Efficient computation of Rankin p-adic L-functions

Alan G.B. Lauder*

October 15, 2012

Abstract

We present an efficient algorithm for computing certain special values of Rankin triple product p-adic L-functions and give an application of this to the explicit construction of rational points on elliptic curves.

1 Introduction

The purpose of this paper is to describe an efficient algorithm for computing certain special values of Rankin triple product p-adic L-functions. These special values are p-adic numbers and our algorithm computes them in polynomial-time in the desired precision. This improves on existing algorithms which require exponential time in the desired precision. Our method has the pleasant feature of also being applicable to Rankin double product p-adic L-functions, and working equally well in weight one as compared to higher weights (Sections 2.2.5 and 2.3.3). We hope it will usefully complement the powerful methods based upon overconvergent modular symbols for computing p-adic L-functions [17], which the author understands are less readily adaptable to higher product p-adic L-functions.

We describe an application of our algorithm to the efficient construction of rational points on elliptic curves over $\mathbb{Q}$. The curves we consider all have rank one and relatively small conductor, and so this application does not yield any "new" points. However, the constructions give experimental verification both of the correctness of the implementation of our algorithm, and various sophisticated and new conjectural constructions of rational points on elliptic curves. Even in the rank one setting these constructions are of interest; for instance, they allow one to carry out by p-adic means the complex analytic calculations in [4] (see Example 3.1), and in fact p-adically interpolate points found using much older but not well-understood methods. A different and enticing application of our algorithm is to the experimental study of conjectural constructions

*Mathematical Institute, 24-29 St Giles, Oxford, United Kingdom. This work is supported in part by a grant from the European Research Council (204083).

of "new" points on elliptic curves over certain number fields using weight one modular forms [5]. In this paper though we shall not address experimentally the calculation of these (Stark-Heegner) points attached to weight one forms or the p-adic interpolation of points. We plan to return to these questions in future joint work.

All of the applications of our algorithm are based upon ideas of Darmon and Rotger [7, 8]. In particular, Darmon encouraged the author to try to apply the method for computing with overconvergent modular forms in [16] to Rankin p-adic L-functions, and gave him invaluable help during the implementation of the algorithm and preparation of this paper. Much of the work behind this paper was in making the methods in [16] sufficiently fast in practice to turn a theoretical algorithm (for higher level) into one useful for experimental mathematics.

In writing this paper the author had the choice between trying to give a comprehensive background to the theory necessary to define Rankin p-adic L-functions and present the work of Darmon and Rotger, or distilling just enough to describe his contribution. He chose the latter, since the long introduction to [8] is already very clear but incompressible. This introduction should be read in parallel to our brief (and simplified) description below by anyone wishing to get a deeper understanding of the significance of the algorithm in our paper. The reader should also refer to that source for definitions of any unfamiliar terms below. (All the definitions we shall really need are gathered in Sections 2.1 and 2.3.1.)

Let f, g, h be newforms of weights $k, l, m \geq 2$, primitive characters χ_f, χ_g, χ_h with $\chi_f\chi_g\chi_h = 1$, and level N. Assume that the Heegner Hypothesis H [8, Section 1] is satisfied. Let p be a prime not dividing the level N, and fix an embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}_p$, the completion of an algebraic closure of the field of p-adic numbers $\mathbb{Q}_p$. Assume f, g and h are ordinary at p. Let $\mathbf{f}, \mathbf{g}$ and $\mathbf{h}$ be the (unique) Hida families of (overconvergent) p-adic modular forms passing through f, g and h. The Rankin p-adic L-function $\mathcal{L}_p^f(\mathbf{f}, \mathbf{g}, \mathbf{h})$ associates to each triple of weights (x, y, z) in (a suitable subset of) $\mathbb{Z}^3_{\geq 2}$ a p-adic number $\mathcal{L}_p^f(\mathbf{f}, \mathbf{g}, \mathbf{h})(x, y, z) \in \mathbb{C}_p$. It has a defining interpolation property over a certain set Σ_f of unbalanced weights, relating it to the special value of the classical (Garrett-)Rankin triple product L-function at its central critical point. (Weights (x, y, z) are balanced if the largest is strictly smaller than the sum of the other two, and otherwise unbalanced.) The theorem of Darmon and Rotger [8, Theorem 1.3] equates its value at the *balanced* weights to an explicit algebraic number times the p-adic Abel-Jacobi map of a certain cycle on a product of Kuga-Sato varieties evaluated at a particular differential form. At balanced weights (x, y, z) for reasons of sign the classical Rankin triple product L-function vanishes at its central critical point, and so the special value $\mathcal{L}_p^f(\mathbf{f}, \mathbf{g}, \mathbf{h})(x, y, z)$ is thought of as some kind of first derivative. (Darmon and Rotger actually construct in addition $\mathcal{L}_p^g(\mathbf{f}, \mathbf{g}, \mathbf{h})(x, y, z)$ and $\mathcal{L}_p^h(\mathbf{f}, \mathbf{g}, \mathbf{h})(x, y, z)$ but we only consider $\mathcal{L}_p^f(\mathbf{f}, \mathbf{g}, \mathbf{h})(x, y, z)$ and shall omit from here-on the superscript f.)

In this paper we present an algorithm for computing $\mathcal{L}_p(\mathbf{f}, \mathbf{g}, \mathbf{h})(x, y, z) \in \mathbb{C}_p$

for balanced weights (x, y, z) to a given p-adic precision in polynomial-time in the precision, provided $p \geq 5$ and *under the following assumption on the weights.* Let us specialise the Hida families back to the original weights (k, l, m) to recover the newforms f, g and h, and assume that (k, l, m) is a balanced triple. (This is only a notational simplification — we are after all really interested in our original newforms, the Hida families being introduced just to define the interpolation properties of the L-function.) Our algorithm requires that $k = l - m + 2$. This is enough for all our present and immediately envisaged arithmetic applications.

The problem which makes finding special values of Rankin triple product p-adic L-functions challenging is that of computing ordinary projections of p-adic modular forms. That is, in the definition of $\mathcal{L}_p(\mathbf{f}, \mathbf{g}, \mathbf{h})(k, l, m)$ one encounters a p-adic modular form "$d^{-(1+t)}(g^{[p]}) \times h$" which is not classical, and then has to compute its ordinary projection to some precision. Since this form is not classical any straightforward approach to this has exponential-time in the desired p-adic precision; for example, by iterating the Atkin operator on q-expansions or on some suitable space of classical modular forms (as the latter necessarily has exponential dimension in the required precision, by consideration of weights cf. [12, Proposition I.2.12 ii.]).

Our solution lies in the fact that "$d^{-(1+t)}(g^{[p]}) \times h$" is nearly overconvergent [8, Section 2.5]. More precisely, our assumption $(k = l - m + 2)$ on the weights is exactly that which ensures it is overconvergent, and so the methods we developed for computing with such forms in [16] can be applied. We expect that our methods can be generalised to handle nearly overconvergent modular forms (using their explicit description in [3]) and thus compute Rankin triple product p-adic L-functions at *any* balanced point (x, y, z), but we have not carried out any detailed work in this direction. The main result of our paper is really the algorithm (and its refinements) in Section 2.2 for computing the ordinary projection of certain overconvergent modular forms and in addition the ordinary subspace. (We give a full and rigorous analysis of this algorithm, but not of two aspects of our overall algorithm for computing Rankin triple product p-adic L-functions. These are of minor practical importance, see Note 2.3 (1) and (3), but difficult to analyse.)

Regarding arithmetic applications, the most immediate is the following one deduced by Darmon from [8, Theorem 1.3] and [10, Lemma 2.4], in a personal communication. Assume that f and g are newforms of weight 2 and trivial character, and that f has rational Fourier coefficients. Let E_f denote the elliptic curve over $\mathbb{Q}$ associated to f, and $\log_{E_f} : E_f(\mathbb{Q}_p) \to \mathbb{Q}_p$ be the formal p-adic logarithm map. Then there exists a point $P_g \in E_f(\mathbb{Q})$ and a computable positive integer d_g such that

$$\log_{E_f}(P_g) = 2d_g \frac{\mathcal{E}_0(g)\mathcal{E}_1(g)}{\mathcal{E}(g, f, g)} \mathcal{L}_p(\mathbf{g}, \mathbf{f}, \mathbf{g})(2, 2, 2). \tag{1}$$

Here $\mathcal{E}(g, f, g)/\mathcal{E}_0(g)\mathcal{E}_1(g)$ is the explicit non-zero algebraic (in fact quadratic) number which occurs in the Darmon-Rotger formula [8, Theorem 1.3] — it depends only upon the pth coefficients in the q-expansions of f and g. Thus if

$\mathcal{L}_p(\mathbf{g},\mathbf{f},\mathbf{g})(2,2,2)$ is non-vanishing one can recover a point of infinite order on $E_f(\mathbb{Q})$. (The integer d_g is that which appears, in different notation "d_T" for "$T := T_g$", in [4, Remark 3.1.3].) The point P_g is closely related to classically constructed points ("Zhang points"). We give an example of this application (Example 3.1), and understand it will be worked out in detail in the forthcoming Ph.D. thesis of Michael Daub [11]. In addition, we also present a number of variations of this application which suggest generalisations of the different underlying theoretical constructions and also illustrate our algorithm (Section 3).

The paper is organised in a simple manner, Section 2 containing the theoretical background and algorithms, and Section 3 our illustrative computations.

Acknowledgements: This paper would have been neither started nor finished without the constant help and encouragement of Henri Darmon. It is a pleasure to thank him for this, and to thank also David Loeffler, Victor Rotger and Andrew Wiles for enlightening discussions, and the anonymous referee for many useful comments.

2 The Algorithm

In this section we present our algorithm for computing the ordinary projection of overconvergent modular forms and certain special values of Rankin triple product p-adic L-functions.

2.1 Theoretical background

We first gather some background material on overconvergent modular forms and the ordinary subspace.

2.1.1 Katz expansions of overconvergent modular forms

Let N be a positive integer, and $p \geq 5$ be a prime not dividing N. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{Z}_p^*$ be a Dirichlet character with image in $\mathbb{Z}_p^*$. The condition that χ has image in $\mathbb{Z}_p^*$ is partly for notational convenience, but see also Note 2.2 (4).

For each integer k let $\mathbf{M}_k(N,\chi,\mathbb{Z}_p)$ denote the space of classical modular forms for $\Gamma_1(N)$ with character χ whose q-expansions at infinity have coefficients in $\mathbb{Z}_p$. This is a free $\mathbb{Z}_p$-module of finite rank. Let E_{p-1} be the classical Eisenstein series of weight $p-1$ and level 1 normalised to have constant term 1. For each integer $i > 0$, one may choose a free $\mathbb{Z}_p$-module $\mathbf{W}_i(N,\chi,\mathbb{Z}_p)$ of $\mathbf{M}_{k+i(p-1)}(N,\chi,\mathbb{Z}_p)$ such that

$$\mathbf{M}_{k+i(p-1)}(N,\chi,\mathbb{Z}_p) = E_{p-1}\cdot\mathbf{M}_{k+(i-1)(p-1)}(N,\chi,\mathbb{Z}_p)\oplus\mathbf{W}_i(N,\chi,\mathbb{Z}_p).$$

(This choice is not canonical cf. [14, Page 105].) Define $\mathbf{W}_0(N,\chi,\mathbb{Z}_p) := \mathbf{M}_k(N,\chi,\mathbb{Z}_p)$. Let K be a finite extension of $\mathbb{Q}_p$ with ring of integers B. Define $\mathbf{W}_i(N,\chi,B) := \mathbf{W}_i(N,\chi,\mathbb{Z}_p)\otimes_{\mathbb{Z}_p} B$. For $r \in B$ the space $M_k(N,\chi,B;r)$ of

r-overconvergent modular forms is by (our) definition the space of all "Katz expansions" of the form

$$f = \sum_{i=0}^{\infty} r^i \frac{b_i}{E_{p-1}^i}, \quad b_i \in \mathbf{W}_i(N, \chi, B), \quad \lim_{i\to\infty} b_i = 0$$

where $b_i \to 0$ as $i \to \infty$ means the q-expansions of b_i are more and more divisible by p as i goes to infinity, see [14, Proposition 2.6.2]. We define $M_k(N, \chi, K; r) := M_k(N, \chi, B; r) \otimes_B K$, a p-adic Banach space.

The element $r \in B$ plays a purely auxiliary role, determining the inner radius $p^{-\mathrm{ord}_p(r)}$ of the annuli of overconvergence into the supersingular locus. (Here $\mathrm{ord}_p(\cdot)$ is the p-adic valuation normalised with $\mathrm{ord}_p(p) = 1$.) From a computational point of view it is more convenient for each rational number $\alpha > 0$ to consider series of the form

$$f = \sum_{i=0}^{\infty} p^{\lfloor \alpha i \rfloor} \frac{b_i}{E_{p-1}^i}, \quad b_i \in \mathbf{W}_i(N, \chi, \mathbb{Z}_p).$$

We just write $M_k(N, \chi, \mathbb{Z}_p, \alpha)$ for the space of all such elements and call it again the space of α-overconvergent modular forms as no confusion is likely to arise. The space of *overconvergent modular forms* $M_k(N, \chi, \mathbb{Z}_p)$ is the union $\cup_{\alpha>0} M_k(N, \chi, \mathbb{Z}_p, \alpha)$. In everything just defined we may also just forget the character χ and consider the space $M_k(N, \mathbb{Z}_p)$ of overconvergent modular forms for $\Gamma_1(N)$ itself.

2.1.2 The ordinary subspace

Any overconvergent modular form $f \in M_k(N, \mathbb{Z}_p)$ is also a p-adic modular form [18, Section 1.4(b)] and has a q-expansion, and we define the *ordinary projection* in the usual way as $e_{ord}(f) := \lim_{n\to\infty} U_p^{n!}(f)$, where U_p is the Atkin operator on q-expansions, i.e., $U_p : \sum_n a_n q^n \mapsto \sum_n a_{np} q^n$. When $k \geq 2$ the image of e_{ord} on p-adic modular forms of level N over $\mathbb{Z}_p$ is equal to its image on the space of classical modular forms $\mathbf{M}_k(\Gamma_1(N) \cap \Gamma_0(p), \mathbb{Z}_p)$ of level Np with trivial character at p, see e.g. [2, Theorem 6.1] or for a precise statement (when $k \geq 3$) [12, Theorem II.4.3 ii]. We have for each $\nu \geq 1$ an embedding

$$\mathbf{M}_k(\Gamma_1(N) \cap \Gamma_0(p^\nu), B) \hookrightarrow M_k(N, B; r) \tag{2}$$

for any $r \in B$ with $\mathrm{ord}_p(r) < 1/p^{\nu-2}(p+1)$, see (at least for $N \geq 3$) [12, Corollary II.2.8], and also [3, Page 25]. Thus taking $\nu = 1$ here, one observes for $k \geq 2$ that the image of e_{ord} on p-adic modular forms of level N over $\mathbb{Z}_p$ is equal (after base change to B) to its image on $M_k(N, B; r)$ for any $r \in B$ with $\mathrm{ord}_p(r) < p/(p+1)$. We shall define the p-adic *ordinary subspace* over $\mathbb{Z}_p$ in level N, character χ and weight k to be the image under e_{ord} of $M_k(N, \chi, \mathbb{Z}_p, \frac{1}{p+1})$. (We make this definition since this is precisely the space computed by Algorithm 2.1. For weight $k \geq 2$ this is equivalent to the usual definition as the image of p-adic modular forms under e_{ord}, by our preceding observation. The definition

should also be equivalent for general weight (certainly over K) since the ordinary subspace over K can be described as the space of overconvergent (generalised) eigenforms of slope zero [12, Page 59], and (generalised) eigenforms of finite slope are r-overconvergent for any r with $\mathrm{ord}_p(r) < p/(p+1)$ [3, Page 25].)

2.2 Projection of overconvergent forms

Underlying our algorithm for computing Rankin p-adic L-functions is an algorithm for computing ordinary projections of overconvergent modular forms and also a basis for the ordinary subspace. It is an extension of [16, Algorithm 2.1].

2.2.1 The basic algorithm

We first present the basic algorithm, before discussing the steps in more detail and giving some practical refinements. Here the notation and assumptions are as in Section 2.1.1. (We apologise that the notation "m" for the p-adic precision gives a clash with that used for a weight in the introduction and later, but we wished to follow closely that in [16].)

Algorithm 2.1 *Given an element $H \in M_k(N, \chi, \mathbb{Z}_p, \frac{1}{p+1})$ where $0 \le k < p-1$ and integer $m \ge 1$, this algorithm computes the image in $R := \mathbb{Z}[[q]]/(p^m, q^{s(m,p)})$ of the ordinary projection $e_{ord}(H)$ and in addition the image in R of an echelonised basis for the ordinary subspace. (Here $s(m,p)$ is some explicit function of m and p defined during the algorithm.)*

(1) [Dimensions] Write $k_0 := k$. Compute $n := \lfloor \frac{p+1}{p-1}(m+1) \rfloor$. For $i = 0, 1, \ldots, n$ compute d_i, the dimension of the space of classical modular forms of level N character χ and weight $k_0 + i(p-1)$. Compute $m_i := d_i - d_{i-1}$, for $i \ge 1, m_0 := d_0$, and $\ell := m_0 + m_1 + \cdots + m_n = d_n$. Compute working precision $m' := m + \lceil \frac{n}{p+1} \rceil$. Compute $\ell' \ge \ell$, the Sturm bound for the space of classical modular forms of level N, character χ and weight $k_0 + (p-1)n$.

(2) [Complementary spaces] For each $0 \le i \le n$ compute a row-reduced basis W_i of q-expansions in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell' p})$ for some choice of the complementary space $\mathbf{W}_i(N, \chi, \mathbb{Z}_p)$.

(3) [Katz expansions] Compute the q-expansion in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell' p})$ of the Eisenstein series $E_{p-1}(q)$. For each $0 \le i \le n$, let $b_{i,1}, \ldots, b_{i,m_i}$ denote the elements in W_i. Compute the "Katz basis" elements $e_{i,s} := p^{\lfloor \frac{i}{p+1} \rfloor} E_{p-1}^{-i} b_{i,s}$ in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell' p})$.

(4) [Atkin operator] For each $0 \le i \le n$ and $1 \le s \le m_i$ compute $t_{i,s} := U_p(u_{i,s})$ in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell'})$, where U_p is the Atkin operator on q-expansions and $u_{i,s} := e_{i,s}$.

(5) [Atkin matrix] Compute T, the $\ell \times \ell'$ matrix over $\mathbb{Z}/(p^{m'})$ whose entries are the coefficients in the q-expansions modulo $q^{\ell'}$ of the ℓ elements $t_{i,s}$.

Compute E, the $\ell \times \ell'$ matrix over $\mathbb{Z}/(p^{m'})$ whose entries are the coefficients in the q-expansions modulo $q^{\ell'}$ of the ℓ elements $e_{i,s}$. Use linear algebra over $\mathbb{Z}/(p^{m'})$ to compute the matrix A' over $\mathbb{Z}/(p^{m'})$ such that $T = A'E$. Let A be the "Atkin matrix" over $\mathbb{Z}/(p^m)$ obtained by reducing entries in A' modulo p^m.

(6) [Two-stage projection] Compute the image $H \in \mathbb{Z}[[q]]/(p^{m'}, q^{\ell' p})$.

  (a) [Improve overconvergence] Compute $U_p(H) \in \mathbb{Z}[[q]]/(p^{m'}, q^{\ell'})$ and find coefficients $\alpha_{i,s} \in \mathbb{Z}/(p^m)$ such that $U_p(H) \equiv \sum_{i,s} \alpha_{i,s} e_{i,s} \bmod (p^m, q^{\ell'})$.

  (b) [Projection via Katz expansion] Compute a positive integer f such that all the unit roots of the reverse characteristic polynomial of A lie in some extension of $\mathbb{Z}_p$ with residue class field of degree f over $\mathbb{F}_p$. Compute A^{r-1} for $r := (p^f - 1)p^m$ using fast exponentiation. Compute $\gamma := \alpha A^{r-1}$ where α is the row vector $(\alpha_{i,s})$. Write $\gamma = (\gamma_{i,s})$ and return the ordinary projection $e_{ord}(H) = \sum_{i,s} \gamma_{i,s} e_{i,s} \in \mathbb{Z}[[q]]/(p^m, q^{s(m,p)})$ where $s(m,p) := \ell' p$.

(7) [Ordinary subspace] Compute $A^r = A^{r-1}A$ and let $\{(B_{i,s})\}$ be the set of non-zero rows in the echelon form B of the matrix A^r. Return $\sum_{i,s} B_{i,s} e_{i,s} \in \mathbb{Z}[[q]]/(p^m, q^{s(m,p)})$ for each non-zero row $(B_{i,s})$, the image of a basis for the ordinary subspace.

In this algorithm we assume that the q-expansion of the input modular form H can be computed in polynomial-time in N, p and any desired p-adic and q-adic precisions. Regarding the complexity of the whole algorithm, we just refer the reader to the analysis of Steps 1-5 in [16, Sections 3.2.2, 3.3.1], and observe that Steps 6 and 7 can be carried out using standard methods in linear algebra. In particular, the algorithm is certainly polynomial time in N, p and m.

2.2.2 Proof of correctness

The analysis of the correctness of the algorithm is very similar to that in [16, Section 3.2.1]. The essential idea is the following. One considers an infinite square matrix for the Atkin U_p operator on the space of $\frac{1}{p+1}$-overconvergent modular forms w.r.t. some choice of Katz basis. Reducing this (assumed integral, see Note 2.2 (3)) matrix modulo p^m, it vanishes except for an $\infty \times \ell$ strip down the lefthand side. The matrix A modulo p^m we compute is the $\ell \times \ell$ matrix which occurs in the top lefthand corner, for our choice of basis (this is proved in [16, Section 3]). We would like to iterate the infinite matrix on the infinite row vector representing an overconvergent modular form H. When $H \in M_k(N, \chi, \mathbb{Z}_p, \frac{p}{p+1})$ we notice that the coefficients in the infinite vector representing H w.r.t. our Katz basis decay p-adically (since $p/(p+1) > 1/(p+1)$) and in fact vanish modulo p^m, except for the first ℓ elements (see the final paragraph in [16, Section 3.4.2]). Hence we can iterate U_p on H by iterating the

finite matrix A on a finite vector of length ℓ. (The actual power r is chosen to ensure that we iterate sufficiently often to obtain the correct answer modulo p^m.) In our application to Rankin p-adic L-functions we will find that in fact $H \in M_k(N, \chi, \mathbb{Z}_p, \frac{1}{p+1})$. Hence the preliminary Step 6 (a) is to apply the U_p operator once to q-expansions to improve overconvergence by a factor p, see [16, Equation (2)] and Note 2.2 (3). (There is a loss of precision of $m' - m$ when one writes $U_p(H)$ as a Katz expansion, cf. the last paragraph of [16, Section 3.2.1] where a similar loss occurs during the computation of the matrix A.) Observe that this preliminary step is harmless, since we need to compute the elements in our Katz basis to the higher precision modulo $q^{\ell' p}$ anyway. (To make the above argument completely rigorous one fusses over the minor difference between r-overconvergent for all $\mathrm{ord}_p(r) < p/(p+1)$, and $\frac{p}{p+1}$-overconvergent, as in [16, Section 3.2.1].)

Note 2.2 We make some minor comments on the algorithm.

(1) For weight $k \geq 2$ the ordinary subspace can be computed instead using classical methods; however, our algorithm is the only "polynomial-time" method known to the author for computing this subspace in weight $k \leq 1$.

(2) We assume that the smallest non-zero slope s_0 of (the Newton polygon of) the reverse characteristic polynomial of A is such that $\lceil m/s_0 \rceil \leq (p^f - 1)p^m$. This is reasonable as the smallest non-zero slope which has ever been experimentally observed is $1/2$. (One could of course compute s_0 and adjust r accordingly to remove this assumption.) The integer f can be easily computed by reducing the matrix A modulo p. The exponent m rather than $m-1$ in the definition of r accounts for the possibility that the unit roots may lie in ramified extensions. (So $u^r \equiv 1 \bmod p^m$ for each unit root u, and $u^r \equiv 0 \bmod p^m$ for all other roots u of the reverse characteristic polynomial.)

(3) The correctness of the algorithm relies on the assumption that we can solve $T = A'E$ for a p-adically integral matrix A', although the theory only guarantees that pA' has integral coefficients, see [16, Note 3.2, Section 3.2.1] and also [12, II.3], [14, Section 3.11]. One could modify the algorithm (or rather the refined version in Section 2.2.4) to remove this assumption; however, in practice the author has never encountered a situation in which the matrix A' fails to have p-adically integral coefficients.

(4) The assumption that $\mathbb{Z}[\chi]$ embeds in $\mathbb{Z}_p$ allows one to exploit fast algorithms for matrix and polynomial arithmetic over rings of the form $\mathbb{Z}_p/(p^m) \cong \mathbb{Z}/(p^m)$ which are integrated into the systems Magma and Sage. The algorithm works perfectly well in principle without this assumption, but it will be much more difficult to get a comparably fast implementation.

(5) The hypothesis $0 \leq k < p-1$ can be removed as follows. In Step 1 write $k := k_0 + j(p-1)$ where $0 \leq k_0 < p-1$. In Step 4 compute $G := E_{p-1}(q)/E_{p-1}(q^p)$ and $G^j \in \mathbb{Z}[[q]]/(p^{m'}, q^{\ell' p})$, and let $u_{i,s} := G^j e_{i,s}$. The matrix A computed

in Step 5 is then for the "twisted" Atkin operator $U_p \circ G^j$. After Step 6(a) multiply the q-expansion of $U_p(H)$ by E_{p-1}^{-j} and in Step 6(b) multiply the q-expansion $\sum_{i,s} \gamma_{i,s} e_{i,s}$ by E_{p-1}^{j} and return this product as $e_{ord}(H)$. In Step 7 multiply each q-expansion $\sum_{i,s} b_{i,s} e_{i,s}$ by E_{p-1}^{j} to get the basis for ordinary space. For $j \geq 1$, to ensure $E_{p-1}^{-j} U_p(H)$ lies in the correct space one should multiply it by $p^{\lceil \frac{j}{p+1} \rceil}$, and so the final answer will only be correct modulo $p^{m - \lceil \frac{j}{p+1} \rceil}$. (One could of course also just run the algorithm without twisting, but then the auxiliary parameters n, ℓ, m' etc would have to be worked out afresh, since the algorithm would no longer be an extension of [16, Algorithm 2.1].)

(6) In practice the output q-adic precision $s(m,p) = \ell' p$ is always large enough for our needed application to Rankin p-adic L-functions. One can insist though on any output precision $s' \geq \ell' p$ simply by computing the Katz basis elements in Step 3 to that q-adic precision.

2.2.3 Finding complementary spaces in Step 2

A key step in the algorithm is the efficient construction in practice of the image in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell' p})$ of a basis for some choice of complementary spaces $\mathbf{W}_i(N, \chi, \mathbb{Z}_p)$, for each $0 \leq i \leq n$. The author's implementation (which is at present restricted to trivial or quadratic characters χ) is based upon suggestions of David Loeffler and John Voight. The idea is to use the multiplicative structure on the ring of modular forms.

One fixes a choice of weight bound $\mathcal{B} \geq 1$ and computes the image in $\mathbb{Z}[[q]]/(p^{m'}, q^{\ell' p})$ of a $\mathbb{Z}[\chi']$-basis for each of the spaces of classical modular forms $\mathbf{M}_b(N, \chi', \mathbb{Q}(\chi'))$ where $1 \leq b \leq \mathcal{B}$ and χ' vary over a set of characters which generate a group containing χ. One then reduces these basis elements modulo $(p, q^{\ell'})$ and for each $0 \leq i \leq n$ looks for random products of these q-expansions which generate an $\mathbb{F}_p$-vector space of dimension d_i and have weight $k_0 + i(p-1)$ and character χ. This is done in a recursive manner. Once one has computed the required forms in weight $k_0 + (i-1)(p-1)$ one maps then (via the identity map) into weight $k_0 + i(p-1)$ (recall $E_{p-1} \equiv 1 \mod p$) and generates a further $m_i = d_i - d_{i-1}$ linearly independent forms in weight $k_0 + i(p-1)$ and character χ. The correct choices of products, which give forms not in the space already generated, are "encoded" in an appropriate manner; that is, the basis elements for each weight b and character χ' are stored as an ordered list, and products of them (modulo $(p, q^{\ell'})$) can then be represented by "codes" which give the positions chosen in each list.

Having found these correct choices modulo $(p, q^{\ell'})$ one then repeats the process modulo $(p^{m'}, q^{\ell' p})$ to find the complementary spaces $\mathbf{W}_i(N, \chi, \mathbb{Z}_p)$, but crucially this time using the "codes" to only take products of modular forms which give something not in the $\mathbb{Z}_p$-span of the forms already computed. In this way when working to the full precision one does not waste time computing

products of modular forms that lie in the space one has already generated. (It surprised the author to discover that in practice in some examples, e.g. Example 3.5, one can generate many such "dud" forms — he has no intuition as to why this is the case.)

A good bound to take is $\mathcal{B} := 6$, but one can vary this, playing the time it takes to generate the spaces in low weight off against the time spent looking for suitable products. This choice of bound fits with some theoretical predictions communicated to the author by David Loeffler.

2.2.4 A three-stage projection in Step 6

In Algorithm 2.1 we find $U_p^r(H)$, where r is chosen so that the answer is correct modulo p^m, in two separate stages. First, one computes $U_p(H) \in M_k(N, \chi, \mathbb{Z}_p, \frac{p}{p+1})$ using q-expansions. Second, one computes $U_p^{r-1}(U_p(H))$ using Katz expansions. However, the matrix A has size growing linearly with m and so the computation of the high power A^{r-1} becomes a bottleneck as the precision m increases.

A better aproach is to factor the projection map into three parts, as follows. Write s_0 for the smallest non-zero slope in the characteristic series of A (one can safely just set $s_0 := 1/2$). Computing $A^{\lceil m/s_0 \rceil}$ and writing its non-zero rows (which are w.r.t. the Katz basis) as q-expansions in $\mathbb{Z}[[q]]/(p^m, q^{\ell' p})$ gives (the image of) a basis for the ordinary subspace. One can now compute a matrix A_{ord} over $\mathbb{Z}/(p^m)$ for the U_p operator on this basis by explicitly computing with q-expansions. This matrix is significantly smaller than A itself, since its dimension has no dependence on m. To project H, one computes as before $U_p(H)$ using q-expansions, then $U_p^{\lceil m/s_0 \rceil}(U_p(H))$ via Katz expansions as the product $\beta := \alpha A^{\lceil m/s_0 \rceil}$. Next, one writes the "Katz vector" β as the image of a q-expansion in $\mathbb{Z}[[q]]/(p^m, q^{\ell' p})$ and thus as a new vector β' over $\mathbb{Z}/(p^m)$ in terms of the basis for the ordinary subspace. Finally, one computes $U_p^{r-\lceil m/s_0 \rceil - 1}$ on $U_p^{\lceil m/s_0 \rceil}(U_p(H))$ as $\gamma' := \beta' A_{ord}^{r-\lceil m/s_0 \rceil - 1}$ and returns the q-expansion associated to γ' as the ordinary projection of H modulo $(p^m, q^{s(m,p)})$.

This three-stage projection method also works for $k < 0$ or $k \geq p-1$, but one must take care to twist and un-twist by powers of E_{p-1} at the appropriate times.

2.2.5 Avoiding weight one forms

In the case that $k = 1$, one can compute the ordinary projection $e_{ord}(H)$ of the weight one form H without doing *any* computations in weight one, except computing the q-expansion of H itself modulo $(p^{m'}, q^{\ell' p})$. The idea is to use the Eisenstein series to "twist" up to weight $p = 1 + (p-1)$. That is, one proceeds as in Note 2.2 (5), only writing $k = 1 = k_0 + j(p-1)$ where now $k_0 := p$ and $j := -1$. In addition, when generating complementary spaces (see Section 2.2.3) one only computes bases of classical modular forms in low weights $2 \leq b \leq \mathcal{B}$.

The author has implemented this variation in both Magma and Sage, and used it to compute the characteristic series of the Atkin operator on p-adic

overconvergent modular forms in weight one (for a quadratic character, and various levels N and primes p) without computing the q-expansions of any modular forms in weight one.

2.3 Application to p-adic L-functions

We now describe the application of Algorithm 2.1 to the computation of p-adic L-functions.

2.3.1 Definition of Rankin triple product p-adic L-functions

Let f, g, h be newforms of balanced weights $k, l, m \geq 2$, primitive characters χ_f, χ_g, χ_h, with $\chi_f\chi_g\chi_h = 1$ and level N. Assume that the Heegner hypothesis H from [8, Section 1] is satisfied, e.g. N is squarefree and for each prime ℓ dividing N the product of the ℓth Fourier coefficients of f, g and h is $-\ell^{(k+l+m-6)/2}$. Write $k = l + m - 2 - 2t$ with $t \geq 0$, which is possible since the sum of the weights must be even. We fix an embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ and assume f, g and h are ordinary at p. That is, the pth coefficient in the q-expansion of each is a p-adic unit.

Define the map $d = q\frac{d}{dq}$ on q-expansions as $d : \sum_{n\geq 0} a_n q^n \mapsto \sum_{n\geq 0} n a_n q^n$. Then for $s \geq 0$, the map d^s acts on p-adic modular forms increasing weights by $2s$ [18, Théorème 5(a)]. For a p-adic modular form $a(q) := \sum_{n\geq 0} a_n q^n$ let $a^{[p]} := \sum_{n\geq 1,\, p\not| n} a_n q^n$ denote its p-depletion. Then for $s \geq 1$ the map

$$a \mapsto d^{-s}(a^{[p]}) = \sum_{\substack{n=1 \\ p\not| n}}^{\infty} \frac{a_n}{n^s} q^n$$

acts on p-adic modular forms shifting weights by $-2s$ [18, Théorème 5(b)]. So $d^{-(1+t)}(g^{[p]}) \times h$ is a p-adic modular form of weight $l - 2(1+t) + m = k$ and character $\chi_g\chi_h = \chi_f^{-1}$.

Let f^* be the dual form to f and $f^{*(p)}$ be the ordinary p-stabilisation of f^*, see [8, Sections 1 and 4]. So $f^{*(p)}$ is an ordinary eigenform of character χ_f^{-1}. We define

$$\mathcal{L}_p(\mathbf{f}, \mathbf{g}, \mathbf{h})(k, l, m) := c(f^{*(p)}, e_{ord}(d^{-(1+t)}(g^{p]}) \times h)) \in \mathbb{C}_p.$$

Here we are assuming the action of the Hecke algebra on the ordinary subspace in weight k is semisimple (which the author understands is well-known for N squarefree since $k \geq 2$) and $c(f^{*(p)}, \bullet)$ denotes the coefficient of $f^{*(p)}$ when one writes an ordinary form $\bullet$ as a linear combination of ordinary eigenforms, see [13, Page 222]. (Darmon and Rotger take a different but equivalent approach, using the Poincaré pairing in algebraic de Rham cohomology to extract the coefficient $\mathcal{L}_p(\mathbf{f}, \mathbf{g}, \mathbf{h})(k, l, m)$ [8, Proposition 4.10].)

2.3.2 Computation of Rankin triple product p-adic L-functions

We shall now (with another apology) introduce the clashing notation m to refer to the p-adic precision, as in Section 2.2. We wish to apply Algorithm 2.1 to compute $e_{ord}(H)$ for $H := d^{-(1+t)}(g^{[p]}) \times h$ modulo p^m (and q-adic precision $s(m,p)$) and also a basis for the ordinary subspace in level N, weight k and character $\chi := \chi_f^{-1}$. (So we should assume that the image of χ lies in $\mathbb{Z}_p$ and g and h are defined over $\mathbb{Z}_p$, but see also Notes 2.2 (4) and 2.3 (2).) Given these, one can use Hecke operators on the ordinary subspace to extract the coefficient $c(f^{*(p)}, e_{ord}(H))$, see Note 2.3 (3), as $f^{*(p)}$ (and H) are easy to compute (at least within Magma and Sage using the algorithms from [19]).

For our projection algorithm to work we require that H is overconvergent (rather than just nearly overconvergent [8, Section 2.5]) and in particular that $H \in M_k(N, \chi, \mathbb{Z}_p, \frac{1}{p+1})$ for $\chi := \chi_f^{-1}$. Overconvergence is guaranteed provided $t = l - 2$, since $a \mapsto d^{-s}(a^{[p]})$ maps overconvergent forms in weight $1+s$ to overconvergent forms in weight $1-s$ [2, Proposition 4.3]. That is, provided

$$k = m - l + 2 \tag{3}$$

we will have that $d^{-(1+t)}(g^{[p]})$, and hence also H, is overconvergent. When this condition is not satisfied our algorithm with fail.

Regarding the precise radius of convergence of $d^{-(1+t)}(g^{[p]})$, Darmon has explained to the author that when our condition (3) is met the methods used by Coleman (the geometric interpretation of the d operator in terms of the Gauss-Manin connection [8, Section 2.5]) show the form $d^{-(1+t)}(g^{[p]})$ lies in the space $M_k(N, \chi_g, K; r)$ for any $r \in B \subset \mathbb{C}_p$ with $\mathrm{ord}_p(r) < 1/(p+1)$. Let us outline the argument to get an idea why this is true. First, the p-depletion $g^{[p]} := (1 - V_p U_p)g$ is a classical modular form for $\Gamma_1(N) \cap \Gamma_0(p^2)$ with trivial character at p and infinite slope. (Here V_p is the one-sided inverse of U_p [8, Equation (12)] and increases the level of $U_p(g)$ by p.) Hence by (2) with $\nu := 2$, $g^{[p]}$ lies in $M_\ell(N, \chi_g, B; r)$ for any $r \in B$ with $\mathrm{ord}_p(r) < 1/(p+1)$. Next, [2, Theorem 5.4] gives an explicit relation between the action of powers of the d operator on spaces of overconvergent modular forms and that of the Gauss-Manin connection of certain de Rham cohomology spaces associated to rigid analytic modular curves. This relationship associates to $g^{[p]}$ a trivial class in the de Rham cohomology space (the righthand side of [8, Equation (34)] for "r" equals t and any "ϵ" less than $1/(p+1)$), and hence one in the image of the Gauss-Manin connection. (The class is trivial because the form has infinite slope, cf. [2, Lemma 6.3].) The Gauss-Manin connection preserves the radius of convergence, and taking the preimage and untangling the relationship one finds that $d^{-(1+t)}(g^{[p]})$ is an overconvergent modular form of the same radius of convergence as $g^{[p]}$, i.e. $d^{-(1+t)}(g^{[p]}) \in M_\ell(N, \chi_g, K; r)$ for any $r \in B$ with $\mathrm{ord}_p(r) < 1/(p+1)$. Thus multiplying by h (and using (2) with $\nu := 1$ to determine the overconvergence of h itself) we find also

$$d^{-(1+t)}(g^{[p]}) \times h \in M_k(N, \chi, K; r) \tag{4}$$

for any $r \in B$ with $\mathrm{ord}_p(r) < 1/(p+1)$.

Note 2.3

(1) The above argument does not quite show that $H := d^{-(1+t)}(g^{[p]}) \times h$ lies in $M_k(N, \chi, \mathbb{Z}_p, \frac{1}{p+1})$ as for this one would need to replace "K" by "B" in (4). However, the author just *assumed* this was true, and this was not contradicted by our experiments; in particular, when one could relate the value of the Rankin p-adic L-function to the p-adic logarithm of a point on an elliptic curve, the relationship held to exactly the precision predicted by the algorithm. To be completely rigorous though one would have to carry out a detailed analysis of Darmon's argument and the constructions used by Coleman (and one may have to account for some extra logarithmic growth and loss of precision).

(2) It is helpful to notice that the map $\phi : (g, h) \mapsto e_{ord}(d^{-(1+t)}(g^{[p]}) \times h)$ is bi-linear in g and h. Thus one can compute $\phi((g, h))$ by first computing it on a product of bases for the spaces $\mathbf{S}_l(N, \chi_g)$ and $\mathbf{S}_m(N, \chi_h)$. This is useful when these spaces are defined over $\mathbb{Z}_p$ but the newforms themselves are defined over algebraic number fields which do not embed in $\mathbb{Z}_p$.

(3) The author implemented a number of different approaches to computing $c(f^{*(p)}, e_{ord}(H))$. The most straightforward is to compute matrices for the Hecke operators U_ℓ (for $\ell | Np$) and T_ℓ (otherwise) on the ordinary subspace for many small ℓ by explicitly computing on the q-expansion basis for the ordinary subspace output by Algorithm 2.1. One can then try to project onto the "$f^{*(p)}$-eigenspace" using any one of these matrices. One difficulty which arises is that congruences between eigenforms may force a small loss of p-adic precision during this step. (Congruences with Eisenstein series can be avoided for $k \geq 2$ by using classical methods to compute a basis for the ordinary cuspidal subspace, and working with that space instead.) We did not carry out a rigorous analysis of what loss of precision could occur due to these congruences, but in our examples it was never more than a few p-adic coefficients and one could always determine exactly what loss of precision had occurred after the experiment. The author understands from discussions with Wiles that one should be able to compute an "upper bound" on the p-adic congruences which can occur, and thus on the loss of precision. This bound of course is entirely independent of the precision m. However, such a calculation is beyond the scope of this paper.

2.3.3 Single and double product L-functions

The author understands that usual p-adic L-functions can be computed using our methods, by substituting Eisenstein series for newforms in the appropriate places in the triple product L-function, cf. [1, Section 3]. However, he has not looked at this application at all, as the methods based upon overconvergent modular symbols are already very good (for $k \geq 2$) [17]. One can similarly compute double product Rankin p-adic L-functions using our approach. In

particular, we have used our algorithm to compute a (suitably defined) Rankin double product p-adic L-function special value "$\mathcal{L}_p(\mathbf{f},\mathbf{g})(2,1)$" for f of weight 2 and g of weight 1, see the forthcoming [5] and also [7, Conjecture 10.1].

3 Examples

In this section we shall freely use the notation from [8, Section 1]. We implemented our basic algorithms in both Magma and Sage, but focussed our refinements on the former and all the examples we present here were computed using this package. The running time and space for the examples varied from around 100 seconds with 201 MB RAM (Example 3.4) to around 19000 seconds with 9.7 GB RAM (Example 3.3) on a 2.93 GHz machine.

All of the examples here are for weights k, l, m with $k = m-l+2$ and $t = l-2$, where $t = 0$, i.e., $l = 2$ and $k = m$ (and in fact $f = h$). We implemented our algorithm for arbitrary $t \geq 0$ and computed $\mathcal{L}_p(\mathbf{f},\mathbf{g},\mathbf{h})(k,l,m)$ in cases when $t > 0$; however, the author does not know of any geometric constructions of points when $t > 0$ (or even when $f \neq h$) and so we do not present these computations here.

We begin with an example of the explicit construction of rational points mentioned in our introduction, see Equation (1).

Example 3.1 Let $E_f : y^2 + y = x^3 - x^2 - 2x + 2$ be the rank 1 curve of conductor 57 with Cremona label "57a" associated to the cusp form

$$f := q - 2q^2 - q^3 + 2q^4 - 3q^5 + 2q^6 - 5q^7 + q^9 + \cdots .$$

We choose two other newforms of level 57 (associated to curves of rank zero):

$$\begin{array}{rcl} g_1 & := & q + q^2 + q^3 - q^4 - 2q^5 + q^6 - 3q^8 + q^9 - \cdots \\ g_2 & := & q - 2q^2 + q^3 + 2q^4 + q^5 - 2q^6 + 3q^7 + q^9 - \cdots . \end{array}$$

Taking $p := 5$ and writing $\mathbf{f}, \mathbf{g}_1, \mathbf{g}_2$ for the Hida families we compute the special values

$$\begin{array}{rcl} \mathcal{L}_5(\mathbf{g}_1,\mathbf{f},\mathbf{g}_1)(2,2,2) & \equiv & -260429402433721822483 \bmod 5^{30} \\ 5\mathcal{L}_5(\mathbf{g}_2,\mathbf{f},\mathbf{g}_2)(2,2,2) & \equiv & -279706401244025789341 \bmod 5^{31}. \end{array}$$

One computes that for each newform g_i, if one multiplies the operator of projection onto the g_i-eigenspace by 3 then one obtains an element in the integral (rather than rational) Hecke algebra. Thus equation (1) predicts that there exist global points $P_1, P_2 \in E_f(\mathbb{Q})$ such that

$$\log_{E_f}(P_i) = 6 \times \frac{\mathcal{E}_0(g_i)\mathcal{E}_1(g_i)}{\mathcal{E}(g_i,f,g_i)} \times \mathcal{L}_5(\mathbf{g}_i,\mathbf{f},\mathbf{g}_i).$$

One finds

$$\begin{array}{rcl} \log_{E_f}(P_1) & \equiv & 37060573996879427247 \times 5 \bmod 5^{30} \\ \log_{E_f}(P_2) & \equiv & -18578369245374641968 \times 5 \bmod 5^{30}. \end{array}$$

Adapting the method in [15, Section 2.7] we recover the points

$$P_1 \quad = \quad \left(-\tfrac{1976}{7569}, \tfrac{750007}{658503}\right) \quad = \quad -16P$$

and $P_2 = (0,1) = 4P$, where $P := (2,-2)$ is a generator for $E_f(\mathbb{Q})$.

Next we look at an example where the Darmon-Rotger formula may be applied, but the application to constructing points has not been fully worked out. (At least, at the time of author's computations — we understand from a personal communication from Darmon and Rotger that this has now been done.)

Example 3.2 Let $E_f : y^2+xy+y = x^3-x^2$ be the rank 1 curve of conductor 53 with Cremona label "53a" associated to the cusp form

$$f := q - q^2 - 3q^3 - q^4 + 3q^6 - 4q^7 + 3q^8 + 6q^9 + \cdots .$$

There is one newform g of level 53 and weight 4 and trivial character with rational Fourier coefficients:

$$g := q + q^3 - 8q^4 - 18q^5 + 2q^7 - 26q^9 + 54q^{11} + \cdots .$$

Taking $p := 7$ and writing $\mathbf{f}$ and $\mathbf{g}$ for the Hida families we compute the special value

$$\mathcal{L}_7(\mathbf{g},\mathbf{f},\mathbf{g})(4,2,4) \equiv -12581507765759084963366603 \bmod 7^{30}.$$

The Darmon-Rotger formula [8, Theorem 1.3] then predicts that

$$\mathrm{AJ}_7(\Delta)(\eta_g^{\mathrm{u-r}} \otimes \omega_f \otimes \omega_g) = \frac{\mathcal{E}_0(g)\mathcal{E}_1(g)}{\mathcal{E}(g,f,g)}\mathcal{L}_7(\mathbf{g},\mathbf{f},\mathbf{g})(4,2,4)$$

and we find that

$$\mathrm{AJ}_7(\Delta)(\eta_g^{\mathrm{u-r}} \otimes \omega_f \otimes \omega_g) \equiv 1025211670724558054729221 \times 7 \bmod 7^{30}.$$

Equation (1) does not apply in this setting, but one can hope that this equals $\log_{E_f}(P)$ for some point $P \in E_f(\mathbb{Q}) \otimes \mathbb{Q}$. Exponentiating one finds a point $\hat{P} = (x(\hat{P}), y(\hat{P})) \in E_1(\mathbb{Q}_7)$ with coordinates $7^2x(\hat{P})$, $7^3y(\hat{P})$ modulo 7^{30} (where $E := E_f$). We have $|E(\mathbb{F}_7)| = 12$ and translating $\hat{P}$ by elements $Q \in E(\mathbb{Q}_7)[12]$ we find exactly one rational point, $P = (0,-1)$ (see the method in [15, Section 2.7]). Thus we have computed a generator in a rather elaborate manner.

The author also considered again the curve E_f with Cremona label "57a" but took g to be the unique newform of level 57 and weight 4 with trivial character and rational Fourier coefficients, and found that $\mathrm{AJ}_5(\Delta)(\eta_g^{\mathrm{u-r}} \otimes \omega_f \otimes \omega_g) \equiv -\frac{15}{13}\log_{E_f}(P) \bmod 5^{31}$ for $P := (2,-2)$ a generator of $E_f(\mathbb{Q})$. (So here $p = k-1$, and we used the "twisted" version of the algorithm described in Note 2.2 (5).)

The next example has a similar flavour but involves cusp forms of odd weight.

Example 3.3 Let $E_f : y^2 + y = x^3 + x^2$ be the rank 1 curve of conductor 43 with Cremona label "43a" associated to the cusp form

$$f := q - 2q^2 - 2q^3 + 2q^4 - 4q^5 + 4q^6 + q^9 + 8q^{10} + 3q^{11} + \cdots .$$

Let χ be the Legendre character modulo 43. Then we find unique newforms $g \in S_3(43, \chi)$ and $h \in S_5(43, \chi)$ with rational Fourier coefficients:

$$\begin{array}{rcl} g & := & q + 4q^4 + 9q^9 - 21q^{11} + \cdots \\ h & := & q + 16q^4 + 81q^9 + 199q^{11} + \cdots . \end{array}$$

Taking $p := 11$ and writing $\mathbf{f}, \mathbf{g}$ and $\mathbf{h}$ for the Hida families we compute the special values

$$\begin{array}{rcl} \mathcal{L}_{11}(\mathbf{g}, \mathbf{f}, \mathbf{g})(3, 2, 3) & \equiv & -783131927094751000 9065871543799 \bmod 11^{30} \\ \mathcal{L}_{11}(\mathbf{h}, \mathbf{f}, \mathbf{h})(5, 2, 5) & \equiv & 47915605772751087905814144445515 \bmod 11^{30}. \end{array}$$

Using the Darmon-Rotger formula we compute

$$\mathrm{AJ}_{11}(\Delta)(\eta_g^{\mathrm{u-r}} \otimes \omega_f \otimes \omega_g) \equiv -64607327623075457821331812 5190 \times 11 \bmod 11^{30}.$$

Rather than attempt to recover a point from this, we take the generator $P = (0, 0)$ for $E_f(\mathbb{Q})$ and compute $\log_{E_f}(P)$ and then try to determine a relationship. One finds

$$\mathrm{AJ}_{11}(\Delta)(\eta_g^{\mathrm{u-r}} \otimes \omega_f \otimes \omega_g) \equiv \frac{258}{107} \log_{E_f}(P) \bmod 11^{30}.$$

(We checked that multiplying the relevant projection operator by 2×107 gives an element in the integral Hecke algebra.) Similarly we found

$$\mathrm{AJ}_{11}(\Delta)(\eta_h^{\mathrm{u-r}} \otimes \omega_f \otimes \omega_h) \equiv -\frac{6708}{5647} \log_{E_f}(P) \bmod 11^{30}.$$

The examples above suggest the construction in [10] can be generalised, at least in a p-adic setting.

We now look at some examples in which one removes one of the main conditions in the Darmon-Rotger theorem [8, Theorem 1.3] itself, that the prime does not divide the level. In each example rather than try to recover a rational point, we look for an algebraic relationship between the logarithm of a generator and the special value we compute.

Example 3.4 Let $E_f : y^2 + y = x^3 + 2x$ be the rank 1 curve of conductor 77 with Cremona label "77a" associated to the cusp form

$$f := q - 3q^3 - 2q^4 - q^5 - q^7 + 6q^9 - q^{11} + \cdots .$$

Let g be the level 11 and weight 2 newform (associated to a rank zero elliptic curve):

$$g := q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} + \cdots .$$

We take the prime $p := 7$, which divides the level of f, and writing $\mathbf{f}$ and $\mathbf{g}$ for the Hida families compute

$$\mathcal{L}_7(\mathbf{g},\mathbf{f},\mathbf{g})(2,2,2) \equiv -18615841040047343132294 93 \times 7 \bmod 7^{31}.$$

Taking the generator $P = (2,3)$ we compute $\log_{E_f}(P) \bmod 7^{31}$ and find that $\log_{E_f}(P)/7\mathcal{L}_7(\mathbf{g},\mathbf{f},\mathbf{g})(2,2,2)$ satisfies the quadratic equation $1600t^2+48t+9 = 0$ modulo 7^{29}.

The factor p which occurs in the expression relating the special value to the logarithm of a point when the prime divides the level is also seen in the next examples.

Example 3.5 Let $E_f : y^2 + xy + y = x^3 - 80x - 275$ and $E_g : y^2 + xy + y = x^3 - x^2 - 12x + 18$ be the rank 1 curves of conductor 469 with Cremona labels "469a" and "469b", respectively, associated to the cusp forms

$$\begin{aligned} f &:= q + q^2 + q^3 - q^4 - 3q^5 + q^6 - q^7 - 3q^8 - 2q^9 - 3q^{10} + \cdots \\ g &:= q - q^2 - 3q^3 - q^4 + q^5 + 3q^6 - q^7 + 3q^8 + 6q^9 - q^{10} + \cdots . \end{aligned}$$

Taking the prime $p := 7$ we compute

$$\begin{aligned} \mathcal{L}_7(\mathbf{g},\mathbf{f},\mathbf{g})(2,2,2) &\equiv 14354095458495109417838 17 \bmod 7^{30} \\ \mathcal{L}_7(\mathbf{f},\mathbf{g},\mathbf{f})(2,2,2) &\equiv 69154726390414601590953 63 \bmod 7^{30}. \end{aligned}$$

Using generators $P_f = (-5,4)$ and $P_g = (2,-1)$ for $E_f(\mathbb{Q})$ and $E_g(\mathbb{Q})$, respectively, we found

$$\begin{aligned} 7\mathcal{L}_7(\mathbf{g},\mathbf{f},\mathbf{g})(2,2,2) &\equiv 4\log_{E_f}(P_f) \bmod 7^{30} \\ 35\mathcal{L}_7(\mathbf{f},\mathbf{g},\mathbf{f})(2,2,2) &\equiv -16\log_{E_g}(P_g) \bmod 7^{30}. \end{aligned}$$

In the above example the "tame" level used in our computation was $N = 67 = \frac{469}{7}$. In the next example it is one: for tame level one the author's algorithm does not use the theory of modular symbols at all, cf. [16, Section 3.2].

Example 3.6 Let $E_f : y^2 + xy + y = x^3 + x^2 - x$ be the rank 1 curve of conductor 89 with Cremona label "89a" associated to the cusp form

$$f := q - q^2 - q^3 - q^4 - q^5 + q^6 - 4q^7 + 3q^8 - 2q^9 + q^{10} - 2q^{11} + \cdots .$$

Let g be the level 89 and weight 2 newform (associated to a rank zero elliptic curve):

$$g := q + q^2 + 2q^3 - q^4 - 2q^5 + 2q^6 + 2q^7 - 3q^8 + q^9 - 2q^{10} - 4q^{11} + \cdots .$$

Taking the prime $p := 89$ we found that

$$89\mathcal{L}_{89}(\mathbf{g},\mathbf{f},\mathbf{g})(2,2,2) \equiv 72\log_{E_f}(P) \bmod 89^{21}$$

where $P = (0, 0)$ is a generator.

The author understands that the above examples are consistent with ongoing work of Darmon and Rotger to generalise their formula to the situation in which the prime p does divide the level N [9].

References

[1] M. Bertolini and H. Darmon, Kato's Euler system and rational points on elliptic curves I: a p-adic Beilinson formula, submitted. Available at http://www.math.mcgill.ca/darmon/pub/pub.html

[2] R. Coleman, Classical and overconvergent modular forms, Invent. Math. 124, (1996), 251-241.

[3] R. Coleman, F. Gouvêa and N. Jochnowitz, E_2, Θ and overconvergence, International Mathematics Research Notices, No.1, (1995), 23-41.

[4] H. Darmon, M. Daub, S. Lichtenstein and V. Rotger, Algorithms for Chow-Heegner points via iterated integrals, submitted. Available at http://www.math.mcgill.ca/darmon/pub/pub.html

[5] H. Darmon, A.G.B. Lauder, V. Rotger, Chow-Heegner and Stark-Heegner points via p-adic iterated integrals, in progress.

[6] H. Darmon and R. Pollack, Efficient calculation of Stark-Heegner points via overconvergent modular symbols, Israel J. Math. 153, (2006), 319-354.

[7] H. Darmon and V. Rotger, Algebraic cycles and Stark-Heegner points, Arizona Winter School 2011. Available at http://www-ma2.upc.edu/vrotger/docs/AWS2011/aws.pdf

[8] H. Darmon and V. Rotger, Diagonal cycles and Euler systems I: A p-adic Gross-Zagier formula, submitted. Available at http://www.math.mcgill.ca/darmon/pub/pub.html

[9] H. Darmon and V. Rotger, Diagonal cycles and Euler systems II: p-adic families of cohomology classes, in progress.

[10] H. Darmon, V. Rotger and I. Sols, Iterated integrals, diagonal cycles and rational points on elliptic curves, submitted. Available at http://www.math.mcgill.ca/darmon/pub/pub.html

[11] M. Daub, Berkeley Ph.D. thesis, in progress.

[12] F. Q. Gouvêa, Arithmetic of p-adic modular forms (SLN 1304), Springer-Verlag, 1988.

[13] H. Hida, Elementary theory of L-functions and Eisenstein series, LMS Student Texts 26, Cambridge University Press, 1993.

[14] N.M. Katz, p-Adic properties of modular schemes and modular forms, in Modular Forms in One Variable III (SLN 350), Springer-Verlag, (1973), 69-190.

[15] M. Kurihara and R. Pollack, Two p-adic L-functions and rational points on elliptic curves with supersingular reduction, L-Functions and Galois Representations (Durham, 2007), LMS (LNS 320), Cambridge University Press, 300-332.

[16] A.G.B. Lauder, Computations with classical and p-adic modular forms, LMS J. Comput. Math. 14 (2011) 214-231.

[17] R. Pollack and G. Stevens, Overconvergent modular symbols and p-adic L-functions, Annales Scientifiques de l'Ecole Normale Superieure, Vol. 44 (1), 1-42, 2011.

[18] J.-P. Serre, Formes modulaires et fonctions zêta p-adiques, in Modular Forms in One Variable III (SLN 350), Springer-Verlag, (1973), 191-268.

[19] W. Stein, Modular Forms, a Computational Approach, Graduate Studies in Mathematics 79, AMS, 2007.