ELEMENTARY MATRIX DECOMPOSITION AND THE COMPUTATION OF DARMON POINTS WITH HIGHER CONDUCTOR

XAVIER GUITART AND MARC MASDEU

Abstract. We extend the algorithm of [DG02] and [DP06] for computing p-adic Darmon points on elliptic curves to the case of composite conductor. We also extend the algorithm of [DL03] for computing ATR Darmon points to treat curves of nontrivial conductor. Both cases involve an algorithmic decomposition into elementary matrices in congruence subgroups $\Gamma_1(\mathfrak{N})$ for ideals $\mathfrak{N}$ in certain rings of S-integers. We use these extensions to provide additional evidence in support of the conjectures on the rationality of Darmon points.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ of conductor pM, with p a prime not dividing M. Let K be a real quadratic field in which p is inert and all the primes dividing M are split, and denote by $\mathcal{H}_p = \mathbb{P}^1(K_p)\setminus\mathbb{P}^1(\mathbb{Q}_p)$ the K_p-points of the p-adic upper half plane.

A construction of Darmon [Dar01] associates to every $\tau \in \mathcal{H}_p \cap K$ a local point $P_\tau \in E(K_p)$, which is defined as a certain Coleman integral of the modular form f corresponding to E under the Modularity Theorem. The points P_τ are conjectured to be rational over ring class fields of K, and to behave in many aspects as Heegner points.

An algorithm for the effective calculation of p-adic Darmon points was given in [DG02] and was improved in [DP06]. Some P_τ's were computed in concrete examples and checked to be p-adically close to global points, providing extensive numerical evidence in support of the conjectures. However, due to the restrictions imposed by the algorithm, only elliptic curves of prime conductor p (that is, with $M = 1$) could be treated.

In the articles [DG02] and [DP06] it is crucial to assume that $M = 1$ when applying the "continued fraction trick" (see [DG02, p. 42]) in order to transform certain semi-indefinite integrals into double integrals. The present article provides a different procedure for performing this step when $M > 1$.

In other words, we extend the algorithm of [DG02] and [DP06] to a much larger class of curves. As an application, we compute p-adic Darmon points on curves of composite conductor and we check that they are close to global points, which provides new experimental evidence in support of the validity of Darmon's construction in its stated generality.

Date: June 21, 2013.

2010 *Mathematics Subject Classification.* 11G40 (11F41, 11Y99).

The method for transforming semi-indefinite integrals into double integrals is based on an algorithmic decomposition into elementary matrices in congruence subgroups $\Gamma_1(\mathfrak{N})$ for ideals $\mathfrak{N}$ in certain rings of S-integers. This can be seen as an algorithmic version of the congruence subgroup problem. In particular we improve on a theorem of Cooke-Weinberger (see Corollary 2.4).

In addition, essentially the same method of elementary matrix decompositions can also be applied to the so-called ATR points, a different instance of Darmon points introduced in [Dar04, §8] and [DL03, §4] for elliptic curves over totally real fields. Although the construction of ATR points is radically different (for instance, they are defined by means of complex integrals), their explicit computation has some formal similarities with respect to the p-adic setting. In particular the methods used until the present have all used a "continued fraction trick" which in this case only applies to curves of trivial conductor (cf. [Gär11, p. 108] for a discussion of this issue). The present article provides also a method for computing ATR Darmon points in curves of non-trivial conductor.

The rest of the article is organized as follows. In Section 2 we introduce an algorithm for computing elementary matrix decompositions in certain congruence subgroups. We state it in a level of generality so that it can be applied both to the p-adic and the ATR setting. In Section 3 we recall the definition of p-adic Darmon points, we discuss the algorithm for computing them in curves of composite level and we include some tables of numerical computations performed using it. Finally, in Section 4 we briefly recall ATR points and we make explicit the method for computing them in curves of non-trivial conductor, as well as a detailed example of a numerical verification of Darmon's conjecture in this case.

Acknowledgments. It is a pleasure to thank John Voight for helpful comments on elementary matrix decompositions, Robert Pollack for clarifying to us some details on his implementation of the overconvergent modular symbols algorithm, Kate Petersen for pointing out some relevant references, and Henri Darmon for many valuable observations. Guitart wants to thank the Max Planck Institute for Mathematics for their hospitality and financial support during his stay at the Institute, where part of the present work has been carried out. The authors were partially supported by MTM2009-13060-C02-01 and 2009 SGR 1220.

2. Elementary matrix decomposition in Γ_1

Let F be a number field with ring of integers $\mathcal{O}$, and let S be a finite set of places of F containing the archimedean ones. Let $\mathcal{O}_S$ denote the subring of F consisting of those elements whose valuation is non-negative at all the places outside S.

For an ideal $\mathfrak{N}$ of $\mathcal{O}_S$, we denote by $\Gamma_1(\mathfrak{N})$ the subgroup of $\mathrm{SL}_2(\mathcal{O}_S)$ defined as

$$\Gamma_1(\mathfrak{N}) = \left\{\gamma \in \mathrm{SL}_2(\mathcal{O}_S)\colon \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{\mathfrak{N}}\right\}, \tag{2.1}$$

and by $E_{1,\mathfrak{N}}$ the subgroup of $\Gamma_1(\mathfrak{N})$ generated by the *elementary matrices* of the form

$$\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \text{ with } y \in \mathfrak{N} \text{ and } \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \text{ with } x \in \mathcal{O}_S. \tag{2.2}$$

If the group of units $\mathcal{O}_S^\times$ is infinite, then $\Gamma_1(\mathfrak{N}) = E_{1,\mathfrak{N}}$; see for instance [Vas72] for a proof of this result, and also for its relation with the Congruence Subgroup

Problem. Therefore, when $\mathcal{O}_S^\times$ is infinite every matrix in $\Gamma_1(\mathfrak{N})$ can be factored into a product of elementary matrices of type (2.2). However, the proof given in [Vas72] is not explicit, so it does not give rise to an algorithm for systematically performing such decomposition. In this section we see that the results and techniques introduced in [CW75] can be adapted to provide –assuming GRH– such an algorithm, in the particular case where F has at least one real archimedean place. Thus from now on we will assume that $\mathcal{O}_S^\times$ is infinite and that F has at least one real place.

The following lemma is stated and proved in [BMS67, Lemma 2.2 (b)] using the notation of Mennicke symbols. For the convenience of the reader we restate it in terms of explicit matrix formulas.

Lemma 2.1. *Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be an element in $\Gamma_1(\mathfrak{N})$. Suppose that $c = u + ta$ for some unit $u \in \mathcal{O}_S^\times$ and some $t \in \mathcal{O}_S$, and let T be the matrix*

$$T = \begin{pmatrix} 1 & 0 \\ u(a-1) & 1 \end{pmatrix} \begin{pmatrix} 1 & u^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t(a-1) & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -c & 1 \end{pmatrix}.$$

Then $T\gamma = \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ for some $x \in \mathcal{O}_S$. In particular,

$$\gamma = \begin{pmatrix} 1 & 0 \\ c + t(1-a) & 1 \end{pmatrix} \begin{pmatrix} 1 & -u^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ u(1-a) & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}. \tag{2.3}$$

Proof. A direct computation shows that the first column of $T\gamma$ is $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. Since $T\gamma$ belongs to $\Gamma_1(\mathfrak{N})$, we see that $T\gamma = \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ for some $x \in \mathcal{O}_S$. □

Observe that, since $a - 1$ and c belong to $\mathfrak{N}$, identity (2.3) already expresses γ as a product of elementary matrices of type (2.2). The next step is to show that, assuming GRH, one can reduce to the case where a is congruent to a unit mod c by multiplying γ by an elementary matrix. Before stating the result of [CW75] that grants this, we recall some terminology related to ray class groups.

Let $\mathfrak{m}$ be an ideal of $\mathcal{O}$, with factorization into prime ideals of the form

$$\mathfrak{m} = \prod_{\mathfrak{p}|\mathfrak{m}} \mathfrak{p}^{m(\mathfrak{p})}.$$

Let $I^{\mathfrak{m}}$ be the multiplicative group of ideals of $\mathcal{O}$ relatively prime to $\mathfrak{m}$, and let

$$F_{1,\mathfrak{m}} = \{x \in F \colon v_{\mathfrak{p}}(x-1) \geq m(\mathfrak{p}) \ \text{ for all } \mathfrak{p} \mid \mathfrak{m}\}.$$

There is a natural map $i \colon F_{1,\mathfrak{m}} \to I^{\mathfrak{m}}$ given by $x \mapsto (x)$. The quotient

$$C_{\mathfrak{m}} = I^{\mathfrak{m}}/i(F_{1,\mathfrak{m}})$$

is the *ray class group modulo* $\mathfrak{m}$. The following result is [CW75, Theorem 2.13].

Theorem 2.2 (Cooke–Weinberger)**.** *Assume GRH. Let $\mathfrak{m}$ be an ideal in $\mathcal{O}$, and let α be an ideal class in $C_{\mathfrak{m}}$. Then the set of prime ideals $\mathfrak{q}$ contained in α such that the reduction map*

$$\mathcal{O}_S^\times \longrightarrow (\mathcal{O}_S/\mathfrak{q}\mathcal{O}_S)^\times$$

is surjective has positive density.

From this we obtain the main result of this section.

Theorem 2.3. *Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be an element of $\Gamma_1(\mathfrak{N})$. Assuming GRH, the following algorithm terminates and computes an expression of γ as a product of elementary matrices.*

(1) *Iterate over the elements $\lambda \in \mathcal{O}$ to find λ such that $a' = a + \lambda c$ generates a prime ideal and*

$$\mathcal{O}_S^\times \longrightarrow (\mathcal{O}_S/a'\mathcal{O}_S)^\times \quad \text{is surjective.} \tag{2.4}$$

(2) *Set $\gamma' = \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)\gamma$, and let $\gamma' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$.*

(3) *Iterate over the elements $u \in \mathcal{O}_S^\times$ until finding u such that*

$$c' \equiv u \pmod{a'}.$$

(4) *Use Lemma 2.1 to find an expression of γ' as a product of elementary matrices.*

Proof. We can, and do, choose $e \in \mathcal{O}_S^\times$ such that ea and ec belong to $\mathcal{O}$. By applying Theorem 2.2 with $\mathfrak{m} = (ec)$, we see that there exists a prime ideal $\mathfrak{q}$ in the same class of $[(ea)] \in C_{\mathfrak{m}}$ such that $\mathcal{O}_S^\times \to (\mathcal{O}/\mathfrak{a}'\mathcal{O}_S)^\times$ is surjective. Since (ea) is integral and principal, we see that $\mathfrak{q}$ is also principal. Therefore, $\mathfrak{q} = (q)$ for some $q \equiv ea \pmod{(ec)}$, so that $q = ea + \lambda ec$ for some $\lambda \in \mathcal{O}$. But q and $a' = a + \lambda c$ generate the same ideal in $\mathcal{O}_S$, so that $\mathcal{O}_S^\times \to (\mathcal{O}/a'\mathcal{O}_S)^\times$ is surjective. This justifies that step (1) of the algorithm can be accomplished.

Now the class of c' in $(\mathcal{O}_S/a')^\times$ can be represented by some unit $u \in \mathcal{O}_S^\times$, and this justifies step (3). □

In the particular case $\mathfrak{N} = \mathcal{O}_S$, the result in [CW75, Th. 2.14] asserts that any matrix $\gamma \in \mathrm{SL}_2(\mathcal{O}_S)$ can be expressed as a product of at most 7 elementary matrices. Theorem 2.3 above and expression (2.3) give the following generalization to arbitrary ideals $\mathfrak{N}$, which also slightly improves the number of elementary matrices needed to 5.

Corollary 2.4. *Under the assumption of GRH, every matrix in $\Gamma_1(\mathfrak{N})$ is a product of at most 5 elementary matrices of type (2.2).*

3. Computation of p-adic Darmon points on curves with composite conductor

In this section we explain the algorithm for computing p-adic Darmon points in curves of composite conductor and some of the related computational issues. After briefly reviewing the definition of p-adic Darmon points in §3.1, in §3.2 we describe the algorithm to transform the semi-indefinite integrals appearing in the definition of these points into double multiplicative integrals. In §3.3 we explain an efficient way of computing these double integrals, and finally in §3.4 we comment on the calculations that have been carried out in support of Darmon's conjecture.

3.1. Review of p-adic Darmon points.

Our presentation of the necessary background and the definition of p-adic Stark–Heegner points follows closely [DP06, §1], to which we refer the reader for more details and, in fact, for an excellent account of this material in the prime level case.

Let E be an elliptic curve over $\mathbb{Q}$ of conductor $N = pM$, with p a prime not dividing M. Let $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z}$ be the weight two newform on $\Gamma_0(N)$ whose L-series coincides with that of E. The coefficient a_p is 1 (resp. -1) if E has split (resp. non-split) multiplicative reduction at p.

Let R be the order in $\mathrm{M}_2(\mathbb{Z}[1/p])$ consisting of matrices that are upper triangular modulo M, and let $\Gamma = R_1^\times$ denote its group of units of determinant 1. Let K be

a real quadratic field in which p is inert and all primes dividing M are split. Set $\mathcal{H}_p = \mathbb{P}^1(K_p) \setminus \mathbb{P}^1(\mathbb{Q}_p)$, in which Γ acts by Möbius transformations. The p-adic Darmon point construction yields a map

$$\begin{array}{ccc} \Gamma \setminus (\mathcal{H}_p \cap K) & \longrightarrow & E(K_p) \\ \tau & \longmapsto & P_\tau, \end{array}$$

given in terms of certain p-adic integrals, and whose definition ultimately relies on the $\mathbb{Z}$-modular symbol attached to E.

3.1.1. *Measures attached to modular symbols.* If V is a $\mathbb{Z}$-module, a *V-valued modular symbol* φ is a map

$$\varphi\colon \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \longrightarrow V, \quad (r,s) \mapsto \varphi\{r \to s\}$$

such that

$$\varphi\{r \to s\} + \varphi\{s \to t\} = \varphi\{r \to t\} \text{ for all } r,s,t \in \mathbb{P}^1(\mathbb{Q}).$$

For $w_\infty \in \{\pm 1\}$ we denote by $I_f\colon \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \to \mathbb{Z}$ the $\mathbb{Z}$-valued modular symbol attached to E and w_∞. That is to say

$$I_f\{r \to s\} = \begin{cases} \dfrac{1}{\Omega^+} \displaystyle\int_r^s \operatorname{Re} \omega_f & \text{if } w_\infty = +1, \\ \\ \dfrac{1}{\Omega^-} \displaystyle\int_r^s \operatorname{Im} \omega_f & \text{if } w_\infty = -1, \end{cases}$$

where $\omega_f = 2\pi i f(z) dz$ and $\Omega^+, \Omega^- \in \mathbb{R}^{>0}$ are the unique periods with the property that the map I_f defined in this way takes values in $\mathbb{Z}$ and in no proper ideal of $\mathbb{Z}$. To simplify the exposition we assume for the rest of the article that $w_\infty = 1$, but the construction works very similarly for $w_\infty = -1$.

A *$\mathbb{Z}$-valued measure on* $\mathbb{P}^1(\mathbb{Q}_p)$ is a finitely additive function μ from the set of compact open subsets of $\mathbb{P}^1(\mathbb{Q}_p)$ to $\mathbb{Z}$. In [Dar01] Darmon attaches to each pair $r, s \in \mathbb{P}^1(\mathbb{Q})$ a $\mathbb{Z}$-valued measure $\mu_f\{r \to s\}$ on $\mathbb{P}^1(\mathbb{Q}_p)$ with total measure 0 by defining

$$\mu_f\{r \to s\}(\gamma \mathbb{Z}_p) := I_f\{\gamma^{-1} r \to \gamma^{-1} s\}.$$

This is enough to define $\mu_f\{r \to s\}$ for all compact open $U \subset \mathbb{P}_1(\mathbb{Q}_p)$, because either U or $\mathbb{P}^1(\mathbb{Q}_p) \setminus U$ is of the form $\gamma \mathbb{Z}_p$ for some $\gamma \in \Gamma$.

3.1.2. *Double multiplicative integrals.* If h is a continuous function on $\mathbb{P}_1(\mathbb{Q}_p)$ and μ is a measure on $\mathbb{P}^1(\mathbb{Q}_p)$ then the integral $\int_{\mathbb{P}^1(\mathbb{Q}_p)} h(x) d\mu(x)$ is defined by means of the Riemann sum

$$\int_{\mathbb{P}^1(\mathbb{Q}_p)} h(x) d\mu(x) = \lim_{\mathcal{U} = \{U_\alpha\}} \sum_\alpha h(x_\alpha) \mu(U_\alpha),$$

where the limit is taken over increasingly finer coverings $\mathcal{U}$ of $\mathbb{P}^1(\mathbb{Q}_p)$ by compact open subsets U_α, and x_α is any point in U_α. If μ is $\mathbb{Z}$-valued the *multiplicative integral* is defined by replacing the Riemann sum by a Riemann product:

$$\oint_{\mathbb{P}^1(\mathbb{Q}_p)} h(x) d\mu(x) = \lim_{\mathcal{U} = \{U_\alpha\}} \prod_\alpha h(x_\alpha)^{\mu(U_\alpha)}.$$

For $\tau_1, \tau_2 \in \mathcal{H}_p$ and $r, s \in \mathbb{P}^1(\mathbb{Q}_p)$ Darmon defines a K_p-valued *double integral* as

$$\int_{\tau_1}^{\tau_2} \int_r^s \omega_f = \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{x-\tau_2}{x-\tau_1}\right) d\mu_f\{r \to s\}(x),$$

where log denotes a fixed branch of the p-adic logarithm. Since $\mu_f\{r \to s\}$ takes values in $\mathbb{Z}$ a $K_p^\times$-valued *double multiplicative integral* can be defined as

$$\prod_{\tau_1}^{\tau_2} \int_r^s \omega_f = \prod_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{x-\tau_2}{x-\tau_1}\right) d\mu_f\{r \to s\}(x).$$

These two integrals are related by the formula

$$\int_{\tau_1}^{\tau_2} \int_r^s \omega_f = \log\left(\prod_{\tau_1}^{\tau_2} \int_r^s \omega_f\right).$$

3.1.3. *Semi-indefinite integrals.* The double multiplicative integral satisfies the usual additivity properties with respect to the limits, as well as the Γ-invariance property

$$\prod_{\gamma\tau_1}^{\gamma\tau_2} \int_{\gamma r}^{\gamma s} \omega_f = \prod_{\tau_1}^{\tau_2} \int_r^s \omega_f \quad \text{for all } \gamma \in \Gamma.$$

Therefore, it gives rise to a group homomorphism

$$\mathrm{Int}^\times \colon \left(\mathrm{Div}^0(\mathcal{H}_p) \otimes \mathrm{Div}^0(\mathbb{P}^1(\mathbb{Q}))\right)_\Gamma \longrightarrow K_p^\times,$$

where the subscript Γ denotes the subgroup of Γ-coinvariants. Let $\mathbb{Z}[\Gamma]$ denote the group ring of Γ and let I_Γ denote the augmentation ideal, defined by the exact sequence

$$0 \longrightarrow I_\Gamma \longrightarrow \mathbb{Z}[\Gamma] \longrightarrow \mathbb{Z} \longrightarrow 0.$$

Tensoring with I_Γ over $\mathbb{Z}$ and taking Γ-coinvariants gives

$$0 \longrightarrow K_\Gamma \longrightarrow (I_\Gamma \otimes I_\Gamma)_\Gamma \xrightarrow{r} (\mathbb{Z}[\Gamma] \otimes I_\Gamma)_\Gamma \longrightarrow (I_\Gamma)_\Gamma \longrightarrow 0. \tag{3.1}$$

Since I_Γ is generated over $\mathbb{Z}$ by elements of the form $\gamma - 1$, choosing base points $\tau \in \mathcal{H}_p$ and $x \in \mathbb{P}^1(\mathbb{Q})$ one can define integration maps

$$\mathrm{Int}^\times_{\tau,x} \colon (I_\Gamma \otimes I_\Gamma)_\Gamma \longrightarrow K_p^\times$$

determined by

$$\mathrm{Int}^\times_{\tau,x}((\gamma_0 - 1) \otimes (\gamma_1 - 1)) = \int_\tau^{\gamma_0\tau} \int_x^{\gamma_1 x} \omega_f, \quad \text{for } \gamma_0, \gamma_1 \in \Gamma. \tag{3.2}$$

Letting $\Lambda = I_{\tau,x}(K_\Gamma) \subset K_p^\times$ yields a well defined map

$$\mathrm{Int}^\times_{\tau,x} \colon \mathrm{Im}(r) \longrightarrow K_p^\times/\Lambda. \tag{3.3}$$

The group $(I_\Gamma)_\Gamma \simeq \Gamma_{ab}$ is finite, say of exponent e_Γ. If $y = \gamma x \in \mathbb{P}^1(\mathbb{Q})$ is in the same Γ-orbit as x, define

$$\prod_x^\tau \int_x^y e_\Gamma \omega_f := \mathrm{Int}^\times_{\tau,x}(e_\Gamma \cdot 1 \otimes (\gamma - 1)) \in K_p^\times/\Lambda.$$

This *semi-indefinite integral* satisfies the following properties:

(1) $\prod_r^\tau \int_r^s e_\Gamma\omega_f \times \prod_s^\tau \int_s^t e_\Gamma\omega_f = \prod_r^\tau \int_r^t e_\Gamma\omega_f$, for all $\tau \in \mathcal{H}_p$, $r, s, t \in \Gamma x$;
(2) $\prod_r^{\tau_2} \int_r^s e_\Gamma\omega_f \div \prod_r^{\tau_1} \int_r^s e_\Gamma\omega_f = \prod_{\tau_1}^{\tau_2} \int_r^s e_\Gamma\omega_f$, for all $\tau_1, \tau_2 \in \mathcal{H}_p$, $r, s \in \Gamma x$;

(3) $\int\!\!\!\!\!\!\diagup^{\gamma\tau}_{\gamma r} \int_{\gamma r}^{\gamma s} e_\Gamma \omega_f = \int\!\!\!\!\!\!\diagup^{\tau}_{r} \int_{r}^{s} e_\Gamma \omega_f$, for all $\gamma \in \Gamma$.

3.1.4. *Darmon points.* Let q denote the p-adic period of E and let $\Phi_{\mathrm{Tate}}\colon K_p^\times/q^{\mathbb{Z}} \to E(K_p)$ be Tate's uniformization map.

Given $\tau \in \mathcal{H}_p \cap K$, let $\mathcal{O}_\tau$ be the ring of matrices in R that have the vector $(\tau, 1)$ as eigenvector, which is isomorphic to a $\mathbb{Z}[1/p]$-order of K. Let H_τ denote the ring class field of $\mathcal{O}_\tau$ which we can, and do, view as a subfield of K_p by choosing a prime of H_τ above p. By Dirichlet's unit theorem the stabilizer Γ_τ of τ in Γ is a cyclic group of infinite order isomorphic to $\mathcal{O}_{\tau,1}^\times/\langle\pm 1\rangle$. Let γ_τ be a generator of Γ_τ, and define

$$J_\tau = \int\!\!\!\!\!\!\diagup^{\tau}_{\infty} \int_{\infty}^{\gamma_\tau \infty} e_\Gamma \omega_f.$$

Conjecture 3.1 (Darmon)**.** *The local point $P_\tau = \Phi_{\mathrm{Tate}}(J_\tau)$ belongs to $E(H_\tau)$.*

3.2. **Computation of semi-indefinite integrals.** In order to effectively compute the points J_τ one needs to compute the semi-indefinite integrals

$$\int\!\!\!\!\!\!\diagup^{\tau}_{\infty} \int_{\infty}^{\gamma_\tau \infty} e_\Gamma \omega_f. \tag{3.4}$$

The method used in [DG02] and [DP06] boils down to using properties (1), (2) and (3) of semi-indefinite integrals to express them in terms of double integrals, which can be effectively computed either via Riemann products as in [DG02] or, more efficiently, via overconvergent modular symbols as in [DP06].

The algorithm for expressing semi-indefinite integrals in terms of double integrals of [DG02] and [DP06] is based on the continued fraction algorithm, and it only works under the assumption that $M = 1$ (i.e., that E has conductor equal to p). In this section we introduce an algorithm that, assuming GRH, works for all levels M. In Section 3.3 we will see that the resulting definite double integrals obtained by this method can also be computed using overconvergent modular symbols, by suitably adapting the techniques of [DP06].

In order to simplify the description of the algorithm, let us make the following inessential assumption on f (cf. Remark 3.5 for how the algorithm works without it):

Assumption 3.2. There is a $d > 1$, $d \mid M$ such that f has eigenvalue 1 with respect to the Atkin-Lehner operator W_d.

Observe that if M is a composite integer then Assumption 3.2 is always fulfilled. Indeed, if p_1 and p_2 are distinct prime divisors of M such that f has eigenvalue -1 with respect to W_{p_1} and W_{p_2}, then f has eigenvalue 1 with respect to $W_{p_1 p_2}$.

Remark 3.3. Under Assumption 3.2, the double multiplicative integral is also invariant under the matrix $w_d = \left(\begin{smallmatrix} 0 & 1 \\ -d & 0 \end{smallmatrix}\right)$:

$$\int\!\!\!\!\!\!\diagup^{w_d\tau_2}_{w_d\tau_1} \int_{w_d r}^{w_d s} e_\Gamma \omega_f = \int\!\!\!\!\!\!\diagup^{\tau_2}_{\tau_1} \int_{r}^{s} e_\Gamma \omega_f.$$

Let $\tilde{\Gamma}$ be the subgroup of $\mathrm{PGL}_2(\mathbb{Q})$ generated by Γ and w_d. Then, by replacing Γ by $\tilde{\Gamma}$ in the argument of Section 3.3 one can extend the definition of the semi-indefinite integrals $\int\!\!\!\!\!\!\diagup^{\tau}_{r} \int_r^s e_\Gamma \omega_f$ to all pairs $r, s \in \mathbb{P}^1(\mathbb{Q})$ lying in the same $\tilde{\Gamma}$-orbit.

Let Γ_1 be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}[1/p])$ defined as

$$\Gamma_1 = \{\gamma \in \Gamma \colon \gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod{M}\} \subset \Gamma.$$

Using the properties of the multiplicative integral it is easy to see that

$$(J_\tau)^m = \fint_\tau \int_\infty^{\gamma_\tau^m \infty} \omega_f.$$

Therefore, replacing P_τ by a multiple of it if necessary we can always assume that γ_τ belongs to Γ_1 (but see also Remark 3.4).

Observe that Γ_1 is one of the groups treated in Section 2. Indeed, with the notation as in that section, if we let $F = \mathbb{Q}$, $S = \{\infty, p\}$ and $\mathfrak{N} = M \cdot \mathbb{Z}[1/p]$ we have that $\Gamma_1 = \Gamma_1(\mathfrak{N})$. In particular, the algorithm described in Theorem 2.3 gives an algorithmic method (under our running assumption of GRH) for computing a decomposition of γ_τ of the form

$$\gamma_\tau = U_1 L_1 U_2 L_2 U_3, \tag{3.5}$$

where the matrices U_i and L_i are of the form

$$U_i = \begin{pmatrix} 1 & x_i \\ 0 & 1 \end{pmatrix} \text{ for some } x_i \in \mathbb{Z}[1/p], \quad L_i = \begin{pmatrix} 1 & 0 \\ y_i & 1 \end{pmatrix} \text{ for some } y_i \in M \cdot \mathbb{Z}[1/p].$$

In particular, L_i and U_i belong to Γ. Then, for $G \in \Gamma$ we have that

$$\fint_\tau \int_\infty^{U_i G \infty} e_\Gamma \omega_f = \fint_{U_i^{-1}\tau} \int_\infty^{G\infty} e_\Gamma \omega_f \tag{3.6}$$

and

$$\begin{aligned} \fint_\tau \int_\infty^{L_i G \infty} e_\Gamma \omega_f &= \fint_\tau \int_\infty^0 e_\Gamma \omega_f \times \fint_\tau \int_0^{L_i G \cdot \infty} e_\Gamma \omega_f \\ &= \fint_\tau \int_\infty^0 e_\Gamma \omega_f \times \fint_{L_i^{-1}\cdot\tau} \int_0^{G\cdot\infty} \omega_f^+ \\ &= \fint_\tau \int_\infty^0 e_\Gamma \omega_f \times \fint_{L_i^{-1}\cdot\tau} \int_0^{\infty} e_\Gamma \omega_f \times \fint_{L_i^{-1}\cdot\tau} \int_\infty^{G\cdot\infty} e_\Gamma \omega_f \\ &= \fint_\tau^{L_i^{-1}\cdot\tau} \int_0^{\infty} e_\Gamma \omega_f \times \fint_{L_i^{-1}\cdot\tau} \int_\infty^{G\cdot\infty} e_\Gamma \omega_f. \end{aligned} \tag{3.7}$$

In view of decomposition (3.5), repeated application of (3.6) and (3.7) transforms the semi-indefinite integral (3.4) into a product of double multiplicative integrals. Observe that Assumption 3.2 is used in (3.7) because of the integral $\fint_\tau^\tau \int_\infty^0 e_\Gamma \omega_f$. Indeed, the cusps 0 and ∞ are never in the same Γ-orbit if $M > 1$. But since $w_d \infty = 0$, they are in the same $\tilde{\Gamma}$-orbit. Therefore, the integral $\fint_\tau^\tau \int_\infty^0 e_\Gamma \omega_f$ is well-defined by Remark 3.3.

Remark 3.4. As we already mentioned, one can overcome the fact that $\gamma_\tau = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ does not generally belong to Γ_1 by computing an appropriate power $(J_\tau)^m$. In some cases one can apply an alternative procedure instead. This turns out to be more convenient in the actual computations and it allows for the computation of J_τ itself. Namely, if $a \equiv p^n \pmod{M}$ for some integer n, then the matrix $g = \begin{pmatrix} p^{-n} & 0 \\ 0 & p^n \end{pmatrix}$

belongs to Γ and

$$J_\tau = \not\int^{\tau} \int_\infty^{\gamma_\tau \infty} e_\Gamma \omega_f = \not\int^{g\tau} \int_\infty^{g\gamma_\tau \infty} e_\Gamma \omega_f$$

with $g\gamma_\tau$ belonging to Γ_1.

Remark 3.5. The manipulations of the semi-indefinite integrals (3.7) are similar to, and can be seen as a generalization of, those of [DG02] and [DP06]. However, they are only valid under Assumption 3.2. In case f does not satisfy this assumption one can then directly compute a preimage of an appropriate multiple of $1 \otimes \gamma_\tau$ by the map r of (3.1) as follows. First of all, if we let $P = \left(\begin{smallmatrix} p & 0 \\ 0 & 1/p \end{smallmatrix}\right)$, $U_x = \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ and $L_y = \left(\begin{smallmatrix} 1 & 0 \\ y & 1 \end{smallmatrix}\right)$ we have that

$$PU_xP^{-1} = U_{p^2x}, \quad P^{-1}L_yP = L_{p^2y}. \tag{3.8}$$

If we let $e = p^2 - 1$, relations (3.8) show that U_x^e and L_y^e can be written as products of commutators in Γ. Combining this with (3.5) one can algorithmically decompose γ_τ^e as a product of commutators. By using the identity in I_Γ

$$gh - 1 = (g-1)(h-1) + (g-1) + (h-1),$$

one deduces first that

$$0 = (gg^{-1} - 1) = (g-1)(g^{-1}-1) + (g-1) + (g^{-1}-1),$$

and hence:

$$\begin{aligned} ghg^{-1}h^{-1} - 1 = {} & (gh-1)(g^{-1}h^{-1}-1) + (g-1)(h-1) \\ & + (g^{-1}-1)(h^{-1}-1) - (g-1)(g^{-1}-1) - (h-1)(h^{-1}-1). \end{aligned}$$

We can then find an expression of $\gamma_\tau^e - 1$ as an element of I_Γ^2, namely $\gamma_\tau^e - 1 = \sum_i (\alpha_i - 1)(\beta_i - 1)$. Thus in $(\mathbb{Z}[\Gamma] \otimes I_\Gamma)_\Gamma$ we have that

$$\begin{aligned} e(1 \otimes (\gamma_\tau - 1)) = 1 \otimes (\gamma_\tau^e - 1) &= \sum_i 1 \otimes (\alpha_i - 1)(\beta_i - 1) \\ &= \sum_i 1 \otimes \alpha_i(\beta_i - 1) - 1 \otimes (\beta_i - 1) \\ &= \sum_i \alpha_i^{-1} \otimes (\beta_i - 1) - 1 \otimes (\beta_i - 1) \\ &= \sum_i (\alpha_i^{-1} - 1) \otimes (\beta_i - 1), \end{aligned}$$

which gives a preimage of $e(1 \otimes (\gamma_\tau - 1))$ under the map r. Then the semi-indefinite integral is computed using (3.2).

3.3. **Computation of the definite double integrals.** As we have seen in Subsection 3.2 the computation of J_τ is reduced to products of integrals of the form

$$\not\int_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{x - \tau_2}{x - \tau_1}\right) d\mu_f\{r \to s\}(x). \tag{3.9}$$

Write μ for the measure $\mu_f\{r \to s\}$, and consider a decomposition of $\mathbb{P}^1(\mathbb{Q}_p)$ into a disjoint union of L open balls of the form

$$\mathbb{P}^1(\mathbb{Q}_p) = \bigcup_{i=1}^{L} g_i \cdot \mathbb{Z}_p, \quad g_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}), \tag{3.10}$$

which will be fixed later. This yields in turn a decomposition

$$⨍_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{x-\tau_2}{x-\tau_1}\right) d\mu(x) = \prod_{i=1}^{L} ⨍_{g_i\mathbb{Z}_p} \left(\frac{x-\tau_2}{x-\tau_1}\right) d\mu(x).$$

Fix such an i and let $g = g_i$ be the corresponding matrix, written $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. We are thus reduced to calculating

$$⨍_{g\mathbb{Z}_p} \left(\frac{x-\tau_2}{x-\tau_1}\right) d\mu(x).$$

Apply the change of variables $x = g \cdot t$ to get

$$⨍_{g\mathbb{Z}_p} \left(\frac{x-\tau_2}{x-\tau_1}\right) d\mu(x) = ⨍_{\mathbb{Z}_p} \left(\frac{g\cdot t-\tau_2}{g\cdot t-\tau_1}\right) d\mu(g\cdot t).$$

Let $\log_p$ be the unique homomorphism $K_p^\times \to K_p$ such that $\log_p(1-t) = -\sum_{n=1}^{\infty} t^n/n$ and $\log_p(p) = 0$. It is surjective, with kernel

$$\ker\left(\log_p \colon K_p^\times \to K_p\right) = p^{\mathbb{Z}} \times \mathbf{U},$$

where $\mathbf{U}$ is the group of roots of unity in $K_p^\times$. Suppose that we can express the integrand as a power series in t of the form

$$\left(\frac{g\cdot t-\tau_2}{g\cdot t-\tau_1}\right) = \alpha_0 \left(1 + \sum_{n=1}^{\infty} \alpha_n p^n t^n\right), \tag{3.11}$$

with α_n belonging to $\mathcal{O}_p$, the ring of integers of K_p, for all $n \geq 1$. Then the expression in (3.11) converges for $t \in \mathbb{Z}_p$ and is constant modulo $p^{v_p(\alpha_0)+1}$. Therefore the expression of (3.9) can be determined modulo $p^{v_p(\alpha_0)+1}$ by evaluating L truncated power series. The logarithm $\log_p(J_\tau)$ is evaluated by noting that

$$\log_p\left(\alpha_0(1+\sum \alpha_n p^n t^n)\right) = \log_p \alpha_0 + \sum_{n=1}^{\infty} \beta_n \frac{p^n t^n}{n},$$

for a sequence of $\beta_n \in \mathcal{O}_p$. By interchanging the infinite sum with the integral, to compute $\log_p(J_\tau)$ it is enough to compute

$$\int_{\mathbb{Z}_p} t^n d\mu(g\cdot t) = \int_{g\mathbb{Z}_p} (g^{-1}\cdot t)^n d\mu(t),$$

which is the nth moment of μ at $g\mathbb{Z}_p$. This data can be efficiently computed in time polynomial in the number of p-adic digits of precision, thanks to the methods of Darmon and Pollack (see for instance [DP06, display 23]). Finally, one recovers J_τ via the formula

$$J_\tau = p^{v_p(J_\tau)} \cdot \zeta \cdot \exp_p(\log_p J_\tau),$$

where ζ is the Teichmuller lift of the unit part modulo p of the multiplicative integral. Note also that $v_p(J_\tau)$ is the sum of the valuations of the α_0 appearing in

the decomposition (3.10). In order to find the power series in (3.11), we calculate:

$$\begin{aligned}\frac{gt-\tau_2}{gt-\tau_1} &= \frac{\frac{at+b}{ct+d}-\tau_2}{\frac{at+b}{ct+d}-\tau_1}\\ &= \frac{(a-c\tau_2)t+(b-d\tau_2)}{(a-c\tau_1)t+(b-d\tau_1)}\\ &= \frac{b-d\tau_2}{b-d\tau_1}\frac{1+t\frac{c\tau_2-a}{d\tau_2-b}}{1+t\frac{c\tau_1-a}{d\tau_1-b}}\\ &= \frac{b-d\tau_2}{b-d\tau_1}\left(1+\frac{\overline{g}\tau_1-\overline{g}\tau_2}{\overline{g}\tau_1}\sum_{i=1}^{\infty}(-1)^n(\overline{g}\tau_1)^n t^n\right)\end{aligned}$$

where $\overline{g}$ is the matrix

$$\overline{g} = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} g^{-1}.$$

Note that for any two matrices g, h we have $\overline{hg} = \overline{g}h^{-1}$. Also, for any choice of h, a decomposition

$$\mathbb{P}^1(\mathbb{Q}_p) = \bigcup_i g_i \cdot \mathbb{Z}_p$$

gives rise to another decomposition

$$\mathbb{P}^1(\mathbb{Q}_p) = \bigcup_i (hg_i) \cdot \mathbb{Z}_p.$$

Therefore by choosing an appropriate $h \in \mathrm{GL}_2(\mathbb{Q}_p) \cap M_2(\mathbb{Z})$ we can assume that $v_p(\tau_1 - a) = 0$ for all $a = 0, 1, \ldots, p-1$ and that $v_p(\tau_2) \geq 0$.

In order to obtain a power series as in (3.11), the matrices $g = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ that we consider should satisfy

$$v_p\left(\frac{c\tau_1 - a}{d\tau_1 - b}\right) \geq 1. \tag{3.12}$$

The conditions on τ_1 and τ_2 imply that the matrix corresponding to the contribution of $\mathbb{P}^1(\mathbb{Q}_p)\backslash\mathbb{Z}_p$ satisfies (3.12), and we concentrate on the integral on $\mathbb{Z}_p$. Let $r \geq 0$ be the largest integer such that τ_1 is congruent to some integer modulo p^r. Let $t_1 \in \mathbb{Z}$ be a representative for the class of $\tau_1 \pmod{p^r}$. Write also $t^{(i)}$ for the representative of $t_1 \pmod{p^i}$ in the range $0, \ldots, p^i - 1$. We can then use the decomposition given by the matrices g in the set $G = \cup_{i=1}^{r+1} G_i$, where

$$\begin{aligned}G_i &= \left\{\begin{pmatrix}p^i & t^{(i)} + bp^{i-1}\\ 0 & 1\end{pmatrix} \mid b = 1, \ldots, p-1\right\} \qquad i = 1, \ldots, r,\\ G_{r+1} &= \left\{\begin{pmatrix}p^{r+1} & p^r b\\ 0 & 1\end{pmatrix} \mid b = 0, \ldots, p-1\right\}.\end{aligned}$$

Together with $\mathbb{P}^1(\mathbb{Q}_p)\backslash\mathbb{Z}_p$ this yields a decomposition of $\mathbb{P}^1(\mathbb{Q}_p)$ into $p+1+r(p-1)$ opens.

3.4. **Numerical computations.** To test our methods we have written a Sage implementation of the above algorithms, modifying an existing implementation written by Robert Pollack which in turn adapted part of the code originally written in Magma by Darmon and Pollack ([DP06]). The code can be found on the second author's web page.

Given an elliptic curve of conductor $N = pM$ and a quadratic field K, the code finds all the optimal embeddings of level N of K into $M_2(\mathbb{Z}[\frac{1}{p}])$, and computes the Stark-Heegner integral corresponding to the fixed point of K acting on $\mathcal{H}_p$ via each embedding to a prescribed precision. The Tate parametrization yields the coordinates of the Stark-Heegner point on $E(K_p)$ which are then recognized as algebraic coordinates using standard routines.

Apart from gathering numerical evidence in support of Darmon's conjecture, it is also worth remarking that the relative large height of the points thus found would make it impossible to find them using naive point search methods. This is, therefore, the only known method to finding points of infinite order on such curves.

The rest of this subsection contains the evidence that we have collected in support of Conjecture 3.1. Although the algorithm works for arbitrary $M > 1$ (provided that all its prime factors split in K), we do not intend to be exhaustive and we just provide some examples of curves of small composite conductor. For each of these curves we consider all the real quadratic fields K of discriminant $D < 200$ allowed by the splitting conditions on p and M; for each such field, we consider $\tau \in \mathcal{H}_p$ such that H_τ equals the Hilbert class field of K, and we are able to recognize in all the cases P_τ as an algebraic point defined over the Hilbert class field of K. For those fields with nontrivial class group, we give the relative minimal polynomial h_D of the X-coordinate of the point.

D	h	P^+
13	1	$\left(-\sqrt{13}+1, 2\sqrt{13}-4\right)$
28	1	$\left(-15\sqrt{7}+43, 150\sqrt{7}-402\right)$
37	1	$\left(-\frac{5}{9}\sqrt{37}+\frac{5}{9}, \frac{25}{27}\sqrt{37}-\frac{70}{27}\right)$
73	1	$\left(-\frac{17}{32}\sqrt{73}+\frac{77}{32}, \frac{187}{128}\sqrt{73}-\frac{1199}{128}\right)$
88	1	$\left(-\frac{17}{9}, \frac{14}{27}\sqrt{22}+\frac{4}{9}\right)$
97	1	$\left(-\frac{25}{121}\sqrt{97}+\frac{123}{121}, \frac{375}{2662}\sqrt{97}-\frac{4749}{2662}\right)$
133	1	$\left(\frac{103}{9}, \frac{92}{27}\sqrt{133}-\frac{56}{9}\right)$
172	1	$\left(-\frac{1923}{1681}, \frac{11781}{68921}\sqrt{43}+\frac{121}{1681}\right)$
193	1	$\left(\frac{1885}{288}\sqrt{193}+\frac{25885}{288}, \frac{292175}{3456}\sqrt{193}+\frac{4056815}{3456}\right)$

TABLE 1. Points on elliptic curve 15A1, with $p = 5$

D	h	P^+
8	1	$\left(-9\sqrt{2}+11, 45\sqrt{2}-64\right)$
29	1	$\left(-\frac{9}{25}\sqrt{29}+\frac{32}{25}, \frac{63}{125}\sqrt{29}-\frac{449}{125}\right)$
44	1	$\left(-\frac{9}{49}\sqrt{11}-\frac{52}{49}, \frac{54}{343}\sqrt{11}+\frac{557}{343}\right)$
53	1	$\left(-\frac{37}{169}\sqrt{53}+\frac{184}{169}, \frac{555}{2197}\sqrt{53}-\frac{5633}{2197}\right)$
92	1	$\left(\frac{533}{46}, \frac{17325}{2116}\sqrt{23}-\frac{533}{92}\right)$
137	1	$\left(-\frac{1959}{11449}\sqrt{137}+\frac{242}{11449}, \frac{295809}{2450086}\sqrt{137}-\frac{162481}{2450086}\right)$
149	1	$\left(-\frac{261}{2809}\sqrt{149}+\frac{2468}{2809}, \frac{8091}{148877}\sqrt{149}-\frac{101789}{148877}\right)$
197	1	$\left(-\frac{79135143}{209961032}\sqrt{197}+\frac{977125081}{209961032}, \frac{1439547386313}{1075630366936}\sqrt{197}-\frac{9297639417941}{537815183468}\right)$

D	h	$h_D(x)$
65	2	$x^2+\left(\frac{61851}{6241}\sqrt{65}-\frac{491926}{6241}\right)x-\frac{403782}{6241}\sqrt{65}+\frac{3256777}{6241}$

TABLE 2. Points on elliptic curve 21A1, with $p=3$

D	h	P^+
13	1	$\left(-\frac{1}{2}\sqrt{13}+\frac{3}{2}, \frac{1}{2}\sqrt{13}-\frac{7}{2}\right)$
28	1	$\left(\frac{22}{7}, \frac{55}{49}\sqrt{7}-\frac{11}{7}\right)$
61	1	$\left(-\frac{1}{2}\sqrt{61}+\frac{5}{2}, \sqrt{61}-11\right)$
73	1	$\left(-\frac{53339}{49928}\sqrt{73}+\frac{324687}{49928}, \frac{31203315}{7888624}\sqrt{73}-\frac{290996167}{7888624}\right)$
76	1	$\left(-2, \sqrt{19}+1\right)$
109	1	$\left(-\frac{143}{2}\sqrt{109}+\frac{1485}{2}, \frac{5577}{2}\sqrt{109}-\frac{58223}{2}\right)$
172	1	$\left(-\frac{51842}{21025}, \frac{2065147}{3048625}\sqrt{43}+\frac{25921}{21025}\right)$
184	1	$\left(\frac{59488}{21609}, \frac{109252}{3176523}\sqrt{46}-\frac{29744}{21609}\right)$
193	1	$\Big(\frac{94663533349261}{678412148664608}\sqrt{193}+\frac{1048806825770477}{678412148664608}, \frac{1477789579209312993 17}{12494688311813553741184}\sqrt{193}+\frac{308629344930924160355 41}{12494688311813553741184}\Big)$

D	h	$h_D(x)$
40	2	$x^2+\left(\frac{2849}{1681}\sqrt{10}-\frac{6347}{1681}\right)x-\frac{5082}{1681}\sqrt{10}+\frac{16819}{1681}$
85	2	$x^2+\left(\frac{119}{361}\sqrt{85}-\frac{1022}{361}\right)x-\frac{168}{361}\sqrt{85}+\frac{1549}{361}$
145	4	$x^4+\left(\frac{169016003453}{83168215321}\sqrt{145}-\frac{1621540207320}{83168215321}\right)x^3$ $+\left(-\frac{1534717557538}{83168215321}\sqrt{145}+\frac{18972823294799}{83168215321}\right)x^2$ $+\left(\frac{5533405190489}{83168215321}\sqrt{145}-\frac{66553066916820}{83168215321}\right)x$ $+-\frac{6414913389456}{83168215321}\sqrt{145}+\frac{77248348177561}{83168215321}$

TABLE 3. Points on elliptic curve 33A1, with $p = 11$

D	h	P^+
24	1	$\left(\frac{12565}{19321}\sqrt{6}+\frac{31879}{19321}, \frac{4020800}{2685619}\sqrt{6}+\frac{12075417}{2685619}\right)$
41	1	$\left(70\sqrt{41}+449, 2100\sqrt{41}+13443\right)$
61	1	$\left(\frac{7444913385}{279945122}\sqrt{61}+\frac{58532610047}{279945122}, \frac{1805488279736505}{3312030738382}\sqrt{61}+\frac{14113780406002997}{3312030738382}\right)$
69	1	$\left(\frac{63742245}{280513298}\sqrt{69}+\frac{526671623}{280513298}, \frac{1810980922695}{3322118988214}\sqrt{69}+\frac{16959961136217}{3322118988214}\right)$
76	1	$\Big(-\frac{4398502037370}{1404725114521}\sqrt{19}+\frac{19299436937929}{1404725114521},$ $\frac{28304052715333334100}{1664895657706548931}\sqrt{19}-\frac{121810800584629037164}{1664895657706548931}\Big)$
89	1	$\left(\frac{981}{100}, \frac{3563}{1000}\sqrt{89}-\frac{1}{2}\right)$
101	1	$\left(\frac{7505}{10404}, \frac{310345}{1061208}\sqrt{101}-\frac{1}{2}\right)$
124	1	$\left(-\frac{210}{1681}\sqrt{31}+\frac{12769}{1681}, \frac{35700}{68921}\sqrt{31}-\frac{1678197}{68921}\right)$
129	1	$\Big(\frac{9526581863470}{129638878212649}\sqrt{129}+\frac{154639065911401}{129638878212649},$ $\frac{2271557238511427027 00}{1476056210913547737643}\sqrt{129}+\frac{5024283358306642389249}{1476056210913547737643}\Big)$
181	1	$\left(-\frac{4166720}{31843449}, \frac{7889580565}{359385165414}\sqrt{181}-\frac{1}{2}\right)$

D	h	$h_D(x)$
104	2	$x^2-\frac{87841}{9522}x+\frac{85397}{6348}$
136	2	$x^2+\left(\frac{132755895957027}{12703756878289}\sqrt{34}-\frac{805260717153160}{12703756878289}\right)x$ $-\frac{4207164401474475}{12703756878289}\sqrt{34}+\frac{24540106232139359}{12703756878289}$

TABLE 4. Points on elliptic curve 35A1, with $p=7$

D	h	P^+
8	1	$\left(\frac{1}{2}, \frac{1}{4}\sqrt{2} - \frac{1}{2}\right)$
53	1	$\left(\frac{3}{2}\sqrt{53} + \frac{23}{2}, \frac{15}{2}\sqrt{53} + \frac{107}{2}\right)$
77	1	$\left(\frac{5559}{55778}\sqrt{77} + \frac{78911}{55778}, \frac{2040153}{9314926}\sqrt{77} + \frac{17804737}{9314926}\right)$
89	1	$\left(\frac{793511}{2401}, \frac{150079871}{235298}\sqrt{89} - \frac{1}{2}\right)$
101	1	$\Big(-\frac{656788148124048}{108395925566683225}\sqrt{101} + \frac{108663526315570777}{108395925566683225},$ $\frac{432742605985104670344096}{356877721184597834222521 25}\sqrt{101} - \frac{715518602160795519413833 54}{356877721184597834222521 25}\Big)$
137	1	$\left(\frac{83}{81}, \frac{193}{1458}\sqrt{137} - \frac{1}{2}\right)$
149	1	$\Big(-\frac{41662615293}{110013332450}\sqrt{149} + \frac{802189306199}{110013332450},$ $\frac{39791672228037249}{25801976926160750}\sqrt{149} - \frac{635290450369692907}{25801976926160750}\Big)$
152	1	$\Big(-\frac{1915814571}{20670100441}\sqrt{38} + \frac{24731592007}{20670100441},$ $\frac{577303899566856}{2971761010503011}\sqrt{38} - \frac{7167395643538198}{2971761010503011}\Big)$
161	1	$\left(\frac{62146167667}{49710362300}, \frac{8395974419456303}{53153799096521000}\sqrt{161} - \frac{1}{2}\right)$
188	1	$\Big(\frac{3178296211866}{1135825194001}\sqrt{47} + \frac{22525829850817}{1135825194001},$ $\frac{21864116230891316004}{1210506836331759751}\sqrt{47} + \frac{148356498531472446055}{1210506836331759751}\Big)$

D	h	$h_D(x)$
104	2	$x^2 + \left(-\frac{992302702743}{1960400420449}\sqrt{26} - \frac{57132410901980}{1960400420449}\right)x$ $-\frac{4968445297101}{1960400420449}\sqrt{26} + \frac{61480175149213}{1960400420449}$
140	2	$x^2 - \frac{7073157}{13924}x + \frac{398237221}{55696}$
185	2	$x^2 + \left(-\frac{908505900}{7532677681}\sqrt{185} - \frac{54207252962}{7532677681}\right)x$ $-\frac{787814100}{7532677681}\sqrt{185} + \frac{45005684581}{7532677681}$

TABLE 5. Points on elliptic curve 51A1, with $p = 3$

D	h	P^+
29	1	$2 \cdot \left(\frac{5}{2}\sqrt{29} + \frac{29}{2}, \frac{25}{2}\sqrt{29} + \frac{133}{2}\right)$
44	1	$\left(\frac{47}{36}, \frac{13}{54}\sqrt{11} - \frac{83}{72}\right)$
149	1	$\left(\frac{41297}{48050}\sqrt{149} + \frac{554429}{48050}, \frac{28371039}{7447750}\sqrt{149} + \frac{340434623}{7447750}\right)$

TABLE 6. Points on elliptic curve 105A1, with $p = 3$

4. Computation of ATR Darmon points on curves of non-trivial conductor

In Section 3 we have seen that the algorithm of Theorem 2.3 can be used in the computation of the semi-indefinite integrals entering the definition of p-adic Darmon points. It is a substitute for the continued fractions trick of [DG02] and [DP06].

There is another type of Darmon points, called ATR, whose definition also relies in certain semi-indefinite integrals. Although the framework is different (e.g., they are points on elliptic curves over number fields, and the integrals are complex instead of p-adic), the formal properties satisfied by the semi-indefinite integrals are the same in both settings. In the ATR case, the continued fraction algorithm over number fields had been used for computing ATR points on curves with trivial conductor (cf. [DL03], [GM13]). Using a method analogous to that of Section 3.2, Theorem 2.3 also allows for the computation of ATR points on curves with non-trivial conductor.

To be more precise, let F be a real quadratic number field of narrow class number 1 and let $\mathcal{O}$ denote its ring of integers. Let E be an elliptic curve over F of conductor $\mathfrak{N}$, and let Γ be the congruence subgroup consisting of matrices in $\mathrm{SL}_2(\mathcal{O})$ that are upper triangular modulo $\mathfrak{N}$. Assuming that E is modular, there is a Hilbert modular form f of parallel weight two and level $\mathfrak{N}$ whose L-series coincides with that of E. Let ω_f denote the corresponding Γ-invariant differential 2-form on $\mathcal{H}\times\mathcal{H}$ (with Γ acting on it via the product of the two embeddings of F into $\mathbb{R}$).

The following is analogous to Assumption 3.2.

Assumption 4.1. There exists an ideal $\mathfrak{D}\mid\mathfrak{N}$ such that f has eigenvalue 1 for the Atkin–Lehner operator $W_{\mathfrak{D}}$.

Let $\tilde{\Gamma}$ be the subgroup of $\mathrm{PGL}_2(F)$ generated by Γ and the Atkin–Lehner matrix corresponding to $W_{\mathfrak{D}}$. The previous assumption guarantees that $0,\infty\in\mathbb{P}^1(F)$ are $\tilde{\Gamma}$-related.

Let K be a quadratic almost totally real (ATR) extension of F; i.e., a quadratic extension of F that has exactly one non-real archimedean place. Suppose that all primes dividing $\mathfrak{N}$ are split in K. We refer the reader to [DL03] and [Dar04, §8] for the definition of the semi-indefinite integrals in this setting. We will just mention that they are expressions of the form

$$\int^{\tau}\int_{x}^{y}\omega_f^{+}\in\mathbb{C}/\Lambda_f,$$

where $\tau\in\mathcal{H}$, $x,y\in\mathbb{P}^1(F)$ are in the same $\tilde{\Gamma}$-orbit, Λ_f is a certain period lattice that depends on f, and ω_f^+ is a non-holomorphic differential easily related to ω_f. They satisfy analogous properties to those of p-adic semi-indefinite integrals; namely

(i) $\int^{\gamma\tau}\int_{\gamma r}^{\gamma s}\omega_f^+=\int^{\tau}\int_r^s\omega_f^+$ for all $\gamma\in\tilde{\Gamma}$, $\quad r,s\in\tilde{\Gamma}x$,
(ii) $\int^{\tau}\int_r^s\omega_f^+ + \int^{\tau}\int_r^s\omega_f^+=\int^{\tau}\int_r^s\omega_f^+$, for all $\tau\in\mathcal{H}$, $\quad r,s\in\tilde{\Gamma}x$,
(iii) $\int^{\tau_2}\int_r^s\omega_f^+ - \int^{\tau_1}\int_r^s\omega_f^+=\int_{\tau_1}^{\tau_2}\int_r^s\omega_f^+$, for all $\tau_1,\tau_2\in\mathcal{H}$, $\quad r,s\in\tilde{\Gamma}x$.

ATR Darmon points are given by expressions of the form $P_\tau=\Phi(\lambda\int^{\tau}\int_{\infty}^{\gamma_\tau\infty}\omega_f^+)$, where γ_τ belongs to Γ, Φ is the complex uniformization map $\Phi\colon\mathbb{C}/\Lambda_E\to E(\mathbb{C})$, and λ is a period conjecturally relating Λ_E and Λ_f. At the cost of replacing P_τ by a multiple of it, we can assume that γ_τ actually belongs to $\Gamma_1(\mathfrak{N})$ (the notation is

as in (2.3), with S equal to the archimedean places of F). Then the algorithm of Theorem 2.3 computes a decomposition of γ_τ of the form

$$\gamma_\tau = U_1 L_1 U_2 L_2 U_3, \tag{4.1}$$

where the matrices U_i and L_i are of the form

$$U_i = \begin{pmatrix} 1 & x_i \\ 0 & 1 \end{pmatrix} \text{ for some } x_i \in \mathcal{O}, \quad L_i = \begin{pmatrix} 1 & 0 \\ y_i & 1 \end{pmatrix} \text{ for some } y_i \in \mathfrak{N}.$$

In particular, they belong to Γ and the same expressions of (3.6) and (3.7) (changing the multiplicative by the additive notation) express $\int^\tau \int_\infty^{\gamma_\tau \infty} \omega_f^+$ in terms of usual double integrals of the form $\int_{\tau_1}^{\tau_2} \int_0^\infty \omega_f^+$, which in principle can be evaluated by integrating the Fourier expansion of ω_f^+.

It is worth remarking that, although the method described above certainly expresses the semi-indefinite integrals in terms of definite ones, the running time to directly compute the resulting double integrals to a useful accuracy often turns out to be too high. The problem is that if the limits of integration are too close to the real axis, then the number of Fourier coefficients needed to sum the series to an accurate precision is too high.

These kind of computational difficulties seem to be inherent to the ATR setting, as they were also to some extent present in the initial work of Darmon and Logan [DL03]. In [GM13] some methods for accelerating the computation of double integrals in the trivial level case were introduced. The authors believe that similar techniques can be applied to the non-trivial level setting in order to perform a systematical calculation similar to the one of Section 3.4.

In spite of this, in some simple examples it is possible to directly compute the integrals provided by Theorem 2.3, and hence to compute approximations to the ATR points. The following is an example of this, which we detail because it provides numerical evidence of the validity of Darmon's conjecture in elliptic curves of non-prime conductor.

Example 4.2. Let $F = \mathbb{Q}(\sqrt{5})$ and let E be the curve

$$y^2 + xy + \omega y = x^3 - (\omega+1)x^2 - (30\omega + 45)x - (111\omega + 117), \quad \omega = \frac{1+\sqrt{5}}{2}.$$

The conductor of E is $\mathfrak{N} = (\sqrt{5}+6)$, which has norm 31. This curve was previously considered in [Gre06] and [Gär11] (but note the typo in the displayed equation in both references). Let $\alpha = 1 - \sqrt{5}$ and let $K = F(\sqrt{\alpha})$. The embedding $\varphi\colon K \hookrightarrow \mathrm{M}_2(F)$ sending ω to the matrix

$$W = \begin{pmatrix} 3-\omega & -1 \\ 8-3\omega & -3+\omega \end{pmatrix}$$

is an optimal embedding of level $\mathfrak{N}$. Under the embedding $F \hookrightarrow \mathbb{R}$ sending $\sqrt{5}$ to the positive square root of 5, the fixed point of W acting on $\mathbb{C}^\times$ is

$$\tau = 0.439291418991 + i \cdot 0.353408129753,$$

and the image of the unit $(-3+2\omega)\omega + 4 - 3\omega \in \mathcal{O}_K^\times$ under φ is

$$\gamma_\tau = \begin{pmatrix} -4+3\omega & 2-2\omega \\ -22+16\omega & 12-9\omega \end{pmatrix}.$$

The ATR point attached to (the maximal order of) K is $J_\tau = \int^\tau \int_\infty^{\gamma_\tau \infty} \omega_f^+$. The determinant of γ_τ is $\omega + 1$, which is a unit. However its upper left entry is not congruent to 1 modulo $\mathfrak{N}$. If we let $u = -\sqrt{5} - 2$, which is a fundamental unit of F, then $-4 + 3\omega \equiv u \pmod{\mathfrak{N}}$. This implies that the matrix $\gamma'_\tau = \left(\begin{smallmatrix} u^{-1} & 0 \\ 0 & u \end{smallmatrix}\right) \gamma_\tau$ has its upper left entry congruent to 1 modulo $\mathfrak{N}$. We can work with γ'_τ because

$$J_\tau = \int^{u^{-2}\tau} \int_\infty^{\gamma'_\tau \infty} \omega_f^+. \tag{4.2}$$

Observe that $\det(\gamma'_\tau) = w+1$, which is a unit. The algorithm of Theorem 2.3 works for invertible matrices, not just determinant 1 matrices, and it gives the following decomposition of γ'_τ:

$$\left(\begin{smallmatrix} 1 & 1-w \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ 118739-73384\omega & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 46368+75025\omega \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ -5431444+\omega 3356817 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & -37268-60300\omega \\ 0 & 1+w \end{smallmatrix}\right).$$

We use this decomposition to transform (4.2) into a sum of usual double integrals. The resulting integrals have limits not too close to the real axis (the smallest imaginary part is $\simeq 0.011$). Integrating the Fourier series with coefficients $a_{\mathfrak{m}}$ with norm of $\mathfrak{m}$ up to $180,000$ gives J_τ to an accuracy of approximately 12 digits:

$$J_\tau \simeq -4.828954817077 + i \cdot 4.534696532333.$$

There is a point P of infinite order in $E(K)$ having x-coordinate equal to $18883/2420\alpha - 16127/2420$ (this was found using naive search algorithms); let J denote its corresponding image in $\mathbb{C}/\Lambda_E$. Then the equality

$$J_\tau = -2J \pmod{\Lambda_E}$$

holds up to the computed accuracy, giving numerical evidence of the equality $P_\tau = -2P$ and, therefore, of the rationality of P_τ.

References

[BMS67] H. Bass, J. Milnor, and J.-P. Serre. Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$). *Inst. Hautes Études Sci. Publ. Math.*, (33):59–137, 1967.

[CW75] George Cooke and Peter J. Weinberger. On the construction of division chains in algebraic number rings, with applications to SL_2. *Comm. Algebra*, 3:481–524, 1975.

[Dar01] Henri Darmon. Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications. *Ann. of Math. (2)*, 154(3):589–639, 2001.

[Dar04] Henri Darmon. *Rational points on modular elliptic curves*, volume 101 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.

[DG02] Henri Darmon and Peter Green. Elliptic curves and class fields of real quadratic fields: algorithms and evidence. *Experiment. Math.*, 11(1):37–55, 2002.

[DL03] Henri Darmon and Adam Logan. Periods of Hilbert modular forms and rational points on elliptic curves. *Int. Math. Res. Not.*, (40):2153–2180, 2003.

[DP06] Henri Darmon and Robert Pollack. Efficient calculation of Stark-Heegner points via overconvergent modular symbols. *Israel J. Math.*, 153:319–354, 2006.

[Gär11] Jérôme Gärtner. Points de Darmon et variétés de Shimura, 2011. Ph.D. Thesis, Institut de Mathématiques de Jussieu.

[GM13] Xavier Guitart and Marc Masdeu. Computation of ATR Darmon points on nongeometrically modular elliptic curves. *Experimental Mathematics*, 22(1):85–98, 2013.

[Gre06] Matthew Greenberg. Heegner points and rigid analytic modular forms, 2006. Ph.D. Thesis, McGill University.

[Vas72] L. N. Vaserštein. The group SL_2 over Dedekind rings of arithmetic type. *Mat. Sb. (N.S.)*, 89(131):313–322, 351, 1972.

Universitat Politècnica de Catalunya, Dept. Matematica Aplicada II, C/ Jordi Girona, 1-3, 08034 Barcelona (Spain)
E-mail address: xevi.guitart@gmail.com

Columbia University, Mathematics Department, Room 415, MC 4441, 2990 Broadway, New York, NY 10027
E-mail address: masdeu@math.columbia.edu