Heegner points and rigid analytic modular forms

Matthew Greenberg

Department of Mathematics and Statistics
McGill University
Montréal, Québec, Canada

February 2006

Research in partial fulfillment of the requirements of the degree of
Doctor of Philosophy

Abstract

In the first part of this thesis, building on ideas of R. Pollack and G. Stevens, we present an efficient algorithm for integrating certain rigid analytic functions attached to automorphic forms on definite quaternion algebras. We then apply these methods, in conjunction with the Jacquet-Langlands correspondence and the uniformization theorem of Cerednik-Drinfeld, to the computation p-adic periods of and Heegner points on elliptic curves defined over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$ which are uniformized by Shimura curves. In part two, we give a new proof of the result, originally proved in unpublished work of Glenn Stevens [**27**], that every modular eigensymbol of non-critical slope lifts uniquely to a rigid-analytic distribution-valued eigensymbol. The proof is algorithmic and facilitates the efficient calculation of certain p-adic integrals. This has applications to the calculation of Stark-Heegner points on elliptic curves defined over $\mathbb{Q}$ as well as over certain imaginary quadratic fields.

Resumé

Dans la première partie de cette thèse, nous donnons un algorithme pour intégrer certaines fonctions rigide-analytiques attachées à une forme automorphe sur une algèbre definie de quaternions. En utilisant la correspondence de Jacquet-Langlands et le théorème de Cerednik et Drinfeld, nous appliquons cet algorithme au calcul des points de Heegner sur des courbes élliptiques définies sur $\mathbb{Q}$ et sur $\mathbb{Q}(\sqrt{5})$ qui sont parametrées par des courbes de Shimura. En deuxième lieu, nous présentons une nouvelle preuve d'un théorème de G. Stevens ([**27**], non-publié) stipulant que chaque symbole modulaire, vecteur propre pour les opérateurs de Hecke, se relève uniquement en un symbole modulaire à valeurs dans un module de distributions. Notre démontsration est algorithmique et s'applique au calcul des points de Stark-Heegner sur des courbes elliptiques définies sur $\mathbb{Q}$ ainsi que sur certains corps quadratiques imaginaires.

Acknowledgements

There are many people whom I would like to acknowledge for their support over the last years.

It is a great pleasure for me to express my gratitude to my doctoral supervisor Prof. Henri Darmon for his dedication and encouragement over the course of my program. He never failed to take time for me when I felt the need to discuss mathematics and was always generous with his ideas and insights. I came away from every meeting with him highly motivated and with renewed enthusiasm for my projects. I count returning to Montreal in January 2003 to work with him among the best decisions I've ever made.

I would also like to single out my M.Sc. advisor Prof. Eyal Goren for thanks. Not only did he teach me an incredible amount of mathematics over my years at McGill, but he was always forthcoming with valuable advice. I would like to express my appreciation for the kindness and support he extended to me throughout my time in Montreal, especially during a few rough patches.

Montreal is an wonderful place to learn number theory, owing in large part to the presence of numerous friendly graduate students and postdocs who are always up for a good mathematical (or philosophical or political or hockey-related...) discussion. I would like to thank Hugo Chapdelaine and Mak Trifkovic in particular for many enlightening, entertaining exchanges.

During my time at McGill I made a lot of good friends who are directly responsible for my stay in Montreal being as enjoyable as it was: Alice, Ben, Deidre, Charles and Mélanie, just to name a few.

There are also several Winnipeggers who deserve acknowledgement. Beginning with the mathematical, I would like to thank Profs. Grant Woods and George Grätzer of the University of Manitoba. Prof. Woods taught me my first "real" math course, his expert teaching of which was directly responsible for hooking me on the subject. I also thank him for much valuable advice over the years. I owe a great deal to Prof. Grätzer, whom I view as my mentor. It is he who introduced me to mathematical research and taught me the skills to pursue it effectively.

And of course, I would like to send a giant "Thanks!" out to my great friends from Winnipeg: Josh, Erik, Sigrid, Jason, Scott, Jason a.k.a. Jim, and Corey.

On to my family, I would like to thank my dad for his constant support, my sister Michelle for always being up for an MSN chat when I didn't feel like working, and my mom for always having a sense for when I needed a pep-talk and when I just needed to vent for fifteen minutes on the phone. I would also like to send a shout out to Nick, Vicky, Joey and Paul.

Finally, many thanks go out to my lovely girlfriend Kristina for her support, patience, tolerance, and especially for her inexplicable willingness to put up with a half-time long-distance relationship with an admitted math-freak.

Contents

Introduction

This thesis is composed of two papers whose underlying theme is the connection between Heegner points and rigid analytic modular forms.

The goal of the first paper is the development of a polynomial-time algorithm for computing Heegner points on elliptic curves over $\mathbb{Q}$, arising from certain Shimura curve parametrizations. Let E be an elliptic curve over $\mathbb{Q}$ admitting a uniformization

$$\Phi : J \to E \tag{1}$$

by the Jacobian variety J of a Shimura curve X. The Heegner points under consideration are the images under Φ of CM divisors of degree 0 on X. (See Chapter 1 for a more detailed exposition.) Due to the lack of cusps on X, or equivalently, to the fact that modular forms for groups arising from indefinite quaternion algebras to not admit q-expansions, we know of no explicit formula for the uniformization Φ in terms of classical (i.e. archimedian) analysis. This is in stark contrast to the case of parametrizations by the classical modular curves $X_0(N)$.

However, the lack of q-expansions in the Shimura curve case is in some sense compensated for by a p-adic uniformization

$$\pi : \mathfrak{H}_p \to X(\mathbb{C}_p)$$

of X, where $\mathfrak{H}_p = \mathbb{P}^1(\mathbb{C}_p) - \mathbb{P}^1(\mathbb{Q}_p)$ is the so-called *p-adic upper half plane*. The existence of this uniformization was proved (independently, using different methods) by Cerednik [**4**] and Drinfeld [**14**]. In [**1**], Bertolini and Darmon (developing work of Gross [**19**]) use Drinfeld's moduli theoretic construction of π to identify the preimages in $\mathfrak{H}_p$ of the CM points on $X(\mathbb{C}_p)$ with fixed points of the action of an algebraic torus in $\mathrm{GL}_2(\mathbb{Q}_p)$ arising from a quadratic order in a *definite* quaternion algebra; see Chapter 1, § 7. Using ideas developed independently by Iovita and Spiess, the above work is reinterpreted in [**3**] to give a formula for the Heegner points on E in terms of p-adic integration.

We are able to give an algorithm, running in polynomial time, for evaluating this p-adic integral formula. The key to this algorithm is a method devised by Pollack and Stevens [**22**] for explicitly lifting standard modular symbols to overconvergent ones; see Chapter 2,§3. We successfully adapt their method to our situation, where the role of the modular symbols is played by automorphic forms on definite quaternion algebras; see Chapter 1, § 7.

The crucial step in the algorithm of Pollack and Stevens for lifting a modular eigensymbolsymbol ψ to an overconvergent eigensymbol Ψ is the *explicit* construction of an initial lift of ψ to an overconvergent not-necessarily-eigen-symbol Ψ_0. This is a nontrivial process involving a careful analysis of the geometry of the modular curve $X_0(pN)$ which is necessary in order to ensure that certain relations (mirroring the phenomenon of certain unimodular paths on $\mathfrak{H}$ collapsing to 0 in $H_1(X_0(pN), \mathbb{Z})$) are satisfied by Ψ_0. In our Shimura curve situation, however, the automorphic forms in question are really just functions on the *finite* set of right ideal classes of a certain quaternion order.

Consequently, the difficulties arising in producing an initial lift do not arise for us. More conceptually, ideas of Gross [**19**] lead to the identification of the above mentioned set of right ideal classes with the set of connected components of a certain conic, i.e. with an H_0. Therefore, there are no nontrivial coboundary relations to be satisfied.

When coding and testing our algorithm, we realized that it was not necessary to compute the initial lift Ψ_0 at all. This led us to examine the work of Pollack and Stevens more closely to determine whether this involved computation could be dispensed with in the modular symbol situation as well. (Our interest in such a possibility was mainly due to potential applications to the calculation of Stark-Heegner points – see below.)

We realized that the necessity of computing the initial lift Ψ_0 as Pollack and Stevens did was an artifact of their initial purpose in designing their method – the investigation of the p-adic L-function(s) associated to a modular form of critical slope at p, i.e. a modular eigenform $f \in S_{k+2}(\Gamma_0(pN))$ such that the $\mathrm{ord}_p\, a_p(f) = k+1$, where $f|U_p = a_p(f)f$. For our applications of interest, however, the modular forms f which arise all have weight 2 and satisfy $a_p(f) = \pm 1$.

In the second paper, we give an algorithm for lifting a modular symbol Ψ, of arbitrary weight and non-critical slope, to a rigid analytic (and therefore overconvergent) modular symbol Ψ which does not necessitate the construction of an initial lift Ψ_0. This algorithm is based on a new proof of the result, originally due to Stevens [**27**], that a modular symbol of noncritical slope lifts uniquely to a rigid analytic modular symbol.

As mentioned above, our motivation for pursuing the work of this second paper was to facilite of the computation of algebraic points on elliptic curves, in particular, *Stark-Heegner points*. These points, first constructed by Darmon in [**6**], are local points on elliptic curves which are conjecturally defined over global class fields of *real* quadratic fields. Otherwise, though, they are believed to behave like classical Heegner points. In [**10**], Darmon and Pollack give an efficient algorithm, based on [**22**], for computing Stark-Heegner points, thereby presenting convincing evidence for the conjectures of [**7**]. The results of our second paper serve to simplify the approach of [**10**], both technically and conceptually.

Moreover, since the method described in Chapter 2 is "geometry free", it to generalizes to situations where the geometry involved is more complicated. In [**28**], Trifković has adapted these ideas to work with modular symbols constructed from certain automorphic forms on GL_2 of an imaginary quadratic field F, and has implemented his generalization in PARI to compute certain Stark-Heegner points on elliptic curves defined over F. In his situation, the automorphic forms in question manifest themselves geometrically as harmonic forms on certain real-analytic threefolds. As the geometry of these threefolds is quite complicated compared to that of modular curves, our "geometry free" method proves quite helpful.

This thesis is organized as follows. Chapter 1 contains the text of the first, with several complements following as appendices. The second paper is presented in Chapter 2. Chapter 3 consists of a discussion of the results of the first two chapters and raises several natural questions for further investigation.

CHAPTER 1

Heegner point computations via numerical p-adic integration

1. Heegner points on elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Then by the work of Wiles and his school, there exists a dominant morphism defined over $\mathbb{Q}$,

$$\Phi_N : X_0(N) \to E,$$

arising from the modularity of E. Let $A \to A'$ be an isogeny of elliptic curves with complex multiplication (henceforth, CM) by the same imaginary quadratic order $\mathfrak{o} \subset K$. Then by the classical theory of complex multiplication, the point $P = (A \to A')$ represents an element of $X_0(N)(H_\mathfrak{o})$, where $H_\mathfrak{o}$ is the ring class field attached to the order $\mathfrak{o}$. As Φ_N is defined over $\mathbb{Q}$, the point $\Phi_N(P)$ belongs to $E(H_\mathfrak{o})$. Such a point on E is called a *(classical) Heegner point*. These points are of significant interest. In particular, the proof of the conjecture of Birch and Swinnerton-Dyer for elliptic curves over $\mathbb{Q}$ of analytic rank at most one (due to Gross-Zagier and Kolyvagin) depends essentially on their properties.

These classical Heegner points may be efficiently computed in practice. Let $f_E \in S_2(N)$ be the normalized newform attached to E and let $\tau \in \mathfrak{H}$ represent the point P, where $\mathfrak{H}$ is the complex upper

half plane. Then

$$\Phi_N(P) = W\left(\int_\infty^\tau f_E(z)dz\right) = W\left(\sum_{n\geq 1}\frac{a_n(f_E)}{n}e^{2\pi i n\tau}\right) \tag{2}$$

where

- $W : \mathbb{C} \to \mathbb{C}/\Lambda \cong E(\mathbb{C})$ is the Weierstrass uniformization of $E(\mathbb{C})$, and
- $a_n(f_E)$ is the n-th Fourier coefficient of f_E.

The quantities $a_p(E)$ may be computed by counting points on E modulo p. The existence of a point $P = (A \to A')$ on $X_0(N)$ where both A and A' have CM by an order in K implies the validity of the *classical Heegner hypothesis*: that all primes ℓ dividing N are split in K. Due to the theoretical importance of classical Heegner points, it is natural to desire an analogous systematic construction of algebraic points defined over class fields of imaginary quadratic fields which do not necessarily satisfy this stringent hypothesis, as well as methods to effectively compute these points in practice. Such a generalization requires admitting uniformizations of E by certain *Shimura curves*.

Assume that N is squarefree and $N = N^+N^-$ is factorization of N such that N^- has an even number of prime factors. Let C be the indefinite quaternion $\mathbb{Q}$-algebra ramified precisely at the primes dividing N^- and let S be an Eichler $\mathbb{Z}$-order in C of level N^+. (For basic definitions and terminology concerning quaternion algebras, see **[31]**.) Fix in identification ι_∞ of $C \otimes \mathbb{R}$ with $M_2(\mathbb{R})$ and let Γ_{N^+,N^-} denote the image under ι_∞ of the group of units in S of reduced norm 1. Then Γ_{N^+,N^-} acts discontinuously on $\mathfrak{H}$ with compact quotient $X_{N^+,N^-}(\mathbb{C})$.

By Shimura's theory **[24]**, the Riemann surface $X_{N^+,N^-}(\mathbb{C})$ has a canonical model X_{N^+,N^-} over $\mathbb{Q}$. This is proved by interpreting X_{N^+,N^-} as a moduli space for certain abelian surfaces. Consequently, there is a natural notion of a "CM-point" on X_{N^+,N^-}. Let $\mathfrak{H}(\mathfrak{o}) \subset \mathfrak{H}$ be those points whose images on X_{N^+,N^-} have CM by $\mathfrak{o}$. Then $\mathfrak{H}(\mathfrak{o})$ is Γ_{N^+,N^-}-stable and the quotient $\mathrm{CM}(\mathfrak{o}) := \Gamma_{N^+,N^-}\backslash\mathfrak{H}(\mathfrak{o})$ is a finite subset of $X_{N^+,N^-}(H_{\mathfrak{o}})$. The set $\mathrm{CM}(\mathfrak{o})$ is nonempty if and only if all rational primes ℓ dividing N^+ (resp. N^-) are split (resp. inert) in the fraction field K of $\mathfrak{o}$. We dub this condition the *Shimura-Heegner hypothesis*.

Let J_{N^+,N^-} denote the Jacobian variety of X_{N^+,N^-}. By the modularity theorem for elliptic curves over $\mathbb{Q}$ together with the Jacquet-Langlands correspondence, there exists a dominant morphism

$$\Phi_{N^+,N^-} : J_{N^+,N^-} \longrightarrow E \tag{3}$$

defined over $\mathbb{Q}$. (See **[7**, Ch. 4] for a discussion of this point.) The uniformization, Φ_{N^+,N^-} maps the set $\mathrm{CM}(\mathfrak{o})$ into $E(H_{\mathfrak{o}})$. To emphasize their origin, we shall refer to such points on E as *Shimura-Heegner points*.

Shimura formulated a reciprocity law which gives an alternate description of the Galois action on Shimura-Heegner points. Suppose that K satisfies the Shimura-Heegner hypothesis. He showed that there is a natural free action of $\mathrm{Pic}\,\mathfrak{o}$ on $\mathrm{CM}(\mathfrak{o})$ with $2^{\omega(N)}$ orbits ($\omega(N) =$ number of prime factors of N) such that for

$$P' - P \in \mathrm{Div}^0\,\mathrm{CM}(\mathfrak{o}) \subset \mathrm{Div}^0\,X_{N^+,N^-}(H_{\mathfrak{o}}),$$

we have

$$\Phi_{N^+,N^-}((P'-P)^{[\mathfrak{a}]}) = \Phi_{N^+,N^-}(P'-P)^{(\mathfrak{a},H_{\mathfrak{o}}/K)}, \tag{4}$$

where $(-, H_{\mathfrak{o}}/K) : \operatorname{Pic} \mathfrak{o} \to \operatorname{Gal} H_{\mathfrak{o}}/K$ is the reciprocity map of class field theory.

The phenomenon of Shimura curves uniformizing elliptic curves generalizes to certain elliptic curves defined over totally real fields. For simplicity, let $F/\mathbb{Q}$ be a real quadratic field with infinite places σ_1 and σ_2 and let $\mathfrak{p}$ be a finite prime of F. Let C be the quaternion F-algebra ramified at $\mathfrak{p}$ and σ_1 and let S be a maximal order of C. Fix an isomorphism $\iota_{\sigma_2} : C \otimes_{\sigma_2} \mathbb{R} \to M_2(\mathbb{R})$ and let Γ be the image under ι_{σ_2} of the group of units in S with reduced norm 1. Then as above, the quotient $\Gamma \backslash \mathfrak{H}$ is a compact Riemann surface which admits a description as the complex points of a Shimura curve X, as well as a corresponding CM theory.

Let $f \in S_2(\mathfrak{p})$ be a Hilbert modular form. Then the Jacquet-Langlands correspondence together with the appropriate analog of the Eichler-Shimura construction asserts the existence of an elliptic curve E/F of conductor $\mathfrak{p}$ and a uniformization $J \to E$, where J is the Jacobian of X, such that the L-functions of E and f match. The images of CM divisors on X in E, also called Shimura-Heegner points, satisfy a reciprocity law analogous to (4). Zhang [**32**], generalizing the work of Gross-Zagier, has derived formulas relating heights of these Shimura-Heegner points to special values of derivatives of L-functions.

Unfortunately, since modular forms on non-split quaternion algebras do not admit q-expansions, there is no known explicit formula for the map (3) analogous to (2) which may be exploited to compute these important Shimura-Heegner points in practice. Our goal in this work is to describe and implement a p-adic analytic algorithm for performing such computations. The existence of a general

algorithm for performing such Heegner point computations using only classical (i.e. archimedian) analysis remains an open problem, although some progress has been made by N. Elkies [**15**].

This paper is organized as follows: In §§2-5 we introduce p-adic automorphic forms on definite quaternion algebras and adapt ideas of Pollack and Stevens to develop an algorithm for lifting such forms to rigid analytic automorphic ones (see §4 for definitions). In §§6-7, we discuss (following [**1**]) how one may use the Cerednik-Drinfeld theorem on p-adic uniformization of Shimura curves to give a p-adic integral formula for the Shimura-Heegner points introduced above. In §8 we show that the lifting algorithm of §5 may be exploited to evaluate this formula efficiently and to high precision. For simplicity, we will develop the above mentioned theory in the situation where the base field is $\mathbb{Q}$, although an analogous theory exists for totally real base fields. We have implemented these methods in Magma to compute Shimura-Heegner points on

(1) elliptic curves defined over $\mathbb{Q}$ with conductor $2p$, where p is an odd prime,
(2) elliptic curves defined over $\mathbb{Q}(\sqrt{5})$ with degree one prime conductor.

Sample computations are given in §9.

This work owes much to the ideas of Pollack and Stevens, and the author wishes to thank them for providing him with a draft of [**22**]. This paper is part of the author's PhD thesis [**18**], written at McGill University under the supervision of Prof. Henri Darmon, whom the author would like to gratefully acknowledge for his expert guidance, advice, and encouragement.

2. p-adic integration

Let p be a prime, let T be a complete subring of $\mathbb{C}_p$ and let X be a compact, totally disconnected topological space.

DEFINITION 1. A *T-valued distribution on X* is a finitely additive T-valued function on the compact-open subsets of X. If the values of a distribution are p-adically bounded, then we call it a *measure*.

Let $\mathbf{D}(X,T)$ denote the set of T-valued measures on X and let $\mathbf{D}_0(X,T)$ denote the subspace of measures μ of total measure zero. If μ is in $\mathbf{D}(X,T)$ and $f : X \to T$ is locally constant, the symbol $\int_X f(x)d\mu(x)$ can be defined in the obvious way. To ease notation, we will sometimes write $\mu(f)$ instead. If μ is a measure, then we may extend μ to a linear functional on the space $\mathcal{C}(X,T)$ of continuous T-valued functions on X. (For details, see [**17**, §1.2].)

Suppose now that the distribution μ on X takes actually values in $\mathbb{Z}$ (implying, in particular, that μ is a measure). If $f = \sum_i a_i \mathbf{1}_{E_i}$ is a locally constant function on X, we may define the *multiplicative integral* of f against μ by the formula

$$\int\!\!\!\!\!\!\times_X f(x)d\mu(x) = \prod_i a_i^{\mu(E_i)}.$$

By the boundedness of μ, the multiplicative integral extends to a group homomorphism from $\mathcal{C}(X,T^*)$ into the group of units T^* of T.

Let $\mathfrak{H}_p = \mathbb{P}^1(\mathbb{C}_p) - \mathbb{P}^1(\mathbb{Q}_p)$ be the *p-adic upper half-plane*, let μ be a $\mathbb{C}_p$-valued measure on $\mathbb{P}^1(\mathbb{Q}_p)$ and choose points $\tau, \tau' \in \mathfrak{H}_p$. We define a *$p$-adic line integral* by the formula

$$\int_\tau^{\tau'} \omega_\mu = \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{x-\tau'}{x-\tau}\right) d\mu(x), \tag{5}$$

where "$\log$" denote the branch of the p-adic logarithm satistying $\log p = 0$. If μ takes values in $\mathbb{Z}$, we may define a multiplicative analog of (5) above by posing

$$\text{(6)} \qquad \qquad \oint_{\tau}^{\tau'} \omega_\mu = \oint_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{x-\tau'}{x-\tau} \right) d\mu(x).$$

Noting the relation

$$\int_{\tau}^{\tau'} \omega_\mu = \log \oint_{\tau}^{\tau'} \omega_\mu,$$

we see that (6) is actually a refinement of (5) as we avoid the choice of a branch of the p-adic logarithm. For motivation behind the formalism of p-adic line integration, see [**7**, Ch. 6].

3. Rigid analytic distributions

In this section, we consider p-adic integration over $\mathbb{Z}_p$. The problem of computing an integral of the form

$$\text{(7)} \qquad \qquad \int_{\mathbb{Z}_p} v(x) d\mu(x)$$

to an accuracy of p^{-M} is of exponential complexity, where the size of the problem is defined to be M (cf. [**9**]). Fortunately, many of the functions $v(x)$ which arise in practice are of a special type. Let

$$\text{(8)} \qquad \mathbf{A}_{\text{rig}} = \Big\{ v(x) = \sum_{n \geq 0} a_n x^n : a_n \in \mathbb{Q}_p, \quad a_n \to 0 \text{ as } n \to \infty \Big\}.$$

Elements of $\mathbf{A}_{\text{rig}}$ are rigid analytic functions on the closed unit disk in $\mathbb{C}_p$ which are defined over $\mathbb{Q}_p$.

DEFINITION 2. Let $\mathbf{D}_{\text{rig}}$ be the continuous dual of $\mathbf{A}$. Elements of $\mathbf{D}_{\text{rig}}$ are called *rigid analytic distributions*.

Let $\mu \in \mathbf{D}_{\text{rig}}$. Then by the continuity of μ, the problem of computing (7) for $v \in \mathbf{A}_{\text{rig}}$ is reduced to the calculation of the moments

$$\mu(x^n) = \int_{\mathbb{Z}_p} x^n d\mu(x), \quad n \geq 0.$$

A polynomial time algorithm for calculating such moments was recently discovered by R. Pollack and G. Stevens [**22**] in the situation where the measure μ is that attached to a cuspidal eigenform form on $\Gamma_0(N)$ as in [**20**]. Although the main goal of their theory was the study of normalized eigenforms g of weight $k+2$ satisfying $\operatorname{ord}_p a_p(g) = k+1$ (a so-called critical slope eigenform) and their p-adic L-functions, we are interested case $\operatorname{ord}_p a_p(g) = 0$, the so-called ordinary case. The main objects of study in [**22**] are modular symbols. We will develop analogs of their results where the role of the modular symbols are played by automorphic forms on definite quaternion algebras (see §4).

Let $\mathbf{D}^\circ_{\text{rig}}$ be the subset of $\mathbf{D}_{\text{rig}}$ consisting of those distributions with moments in $\mathbb{Z}_p$. The space $\mathbf{D}^\circ_{\text{rig}}$ admits a useful filtration, first introduced by Pollack and Stevens in [**22**]. Define

$$F^0\mathbf{D}_{\text{rig}} = \mathbf{D}^\circ_{\text{rig}},$$
$$F^N\mathbf{D}^\circ_{\text{rig}} = \{\mu \in \mathbf{D}^\circ_{\text{rig}} : \mu(x^j) \in p^{N-j}\mathbb{Z}_p, \quad j = 0, \ldots, N-1\}, \quad N \geq 1.$$

Now let

$$A^N\mathbf{D}^\circ_{\text{rig}} = \mathbf{D}^\circ_{\text{rig}}/F^N\mathbf{D}^\circ_{\text{rig}}, \quad N \geq 1.$$

We call $A^N\mathbf{D}^\circ_{\text{rig}}$ the N-th approximation to the module $\mathbf{D}^\circ_{\text{rig}}$, following the terminology of [**22**].

4. Automorphic forms on definite quaternion algebras

Let N, N^+, and N^- be as in § 1 and assume the existence of a prime p dividing N^-. Let B be the definite quaternion algebra ramified precisely at the infinite place of $\mathbb{Q}$ together with the primes dividing N^-/p, and let R be an Eichler $\mathbb{Z}$-order in B of level pN^+. Fix an identification ι_p of $B_p := B \otimes \mathbb{Q}_p$ with $M_2(\mathbb{Q}_p)$ under which $R_p := R \otimes \mathbb{Z}_p$ corresponds to

$$M_0(p\mathbb{Z}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_p) : c \equiv 0 \pmod{p} \right\}. \tag{9}$$

Let $\hat{\mathbb{Q}}$ be the finite adèles of $\mathbb{Q}$ and let $\hat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$ be the profinite completion of $\mathbb{Z}$. Let $\hat{B} = B \otimes_{\mathbb{Q}} \hat{\mathbb{Q}}$ and $\hat{R} = R \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$ be the adelizations of B and R, respectively.

Define the semigroup

$$\Sigma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_p) : p \mid c,\, d \in \mathbb{Z}_p^*, \text{ and } ad - bc \neq 0 \right\}.$$

Let A be a left $\Sigma_0(p)$-module.

DEFINITION 3. An automorphic form on B of level R taking values in A is a map $f : B^* \backslash \hat{B}^* \to A$ such that $u_p f(zbu) = f(b)$ for all $u \in \hat{R}^*$ and $z \in \hat{\mathbb{Q}}^*$, where u_p denotes the p-component of u.

We denote the set of such automorphic forms by $\mathcal{S}(B, R; A)$.

The double coset space $B^* \backslash \hat{B}^* / \hat{R}^*$ is in bijection with the set of right ideal classes of the order R, which is finite of cardinality h, say. Writing

$$\hat{B}^* = \coprod_{k=1}^{h} B^* b_i \hat{R}^*, \tag{10}$$

we see that an automorphic form $f \in \mathcal{S}(B, R; A)$ is completely determined by the finite sequence $(f(b_1), \ldots, f(b_h))$.

View B_p as a subring of $\hat{B}$ via the natural inclusion j_p. By the *strong approximation theorem*, $\hat{B}^* = B^* B_p^* \hat{R}^*$, so j_p induces a bijection

$$R[1/p]^* \backslash B_p / R_p^* \to B^* \backslash \hat{B}^* / \hat{R}^*.$$

Letting $\mathcal{S}(B_p, R_p; A)$ be the collection of functions $\varphi : R[1/p]^* \backslash B_p \to A$ such that $u\varphi(zbu) = f(b)$ for all $u \in R_p^*$ and $z \in \mathbb{Q}_p^*$, it is easy to see that j_p induces an isomorphism of $\mathcal{S}(B, R; A)$ with $\mathcal{S}(B_p, R_p; A)$. Since it shall be easier for us to work locally at p rather that adelically, we will work mostly with $\mathcal{S}(B_p, R_p; A)$.

The group $\mathcal{S}(B_p, R_p; A)$ is endowed with the action of a Hecke operator U_p given by

$$(U_p\varphi)(b) = \sum_{a=0}^{p-1} (\begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix} \varphi)(b) = \sum_{a=0}^{p-1} \varphi(b \begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix}). \tag{11}$$

When the action of $\Sigma_0(p)$ is trivial, an Atkin-Lehner involution W_p also acts on $\mathcal{S}(B_p, R_p; A)$ by the rule

$$W_p\varphi(b) = \sum_{a=0}^{p-1} \varphi(b \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}).$$

Other Hecke operators T_ℓ for $\ell \nmid N$ may also be defined using standard adelic formluas (see **[19]**, for instance).

Automorphic forms whose coefficient module is equipped with the trivial $\Sigma_0(p)$-action "are" measures on $\mathbb{P}^1(\mathbb{Q}_p)$: Let $\mathcal{B}$ be the set of balls in $\mathbb{P}^1(\mathbb{Q}_p)$, on which $\mathrm{GL}_2(\mathbb{Q}_p)$ acts transitively from the left inducing an identification of $\mathrm{GL}_2(\mathbb{Q}_p)/\Gamma_0(p\mathbb{Z}_p)\mathbb{Q}_p^*$ with $\mathcal{B}$. Therefore, a form $\varphi \in \mathcal{S}(B_p, R_p; \mathbb{C}_p)$ may be viewed as a $R[1/p]^*$-invariant function on the balls in $\mathbb{P}^1(\mathbb{Q}_p)$. With this interpretation, the value of

$U_p\varphi$ on a ball $\mathbf{b}$ is the sum of the values $\varphi(\mathbf{b}^{(i)})$ where the balls $\mathbf{b}^{(i)}$, $i = 1, \dots, p$, form the standard subdivision of the ball $\mathbf{b}$. The value of $W_p\varphi$ on $\mathbf{b}$ is simply the value of φ on its complement $\mathbb{P}^1(\mathbb{Q}_p) - \mathbf{b}$. Suppose that $U_p\varphi = -W_p\varphi = a_p = \pm 1$. Define a function μ_φ on $\mathcal{B}$ by

$$\mu_\varphi(\gamma\mathbb{Z}_p) = \text{sign}_p\gamma \cdot \varphi(\gamma), \quad \gamma \in B_p^*$$

where

$$\text{sign}_p\gamma = a_p^{\text{ord}_p \det\gamma}. \tag{12}$$

Then μ_φ is a $\mathcal{G}$-invariant measure on $\mathbb{P}^1(\mathbb{Q}_p)$ of total measure zero, where $\mathcal{G} := \ker(\text{sign}_p : R[1/p]^* \to \{\pm 1\})$. Note that if $a_p = 1$, then $\mu_\varphi = \varphi$ and $\mathcal{G} = R[1/p]^*$.

The left action of $\Sigma_0(p)$ on $\mathbb{P}^1(\mathbb{Q}_p)$ induces a right action of $\Sigma_0(p)$ on $\mathbf{A}_{\text{rig}}$. The space $\mathbf{D}_{\text{rig}}$ inherits a left action of $\Sigma_0(p)$ by duality. The spaces $\mathbf{D}^\circ_{\text{rig}}$ and $F^N\mathbf{D}^\circ_{\text{rig}}$, $N \geq 1$ are all easily seen to be $\Sigma_0(p)$-stable. Therefore, the approximation modules $A^N\mathbf{D}_{\text{rig}}$ inherit a $\Sigma_0(p)$-action. Consequently, these modules are all valid coefficient groups for p-adic automorphic forms. We shall refer to elements of $\mathcal{S}(B_p, R_p; \mathbf{D}_{\text{rig}})$ as *rigid analytic automorphic forms*.

5. Lifting U_p-eigenforms

5.1. Existence and uniqueness of lifts. Define the *specialization map*

$$\rho : \mathcal{S}(B_p, R_p; \mathbf{D}_{\text{rig}}) \to \mathcal{S}(B_p, R_p; \mathbb{Q}_p)$$

by the rule $\rho(\Phi)(b) = \Phi(b)(\mathbf{1}_{\mathbb{Z}_p})$. It is easily verified that ρ is $U_\mathfrak{p}$-equivariant. Let $\varphi \in \mathcal{S}(B_p, R_p; \mathbb{Q}_p)$ be a U_p-eigenform with eigenvalue $a_p = \pm 1$ and let μ_φ be the associated measure on $\mathbb{P}^1(\mathbb{Q}_p)$ as constructed in §4. The following proposition should be viewed as an

analog of the containment of classical modular forms in the space of p-adic modular forms.

PROPOSITION 4. *The form φ lifts canonically with respect to ρ to a U_p-eigenform Φ satisfying $\Phi(1) = \mu_\varphi$.*

PROOF. Define $\Psi : B_{\mathfrak{p}} \to \mathbf{D}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Q}_p)$ by $\Psi(b) = (\mathrm{sign}_p b) b^{-1}\varphi$ where $\mathrm{sign}_p b$ is as defined in (12), and let $\Phi : B_p^* \to \mathbf{D}_{\mathrm{rig}}$ be given by $\Phi(b) = \Psi(b)|_{\mathbb{Z}_p}$. The conclusions of the proposition are now easily verified. □

The next proposition forms the basis of our algorithm.

PROPOSITION 5. *Let Ψ belong to $\ker\rho \cap \mathcal{S}(B_p, R_p; F^N\mathbf{D}^\circ_{rig})$. Then*

$$U_p\Psi \in \ker\rho \cap \mathcal{S}(B_p, R_p; F^{N+1}\mathbf{D}^\circ_{rig}).$$

PROOF. By the U_p-equivariance of ρ, its kernel is certainly U_p-stable. For $1 \le n \le N$, we have

$$\begin{aligned} U_p\Psi(b)(x^n) &= \sum_{a=0}^{p-1} \begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix} \Psi\left(b \begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix}\right)(x^n) \\ &= \sum_{a=0}^{p-1} \Psi\left(b \begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix}\right)((px+a)^n) \\ &= \sum_{k=0}^{n}\sum_{a=0}^{p-1} \binom{n}{k} p^k a^{n-k} \Psi\left(b \begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix}\right)(x^k). \end{aligned}$$

Note that the $k = 0$ term in the above sum vanishes as $\Psi \in \ker\rho$. If $1 \le k \le n$ and $0 \le a \le p-1$, then

$$\binom{n}{k} p^k a^{n-k} \Psi\left(b \begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix}\right)(x^k) \in p^k p^{N-k}\mathbb{Z}_p = p^N\mathbb{Z}_p \subset p^{N+1-n}\mathbb{Z}_p.$$

The result follows. □

Let $\Phi \in \mathcal{S}(B_p, R_p; \mathbf{D}_{\text{rig}})$ be the lift of φ constructed in Proposition 4. Since the double-coset space $R[1/p]^* \backslash B_p / R_p$ is finite, we may assume without loss of generality that all moments involved are actually in $\mathbb{Z}_p$ (just multiply φ, Φ, and Φ_0 by an suitably chosen scalar $c \in \mathbb{Q}_p$). Let Φ^N be the natural image of Φ in $\mathcal{S}(B_p, R_p; A^N \mathbf{D}^\circ_{\text{rig}})$.

COROLLARY 6.

(1) (a) *Φ^N is the unique U_p-eigenform in $\mathcal{S}(B_p, R_p; A^N \mathbf{D}^\circ_{rig})$ lifting φ.*

(b) *If Φ_0^N is any element of $\mathcal{S}(B_p, R_p; A^N \mathbf{D}^\circ_{rig})$ lifting φ, then*

$$(a_p U_p)^N \Phi_0^N = \Phi.$$

(2) (a) *Φ is the unique U_p-eigenform in $\mathcal{S}(B_p, R_p; \mathbf{D}_{rig})$ satisfying $\rho(\Phi) = \varphi$.*

(b) *If Φ_0 is any element of $\mathcal{S}(B_p, R_p; \mathbf{D}_{rig})$ satisfying $\rho(\Phi_0) = \varphi$, then the sequence $\{(a_p U_p)^n \Phi_0\}$ converges to Φ.*

PROOF. Statement (2) follows from statement (1) and the relation

$$\mathcal{S}(B_p, R_p; \mathbf{D}_{\text{rig}}) = \Big(\varprojlim_N \mathcal{S}(B_p, R_p; A^N \mathbf{D}^\circ_{\text{rig}}) \Big) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

By the above proposition, we have

$$(a_p U_p)^N (\Phi - \Phi_0) \in \mathcal{S}(B_p, R_p; F^N \mathbf{D}^\circ_{\text{rig}}).$$

Statement (1) now follows easily. □

The unicity result 2(a) of the corollary may viewed as an analog of the assertion that ordinary p-adic modular eigenforms are classical.

By Corollary 6, in order to approximate the moments of $\Phi(b)$ for $b \in B_p^*$, it suffices to produce an initial approximation Φ_0 to Φ and then to apply the U_p-operator repeatedly until the desired

accuracy is achieved. Such an initial approximation may be constructed explicitly as follows: Using the decomposition (10), let $S_k = R_p^* \cap b_k^{-1} R[1/p]^* b_k$, which is finite as it is contained in $b_k^{-1} R^* b_k$ (the group of units of a $\mathbb{Z}$-order in a definite quaternion algebra over $\mathbb{Q}$ is finite). For $z \in \mathbb{Z}_p$, let $\delta_z \in \mathbf{D}_{\text{rig}}$ is the Dirac distribution centered at z, i.e. $\delta_z(f) = f(z)$.

PROPOSITION 7. *There is a unique element Φ_0 of $\mathcal{S}(B_p, R_p; \mathbf{D}_{rig})$ satisfying*

$$\Phi_0(b_k) = \frac{\varphi(b_k)}{\#S_k} \sum_{v \in S_k} v^{-1} \delta_0, \quad 1 \le k \le h. \tag{13}$$

Its moments are given by

$$\Phi(b_k)(x^n) = \frac{\varphi(b_k)}{\#S_k} \sum_{v \in S_k} z_v^n, \quad \textit{where} \quad z_v = v \cdot 0.$$

(By $v \cdot 0$ we mean the image of v in $\mathrm{GL}_2(\mathbb{Q}_p)$ acting as a fractional linear transformation on $0 \in \mathbb{P}^1(\mathbb{Q}_p)$.)

PROOF. To see that the formula (13) gives a well defined element of $\mathcal{S}(B_p, R_p; \mathbf{D}_{\text{rig}})$, notice that if $\gamma b_k u = b_k$, then v varies over S_k if and only if vu does. The uniqueness is clear. □

5.2. Computing the lifts in practice. We now turn to the problem of computing Φ^N in practice. Representing an element of the space $\mathcal{S}(B_p, R_p; A^N \mathbf{D}_{\text{rig}}^\circ)$ is straight-forward. First observe that the correspondence

$$\mu \mapsto \left(\mu(x^0) \pmod{p^N}, \mu(x^1) \pmod{p^{N-1}}, \ldots, \mu(x^{N-1}) \pmod{p}\right)$$

for $\mu \in \mathbf{D}_{\text{rig}}^\circ$ descends to an isomorphism

$$A^N \mathbf{D}_{\text{rig}} \cong \mathbb{Z}/p^N\mathbb{Z} \times \mathbb{Z}/p^{N-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}.$$

Therefore, an element of $A^N\mathbf{D}^\circ_{\text{rig}}$ may be stored simply as an N-tuple of integers.

The $\Sigma_0(p)$-action on $A^N\mathbf{D}^\circ_{\text{rig}}$ may be computed as follows: Let $\mu \in \mathbf{D}_{\text{rig}}$ and let ν be any lift of μ to $\mathbf{D}^\circ_{\text{rig}}$. For any $u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Sigma_0$ and $n \geq 0$, the rational function $(\frac{ax+b}{cx+d})^n$ may be expanded in a Taylor series $\sum \alpha_m x^m$, and the moments of $u\nu$ may be computed by "integrating term by term":

$$(u\nu)(x^n) = \nu\Big(\Big(\frac{ax+b}{cx+d}\Big)^n\Big) = \sum_{m\geq 0} \alpha_m \nu(x^m).$$

Moreover, by the stability of $F^N\mathbf{D}^\circ_{\text{rig}}$ under $\Sigma_0(p)$, the image of $u\nu$ is $u\mu$. Therefore, the N-tuple representing $u\mu$ may be computed from that representing μ.

Recall the double-coset decomposition (10). Then since an automorphic form $\Psi \in \mathcal{S}(B_p, R_p; A^N\mathbf{D}^\circ_{\text{rig}})$ is completely determined by $\Psi(b_1), \ldots, \Psi(b_h)$, it may be stored simply as a sequence of h N-tuples of integers. Assuming knowledge of the values of φ, the moments of the initial lift Φ_0^N of φ constructed explicitly in Proposition 7 may be computed and thus Φ_0^N may be stored as a sequence of N-tuples as described above.

It remains to describe how to obtain, for a form Ψ as above, the data

$$((U_p\Psi)(b_k)(x^0) \ \big(\mathrm{mod}\, p^N\big), \ldots, (U_p\Psi)(b_k)(x^{N-1}) \ (\mathrm{mod}\, p)\big), \quad 1 \leq k \leq h$$

from the corresponding data for Ψ. For $1 \leq k \leq h$ and $0 \leq a \leq p-1$, find elements $\gamma(k,a) \in R[1/p]^*$, $u(k,a) \in R_p^*$, and $j(k,a) \in \{0, \ldots, p-1\}$ such that

$$b_k \begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix} = \gamma(k,a) b_{j(k,a)} u(k,a), \tag{14}$$

and let $\xi(k,a) = \left(\begin{smallmatrix} p & a \\ 0 & 1 \end{smallmatrix}\right) u(k,a)^{-1}$. Then $U_p\Psi$ is given by the formula

$$(U_p\Psi)(b_k) = \sum_{a=0}^{p-1} \xi(k,a)\Psi(b_{j(k,a)}). \tag{15}$$

The measures $\Psi(b_{j(k,a)})$ are assumed to be known and the action of the $\xi(k,a)$ on them may be computed as described above. Thus, an algorithm for computing Φ^N from φ may proceed as follows:

(1) Compute the elements $\gamma(k,a)$, $j(k,a)$, and $u(k,a)$ as in (14).
(2) Compute an initial lift Φ_0^N of φ to $\mathcal{S}(B_p, R_p; A^N\mathbf{D}^\circ_{\mathrm{rig}})$ as in Proposition 7.
(3) Compute $(a_pU_p)^N\Phi_0^N$. By Corollary 6, the result is Φ^N.

6. p-adic uniformization

Let $\Gamma^{(p)}_{N^+,N^-}$ denote the image under ι_p of the elements of $R[1/p]$ of reduced norm 1. The group $\Gamma^{(p)}_{N^+,N^-}$ acts discontinuously on $\mathfrak{H}_p$ and the quotient $\Gamma^{(p)}_{N^+,N^-}\backslash\mathfrak{H}_p$, has the structure of a rigid analytic curve $X^{(p)}_{N^+,N^-}$. The following result, due to Cerednik and Drinfeld, connects this rigid variety with the Shimura curves introduced in § 1.

THEOREM 8 (**[4, 14]**). *There is a canonical rigid analytic isomorphism*

$$\mathrm{CD} : X^{(p)}_{N^+,N^-}(\mathbb{C}_p) \to X_{N^+,N^-}(\mathbb{C}_p).$$

Let Ω denote the global sections of the sheaf of rigid analytic differential 1-forms on $X^{(p)}_{N^+,N^-}$.

PROPOSITION 9. *The spaces Ω and $\mathcal{S}(B_p, R_p; \mathbb{C}_p)$ are naturally isomorphic as Hecke-modules.*

(A p-adic residue map and Teitelbaum's p-adic Poisson integral give the mutually inverse isomorphisms proving the theorem. For details, see [7, Ch. 5].) This proposition, together with the Jacquet-Langlands correspondence as invoked in §1, give the following corollary:

COROLLARY 10. *Choosing an isomorphism of $\mathbb{C}$ with $\mathbb{C}_p$, there is an isomorphism of Hecke-modules*

$$S_2(\Gamma_0(N))^{\textit{new-}N^-} \cong \mathcal{S}(B_p, R_p; \mathbb{C}_p).$$

REMARK 11. This result was originally proved by Eichler using his trace formula.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and f_E the associated newform. Then by Corollary 10, there is a corresponding form $\varphi_E \in \mathcal{S}(B_p, R_p; \mathbb{C}_p)$ with the same Hecke-eigenvalues as f_E. In fact, we may (and do) assume that φ takes values in $\mathbb{Z}$. Let $\mu_E = \mu_{\varphi_E}$ be the associated measure on $\mathbb{P}^1(\mathbb{Q}_p)$ as constructed in §4.

Consider the map $\Psi : \mathrm{Div}^0 \mathfrak{H}_p \to \mathbb{C}_p$ given by

$$\Psi(\tau' - \tau) = \int_\tau^{\tau'} \omega_{\mu_E}.$$

Let Tate : $\mathbb{C}_p^* \to E(\mathbb{C}_p)$ be the Tate parametrization of E and recall the map Φ_{N^+,N^-} of (3). Assume that E is the strong Weil curve for (3) at the cost of replacing it by an isogenous curve.

PROPOSITION 12. *The following diagram is commutative:*

$$\begin{array}{ccc} \mathrm{Div}^0 \mathfrak{H}_p & \xrightarrow{\Psi} & \mathbb{C}_p^* \\ {\scriptstyle \mathrm{CD}}\downarrow & & \downarrow{\scriptstyle \textit{Tate}} \\ J_{N^+,N^-}(\mathbb{C}_p) & \xrightarrow[\Phi_{N^+,N^-}]{} & E(\mathbb{C}_p) \end{array}$$

For a discussion of this result, see [**1**].

7. A p-adic integral formula for Heegner points

Let K be an imaginary quadratic field satisfying the Shimura-Heegner hypothesis and $\mathfrak{o}$ be an order in K of conductor prime to N. Let us call an embedding ψ of $\mathfrak{o}[1/p]$ into $R[1/p]$ *optimal* if it does not extend to an embedding of a larger $\mathbb{Z}[1/p]$-order of K. Denote by $\mathcal{E}_p(\mathfrak{o})$ the set of all such. The Shimura-Heegner hypothesis guarantees that $\mathcal{E}_p(\mathfrak{o})$ is nonempty. For each $\psi \in \mathcal{E}_p(\mathfrak{o})$, the order $\mathfrak{o}[1/p]$ acts on $\mathfrak{H}_p$ via the composite $\iota_p \circ \psi$ with a unique fixed point $\tau_\psi \in \mathfrak{H}_p$ satisfying

$$\alpha \begin{pmatrix} \tau_\psi \\ 1 \end{pmatrix} = \psi(\alpha) \begin{pmatrix} \tau_\psi \\ 1 \end{pmatrix}$$

for all $\alpha \in \mathfrak{o}[1/p]$. Let $\mathfrak{H}_p(\mathfrak{o})$ be the set of all such τ_ψ, and let $\mathrm{CM}_p(\mathfrak{o})$ be its image in $X^{(p)}_{N^+,N^-}$. The set $\mathrm{CM}_p(\mathfrak{o})$ is endowed with a natural action of $\mathrm{Pic}\,\mathfrak{o} = \mathrm{Pic}\,\mathfrak{o}[1/p]$ (see **[19]**). The sets $\mathrm{CM}(\mathfrak{o})$ and $\mathrm{CM}_p(\mathfrak{o})$ are related through Theorem 8:

THEOREM 13 (**[1**, Proposition 4.15]). *The map* CD *restricts to a* $\mathrm{Pic}\,\mathfrak{o}$*-equivariant bijection from* $\mathrm{CM}_p(\mathfrak{o})$ *onto* $\mathrm{CM}(\mathfrak{o})$.

Combining this theorem with Proposition 12, we see that module of Shimura-Heegner points on E defined over the ring class field attached to $\mathfrak{o}$ is generated by points of the form $\mathrm{Tate}(J(\tau,\tau'))$, $\tau,\tau' \in \mathfrak{H}_p(\mathfrak{o})$, where

$$J(\tau,\tau') = \int\!\!\!\!\!\!\diagup_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{x-\tau'}{x-\tau}\right) d\mu_E(x) \tag{16}$$

8. Computing the integrals

Let Φ_E be the eigenlift to $\mathcal{S}(B_p, R_p; \mathbf{D}_{\mathrm{rig}})$ of the $\mathbb{C}_p$-valued automorphic form φ_E attached to E, as in §6. The computation of the

integral (16) to precision p^{-M} may be reduced to that of a certain approximation $\Phi_E^{M''} \in \mathcal{S}(B_p, R_p; A^N \mathbf{D}^\circ_{\mathrm{rig}})$ to Φ_E.

It is easy to see that the points of $\mathfrak{H}_p(\mathfrak{o})$ actually lie in the subset $\mathbb{P}^1(\mathbb{Q}_{p^2}) - \mathbb{P}^1(\mathbb{Q}_p)$ of $\mathfrak{H}_p$, where $\mathbb{Q}_{p^2}$ is the quadratic unramified extension of $\mathbb{Q}_p$. Let $\mathfrak{H}_p^0$ be the set of elements τ in $\mathfrak{H}_p$ whose image under the natural reduction map $\mathbb{P}^1(\mathbb{C}_p) \to \mathbb{P}^1(\bar{\mathbb{F}}_p)$ does not belong to $\mathbb{P}^1(\mathbb{F}_p)$. We assume, without loss of generality, that:

(1) τ and τ' reduce to elements of $\mathfrak{H}_p^0$.
(2) there exists an element $i \in R[1/p]$ such that $i^2 = -1$.

By assumption 2., we may choose the isomorphism ι_p in such a way that $\iota_p(i) = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. (Instead of assuming the existence of such an i, one could work with the two measures μ_E and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\mu_E$, and thus no generality is lost.)

By the first assumption, $J(\tau, \tau')$ lies in $\mathbb{Z}_{p^2}^*$ and its Teichmüller representative is the same as that of

$$\prod_{a=0}^{p-1} \Big(\frac{a-\tau'}{a-\tau}\Big)^{\mu_E(a+p\mathbb{Z}_p)},$$

an easily computed quantity (actually, we need only compute it modulo p). Therefore, it suffices to compute $\log J(\tau, \tau')$.

Write

$$\log J(\tau, \tau') = \sum_{a \in \mathbb{P}^1(\mathbb{F}_p)} \log J_a(\tau, \tau'), \quad \text{where}$$
$$J_a(\tau, \tau') = \oint_{\mathbf{b}_a} \frac{x-\tau}{x-\tau'} d\mu_E(x),$$

and $\mathbf{b}_a$ is the standard residue disk around a. Let

$$J_\infty(\tau) = \fint_{\mathbf{b}_0} (1+\tau x) d\mu_E(x),$$
$$J_a(\tau) = \fint_{\mathbf{b}_a} (x-\tau) d\mu_E(x), \quad 0 \le a \le p-1.$$

Then for each $a \in \mathbb{P}^1(\mathbb{F}_p)$, we have

$$J_a(\tau, \tau') = J_a(\tau')/J(\tau).$$

(To prove the above for $a = \infty$, we use assumption 2.)

Straightforward manipulations (see [**10**, §1.3]) show that the expansions

$$\log J_\infty(\tau) = \sum_{n \ge 1} \frac{(-1)^n}{n} \tau^n \omega(0,n), \tag{17}$$

$$\log J_a(\tau) = \sum_{n \ge 1} \frac{1}{n(a-\tau)^n} \omega(a,n), \quad 0 \le a \le p-1 \tag{18}$$

are valid, where (following the notation of [**10**]),

$$\omega(a,n) = \int_{\mathbf{b}_a} (x-a)^n d\mu_E(x), \quad 0 \le a \le p-1.$$

Let

$$M' = \max\{n : \mathrm{ord}_p(p^n/n) < M\}, \quad M'' = M + \left\lfloor \frac{\log M'}{\log p} \right\rfloor. \tag{19}$$

An examination of formulas (17) and (18) shows that they may be computed to a precision of p^{-M} given the data

$$\omega(a,n) \pmod{p^{M''}}, \quad 0 \le a \le p-1, \quad 0 \le n \le M'. \tag{20}$$

PROPOSITION 14. *Let $\Psi \in \mathcal{S}(B_p, R_p; \mathbf{D}_{rig})$ be a U_p-eigenform with eigenvalue $a_p = \pm 1$. Then we have the formula*

$$\int_{a+p\mathbb{Z}_p} (x-a)^n d\Psi(b)(x) = a_p p^n \int_{\mathbb{Z}_p} x^n d\Psi(b \begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix})(x).$$

holds for $1 \leq a \leq p-1$. *Consequently, the data (20) may be extracted from* $\Phi_E^{M''}$.

PROOF.

$$\int_{a+p\mathbb{Z}_p} (x-a)^n d\Psi(b)(x) =$$

$$= (a_p U_p \Psi)(b)((x-a)^n \mathbf{1}_{a+p\mathbb{Z}_p}(x))$$

$$= a_p \sum_{d=0}^{p-1} \Psi\left(b\begin{pmatrix} p & d \\ 0 & 1 \end{pmatrix}\right)((d+px-a)^n \mathbf{1}_{a+p\mathbb{Z}_p}(d+px)$$

$$= a_p p^n \Psi\left(b\begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix}\right)(x^n)$$

$$= a_p p^n \int_{\mathbb{Z}_p} x^n d\Psi\left(b\begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix}\right),$$

as desired.

To prove the second statement, take $\Psi = \Phi_E$ and $b = 1$. By the definition of $\Phi_E^{M''}$,

$$\Phi_E\left(\begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix}\right)(x^n) \pmod{p^{M''-n}} = \Phi_E^{M''}\left(\begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix}\right)(x^n)$$

for $0 \leq a \leq p-1$ and $0 \leq n \leq M''$. Now multiply the above by p^n and apply the first statement of the proposition, noting that $M'' \geq M'$. □

9. Examples

EXAMPLE 15. Consider the elliptic curve

$$E: \ y^2 + xy + y = x^3 + x^2 - 70x - 279 \qquad (38B2),$$

and set $N^+ = 2$, $N^- = p = 19$. Then B is algebra of rational Hamilton quaternions. The field $K = \mathbb{Q}(\xi)$, where $\xi = (1+\sqrt{-195})/2$, satisfies

the Shimura-Heegner hypothesis. Let $\mathfrak{o} = \mathbb{Z}[\xi]$ be its maximal order. The class number of K is 4 and $\operatorname{Pic}\mathfrak{o} \cong (\mathbb{Z}/2\mathbb{Z})^2$. In fact, the Hilbert class field H of K is $K(\sqrt{-3}, \sqrt{5})$. Therefore, $\operatorname{Pic}\mathfrak{o}$ has three characters χ_1, χ_2, χ_3 of exact order 2, corresponding to the three quadratic subfields $K(\sqrt{-15})$, $K(\sqrt{5})$, and $K(\sqrt{65})$ of H. Let $\tau \in \mathfrak{H}_p(\mathfrak{o})$ be a base point and define divisors

$$\mathfrak{d}_i = \sum_{\alpha \in \operatorname{Pic}\mathfrak{o}} \chi_i(\alpha)\tau^\alpha \in \operatorname{Div}^0 \mathfrak{H}_p(\mathfrak{o}), \quad i = 1, 2, 3.$$

Define a divisor $\mathfrak{d}_0$ (corresponding to the trivial character) by

$$\mathfrak{d}_0 = \sum_{\alpha \in \operatorname{Pic}\mathfrak{o}} ((3 + 1 - T_3)\tau)^\alpha$$

where T_3 is the standard Hecke operator. Let

$$P_i = \mathsf{Tate}\Big(\int_{\mathfrak{d}_i} \omega_{\mu_E} \Big), \quad , i = 0, 1, 2, 3.$$

be the corresponding Heegner points. We computed the points P_i as described above and these points were recognized as

$$P_0 = (-4610/39, 1/1521(-277799\xi + 228034)),$$

$$P_1 = (25/12, -94/9u + 265/72),$$

$$P_2 = (10, -11v),$$

$$P_3 = (1928695/2548, 1/463736(-2397574904w + 1023044339)),$$

$$\text{where} \quad u = \frac{1 + \sqrt{-15}}{2} \quad v = \frac{1 + \sqrt{5}}{2}, \quad w = \frac{1 + \sqrt{65}}{2}.$$

EXAMPLE 16. Let $\omega = (1 + \sqrt{5})/2$ and let $F = \mathbb{Q}(\omega)$. Consider the elliptic curve

$$E: \ y^2 + xy + \omega y = x^3 - (\omega + 1)x^2 - (30\omega + 45)x - (11\omega + 117)$$

defined over F. The conductor of E is $3-5\omega$, a degree one prime of F dividing 31. Here, $N = N^- = \mathfrak{p}$, $N^+ = 1$, and B is the base change to F of the $\mathbb{Q}$-algebra of Hamilton's quaternions. Let $\xi = \sqrt{2\omega - 15}$. Then $K = F(\xi)$ is a CM field satisfying the Shimura-Heegner hypothesis in this context. The class group of K is cyclic of order 8 and thus has a unique character χ of exact order 2 whose kernel has fixed field $K(\sqrt{2-13\omega})$. Let $\tau \in \mathfrak{H}_p(\mathfrak{o})$ be a base point, define a divisor $\mathfrak{d}_\chi$ attached to χ as in Example 15, and let P_χ be the corresponding Heegner point. Then our computations, performed to an accuracy of 31^{-60}, yielded a point recognizable as the point $(x, y) \in E(F(\sqrt{2-13\omega}))$, where

$$\begin{aligned} x = {} & 1/501689727224078580 \times (-204893297129553021 81\omega + \\ & 1590697243182535465) \\ y = {} & 1/7945803389515397981338566 00 \times \\ & (-24307562136394751979713438023\omega - \\ & 52244062542753980406680036861)\sqrt{-13\omega+2} + \\ & 1/1003794544481571 60 \times (19987639985731223601\omega \\ & - 1590697243182535465). \end{aligned}$$

Appendix A. Remarks on the computations

A.1. Two special cases. In this section we discuss the implementation of the above methods on a computer. We have written code to compute p-adic periods of and Heegner points on elliptic curves E in the following two cases:

(1) E is defined over $\mathbb{Q}$ and has conductor $N = 2p$, where p is an odd prime.

(2) E is an elliptic curve over $F = \mathbb{Q}(\sqrt{5})$ with prime conductor.

As we shall see below, the consideration of these particular cases allows for certain simplifications which prove extremely convenient for the implementation. In addition, we feel these cases serve to illustrate effectively the utility and scope of the theory presented above. In what follows, we draw freely from the notation of previous sections

In Case 1, we consider the factorization $N^- = 2, N^+ = p$. Thus, the quaternion algebra B which comes into play is the algebra of Hamilton's quaternions. We insist our Eichler $\mathbb{Z}$-order $R \subset B$ of level p to be contained in the maximal order

$$S = \Big\langle 1, i, j, \frac{1+i+j+k}{2} \Big\rangle,$$

the so-called "Hurwitz integral quaternions". Further, we choose our isomorphism $\iota_p : B_p \to M_2(\mathbb{Q}_p)$ in such a way that $\iota_p(S_p) = M_2(\mathbb{Z}_p)$ and $\iota_p(R_p) = M_0(p\mathbb{Z}_p)$.

In Case 2, let $\mathfrak{p}$ denote the conductor of E. For simplicity, assume that $\mathfrak{p}$ has degree one, so that the completion $F_\mathfrak{p}$ is just $\mathbb{Q}_p$, where p is the absolute norm of $\mathfrak{p}$. Here, we choose B to be the quaternion F-algebra ramified at the two infinite places of F. Since 2 is inert if F, it follows that B is simply the base change of the $\mathbb{Q}$-algebra of Hamilton's quaternions to F. We consider the maximal $\mathfrak{o}_F$-order S in B with basis

$$e_1 = (1 - \omega i + \bar{\omega} j)/2 \qquad e_2 = (-\omega i + j + \bar{\omega} k)/2$$
$$e_1 = (\bar{\omega} i - \omega j + k)/2 \qquad e_2 = (i + \bar{\omega} j - \omega k)/2,$$

where $\omega = (1+\sqrt{5})/2$, and choose R to be an Eichler $\mathfrak{o}_F$-order contained in S of level $\mathfrak{p}$. As above, we choose our isomorphism $\iota_{\mathfrak{p}} : B_{\mathfrak{p}} \to M_2(\mathbb{Q}_p)$ in so that $\iota_{\mathfrak{p}}(S_{\mathfrak{p}}) = M_2(\mathbb{Z}_p)$ and $\iota_{\mathfrak{p}}(R_{\mathfrak{p}}) = M_0(p\mathbb{Z}_p)$.

It will be extremely useful for us that in both cases considered above, the maximal quaternion order S has class number one, i.e. there is a single equivalence class of left or right S-ideals in B.

Since, in both cases, much of the computation takes place in $\mathbb{Q}_p$ (thanks to our assumption that $\mathfrak{p}$ is of degree one), the details of the implementation are quite similar for the two cases. Therefore, in what follows, we will describe the highlights of the implementation in Case 1, remarking appropriately when features of the implementation of Case 2 differ.

A.2. Enumeration of quaternions of a given norm. The computation of the measure attached to an elliptic curve, the Hecke-action, and the action of $\mathrm{Pic}\,\mathfrak{o}$ (Shimura reciprocity) all reduce to the problem of enumerating elements of a given norm in the maximal order S.

We first consider Case 1. The problem of enumerating elements of S of norm n is just the problem of representing an integer as a sum of four squares, or equivalently, of finding vectors of length n in the standard 4-dimensional lattice. Efficient methods for enumerating such vectors, based of the LLL-algorithm, are included with the standard Magma distribution.

Case 2 is more complicated. If $\lambda \in S$, then we may write

$$\lambda = (x_1 + y_1\omega)e_1 + (x_2 + y_2\omega)e_2 + (x_3 + y_3\omega)e_3 + (x_4 + y_4\omega)e_4,$$

where $x_i, y_i \in \mathbb{Z}$. One computes that

$$\operatorname{Norm}\lambda = \sum_{i=1}^{4}(x_i^2 + y_i^2) + \omega \sum_{i=1}^{4}(y_i^2 + 2x_i y_i) =: f(x,y) + \omega g(x,y).$$

Note that the quadratic form $f(x,y)$ is positive definite. To solve $\operatorname{Norm}\alpha = u + v\omega$, we continue generating new solutions of $f(x,y) = u$ using the above mentioned techniques (but in an 8-dimensional lattice), each time testing whether $g(x,y) = v$ holds. This method is likely far from optimal, but serves well enough for our purposes.

A.2.1. *Computing the Hecke-action.* Because of its central role in our algorithm, we discuss in detail the computation of the action of the U_p-operator on automorphich forms on B. In §5.2, we showed that in order to compute the U_p-action, it suffices to determine the data (14). As the double-coset space $S[1/p]^*\backslash B_p^*/S_p^*$ parametrizes left ideal classes of S, it follows that

$$B_p^* = S[1/p]^* S_p^*.$$

Therefore, choosing $b_k \in B_p^*$ such that

$$\iota_p(b_k) = \begin{pmatrix} k & -1 \\ 1 & 0 \end{pmatrix}, \quad 0 \le k \le p, \qquad \iota_p(b_p) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

we have

$$B_p = S[1/p]^* S_p^* = \coprod_{i=0}^{p} R[1/p]^* b_k R_p^*.$$

Let

$$\varpi_a = \begin{pmatrix} p & a \\ 0 & 1 \end{pmatrix}, \quad 0 \le k \le p-1, \qquad \varpi_p \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}.$$

For k and a between 0 and p, let $j(k,a)$ be such that

$$R[1/p]^* b_{j(k,a)} R_p^* = R[1/p]^* b_k \varpi_a R_p.$$

Then there exist $\gamma(k,a) \in R[1/p]^*$ and $u(k,a) \in R_p^*$ such that $b_k \varpi_a = \gamma(k,a) b_{j(k,a)} u(k,a)$. Solving for $\gamma(k,a)$, we have

$$\gamma(k,a) = b_k \varpi_a u(k,a)^{-1} b_{j(k,a)}^{-1},$$

implying that $\gamma(a,k) \in R[1/p] \cap R_p = R$ and that $\det \gamma(a,k) = \pm p$. Since B is definite, there are only finitely many elements in R of norm p. Therefore, by enumerating these, the elements $\gamma(k,a) \in R$ and the indices $j(k,a)$ may be determined in practice. This is how we computed the data (14) in our Magma implementation.

A.2.2. *Computing the action of* $\mathrm{Pic}\,\mathfrak{o}$. Let $K = \mathbb{Q}(\xi)$ be an imaginary quadratic field such that the pair (E,K) satisfies the Shimura-Heegner hypothesis with respect to the factorization $N^- = 2, N^+ = p$. Let $\mathfrak{o}$ be the maximal order of K. Let f be an optimal embedding of $\mathfrak{o}[1/p]$ into $R[1/p] = S[1/p]$. Note that f is completely determined by the image of ξ, and thus is easily represented on a computer.

Let $\alpha_1, \ldots, \alpha_h$ be a list of generators of $\mathrm{Pic}\,\mathfrak{o}$. Find ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ of norms $n_1, \ldots, n_h$ (the smaller the better) generating the respective ideal classes. Since S has class number one, the ideals $Sf(\alpha_i)$ are all principal. Therefore, there exist quaternions $\lambda_1, \ldots, \lambda_h \in S$ of norms $n_1 \ldots, n_h$ such that

$$Sf(\mathfrak{a}_i) = S\lambda_i, \quad 1 \leq i \leq h.$$

Such elements may be found using the above enumeration techniques. The optimal embedding $\alpha_i * f$ is given by $\lambda_i f \lambda_i^{-1}$ (cf. **[19]**).

Appendix B. p-adic periods of Shimura curves

Let μ be the $\mathbb{Z}$-valued measure on $\mathbb{P}^1(\mathbb{Q}_p)$ attached to E. The measure μ is invariant under the group

$$\Gamma = \begin{cases} \{\iota_p(\lambda) : \lambda \in R[1/p]^*, \ \ \mathrm{ord}_p \,\mathrm{Norm}\,\lambda \text{ is even}\}. & a_p = -1, \\ \iota_p(R[1/p]), & a_p = 1. \end{cases}$$

Let $\tau \in \mathfrak{H}_p$. By the theory outlined in §6, the group of p-adic periods

$$\Lambda_\mu = \left\{ \not\int_\tau^{\gamma\tau} \omega_\mu : \gamma \in \Gamma \right\} \subset \mathbb{C}_p^*$$

has the form $q^{\mathbb{Z}} \times T$, where T is a finite (cyclic) subgroup of $\mathbb{C}_p$ and $|q| < 1$.

Since S has class number one, it is easy to find generators for the group $\Gamma = \Gamma^{(p)}_{N^+,N^-/p}$:

$$\Gamma = \begin{cases} \langle p, \{i_p(\varpi_1/\varpi_2) : \varpi_i \in S, \quad \mathrm{Norm}\,\varpi_i = p\}\rangle, & a_p = -1 \\ \langle \{\varpi : \varpi \in S, \quad \mathrm{Norm}\,\varpi = p\}\rangle, & a_p = 1. \end{cases}$$

Therefore,

$$\Lambda_\mu = \begin{cases} \left\langle \not\int_\tau^{\varpi_1\tau} \omega_\mu \Big/ \not\int_\tau^{\varpi_2\tau} \omega_\mu : \varpi_i \in S, \quad \mathrm{Norm}\,\varpi_i = p \right\rangle, & a_p = -1, \\ \left\langle \not\int_\tau^{\varpi\tau} \omega_\mu : \varpi \in S, \quad \mathrm{Norm}\,\varpi = p \right\rangle & a_p = 1. \end{cases}$$

In either case, it is clear that an enumeration of the elements in R of norm p should facilitate the calculation of Λ_μ via p-adic integration.

For each $P \in \mathbb{P}^1(\mathbb{Q}_{p^2})$ and $n \geq 0$, let $\mathrm{red}_n P$ be the natural image of P in $\mathbb{P}^1(\mathbb{Z}_{p^2}/p^{n+1}\mathbb{Z}_{p^2})$. Inductively define the sets

$$\mathfrak{H}_p^0 = \{P \in \mathbb{P}^1(\mathbb{Q}_{p^2}) : \mathrm{red}_0 P \notin \mathbb{P}^1(\mathbb{Z}_p/p\mathbb{Z}_p)\},$$

$$\mathfrak{H}_p^n = \{P \in \mathbb{P}^1(\mathbb{Q}_{p^2}) : \mathrm{red}_n P \notin \mathbb{P}^1(\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p)\} - \mathfrak{H}_p^{n-1}, \quad n \geq 1.$$

It is clear that $\mathfrak{H}_p = \bigcup_{n\geq 0} \mathfrak{H}_p^n$.

LEMMA 17. *Let $\tau \in \mathfrak{H}_p^0$ and let $\gamma \in M_2(\mathbb{Q}_p)$ such that $\operatorname{ord}_p \det \gamma = 1$. Then $\gamma\tau \in \mathfrak{H}_p^1$.*

PROOF. Write $\mathbb{Q}_{p^2} = \mathbb{Q}_p(\xi)$ where $\xi^2 \in \mathbb{Q}_p$, write $\tau = u + v\xi$, and let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then

$$\gamma\tau = \frac{acN(\tau) + (ad+bc)u}{N(c\tau+d)} + \frac{(ad-bc)v}{N(c\tau+d)}\xi, \tag{21}$$

where N denotes the norm from $\mathbb{Q}_{p^2}$ to $\mathbb{Q}_p$. We now note that $c\tau+d$ is divisible by p if and only c and d both are. In this case $\operatorname{ord}_p N(c\tau+d)$ is exactly 2 and the valuation of the coefficient of ξ in (21) is -1. If neither c nor d is divisible by p, then the valuation of this coefficient is $+1$. The lemma follows easily from these observations. □

By the above lemma, the theory of §8 does not suffice for the computation of p-adic periods, since assumption (1) of that section can no longer be valid (although we continue to assume, without loss of generality, that assumption (2) is). This can be remedied, however, by considering moments of measures over certain balls of radius p^{-2}. For $0 \le a, b \le p-1$, let

$$\mathbf{b}_{a,b} = \{x \in \mathbb{Q}_p : |x - (a+bp)| \le p^{-2}\}, \quad \mathbf{b}_{\infty,b} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mathbf{b}_{0,b}$$

be the standard partition of $\mathbb{P}^1(\mathbb{Q}_p)$ into p^2+p balls of radius p^{-2}. Suppose that τ is in $\mathfrak{H}_p^0$ and that τ' is in $\mathfrak{H}_p^1$. We generalize the analysis of §8, drawing freely from the notation of that section. The evaluation of the integrals $J_a(\tau)$ remains unchanged. In evaluating $J_\infty(\tau')$, we have two cases to consider:

Case 1: $|\tau'| \le 1$. In this case, $J_\infty(\tau') \in 1 + p^2\mathbb{Z}_p$. Therefore, $J_\infty(\tau') = \exp\log J(\tau')$. Expanding in a Taylor series, convergent as $x \in p\mathbb{Z}_p$

and $\tau' \in \mathbb{Z}_{p^2}$, we see that

$$\log J_\infty(\tau') = \sum_{n\geq 1} \frac{(-1)^n}{n} \tau'^n \int_{\mathbf{b}_0} x^n d\mu(x). \tag{22}$$

Case 2: $|\tau'| > 1$. In this case, we have $|\tau'| = p$ and

$$J_\infty(\tau') = \omega \prod_{b\in\mathbb{P}^1(\mathbb{F}_p)} J_{\infty,b}(\tau')$$

where

$$\omega = \prod_{b\in\mathbb{P}^1(\mathbb{F}_p)} (1+bp\tau')^{\mu(\mathbf{b}_{0,b})} \quad \text{and}$$

$$J_{\infty,b}(\tau') = \oint_{\mathbf{b}_{0,b}} \Big(1 + \frac{(x-bp)\tau'}{1+bp\tau'}\Big) d\mu(x).$$

Notice that $1 + bp\tau' \in \mathbb{Z}_{p^2}^*$ for all b and that $(x-bp)\tau' \in p\mathbb{Z}_{p^2}$ for all $x \in \mathbf{b}_{0,b}$ and all b. Therefore, we have $J_{\infty,b}(\tau') = \exp\log J_\infty(\tau')$. Expanding $\log J_\infty(\tau')$ in a Taylor series, we have

$$\log J_\infty(\tau') = \sum_{n\geq 1} \frac{(-1)^n}{n} \Big(\frac{\tau'}{1+bp\tau'}\Big)^n \int_{\mathbf{b}_{0,b}} (x-bp)^n d\mu(x). \tag{23}$$

We now turn to the evaluation of the terms $J_a(\tau')$ for $0 \leq a \leq p-1$.

Again, we consider two cases:

Case 1: $|\tau' - a| \geq 1$. In this case,

$$J_a(\tau') = (a-\tau')^{\mu(\mathbf{b}_a)} \oint_{\mathbf{b}_a} \Big(1 - \frac{x-a}{\tau'-a}\Big) d\mu(x).$$

Observing that $|\tau' - a| \geq 1$, it follows that the above multiplicative integral is simply the p-adic exponential of the logarithmic series

$$\sum_{n\geq 1} \frac{1}{n(a-\tau')^n} \int_{\mathbf{b}_a} (x-a)^n d\mu(x). \tag{24}$$

Case 2: $|\tau' - a| < 1$. In this case, $\tau' \in \mathfrak{H}_p^1$ and $|\tau' - a| = p^{-1}$. Write

$$J_a(\tau') = \omega \cdot \prod_{b \in \mathbb{P}^1(\mathbb{F}_p)} J_{a,b}(\tau'),$$

where

$$\omega = \prod_{b \in \mathbb{P}^1(\mathbb{F}_p)} ((a+bp) - \tau')^{\mu(\mathbf{b}_{a,b})} \quad \text{and}$$

$$J_{a,b}(\tau') = \int\!\!\!\!\!\!\diagup_{\mathbf{b}_{a,b}} \Big(1 - \frac{x - (a+bp)}{\tau' - (a+bp)}\Big) d\mu(x).$$

Noticing that the integrand in the expression for $J_{a,b}(\tau')$ is in $1 + p^2\mathbb{Z}_{p^2}$, for all $x \in \mathbf{b}_{a,b}$, if follows as above that $J_{a,b}(\tau')$ is the p-adic exponential of the series

$$\log J_{a,b}(\tau) = \sum_{n \geq 1} \frac{1}{n(\tau' - (a+bp))^n} \int_{\mathbf{b}_{a,b}} (x - (a+bp))^n d\mu(x). \tag{25}$$

We introduce the notation

$$\omega(c, p^{-\nu}; n) = \int_{c + p^\nu \mathbb{Z}_p} (x - c)^n d\mu(x) \tag{26}$$

for the various moments of the measure μ, generalizing that introduced in §8.

To compute (22) and (24) to an accuracy of p^{-M}, it suffices to compute

$$\omega(a, p^{-1}; n) \pmod{p^{M''}}, \quad 0 \leq a \leq p-1, \quad 0 \leq n \leq M',$$

where M' and M'' are as in (19).

Turning to (23), we see that

$$\log J_\infty(\tau') \equiv \sum_{n=1}^{M'} \frac{(-1)^n}{n} \Big(\frac{\tau'}{1 + bp\tau'}\Big)^n \mathrm{mom}_\mu(bp, p^{-2}; n) \pmod{p^M},$$

where M' is as above. This time though, to evaluate the n-th summand to an accuracy of p^{-M}, we must compute

$$\omega(bp, p^{-2}; n) \pmod{p^{M+n+\mathrm{ord}_p\, n}}.$$

Therefore, it certainly suffices to compute each of the above moments to an accuracy of $p^{-M'''}$ where

$$M''' = M + M' + \left\lfloor \frac{\log M'}{\log p} \right\rfloor = M + M''.$$

Observe $M'' \approx M$ and $M''' \approx 2M''$ when M is large. Therefore, it is enough (and convenient) to evaluate the data

$$\omega(bp, p^{-\nu}; n) \pmod{p^{2M''}}$$
$$n = 0, \ldots, 2M'', \quad b = 0, \ldots, p^\nu - 1.$$

The analysis of (25) is analogous.

EXAMPLE 18. There are two isogeny classes of elliptic curves over $\mathbb{Q}$ of conductor $2 \cdot 19 = 38$, namely $38A$ and $38B$. Let μ_A and μ_B be the corresponding $\mathbb{Z}$-valued measures on $\mathbb{P}^1(\mathbb{Q}_p)$. Using the p-adic integration techniques outlined above, we compute that the lattices $\Lambda_A = \Lambda_{\mu_A}$ and $\Lambda_B = \Lambda_{\mu_B}$ are generated by periods q_A and q_B, respectively, where

$$q_A \equiv 19 \cdot 264507652379 \pmod{19^{10}},$$
$$q_B \equiv 19^5 \cdot 1545123 \pmod{19^{10}}.$$

Modulo 19^{10}, the periods q_A and q_B are congruent to the Tate periods of the elliptic curves

$$E_A : y^2 + xy + y = x^3 - 86x - 2456 \qquad (38A3)$$
$$E_B : y^2 + xy + y = x^3 + x^2 - 70x - 279 \qquad (38B2).$$

This suggests the rigid analytic isomorphisms

$$E_A(\mathbb{C}_p) \cong \mathbb{C}_p^*/\Lambda_A, \quad E_B(\mathbb{C}_p) \cong \mathbb{C}_p^*/\Lambda_B,$$

and that we should attempt to locate Heegner points on the representatives E_A and E_B of the two isogeny classes of elliptic curves over $\mathbb{Q}$ of conductor 38. It is interesting to note that these are *not* strong Weil curves for $X_0(38)$.

EXAMPLE 19. Let $F = \mathbb{Q}(\omega)$, where $\omega = (1+\sqrt{5})/2$. According to the tables compiled by Dembélé **[12]**, there is a unique Hilbert modular newform f on $\Gamma_0(3-5\omega)$, where $3-5\omega$ is a degree one prime lying over 31. It has the property that $a_{3-5\omega} = -1$. The approximate period computed from the measure attached to the system of Hecke-eigenvalues of f is given by

$$q = 31^8 \cdot 747626750421999505 \pmod{31^{20}}$$

this agrees with the Tate period of the elliptic curve

$$E_{3+5\omega}: \; y^2 + xy + \omega y = x^3 - (\omega+1)x^2 - (30\omega+45)x - (11\omega+117)$$

of Example 16. In the next section, we present a sampling of the Heegner points on this curve.

Appendix C. Tables

In this section, we further demonstrate the utility of our algorithm by presenting more examples of Shimura-Heegner points defined over class fields of imaginary quadratic fields.

Recall the curve E_B of conductor 38 of the previous section. Let K be an imaginary quadratic field such that the pair (E_B, K) satisfies the Shimura-Heegner hypothesis with respect to the factorization $N^- = 2$, $N^+ = 38$, and let $\mathcal{G}_K$ be its genus field, of degree 2^n

over K, say. As in §9, we compute points corresponding to the $2^n - 1$ characters of Cl_K of exact order 2, as well as a point P_0 corresponding to the trivial character. Sometimes, the point $P_0 = \mathrm{Tate}(J_0)$ was of very large height and inconvenient to recognize as an algebraic point. We noted empirically, however, that P_0 is often divisible by factors of $5 = 3 + 1 - a_3$. Thus, if we were unsuccessful in recognizing the point P_0, we attempted to recognize the points

$$Q_{i,j} = \mathrm{Tate}(\zeta_5^i q^{j/5} J_0^{1/5}), \quad 0 \le i, j \le 4$$

where ζ_5 is a primitive 5-th root of units and q is the tate period of E_B. This approach was often successful. We computed these points for imaginary quadratic fields K of even class number and discriminant $D_K \le 500$. The results are displayed below in Table 1. For each field K, the first point listed is that corresponding to the trivial character (such points obtained by "dividing by 5" as above are denoted "$5 \times Q_{i,j}$" in the table).

In Table 2, we display the results of similar computations for the curve $E_{3-5\omega}$ of the previous section. We compute points for CM extensions K of F of the form $F(\sqrt{\varpi})$, where ϖ is a prime element of F of norm ≤ 200. Again, the first point listed in each row is that corresponding to the trivial character.

Table 1: Heegner points on 38B2

$D_K = -35$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{5})$
$(30/7, 1/98(-361\sqrt{-35} - 259))$
$(10, 1/2(-11\sqrt{5} - 11))$
$D_K = -115$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{5})$
$(-895/92, 1/4232(-7942\sqrt{-115} + 18469))$
$(10, 1/2(-11\sqrt{5} - 11))$
$D_K = -123$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{41})$
$(10/243, 1/13122(-19855\sqrt{-123} - 6831))$
$(55/41/8(-50\sqrt{41} - 59))$
$D_K = -187$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{-11})$
$5 \times (-330860/1377, 1/421362(-114395485\sqrt{-187} + 50410899))$
$(-20/9, 1/54(-185\sqrt{-11} + 33))$
$D_K = -195$, $\mathrm{Cl}_K = (\mathbb{Z}/2\mathbb{Z})^2$, $\mathcal{G}_K = K(\sqrt{-15}, \sqrt{5})$
$5 \times (-4610/39, 1/3042(-277799\sqrt{-195} + 178269))$
$(25/12, 1/72(-376\sqrt{-15} - 111))$
$(10, 1/2(-11\sqrt{5} - 11))$
$(1928695/2548, 1/463736(-1198787452\sqrt{65} - 175743113))$
$D_K = -235$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{5})$
$(904/235, 1/110450(-156313\sqrt{-235} - 267665))$
$(52424/605, 1/66550(-24063139\sqrt{5} - 2916595))$
$D_K = -267$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{89})$
$(-410/867, 1/88434(-84835\sqrt{-267} - 23307))$
$(52595/4356, 1/287496(-875080\sqrt{89} - 1879383))$

$D_K = -291$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{97})$

$(2/3, 1/18(-19\sqrt{-291} - 15))$

$(8196823/864900, 1/804357000(-417006106\sqrt{97} - 4213701195))$

$D_K = -339$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{113})$

$(-479/108, 1/1944(-608\sqrt{-339} + 3339))$

$(1774281903006895/39181665744676,$
$1/2452586554521087835 76(-6997901820985564777310\sqrt{113}$
$-5675711179326623107673))$

$D_K = -403$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{-31})$

$5 \times (-617060/122317, 1/308483474(-76393015\sqrt{-403} + 623870923))$

$(-12395/784, 1/21952(-209345\sqrt{-31} + 162554))$

$D_K = -427$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{61})$

$(-33589240/5632263, 1/70729958754$
$5 \times (-19338241135\sqrt{-427} + 175541858583))$

$(280/9, 1/54(-1175\sqrt{61} - 867))$

$D_K = -435$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{145}, \sqrt{-15})$

$(-170/87, 1/15138(-8759\sqrt{-435} + 7221))$

$(4118255/301716, 1/892475928(-2916529916\sqrt{145} - 6537137109))$

$(25/12, 1/72(-376\sqrt{-15} - 111))$

$(36063677855/2150547876,$
$1/99729507201624(-2684620739812946\sqrt{5} - 886073252024697))$

Table 2: Heegner points on $E_{a\omega+b}$

$K = F(\sqrt{-\omega-5})$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{-1})$ $2 \times (1/1892721080644(-54585933978772\omega - 44949443766637),$ $1/650983434837237682(-659831876643213681 79\omega -$ $43925206151868340008)\sqrt{-\omega-5} + 1/3785442161288(52693212898128\omega + 44949443766637))$ $(1/90(578\omega-1), 1/2700(-27178\omega - 9701)\sqrt{-1} + 1/180(-668\omega+1))$
$K = F(\sqrt{\omega-10})$, $\mathrm{Cl}_K = \mathbb{Z}/4\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{-1})$ $4 \times (1/6305718039536929924(31552400795304062108\omega - 6896469078321153517),$ $1/39586019084123018171168062 42(-18261216303749133693083845421\omega - 709195269532882874299157690 2)\sqrt{\omega-10}$ $+1/12611436079073859848(-37858118834840992032\omega + 6896469078321153517))$ $\mathbf{0}$
$K = F(\sqrt{\omega-14})$, $\mathrm{Cl}_K = \mathbb{Z}/10\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{-1})$ $4 \times (1/490977713155175213615 4256(14205622609840941459351 1183\omega - 19023563442911180974214 1545),$ $1/10879092467992056837422758579391299904(-57657243366051156763738586647142382 0619\omega$ $+85270629099408668087602704003303671 4524)\sqrt{\omega-14}+$

$1/98195542631035042723085 12(-1469660032299611667296654 39\omega + 1902356344291118097421415 45))$

$(1/90(578\omega - 1), 1/2700(-27178\omega - 9701)\sqrt{-1} + 1/180(-668\omega + 1))$

$K = F(\sqrt{-2\omega - 7})$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{\omega})$

$4 \times (1/75685512100(100132192628\omega - 660391563537),$

$1/10410920616915500(-62823845900456566\omega + 73750317186356049)\sqrt{-2\omega - 7}$

$+1/151371024200(-175817704728\omega + 660391563537))$

$(1/21780(-178785\omega + 137189), 1/7187400(-48437001\omega + 96416473)\sqrt{-2\omega - 7}\sqrt{\omega} + 1/43560(157005\omega - 137189))$

$K = F(\sqrt{-3\omega - 8})$, $\mathrm{Cl}_K = \mathbb{Z}/4\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{\omega})$

$4 \times (1/52194885444(105459233508\omega - 151033021417),$

$1/5962273959153564(-10003101051835195\omega - 14072800013231530)\sqrt{-3\omega - 8}$

$+1/104389770888(-157654118952\omega + 151033021417))$

$(1/20(-101\omega + 57), 1/200(-78\omega - 71)\sqrt{-3\omega - 8}\sqrt{\omega} + 1/40(81\omega - 57))$

$K = F(\sqrt{5\omega - 17})$, $\mathrm{Cl}_K = \mathbb{Z}/6\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{\omega})$

$4 \times (1/15468461867044602554367090 56(-2699094580311414122855782373\omega - 9384962667717985968313756703),$

$1/81394903391819981347235439942716837763020 8(-2845895189663937627772646864729819401484183\omega$

$-5790974319833681355315943088724271283117 91)\sqrt{5\omega - 17}$

$+1/309369237340892051087341811 2(11522483936069538674190733 17\omega + 938496266771798596831375 6703))$

$(1/106619910654648471999912180(-172527908216123201070510631 93\omega + 291736288368633973485612453 65)$

$1/246174165027907826087985845468288004540 0(-225327289398142752236133966619864456452 4481\omega$

$+365156513441902924245518120031653716709 8338)\sqrt{5\omega - 17}\sqrt{\omega}$

$1/213239821309296943999824360(171461709109576716350511510 13\omega - 291736288368633973485612453 65))$

$K = F(\sqrt{2\omega - 15})$, $\mathrm{Cl}_K = \mathbb{Z}/8\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{\omega})$

0

$(1/501689727224078580(-204893297129553021 81\omega + 15906972431825354 65),$

$1/794580338951539798133856600(-243075621363947519797134380 23\omega$

$-522440625427539804066800368 61)\sqrt{2\omega - 15}\sqrt{\omega}$

$+1/100337945444815716 0(199876399857312236 01\omega - 15906972431825354 65))$

$K = F(\sqrt{2\omega - 9})$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{-\omega})$

$4 \times (1/21780(45524\omega - 256709)1/3593700(-33377604\omega + 29070707)\sqrt{2\omega - 9} + 1/43560(-67304\omega + 256709))$

$(1/873620(-1390901\omega + 9800496),$

$1/1825865800(-23074830142\omega + 73328702231)\sqrt{-\omega} + 1/1747240(517281\omega - 9800496))$

$K = F(\sqrt{-\omega - 3})$, $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{-\omega})$

$(1/1292400241536195583058247726240(85704092177525688230248145253482\omega$
$+325147336143204588972867980729 5),$
$1/4646174808739255259083975332906181761465043200 0(-1328886413513729791815297583668487528864248597 05\omega$
$-1438955945949736188805504178149745238987584388 23)\sqrt{-\omega-3}$
$+1/2584800483072391166116495452480 0(-9862809459288764406083062251588 2\omega$
$-325147336143204588972867980729 5))$
$(1/2(-11\omega+9),1/4(-28\omega+59)\sqrt{-\omega}+1/4(9\omega-9))$

$K=F(\sqrt{2\omega-13})$, $\mathrm{Cl}_K=\mathbb{Z}/6\mathbb{Z}$, $\mathcal{G}_K=K(\sqrt{-\omega})$
$4\times(1/16782027532336(14779551523822\omega-159359342975843),$
$1/8105392384221958094 72(-4475388013943905281774\omega+3328863329971908717157)\sqrt{2\omega-13}$
$+1/33564055064672(-31561579056158\omega+159359342975843))$
$(1/873620(-1390901\omega+9800496),$
$1/1825865800(-23074830142\omega+73328702231)\sqrt{-\omega}+1/1747240(517281\omega-9800496))$

$K=F(\sqrt{6\omega-17})$, $\mathrm{Cl}_K=\mathbb{Z}/8\mathbb{Z}$, $\mathcal{G}_K=K(\sqrt{-\omega})$
$4\times(1/142103012968140 4(5774013608189503 3\omega-105079944675237432),$
$1/6582538426034692644548 08(-6202471221416379136693688 7\omega+1041841351443821623190649 21)\sqrt{6\omega-17}$

$+1/2842060259362808(-59161166211576437\omega + 105079944675237432))$

$(1/2(-11\omega + 9), 1/4(-28\omega + 59)\sqrt{-\omega} + 1/4(9\omega - 9))$

$K = F(\sqrt{3\omega - 16})$, $\mathrm{Cl}_K = \mathbb{Z}/4\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{-\omega})$

$4 \times (1/29974076243995330044110357065397855174 76(2033132737515917064499794003997677230 7207\omega$

$+1443404258046320380336532959238153928107),$

$1/16410382788060382727537771993864973466889764597339058823 7224\times$

$(-25889872506093268620595404778232829701911343716411002127 1745\omega$

$-21330581249964564331199840893888830467520960265118880615 3865)\sqrt{3\omega - 16}$

$+1/59948152487990660088220714130795710349 52(-23328734999558703649408975746516557824683\omega$

$-1443404258046320380336532959238153928107))$

$(1/2(-11\omega + 9), 1/4(-28\omega + 59)\sqrt{-\omega} + 1/4(9\omega - 9))$

$K = F(\sqrt{-2\omega - 13})$, $\mathrm{Cl}_K = \mathbb{Z}/6\mathbb{Z}$, $\mathcal{G}_K = K(\sqrt{-\omega})$

$4 \times (1/1243926464(5928430018\omega - 2286794607),$

$1/606329564200448(-1352880017956328\omega - 1847770546529331)\sqrt{-2\omega - 13}$

$+1/2487852928(-7172356482\omega + 2286794607))$

0

CHAPTER 2

Lifting modular symbols of noncritical slope

1. Introduction

Let p be a prime and let M be a positive integer prime to p. Let $f \in S_2(\Gamma_0(pM))$ be a normalized eigenform with rational (and hence integral) Fourier coefficients. (We will consider higher weights in later sections.) One associates to f a modular symbol

$$\varphi_f : \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \to \mathbb{C}$$

and a measure μ_f on $\mathbb{Z}_p$ by the rules

$$\varphi_f\{r \to s\} = \frac{1}{\Omega^+} \operatorname{Re} \int_r^s 2\pi i f(z) dz,$$

$$\mu_f(a + p^n \mathbb{Z}_p) = a_p(f)^{-n} \varphi_f\{\infty \to a/p^n\}, \tag{27}$$

where Ω^+ is the canonical real period of f and $a_p(f)$ is its p-th Fourier coefficient. Suppose now that $a_p(f) \in \mathbb{Z}_p^*$. Then one may show (using Eichler-Shimura theory, for instance) that φ_f and thus μ_f take values in $\mathbb{Z}_p$. Therefore, the integral

$$\int_{\mathbb{Z}_p} v(x) d\mu_f(x), \tag{28}$$

defined as a limit of Riemann sums over increasingly fine partitions of $\mathbb{Z}_p$, is well defined for any continuous $v : \mathbb{Z}_p \to \mathbb{C}_p$.

Computing such integrals is an important problem in practice with many applications. The application of principal interest to us

is the calculation of algebraic points on elliptic curves via p-adic integration. Unfortunately, the naive method for computing integrals of the form (28) is of exponential complexity in the sense of [**9**]. Fortunately, many of the functions $v(x)$ which arise in practice are of a special type. Let

$$\mathbf{A} = \Big\{ v(x) = \sum_{n \geq 0} a_n x^n : a_n \in \mathbb{Q}_p, \quad a_n \to 0 \text{ as } n \to \infty \Big\}. \tag{29}$$

Elements of $\mathbf{A}$ are rigid analytic functions on the closed unit disk in $\mathbb{C}_p$ which are defined over $\mathbb{Q}_p$. As such series may be integrated term-by-term, the problem of computing (28) is reduced to the calculation of the moments

$$\text{mom}(n, \mu_f) = \int_{\mathbb{Z}_p} x^n d\mu_f(x), \quad n \geq 0.$$

A polynomial time algorithm for calculating such moments was recently discovered by R. Pollack and G. Stevens [**22**]. Although the main goal of their theory was the study of normalized eigenforms g of weight $k+2$ with $\text{ord}_p\, a_p(g) = k+1$ (a so-called critical slope eigenform) and their p-adic L-functions, we are particularly interested in their results in the (we shall see, simpler) case $\text{ord}_p\, a_p(g) < k+1$ (the non-critical slope case). For simplicity of exposition, we remain for the moment in the situation considered above where f has weight two and $a_p(f)$ is a p-adic unit. In later sections, we will deal with general weights and non-critical slopes.

Let $\mathbf{D}$ be the continuous dual of $\mathbf{A}$. Elements of $\mathbf{D}$ are called *rigid-analytic distributions*. Pollack and Stevens were able to produce a $\Gamma_0(pM)$-equivariant eigensymbol

$$\Phi_f : \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \to \mathbf{D}$$

satisfying

$$\int_{\mathbb{Z}_p} v(x) d\mu_f(x) = \Phi_f\{0 \to \infty\}(v).$$

Moreover, Φ_f is a lift of φ_f in the sense that $\varphi_f\{r \to s\}$ is the total measure of $\Phi_f\{r \to s\}$ for all $r, s \in \mathbb{P}^1(\mathbb{Q})$, i.e.

$$\int_{\mathbb{Z}_p} d\Phi_f\{r \to s\} = \varphi_f\{r \to s\}$$

(cf. [**10**, Proposition 1.3]). Through a careful analysis of the geometry of a fundamental domain of $\Gamma_0(pM)$ acting on the upper half-plane $\mathfrak{H}$, a process they dub "solving the Manin relations", Pollack and Stevens are able to give an explicit presentation of the group of $\Gamma_0(pM)$-equivariant $\mathbf{D}$-valued modular symbols. Using this presentation, they explicitly produce a lift Ψ of φ_f in such a way that $\Psi\{r \to s\}(x^n)$ can be easily computed for all $r, s \in \mathbb{P}^1(\mathbb{Q})$ and $n \geq 0$. It can then be shown (see [**10**, Proposition 2.6]) that

$$\Phi_f = \lim_{n \to \infty} a_p(f)^{-n} U_p^n \Psi.$$

is a $\mathbf{D}$-valued eigensymbol lifting φ_f. Moreover, and essential for computational purposes, the moments of the symbols $(\Psi|U_p^{n+1})\{r \to s\}$ can be explicitly computed from those of $(\Psi|U_p^n)\{t \to u\}$. A theory analogous to the above exists for all modular forms of noncritical slope, i.e. forms $f \in S_{k+2}(\Gamma_0(pM))$ with $\operatorname{ord}_p a_p(f) < k + 1$.

In this note, we show that in this non-critical slope situation, one may eliminate geometric considerations, i.e. the need to "solve the

Manin relations", from the Pollack-Stevens algorithm. The Pollack-Stevens algorithm has been applied in [**10**] to the calculation of Stark-Heegner points on elliptic curves defined over $\mathbb{Q}$. The incorporation of our method would simplify this work conceptually, in addition to streamlining the implementation. Our method also generalizes easily to the case of modular symbols constructed from certain automorphic forms on GL_2 over imaginary quadratic fields. These forms manifest themselves geometrically as harmonic forms on certain real-analytic threefolds. M. Trifković has recently implemented a version of our algorithm in PARI to compute certain Stark-Heegner points on elliptic curves defined over imaginary quadratic fields. As the geometry of the real-analytic threefolds arising in the work of Trifković is quite complicated compared to that of the modular curves, our "geometry free" method proves quite helpful. Suitably adapted to certain automorphic forms on definite quaternion algebras, our ideas can be used for the efficient calculation of Heegner points arising from Shimura curve parametrizations via the theory of Cerednik-Drinfeld; see [**1**], [**19**] and [**18**].

The author would like to sincerely thank his PhD supervisor Prof. Henri Darmon as well as Mak Trifković for many useful discussions regarding this work. Finally, the author is extremely grateful to the anonymous referee for many valuable comments, observations and suggestions which led to a significant reworking of this paper.

2. Coefficient modules

Let $p \in \mathbb{Z}$ be a rational prime, and define the semigroup

$$\Sigma_0(p\mathbb{Z}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_p) : c \in p\mathbb{Z}_p,\ a \in \mathbb{Z}_p^*, \text{ and } ad - bc \neq 0 \right\}.$$

For a $\mathbb{Z}_p$-module A and an integer $k \geq 0$, let

$$L_k(A) = \{f \in A[T] : \deg f(T) \leq k\}.$$

The group $L_k(A)$ is equipped with a right action of $\Sigma_0(p\mathbb{Z}_p)$ defined by

$$(f|_k\gamma)(T) = (d - cT)^k f\left(\frac{-b + aT}{d - cT}\right).$$

Let K be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$, uniformizer π, ramification index e, and valuation v, normalized so that $v(\pi) = 1$ (i.e. $v(p) = e$). Generalizing (29) slightly, we let

$$\mathbf{A}_k(K) = \left\{v(x) = \sum_{n\geq 0} a_n x^n : a_n \in K, \quad a_n \to 0 \text{ as } n \to \infty\right\}.$$

equipped with the left weight k action of $\Sigma_0(p\mathbb{Z}_p)$ given by the rule

$$(\gamma \cdot_k f)(x) = (a + cx)^k f\left(\frac{b + dx}{a + cx}\right)$$

for $f \in \mathbf{A}_k(K)$ and $\gamma \in \Sigma_0(p\mathbb{Z}_p)$. The sup-norm equips $\mathbf{A}_k(K)$ with the structure of a p-adic Banach space.

As in the introduction, we let $\mathbf{D}_k(K)$ denote the continuous dual of $\mathbf{A}_k(K)$, the elements of which we refer to as rigid-analytic distributions. As the polynomial functions are dense in $\mathbf{A}_k(K)$, a distribution μ in $\mathbf{D}_k(K)$ is completely determined by its moments $\mu(x^n)$, $n \geq 0$. By duality, $\mathbf{D}_k(K)$ has a weight k action of $\Sigma_0(p\mathbb{Z}_p)$ from the right written $(\mu, \gamma) \mapsto \mu|_k\gamma$, or simply $\mu|\gamma$ if the weight of the action is clear from context.

Set

$$\mathbf{D}_k(\mathcal{O}) = \{\mu \in \mathbf{D}_k(K) : \mu(x^n) \in \mathcal{O} \text{ for all } n \geq 0\}.$$

A simple computation (cf. proof of Lemma 21) shows that $\mathbf{D}_k(\mathcal{O})$ is a $\Sigma_0(p\mathbb{Z}_p)$-stable subspace of $\mathbf{D}_k(K)$.

LEMMA 20. *Let $\mu \in \mathbf{D}_k(K)$. Then moments $\mu(x^n)$ of μ are uniformly bounded. Consequently, $\mathbf{D}_k(K) \cong \mathbf{D}_k(\mathcal{O}) \otimes_{\mathcal{O}} K$.*

PROOF. Let $\|\cdot\|_{\mathbf{A}}$ and $\|\cdot\|_{\mathbf{D}}$ be the sup norm on $\mathbf{A}_k(K)$ and the dual norm on $\mathbf{D}_k(K)$, respectively. By the continuity of μ, we have

$$|\mu(x^n)|_p \leq \|\mu\|_{\mathbf{D}} \cdot \|x^n\|_{\mathbf{A}} = \|\mu\|_{\mathbf{D}} \cdot 1 = \|\mu\|_{\mathbf{D}}$$

□

The space $\mathbf{D}_k(\mathcal{O})$ admits a useful filtration:

$$F^0\mathbf{D}_k(\mathcal{O}) = \{\mu \in \mathbf{D}_k(\mathcal{O}) : \mu(x^0) = \mu(x^1) = \cdots \mu(x^k) = 0\}$$
$$F^N\mathbf{D}_k(\mathcal{O}) = \{\mu \in F^0\mathbf{D}_k(\mathcal{O}) : \mu(x^{k+j}) \in \pi^{N-j+1}\mathcal{O}, \quad j = 1, \ldots, N\},$$

for $N \geq 1$.

LEMMA 21. *The sets $F^N\mathbf{D}_k(\mathcal{O})$ are $\Sigma_0(p\mathbb{Z}_p)$-stable.*

PROOF. It suffices to show that $F^N\mathbf{D}_k(\mathcal{O})$ is stable under the action of matrices of the form

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \quad c \in p\mathbb{Z}_p, \quad \text{and} \quad \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad a \in \mathbb{Z}_p^*,$$

as we have the factorization

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c/a & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & \Delta/a \end{pmatrix}$$

in $\Sigma_0(p\mathbb{Z}_p)$, where $\Delta = ad - bc \neq 0$.

Let $\gamma = \left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right)$ with $c \in p\mathbb{Z}_p$ and let $\mu \in F^N\mathbf{D}_k(\mathcal{O})$. If $0 \leq \ell \leq k$, then

$$(\mu|_k\gamma)(x^\ell) = \mu((1+cx)^{k-\ell}x^\ell) = \mu(\text{polynomial of degree } k) = 0.$$

Now suppose $1 \leq j \leq N$. Then a direct calculation shows that

$$(\mu|_k\gamma)(x^{k+j}) = \sum_{n\geq 0}(-1)^n \binom{n+j-1}{j-1} c^n \mu(x^{k+j+n}). \tag{30}$$

As $c^n \in p^n\mathbb{Z}_p \subset \pi^n\mathcal{O}$ and $\mu(x^{k+j+n}) \in \pi^{N-j-n+1}\mathcal{O}$, it follows that each term in (30), and therefore $(\mu|_k\gamma)(x^{k+j})$, is in $\pi^{N-j+1}\mathcal{O}$. The case $\gamma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ is similar. □

Thanks to the above lemma, we may define the $\Sigma_0(p\mathbb{Z}_p)$-modules

$$A^N\mathbf{D}_k(\mathcal{O}) = \mathbf{D}_k(\mathcal{O})/F^N\mathbf{D}_k(\mathcal{O}), \quad N \geq 0.$$

We call $A^N\mathbf{D}_k(\mathcal{O})$ the N-th approximation to the module $\mathbf{D}_k(\mathcal{O})$, following the terminology of **[22]**. Note that $A^N\mathbf{D}_k(\mathcal{O})$ is a finitely generated $\mathcal{O}$-module. This will be crucial for our computational applications.

3. Modular symbols

DEFINITION 22. Let V be a right $\Sigma_0(p\mathbb{Z}_p)$-module, written $(v, \gamma) \mapsto v|\gamma$ for $v \in V$ and $\gamma \in \Sigma_0(p\mathbb{Z}_p)$. A *$V$-valued pre-modular symbol* is simply a function $\varphi : \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \to V$, written $(r, s) \mapsto \varphi\{r \to s\}$. If φ satisfies the additivity relation

$$\varphi\{r \to t\} = \varphi\{r \to s\} + \varphi\{s \to t\} \tag{31}$$

for all $r, s, t \in \mathbb{P}^1(\mathbb{Q})$, then φ is called a *modular symbol*.

Let $\mathrm{preSymb}\, V$ and $\mathrm{Symb}\, V$ denote the set of pre-modular and modular symbols, respectively.

The semigroup $\Sigma_0(p\mathbb{Z}_p)$ acts on $\mathrm{preSymb}\, V$ and $\mathrm{Symb}\, V$ by the rule

$$(\varphi|\gamma)\{r \to s\} = \varphi\{\gamma r \to \gamma s\}|\gamma,$$

where the action of $\Sigma_0(p\mathbb{Z}_p)$ on $\mathbb{P}^1(\mathbb{Q})$ is by fractional-linear transformations. If $\Gamma \subset \Sigma_0(p\mathbb{Z}_p)$, we denote by $\mathrm{Symb}_\Gamma V$ the set of all $\varphi \in \mathrm{Symb}\, V$ such that $\varphi|\gamma = \varphi$ for all $\gamma \in \Gamma$.

The group $\mathrm{preSymb}\, V$ and $\mathrm{Symb}\, V$ are equipped with the action of a Hecke operator U_p defined by

$$\varphi|U_p = \sum_{a=0}^{p-1} \varphi| \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix}.$$

REMARK 23. Fix a positive integer M prime to p and consider the double-coset decomposition

$$\Gamma_0(pM) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_0(pM) = \coprod_{a=0}^{p-1} \Gamma_0(pM)\gamma_a.$$

If φ belongs to $\mathrm{Symb}_{\Gamma_0(pM)} V$, then $\varphi|U_p \in \mathrm{Symb}_{\Gamma_0(pM)} V$ and

$$(\varphi|U_p)\{r \to s\} = \sum_{a=0}^{p-1} \varphi\{\gamma_a r \to \gamma_a s\}|\gamma_a$$

for any choice of representatives γ_a. This is *not* true if φ is merely taken to be in $\mathrm{Symb}\, V$ or $\mathrm{preSymb}\, V$. Thus, our extension of U_p from $\mathrm{Symb}_{\Gamma_0(pM)} V$ to these larger spaces is non-canonical.

Let W be a K-vector space on which U_p acts linearly, and let $\lambda \in K$ be a U_p-eigenvalue. We shall denote by $W^{U_p=\lambda}$ the corresponding eigenspace.

DEFINITION 24. Let ψ be a nonzero vector in $W^{U_p=\lambda}$. The *slope* of ψ is the number $\mathrm{ord}_p\, \lambda$. If A is one of $L_k(K)$, $A^N\mathbf{D}_k(\mathcal{O})$ or $\mathbf{D}_k(K)$ and $W = \mathrm{Symb}_{\Gamma_0(pM)} A$, then we say that the slope of ψ is *non-critical* if $\mathrm{ord}_p\, \lambda < k + 1$.

REMARK 25. Note that the slope of ψ may be fractional if the eigenvalue λ lies in a ramified extension of $\mathbb{Q}_p$.

By the Eichler-Shimura theory, $L_k(\mathbb{C})$-valued modular symbols correspond to classical modular forms of weight $k+2$. To a form g of weight $k+2$ we associate the modular symbol φ_g where

$$\varphi_g\{r \to s\} = \int_r^s (z+X)^k g(z)dz. \tag{32}$$

The following definition is due to G. Stevens [**27**]:

DEFINITION 26. A *rigid analytic modular symbol* of weight k on $\Gamma_0(pM)$, defined over K, is an element of $\mathrm{Symb}_{\Gamma_0(pM)}\mathbf{D}_k(K)$.

The following simple lemma will be useful.

LEMMA 27. $\mathrm{Symb}_{\Gamma_0(pM)}\mathbf{D}_k(K) \cong (\mathrm{Symb}_{\Gamma_0(pM)}\mathbf{D}_k(\mathcal{O})) \otimes_{\mathcal{O}} K$.

PROOF. The proof follows from Lemma 20, the stability of $\mathbf{D}_k(\mathcal{O})$ under the action of $\Sigma_0(p\mathbb{Z}_p)$, and the following well known fact concerning modular symbols: There exist finitely many pairs

$$(a_i, b_i) \in \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}), \quad i = 1, \ldots, n$$

with the property that for each pair $(r,s) \in \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q})$ there exist $\xi_i \in \mathbb{Z}[\Gamma_0(pM)]$ such that

$$(s) - (r) = \sum_{i=1}^{n} \xi_i((b_i) - (a_i)) \tag{33}$$

as formal divisors on $\mathbb{P}^1(\mathbb{Q})$. Let ψ be in $\mathrm{Symb}_{\Gamma_0(pM)}\mathbf{D}_k(K)$. By Lemma 20, we may find an element c of $\mathcal{O}$ such that $c\psi\{a_i \to b_i\} \in \mathbf{D}_k(\mathcal{O})$ for all $1 \leq i \leq n$, implying that $c\psi \in \mathrm{Symb}_{\Gamma_0(pM)}\mathbf{D}_k(\mathcal{O})$. $\square$

There is a natural $\Sigma_0(p\mathbb{Z}_p)$-equivariant, surjective specialization map

$$\pi^0 : \mathbf{D}_k(K) \to L_k(K)$$

given by

$$\pi^0(\mu)(T) = \int_{\mathbb{Z}_p} (T-t)^k d\mu(t) = \sum_{j=0}^{k} \binom{k}{j} \mu(t^{k-j}) T^j. \tag{34}$$

Let $m \in L_k(K)$ and let μ be the unique preimage of m under π^0 satisfying $\mu(x^j) = 0$ for $j > k$. We define the j-th moment of m, denoted $m(x^j)$, to be the quantity $\mu(x^j)$. Note that the section $m \mapsto \mu$ of π^0 is not $\Sigma_0(p\mathbb{Z}_p)$-equivariant. The map π^0 induces a corresponding function

$$\pi^0_* : \mathrm{Symb}_{\Gamma_0(pM)} \mathbf{D}_k(K) \to \mathrm{Symb}_{\Gamma_0(pM)} L_k(K)$$

in the obvious way. Since π^0 is a $\Sigma_0(p\mathbb{Z}_p)$-module homomorphism, the induced map π^0_* is equivariant with respect to the action of the operator U_p.

We will also have need of notation for families of related maps. We let π^N denote the natural projection from $\mathbf{D}_k(\mathcal{O})$ onto $A^N\mathbf{D}_k(\mathcal{O})$. If $N > M$, then π^M reduces to a map

$$\pi^{N,M} : A^N\mathbf{D}_k(\mathcal{O}) \to A^M\mathbf{D}_k(\mathcal{O}).$$

Since these maps are all $\Sigma_0(p\mathbb{Z}_p)$-equivariant, the induced maps π^N_* and $\pi^{N,M}_*$ on modular symbols are all U_p-equivariant. Note that our notation is consistent, as $L_k(\mathcal{O}) \cong A^0\mathbf{D}_k(\mathcal{O})$.

The main goal of this paper is to give a new proof of the following result of G. Stevens **[27]**, which translates into a simple effective algorithm for computing eigenlifts of $L_k(\mathbb{Q}_p)$-valued modular symbols to rigid analytic modular symbols.

THEOREM 28. *Let λ be an eigenvalue of the U_p operator acting on $\mathrm{Symb}_{\Gamma_0(pM)} L_k(\mathbb{Q}_p)$ such $\mathrm{ord}_p \lambda < k+1$, and let $K = \mathbb{Q}_p(\lambda)$. Then the restriction*

$$\pi_*^0 : (\mathrm{Symb}_{\Gamma_0(pM)} \mathbf{D}_k(K))^{U_p=\lambda} \to (\mathrm{Symb}_{\Gamma_0(pM)} L_k(K))^{U_p=\lambda}. \tag{35}$$

is an isomorphism.

REMARK 29. For applications to the construction of global points on elliptic curves as in **[10]**, **[18]**, and **[28]**, it suffices to consider the case $k = 0$ and $\lambda = \pm 1$.

The next section is devoted to the proof of this theorem. In § 5, we will address the practical implementation of the proof as a computational algorithm.

4. Lifting eigensymbols

Recalling the definition of the moments of an element of $L_k(\mathcal{O})$ given after (34), we set

$$L_k^\lambda(\mathcal{O}) = \{m \in L_k(\mathcal{O}) : m(x^i) \in \pi^{v(\lambda)-ei}\mathcal{O}, \quad 0 \le i \le \lfloor v(\lambda)/e \rfloor\},$$

where e is the ramification index of $K/\mathbb{Q}_p$ and $\lfloor \cdot \rfloor$ is the floor function. That the group $L_k^\lambda(\mathcal{O})$ is $\Sigma_0(p\mathbb{Z}_p)$-stable can be shown using the same ideas as those used in the proof of Lemma 21. Let $\varphi^0 \in \mathrm{Symb}_{\Gamma_0(pM)} L_k(K)$ be an eigensymbol with eigenvalue λ in K of slope strictly less than $k+1$. Assume further that φ^0 takes values in $L_k^\lambda(\mathcal{O})$.

LEMMA 30.

(1) *Let $\mu \in \mathbf{D}_k(\mathcal{O})$ be such that $\pi^0(\mu) \in L_k^\lambda(\mathcal{O})$. Then*

$$\mu| \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix} \in \lambda \mathbf{D}_k(\mathcal{O}).$$

(2) *Let μ be in $F^N\mathbf{D}_k(\mathcal{O})$. Then*

$$\mu|\begin{pmatrix}1 & a\\ 0 & p\end{pmatrix} \in \lambda F^{N+1}\mathbf{D}_k(\mathcal{O}).$$

PROOF. If μ is in $\mathbf{D}_k(\mathcal{O})$, then

$$\Big(\mu|\begin{pmatrix}1 & a\\ 0 & p\end{pmatrix}\Big)(x^j) = \mu((a+px)^j)$$

$$= \sum_{i=0}^{j}\binom{j}{i}a^{j-i}p^i\mu(x^i).$$

Let $t = \lfloor v(\lambda)/e\rfloor$. Suppose first that μ is in $L_k^\lambda(\mathcal{O})$. If $0 \le i \le t$, then

$$p^i\mu(x^i) = p^i\pi^0(\mu)(x^i) \in \pi^{ei+v(\lambda)-ei}\mathcal{O} = \lambda\mathcal{O}.$$

If, on the other hand, $i > t$, then it is clear that $ei > v(\lambda)$, and hence $p^i\mu(x^i) = \pi^{ei}\mu(x^i)$ is once again in $\lambda\mathcal{O}$. This proves (1). Now suppose μ is in $F^N\mathbf{D}_k(\mathcal{O})$. The terms in the above sum with $0 \le i \le k$ vanish. If $j \ge 1$, then $v(p^{k+j}) \ge v(\lambda)+1$, implying that

$$p^{k+j}\mu(x^{k+j}) \in \pi^{v(\lambda)}\pi\pi^{N-j+1}\mathcal{O} = \lambda\pi^{(N+1)-j+1}\mathcal{O}.$$

This completes the proof. □

Assume the existence of a lift φ^N of φ^0 to $\mathrm{Symb}_{\Gamma_0(pM)}A^N\mathbf{D}_k(\mathcal{O})$ such that φ^N is also U_p-eigensymbol with eigenvalue λ. Choose an arbitrary lift φ of φ^N to an element of $\mathrm{preSymb}\,\mathbf{D}_k(\mathcal{O})$. As φ is also a lift of φ^0, part (1) of Lemma 30 implies that

$$\varphi|\lambda^{-1}U_p \in \mathrm{preSymb}\,\mathbf{D}_k(\mathcal{O}).$$

Therefore, we may define the symbol φ^{N+1} by

$$\varphi^{N+1} = \pi_*^{N+1}(\varphi|\lambda^{-1}U_p) \in \mathrm{preSymb}\,A^{N+1}\mathbf{D}_k(\mathcal{O}).$$

The U_p-equivariance of the projection maps together with the relation $\pi^N = \pi^{N+1,N} \circ \pi^{N+1}$ imply that

$$\pi_*^{N+1,N}(\varphi^{N+1}) = \varphi^N.$$

PROPOSITION 31. *The pre-modular symbol φ^{N+1} is a well defined modular symbol in $\mathrm{Symb}_{\Gamma_0(pM)} A^{N+1}\mathbf{D}_k(\mathcal{O})$, independent of the choice of lift φ used in its construction. Moreover, φ^{N+1} is a U_p-eigensymbol with eigenvalue λ.*

We prove the proposition with a series of claims:

CLAIM. The premodular symbol φ^{N+1} does not depend on the choice of lift φ.

PROOF. Let $\varphi' : \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \to \mathbf{D}_k(\mathcal{O})$ be a second lift of φ^N. Then for each pair $(r, s) \in \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q})$, we have

$$(\varphi - \varphi')\{r \to s\} \in F^N\mathbf{D}_k(\mathcal{O}).$$

The claim now follows from the above part (2) of Lemma 30. □

CLAIM. The premodular symbol φ^{N+1} satisfies the additivity relation (31) and is thus a modular symbol.

PROOF. Fix some $s \in \mathbb{P}^1(\mathbb{Q})$, and define a symbol φ' by

$$\varphi'\{r \to t\} = \varphi\left\{r \to \frac{s+a}{p}\right\} + \varphi\left\{\frac{s+a}{p} \to t\right\}.$$

As φ' is also a lift of φ^N, Claim 1 implies that

$$\begin{aligned}\varphi^{N+1}\{r\to t\} &= \pi_*^{N+1}(\varphi'|\lambda^{-1}U_p)\{r\to t\}\\ &= \pi^{N+1}\Big(\frac{1}{\lambda}\sum_{a=0}^{p-1}\varphi\left\{\frac{r+a}{p}\to\frac{s+a}{p}\right\}|\begin{pmatrix}1&a\\0&p\end{pmatrix}+\\ &\qquad\qquad \frac{1}{\lambda}\sum_{a=0}^{p-1}\varphi\left\{\frac{s+a}{p}\to\frac{t+a}{p}\right\}|\begin{pmatrix}1&a\\0&p\end{pmatrix}\Big)\\ &= \pi^{N+1}(\varphi|(\lambda^{-1}U_p)\{r\to s\})+\pi^{N+1}(\varphi|(\lambda^{-1}U_p)\{s\to t\})\\ &= \varphi^{N+1}\{r\to s\}+\varphi^{N+1}\{s\to t\}.\end{aligned}$$

As s was arbitrarily chosen, we are done. □

CLAIM. The modular symbol φ^{N+1} is $\Gamma_0(pM)$-invariant.

PROOF. Let γ be in $\Gamma_0(pM)$. Since the map π_*^{N+1} is equivariant with respect to the action of $\Sigma_0(p\mathbb{Z}_p)$, it follows that

$$\varphi^{N+1}|\gamma\{r\to s\} = \pi_*^{N+1}\Big(\sum_{a=0}^{p-1}\varphi|\begin{pmatrix}1&a\\0&p\end{pmatrix}\gamma\Big)$$

Using the double coset decomposition

$$\Gamma_0(pM)\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma_0(pM) = \coprod_{a=0}^{p-1}\Gamma_0(pM)\begin{pmatrix}1&a\\0&p\end{pmatrix},$$

there exist elements $\gamma^a\in\Gamma_0(pM)$ such that

$$\sum_{a=0}^{p-1}\varphi|\begin{pmatrix}1&a\\0&p\end{pmatrix}\gamma = \sum_{a=0}^{p-1}(\varphi|\gamma^a)|\begin{pmatrix}1&a\\0&p\end{pmatrix}.$$

But since φ^N is $\Gamma_0(pM)$-invariant, each $\varphi|\gamma^a$ is also a lift of φ^N. Therefore, by Claim 1 again,

$$\begin{aligned}\varphi^{N+1}|\gamma &= \pi_*^{N+1}\Big(\sum_{a=0}^{p-1}(\varphi|\gamma^a)|\begin{pmatrix}1 & a\\ 0 & p\end{pmatrix}\Big)\\ &= \pi_*^{N+1}\Big(\sum_{a=0}^{p-1}\varphi|\begin{pmatrix}1 & a\\ 0 & p\end{pmatrix}\Big) = \varphi^{N+1}\end{aligned}$$

as desired. □

CLAIM. φ^{N+1} is a U_p-eigensymbol with eigenvalue λ.

PROOF. Observe that $\varphi|\lambda^{-1}U_p$ is also a lift of φ^N. The claim now follows from the $\Sigma_0(p\mathbb{Z}_p)$-equivariance of π_*^{N+1} and an application of Claim 1 similar in spirit those appearing above. □

Proposition 31 follows from these claims.

PROOF OF THEOREM 28. We begin by showing the injectivity of the map (35). By Lemma 27, it suffices to show that

$$(\mathrm{Symb}_{\Gamma_0(pM)}\mathbf{D}_k(\mathcal{O}))^{U_p=\lambda}\cap\ker\pi_*^0 = 0.$$

Let ψ be in the above intersection and set $u=\lambda^{-1}U_p$. Notice that

$$\mathrm{Symb}_{\Gamma_0(pM)}\mathbf{D}_k(\mathcal{O})\cap\ker\pi_*^0 = \mathrm{Symb}_{\Gamma_0(pM)}F^0\mathbf{D}_k(\mathcal{O}).$$

Therefore, by part 2 of Lemma 30, we see that

$$\psi=\psi|u^N\in\mathrm{Symb}_{\Gamma_0(pM)}F^N\mathbf{D}_k(\mathcal{O}).$$

The injectivity follows.

We not turn to the surjectivity of π_*^0 on λ-eigenspaces. Let $\varphi^0\in\mathrm{Symb}_{\Gamma_0(pM)}L_k^\lambda(\mathcal{O})$ be an eigensymbol with eigenvalue λ. We construct an eigenlift $\varphi^\infty\in\mathrm{Symb}_{\Gamma_0(pM)}\mathbf{D}_k(\mathcal{O})$ of the symbol φ^0. Using

the recipe of §4 together with Proposition 31, we may inductively construct a sequence

$$\varphi^N \in \mathrm{Symb}_{\Gamma_0(pM)} A^N \mathbf{D}_k(\mathcal{O})$$

of U_p-eigensymbols satisfying the compatibility property

$$\pi_*^{N+1,N}(\varphi^{N+1}) = \varphi^N, \quad N \geq 0.$$

By this compatibility relation, the φ^N glue together to a symbol

$$\varphi^\infty \in \varprojlim_{\{\pi_*^{M,N}\}} (\mathrm{Symb}_{\Gamma_0(pM)} F^N \mathbf{D}_k(\mathcal{O}))^{U_p=\lambda} \cong (\mathrm{Symb}_{\Gamma_0(pM)} \mathbf{D}_k(\mathcal{O}))^{U_p=\lambda}.$$

By construction, we have $\pi_*^0(\varphi^\infty) = \varphi^0$. This establishes the surjectivity and thus concludes the proof of Theorem 28. □

REMARK 32. Let $\psi^0 \in \mathrm{Symb}_{\Gamma_0(pM)} L_k(K)$ be an eigensymbol with eigenvalue λ and eigenlift ψ^∞. Let s be the smallest positive integer such that $\pi^s \psi^0 \in \mathrm{Symb}_{\Gamma_0(pM)} L_k^\lambda(\mathcal{O})$. Then it is interesting to note that the above constructions gives an explicit, uniform lower bound of s for the π-adic valuations of the moments $\psi^\infty\{r \to s\}(x^n)$. It would be interesting to know how sharp this bound is in cases where $v(\lambda) > 0$.

The above arguments show that the correspondences $\varphi^0 \mapsto \varphi^N$ extend to injections

$$u_\lambda^N : (\mathrm{Symb}_{\Gamma_0(pM)} L_k^\lambda(\mathcal{O}))^{U_p=\lambda} \hookrightarrow (\mathrm{Symb}_{\Gamma_0(pM)} A^N \mathbf{D}_k(\mathcal{O}))^{U_p=\lambda},$$

which are compatible in the sense that $\pi_*^{N+1,N} \circ u_\lambda^{N+1} = u_\lambda^N$. The maps u_λ^N can be packaged together into an injection

$$u_\lambda^\infty : (\mathrm{Symb}_{\Gamma_0(pM)} L_k^\lambda(\mathcal{O}))^{U_p=\lambda} \hookrightarrow (\mathrm{Symb}_{\Gamma_0(pM)} \mathbf{D}_k(\mathcal{O}))^{U_p=\lambda} \tag{36}$$

which is actually an isomorphism when tensored with K. If φ^0 is ordinary (i.e. $v(\lambda) = 0$), then $L_k^\lambda(\mathcal{O})$ is just $L_k(\mathcal{O})$ and (36) itself is an isomorphism.

5. Computing the lifts in practice

Restricting ourselves to the modular symbols which arise in practice, let $g \in S_{k+2}(\Gamma_0(pM))$ be a normalized Hecke-eigenform with U_p-eigenvalue λ of non-critical slope, and let $\psi_g \in \mathrm{Symb}_{\Gamma_0(pM)} L_k(\mathbb{C})$ be the modular symbol attached to g as in (32). Dividing ψ_g by a suitable transcendental factor Ω, we may assume

$$\psi^0 := \Omega^{-1}\psi_g$$

takes values in $L_k(\mathbb{Q}(g))$, where $\mathbb{Q}(g)$ is the field generated by the Hecke-eigenvalues of g.

Let $\{(a_i, b_i) : 1 \leq i \leq n\}$ be the finite set of pairs in $\mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q})$ considered in Lemma 27. If the field $\mathbb{Q}(g)$ has a simple enough structure (e.g. $\mathbb{Q}(g)$ is $\mathbb{Q}$ or a quadratic field), then by computing (32) to sufficiently high accuracy, one should be able to recognize the values $\psi^0\{a_i \to b_i\}$ as elements of $L_k(\mathbb{Q}(g))$. These values completely determine ψ^0 as an element of $\mathrm{Symb}_{\Gamma_0(pM)} L_k(\mathbb{Q}(g))$. Thus, ψ^0 may be stored as the finite sequence of $(k+1)$-tuples

$$(\psi^0\{a_i \to b_i\}(x^0), \ldots, \psi^0\{a_i \to b_i\}(x^k)) \in \mathbb{Q}(g)^{k+1},$$

$1 \leq i \leq n$. Let K be the completion of $\mathbb{Q}(g)$ at a place $\mathfrak{p}$ above p. Fix an embedding of $\mathbb{Q}(g)$ into K and let $\mathcal{O}$, v, and π be as above. Let $\varphi^0 \in \mathrm{Symb}_{\Gamma_0(pM)} L_k^\lambda(\mathcal{O})$ be obtained from ψ^0 by scaling by an appropriate power of π. Of course, the scaling factor involved in producing φ^0 must be taken into account when deciding on the precision to which the eigenlift of φ^0 must be computed.

A lift φ^N of φ^0 to $\mathrm{Symb}_{\Gamma_0(pM)} A^N\mathbf{D}_k(\mathcal{O})$ is determined by φ^0 together with the sequence of N-tuples

$$(\varphi^N\{a_i \to b_i\}(x^{k+1}), \ldots, \varphi^N\{a_i \to b_i\}(x^{k+N})) \in \prod_{j=1}^{N} \mathcal{O}/\pi^{N+1-j}\mathcal{O},$$

$1 \leq i \leq n$. This data may be easily represented on a computer.

Having dealt with the issue of storing $A^N\mathbf{D}_k(\mathcal{O})$-valued modular symbols, it remains to indicate how the data

$$\varphi^{N+1}\{a_i \to b_i\} \in A^{N+1}\mathbf{D}_k(\mathcal{O}), \quad 1 \leq i \leq n,$$

may be computed given the corresponding data for φ^N. As in the proof of Lemma 27, for $1 \leq i \leq n$ and $0 \leq \alpha \leq p-1$, we may find elements $\xi^i_{\alpha,j} \in \mathbb{Z}[\Gamma_0(pM)]$ such that

$$\Big(\frac{b_i+\alpha}{p}\Big) - \Big(\frac{a_i+\alpha}{p}\Big) = \sum_{j=1}^{n} \xi^i_{\alpha,j}((b_j) - (a_j))$$

as formal divisors on $\mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q})$. For $1 \leq i \leq n$, let μ_i be a lift of $\varphi^N\{a_i \to b_i\}$ to $\mathbf{D}_k(\mathcal{O})$ and define an distribution ν_i by the formula

$$\nu_i = \lambda^{-1} \sum_{\alpha=0}^{p-1} \sum_{j=1}^{n} \mu_j | (\xi^i_{\alpha,j})^{-1} \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix}.$$

Noting that

$$\pi^0(\nu_i) = \lambda^{-1} \sum_{\alpha=0}^{p-1} \varphi^0\Big\{\frac{a_i+\alpha}{p} \to \frac{b_i+\alpha}{p}\Big\} | \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix},$$

it follows by part 1 of Lemma 30 that ν_i is actually in $\mathbf{D}_k(\mathcal{O})$.

PROPOSITION 33. *The identity*

$$\pi^{N+1}(\nu_i) = \varphi^{N+1}\{a_i \to b_i\}$$

holds.

PROOF. Let φ be any lift of φ^N to $\mathrm{preSymb}\,\mathbf{D}_k(\mathcal{O})$ and recall that $\varphi^{N+1} = \pi_*^{N+1}(\varphi|(\lambda^{-1}U_p))$. For each α with $0 \leq \alpha \leq p-1$, we have

$$\varphi\Big\{\frac{a_i+\alpha}{p} \to \frac{b_i+\alpha}{p}\Big\} - \sum_{j=1}^{n} \mu_j|(\xi_{\alpha,j}^i)^{-1} \in F^N\mathbf{D}_k(\mathcal{O}).$$

The proposition now follows from part 2 of Lemma 30. □

The computation of the ν_i from the μ_i boils down to manipulations with formal power series: If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Sigma_0(p\mathbb{Z}_p)$ and $\mu \in \mathbf{D}_k(\mathcal{O})$, then one may compute the m-th moment of $\mu|\gamma$ by expanding $\left(\frac{b+dx}{a+cx}\right)^m$ in a Taylor series and "integrating term-by-term" (see the proof of Lemma 21). Using these methods, our proof of Theorem 28 translates into an efficient algorithm for computing eigenlifts of modular symbols of non-critical slope.

CHAPTER 3

Discussion and future directions

Although we feel that we have convincingly demonstrated the feasibility of computing Shimura-Heegner points on elliptic curves via Cerednik-Drinfeld theory, our treatment of this issue is far from complete. We treated only the cases of curves over $\mathbb{Q}$ of conductor $2p$ and curves over $\mathbb{Q}(\sqrt{5})$ of prime conductor. It seems clear, however, that our methods should generalize fairly directly, at least to curves defined over $\mathbb{Q}$ or over a real quadratic field. The challenge in implementing a more general algorithm would lie in the enumeration of various one-sided ideal classes of a quaternion algebra over such a field. Our approach to this enumeration process in the case of algebras defined over $\mathbb{Q}(\sqrt{5})$– see Chapter 1, Appendix A.2 – is most likely highly inefficient. Further study of this enumerative problem would be interesting.

In the Chapter 1, Appendix B, we showed how one may use p-adic integration to compute the Tate period q attached to a Hilbert modular newform on $\Gamma_0(\mathfrak{p})$ with rational Hecke eigenvalues. From the Tate period, one may compute the corresponding j-invariant $j(q)$. If $E_{j(q)}$ an elliptic curve over $\mathbb{Q}(\sqrt{5})$ with j-invariant $j(q)$, then $E_{j(q)}$ admits a "minimal"quadratic twist E of conductor $\mathfrak{p}$ (see **[25]**). In this way, one may be able to produce tables of elliptic curves, in the spirit of Cremona **[5]**, of prime conductor defined over $\mathbb{Q}(\sqrt{5})$ supplementing the tables of Fourier coefficients of Hilbert modular

forms given in [**12**]. Of course, implementation of more general versions of our algorithm could facilitate construction of further tables. In light of the indispensability of Cremona's tables for number theoretic experimentation, this may be a worthwhile project to pursue.

Let $\tau \in \mathfrak{H}_p$ be a fixed point of an optimal embedding of a quadratic order $\mathfrak{o}$, as in Chapter 1, §7. As we have seen, we may canonically associate to a character $\chi : \mathrm{Pic}\,\mathfrak{o} \twoheadrightarrow \{\pm 1\}$ of exact order 2 a divisor of degree 0 (see Chapter 1, §9). When χ is trivial, however, we are forced to exploit an auxilliary Hecke operator T_ℓ, where ℓ is a prime of good reduction for E, in order to obtain the degree zero divisor

$$\mathfrak{d}_\ell = (\ell + 1 - T_\ell)(\tau).$$

Due to the necessity of choosing an auxilliary prime, the Shimura-Heegner point

$$P_\ell = \mathrm{Tate}\Big(\int_{(\ell+1-T_\ell)\tau} \omega_{\mu_E} \Big).$$

is not canonically associated to the character χ. Although the point P_ℓ certainly depends on ℓ, it is nonetheless true that for any two primes ℓ and ℓ' of good reduction for E, we have

$$(\ell' + 1 - T_{\ell'})P_\ell = (\ell + 1 - T_\ell)P'_\ell.$$

In other words, the element $(\ell + 1 - a_\ell)^{-1}P_\ell$ of $E(H_\mathfrak{o}) \otimes \mathbb{Q}$ is independent of ℓ, where $H_\mathfrak{o}$ is the ring class field attached to the order $\mathfrak{o}$. Although P_ℓ is not in general divisible by $(\ell + 1 - a_\ell)$ in $E(H_\mathfrak{o})$, we have observed empirically that is very often divisible by factors thereof. At least for curves over $\mathbb{Q}$, the point P_ℓ always turned out to be divisible by the quantity $(\ell+1-a_\ell)/\#E(\mathbb{Q})_{\mathrm{tors}}$ in the several cases we have checked. Note that this is an integer as the denominator is

just $\#\tilde{E}(\mathbb{F}_\ell)$, which divides $\#E(\mathbb{Q})_{\text{tors}}$ by [**26**, Chapter VII, Prop. 3.1]. It is tempting to ask something like the following:

- Is there a map $\mathfrak{H}_p \to \mathbb{C}_p$, provisionally denoted

$$\tau \mapsto \Big(\fint^{\tau} \omega_\mu \Big)^{\#E(\mathbb{Q})_{\text{tors}}},$$

  such that

$$\Big(\Big(\fint^{\tau} \omega_\mu \Big)^{\#E(\mathbb{Q})_{\text{tors}}} \Big)^{\ell+1-a_\ell} = \fint_{(\ell+1-T_\ell)\tau} \omega_\mu \quad ?$$

Of course, the above formulation is modelled after Darmon's conjecture on the existence of semi-indefinite (semi-definite?) p-adic integrals, see [**6**, Conjecture 5] or [**10**, Conjecture 1.6]. If anything resembling the above is true, it is almost certainly a p-adic manifestation of a construction of Zhang [**32**]. Here, he defines of a canonical map from a Shimura curve X into $(\operatorname{Jac} X) \otimes \mathbb{Q}$ using the canonical "Hodge" divisor class (of degree one on each component of X) as a base point for defining an Abel-Jacobi map. Due to relations with special values of L-functions, it would be extremely interesting to give a purely p-adic description of this map. Work of Bertolini-Darmon and Dasgupta suggest that Hida theory could perhaps lend some insight into these issues.

The Heegner point phenomenon is not restricted to elliptic curves defined over number fields – there is an analogous construction in the setting of elliptic curves defined over function fields of curves over finite fields. For simplicity, we consider the function field $F = \mathbb{F}_p(t)$ with ring of integers $A = \mathbb{F}_p[t]$. Let ∞ be the place of F with uniformizer t^{-1} and denote by F_∞ the completion of F at ∞. Let $\mathfrak{o}_\infty$ be the ring of integers of F_∞ and let $\mathfrak{m}_\infty$ be the unique maximal ideal

of $\mathfrak{o}_\infty$. Set $\mathbb{C}_\infty$ equal to the completion of an algebraic closure of F_∞ and define the ∞-adic upper half-plane $\mathfrak{H}_\infty$ by

$$\mathfrak{H}_\infty = \mathbb{P}^1(\mathbb{C}_\infty) - \mathbb{P}^1(F_\infty).$$

Let E be an elliptic curve over F of conductor $\mathfrak{n}\infty$, where $\mathfrak{n}$ is an ideal of $\mathbb{F}_p[t]$, and suppose that the reduction of E at ∞ is split multiplicative. Then by Drinfeld's theory [**13**], E is *analytically modular* (borrowing terminology from [**30**, §3.2]) in the sense that one may attach to E an automorphic form φ_E whose L-function matches that of E. By an invocation of strong approximation analogous that of Chapter 1, §4, the form φ_E may be viewed as a function

$$\varphi_E : \Gamma_0(\mathfrak{n}) \backslash \mathrm{GL}_2(F_\infty)/\mathfrak{I}_\infty F_\infty^* \to \mathbb{Z},$$

where $\Gamma_0(\mathfrak{n})$ (resp. $\mathfrak{I}_\infty$) is the subgroup of $\mathrm{GL}_2(A)$ (resp. of $\mathrm{GL}_2(\mathfrak{o}_\infty)$ consisting of matrices which are upper-triangular modulo $\mathfrak{n}$ (resp. modulo $\mathfrak{m}_\infty$). Moreover, we may assume that φ_E takes values in no proper subring of $\mathbb{Z}$. Following the recipe of Chapter 1, §4, we may identify φ_E with a $\mathbb{Z}$-valued measure μ_E on $\mathbb{P}^1(F_\infty)$.

In addition to its analytic modularity, the curve E is, again in the terminology of [**30**, §3.3], *geometrically modular* in the sense that E admits a uniformization Φ by the Jacobian $J_0(\mathfrak{n})$ of the *Drinfeld modular curve* $X_0(\mathfrak{n})$. The curve $X_0(\mathfrak{n})$ is the compactification of an affine curve $Y_0(\mathfrak{n})$ whose $\mathbb{C}_\infty$-points are identified with the rigid analytic quotient $\Gamma_0(\mathfrak{n})\backslash\mathfrak{H}_\infty$. The affine curve $Y_0(\mathfrak{n})$ is a moduli space for pairs of $\mathfrak{n}$-isogenous Drinfeld F-modules.

In [**16**], Gekeler and Reversat make explicit the relationship between the analytic and geometric modularity of E by giving an ∞-adic analytic description of the uniformization $\Phi : J_0(\mathfrak{n}) \to E$ in

terms of the measure μ_E associated to the automorphic form φ_E. This description, originally phrased in terms of Drinfeld-Manin type theta functions, was reinterpreted by Longhi **[17]** in the language of ∞-adic integration. Let

$$\Phi_\infty : \mathrm{Div}^0 \mathfrak{H}_\infty \to E(\mathbb{C}_\infty)$$

be the composition of the projection $\mathrm{Div}^0 \mathfrak{H}_\infty \to \mathrm{Div}^0 X_0(\mathfrak{n})(\mathbb{C}_\infty)$ with the map induced by Φ on $\mathbb{C}_\infty$-points and let $\mathrm{Tate} : \mathbb{C}_\infty^* \to E(\mathbb{C}_\infty)$ be the Tate uniformization of E. Then Longhi's version of the result of Gekeler and Reversat states that for $(\tau') - (\tau) \in \mathrm{Div}^0 \mathfrak{H}_\infty$, we have

$$\Phi_\infty : (\tau') - (\tau) \mapsto \mathrm{Tate}\Big(\fint_{\mathbb{P}^1(F_\infty)} \left(\frac{x-\tau'}{x-\tau} \right) d\mu_E(x) \Big).$$

In addition, Longhi shows that if τ and τ' represent CM points on $X_0(\mathfrak{n})$, then $\Phi_\infty((\tau') - (\tau))$ is a global point on E. We shall refer to global points on E constructed in this manner as *Drinfeld-Heegner points*. An independent construction of Drinfeld-Heegner points was given by Pál in **[21]**. As Drinfeld-Heegner points play an important role in the arithmetic of elliptic curves over function fields (e.g. formulas of Gross-Zagier type are expected to hold), it would be extremely desirable to compute these points in practice. Therefore, we ask the following question:

- Is there an efficient algorithm for computing ∞-adic integrals of the form

$$\fint_{\mathbb{P}^1(F_\infty)} \left(\frac{x-\tau'}{x-\tau} \right) d\mu_E(x) \ ?$$

The obvious analogies with the Shimura-Heegner points considered in Chapter 1 may lead one to believe that our algorithm presented earlier may be easily adapted to the function field setting.

This is not so, however. In §8, we showed that in characteristic zero, the computation of integrals of the above form may be reduced (at least up to roots of unity and powers of p) to that of the moments of μ_E of the form

$$\int_{a+p\mathbb{Z}_p} (x-a)^n d\mu_E(x), \quad a \in \mathbb{Z}/p\mathbb{Z}, n \geq 0.$$

The essential point is that we need the p-adic exponential function – not available in characteristic p – to recover the Teichmüller representative of the multiplicative integral in question from the values of the corresponding additive moments. In the function field case, an incredible amount of data is lost in passing from the measure μ_E to its moments of the form

$$\int_{a+\mathfrak{m}_\infty} (x-a)^n d\mu_E(x), \quad a \in \mathfrak{o}_\infty/\mathfrak{m}_\infty, \quad n \geq 0.$$

Evidently, such moments depend only on the values of μ_E modulo p. Thus, representing μ_E on a computer by the using the above sequences of moments does not preserve enough information to facilitate the computations that we with to carry out. Thus, we ask the following:

- Give a sequence $\mu_E^{(n)}$, $n \geq 0$, of approximations to the measure μ_E, efficiently representable on a computer, such that the sequence $\mu_E^{(n)}$ completely determines μ_E.

This question in complexity theory seems to be fundamental in the theory of automorphic forms of Drinfeld type. There is always the possibility that no such algorithm exists. This possibility strikes us as unlikely, but would nonetheless be extremely fascinating. Thus, progress on this problem in any direction should have extremely interesting consequences.

We find the two problems mentioned above especially tantalizing, especially due to the fact that the rank conjecture for elliptic curves has been proven in the function field context [**23, 29**]. Moreover, a result of Darmon [**8**] inspired by [**29**] states that, assuming the conjecture of Birch and Swinnerton-Dyer, one may construct many examples of elliptic curves of large rank over $\mathbb{F}_p(t)$ where this excess is the result of Drinfeld-Heegner point phenomena. Thus, an algorithm for calculating these Drinfeld-Heegner points might allow us to actually compute examples of Mordell-Weil groups of arbitrarily large rank.

Bibliography

[1] M. Bertolini, H. Darmon, *Heegner points, p-adic L-functions and the Cerednik-Drinfeld uniformization*, Invent. Math. 126 (1996) 413-456.

[2] M. Bertolini, H. Darmon, *Hida families and rational points on elliptic curves*, Submitted.

[3] M. Bertolini, H. Darmon, A. Iovita, M. Spiess, *Teitelbaum's conjecture in the anticyclotomic setting*, American Journal of Mathematics 124 (2002), 411-449.

[4] I. Cerednik, *Uniformization of algebraic curves by discrete arithmetic subgroups of* $\mathrm{PGL}_2(k_w)$, Math. Sbornik 100 (1976) 59-88.

[5] J. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1992.

[6] H. Darmon, *Integration on* $\mathcal{H}_p \times \mathcal{H}$ *and arithmetic applications*, Annals of Math. (2) 154 (2001) no. 3, 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; by the American Mathematical Society, Providence, RI, 2004.

[8] H. Darmon, *Heegner points and elliptic curves of large rank over function fields*, In Heegner points and Rankin L-series, Math. Sci. Res. Inst. Publ., 49, Cambridge Univ. Press, Cambridge, 2004.

[9] H. Darmon, P. Green, *Elliptic curves and class fields of real quadratic fields: algorithms and evidence*, Experimental Mathematics, 11:1 (2002) 37-55.

[10] H. Darmon, R. Pollack, *The efficient calculation of Stark-Heegner points via overconvergent modular symbols*, to appear in Israel Journal of Mathematics.

[11] S. Dasgupta, *Stark-Heegner points on modular Jacobians*, Ann. Scient. c. Norm. Sup., 4e srie, t. 38, 2005, p. 427 469.

[12] L. Dembélé, *Computing Hilbert modular forms on* $\mathbb{Q}(\sqrt{5})$, PhD thesis, McGill University 2002.

[13] V. Drinfeld, *Elliptic modules*, Mat. Sb. (N.S.) 94(136) (1974), 594-627.

[14] V. Drinfeld, *Coverings of p-adic symmetric regions*, Funct. Anal. Appl. 10 (1976) 29-40.

[15] N. Elkies, *Shimura curve computations*, In Algorithmic number theory (Ithaca, NY, 1994) Lecture Notes in Comput. Sci., 877, Springer, Berlin, 1994, 122-133.

[16] E.-U. Gekeler, M. Reversat, *Jacobians of Drinfeld modular curves*, J. reine Angew. Math. 476 (1996), 2793.

[17] I. Longhi, *Non-Archimedean integration and elliptic curves over function fields*, J. Number Theory 94 (2002), 375404.

[18] M. Greenberg, *Heegner points and rigid analytic modular forms*, PhD thesis, McGill University, You're reading it.

[19] B. H. Gross, *Heights and special values of L-series*, CMS Conference Proc., H. Kisilevsky and J. Labute, eds., Vol. 7 (1987).

[20] B. Mazur, P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. 25 (1974) no. 1, 1-61.

[21] A. Pál, *Drinfeld modular curves, Heegner points and interpolation of special values*, Ph.D. thesis, Columbia University, 2000.

[22] R. Pollack, G. Stevens, *Computations with overconvergent modular symbols*, in preparation.

[23] I. Shafarevic, J. Tate, *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR 175 (1967), 770-773.

[24] G. Shimura, *Constructions of class fields and zeta functions of algebraic curves*, Ann. of Math. (2) 85 (1967), 55-159.

[25] J. Silverman, *Weierstrass equations and the minimal discriminant of an elliptic curve*, Mathematika 31 (1984) no. 2, 245-251.

[26] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106, Springer-verlag, New York, 1986.

[27] G. Stevens, *Rigid analytic modular symbols*, `http://math.bu.edu/people/ghs/research.d`, in preparation.

[28] M. Trifković, *Stark-Heegner points on elliptic curves defined over imaginary quadratic fields*, Submitted.

[29] D. Ulmer, *Elliptic curves with large rank over function fields*, Ann. of Math. (2) 155 (2002), 295-315.

[30] D. Ulmer, *Elliptic curves and analogies between number fields and function fields*, In Heegner points and Rankin L-series, Math. Sci. Res. Inst. Publ., 49, Cambridge Univ. Press, Cambridge, 2004.

[31] M.F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics 800, Springer, Berlin, 1980.

[32] S. Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math., 153 (2001), 27-147.