J. London Math. Soc. (2) 90 (2014) 495–524
doi:10.1112/jlms/jdu036

Overconvergent cohomology and quaternionic Darmon points

Xavier Guitart and Marc Masdeu

Abstract

We develop the (co)homological tools that make effective the construction of the quaternionic Darmon points introduced by Matthew Greenberg. In addition, we use the overconvergent cohomology techniques of Pollack–Pollack to allow for the efficient calculation of such points. Finally, we provide the first numerical evidence supporting the conjectures on their rationality.

1. *Introduction*

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and let p be a prime dividing N exactly. Consider a factorization of the form $N = pDM$, with D the product of an even (possibly zero) number of distinct primes and $(D, M) = 1$. Let K be a real quadratic field in which all primes dividing M are split, and all primes dividing pD are inert. Denote by $\mathcal{H}_p = K_p \setminus \mathbb{Q}_p$ the K_p-points of the p-adic upper half plane.

In the case $D = 1$, Darmon introduced in the seminal article [**6**] a construction of local points $P_\tau \in E(K_p)$ associated to elements $\tau \in K \cap \mathcal{H}_p$, defined as certain Coleman integrals of the modular form attached to E. He conjectured these points to be rational over certain ring class fields of K, and to behave in many aspects as the classical Heegner points arising from quadratic imaginary fields. A proof of these conjectures would certainly shed new light on new instances of the Birch–Swinnerton–Dyer conjecture. The reader can consult [**6**, Section 5; **8**, Section 4] for a discussion of this circle of ideas.

These conjectures are supported by some partial theoretical results such as [**2**], but at the moment the main evidence comes from explicit numerical computations. Darmon and Green [**8**] provided the first systematic algorithm and numerical calculations for curves satisfying the additional restriction that $M = 1$. Using overconvergent methods in the evaluation of the integrals, Darmon and Pollack [**10**] were able to give a much faster algorithm, which in practice can be used (assuming Darmon's conjectures) as an efficient method for computing algebraic points of infinite order on $E(K^{\mathrm{ab}})$. The restriction $M = 1$ in these algorithms was dispensed with in [**13**], which allowed to provide numerical evidence for curves of non-prime conductor.

In the case $D > 1$, Greenberg [**11**] proposed a construction of Darmon-like points in $E(K_p)$, by means of certain p-adic integrals related to modular forms on quaternion division algebras of discriminant D. He also conjectured that these points behave in many aspects as Heegner points and, in particular, that they are rational over ring class fields of K.

Greenberg's conjecture was motivated by the analogy with [**6**], but up to now, there was no numerical evidence of the rationality of such points in the quaternionic case $D > 1$. In fact, as Greenberg points out in [**11**, Section 12], the lack of sufficiently developed algorithms for computing in the cohomology of arithmetic groups has prevented the finding of any such evidence. The main purpose of the present work is precisely to provide an explicit algorithm

Received 4 November 2013; revised 28 April 2014; published online 26 July 2014.

2010 *Mathematics Subject Classification* 11G40 (primary); 11F41, 11Y50 (secondary).

Both authors were partially supported by MTM2009-13060-C02-01 and 2009 SGR 1220, and Xavier Guitart was also partially supported by SFB/TR 45.

that allows for the effective computation of the quaternionic p-adic Darmon points introduced by Greenberg.

Actually, the aim of the article is threefold. First, we develop the (co)homological methods that make effective the construction of [**11**]. Secondly, we relate the p-adic integrals that appear in the construction to certain overconvergent cohomology classes, in order to derive an efficient algorithm for the computation of the quaternionic Darmon points. Finally, we gather extensive evidence supporting the rationality conjectures of [**11**].

To describe more precisely the contents of the article, it is useful to briefly recall the structure of Greenberg's construction (a more complete and detailed account will be given in Section 3). Let $B/\mathbb{Q}$ be the indefinite quaternion algebra of discriminant D. Let also $R_0(M) \subset B$ be an Eichler order of level M, and denote by Γ the group of reduced norm 1 units in $R_0(M) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$. The construction of the point $P_\tau \in E(K_p)$ can be divided into three stages:

(1) the construction a certain cohomology class $\mu_E \in H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z}))$ canonically attached to E, where $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z})$ denotes the $\mathbb{Z}$-valued measures of $\mathbb{P}^1(\mathbb{Q}_p)$;
(2) the construction of a homology class $c_\tau \in H_1(\Gamma, \mathrm{Div}^0 K \cap \mathcal{H}_p)$, associated to the element $\tau \in \mathcal{H}_p$; and
(3) finally, the construction of a natural $K_p^\times$-valued integration pairing $\int\!\!\!\!\!\!\diagup \langle\, ,\, \rangle$ between the above cohomology and homology groups.

The point P_τ is then defined as the image under Tate's isomorphism $K_p^\times / \langle q_E \rangle \simeq E(K_p)$ of the quantity $J_\tau := \int\!\!\!\!\!\!\diagup \langle c_\tau, \mu_E \rangle \in K_p^\times$.

Section 2 is devoted to background material and to fix certain choices on the (co)homology groups that will be useful in our algorithms, and in Section 3 we give a more detailed description of the construction of Greenberg. The main contributions of this work are presented in Sections 4–6.

In Section 4, we provide algorithms for computing the homology class c_τ and the cohomology class μ_E. That is to say, we give explicit methods for working with the (co)homology groups arising in the construction, which allow for the effective numerical calculation of μ_E and c_τ in concrete examples. This already gives rise to an algorithm for the calculation of the point P_τ, since the integration pairing $\int\!\!\!\!\!\!\diagup \langle c_\tau, \mu_E \rangle$ can then be computed by the well-known method of Riemann products. We end Section 4 with a detailed concrete calculation of a Darmon point P_τ by means of this algorithm.

Although the method of Riemann products is completely explicit and can be used in principle to evaluate the integration pairing, it has the drawback of being computationally inefficient. In fact, its running time depends exponentially on the number of p-adic digits of accuracy to which the output is desired. This is the problem that we address in Section 5, in which we give an efficient, polynomial-time, algorithm for computing the integration pairing $\int\!\!\!\!\!\!\diagup \langle\, ,\, \rangle$. This method is based on the overconvergent cohomology lifting theorems of [**16**], and can be seen as a generalization to the quaternionic setting of the overconvergent modular symbols method of [**10**]. Used in conjunction with the algorithms of Section 4 for the homology and cohomology classes, it provides an efficient algorithm for computing the quaternionic Darmon points.

Finally, in Section 6 we provide extensive calculations and numerical evidence in support of the conjectured rationality of Greenberg's Darmon points, which were computed using an implementation in Sage [**18**] and Magma [**3**] of the algorithms described in Sections 4 and 5.

Notation

The following notation shall be in force throughout the article. Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and let p be a prime dividing N exactly. The conductor is factored as $N = pDM$, where $D > 1$ is the product of an even number of distinct primes, and M and D

are relatively prime. Let K be a real quadratic field in which all primes dividing M are split and all primes dividing pD are inert, and let $\mathcal{O}_K$ be the ring of integers of K.

Let B be the quaternion algebra over $\mathbb{Q}$ of discriminant D. For every $\ell \mid pM$, we fix an algebra isomorphism

$$\iota_\ell \colon B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \xrightarrow{\simeq} \mathrm{M}_2(\mathbb{Q}_\ell).$$

Let $R_0(M) \subset B$ be an Eichler order of level M such that for every $\ell \mid M$

$$\iota_\ell(R_0(M)) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_\ell) \colon c \equiv 0 \pmod{\ell} \right\}. \tag{1.1}$$

Similarly, let $R_0(pM) \subset R_0(M)$ be an Eichler order of level pM that satisfies (1.1) also for $\ell = p$. Denote by $\Gamma_0^D(M) = R_0(M)_1^\times$ and $\Gamma_0^D(pM) = R_0(pM)_1^\times$ their group of reduced norm 1 units. Finally, let

$$R = R_0(M) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p] \quad \text{and} \quad \Gamma = R_1^\times = \{\gamma \in R \colon \mathrm{nrd}(\gamma) = 1\}.$$

2. *Preliminaries on Hecke operators, the Bruhat–Tits tree and measures*

All the material in this section is well known. We present it particularized to our setting and we fix certain choices that will be important especially in Subsection 5.2.

2.1. *Hecke operators on homology and cohomology*

We recall first some well-known facts on group (co)homology which can all be found for example in [5]. This will also fix the notation to be used in the sequel.

Let G be a group and V a commutative left G-module. The groups of 1-*chains* and 2-*chains* are defined, respectively, as

$$C_1(G,V) = \mathbb{Z}[G] \otimes_{\mathbb{Z}} V, \quad C_2(G,V) = \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[G] \otimes_{\mathbb{Z}} V.$$

The *boundary maps* are induced by the formulas, for g and h in G and $v \in V$,

$$\partial_1(g \otimes v) = g^{-1}v - v; \quad \partial_2(g \otimes h \otimes v) = h \otimes g^{-1}v - gh \otimes v + g \otimes v. \tag{2.1}$$

We denote by $Z_1(G,V) = \ker \partial_1$ the group of 1-cycles, by $B_1(G,V) = \mathrm{im}\, \partial_2$ the group of 1-boundaries, and by $H_1(G,V) = Z_1/B_1$ the first homology group of G with coefficients in V.

Dually, one defines the group of 1-*cochains* $C^1(G,V)$, the group of 1-*coboundaries* $B^1(G,V)$, the group of 1-cocycles $Z^1(G,V)$ and the first cohomology group $H^1(G,V) = Z^1/B^1$.

We are mainly interested in the (co)homology of the group $G = \Gamma_0^D(pM)$. Consider also the semigroup $\Sigma_0(pM)$ defined as

$$\Sigma_0(pM) = B^\times \cap \prod_\ell \Sigma_\ell, \quad \text{where} \tag{2.2}$$

$$\Sigma_\ell = \begin{cases} \text{the set of elements in } R_0(pM) \text{ with non-zero norm} & \text{if } \ell \nmid pM; \\ \iota_\ell^{-1}\left(\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_\ell) \colon c \equiv 0 \pmod{\ell},\ d \in \mathbb{Z}_\ell^\times,\ ad - bc \neq 0 \right\} \right) & \text{if } \ell \mid pM. \end{cases}$$

Suppose that the $\Gamma_0^D(pM)$-action on V extends to an action of the semigroup $\Sigma_0(pM)$. Then, there are natural Hecke operators acting on $H_1(\Gamma_0^D(pM), V)$ and $H^1(\Gamma_0^D(pM), V)$ whose denition we proceed to recall, following [1].

The operators T_ℓ and U_ℓ. Let ℓ be a prime not dividing D, and let $g(\ell) \in \Sigma_0(pM)$ be an element of reduced norm ℓ. The double coset $\Gamma_0^D(pM) g(\ell) \Gamma_0^D(pM)$ decomposes as a finite

disjoint union of right $\Gamma_0^D(pM)$-cosets:

$$\Gamma_0^D(pM)g(\ell)\Gamma_0^D(pM) = \bigsqcup_{i\in I_\ell} g_i\Gamma_0^D(pM), \tag{2.3}$$

for certain $g_i \in \Sigma_0(pM)$ of reduced norm ℓ. The number of cosets in (2.3), that is, the cardinal of I_ℓ, is $\ell+1$ if $\ell \nmid pM$ and ℓ otherwise. Let $t_i : \Gamma_0^D(pM) \to \Gamma_0^D(pM)$ be the map defined by the equation

$$\gamma^{-1}g_i = g_{\gamma\cdot i}t_i(\gamma)^{-1} \quad \text{for some index } \gamma\cdot i \in I_\ell.$$

We remark that $i \mapsto \gamma\cdot i$ is a permutation of I_ℓ. Decomposition (2.3) induces maps T_ℓ on 1-chains and 1-cochains as follows: for a chain $c = \sum_g g\otimes v_g \in C_1(\Gamma_0^D(pM), V)$ and a cochain $f \in C^1(\Gamma_0^D(pM), V)$, then

$$T_\ell c = \sum_{i\in I_\ell}\sum_g t_i(g)\otimes g_i^{-1}v_g; \quad (T_\ell f)(g) = \sum_{i\in I_\ell} g_i f(t_i(g)). \tag{2.4}$$

The map T_ℓ on chains (respectively, cochains) respects cycles and boundaries (respectively, cocycles and coboundaries). The Hecke operators are the induced endomorphisms on homology and cohomology, which do not depend neither on the choice of $g(\ell)$ nor on the representatives g_i of (2.3). Following the usual notational conventions if $\ell \mid pM$, then we set $U_\ell = T_\ell$. We remark that the operators T_ℓ and U_ℓ on homology and cohomology are independent of the choices made in the definition. However, as maps on chains and cochains (and even as maps on cycles and cocycles) they do depend on these choices.

In Section 5, it will be important to work with the U_p-operator on cochains obtained by means of a specific decomposition (2.3) which we now describe. To do so, we next fix a choice of certain elements of $\Sigma_0(pM)$; these elements (and the notation for them) shall be in force for the rest of the article.

(1) Let $\Upsilon = \{\gamma_0, \dots, \gamma_p\}$ be a system of representatives for $\Gamma_0^D(pM)\backslash\Gamma_0^D(M)$ satisfying that

$$\gamma_0 = 1, \quad \text{and for } i>0 \;\; \iota_p(\gamma_i) = u_i\begin{pmatrix}0 & -1\\ 1 & i\end{pmatrix}, \tag{2.5}$$

for some u_i belonging to

$$\Gamma_0^{\mathrm{loc}}(p) = \left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}_p)\colon c \equiv 0 \pmod p\right\}.$$

(2) Let $\omega_p \in R_0(pM)$ be an element that normalizes $\Gamma_0^D(pM)$ and such that

$$\iota_p(\omega_p) = u'\begin{pmatrix}0 & -1\\ p & 0\end{pmatrix} \quad \text{for some } u' \in \Gamma_0^{\mathrm{loc}}(p). \tag{2.6}$$

Also, let $\omega_\infty \in R(pM)$ be an element of reduced norm -1 that normalizes $\Gamma_0^D(pM)$.

(3) Finally, set

$$\pi = \gamma_p^{-1}\omega_p \quad \text{and} \quad s_i = \gamma_i^{-1}\omega_p^{-1} \;\text{ for } i = 1, \dots, p. \tag{2.7}$$

We remark that

$$\iota_p(\pi) = \begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}u_\pi \quad \text{and} \quad \iota_p(s_i) = \begin{pmatrix}p & -i\\ 0 & 1\end{pmatrix}u_i' \tag{2.8}$$

for some $u_\pi, u_i' \in \Gamma_0^{\mathrm{loc}}(p)$.

Observe that $\pi \in \Sigma_0(pM)$ has reduced norm p; we will work with the Hecke operator on cycles and cocycles associated to the double coset $\Gamma_0^D(pM)\pi\Gamma_0^D(pM)$. One checks that the s_i defined

above decompose it into right cosets, namely

$$\Gamma_0^D(pM)\pi\Gamma_0^D(pM) = \bigsqcup_{i=1}^{p} s_i\Gamma_0^D(pM). \tag{2.9}$$

Then, $t_i : \Gamma_0^D(pM) \to \Gamma_0^D(pM)$ is the function defined by

$$\gamma^{-1}s_i = s_{\gamma\cdot i}t_i(\gamma)^{-1}, \quad \text{for certain index } \gamma\cdot i \in \{1,\dots,p\}. \tag{2.10}$$

For $c = \sum_g g\otimes v_g \in Z_1(\Gamma_0^D(pM), V)$ and $f \in Z^1(G,V)$ formulas (2.4) particularize to

$$U_p c = \sum_{i=1}^{p}\sum_g t_i(g)\otimes s_i^{-1}v_g; \quad (U_p f)(g) = \sum_{i=1}^{p} s_i f(t_i(g)). \tag{2.11}$$

Atkin–Lehner involutions. The Atkin–Lehner involutions at p on cycles and cocycles are given by the formulas:

$$W_p c = \sum_g \omega_p^{-1}g\omega_p\otimes\omega_p^{-1}v_g; \quad (W_p f)(g) = \omega_p f(\omega_p^{-1}g\omega_p).$$

Similarly, Atkin–Lehner involutions at infinity are defined as

$$W_\infty c = \sum_g \omega_\infty^{-1}g\omega_\infty\otimes\omega_\infty^{-1}v_g; \quad (W_\infty f)(g) = \omega_\infty f(\omega_\infty^{-1}g\omega_\infty).$$

These formulas induce well-defined involutions on the homology $H_1(\Gamma_0^D(pM), V)$ and on the cohomology $H^1(\Gamma_0^D(pM), V)$.

Hecke algebras. Let $[T_\ell]$, $[U_\ell]$ and $[W_\infty]$ be formal variables. If $m \in \mathbb{Z}_{>0}$, then we denote by $\mathbb{T}^{(m)}$ the Hecke algebra 'away from m'; that is, the $\mathbb{Z}$-algebra generated by $[W_\infty]$ and by the $[T_\ell]$ and $[U_\ell]$ with $\ell \nmid m$. Since the Hecke operators commute with each other, $\mathbb{T}^{(m)}$ acts on $H_1(\Gamma_0^D(pM), V)$ and $H^1(\Gamma_0^D(pM), V)$ by letting each formal variable act as the corresponding Hecke operator.

If $\lambda : \mathbb{T}^{(m)} \to \mathbb{Z}$ is a ring homomorphism and H is a $\mathbb{T}^{(m)}$-module, let

$$H^\lambda = \{x \in H : tm = \lambda(t)x \text{ for all } t \in \mathbb{T}^{(m)}\}.$$

The *degree character* $\deg : \mathbb{T}^{(pD)} \to \mathbb{Z}$ is defined by

$$\deg[T_\ell] = \ell + 1, \quad \deg[U_\ell] = \ell, \quad \deg W_\infty = 1.$$

Thanks to the modularity theorem of [**4**, **20**], the elliptic curve $E/\mathbb{Q}$ defines two characters $\lambda_E^+, \lambda_E^- : \mathbb{T}^{(pD)} \to \mathbb{Z}$ by

$$\lambda_E^\pm[T_\ell] = \ell + 1 - |E(\mathbb{F}_\ell)|, \quad \lambda_E^\pm[U_\ell] = \ell + 1 - |E(\mathbb{F}_\ell)|, \quad \lambda_E^\pm[W_\infty] = \pm 1. \tag{2.12}$$

Remark 2.1. There are also Hecke operators acting on $H_1(\Gamma, V)$ and $H^1(\Gamma, V)$. They are defined similarly, but using double cosets of the form $\Gamma g'(\ell)\Gamma$ (this time $g'(\ell)$ is an element of R of reduced norm ℓ); see, for example, [**14**, Section 2] for more details. For our purposes, it is enough to say that for $\ell \nmid pM$ one can choose $g(\ell) \in R_0(pM)$ and $g'(\ell) \in R$ elements of reduced norm ℓ such that the decompositions

$$\Gamma_0^D(pM)g(\ell)\Gamma_0^D(pM) = \bigsqcup_{i=0}^{\ell} g_i\Gamma_0^D(pM) \quad \text{and} \quad \Gamma g'(\ell)\Gamma = \bigsqcup_{i=0}^{\ell} g_i\Gamma$$

hold with the same choice of $g_i \in \Sigma_0(pM)$. Thus, formulas (2.4) also give the T_ℓ operator on $H_1(\Gamma, V)$ and $H^1(\Gamma, V)$ in this case.

2.2. *The Bruhat–Tits tree*

Let $\mathcal{T}$ be the Bruhat–Tits tree of $\mathrm{PGL}_2(\mathbb{Q}_p)$, and denote by $\mathcal{V}$ its set of vertices and by $\mathcal{E}$ its set of (directed) edges. It is well known that $\mathcal{T}$ is a $(p+1)$-regular tree. In addition, $\mathcal{V}$ can be identified with the set of homothety classes of $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^2$, and directed edges with ordered pairs of vertices (v_1, v_2) such that v_1 and v_2 can be represented by lattices Λ_1, Λ_2 with $p\Lambda_1 \subsetneq \Lambda_2 \subsetneq \Lambda_1$. For $e = (v_1, v_2) \in \mathcal{E}$, we denote by $s(e) = v_1$ the source of e, by $t(e) = v_1$ its target and by $\bar{e} = (v_2, v_1)$ its opposite.

Let v_* be the vertex represented by $\mathbb{Z}_p^2$, let $\hat{v}_*$ be the one represented by $\mathbb{Z}_p \oplus p\mathbb{Z}_p$ and let e_* be the edge $(v_*, \hat{v}_*)$. A vertex v is said to be even (respectively, odd) if its distance $d(v, v_*)$ to v_* is even (respectively, odd), and $e \in \mathcal{E}$ is said to be even (respectively, odd) if $s(e)$ is even (respectively, odd). We denote by $\mathcal{V}^+$ (respectively, $\mathcal{V}^-$) the set of even (respectively, odd) vertices and by $\mathcal{E}^+$ (respectively, $\mathcal{E}^-$) the set of even (respectively, odd) edges.

The group $\mathrm{GL}_2(\mathbb{Q}_p)$ acts on $\mathbb{Q}_p$ by fractional linear transformations

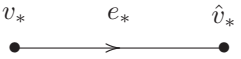
$$g\tau = \frac{a\tau + b}{c\tau + d}, \quad \text{for } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_p) \text{ and } \tau \in \mathbb{Q}_p.$$

This induces an action of $\mathrm{GL}_2(\mathbb{Q}_p)$ on $\mathbb{Z}_p$-lattices, which gives rise to an action of $\mathrm{GL}_2(\mathbb{Q}_p)$ on $\mathcal{V}$ that preserves distance, thus inducing an action on $\mathcal{T}$ and on $\mathcal{E}$.

We can make Γ act on $\mathcal{T}$ by means of the fixed isomorphism

$$\iota_p \colon B \otimes \mathbb{Q}_p \longrightarrow \mathrm{M}_2(\mathbb{Q}_p).$$

We denote this action simply as $g(v)$ and $g(e)$, for $g \in \Gamma$ and $v \in \mathcal{V}$, $e \in \mathcal{E}$. Strong approximation, using the fact that B is unramified at infinity, implies that Γ acts transitively on $\mathcal{E}^+$. A fundamental domain (in the sense of [**17**, Section 4.1]) for this action is given by



Moreover, we have

(1) $\mathrm{Stab}_\Gamma(v_*) = \Gamma_0^D(M)$, and $\mathrm{Stab}_\Gamma(\hat{v}_*) = \hat{\Gamma}_0^D(M) := \omega_p^{-1}\Gamma_0^D(M)\omega_p$.
(2) $\mathrm{Stab}_\Gamma(e_*) = \Gamma_0^D(pM)$.

This implies that $\Gamma = \Gamma_0^D(M) \star_{\Gamma_0^D(pM)} \hat{\Gamma}_0^D(M)$, where $\star$ denotes 'amalgamated product'.

In particular, the maps $g \mapsto g^{-1}(e_*)$ and $g \mapsto g^{-1}(v_*)$ induce bijections

$$\Gamma_0^D(pM)\backslash\Gamma \overset{1:1}{\longleftrightarrow} \mathcal{E}^+, \quad \Gamma_0^D(M)\backslash\Gamma \overset{1:1}{\longleftrightarrow} \mathcal{V}^+.$$

In the following, we will fix a convenient system of coset representatives of $\Gamma_0^D(pM)\backslash\Gamma$ indexed by the even edges, and another system of coset representatives of $\Gamma_0^D(M)\backslash\Gamma$ indexed by the even vertices. These were introduced in [**14**, Definition 4.7] and are called *radial systems*.

Recall $\Upsilon = \{\gamma_0 = 1, \gamma_1, \ldots, \gamma_p\}$ the set of representatives for $\Gamma_0^D(pM)\backslash\Gamma_0^D(M)$ we fixed in (2.5). Define $\tilde{\gamma}_0 = 1$ and, for $i = 1, \ldots, p$, define $\tilde{\gamma}_i = p^{-1}\omega_p\gamma_i\omega_p$.

LEMMA 2.2. *We have*

$$\Gamma_0^D(pM)\backslash\hat{\Gamma}_0^D(M) = \coprod_{i=0}^{p} \Gamma_0^D(pM)\tilde{\gamma}_i.$$

Proof. Clearly, the set $\{1, \omega_p^{-1}\gamma_1\omega_p, \ldots, \omega_p^{-1}\gamma_p\omega_p\}$ is a system of representatives for the quotient $\Gamma_0^D(pM)\backslash\hat{\Gamma}_0^D(M)$. The elements $p^{-1}\omega_p\gamma_i\omega_p$ and $\omega_p^{-1}\gamma_i\omega_p$ belong to the same coset

modulo $\Gamma_0^D(pM)$. Indeed, this follows from the identity

$$p^{-1}\omega_p\gamma_i\omega_p = p^{-1}\omega_p^2\omega_p^{-1}\gamma_i\omega_p,$$

and the fact that $p^{-1}\omega_p^2 \in \Gamma_0^D(pM)$ (see, for example, [11, Section 3.2]). □

DEFINITION 2.3. Define $\{\gamma_e\}_{e\in\mathcal{E}^+}$ and $\{\gamma_v\}_{v\in\mathcal{V}}$ to be the systems of representatives, respectively, for $\Gamma_0^D(pM)\backslash\Gamma$ and $\Gamma_0^D(M)\backslash\Gamma$ uniquely determined by the conditions:

(i) The representatives at the distinguished vertices are the unit element. That is, $\gamma_{v_*} = \gamma_{\hat{v}_*} = 1$;
(ii) for all $v \in \mathcal{V}^+$, we have $\{\gamma_e\}_{s(e)=v} = \{\gamma_i\gamma_v\}_{i=0}^p$;
(iii) for all $v \in \mathcal{V}^-$, we have $\{\gamma_e\}_{t(e)=v} = \{\tilde{\gamma}_i\gamma_v\}_{i=0}^p$;
(iv) for all $e \in \mathcal{E}^+$ such that $d(t(e), v_*) < d(s(e), v_*)$, we have $\gamma_{s(e)} = \gamma_e$; and
(v) for all $e \in \mathcal{E}^+$ such that $d(t(e), v_*) > d(s(e), v_*)$, we have $\gamma_{t(e)} = \gamma_e$.

By construction, $\mathcal{Y} = \{\gamma_e\}_{e\in\mathcal{E}^+}$ is a radial system. Indeed, by definition a radial system is one satisfying conditions (i)–(iii) above for some set of representatives for $\Gamma_0^D(pM)\backslash\Gamma_0^D(M)$ and $\Gamma_0^D(pM)\backslash\hat{\Gamma}_0^D(M)$. What we have done is to fix a choice of radial system by choosing $\{\gamma_0, \dots, \gamma_p\}$ and $\{\tilde{\gamma}_0, \dots, \tilde{\gamma}_p\}$ as such representatives, and adding conditions (iv) and (v) to make the choice unique. Figure 1 shows the first even edges of $\mathcal{T}$ labeled with representatives of $\mathcal{Y}$, in the simple case $p = 2$.

2.3. *Measures on* $\mathbb{P}^1(\mathbb{Q}_p)$

Let $\mathcal{B}(\mathbb{P}^1(\mathbb{Q}_p))$ be the set of compact-open balls in $\mathbb{P}^1(\mathbb{Q}_p)$, which forms a basis for the topology of $\mathbb{P}^1(\mathbb{Q}_p)$. There is a $\mathrm{GL}_2(\mathbb{Q}_p)$-equivariant bijection

$$\begin{aligned} \mathcal{E} &\xrightarrow{\cong} \mathcal{B}(\mathbb{P}^1(\mathbb{Q}_p)), \\ e &\longmapsto U_e \end{aligned}$$

sending e_* to $\mathbb{Z}_p$. Therefore, if $\gamma(e) = e_*$, then $U_e = \gamma^{-1}\mathbb{Z}_p$; in particular, $U_e = \gamma_e^{-1}\mathbb{Z}_p$. Under this bijection, an open ball U_e is contained in $U_{e'}$ if and only if there is a path (directed and without backtracking) in $\mathcal{T}$ having initial edge e and final edge e'.

The following basic lemma will be useful in Section 5. We denote by $|U|$ the diameter of an open ball $U \in \mathcal{B}(\mathbb{P}^1(\mathbb{Q}_p))$.

LEMMA 2.4. *Let $g_i = s_i^{-1} = \omega_p\gamma_i$. For each $r \geqslant 0$, denote by $\mathcal{B}(\mathbb{Z}_p, p^{-r})$ the set of open balls $U \subseteq \mathbb{Z}_p$ of diameter p^{-r}. Then, for all $r \geqslant 0$,*

$$\mathcal{B}(\mathbb{Z}_p, p^{-r}) = \{(g_{i_1}\cdots g_{i_r})^{-1}\mathbb{Z}_p \mid 1 \leqslant i_k \leqslant p\}. \tag{2.13}$$

Proof. We do induction on r, and note that the case of $r = 0$ is trivial since both sets consist of only one open, namely $\mathbb{Z}_p$.

Note that $g_i^{-1}\mathbb{Z}_p \subset \mathbb{Z}_p$, and actually

$$\mathbb{Z}_p = \coprod_{i=1}^p g_i^{-1}\mathbb{Z}_p.$$

This follows from the local form of the g_i as in (2.8): for $i \geqslant 1$, $\iota_p(g_i^{-1}) = \left(\begin{smallmatrix} p & -i \\ 0 & 1 \end{smallmatrix}\right) u_i$ with the $u_i \in \Gamma_0^{\mathrm{loc}}(p)$. Therefore, we obtain the inclusion $\supseteq$ in (2.13). The set $\mathcal{B}(\mathbb{Z}_p, p^{-r})$ has size p^r, so

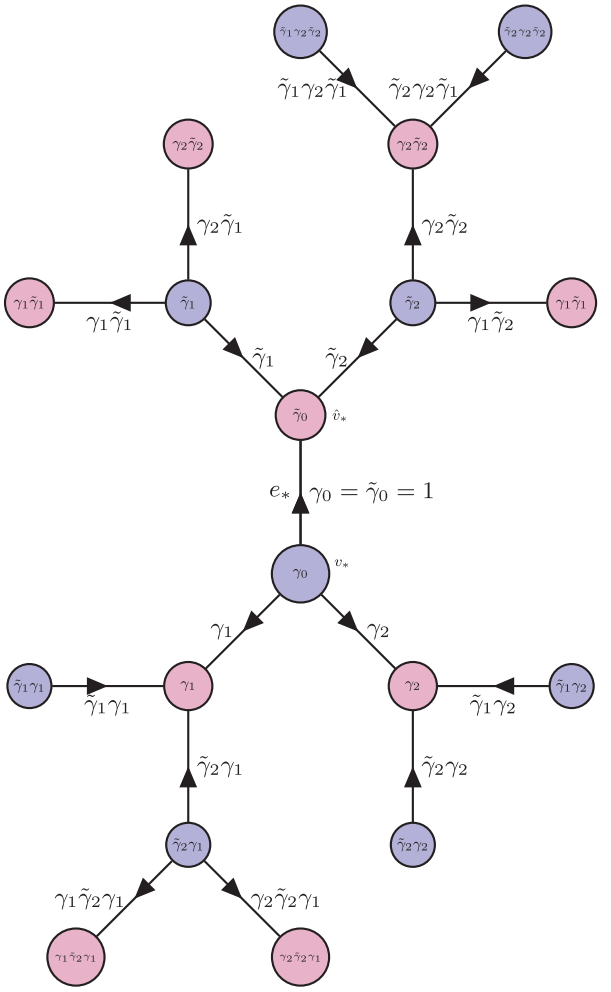


FIGURE 1 (color online). *Vertices and edges of the Bruhat–Tits tree labeled using the radial system* (p = 2). *Only the even edges are shown.*

it only remains to show that:

$$(i_1, \ldots, i_r) \neq (j_1, \ldots, j_r) \implies (g_{i_1} \cdots g_{i_r})^{-1}\mathbb{Z}_p \neq (g_{j_1} \cdots g_{j_r})^{-1}\mathbb{Z}_p.$$

Again, the previous decomposition of $\mathbb{Z}_p$ and the induction hypothesis prove the above claim. □

From the above lemma, we deduce the following corollary.

COROLLARY 2.5. (i) *An open ball U_e corresponding to an even edge e is contained in $\mathbb{Z}_p$ if and only if γ_e is of the form*

$$\gamma_e = \tilde{\gamma}_{i_1}\gamma_{j_1} \cdots \tilde{\gamma}_{i_n}\gamma_{j_n}, \quad \textit{with all } i_k, j_k \in \{1, \ldots, p\} \textit{ and some } n \geqslant 0.$$

(ii) *An open ball $U_{\overline{e}}$ corresponding to the opposite of an even edge e is contained in $\mathbb{Z}_p$ if and only if γ_e is of the form*

$$\gamma_e = \gamma_{j_1}\tilde{\gamma}_{i_2}\gamma_{j_2}\cdots\tilde{\gamma}_{i_n}\gamma_{j_n}$$

with all $i_k, j_k \in \{1,\dots,p\}$, and some $n \geqslant 0$.

Proof. Note that $\tilde{\gamma}_{i_k}\gamma_{j_k} = p^{-1}g_{i_k}g_{j_k}$, so

$$(\tilde{\gamma}_{i_k}\gamma_{j_k})^{-1}\mathbb{Z}_p = (g_{i_k}g_{j_k})^{-1}\mathbb{Z}_p.$$

Now the first claim follows from the fact that even edges correspond to balls of diameter p^{-2n} for some $n \geqslant 0$ and the lemma. The second claim is similar. □

Let $\mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p),\mathbb{Z})$ denote the set of $\mathbb{Z}$-valued measures on $\mathbb{P}^1(\mathbb{Q}_p)$ of total measure 0. It acquires the structure of left $\mathrm{GL}_2(\mathbb{Q}_p)$-module as follows: for $m \in \mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p),\mathbb{Z})$ and $g \in \mathrm{GL}_2(\mathbb{Q}_p)$

$$(gm)(U) = m(g^{-1}U) \quad \text{for all compact-open } U.$$

Let $\mathcal{F}(\mathcal{E},\mathbb{Z})$ denote the set of functions from $\mathcal{E}$ to $\mathbb{Z}$ and let

$$\mathcal{F}_0(\mathcal{E},\mathbb{Z}) = \{c \in \mathcal{F}(\mathcal{E},\mathbb{Z})\colon c(e) = -c(\bar{e}) \text{ for all } e \in \mathcal{E}\}.$$

A *$\mathbb{Z}$-valued harmonic cocycle* is a function $c \in \mathcal{F}_0(\mathcal{E},\mathbb{Z})$ such that

$$\sum_{s(e)=v} c(e) = 0 \text{ for all } v \in \mathcal{V}.$$

The bijection $\mathcal{E} \leftrightarrow \mathcal{B}(\mathbb{P}^1(\mathbb{Q}_p))$ induces an identification between $\mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p),\mathbb{Z})$ and $\mathcal{F}_{\mathrm{har}}(\mathbb{Z})$.

Remark 2.6. The module $\mathcal{F}_{\mathrm{har}}(\mathbb{Z})$ also appears in the theory of modular forms. Indeed, the Jacquet–Langlands correspondence and the theory of Cerednik–Drinfeld relate harmonic cocycles that are invariant with respect to arithmetic subgroups of *definite* quaternion algebras of discriminant D to pD-new modular forms (see, for example, [7, Section 5]). However, in this work, we only consider *indefinite* quaternion algebras. In this case, the corresponding invariant harmonic cocycles are trivial, and one needs to look at higher cohomology groups (cf. Section 3), hence deviating from the more classical theory.

3. *Quaternionic p-adic Darmon points*

This section is devoted to reviewing Greenberg's construction of quaternionic p-adic Darmon points [11] in the case of elliptic curves over $\mathbb{Q}$. Recall that in this setting E is an elliptic curve over $\mathbb{Q}$ of conductor $N = pDM$, and K a real quadratic field in which all primes dividing pD are inert and all primes dividing M are split.

The method attaches to any embedding of $\mathbb{Z}[1/p]$-algebras $\psi : \mathcal{O}_K \hookrightarrow R$ a Darmon point $P_\psi \in E(K_p)$, which is the image under Tate's uniformization map of a certain quantity $J_\psi \in K_p^\times$. The construction of J_ψ can be divided into three stages:

(1) construct a 1-cohomology class $[\tilde{\mu}] = [\tilde{\mu}_E] \in H^1(\Gamma, \mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p),\mathbb{Z}))$ associated to E;
(2) construct a 1-homology class $[c_\psi] \in H_1(\Gamma, \mathrm{Div}^0(\mathcal{H}_p))$ associated to ψ; and
(3) set $J_\psi = \oint\langle [c_\psi], [\tilde{\mu}]\rangle$, where $\oint\langle\ ,\ \rangle$ is a certain 'integration pairing'.

We describe each one of the steps separately.

3.1. *The cohomology class attached to E*

Recall the two characters $\lambda_E^{\pm}$ of the Hecke algebra associated to E in (2.12). Choose a sign $\sigma \in \{\pm\}$ and consider the character $\lambda = \lambda_E^{\sigma}$. If we denote by $H^1(\Gamma_0^D(pM), \mathbb{Z})_{p\text{-new}}$ the p-new subspace (see, for example, [**11**, Section 3] for the definition), then the submodule $(H^1(\Gamma_0^D(pM), \mathbb{Z})_{p\text{-new}})^{\lambda}$ is free of rank 1. In fact, the coboundary group $B^1(\Gamma_0^D(pM), \mathbb{Z})$ is trivial (for $\Gamma_0^D(pM)$ acts trivially on $\mathbb{Z}$), so there exists a cocycle $\varphi = \varphi_E \in Z^1(\Gamma_0^D(pM), \mathbb{Z})_{p\text{-new}}$ such that:

(1) for all $\ell \mid pM$, we have $U_\ell \varphi = a_\ell \varphi$;
(2) for all primes $\ell \nmid pMD$, we have $T_\ell \varphi = a_\ell \varphi$;
(3) $W_\infty \varphi = \sigma \varphi$; and
(4) the image of φ is not contained in any proper ideal of $\mathbb{Z}$.

The cocycle φ is uniquely determined, up to sign, by these conditions, and therefore we may and do fix such a cocycle φ. The following theorem can be seen as a generalization of [**10**, Proposition 1.3] to the case where B is a division algebra.

THEOREM 3.1 (Greenberg [**11**]). *There exists* $\tilde{\mu} \in Z^1(\Gamma, \mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z}))$ *whose cohomology class* $[\tilde{\mu}] \in H^1(\Gamma, \mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z}))$ *satisfies*:

(i) *for all primes* $\ell \nmid pM$, *we have* $T_\ell[\tilde{\mu}] = a_\ell[\tilde{\mu}]$;
(ii) *for all* $\ell \mid M$, *we have* $U_\ell[\tilde{\mu}] = a_\ell[\tilde{\mu}]$;
(iii) $W_\infty[\tilde{\mu}] = \sigma[\tilde{\mu}]$; *and*
(iv) *for all* $\gamma \in \Gamma_0^D(pM)$, *we have* $\tilde{\mu}_\gamma(\mathbb{Z}_p) = \varphi_\gamma$.

In addition, $[\tilde{\mu}]$ *is uniquely determined by these conditions.*

One can think of the cocycle $\tilde{\mu}$ as a 'system of measures': for any $\gamma \in \Gamma$ there is an associated measure $\tilde{\mu}_\gamma$. A cocycle $\tilde{\mu}$ as in the above theorem can be explicitly constructed by applying the methods of [**14**, Section 4.2] as follows. First of all, we need to define a related cocycle $\mu = \mu_E$, which will actually play an important role in our explicit algorithms. Given $e \in \mathcal{E}^+$ and $g \in \Gamma$, let $h(g, e)$ be the element of $\Gamma_0^D(pM)$ defined by the equation

$$\gamma_e g = h(g, e)\gamma_{g^{-1}(e)}. \tag{3.1}$$

Recall $\mathcal{Y} = \{\gamma_e\}_{e \in \mathcal{E}^+}$ the radial system fixed in Definition 2.3. For $g \in \Gamma$, let $\mu_g \in \mathcal{F}(\mathcal{E}_0, \mathbb{Z})$ be the function defined by

$$\mu_g(e) = \varphi_{h(g,e)}, \quad \text{if } e \in \mathcal{E}^+. \tag{3.2}$$

This condition already determines the values of $\mu_g(e)$ for $e \in \mathcal{E}^-$, for if μ_g belongs to $\mathcal{F}_0(\mathcal{E}, \mathbb{Z})$, then $\mu_g(e) = -\mu_g(\bar{e})$ and $\bar{e} \in \mathcal{E}^+$. The map defined in this way turns out to be a 1-cocycle.

Fix a prime r not dividing N and set $t_r = (T_r - r - 1) \in \mathbb{T}^{(pD)}$. The following proposition, which essentially restates results of [**11**, **14**], claims that $[\tilde{\mu}]$ can be computed from $t_r[\mu]$.

PROPOSITION 3.2. *The cocycle* μ *belongs to* $Z^1(\Gamma, \mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z}))$, *and* $t_r[\mu]$ *is a multiple of the cohomology class* $[\tilde{\mu}]$ *given by Theorem* 3.1.

Proof. Recall the identification $\mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z})$ with $\mathcal{F}_{\mathrm{har}}(\mathbb{Z})$. First of all, since φ belongs to $(H^1(\Gamma_0^D(pM), \mathbb{Z})_{p\text{-new}})^{\lambda}$ by Remark 3.3 and the fact that the isomorphism of Shapiro's lemma commutes with the Hecke action [**1**, Lemma 1.1.4], we see that $[\mu] \in H^1(\Gamma, \mathcal{F}_0(\mathcal{E}, \mathbb{Z}))^{\lambda}$. The system $\mathcal{Y}$ used to define μ is radial, and by [**14**, Proposition 4.8] this implies that μ_g belongs to $\mathcal{F}_{\mathrm{har}}(\mathbb{Z})$ for all $g \in \Gamma$. In particular, $[\mu]$ can be viewed as an element of $H^1(\Gamma, \mathcal{F}_{\mathrm{har}}(\mathbb{Z}))$. The

natural map

$$\rho : \mathbb{Q} \otimes H^1(\Gamma, \mathcal{F}_{\mathrm{har}}(\mathbb{Z})) \longrightarrow \mathbb{Q} \otimes H^1(\Gamma, \mathcal{F}_0(\mathcal{E}, \mathbb{Z}))_{p\text{-new}}$$

is surjective but not injective: its kernel is $H^1(\Gamma, \mathcal{F}_{\mathrm{har}}(\mathbb{Z}))^{\deg}$ (see [11, Section 8]). Since λ arises from a cuspidal eigenform, $\lambda(T_r)$ is not $r+1 = \deg(T_r)$, and thus $T_r - r - 1$ projects to the complementary of $\mathbb{Q} \otimes H^1(\Gamma, \mathcal{F}_{\mathrm{har}}(\mathbb{Z}))^{\deg}$, and it acts as multiplication by $a_r - r - 1$ on $\mathbb{Q} \otimes H^1(\Gamma, \mathcal{F}_{\mathrm{har}}(\mathbb{Z}))^{\lambda}_{p\text{-new}}$. □

In view of this result, there exists an integer c_r such that $t_r[\mu] = c_r[\tilde{\mu}]$. We abuse the notation to denote $c_r^{-1}t_r$ simply as t_r, so that we have an equality $[\tilde{\mu}] = t_r[\mu]$.

REMARK 3.3. In fact, the cohomology class of $[\tilde{\mu}] \in H^1(\Gamma, \mathcal{F}_0(\mathcal{E}, \mathbb{Z}))$ is nothing but the image of φ under the isomorphisms

$$H^1(\Gamma_0^D(pM), \mathbb{Z}) \simeq H^1(\Gamma, \mathrm{coind}_{\Gamma_0^D(pM)}^{\Gamma}(\mathbb{Z})) \simeq H^1(\Gamma, \mathcal{F}_0(\mathcal{E}, \mathbb{Z})),$$

where the first isomorphism is given by Shapiro's lemma and the second comes from the isomorphism $\mathrm{coind}_{\Gamma_0^D(pM)}^{\Gamma}(\mathbb{Z}) \simeq \mathcal{F}_0(\mathcal{E}, \mathbb{Z})$ (cf. [11, Corollary 16]).

3.2. *The homology class attached to ψ*

Let $\mathcal{H}_p = K_p \setminus \mathbb{Q}_p$ be the K_p-rational points of the p-adic upper half plane. The group $\psi(\mathcal{O}_K^{\times})$ acts on $\mathcal{H}_p$ via the isomorphism $\iota_p : B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$. Since p is inert in K, the action has two fixed points; let $\tau_\psi \in \mathcal{H}_p$ be one of them. Let also $\varepsilon_K \in \mathcal{O}_K^{\times}$ be a unit of norm 1, and set $\gamma_\psi = \psi(\varepsilon_K)$. Since $\gamma_\psi \tau_\psi = \tau_\psi$, the element $\gamma_\psi \otimes \tau_\psi$ belongs to $Z_1(\Gamma, \mathrm{Div}\,\mathcal{H}_p)$. From the exact sequence

$$0 \longrightarrow \mathrm{Div}^0 \mathcal{H}_p \longrightarrow \mathrm{Div}\,\mathcal{H}_p \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0, \tag{3.3}$$

we obtain the long exact sequence in Γ-homology

$$\cdots \longrightarrow H_2(\Gamma, \mathbb{Z}) \xrightarrow{\delta} H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \longrightarrow H_1(\Gamma, \mathrm{Div}\,\mathcal{H}_p) \xrightarrow{\deg_*} H_1(\Gamma, \mathbb{Z}) \longrightarrow \cdots, \tag{3.4}$$

where δ is the connecting homomorphism. The group $H_1(\Gamma, \mathbb{Z})$ is isomorphic to the abelianization of Γ, which is finite (see, for example, [15, Section 2]). If we let e_Γ denote its exponent, then $e_\Gamma[\gamma_\psi \otimes \tau_\psi]$ has a preimage $[c_\psi] \in H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p)$, and this is the homology class attached to ψ we were looking for.

REMARK 3.4. The homology class $[c_\psi]$ is well-defined up to elements in $\delta(H_2(\Gamma, \mathbb{Z}))$.

3.3. *Integration pairing and Darmon points*

Let $f : \mathbb{P}^1(\mathbb{Q}_p) \to K_p^{\times}$ be a continuous function and let $m \in \mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z})$. The *multiplicative integral* of f with respect to m is defined as the limit of Riemann products

$$\int\!\!\!\!\!\!\times_{\mathbb{P}^1(\mathbb{Q}_p)} f(t)\, dm(t) = \lim_{||\mathcal{U}|| \to 0} \prod_{U \in \mathcal{U}} f(t_U)^{m(U)} \in K_p^{\times},$$

where the limit is taken over increasingly finer finite coverings $\mathcal{U}$ of $\mathbb{P}^1(\mathbb{Q}_p)$ by compact-opens, and t_U is any sample point in U. If $U \subset \mathbb{P}^1(\mathbb{Q}_p)$ it is customary to denote

$$\int\!\!\!\!\!\!\times_U f(t)\, dm(t) = \int\!\!\!\!\!\!\times_{\mathbb{P}^1(\mathbb{Q}_p)} f(t) \mathbb{1}_U(t)\, dm(t).$$

For $D \in \mathrm{Div}^0(\mathcal{H}_p)$, let $f_D : \mathbb{P}^1(\mathbb{Q}_p) \to K_p^\times$ be a function with divisor D (for instance, if $D = (\tau_0) - (\tau_1)$, one can take $f_D(t) = (t-\tau_0)/(t-\tau_1)$). Observe that f_D is well-defined up to multiplication by scalars in $K_p^\times$; nevertheless, since these scalars integrate to 1 there is a well-defined pairing

$$\begin{aligned} \mathrm{Div}^0(\mathcal{H}_p) \times \mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z}) &\longrightarrow K_p^\times \\ (D, m) &\longmapsto \fint_{\mathbb{P}^1(\mathbb{Q}_p)} f_D(t)\, dm(t). \end{aligned}$$

By cup product, this defines a pairing

$$\begin{aligned} H_1(\Gamma, \mathrm{Div}^0(\mathcal{H}_p)) \times H^1(\Gamma, \mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z})) &\xrightarrow{\fint\langle\ ,\ \rangle} K_p^\times \\ \left(\sum_g g \otimes D_g, \xi\right) &\longmapsto \prod_g \fint_{\mathbb{P}^1(\mathbb{Q}_p)} f_{D_g}(t)\, d\xi_g(t), \end{aligned}$$

which is equivariant for the Hecke action:

$$\fint \left\langle T_\ell \sum_g g \otimes D_g, \xi \right\rangle = \fint \left\langle \sum_g g \otimes D_g, T_\ell \xi \right\rangle. \tag{3.5}$$

Define

$$L = \left\{ \fint \langle \delta c, [\tilde{\mu}] \rangle : c \in H_2(\Gamma, \mathbb{Z}) \right\} \subset K_p^\times,$$

where $[\tilde{\mu}] = t_r[\mu]$ is the cohomology class associated to E in Subsection 3.1. It turns out that L is a lattice in $K_p^\times$ (see [**11**, Proposition 30]). The following key result, which was independently proved by Dasgupta–Greenberg and Longo–Rotger–Vigni, relates L to the Tate lattice of E.

THEOREM 3.5 [**9**, **14**]. *The lattice L is commensurable to the Tate lattice $\langle q_E \rangle$ of E/K_p.*

Thanks to this theorem, one can find an isogeny $\beta : K_p^\times/L \to K_p^\times/\langle q_E \rangle$. Denote by $\Phi_{\mathrm{Tate}} : K_p^\times/\langle q_E \rangle \to E(K_p)$ Tate's uniformization map and let

$$J_\psi = \fint \langle c_\psi, [\tilde{\mu}] \rangle.$$

Observe that J_ψ is a well-defined quantity in $K^\times/L$ thanks to Remark 3.4.

CONJECTURE 3.6 (Greenberg). The local point $P_\psi = (\Phi_{\mathrm{Tate}} \circ \beta)(J_\psi) \in E(K_p)$ is a global point. More precisely, it is rational over the narrow Hilbert class field H_K^+ of K.

REMARK 3.7. The integration pairing is equivariant with respect to the Hecke action, so J_ψ can also be computed as

$$J_\psi = \fint \langle [t_r c_\psi], [\mu] \rangle. \tag{3.6}$$

4. *The effective computation of quaternionic p-adic Darmon points*

In this section, we present the explicit algorithms that allow for the effective calculation of the quaternionic p-adic Darmon points. As we reviewed in Section 3, this amounts to compute

the cohomology class associated to the elliptic curve, the homology class corresponding to an optimal embedding, and the integration pairing.

In Subsection 4.1, we show how to compute the cohomology class (the main algorithmic result is given in Theorem 4.1), and in Subsection 4.2 how to compute the homology class (the main algorithm is stated as Theorem 4.2). In fact, these two algorithms are already enough to compute the Darmon points, as one can then evaluate the integration pairing via Riemann products, which can be thought of as the most naïve method of integration. This is briefly recalled in Subsection 4.3.

Finally, in Subsection 4.4 we illustrate the use of this method by giving a detailed explicit example of a Darmon point calculated with the algorithms introduced in this section, together with Riemann products for approximating the integrals. This also serves as a motivation for Section 5, because even though, in principle, it is possible to compute the integrals using Riemann products, it is too computationally costly. Section 5 will be devoted to an efficient method for calculating the type of integrals arising in p-adic Darmon points.

4.1. *Computation of the cohomology class*

The first step is to calculate a cocycle $\varphi \in H^1(\Gamma_0^D(pM), \mathbb{Z})_{p\text{-new}}$ that lies in the λ-isotypical component by the Hecke action. We remark that there are algorithms for effectively dealing with arithmetic subgroups of indefinite quaternion division algebras. More concretely, there are algorithms that:

(1) compute a presentation of $\Gamma_0^D(M)$ and $\Gamma_0^D(pM)$ in terms of generators and relations; and
(2) express an element of $\Gamma_0^D(M)$ or $\Gamma_0^D(pM)$ as a word in the generators.

These algorithms were introduced by Voight [**19**] and are implemented in Magma [**3**].

Note that we have

$$H^1(\Gamma_0^D(pM), \mathbb{Z}) = \mathrm{Hom}(\Gamma_0^D(pM), \mathbb{Z}) = \mathrm{Hom}(\Gamma_0^D(pM)_{\mathrm{ab}}, \mathbb{Z}),$$

and that the finitely generated abelian group $\Gamma_0^D(pM)_{\mathrm{ab}}$ is easy to calculate from an explicit presentation of $\Gamma_0^D(pM)$. Using this description and formula (2.4), one can algorithmically compute the Hecke action on $H^1(\Gamma_0^D(pM), \mathbb{Z})$ (cf. [**12**] for more details).

Using the Atkin–Lehner operator W_p, one computes the p-new part of the group $H^1(\Gamma_0^D(pM), \mathbb{Z})$, and one then proceeds to diagonalize it with respect to several Hecke operators T_ℓ, until the common eigenspace corresponding to λ has rank 2. In practice, a few values of ℓ are usually enough. Then the space where the Atkin–Lehner operator W_∞ acts with sign $\sigma \in \{\pm 1\}$ has rank 1, and we can take φ to be one of its generators.

The final step is to compute the values of μ by means of formula (3.2). To do so, one needs to be able to express any element $g \in \Gamma$ as $g = h(g)\gamma_e$, where $h(g) \in \Gamma_0^D(pM)$ and $\gamma_e \in \mathcal{Y}$. In the next theorem, we show that this can be, indeed, computed in an algorithmic fashion.

THEOREM 4.1. *There is an algorithm that, given $g \in \Gamma$, outputs $h(g) \in \Gamma_0^D(pM)$ and $\gamma_e \in \mathcal{Y}$ such that $g = h(g)\gamma_e$, in time proportional to the distance from e_* to $e = g^{-1}(e_*)$.*

To describe the algorithm and prove its correctness, it is useful to recall the notion of *distance between lattices* (cf. [**17**, Chapter II, Section 1.1]). If Λ and Λ' are lattices in $\mathbb{Q}_p^2$, then there exists a basis $\{b_1, b_2\}$ for Λ such that $\{p^x b_1, p^y b_2\}$ is a basis for Λ' for certain $x, y \in \mathbb{Z}$. Then the distance $d(\Lambda, \Lambda')$ is defined to be $|x - y|$. It is independent of the choice for $\{b_1, b_2\}$, and it depends only on the homothety classes of Λ and Λ'. In addition, this notion of distance coincides

with the distance in the Bruhat–Tits tree; that is to say, if Λ and Λ' represent vertices v and v' in $\mathcal{V}$, then $d(\Lambda,\Lambda') = d(v,v')$.

Under the correspondence $\Gamma_0^D(pM)\setminus\Gamma \leftrightarrow \mathcal{E}^+$, an element $g\in\Gamma$ is associated with $e = g^{-1}(e_*)\in\mathcal{E}^+$. Its source $s(e) = g^{-1}(v_*)$ is then represented by the lattice $g^{-1}(\mathbb{Z}_p\oplus\mathbb{Z}_p)$, and its target $t(e) = g^{-1}(\hat{\imath}_*)$ by the lattice $g^{-1}(\mathbb{Z}_p\oplus p\mathbb{Z}_p)$. Thus, if we let $\iota_p(g^{-1}) = \left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)$, then the columns $\left(\begin{smallmatrix} a\\ c\end{smallmatrix}\right)$ $\left(\begin{smallmatrix} b\\ d\end{smallmatrix}\right)$ are a basis for the lattice $s(e)$ and the columns of $\left(\begin{smallmatrix} a & bp\\ c & dp\end{smallmatrix}\right)$ are a basis for $t(e)$. The distances $d(s(e),v_*)$ and $d(t(e),v_*)$ are easily read from the Smith normal form of these matrices: if

$$\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right) = G\left(\begin{smallmatrix} d_1 & 0\\ 0 & d_2\end{smallmatrix}\right)H, \quad \left(\begin{smallmatrix} a & pb\\ c & pd\end{smallmatrix}\right) = G'\left(\begin{smallmatrix} d_1' & 0\\ 0 & d_2'\end{smallmatrix}\right)H' \text{ for some } G,G',H,H'\in \mathrm{GL}_2(\mathbb{Z}_p),$$

then

$$d(s(e),v_*) = |v_p(d_1) - v_p(d_2)| \quad\text{and}\quad d(t(e),v_*) = |v_p(d_1') - v_p(d_2')|. \tag{4.1}$$

We may identify g with its associated edge $e = g^{-1}(e_*)$, and use expressions such as $d(s(g),v_*)$ or $d(t(g),v_*)$. We say that e (or g) is an *outward* edge if $d(s(g),v_*) < d(t(g),v_*)$ and that it is *inward* otherwise. Observe that one can easily determine whether g is inward or outward by means of formula (4.1).

Proof of Theorem 4.1. Given an element $g\in\Gamma$, let e be the edge $g^{-1}(e_*)$. It is enough to compute the representative $\gamma_e\in\mathcal{Y}$, since then $h(g) = g\gamma_e^{-1}\in\Gamma_0^D(pM)$.

Observe that if g is outward and $d(s(g),v_*) = 0$, then γ_e equals some $\gamma_i\in\Upsilon$ (see the edges leaving v_* in Figure 1), and it is easily computed, since it is the single γ_i such that $\gamma_i^{-1}g\in\Gamma_0^D(pM)$. For general g, the algorithm consists of recursively reducing to this particular case as follows.

(1) If g is outward and $d(s(g),v_*) > 0$, then there exists a single γ_i such that $\gamma_i^{-1}g$ is associated with an inward edge. Compute such γ_i and set $g = \gamma_i^{-1}g$.

(2) If g is inward, then there exists a single $\tilde{\gamma}_i$ such that $\tilde{\gamma}_i^{-1}g$ is outward. In addition, for such $\tilde{\gamma}_i$ we have that $d(s(\tilde{\gamma}_i^{-1}g),v_*) < d(s(g),v_*)$. Set $g = \tilde{\gamma}_i^{-1}g$.

(3) If g is outward and $d(s(g),v_*) = 0$, compute the single γ_i such that $\gamma_i^{-1}g\in\Gamma_0^D(pM)$ and end the algorithm. Otherwise, go to step (1).

Every time we run step (2) the distance $d(s(g),v_*)$ decreases, so the algorithm terminates. The representative γ_e is then the product of all the γ_i and $\tilde{\gamma}_j$ computed in each step. Finally, it is clear that the number of stages is $d(s(e),v_*)$. □

4.2. *Computation of the homology class*

Given the real quadratic field K and its ring of integers $\mathcal{O}_K = \mathbb{Z}[\omega]$, the first step is to compute an embedding of $\mathbb{Z}[1/p]$-algebras $\mathcal{O}_K\hookrightarrow R$. In fact, thanks to our running assumptions on K we can find $\mathbb{Z}$-algebra embeddings $\mathcal{O}_K\hookrightarrow R_0(M)$. Computing them in practice amounts to finding elements in B, whose reduced norm and trace coincide with that of ω, and one can use the routines of Magma [**3**] to compute them (for example, the routine `Embed( , )`).

Every embedding $\psi_0:\mathcal{O}_K\hookrightarrow R_0(M)$ induces $\psi\colon\mathcal{O}_K\hookrightarrow R$ via the inclusion $R_0(M)\subset R$, giving rise to the 1-cycle $\gamma_\psi\otimes\tau_\psi$ in $Z^1(\Gamma,\operatorname{Div}\mathcal{H}_p)$ via the process described in Subsection 3.2. Denote by e_Γ the exponent of $H_1(\Gamma,\mathbb{Z})$, so that the element

$$e_\Gamma[\gamma_\psi\otimes\tau_\psi]\in H_1(\Gamma,\operatorname{Div}\mathcal{H}_p)$$

lifts under $\deg_*$ to an element $[c_\psi]\in H_1(\Gamma,\operatorname{Div}^0\mathcal{H}_p)$ (cf. the exact sequence (3.4)).

We devote the rest of this subsection to describe an algorithm for computing c_ψ. Note that once c_ψ is found, it is easy to compute $\tilde{c}_\psi$ by means of formula (2.4).

Let $\langle X \mid R\rangle$ be a presentation of Γ, where $X = \{x_1, \dots, x_n\}$ are the generators and $R = \{r_1, \dots, r_m\}$ the relations. It can be explicitly computed by means of Voight's algorithms, which provide presentations for $\Gamma_0^D(M)$ and $\Gamma_0^D(pM)$, say

$$\Gamma_0^D(M) = \langle Y \mid S\rangle \quad \text{and} \quad \Gamma_0^D(pM) = \langle Z \mid T\rangle.$$

A set of generators of $\hat{\Gamma}_0^D(M)$ is $\hat{Y} = \{\hat{y}_i := \omega_p^{-1} y_i \omega_p \colon y_i \in Y\}$, and a set of relations $\hat{S}$ is that in which the $\hat{y}_i$ satisfy the same relations as the y_i. Then each $z \in Z$ can be expressed as a word in the generators of Y, that we denote $\alpha(z)$, and as a word in the generators of $\hat{Y}$, that we denote $\hat{\alpha}(z)$. If we let $S_Z = \{\alpha(z)\hat{\alpha}(z)^{-1} \colon z \in Z\}$, then a presentation of $\Gamma = \Gamma_0^D(M) \star_{\Gamma_0^D(pM)} \hat{\Gamma}_0^D(M)$ is given by

$$\langle X \mid R\rangle = \langle Y \cup \hat{Y} \mid S \cup \hat{S} \cup S_Z\rangle.$$

Any $g \in \Gamma_0^D(M)$ can be expressed as a word in Y by means of Voight's algorithm [**19**]. Combining this with the algorithm of Theorem 4.1, we obtain an algorithm for expressing any $g \in \Gamma$ as a word in X.

The following notation will be useful in describing the algorithm for computing c_ψ: If w is a word and $x \in X$, then we define $v_x(w) \in \mathbb{Z}$ as the sum of the exponents of x appearing in w. We also set $v_X(w) = (v_{x_1}(w), \dots, v_{x_n}(w))$. For example, if $w = x_1^3 x_2^3 x_3^{-1} x_1^{-2} x_3^3$, then $v_X(w) = (1, 3, 2)$.

The first step in lifting $e_\Gamma[\gamma_\psi \otimes \tau_\psi] = [\gamma_\psi^{e_\Gamma} \otimes \tau_\psi]$ consists of computing e_Γ. This is easily obtained using integral linear algebra to obtain the structure of Γ_{ab} from the presentation of Γ.

Next, one obtains a word representation w for $\gamma_\psi^{e_\Gamma}$. Since we are assuming that $\gamma_\psi^{e_\Gamma}$ is trivial in $H_1(\Gamma, \mathbb{Z}) \cong \Gamma_{\mathrm{ab}}$, the vector $v_X(w)$ belongs to the image of the abelianized relations, say $v_X(w) = a_1 v_X(r_1) + \cdots + a_k v_X(r_m)$. We consider instead the word $w' = w r_1^{-a_1} \cdots r_m^{-a_m}$, which represents the same element $\gamma_\psi^{e_\Gamma} \in \Gamma$, but which satisfies $v_X(w') = 0$.

In what follows, we write $\equiv$ to mean equality up to boundaries. The algorithm of Theorem 4.2 provides a way to find elements $x_i \in \Gamma$ and $D_i \in \mathrm{Div}^0(\mathcal{H}_p)$ such that

$$w' \otimes \tau_\psi \equiv \sum_{i=1}^{n} x_i \otimes D_i, \quad \text{with the } D_i \in \mathrm{Div}^0(\mathcal{H}_p),$$

and therefore to compute $c_\psi = \sum_{i=1}^n x_i \otimes D_i$.

THEOREM 4.2. *There exists an algorithm that, given $g \in \Gamma$ represented by a word w and given $D \in \mathrm{Div}\,\mathcal{H}_p$, computes elements $x_i \in \Gamma$ and $D_i \in \mathrm{Div}^0\,\mathcal{H}_p$ such that*

$$g \otimes D \equiv \sum_{i=1}^{n} x_i \otimes D_i, \quad \textit{with } \deg(D_i) = v_{x_i}(w)\deg(D).$$

The proof of this theorem consists of making systematic use of the following lemma.

LEMMA 4.3. *The following relations hold true in $Z_1(\Gamma, \mathrm{Div}\,\mathcal{H}_p)$:*

(i) *for all $g, h \in \Gamma$ and $D \in \mathrm{Div}\,\mathcal{H}_p$, $gh \otimes D \equiv g \otimes D + h \otimes g^{-1}D$;*
(ii) *for all $k \geqslant 0$, $g^k \otimes D \equiv g \otimes D'$, with $D' = D + g^{-1}D + \cdots + g^{1-k}D$;*
(iii) *for all $g \in \Gamma$ and $D \in \mathrm{Div}\,\mathcal{H}_p$, $g^{-1} \otimes D \equiv -g \otimes gD$; and*
(iv) *if $gD = D$, then $g^k \otimes D \equiv kg \otimes D$ for all $k \in \mathbb{Z}$.*

Proof. The first statement is direct from the relation in homology (cf. (2.1)). Note that $D' = g^{-1}D$ has the same degree as D.

Next, observe that

$$0 \equiv g^{-1}g \otimes D \equiv g^{-1} \otimes D + g \otimes gD,$$

so we obtain $g^{-1} \otimes D \equiv g \otimes D'$, with $D' = -gD$ satisfying $\deg(D') = -\deg(D)$, which is the third statement. The second statement is proved using induction on k, and the last statement is a particular case of the second and third ones. □

Proof of Theorem 4.2. Suppose that $w = x_{i_1}^{a_1} \cdots x_{i_t}^{a_t}$ is a word representing g. Repeated applications of Lemma 4.3, part (i) allow one to express:

$$g \otimes D \equiv \sum_{s=1}^{t} x_{i_s}^{a_s} \otimes D'_s, \quad \deg(D'_s) = \deg(D).$$

Using Lemma 4.3, part (ii), the above can be rewritten as

$$g \otimes D \equiv \sum_{s=1}^{t} x_{i_s} \otimes D''_s, \quad \deg D''_s = a_s \deg(D).$$

Finally, one can collect the terms involving each of the generators $x \in X$, to obtain

$$g \otimes D \equiv \sum_{i=1}^{n} x_i \otimes D_i,$$

and note that $\deg(D_i) = v_{x_i}(w)\deg(D)$, as wanted. □

4.3. *Computation of the integration pairing via Riemann products*

In Subsections 4.1 and 4.2, we have seen how to compute in practice the cocycle μ attached to E and the cycle c_ψ attached to an optimal embedding. The integration pairing then gives the Darmon point attached to ψ. That is to say,

$$J_\psi = \int\!\!\!\!\!\!\diagup \langle [\tilde{c}_\psi], [\mu] \rangle = \prod_{k=1}^{C} \int\!\!\!\!\!\!\diagup_{\mathbb{P}^1(\mathbb{Q}_p)} f_{D_k}(t) d\mu_{g_k}(t). \tag{4.2}$$

Each individual term $\int\!\!\!\!\!\!\diagup_{\mathbb{P}^1(\mathbb{Q}_p)} f_D(t) d\mu_g(t)$ can be numerically approximated by a partial Riemann product, which for a covering $\mathcal{U}$ of $\mathbb{P}^1(\mathbb{Q}_p)$ is

$$\prod_{U \in \mathcal{U}} f_D(t_U)^{\mu_g(U)}, \quad t_U \text{ any sample point in } U.$$

Suppose that $D = \tau_2 - \tau_1 \in \mathrm{Div}^0 \mathcal{H}_p$, and that we want to compute the integral

$$\int\!\!\!\!\!\!\diagup_{\mathbb{P}^1(\mathbb{Q}_p)} f_D(t)\, d\mu_g = \int\!\!\!\!\!\!\diagup_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{t-\tau_2}{t-\tau_1} \right) d\mu_g$$

with an accuracy of p^{-n}. The size of the covering $\mathcal{U}$ is determined by the affinoids in which τ_1 and τ_2 lie. To be more precise, let r be a positive integer such that none of the elements $\tau_1, \tau_2, \omega_p\tau_1, \omega_p\tau_2$ is congruent to an integer modulo p^r. That is to say, such that

$$|\tau_1 - i|_p > p^{-r},\ |\tau_2 - i|_p > p^{-r},\ |\omega_p\tau_1 - i|_p > p^{-r},\ |\omega_p\tau_2 - i|_p > p^{-r} \quad \text{for all } i \in \mathbb{Z}. \tag{4.3}$$

Observe that we can find such an r because $\tau_1, \tau_2, \omega_p\tau_1, \omega_p\tau_2$ do not belong to $\mathbb{Q}_p$. The function $f_D(t)$ is locally constant modulo p^n when restricted to open balls of diameter $p^{-(n+r)}$. Therefore, in order to obtain the value of J_ψ correct modulo p^n, it is enough to consider a finite covering $\mathcal{U}_{n+r}$ of $\mathbb{P}^1(\mathbb{Q}_p)$ consisting of open balls of diameter $p^{-(n+r)}$.

Since μ_g is defined as an element of $\mathcal{F}_0(\mathcal{E},\mathbb{Z}) \simeq \mathcal{F}(\mathcal{E}^+,\mathbb{Z})$ it is useful to describe this covering of $\mathbb{P}^1(\mathbb{Q}_p)$ in terms of $\mathcal{E}^+$ as follows. Note that

$$\mathbb{P}^1(\mathbb{Q}_p) = \coprod_{t=0}^{p} \tilde{\gamma}_t^{-1}\mathbb{Z}_p,$$

with $\tilde{\gamma}_t^{-1}\mathbb{Z}_p$ of diameter $1/p$. In Corollary 2.5, we have described a covering $\mathcal{B}(\mathbb{Z}_p, p^{-n})$ of $\mathbb{Z}_p$, and therefore one obtains the corresponding covering of $\mathbb{P}^1(\mathbb{Q}_p)$ as

$$\mathbb{P}^1(\mathbb{Q}_p) = \coprod_{t,i_m,j_m} (\tilde{\gamma}_{i_1}\gamma_{j_1}\cdots\tilde{\gamma}_{i_n}\gamma_{j_n}\tilde{\gamma}_t)^{-1}\mathbb{Z}_p,$$

where the indexes i_m, j_m vary over $\{1,\dots,p\}$ and t varies over $\{0,\dots,p\}$.

4.4. *A numerical example*

We let $p = 13$, $D = 2\cdot 3$, and $M = 1$. Consider the elliptic curve with Cremona label '78a1':

$$E\colon y^2 + xy = x^3 + x^2 - 19x + 685.$$

Let $K = \mathbb{Q}(\sqrt{5})$, which is the quadratic field with smallest discriminant satisfying that 2, 3 and 13 are inert in K. One observes that the point $P = (-2, 12\sqrt{5}+1) \in E(K)$ generates the free part of $E(K)$.

Let B be the quaternion algebra ramified precisely at 2 and 3. It can be given as the $\mathbb{Q}$-algebra $\mathbb{Q}\langle i,j\rangle$, with relations $i^2 = 6$, $j^2 = -1$, $ij = -ji$.

Let ι_{13} be the $\mathbb{Q}$-algebra embedding of $B \to M_2(\mathbb{Q}_{13})$ which sends

$$i \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad j \mapsto \frac{1}{\rho}\begin{pmatrix} -1 & -24 \\ 4 & 1 \end{pmatrix},$$

with ρ being the unique square root of 95 in $\mathbb{Q}_{13}$ which satisfies $\rho \equiv 2 \pmod{13}$. Let $R_0(1) \subset B$ be the maximal order with generators $\{1, i, (1+i+j)/2, (i+k)/2\}$, and let $\psi : \mathcal{O}_K \hookrightarrow R_0(1)$ be the embedding that sends $\sqrt{5} \in K$ to $-i-j$. This yields:

$$\tau_\psi = (11\,g+9) + (12\,g+7)\cdot 13 + (12\,g+11)\cdot 13^2 + (12\,g+12)\cdot 13^3 + (12\,g+7)\cdot 13^4 + O(13^5),$$

where $g \in K_{13}$ satisfies $g^2 - g - 1 = 0$ and $\gamma_\psi = (3-i-j)/2$.

The element γ_ψ does not belong to the commutator subgroup of $\Gamma_0^6(1)_{\mathrm{ab}}$, but γ_ψ^{12} does. We rewrite the cycle $\gamma_\psi^{12} \otimes \tau_\psi$ in $H_1(\Gamma_0^6(1), \operatorname{Div}\mathcal{H}_{13})$ as the sum of 16 terms. Also, we act on γ_ψ^{12} with t_5.

Finally, we compute the integration pairing using Riemann products on coverings consisting of those opens of diameter 13^{-n} for $n \in \{1,2,3\}$. Table 1 gives the time that this computation took in our test computer. Observe that the number of evaluations grows exponentially in n, and therefore so does the time it takes to complete the integration.

We obtain the value $J_\psi = (3g+2)13 + (g+9)13^2 + O(13^3)$ and, after applying the Tate parameterization, obtain $P_\psi \in E(K_{13})$ having coordinates

$$(x,y) = (11 + 8\cdot 13 + 5\cdot 13^2 + O(13^3), (11g+2) + (7g+11)\cdot 13 + (7g+12)\cdot 13^2 + O(13^3)).$$

TABLE 1. *Running time increases exponentially with the precision.*

n	Number of opens	Time (s)
1	14	3
2	182	49
3	2366	1158

This point agrees with $48 \cdot P$ up to the working precision of three 13-adic digits. Note that $48 = 12 \cdot (5 + 1 - a_5(E))$. The factor of $5 + 1 - a_5(E)$ appears because of the application of t_5, and the factor of 12 appears because it was needed to kill the torsion of $\Gamma_0^6(1)_{\mathrm{ab}}$.

Although the previous computation gives evidence in support of the conjecture, the result is not very satisfying. First, an approximation modulo 13^3 could conceivably come from a numerical coincidence. More importantly, a previous knowledge of a generator for $E(K)$ was needed, and finding such a point is a hard problem in general. If we had a way to obtain a much better approximation, then we could use algebraic recognition routines to guess the algebraic point. This is, in fact, the goal of the next section.

5. *The integration pairing via overconvergent cohomology*

We continue with the notation of Subsection 4.3. Namely, μ denotes the cohomology class associated to E and $\tilde{c}_\psi$ the homology class associated to an optimal embedding ψ, which is of the form

$$\tilde{c}_\psi = \sum_k g_k \otimes (\tau_k' - \tau_k)$$

for some $g_k \in \Gamma$ and $\tau_k, \tau_k' \in \mathcal{H}_p$. Therefore, the integrals involved in the computation of J_ψ are of the form

$$\int\!\!\!\!\!\!\diagup_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_g(t), \quad \text{with } g \in \Gamma \text{ and } \tau_1, \tau_2 \in \mathcal{H}_p. \tag{5.1}$$

The goal of this section is to provide an algorithm for computing these integrals based on the overconvergent cohomology lifting theorems of [**16**], which is more efficient than evaluating the Riemann products. In fact, the complexity of the overconvergent method that we present is polynomial in the number of p-adic digits of accuracy, whereas computing via Riemann sums is of exponential complexity.

Since the type of integrals that can be directly computed by means of overconvergent cohomology are not exactly of the form (5.1), we first need to perform certain transformations and reductions. Thus, the method that we next describe can be divided into the following two steps.

(1) Reduce the problem of computing integrals of the form (5.1) to that of computing the so-called *moments* of μ at elements of $\Gamma_0^D(pM)$. That is to say, express the integrals of (5.1) in terms of integrals of the form

$$\int_{\mathbb{Z}_p} t^i d\mu_g \quad \text{for } g \in \Gamma_0^D(pM) \text{ and } i \in \mathbb{Z}_{\geqslant 0}. \tag{5.2}$$

(2) Give an algorithm for computing the integrals (5.2) by means of the overconvergent cohomology lifting techniques of [**16**].

These two steps are explained in Subsections 5.1 and 5.2, respectively.

5.1. *From general integrals to moments*

The first step in order to express integrals of the form (5.1) in terms of the moments (5.2) is to consider covers of $\mathbb{P}^1(\mathbb{Q}_p)$, such that the integrand is analytic on each of the opens. Before fixing our choice of cover, we begin by proving a lemma that we will need in this process.

LEMMA 5.1. *Suppose that $\gamma \in \Gamma$ is of the form $\gamma = \tilde{\gamma}_{k_1}\gamma_{k_2}\tilde{\gamma}_{k_3}\cdots$ for some $k_\ell \in \{1, \dots, p\}$. Then $\mu_{\gamma|\mathbb{Z}_p} = 0$ (that is, the restriction of μ_γ to $\mathbb{Z}_p$ is 0).*

Proof. It is enough to show that $\mu_\gamma(U_e) = 0$ for all U_e contained in $\mathbb{Z}_p$. By Corollary 2.5, if $U_e = \gamma_e^{-1}\mathbb{Z}_p$ is contained in $\mathbb{Z}_p$, then $\gamma_e = \tilde{\gamma}_{i_1}\gamma_{j_1}\cdots\tilde{\gamma}_{i_r}\gamma_{j_r}$ for some $i_s, j_s \in \{1,\dots,p\}$. Then we see that

$$\gamma_e\gamma = \tilde{\gamma}_{i_1}\gamma_{j_1}\cdots\tilde{\gamma}_{i_r}\gamma_{j_r}\tilde{\gamma}_{k_1}\gamma_{k_2}\tilde{\gamma}_{k_3}\cdots,$$

from which we see that $\gamma_e\gamma$ belongs to our system of representatives $\mathcal{Y}$ for $\Gamma_0^D(pM)\backslash\Gamma$. Therefore, from the identity $\gamma_e\gamma = 1\cdot\gamma_e\gamma$ and the definition of μ (see (3.2)), we obtain that $\mu_\gamma(U_e) = \varphi_1 = 0$. □

Let r be a positive integer such that none of the elements $\tau_1, \tau_2, \omega_p\tau_1, \omega_p\tau_2$ is congruent to an integer modulo p^r, as in (4.3). Consider a covering of $\mathbb{P}^1(\mathbb{Q}_p)$ of the form

$$\mathbb{P}^1(\mathbb{Q}_p) = \bigsqcup_{t=0}^{p}\bigsqcup_{i_m,j_m}(\tilde{\gamma}_{i_1}\gamma_{j_1}\cdots\tilde{\gamma}_{i_n}\gamma_{j_n}\tilde{\gamma}_t)^{-1}\mathbb{Z}_p,$$

with the i_m, j_m varying over $\{1,\dots,p\}$, and such that every open has diameter $\leqslant p^{-(r+1)}$. Using this covering for breaking the integral (5.1), we are reduced to consider integrals of the form

$$\int\!\!\!\!\!\!\diagup_{(\tilde{\gamma}_{i_1}\gamma_{j_1}\cdots\tilde{\gamma}_{i_n}\gamma_{j_n}\tilde{\gamma}_t)^{-1}\mathbb{Z}_p}\left(\frac{t-\tau_2}{t-\tau_1}\right)d\mu_g(t) \quad \text{for } g\in\Gamma$$

and $t \in \{0,\dots,p\}$, $i_s, j_s \in \{1,\dots,p\}$.

To lighten the notation set $\alpha = \tilde{\gamma}_{i_1}\gamma_{j_1}\cdots\tilde{\gamma}_{i_n}\gamma_{j_n}\tilde{\gamma}_t$. Then we have that

$$\begin{aligned}\int\!\!\!\!\!\!\diagup_{\alpha^{-1}\mathbb{Z}_p}\left(\frac{t-\tau_2}{t-\tau_1}\right)d\mu_g(t) &= \int\!\!\!\!\!\!\diagup_{\mathbb{Z}_p}\left(\frac{\alpha^{-1}t-\tau_2}{\alpha^{-1}t-\tau_1}\right)d\mu_g(\alpha^{-1}t) = \int\!\!\!\!\!\!\diagup_{\mathbb{Z}_p}\left(\frac{\alpha^{-1}t-\tau_2}{\alpha^{-1}t-\tau_1}\right)d(\alpha\mu_g)(t)\\ &= \int\!\!\!\!\!\!\diagup_{\mathbb{Z}_p}\left(\frac{\alpha^{-1}t-\tau_2}{\alpha^{-1}t-\tau_1}\right)d\mu_{\alpha g}(t) \div \int\!\!\!\!\!\!\diagup_{\mathbb{Z}_p}\left(\frac{\alpha^{-1}t-\tau_2}{\alpha^{-1}t-\tau_1}\right)d\mu_\alpha(t)\\ &= \int\!\!\!\!\!\!\diagup_{\mathbb{Z}_p}\left(\frac{\alpha^{-1}t-\tau_2}{\alpha^{-1}t-\tau_1}\right)d\mu_{\alpha g}(t),\end{aligned}$$

where we have used the cocycle property of μ and the fact that $\mu_{\alpha|\mathbb{Z}_p} = 0$ by Lemma 5.1. Therefore, letting $\phi_0(t) := ((\alpha^{-1}t-\tau_2)/(\alpha^{-1}t-\tau_1))$, we have reduced the problem to compute integrals of the form

$$\int\!\!\!\!\!\!\diagup_{\mathbb{Z}_p}\phi_0(t)\,d\mu_g \quad \text{for } g\in\Gamma. \tag{5.3}$$

The next step is to express the above integrals in terms of integrals with respect to measures of the form μ_{g_0}, where $g_0 \in \Gamma_0^D(pM)$. For instance, if we write $g = g_0\gamma$ with $g_0 \in \Gamma_0^D(pM)$ and $\gamma \in \mathcal{Y}$, Proposition 5.2 asserts that, under a certain condition on γ, then we have an equality

$$\int\!\!\!\!\!\!\diagup_{\mathbb{Z}_p}\phi_0(t)\,d\mu_g(t) = \int\!\!\!\!\!\!\diagup_{\mathbb{Z}_p}\phi_0(t)\,d\mu_{g_0}(t).$$

Recall that an edge $e \in \mathcal{E}$ is said to be inward if $d(t(e), e_*) < d(s(e), e_*)$. Given $g \in \Gamma$, the edge $g^{-1}(e_*)$ is inward if and only if $g = g_0\gamma$ with $g_0 \in \Gamma_0^D(pM)$ and $\gamma \in \mathcal{Y}$ of the form

$$\gamma = \tilde{\gamma}_t\gamma_{i_1}\tilde{\gamma}_{i_2}\cdots \quad \text{for some } t, i_1, \dots, i_n \in \{1,\dots,p\}. \tag{5.4}$$

Proposition 5.2. *Let g be an element in Γ such that $g^{-1}(e_*)$ is an inward edge. If $g = g_0\gamma$ with γ as in (5.4), then $\mu_{g|\mathbb{Z}_p} = \mu_{g_0|\mathbb{Z}_p}$.*

Proof. By Lemma 5.1, the measure μ_γ is 0 when restricted to $\mathbb{Z}_p$. By the cocycle condition, we have that $\mu_g = \mu_{g_0\gamma} = \mu_{g_0} + g_0\mu_\gamma$. Since $g_0 \in \Gamma_0^D(pM)$ if $U \subset \mathbb{Z}_p$, then $g_0^{-1}U \subset \mathbb{Z}_p$, so that $g_0\mu_\gamma(U) = \mu_\gamma(g_0^{-1}U) = 0$ and we see that $g_0\mu_\gamma$ is 0 when restricted to $\mathbb{Z}_p$. □

Suppose now that $g^{-1}(e_*)$ is outward, so that we cannot directly apply Proposition 5.2. In this case, observe that $(\tilde{\gamma}_i g)^{-1}(e_*)$ is inward for all $i \in \{1, \dots, p\}$. Thus, we can write

$$\begin{aligned}\int\!\!\!\!\!\!\diagup_{\mathbb{Z}_p} \phi_0(t)\, d\mu_g(t) &= \left(\int\!\!\!\!\!\!\diagup_{\mathbb{P}^1(\mathbb{Q}_p)\setminus\mathbb{Z}_p} \phi_0(t)\, d\mu_g(t) \right)^{-1} = \prod_{i=1}^{p} \left(\int_{\tilde{\gamma}_i^{-1}\mathbb{Z}_p} \phi_0(t)\, d\mu_g(t) \right)^{-1} \\ &= \prod_{i=1}^{p} \left(\int_{\mathbb{Z}_p} \phi_0(\tilde{\gamma}_i^{-1}t)\, d\mu_g(\tilde{\gamma}_i^{-1}t) \right)^{-1} = \prod_{i=1}^{p} \left(\int_{\mathbb{Z}_p} \phi_0(\tilde{\gamma}_i^{-1}t)\, d\mu_{\tilde{\gamma}_i g}(t) \right)^{-1}\end{aligned}$$

and apply Proposition 5.2 to each of the integrals in the last term.

Summing up, we have expressed any integral as in (5.1) as a product of integrals of the form

$$\int\!\!\!\!\!\!\diagup_{\mathbb{Z}_p} \phi_i(t)\, d\mu_g(t) \quad \text{for } g \in \Gamma_0^D(pM),$$

where $\phi_i := \phi_0(\tilde{\gamma}_i^{-1}t)$ for $i = 0, 1, \dots, p$.

Next, we show that the functions $\phi_i(t)$ are analytic on $\mathbb{Z}_p$, thanks to our choice of the covering of $\mathbb{P}^1(\mathbb{Q}_p)$. We begin by analyzing $\phi_0(t)$, since the result for the other $\phi_i(t)$ will follow easily from this case.

LEMMA 5.3. *The function $\phi_0(t) = (\alpha^{-1}t - \tau_2)/(\alpha^{-1}t - \tau_1)$ is analytic on $\mathbb{Z}_p$ and has a series expansion of the form*

$$\frac{\alpha^{-1}t - \tau_2}{\alpha^{-1}t - \tau_1} = \alpha_0 \left(1 + \sum_{n=1}^{\infty} \alpha_n p^{2n} t^n \right) \tag{5.5}$$

with the α_n belonging to $\mathcal{O}_p$, the ring of integers of K_p, for all $n \geqslant 1$.

Proof. Let $\mathfrak{J} = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}_p) \colon p \mid c \}$, which is the stabilizer of $\mathbb{Z}_p$ under the action $\mathrm{GL}_2(\mathbb{Q}_p)$ in the set of balls of $\mathbb{P}^1(\mathbb{Q}_p)$. Observe that if a function $\phi(t)$ satisfies the conclusions of the lemma, then also $\phi(\gamma t)$ does for all $\gamma \in \mathfrak{J}$. There are two cases to consider:

(i) The open $\alpha^{-1}\mathbb{Z}_p$ is contained in $\mathbb{Z}_p$. Then, since $\alpha^{-1}\mathbb{Z}_p$ is a ball of diameter $p^{-(r+1)}$, we find that

$$\alpha^{-1}\mathbb{Z}_p = \begin{pmatrix} p^{r+1} & i \\ 0 & 1 \end{pmatrix} \mathbb{Z}_p \quad \text{for some } i \in \mathbb{Z}.$$

Therefore, $\alpha^{-1}u_0 = \left(\begin{smallmatrix} p^{r+1} & i \\ 0 & 1 \end{smallmatrix}\right)$ for some $u_0 \in \mathfrak{J}$. Then, by our previous remark, we can replace t by $u_0 t$, and we find that

$$\phi_0(u_0 t) = \frac{\alpha^{-1}u_0 t - \tau_2}{\alpha^{-1}u_0 t - \tau_1} = \frac{\begin{pmatrix} p^{r+1} & i \\ 0 & 1 \end{pmatrix} t - \tau_2}{\begin{pmatrix} p^{r+1} & i \\ 0 & 1 \end{pmatrix} t - \tau_1} = \frac{(i - \tau_2)}{(i - \tau_1)} \frac{(1 + (p^{r+1}/(i - \tau_2))t)}{(1 + (p^{r+1}/(i - \tau_1))t)}.$$

Now the key point is that by our choice of r in (4.3), we have that $v_p(i - \tau_2) < r$, so that $v_p(p^{r+1}/(i - \tau_j)) \geqslant 2$, and the result follows by taking the power series expansion in the above expression.

(ii) The open $\alpha^{-1}\mathbb{Z}_p$ is contained in $\mathbb{P}^1(\mathbb{Q}_p) \setminus \mathbb{Z}_p$. In this case, observe that $\omega_p\alpha^{-1}\mathbb{Z}_p \subset \mathbb{Z}_p$. Therefore,

$$\frac{\alpha^{-1}t - \tau_2}{\alpha^{-1}t - \tau_1} = \frac{\omega_p\alpha^{-1}t - \omega_p\tau_2}{\omega_p\alpha^{-1}t - \omega_p\tau_1},$$

and the argument is exactly the same as before by noting that $\omega_p\alpha^{-1}\mathbb{Z}_p$ is of diameter $p^{-(r+1)}$ and therefore $\omega_p\alpha^{-1} = \left(\begin{smallmatrix} p^{r+1} & i \\ 0 & 1 \end{smallmatrix}\right)$ for some i, and that our choice of r also works well for $\omega_p\tau_1$ and $\omega_p\tau_2$. □

PROPOSITION 5.4. *For every $i = 0, 1, \ldots, p$ the function $\phi_i(t) = \phi_0(\tilde{\gamma}_i^{-1}t)$ is analytic on $\mathbb{Z}_p$ and has a series expansion of the form*

$$\frac{\alpha^{-1}t - \tau_2}{\alpha^{-1}t - \tau_1} = \alpha_0\left(1 + \sum_{n=1}^{\infty} \alpha_n p^n t^n\right) \tag{5.6}$$

with the α_n belonging to $\mathcal{O}_p$, the ring of integers of K_p, for all $n \geqslant 1$.

Proof. The result is clear for $i = 0$. For $i > 0$, observe that $\tilde{\gamma}_i$ is (up to an element in $\mathfrak{J}$) locally of the form $\left(\begin{smallmatrix} -i & 1/p \\ p & 0 \end{smallmatrix}\right)$. Thus, we can assume that

$$\phi_i(t) = \phi_0\left(\frac{-1/p}{pt - i}\right) \tag{5.7}$$

and the result follows directly from Lemma 5.3 (note the factor p^{2n} in the series expansion (5.5)). □

At this point, we have reduced to compute integrals of the form

$$I = \int_{\mathbb{Z}_p} \phi(t)\, d\mu_g(t), \quad \text{where } g \in \Gamma_0^D(pM) \text{ and } \phi(t) = \alpha_0\left(1 + \sum_{n=1}^{\infty} \alpha_n p^n t^n\right). \tag{5.8}$$

Let log be the unique homomorphism $\log\colon K_p^\times \to K_p$ such that $\log(1-t) = -\sum_{n=1}^{\infty} t^n/n$ and $\log(p) = 0$. Its kernel is $p^{\mathbb{Z}} \times \mathbb{U}$, where $\mathbb{U}$ denotes the group of roots of unity in $K_p^\times$. Observe that the series of $\phi(t)$ converges for $t \in \mathbb{Z}_p$ and is constant modulo $p^{v_p(\alpha_0)+1}$. Thus, the integral I of (5.8) can be computed as

$$I = p^{v_p(\alpha_0)} \cdot \zeta \cdot \exp(\log I),$$

where ζ is the Teichmüller lift of the unit part of I modulo p, which can be computed as the Riemann product in the covering of $\mathbb{Z}_p$ by balls of diameter p^{-1}. Therefore, it only remains to compute the logarithm of I, which is the additive integral

$$\log I = \int_{\mathbb{Z}_p} \log \phi(t)\, d\mu_g(t). \tag{5.9}$$

Observe that $\log \phi(t)$ is analytic on $\mathbb{Z}_p$ and it has a series expansion of the form

$$\log(\phi(t)) = \beta_0 + \sum_{n=1}^{\infty} \frac{\beta_n}{n} p^n t^n, \quad \text{with } \beta_i \in \mathcal{O}_p.$$

Let $\mu_{g_{|\mathbb{Z}_p}}$ denote the measure on $\mathbb{Z}_p$ obtained by restriction of μ_g, and let $\omega_g(n)$ denote its nth moment

$$\omega_g(n) = \int_{\mathbb{Z}_p} t^n\, d\mu_g(t).$$

We see that the additive integral of (5.9) can be expressed as

$$\beta_0\omega_g(0) + \sum_{n\geqslant 1} \frac{p^n}{n}\beta_n\omega_g(n) \tag{5.10}$$

for some $\beta_n \in \mathcal{O}_p$. Now, suppose that we want to evaluate (5.10) modulo p^M; that is, we want to compute the first M p-adic digits of (5.10). For this it is enough to compute, for each $i = 0, 1, \ldots, M'$, the moment $\omega_g(i)$ to an accuracy of $p^{M''-i}$, where

$$M' = \sup\{n\colon \operatorname{ord}_p(p^n/n) < M\} \quad \text{and} \quad M'' = M + [\log(M')/\log(p)].$$

Summing up, we have reduced the problem of computing integrals as in (5.1) to that of computing moments of the form

$$\omega_g(i) = \int_{\mathbb{Z}_p} t^n d\mu_g(t) \ (\operatorname{mod} p^{M''-i}) \quad \text{for } g \in \Gamma_0^D(pM) \text{ and } i = 0, \ldots, M'. \tag{5.11}$$

In the next subsection, we present an algorithm for computing the moments (5.11) based on overconvergent cohomology.

5.2. *Computing the moments via overconvergent cohomology*

We present an algorithm for efficiently computing the moments $\omega_g(n) = \int_{\mathbb{Z}_p} t^n d\mu_g(t)$ for $g \in \Gamma_0^D(pM)$, based on the overconvergent cohomology methods of Pollack and Pollack [**16**]. We begin by slightly adapting the lifting results of [**16**, Section 3] (because we need to lift cocycles rather than just cohomology classes), and then we will show how to compute the moments μ by means of the lifted overconvergent cocycles.

Consider the module $\mathcal{D}$ of locally analytic $\mathbb{Z}_p$-valued distributions on $\mathbb{Z}_p$. That is to say, given a distribution $\nu \in \mathcal{D}$ and a locally analytic function $h : \mathbb{Z}_p \to \mathbb{Z}_p$, we have that $\nu(h(t)) \in \mathbb{Z}_p$, and the map $h(t) \mapsto \nu(h(t))$ is linear and continuous. Let $\Sigma_0(p)$ be the subsemigroup of $B^\times$

$$\Sigma_0(p) = \iota_p^{-1}\left(\left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_p)\colon c \equiv 0 \ (\operatorname{mod} p),\ d \in \mathbb{Z}_p^\times,\ ad - bc \neq 0\right\}\right).$$

It acts on the left on $\mathcal{D}$ as follows: if $h(t)$ is a locally analytic function on $\mathbb{Z}_p$, then

$$(\gamma \cdot \nu)(h(t)) = \nu(h(\gamma \cdot t)) \quad \text{for } \nu \in \mathcal{D}, \gamma \in \Sigma_0(p),$$

where

$$\gamma \cdot t = \frac{at + b}{ct + d} \quad \text{if } \iota_p(\gamma) = \begin{pmatrix} a & b \\ c & d\end{pmatrix}.$$

The element $\pi \in R_0(pM)$ defined in (2.7) lies in $\Sigma_0(p)$, and the double coset $\Gamma_0^D(pM)\pi\Gamma_0^D(pM)$ induces the U_p-operator on the cocycles $Z^1(\Gamma_0^D(pM), \mathcal{D})$, and on $H^1(\Gamma_0^D(pM), \mathcal{D})$. On cocycles, it is given explicitly by formula (2.11).

The module $\mathcal{D}$ is equipped with the decreasing filtration

$$\operatorname{Fil}^n \mathcal{D} = \{\nu \in \mathcal{D}\colon \nu(1) = 0,\ \nu(t^i) \in p^{n-i+1}\mathbb{Z}_p,\ \forall i \geqslant 1\},$$

which enjoys the following key properties.

LEMMA 5.5. (i) *The natural projection* $\mathcal{D} \to \varprojlim_n \mathcal{D}/\operatorname{Fil}^n \mathcal{D}$ *is an isomorphism.*

(ii) *If* $\nu \in \operatorname{Fil}^n \mathcal{D}$, *then* $\pi \cdot \nu \in \operatorname{Fil}^{n+1} \mathcal{D}$.

Proof. If ν lies in $\operatorname{Fil}^n \mathcal{D}$ for all n, then it is necessarily the 0 distribution, and this gives the first property. As for the second, we shall see that $\pi \cdot \nu(t^i) = \nu(\pi \cdot t^i)$ lies in $p^{n-i+2}\mathbb{Z}_p$ whenever

$\nu \in \mathrm{Fil}^n \mathcal{D}$. Recall that $\pi = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) u_\pi$ for some $u_\pi \in \Gamma_0^{\mathrm{loc}}(p)$, say $u_\pi = \left(\begin{smallmatrix} a & b \\ pc & d \end{smallmatrix}\right) = \frac{1}{d}\left(\begin{smallmatrix} a_0 & b_0 \\ pc_0 & 1 \end{smallmatrix}\right)$. Then

$$\pi \cdot t^i = p(u_\pi \cdot t^i) = \frac{a_0 p t^i + b_0 p}{c_0 p t^i + 1} = \sum_{j \geqslant 0} e_j (p t^i)^j,$$

where the $e_j \in \mathbb{Z}_p$ arise from the series expansion of $1/(c_0 p t^i + 1)$. Since $\nu \in \mathrm{Fil}^n \mathcal{D}$, we have that

$$\nu(1) = 0 \quad \text{and} \quad \nu(t^i) \in p^{n-i+1}\mathbb{Z}_p \ \text{ for all } i \geqslant 1,$$

which implies that $\nu(\pi \cdot t^i)$ belongs to $p^{n-i+2}\mathbb{Z}_p$. □

Thanks to these two properties, we are in the setting of [16, Section 3], in which very general lifting theorems for cohomology classes hold. However, we will need the following slightly refined version of [16, Theorem 3.1], as we are interested in lifting cocycles rather than cohomology classes.

PROPOSITION 5.6. *Let $\theta_0 \in Z^r(\Gamma_0^D(pM), \mathcal{D}/\mathrm{Fil}^0 \mathcal{D})$ be an element such that $U_p\theta_0 = \alpha\theta_0$ for some $\alpha \in \mathbb{Z}_p^\times$. Then there exists $\Theta \in Z^r(\Gamma_0^D(pM), \mathcal{D})$ such that:*

(i) *the image of Θ in $Z^r(\Gamma_0^D(pM), \mathcal{D}/\mathrm{Fil}^0 \mathcal{D})$ is equal to θ_0 (that is, Θ is a lift of θ_0); and*
(ii) *the r-cocycle Θ satisfies $U_p\Theta = \alpha\Theta$.*

Moreover, if $\Theta' \in Z^r(\Gamma_0^D(pM), \mathcal{D})$ is another cocycle that lifts θ_0 such that $U_p\Theta' = \alpha\Theta'$, then $\Theta' = \Theta$.

As in [16], before proving this we state two lemmas that are, in fact, key to the proof.

LEMMA 5.7. *If $\theta \in C^r(\Gamma_0^D(pM), \mathrm{Fil}^n \mathcal{D})$, then $U_p\theta$ lies in $C^r(\Gamma_0^D(pM), \mathrm{Fil}^{n+1} \mathcal{D})$.*

Proof. This is identical to the proof of [16, Lemma 3.3]. □

LEMMA 5.8. *If θ lies in the kernel of $Z^r(\Gamma_0^D(pM), \mathcal{D}) \to Z^r(\Gamma_0^D(pM), \mathcal{D}/\mathrm{Fil}^0 \mathcal{D})$ and $U_p\theta = \alpha\theta$ for some $\alpha \in \mathbb{Z}_p^\times$, then $\theta = 0$.*

Proof. That θ lies in the kernel of $Z^r(\Gamma_0^D(pM), \mathcal{D}) \to Z^r(\Gamma_0^D(pM), \mathcal{D}/\mathrm{Fil}^0 \mathcal{D})$ is equivalent to the fact that $\theta \in Z^r(\Gamma_0^D(pM), \mathrm{Fil}^0 \mathcal{D})$. Now $\theta = \alpha^{-1}U_p\theta$, and iterating this we find that $\theta = \alpha^{-n}U_p^n\theta$. Thus, by Lemma 5.7, we see that θ lies in $Z^r(\Gamma_0^D(pM), \mathrm{Fil}^n \mathcal{D})$ for all n, and it must be $\theta = 0$. □

Proof of Proposition 5.6. The proof is essentially the same as in [16], but keeping track of the cocycles and not just the cohomology classes. It is important to mention that the proof is actually constructive, and it provides us with a very efficient method for algorithmically computing such lifts.

First, we show the existence of Θ. Let $\tilde{\theta}_0 \in C^r(\Gamma_0^D(pM), \mathcal{D})$ be an arbitrary lift of θ_0, and for $n > 0$ define $\tilde{\theta}_n := \alpha^{-n}U_p^n\tilde{\theta}_0$. Since θ_0 is a cocycle and $\tilde{\theta}_0$ is a lift of θ_0, we have that $\partial^r\tilde{\theta}_0 \in C^{r+1}(\Gamma_0^D(pM), \mathrm{Fil}^0 \mathcal{D})$. Now

$$\partial^r\tilde{\theta}_n = \alpha^{-n}\partial^r(U_p^n\tilde{\theta}_0) = \alpha^{-n}U_p^n(\partial^r\tilde{\theta}_0);$$

by Lemma 5.7, this takes values in $\mathrm{Fil}^n \mathcal{D}$. Let θ_n be the image of $\tilde{\theta}_n$ in

$$C^r(\Gamma_0^D(pM), \mathcal{D}/\mathrm{Fil}^n \mathcal{D}).$$

We have seen that, in fact, $\theta_n \in Z^r(\Gamma_0^D(pM), \mathcal{D}/\mathrm{Fil}^n \mathcal{D})$. Since $U_p\theta_0 = \alpha\theta_0$, we have that $U_p\tilde{\theta}_0 - \alpha\tilde{\theta}_0$ belongs to $C^r(\Gamma_0^D(pM), \mathrm{Fil}^0 \mathcal{D})$. Therefore, one easily checks that $U_p\tilde{\theta}_n - \alpha\tilde{\theta}_n$ lies in $C^r(\Gamma_0^D(pM), \mathrm{Fil}^n \mathcal{D})$, and we see that $U_p\theta_n = \alpha\theta_n$. Also, it is easy to see that $\tilde{\theta}_n - \tilde{\theta}_{n-1}$ is in $C^r(\Gamma_0^D(pM), \mathrm{Fil}^n \mathcal{D})$. Then we can define Θ as

$$\Theta = \{\theta_n\} \in \varprojlim Z^r(\Gamma_0^D(pM), \mathcal{D}/\mathrm{Fil}^n \mathcal{D}) = Z^r(\Gamma_0^D(pM), \mathcal{D}).$$

By construction, Θ lifts θ_0 and $U_p\Theta = \alpha\Theta$.

Now in order to prove uniqueness, let $\Theta' \in Z^n(\Gamma_0^D(pM), \mathcal{D})$ be an element that lifts θ_0 and such that $U_p\Theta' = \alpha\Theta'$. The difference $\Theta - \Theta'$ will be an element in the kernel of

$$Z^r(\Gamma_0^D(pM), \mathcal{D}) \to Z^r(\Gamma_0^D(pM), \mathcal{D}/\mathrm{Fil}^0 \mathcal{D})$$

such that $U_p(\Theta - \Theta') = \alpha(\Theta - \Theta')$. By Lemma 5.8, we have that $\Theta - \Theta' = 0$. □

We will apply Proposition 5.6 to the cocycle $\varphi = \varphi_E \in Z^1(\Gamma_0^D(pM), \mathbb{Z})$ attached to E (and to a choice of sign at infinity) that we fixed in Subsection 3.1. Indeed, since

$$\mathrm{Fil}^0 \mathcal{D} = \{\nu \in \mathcal{D}(\mathbb{Z}_p) \colon \nu(1) = 0\}$$

the map $\nu \mapsto \nu(1)$ induces an isomorphism $\mathcal{D}/\mathrm{Fil}^0 \mathcal{D} \cong \mathbb{Z}_p$. Thus φ can be naturally seen, after extending scalars to $\mathbb{Z}_p$, as a 1-cocycle

$$\varphi \in Z^1(\Gamma_0^D(pM), \mathbb{Z}_p) = Z^1(\Gamma_0^D(pM), \mathcal{D}/\mathrm{Fil}^0 \mathcal{D}).$$

Since $U_p\varphi = a_p\varphi$ with $a_p \in \{\pm 1\}$, as a direct application of Proposition 5.6, we have the following propositions.

Proposition 5.9. *There exists a unique $\Phi \in Z^1(\Gamma_0^D(pM), \mathcal{D})$ lifting φ and such that $U_p\Phi = a_p\Phi$.*

The proof of Proposition 5.6 gives an effective method for computing (approximations to) Φ: one takes any cochain $\tilde{\Phi}$ in $C^1(\Gamma_0^D(pM), \mathcal{D})$ that lifts φ, and iterates a_pU_p. After k iterations, the natural image of the resulting cochain $a_p^k U_p^k \tilde{\Phi}$ belongs to $Z^1(\Gamma_0^D(pM), \mathcal{D}/\mathrm{Fil}^k \mathcal{D})$, and we can think of it as an approximation to the desired Φ, correct up to an element of $Z^1(\Gamma_0^D(pM), \mathrm{Fil}^k \mathcal{D})$.

Let $g_1, \dots, g_t$ be the generators of $\Gamma_0^D(pM)$, explicitly provided by Voight's algorithms [**19**]. If $g \in \Gamma_0^D(pM)$, then we can express Φ_g in terms of the Φ_{g_j} by means of the cocycle relation of Φ. A possible choice for $\tilde{\Phi}$ is then the chain determined by

$$\tilde{\Phi}_{g_j}(1) = \varphi_{g_j}, \quad \tilde{\Phi}_{g_j}(t^i) = 0 \text{ for } i > 0.$$

The action of a_pU_p is computed by means of formula (2.11). After k iterations, only the values $a_p\tilde{\Phi}_{g_j}(t^i)$ with $i \leqslant k$ will be different from 0, and the resulting chain will be equal to Φ modulo $\mathrm{Fil}^k \mathcal{D}$. Namely, we will have computed the quantities

$$\Phi_{g_j}(t^i) \pmod{p^{k-i+1}}, \quad i = 0, \dots, k. \tag{5.12}$$

The next step is to show that $\Phi_g(t^i)$ is equal to the moment $\omega_g(i)$ for any $g \in \Gamma_0^D(pM)$. This means that the moments $\omega_g(i) \pmod{p^{k-i+1}}$ for $g \in \Gamma_0^D(pM)$ can be computed by the method explained above.

PROPOSITION 5.10. *Let h be an analytic function on $\mathbb{Z}_p$ and $g \in \Gamma_0^D(pM)$. Then*

$$\Phi_g(h(t)) = \int_{\mathbb{Z}_p} h(t)\, d\mu_g(t).$$

Proof. Let Ψ be the cochain $\Psi \in C^1(\Gamma_0^D(pM), \mathcal{D})$ defined by the formula

$$\Psi_g(h(t)) = \int_{\mathbb{Z}_p} h(t)\, d\mu_g(t).$$

We will show that Ψ is a cocycle, which lifts φ, and which satisfies $U_p\Psi = a_p\Psi$. This will finish the proof, because the uniqueness part of Proposition 5.6 will imply that $\Psi = \Phi$.

That Φ lifts φ is an immediate consequence of property (iv) of Theorem 3.1. The cocycle property of μ implies that of Ψ:

$$\begin{aligned}\Psi_{gh}(h(t)) &= \int_{\mathbb{Z}_p} h(t)\, d\mu_{gh}(t) = \int_{\mathbb{Z}_p} h(t)\, d(\mu_g(t) + \mu_h(g^{-1}t)) \\ &= \int_{\mathbb{Z}_p} h(t)\, d\mu_g(t) + \int_{\mathbb{Z}_p} h(gt)\, d\mu_h(t) = \Psi_g(h(t)) + (g \cdot \Psi_h)(h(t)),\end{aligned}$$

where the second equality follows from a change of variables and the fact that $g^{-1}\mathbb{Z}_p = \mathbb{Z}_p$ for all $g \in \Gamma_0^D(pM)$. As for the last claim, it follows from the computation:

$$\begin{aligned}(U_p\Psi)_g(h(t)) &= \sum_{i=1}^{p} \int_{\mathbb{Z}_p} h(s_i t)\, d\mu_{t_i(g)}(t) \overset{(*)}{=} \sum_{i=1}^{p} \int_{\mathbb{Z}_p} h(s_i t)\, d(a_p\mu_g(s_i t)) \\ &= a_p \sum_{i=1}^{p} \int_{s_i\mathbb{Z}_p} h(t)\, d\mu_g(t) = a_p \int_{\mathbb{Z}_p} h(t)\, d\mu_g(t) = a_p\Psi_g(h(t)),\end{aligned}$$

where the equality $(*)$ is justified by Lemma 5.13. □

We remark that Lemma 5.13, although of a technical nature, provides the key calculation in the proof of the above proposition. Before proving it, we need two easy lemmas.

LEMMA 5.11. *Suppose $\gamma_e \in \mathcal{Y}$ is of the form $\gamma_e = \tilde{\gamma}_{i_1}\gamma_{j_1}\cdots\tilde{\gamma}_{i_n}\gamma_{j_n}$ with all $i_k, j_k > 0$. Then $\omega_p^{-1}\gamma_e\omega_p = \gamma_{i_1}\tilde{\gamma}_{j_1}\cdots\gamma_{i_n}\tilde{\gamma}_{j_n}$.*

Proof. We will see it by induction. If $n = 1$, we have that $\gamma_e = \tilde{\gamma}_{i_1}\gamma_{j_1}$, and then

$$\omega_p^{-1}\gamma_e\omega_p = \omega_p^{-1}(p^{-1}\omega_p\gamma_{i_1}\omega_p)\gamma_{j_1}\omega_p = \gamma_{i_1}p^{-1}\omega_p\gamma_{j_1}\omega_p = \gamma_{i_1}\tilde{\gamma}_{j_1}.$$

For $n > 1$, we write $\gamma_e = \gamma_{e'}\tilde{\gamma}_{i_n}\gamma_{j_n}$, where $\gamma_{e'} = \tilde{\gamma}_{i_1}\gamma_{j_1}\cdots\tilde{\gamma}_{i_{n-1}}\gamma_{j_{n-1}}$. Then

$$\omega_p^{-1}\gamma_e\omega_p = (\omega_p^{-1}\gamma_{e'}\omega_p)(\omega_p^{-1}\tilde{\gamma}_{i_n}\gamma_{j_n}\omega_p)$$

and now the result follows directly from the induction hypothesis. □

LEMMA 5.12. *Let $\gamma_e \in \mathcal{Y}$ be such that $U_e \subseteq \mathbb{Z}_p$. Then $\omega_p^{-1}\gamma_e\omega_p\gamma_k$ belongs to $\mathcal{Y}$ for all $k = 0, \ldots, p$.*

Proof. The statement is clear if $\gamma_e = 1$. If $\gamma_e \neq 1$, then by Corollary 2.5, we have that γ_e is of the form $\gamma_e = \tilde{\gamma}_{i_1}\gamma_{j_1}\cdots\tilde{\gamma}_{i_n}\gamma_{j_n}$. Now, by Lemma 5.11, we see that

$$\omega_p^{-1}\gamma_e\omega_p\gamma_k = \gamma_{i_1}\tilde{\gamma}_{j_1}\cdots\gamma_{i_n}\tilde{\gamma}_{j_n}\gamma_k,$$

which clearly belongs to $\mathcal{Y}$. □

LEMMA 5.13. *Let g be an element in $\Gamma_0^D(pM)$. For each $k = 1, \dots, p$, we have*

$$(\mu_{t_k(g)})_{|\mathbb{Z}_p} = (a_p s_k^{-1} \mu_g)_{|\mathbb{Z}_p}; \tag{5.13}$$

that is to say, the measures $\mu_{t_k(g)}$ and $a_p s_k^{-1}\mu_g$ coincide when restricted to $\mathbb{Z}_p$.

Proof. It is enough to show that for every $U_e \subset \mathbb{Z}_p$ one has

$$\mu_{t_k(g)}(U_e) = a_p \mu_g(s_k U_e). \tag{5.14}$$

Recall that $U_e = \gamma_e^{-1}\mathbb{Z}_p$ with $\gamma_e \in \mathcal{Y}$. By the definition of μ (see (3.2)), we have that

$$\mu_{t_k(g)}(U_e) = \varphi_b,$$

where $b \in \Gamma_0^D(pM)$ is the element uniquely determined by the equation

$$\gamma_e t_k(g) = b\gamma_{e'} \quad \text{for some } \gamma_{e'} \in \mathcal{Y}. \tag{5.15}$$

Because of the definition of $t_k(g)$ (see (2.10)), we have

$$\gamma_e t_k(g) = \gamma_e s_k^{-1} g s_{g\cdot k} = \gamma_e \omega_p \gamma_k g \gamma_{g\cdot k}^{-1} \omega_p^{-1},$$

and combining this with (5.15), we obtain

$$\gamma_e \omega_p \gamma_k g = b\gamma_{e'} \omega_p \gamma_{g\cdot k}. \tag{5.16}$$

Now to calculate the right-hand side of (5.14), we need to consider the open

$$\begin{aligned} s_k U_e &= s_k \gamma_e^{-1}\mathbb{Z}_p = \gamma_k^{-1}\omega_p^{-1}\gamma_e^{-1}\mathbb{Z}_p = (\omega_p^{-1}\gamma_e\omega_p\gamma_k)^{-1}\omega_p^{-1}\mathbb{Z}_p \\ &= \mathbb{P}^1(\mathbb{Q}_p) \setminus ((\omega_p^{-1}\gamma_e\omega_p\gamma_k)^{-1}\mathbb{Z}_p). \end{aligned}$$

Therefore, the measure on the right-hand side of (5.14) can be computed as

$$\mu_g(s_k U_e) = -\mu_g((\omega_p^{-1}\gamma_e\omega_p\gamma_k)^{-1}\mathbb{Z}_p). \tag{5.17}$$

Note that $\omega_p^{-1}\gamma_e\omega_p\gamma_k \in \mathcal{Y}$ thanks to Lemma 5.12, so in order to compute (5.17) we use (5.16) to get the identity

$$\omega_p^{-1}\gamma_e\omega_p\gamma_k g = \omega_p^{-1} b \gamma_{e'} \omega_p \gamma_{g\cdot k} = (\omega_p^{-1} b \omega_p)\omega_p^{-1}\gamma_{e'}\omega_p\gamma_{g\cdot k}.$$

Now observe that $\gamma_{e'}^{-1}\mathbb{Z}_p \subset \mathbb{Z}_p$, so again Lemma 5.12 gives that $\omega_p^{-1}\gamma_{e'}\omega_p\gamma_{g\cdot k} \in \mathcal{Y}$, and we see that

$$\mu_g(s_k U_e) = -\varphi_{\omega_p^{-1} b \omega_p} = -(W_p\varphi)_b = (U_p\varphi)_b = a_p\varphi_b,$$

and this concludes the proof. □

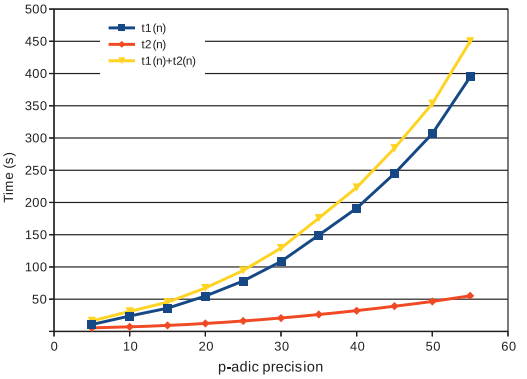
6. *Implementation and numerical evidence*

We have implemented[†] the algorithms of Sections 4 and 5 in Sage [**18**] and Magma [**3**]. Thanks to the overconvergent method, we have been able to compute the integrals up to a precision of p^{60}, although one can easily reach much higher precision if needed. Recall the sample calculation of Subsection 4.4, which we have recalculated using the overconvergent method. In Table 2, we list the time t_1 that it took to lift the original cocycle to the target precision n, and the time t_2 that it took to integrate the cycle to obtain J_τ with the target precision. One observes, as

[†]The code is available at https://github.com/mmasdeu/darmonpoints.

TABLE 2. *Running time increases sub-quadratically with the precision n.*

n	t_1 (s)	t_2 (s)	$t_1 + t_2$ (s)
10	24	7	31
20	55	12	67
30	108	21	129
40	191	32	223
50	307	46	353



expected from the analysis carried out in [**10**] and which would easily carry over to our setting, that the complexity of the algorithms is polynomial (indeed quadratic). Note also that, while it took 1158 s to obtain three digits of precision using Riemann products, it took less than a third of this time to obtain 55 digits of precision using the overconvergent method.

Another salient feature of the overconvergent method is that one can regard the lifting of the cohomology class as a precomputation that depends only on the elliptic curve and the prime p. Note that, as the table indicates, this is what dominates the computing time. With this precomputation at hand, one can perform several integrals of different cycles (that is, yielding points attached to different real quadratic fields) with little extra effort. All this allows for a direct computation of rational points, as opposite to the example of Subsection 4.4, in which the low precision only permitted to compare the computed Darmon point with an algebraic point previously found by naïve search.

Indeed, let $J_\tau \in K_p^\times$ be a Darmon point and let $P_\tau \in E(K_p)$ denote its image under Tate's uniformization, whose coordinates conjecturally belong to a number field H. Using the algorithms described in this article, one can compute an approximation to J_τ, and therefore to P_τ. Then one can try to recognize its coordinates as algebraic numbers via standard reconstruction techniques (see, for instance, [**10**, Section 1.6]). For this to work, the number of correct digits one needs to know of J_τ is roughly the height of P_τ.

One difficulty that arises in this method is that P_τ is usually a multiple of the generator of $E(H)/E(H)_{\mathrm{tors}}$, say $P_\tau = nP'_\tau$. Therefore, P_τ might have very large height, even if the generator P'_τ had small height. In this case, it is easier to reconstruct P'_τ, which has smaller height. Note that P'_τ is the image under Tate's uniformization of an element of the form

$$J'_\tau = \zeta \exp\left(\frac{1}{n}\log J_\tau\right),$$

where ζ is some Teichmüller representative in K_p. Therefore, since we can compute good approximations to $\log J_\tau$, we can try to reconstruct J'_τ by trial and error on ζ.

As a first example, consider the curve with Cremona label 78a1 with equation

$$E\colon y^2 + xy = x^3 + x^2 - 19x + 685.$$

Table 3 lists points on $E(\mathbb{Q}(\sqrt{d_K}))$ for those discriminants $d_K < 600$, in which 2, 3 and 13 are inert and such that $K = \mathbb{Q}(\sqrt{d_K})$ has class number 1. They are computed using the plus character λ_E^+ and optimal embeddings of the maximal order $\mathcal{O}_K$. Observe that the points are defined over K rather than over abelian extensions, since the class number is 1.

Table 4 lists similar computations for the curve with Cremona label 110a1 and equation

$$E\colon y^2 + xy + y = x^3 + x^2 + 10x - 45.$$

TABLE 3. *Darmon points on curve* 78a1 *with* $p = 13$ *and* $D = 6$.

d_K	P
5	$1 \cdot 48 \cdot \left(-2, 12\sqrt{5} + 1\right)$
149	$1 \cdot 48 \cdot \left(1558, -5040\sqrt{149} - 779\right)$
197	$1 \cdot 48 \cdot \left(\frac{310}{49}, \frac{720}{343}\sqrt{197} - \frac{155}{49}\right)$
293	$1 \cdot 48 \cdot \left(40, -15\sqrt{293} - 20\right)$
317	$1 \cdot 48 \cdot \left(382, -420\sqrt{317} - 191\right)$
437	$1 \cdot 48 \cdot \left(\frac{986}{23}, \frac{7200}{529}\sqrt{437} - \frac{493}{23}\right)$
461	$1 \cdot 48 \cdot \left(232, -165\sqrt{461} - 116\right)$
509	$1 \cdot 48 \cdot \left(-\frac{2}{289}, -\frac{5700}{4913}\sqrt{509} + \frac{1}{289}\right)$
557	$1 \cdot 48 \cdot \left(\frac{75622}{121}, \frac{882000}{1331}\sqrt{557} - \frac{37811}{121}\right)$

TABLE 4. *Darmon points on curve* 110a1 *with* $p = 11$ *and* $D = 10$.

d_K	P
13	$2 \cdot 30 \cdot \left(\frac{1103}{81} - \frac{250}{81}\sqrt{13}, -\frac{52403}{729} + \frac{13750}{729}\sqrt{13}\right)$
173	$2 \cdot 30 \cdot \left(\frac{1532132}{9025}, -\frac{1541157}{18050} - \frac{289481483}{1714750}\sqrt{173}\right)$
237	$2 \cdot 30 \cdot \left(\frac{190966548837842073867}{4016648659658412649} - \frac{10722443619184119320}{4016648659658412649}\sqrt{237},\right.$
	$\left. -\frac{3505590193011437142853233857149}{804999791382984541142375610 7} + \frac{235448460130564520991320372200}{804999791382984541142375610 7}\sqrt{237}\right)$
277	$2 \cdot 30 \left(\frac{46317716623881}{12553387541776}, -\frac{58871104165657}{25106775083552} - \frac{20912769335239055243}{4447760611796554 2976}\sqrt{277}\right)$
293	$2 \cdot 30 \cdot \left(\frac{7088486530742}{2971834657801}, -\frac{10060321188543}{5943669315602} - \frac{591566427769149607}{102462974768356034 02}\sqrt{293}\right)$
373	$2 \cdot 30 \cdot \left(\frac{298780258398}{62087183929}, -\frac{360867442327}{124174367858} - \frac{19368919551426449}{309408997622814 34}\sqrt{373}\right)$

TABLE 5. *Darmon points on curve* 110a1 *with* $p = 5$ *and* $D = 22$.

d_K	P
13	$2 \cdot 12 \cdot \left(4, \frac{5}{2}\sqrt{13} - \frac{5}{2}\right)$
173	$2 \cdot 12 \cdot \left(\frac{1532132}{9025}, -\frac{289481483}{1714750}\sqrt{173} - \frac{1541157}{18050}\right)$
237	$2 \cdot 12 \cdot \left(\frac{5585462179}{1193768112}, -\frac{53751973226309}{71439858894528}\sqrt{237} - \frac{6779230291}{2387536224}\right)$
277	—
293	$2 \cdot 12 \cdot \left(\frac{7088486530742}{2971834657801}, -\frac{591566427769149607}{102462974768356034 02}\sqrt{293} - \frac{10060321188543}{5943669315602}\right)$
373	$2 \cdot 12 \cdot \left(\frac{298780258398}{62087183929}, \frac{19368919551426449}{309408997622814 34}\sqrt{373} - \frac{360867442327}{124174367858}\right)$

Observe that some of the points, for example, the one over $\mathbb{Q}(\sqrt{237})$, could have not been found by naïve search methods due to their height. Table 5 shows the same points computed with the different factorization of the conductor 110, namely $p = 11$ and $D = 10$. Note that for $d_K = 277$, we were not able to recognize the point. This is probably due to the fact that the working precision (p^{60} in this case) is lower, since $p = 5$ instead of $p = 11$. In these two cases, the points obtained are twice the expected multiple of the generator. Table 6 is another

TABLE 6. *Darmon points on curve* 114a1 *with* $p = 19$ *and* $D = 6$.

d_K	P
29	$1 \cdot 72 \cdot \left(-\frac{6}{25}\sqrt{29} - \frac{38}{25}, -\frac{18}{125}\sqrt{29} + \frac{86}{125}\right)$
53	$1 \cdot 72 \cdot \left(-\frac{1}{9}, \frac{7}{54}\sqrt{53} + \frac{1}{18}\right)$
173	$1 \cdot 72 \cdot \left(-\frac{3481}{13689}, \frac{347333}{3203226}\sqrt{173} + \frac{3481}{27378}\right)$
269	$1 \cdot 72 \cdot \left(\frac{1647149414400}{23887470525361}\sqrt{269} - \frac{43248475603556}{23887470525361},$ $\frac{2359447648611379200}{116749558330761905641}\sqrt{269} + \frac{2681774974170243075 64}{116749558330761905641}\right)$
293	$1 \cdot 72 \cdot \left(\frac{21289143620808}{4902225525409}, \frac{4567039561444642548}{10854002829131490673}\sqrt{293} - \frac{10644571810404}{4902225525409}\right)$
317	$1 \cdot 72 \cdot \left(-\frac{25}{9}, -\frac{5}{54}\sqrt{317} + \frac{25}{18}\right)$
341	$1 \cdot 72 \cdot \left(\frac{3449809443179}{499880896975}, \frac{3600393040902501011}{3935597293546963250}\sqrt{341} - \frac{3449809443179}{999761793950}\right)$
413	$1 \cdot 72 \cdot \left(\frac{59}{7}, \frac{113}{98}\sqrt{413} - \frac{59}{14}\right)$

example with $D = 6$, but in this case some of the points obtained (note, for example, $d_K = 269$) have considerable height.

The examples shown above have in common that the group $H_1(\Gamma_0^D(M), \mathbb{Z})$ is finite. Although our algorithms do not require this condition to be true, the implementation is greatly simplified in this case. However, our implementation works in a broader range of cases. As an example, we have computed an example with $D = 15$, where the above group has $\mathbb{Z}$-rank 1: consider the elliptic curve with Cremona label 285c1 ($285 = 19 \cdot 15$) given by the equation

$$E\colon y^2 + xy = x^3 + x^2 + 23x - 176.$$

Working with $p = 19$ and precision 19^{60}, our algorithm has been able to recover the point:

$$P = \left(\frac{372503}{60543}, \frac{60805639}{78826986}\sqrt{413} - \frac{372503}{121086}\right) \in E\left(\mathbb{Q}(\sqrt{413})\right).$$

Acknowledgements. We are grateful to Victor Rotger for suggesting the problem, as well as to Henri Darmon, Matthew Greenberg, Matteo Longo, Robert Pollack, Eric Urban and John Voight for valuable exchanges and suggestions. We also wish to express our gratitude to the anonymous referee, whose comments encouraged us to strengthen some of the results. Guitart wants to thank the Max Planck Institute for Mathematics and the Hausdorff Research Institute for Mathematics. The work in this article was carried out while Masdeu was at Columbia University as a Ritt assistant professor.

References

1. A. ASH and G. STEVENS, 'Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues', *J. reine angew. Math.* 365 (1986) 192–220.
2. M. BERTOLINI and H. DARMON, 'The rationality of Stark–Heegner points over genus fields of real quadratic fields', *Ann. of Math.* (2) 170 (2009) 343–370.
3. W. BOSMA, J. CANNON and C. PLAYOUST, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* 24 (1997) 235–265. Computational algebra and number theory (London, 1993).
4. C. BREUIL, B. CONRAD, F. DIAMOND and R. TAYLOR, 'On the modularity of elliptic curves over **Q**: wild 3-adic exercises', *J. Amer. Math. Soc.* 14 (2001) 843–939 (electronic).
5. K. S. BROWN, *Cohomology of groups*, Graduate Texts in Mathematics 87 (Springer, New York, 1982).
6. H. DARMON, 'Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications', *Ann. of Math.* (2) 154 (2001) 589–639.
7. H. DARMON, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics 101 (Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004).

8. H. Darmon and P. Green, 'Elliptic curves and class fields of real quadratic fields: algorithms and evidence', *Experiment. Math.* 11 (2002) 37–55.
9. S. Dasgupta and M. Greenberg, '$\mathcal{L}$-invariants and Shimura curves', *Algebra Number Theory* 6 (2012) 455–485.
10. H. Darmon and R. Pollack, 'Efficient calculation of Stark–Heegner points via overconvergent modular symbols', *Israel J. Math.* 153 (2006) 319–354.
11. M. Greenberg, 'Stark–Heegner points and the cohomology of quaternionic Shimura varieties', *Duke Math. J.* 147 (2009) 541–575.
12. M. Greenberg and J. Voight, 'Computing systems of Hecke eigenvalues associated to Hilbert modular forms', *Math. Comp.* 80 (2011) 1071–1092.
13. X. Guitart and M. Masdeu, 'Elementary matrix decomposition and the computation of Darmon points with higher conductor', *Math. Comp.* (2014), to appear.
14. M. Longo, V. Rotger and S. Vigni, 'On rigid analytic uniformizations of Jacobians of Shimura curves', *Amer. J. Math.* 134 (2012) 1197–1246.
15. M. Longo, V. Rotger and S. Vigni, 'Special values of L-functions and the arithmetic of Darmon points', *J. reine angew. Math.* 684 (2013) 199–244.
16. D. Pollack and R. Pollack, 'A construction of rigid analytic cohomology classes for congruence subgroups of $\mathrm{SL}_3(\mathbb{Z})$', *Canad. J. Math.* 61 (2009) 674–690.
17. J.-P. Serre, *Trees* (Springer, Berlin, 1980), Translated from the French by John Stillwell.
18. W. A. Stein *et al.*, 'Sage Mathematics Software (Version 5.9)', The Sage Development Team, 2013, `http://www.sagemath.org`.
19. J. Voight, 'Computing fundamental domains for Fuchsian groups', *J. Théor. Nombres Bordeaux* 21 (2009) 469–491.
20. A. J. Wiles, 'Modular elliptic curves and Fermat's last theorem', *Ann. of Math.* (2) 141 (1995) 443–551.

Xavier Guitart
Institut für Experimentelle Mathematik
Ellernstr. 29
45326 Essen
Germany

xevi.guitart@gmail.com

Marc Masdeu
Mathematics Institute
University of Warwick
Coventry
CV4 7AL
United Kingdom

m.masdeu@warwick.ac.uk