\Delta)$	$m_\Delta$
5	1	(0, 0)	1	61	1	$\infty$	0
8	1	(0, 0)	1	69	1	$\infty$	0
13	1	(0, -1)	-1	76	1	(0, -1)	-1
17	1	(0, -1)	-1	88	1	(0, -1)	-1
24	1	(0, -1)	-1	89	1	(0, -1)	-1
29	1	(1, 0)	2	92	1	(1, -1)	-2
56	1	(0, -1)	-1	93	1	(1, 0)	2
57	1	(0, -1)	-1	97	1	$\infty$	0
60	2	(0, 0)	1	105	2	(0, -1)	-1

### 6.1 The curve 37a

The smallest prime conductor for which there is an elliptic curve with sign  $-1$  in its functional equation is  $p = 37$ . Indeed, the quotient of the modular curve  $X_0(37)$  by the Atkin–Lehner involution is an elliptic curve, denoted by 37a in the tables of Cremona, and given by the equation

$$E : y^2 + y = x^3 - x.$$

Note that this curve is unique in its  $\mathbb{Q}$ -isogeny class.

The computation of the Stark–Heegner points for this curve has been discussed in [DP06], which focuses on a few small discriminants with relatively large class number. This time we computed the traces of the Stark–Heegner points over a much larger range, for discriminants  $\Delta \leq 10\,000$  with  $\chi_\Delta(37) = -1$ . The computations were carried to 20 significant 37-adic digits, which was enough to recognise all of the traces but one (see below).

To compare these traces with coefficients of modular forms of weight  $3/2$ , we write  $P(\Delta) = m_\Delta P_0$ , where  $m_\Delta \in \mathbb{Z}$  and  $P_0 = (0, 0)$  is a fixed generator of  $E(\mathbb{Q})$ . The traces  $P(\Delta)$  and the values  $m_\Delta$  for fundamental discriminants  $\Delta \leq 105$  are shown in Table 1.

Note that the values of  $m_\Delta$  in the table being rather small, the points  $P(\Delta)$  are usually of small height, and thus rational reconstruction from the 37-adic approximation is very easy. For instance

$$P(461) \equiv (3606\,438\,279\,313\,387, 3005\,365\,232\,761\,155) \pmod{37^{10}}$$

is easily recognised as the global point  $P(461) = (\frac{1}{4}, -\frac{5}{8}) = 5P_0$ .

As the discriminant  $\Delta$  gets larger, so does  $m_\Delta$ . In our computation for  $\Delta \leq 10\,000$  we found one discriminant for which the working precision of 20 significant 37-adic digits is not enough to recognize  $P(\Delta)$ :

$$P(8357) = \left( \frac{51\,678\,803\,961}{12\,925\,188\,721}, -\frac{12\,133\,184\,284\,073\,305}{1469\,451\,780\,501\,769} \right) = -22P_0.$$

It turns out this is the largest value of  $m_\Delta$  in our range. Of course we expect  $|m_{8357}| = 22$  from reading a coefficient of a modular form of weight  $3/2$  (see Table 2), and we can still check *a posteriori* that this is consistent with the value of  $P(8357)$  computed modulo  $37^{20}$ .

The computation of the modular form  $g_+$  of weight  $3/2$  corresponding to 37a can be done following [MRVT07]. The Fourier expansion of  $g_+$  begins

$$g_+ = q^5 - q^8 - q^{13} - q^{17} + q^{20} + q^{24} - 2q^{29} + O(q^{30}).$$

Note that, owing to some choices in the construction, the sign of the coefficients is not well defined. The sign of the coefficients here may differ from the ones given in [MRVT07].

TABLE 2. Coefficients of  $g_+$  corresponding to 37a.

$\Delta$	5	8	13	17	24	29	56	57	60	61	69
$c(\Delta)$	1	-1	-1	-1	1	-2	-1	-1	-1	0	0
$\Delta$	76	88	89	92	93	97	105	...	461	...	8357
$c(\Delta)$	-1	1	-1	-2	2	0	-1	...	5	...	22

TABLE 3. Traces of Stark–Heegner points in 37a for  $\Delta \equiv 2 \pmod{37}$ .

$\Delta$	$h(\Delta)$	$P(\Delta)$	$m_\Delta$	$\Delta$	$h(\Delta)$	$P(\Delta)$	$m_\Delta$
76	1	(0, -1)	-1	1001	2	(0, 0)	1
113	1	$\infty$	0	1112	1	$\infty$	0
409	1	$\infty$	0	1149	1	(1, 0)	2
520	4	$\infty$	0	1297	11	(0, -1)	-1
557	1	$(\frac{21}{25}, -\frac{56}{125})$	-8	1704	2	(0, -1)	-1
				1741	1	(0, -1)	-1
668	1	$(-\frac{5}{9}, \frac{8}{27})$	7	1852	1	$\infty$	0
				1889	1	(-1, -1)	3
705	2	(0, -1)	-1				
853	1	(1, 0)	2				

The coefficients of  $g_+ = \sum c(\Delta) q^\Delta$  for the fundamental discriminants  $\Delta \leq 105$ ,  $\Delta = 461$  and  $\Delta = 8357$  are shown in Table 2.

### 6.2 The mysterious signs

The Stark–Heegner points as we have described them have an inherent ambiguity of sign. This is because their calculation depends essentially on a choice of  $\sqrt{\Delta} \in \mathbb{C}_p$ . In the case of classical Heegner points in the original Gross–Kohnen–Zagier formula, square roots in  $\mathbb{C}$  of imaginary quadratic discriminants are canonically chosen to be in the upper half-plane. At this stage, Conjecture 5.3 only makes sense up to a sign; this is tantamount to a Gross–Zagier type formula for the heights of the (traces of) Stark–Heegner points, and does not include a statement about the ‘mysterious signs’.

We remark that  $g_+$  itself is not unique (not even up to a single constant, unlike for the case of classical Heegner points). However, having the level bounded at  $4p^2$  restricts the choices quite a lot. There is still room to change signs of the different coefficients *so long* as the change is periodic modulo  $p$ . In particular, the sign of  $c(\Delta_1)/c(\Delta_2)$  is well defined, provided  $\Delta_1 \equiv \Delta_2 \pmod{p}$ .

In harmony with this observation, notice that, if  $\Delta_1 \equiv \Delta_2 \not\equiv 0 \pmod{p}$ , there is a natural way to choose  $\sqrt{\Delta_2} \in \mathbb{C}_p$  once  $\sqrt{\Delta_1} \in \mathbb{C}_p$  has been chosen: namely, make the unique choice such that  $\sqrt{\Delta_2}$  is congruent to  $\sqrt{\Delta_1}$  modulo  $p$ . Thus, the ambiguity in sign can be resolved for Stark–Heegner points attached to like discriminants modulo  $p$ .

For instance, the traces  $P(\Delta)$  and the values  $m_\Delta$  for fundamental discriminants  $\Delta \equiv 2 \pmod{37}$  with  $\Delta \leq 2000$  are shown in Table 3. The coefficients of  $g_+$ , which are displayed in Table 4, agree with the  $m_\Delta$  including the sign.

There is also a special case in which the signs can be completely well defined. Namely, when  $p \equiv 3 \pmod{4}$  we can employ the fact that the quadratic character  $\chi_{-p}$  of conductor  $p$  is *odd*.

TABLE 4. Coefficients of  $g_+$  for  $\Delta \equiv 2 \pmod{37}$ .

$\Delta$	76	113	409	520	557	668	705	853
$c(\Delta)$	-1	0	0	0	-8	7	-1	2
$\Delta$	1001	1112	1149	1297	1704	1741	1852	1889
$c(\Delta)$	1	0	2	-1	-1	-1	0	3

TABLE 5. Traces of Stark–Heegner points in 43a.

$\Delta$	$h(\Delta)$	$P(\Delta)$	$m_\Delta$	$\Delta$	$h(\Delta)$	$P(\Delta)$	$m_\Delta$
5	1	(0, 0)	1	69	1	(0, -1)	-1
8	1	(0, -1)	-1	73	1	(0, 0)	1
12	1	(0, 0)	1	76	1	$\infty$	0
28	1	(0, -1)	-1	77	1	(1, 1)	-3
29	1	(0, -1)	-1	85	2	(0, 0)	1
33	1	(0, -1)	-1	88	1	(0, -1)	-1
37	1	(-1, -1)	2	89	1	(0, 0)	1
61	1	(0, 0)	1	93	1	(1, -2)	3
65	2	(0, -1)	-1	104	2	(0, 0)	1

Once  $\sqrt{\Delta_0}$  has been chosen, it determines a canonical choice for  $\sqrt{\Delta} \in \mathbb{C}_p$  by requiring

$$\chi_{-p}(\sqrt{\Delta}/\sqrt{\Delta_0}) = 1.$$

On the side of half-integral weight modular forms, the form  $g_+$  is also determined uniquely up to a single constant by requiring it to have character  $\chi_{4p} = \chi_{-4}\chi_{-p}$  of conductor  $4p$ . This weight  $3/2$  modular form  $g_+$  can be characterised as being in Shimura correspondence with the quadratic twist  $f \otimes \chi_{-p}$ , of level  $p^2$ . The Shimura correspondence for level  $p^2$  has been worked out explicitly in [PT07a], and examples of its application to central values of real quadratic twists, and in particular to computing the Fourier coefficients of  $g_+$ , appear in [PT07b].

### 6.3 The curve 43a

The smallest conductor  $p \equiv 3 \pmod{4}$  for which there is an elliptic curve with sign  $-1$  in its functional equation is  $p = 43$ . The quotient of the modular curve  $X_0(43)$  by the Atkin–Lehner involution is again an elliptic curve, denoted by 43a in the tables of Cremona, and is given by the equation

$$E : y^2 + y = x^3 + x^2.$$

This curve is unique in its  $\mathbb{Q}$ -isogeny class.

We computed the traces of the Stark–Heegner points for fundamental discriminants  $\Delta \leq 10\,000$  with  $\chi_\Delta(43) = -1$ , using a precision of 20 significant 43-adic digits, which was enough to recognise all of the traces as global points in  $E(\mathbb{Q})$  except for  $P(7613) = 21P_0$ .

We will write  $P(\Delta) = m_\Delta P_0$  with  $m_\Delta \in \mathbb{Z}$  and  $P_0 = (0, 0)$  is a fixed generator of  $E(\mathbb{Q})$ . These data, for fundamental discriminants  $\Delta \leq 104$ , are shown in Table 5.

The computation of the modular form  $g_+$  of weight  $3/2$  corresponding to 43a can be done following either [PT07b] or [MRVT07]. The Fourier expansion of  $g_+$  begins

$$g_+ = q^5 - q^8 + q^{12} + q^{20} - q^{28} - q^{29} + O(q^{30}).$$

In this case the sign of its coefficients is canonically defined, after setting  $c(g^+, 5) = 1$ . We verified that the resulting coefficients agree with the values of  $m_\Delta$  computed above, for all  $\Delta \leq 10\,000$ .

TABLE 6. Coefficients of  $g_+$  corresponding to  $43a$ .

$\Delta$	5	8	12	28	29	33	37	61	65
$c(\Delta)$	1	-1	1	-1	-1	-1	2	1	-1
$\Delta$	69	73	76	77	85	88	89	93	104
$c(\Delta)$	-1	1	0	-3	1	-1	1	3	1

TABLE 7. Number of discriminants  $\Delta \leq 10\,000$  we used for each curve. The column labelled  $x$  indicates the number of such discriminants for which the precision of 20 significant  $p$ -adic digits was not enough to recognise the trace of the Stark–Heegner point.

$E$	$\#\Delta$	$x$	$E$	$\#\Delta$	$x$
$37a$	1483	1	$101a$	1514	0
$43a$	1491	1	$131a$	1515	0
$53a$	1490	3	$163a$	1508	2
$61a$	1504	0	$197a$	1524	1
$79a$	1504	0	$229a$	1525	10
$83a$	1513	10	$269a$	1519	4
$89a$	1509	0	$277a$	1524	106

The coefficients of  $g_+ = \sum c(\Delta)q^\Delta$  for the fundamental discriminants  $\Delta \leq 104$  are shown in Table 6. A few more coefficients (for all  $\Delta < 200$ ) can be found in [MRVT07].

### 6.4 Other curves

In addition to the elliptic curves of  $37a$  and  $43a$  already discussed, we also did computations for the following 12 curves:

$$\begin{aligned}
 53a : & \quad y^2 + xy + y = x^3 - x \\
 61a : & \quad y^2 + xy = x^3 - 2x + 1 \\
 79a : & \quad y^2 + xy + y = x^3 + x^2 - 2x \\
 83a : & \quad y^2 + xy + y = x^3 + x^2 + x \\
 89a : & \quad y^2 + xy + y = x^3 + x^2 - x \\
 101a : & \quad y^2 + y = x^3 + x^2 - x - 1 \\
 131a : & \quad y^2 + y = x^3 - x^2 + x \\
 163a : & \quad y^2 + y = x^3 - 2x + 1 \\
 197a : & \quad y^2 + y = x^3 - 5x + 4 \\
 229a : & \quad y^2 + xy = x^3 - 2x - 1 \\
 269a : & \quad y^2 + y = x^3 - 2x - 1 \\
 277a : & \quad y^2 + xy + y = x^3 - 1.
 \end{aligned}$$

These are all the isogeny classes of elliptic curves of prime conductor  $p < 300$  and rank 1. Note that for  $p$  up to 131, these are isomorphic to the quotient of the modular curve  $X_0(p)$  by the Atkin–Lehner involution. All of these curves are unique in their  $\mathbb{Q}$ -isogeny class.

For each of these curves we computed the traces of the Stark–Heegner points for discriminants  $\Delta \leq 10\,000$  with  $\chi_\Delta(p) = -1$ . All the computations were carried to 20 significant  $p$ -adic digits, which was enough to recognise almost all of the traces. In Table 7 we indicate the number of discriminants for each curve, and the number of discriminants for which the precision was insufficient to recognise the point.

For the five curves with conductor  $p \equiv 3 \pmod{4}$ , the corresponding modular forms of weight  $3/2$  level  $4p^2$  and character  $\chi_{4p}$  (and many more) can be obtained from the data in [Tor04]. We verified that their coefficients agree with the values of  $m_\Delta$ , for  $\Delta \leq 10\,000$ .

For the other seven curves with conductor  $p \equiv 1 \pmod{4}$ , we computed the corresponding modular forms of weight  $3/2$  for  $\Gamma_1(4p^2)$  following the method explained in [MRVT07], and verified that their coefficients agree with the values of  $m_\Delta$  up to a sign function defined modulo  $p$ , for all  $\Delta \leq 10\,000$ .

The complete set of data that we computed, comprising the traces of the Stark–Heegner points and the values  $m_\Delta$  for discriminants  $\Delta \leq 10\,000$  with  $\chi_\Delta(p) = -1$ , for each of the curves mentioned above, is available online at [DT07].

## REFERENCES

- BD07 M. Bertolini and H. Darmon, *Hida families and rational points on elliptic curves*, *Invent. Math.* **168** (2007), 371–431.
- BD08 M. Bertolini and H. Darmon, *The rationality of Stark–Heegner points over genus fields of real quadratic fields*, *Annals of Mathematics*, to appear.
- CNT Computational Number Theory, <http://www.ma.utexas.edu/cnt/>.
- Dar01 H. Darmon, *Integration on  $\mathcal{H}_p \times \mathcal{H}$  and arithmetic applications*, *Ann. of Math. (2)* **154** (2001), 589–639.
- Dar06 H. Darmon, *Heegner points, Stark–Heegner points, and values of  $L$ -series*, in *Proceedings of the ICM*, Madrid, 2006.
- DP06 H. Darmon and R. Pollack, *The efficient calculation of Stark–Heegner points via overconvergent modular symbols*, *Israel J. Math.* **153** (2006), 319–354.
- DP08 H. Darmon and R. Pollack, *Stark–Heegner points via overconvergent modular symbols*, <http://www.math.mcgill.ca/darmon/programs/shp/shp.html>.
- DT07 H. Darmon and G. Tornaría, *Traces of Stark–Heegner points for elliptic curves of prime conductor and rank 1*, <http://www.ma.utexas.edu/users/tornaria/cnt/>.
- GKZ87 B. Gross, W. Kohnen and D. Zagier, *Heegner points and derivatives of  $L$ -series. II*, *Math. Ann.* **278** (1987), 497–562.
- Koh82 W. Kohnen, *Newforms of half-integral weight*, *J. reine angew. Math.* **333** (1982), 32–72.
- Koh85 W. Kohnen, *Fourier coefficients of modular forms of half-integral weight*, *Math. Ann.* **271** (1985), 237–268.
- MTT86 B. Mazur, J. Tate and J. Teitelbaum, *On  $p$ -adic analogues of the conjectures of Birch and Swinnerton-Dyer*, *Invent. Math.* **84** (1986), 1–48.
- Mao08 Z. Mao, *A generalized Shimura correspondence for newforms*, *J. Number Theory* **128** (2008), 71–95.
- MRVT07 Z. Mao, F. Rodriguez-Villegas and G. Tornaría, *Computation of central value of quadratic twists of modular  $L$ -functions*, in *Ranks of elliptic curves and random matrix theory*, London Mathematical Society Lecture Note Series, vol. 341 (Cambridge University Press, Cambridge, 2007), 273–288.
- PARI PARI/GP, version 2.3.1, <http://pari.math.u-bordeaux.fr/>.
- PT07a A. Pacetti and G. Tornaría, *Shimura correspondence for level  $p^2$  and the central values of  $L$ -series*, *J. Number Theory* **124** (2007), 396–414.
- PT07b A. Pacetti and G. Tornaría, *Examples of the Shimura correspondence for level  $p^2$  and real quadratic twists*, in *Ranks of elliptic curves and random matrix theory*, London Mathematical Society Lecture Note Series, vol. 341 (Cambridge University Press, Cambridge, 2007), 289–314.
- PT08 A. Pacetti and G. Tornaría, *Computing central values of twisted  $L$ -series: the case of composite levels*, *Experiment. Math.*, to appear.

- Ste94 G. Stevens,  *$\Lambda$ -adic modular forms of half-integral weight and a  $\Lambda$ -adic Shintani lifting*, in *Arithmetic geometry*, Tempe, AZ, 1993, Contemporary Mathematics, vol. 174 (American Mathematical Society, Providence, RI, 1994), 129–151.
- Tor04 G. Tornaría, *Data about the central values of the  $L$ -series of (imaginary and real) quadratic twists of elliptic curves*, <http://www.ma.utexas.edu/users/tornaria/cnt/>.

Henri Darmon [darmon@math.mcgill.ca](mailto:darmon@math.mcgill.ca)

Department of Mathematics, McGill University, Burnside Hall, Montreal, QC, Canada H3A 2K6

Gonzalo Tornaría [tornaria@cmat.edu.uy](mailto:tornaria@cmat.edu.uy)

Centro de Matemática, Facultad de Ciencias, Iguá 4225, Montevideo 11400, Uruguay