MATHEMATICS OF COMPUTATION
Volume 91, Number 334, March 2022, Pages 921–942
https://doi.org/10.1090/mcom/3678
Article electronically published on October 15, 2021

COMPUTING p-ADIC L-FUNCTIONS OF TOTALLY REAL FIELDS

ALAN LAUDER AND JAN VONK

Abstract. We describe an algorithm for computing p-adic L-functions of characters of totally real fields, using the Fourier expansions of diagonal restrictions of Hilbert modular forms.

1. Introduction

We describe an algorithm for computing p-adic L-functions of characters of totally real fields. Such p-adic L-functions were constructed in the 1970's independently by Barsky and Cassou-Noguès [Bar78, CN79] based on the explicit formula for zeta values of Shintani [Shi76] and by Serre and Deligne–Ribet [Ser73, DR80] using Hilbert modular forms and an idea of Siegel [Sie68] going back to Hecke [Hec24, Satz 3]. An algorithm for computing via the approach of Cassou-Noguès was developed by Roblot[1] [Rob15]. Our algorithm follows the approach of Serre and Siegel, and its computational efficiency rests upon a method for computing with p-adic spaces of modular forms developed in previous work by the authors.

The idea of our method is simple. In Serre's approach, the value of the p-adic L-function of a totally real field of degree d at a non-positive integer $1-k$ is interpreted as the constant term of a classical modular form of weight dk obtained by diagonally restricting a Hilbert Eisenstein series. For small values of k these constants can be computed easily using an idea of Siegel that goes back to Hecke. To compute the p-adic L-function at arbitrary points in its domain, to some finite p-adic precision, we use a method for computing p-adically with modular forms in larger weight developed in [Lau11, Von15]. We compute the required constant term in very large weight indirectly, by finding sufficiently many of its higher Fourier coefficients and using linear algebra to deduce the unknown constant term. Thus our approach is an algorithmic incarnation of Serre's approach to p-adic L-functions of totally real fields [Ser73], obtaining p-adic congruences between the constant terms of modular forms by studying their higher Fourier coefficients.

Our method is somewhat orthogonal to that of Roblot [Rob15] based on the "explicit formula" of Shintani [Shi76] that underlies also the related algorithms in

Received by the editor October 19, 2019, and, in revised form, January 30, 2021, and June 8, 2021.

2020 *Mathematics Subject Classification.* Primary 11R42, 11F41, 11Y40.

The second author was supported by Francis Brown and ERC-COG 724638 'GALOP', the Carolyn and Franco Gianturco Fellowship at Linacre College (Oxford), the Max-Planck-Institut für Mathematik (Bonn), and NSF Grant No. DMS-1638352 at the Institute for Advanced Study (Princeton), during various stages of this project.

[1]We mention also the unpublished algorithm of Charollois, based on cocycle relations for GL_n as in [CD14, CDG15] that is inspired by the approach via explicit formulae of Shintani that underlies Barsky/Cassou-Noguès.

[Das07, Sla07]. In spite of this, similarities arise in certain steps, as will be visible in the selection of instructive examples we illustrate our method with below. Our algorithmic contribution is as follows:

- In the general case, we take an approach similar to the one used by Cohen [Coh76]. We replace the calculations in level one in *loc. cit.* by the methods of [Lau11, Lau14] for computing p-adically with modular forms in large weights, obtaining the p-adic L-series by interpolation (see Cartier–Roy [CR73]) of p-adic approximations of classical L-values.
- In the real quadratic case, we present a far superior method that relies on the reduction theory of binary quadratic forms. When p is inert, the p-adic L-function has an exceptional zero, and the derivative is of great interest. We present an algorithm to compute this quantity directly, using the recent results of [DPV1] and the methods of [Lau11, Lau14].

The methods of [Lau11, Von15] were also used in the computation of p-adic L-values attached to modular forms and their double and triple Rankin products [Lau14]. The arithmetic invariants obtained in *loc. cit.* are of a very different nature, but in spite of these apparent differences, the current application follows exactly the same pattern, whereby the p-adic L-function is computed through its interpretation as a "twisted" triple product; see [DPV1] for more details.

1.1. **Definitions.** Let us fix some notation for the rest of this paper. We let F denote a totally real number field, with $[F:\mathbb{Q}] = d$, and $\{\sigma_1, \dots, \sigma_d\}$ the set of its d real embeddings. For any element $\alpha \in F$, we frequently use the abbreviation

$$\alpha_i := \sigma_i(\alpha) \in \mathbb{R}. \tag{1}$$

The ring of integers of F is denoted by $\mathcal{O}_F$, and its different ideal by $\mathfrak{d}$. For any ideal $\mathfrak{a} \lhd \mathcal{O}_F$, the set of totally positive elements contained in $\mathfrak{a}$ is denoted by $\mathfrak{a}_+$.

Let $\mathfrak{m} \lhd \mathcal{O}_F$ be a modulus, and denote the set of integral ideals of F coprime to $\mathfrak{m}$ by $\mathscr{I}_{F,\mathfrak{m}}$. The *narrow ray class group* $\mathrm{Cl}^+_{\mathfrak{m}}$ is the quotient of $\mathscr{I}_{F,\mathfrak{m}}$ by the relation

$$\mathfrak{a} \sim \mathfrak{b} \text{ if and only if } \mathfrak{a}\mathfrak{b}^{-1} = (\alpha)$$

for some totally positive α such that $v_{\mathfrak{q}}(\alpha - 1) \geq v_{\mathfrak{q}}(\mathfrak{m})$ for all primes $\mathfrak{q}$ dividing $\mathfrak{m}$. In this article we will consider ray class characters

$$\psi : \mathrm{Cl}^+_{\mathfrak{m}} \longrightarrow \overline{\mathbb{Q}}^{\times} \tag{2}$$

that are either *totally odd* or *totally even*. This means that for any $\alpha \in 1 + \mathfrak{m}$ we have

$$\begin{array}{rcll} \psi(\alpha) & = & \mathrm{sgn}(\mathrm{Nm}(\alpha)) & \text{if } \psi \text{ is totally odd,} \\ \psi(\alpha) & = & 1 & \text{if } \psi \text{ is totally even.} \end{array} \tag{3}$$

The L-series of ψ is defined for $\mathrm{Re}(s) > 1$ by the absolutely convergent expression

$$L(\psi, s) = \sum_{\mathfrak{a}} \psi(\mathfrak{a})\mathrm{Nm}(\mathfrak{a})^{-s}, \tag{4}$$

where the first sum is over all non-zero ideals of $\mathcal{O}_F$. The L-series meromorphically continues to all $s \in \mathbb{C}$, and is analytic outside $s = 1$. Let p be a prime number such that $(\mathfrak{m}, p) = 1$, the p-adic L-function $L_p(\psi\omega, s)$ for $s \in \mathbb{Z}_p$ is defined by the interpolation property

$$L_p(\psi\omega, n) = L(\psi\omega^n, n) \prod_{\mathfrak{p} \mid (p)} (1 - \psi\omega^n(\mathfrak{p})\mathrm{Nm}(\mathfrak{p})^{-n}) \tag{5}$$

for all integers $n \leq 0$, where ω is the p-adic Teichmüller character. The function $L_p(\psi\omega, s)$ defines an element of the field of fractions of the Iwasawa algebra $\Lambda_{\mathcal{O}}$; see §2.2. The explicit computation of this p-adic L-function is the subject of the rest of this article.

2. Diagonal restrictions of p-adic Eisenstein families

We now describe Hilbert Eisenstein series, their p-stabilisations, and their diagonal restrictions. These are central to our approach. A general algorithm, described in §3.2, reduces the computation of $L_p(\psi\omega, s)$ to a computation of the elementary higher Fourier coefficients of these diagonal restrictions.

2.1. **Hilbert Eisenstein series.** We begin by recalling some of the basic properties of Hilbert Eisenstein series attached to a character ψ of modulus $\mathfrak{m}$. Proofs are omitted, and may be found in Katz [Kat78, Section III]; see also Dasgupta–Darmon–Pollack [DDP11, Sections 2 and 3].

Suppose $k \geq 1$ is an integer, and assume that the character ψ is totally odd if k is odd, and totally even if k is even. Shimura [Shi78] defines the space

$$M_k(\mathfrak{m}, \psi) \tag{6}$$

of Hilbert modular forms of (parallel) weight k, level $\mathfrak{m}$ and character ψ. It consists of tuples of holomorphic functions, which we will refer to as its *components*, on the d-fold product of upper half-planes $\mathcal{H}^d$, indexed by the narrow class group of F, satisfying certain conditions. Each form has in particular a component associated to the class of $\mathfrak{d}^{-1}$, which is a holomorphic function $f : \mathcal{H}^d \to \mathbb{C}$ satisfying

$$(\mathrm{c}_1 z_1 + \mathrm{d}_1)^{-k} \cdots (\mathrm{c}_d z_d + \mathrm{d}_d)^{-k} f\left(\frac{\mathrm{a}_1 z_1 + \mathrm{b}_1}{\mathrm{c}_1 z_1 + \mathrm{d}_1}, \ldots, \frac{\mathrm{a}_d z_d + \mathrm{b}_d}{\mathrm{c}_d z_d + \mathrm{d}_d}\right) = \psi_f(\mathrm{a}) f(z), \tag{7}$$

for all matrices

$$\gamma = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_F) \quad \text{such that } \mathrm{c} \in \mathfrak{m}, \tag{8}$$

where $z = (z_1, \ldots, z_d)$ is the variable in $\mathcal{H}^d$, and ψ_f is the *finite part* of ψ, defined on any α coprime to $\mathfrak{m}$ by $\psi_f(\alpha) = \psi((\alpha))$ if ψ is totally even, and $\psi_f(\alpha) = \mathrm{sgn}(\mathrm{Nm}(\alpha))\psi((\alpha))$ if ψ is totally odd. The transformation law (7) implies that every Hilbert modular form has a component associated to the class of $\mathfrak{d}^{-1}$ with q-expansion indexed by the totally positive elements $\mathfrak{d}_+^{-1}$ of the inverse different.

In this paper, we exclusively use the very special examples given by Hilbert Eisenstein series, whose basic properties are discussed in Katz [Kat78]. More precisely, there exists a Hilbert modular eigenform

$$G_{k,\psi} \in M_k(\mathfrak{m}, \psi) \tag{9}$$

whose component associated to the class of $\mathfrak{d}^{-1}$ has q-expansion given by

$$G_{k,\psi}(z) = L(\psi, 1-k) + 2^d \sum_{\nu \in \mathfrak{d}_+^{-1}} \left(\sum_{\mathfrak{a} | (\nu)\mathfrak{d}} \psi(\mathfrak{a}) \mathrm{Nm}(\mathfrak{a})^{k-1} \right) q^\nu, \tag{10}$$

where we use the notation

$$q^\nu = \exp\left(2\pi i(\nu_1 z_1 + \nu_2 z_2 + \ldots + \nu_d z_d)\right) \tag{11}$$

with ν_i the image of ν under the i-th embedding $\sigma_i : F \hookrightarrow \mathbb{R}$. In the case where $k = 1$ and $\mathfrak{m} = (1)$, the constant term of (10) must be modified, but since we

will not need this case, we refer the interested reader to Dasgupta–Darmon–Pollack [DDP11, Proposition 2.11].

2.2. ***p*-Adic Eisenstein families.** In the approach to p-adic L-series pioneered by Serre, the necessary p-adic congruences between special values of the constant coefficients of Eisenstein series are inherited from congruences between the higher coefficients, which are of a more elementary nature. Just as the L-series needs to be modified by taking out its Euler factors at p, we will need to modify all the higher coefficients of the Eisenstein series.

First, let us fix some notation. Denote Δ for the torsion subgroup of $\mathbb{Z}_p^\times$. It is cyclic of order $\phi(\mathfrak{q})$, where $\mathfrak{q} = 4$ if $p = 2$, and $\mathfrak{q} = p$ otherwise. Let $\Lambda = \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$ be the Iwasawa algebra, and ω the p-adic Teichmüller character. Then we have isomorphisms

$$\begin{array}{ccccccc} \mathbb{Z}_p^\times & \xrightarrow{\sim} & \Delta \times (1+\mathfrak{q}\mathbb{Z}_p), & & a & \longmapsto & (\omega(a), \langle a \rangle), \\ \Lambda & \xrightarrow{\sim} & \mathbb{Z}_p[\Delta][\![T]\!], & & 1+\mathfrak{q} & \longmapsto & 1+T. \end{array} \tag{12}$$

We define a Λ-*adic Hilbert modular form* of level $\mathfrak{m}$ and character ψ to be an element of the ring $\mathrm{Frac}(\Lambda_{\mathcal{O}}) \otimes_{\Lambda_{\mathcal{O}}} \Lambda_{\mathcal{O}}[\![q]\!]$, such that its specialisation at the ideal

$$\mathfrak{I}_k = \left(1 + T - (1+\mathfrak{q})^{1-k}\right) \tag{13}$$

is the q-expansion at infinity of a form in $M_k(\mathfrak{m}(p), \psi\omega^{1-k})$, for $k \in \mathbb{Z}$ sufficiently large. Here, $\mathcal{O}$ is the ring of integers in a finite extension of $\mathbb{Q}_p$ containing the values of the character ψ, and $\Lambda_{\mathcal{O}} \simeq \mathcal{O}[\![T]\!]$.

The prototypical example of a Λ-adic Hilbert modular form is the family of Eisenstein series $\mathcal{G}_\psi$; see [DDP11, Proposition 3.2]. Its specialisation at $\mathfrak{I}_k$ is the *ordinary p-stabilisation* of the Eisenstein series $G_{k,\psi}$ from §2.1, whose component associated to the class of $\mathfrak{d}^{-1}$ has q-expansion

$$G_{k,\psi}^{(p)}(z) = L_p(\psi\omega, 1-k) + 2^d \sum_{\nu \in \mathfrak{d}_+^{-1}} \left(\sum_{\substack{\mathfrak{a} \mid (\nu)\mathfrak{d} \\ (\mathfrak{a}, p) = 1}} \psi(\mathfrak{a}) \langle \mathrm{Nm}(\mathfrak{a}) \rangle^{k-1} \right) q^\nu. \tag{14}$$

2.3. **Diagonal restrictions.** Suppose that we are given a Hilbert modular form in $M_k(\mathfrak{m}, \psi)$ whose component associated to the class of $\mathfrak{d}^{-1}$ is $f : \mathcal{H}^d \to \mathbb{C}$. Its *diagonal restriction* is the restriction of f to the diagonally embedded copy of the upper half plane in $\mathcal{H}^d$. By the transformation property (7), this procedure yields a one-variable (i.e. elliptic) modular form of weight dk. It is of level M, where M is the positive generator of $\mathbb{Z} \cap \mathfrak{m}$, and its character Ψ is obtained by restriction of the finite part ψ_f of ψ:

$$\Psi : (\mathbb{Z}/M\mathbb{Z})^\times \hookrightarrow (\mathcal{O}_F/\mathfrak{m})^\times \xrightarrow{\psi_f} \overline{\mathbb{Q}}^\times. \tag{15}$$

When applied to the Eisenstein series $G_{k,\psi}^{(p)}$ of level $\mathfrak{m}(p)$ and nebentype $\psi\omega^{1-k}$ introduced in §2.2, we obtain a diagonal restriction of level Mp, and weight dk. Its q-expansion is given by

$$\Delta_{k,\psi}^{(p)}(q) = L_p(\psi\omega, 1-k) + 2^d \sum_{n \geq 1} \left(\sum_{\substack{\nu \in \mathfrak{d}_+^{-1} \\ \mathrm{Tr}(\nu) = n}} \sum_{\substack{\mathfrak{a} \mid (\nu)\mathfrak{d} \\ (\mathfrak{a}, \mathfrak{m}(p)) = 1}} \psi(\mathfrak{a}) \langle \mathrm{Nm}(\mathfrak{a}) \rangle^{k-1} \right) q^n. \tag{16}$$

The n-th Fourier coefficient a_n of the diagonal restriction (16) may be written as

$$a_n = 2^d \sum_{\mathcal{C}\in \mathrm{Cl}_{\mathfrak{m}}^+} \psi(\mathcal{C}) \sum_{(\mathfrak{a},\nu)\ \in\ \mathbb{I}(n,\mathcal{C})_{\mathfrak{m}(p)}} \langle \mathrm{Nm}(\mathfrak{a})\rangle^{k-1}, \tag{17}$$

where we define the index set by

$$\mathbb{I}(n,\mathcal{C})_{\mathfrak{b}} := \left\{ (\mathfrak{a},\nu) \in \mathscr{I}_{F,\mathfrak{m}} \times \mathfrak{d}_+^{-1} \ : \ \begin{array}{ll} \mathrm{Tr}(\nu) = n, & \mathfrak{a} \,|\, (\nu)\mathfrak{d} \\ (\mathfrak{a},\mathfrak{b}) = 1, & [\mathfrak{a}] = \mathcal{C} \end{array} \right\}. \tag{18}$$

An important feature of a_n is that the index set $\mathbb{I}(n,\mathcal{C}) = \mathbb{I}(n,\mathcal{C})_{\mathfrak{m}(p)}$ in the sum (17) is independent of k, and the dependence on k of the terms in the sum is of a very elementary nature. In explicit computations, this makes it easy to efficiently compute the higher Fourier coefficients a_n for a great multitude of different weights k, once the sets $\mathbb{I}(n,\mathcal{C})$ have been computed.

3. Computing p-adic L-functions of totally real fields

We now present the general method to compute p-adic L-functions for totally real fields.

3.1. **The method of Klingen–Siegel.** Following an idea of Hecke [Hec24, Satz 3], Klingen–Siegel [Kli62, Sie68] use diagonal restrictions to show the rationality of special values $L(\psi, 1-k)$, and to give explicit closed formulae for some small values of k. For instance, they showed that

$$\zeta_F(-1) = \frac{1}{60} \sum_{\substack{b < \sqrt{D} \\ b \equiv D \pmod 2}} \sigma_1\left(\frac{D-b^2}{4}\right) \tag{19}$$

when $F = \mathbb{Q}(\sqrt{D})$ is real quadratic. The key idea is to use the fact that the diagonal restrictions of Hilbert Eisenstein series are elliptic modular forms. Computing a $\mathbb{Q}$-basis of q-expansions for the space of elliptic modular forms of the appropriate weight and level, we can determine the diagonal restriction as a linear combination, with rational coefficients, of the basis elements using only the higher coefficients. The constant coefficient, necessarily a rational number, is then also determined. This idea is perhaps best illustrated with an explicit example:

Example 3.1. Suppose $F = \mathbb{Q}(\sqrt{89}$; then $(5) = \mathfrak{p}\mathfrak{p}'$ splits. We have that

$$\mathrm{Cl}_{\mathfrak{p}}^+ \simeq \mathbb{Z}/4\mathbb{Z} \tag{20}$$

so there is a unique quadratic character ψ of conductor $\mathfrak{p}$ that is totally even. Then $5\mathbb{Z} = \mathbb{Z} \cap \mathfrak{p}$, and the restriction of ψ to $(\mathbb{Z}/5\mathbb{Z})^\times$ is the character $\left(\frac{5}{\cdot}\right)$. We compute that the space

$$M_4\left(\Gamma_1(5), \left(\frac{5}{\cdot}\right)\right) \tag{21}$$

is 2-dimensional, and has a basis of the form

$$\left\{ \begin{array}{lllllllll} f_1 = & 1 & & - & 14q^2 & - & 52q^3 & + & \ldots, \\ f_2 = & & q & + & 7q^2 & + & 26q^3 & + & \ldots. \end{array} \right. \tag{22}$$

On the other hand, we compute that the diagonal restriction of $G_{k,\psi}$ for $k = 2$ is

$$\Delta_{2,\psi} = \ L(\psi,-1) \ + \ 24q - 168q^2 - 624q^3 + \ldots \tag{23}$$

which, by inspection of the coefficients of q and q^2, must be equal to the linear combination $24f_1+24f_2$ of the basis elements above. It follows that $L(\psi,-1)=24$.

3.2. **An algorithm to compute p-adic L-functions.** To compute the p-adic L-series $L_p(\psi\omega^r,T)$ for general totally real fields, we elaborate on the above idea of Siegel to find its value at sufficiently many weights k and then use finite differences for interpolation. We now outline the main algorithm, and in the next section we discuss some efficient methods for carrying out the various steps.

Remark 3.2. For simplicity, we will assume that $L_p(\psi\omega^r,T)$ is an element of $\mathcal{O}[\![T]\!]$, which is automatic whenever the field cut out by $\psi\omega^r$ is not contained in the cyclotomic $\mathbb{Z}_p$-extension of F. If this fails,[2] some poles of an elementary nature may be present, and one needs to suitably modify the statements below. Since this modification is entirely straightforward, and would only cloud the explanation of the algorithm, we thought it appropriate to exclude this case from the discussion. See Example 4.7, where $\psi\omega^r=1$.

We use finite differences to interpolate special values at integer weights, to compute the p-adic L-series

$$L_p(\psi\omega^r,s),\quad r\in\mathbb{Z}$$

as a power series in $\mathcal{O}[\![s]\!]/(p^m)$ for any p-adic precision m, with respect to the variable $s=1-k$ in $\mathbb{Z}_p$. We obtain a power series for every residue class of r modulo $(p-1)$, and the interpolation only involves integers k in a fixed residue class modulo $(p-1)$. For a discussion of this interpolation, see Cartier–Roy [CR73]. Since $L_p(\psi\omega^r,T)$ belongs to $\mathcal{O}[\![T]\!]$ and $T=(1+q)^s-1$, the series $L_p(\psi\omega^r,s)$ mod p^m is in fact a polynomial of degree at most δ_m, where δ_m is the smallest integer such that

$$\begin{array}{lll}(p\neq 2) & i-v_p(i!)\geq m & \text{for all } i\geq\delta_m+1,\\ (p=2) & 2i-v_p(i!)\geq m & \text{for all } i\geq\delta_m+1,\end{array}\tag{24}$$

see Serre [Ser73, Théorème 13]. (Note that $\delta_m\leq\frac{p-1}{p-2}m$ when $p\neq 2$, and $\delta_m\leq m$ when $p=2$.) Thus it will be sufficient to evaluate this polynomial at δ_m+1 points and use interpolation. For each fixed $2\leq k_0\leq p$, we shall choose interpolation points

$$\begin{array}{lll}(p\neq 2) & k_j:=k_0+j(p-1) & \text{for } 0\leq j\leq\delta_m,\\ (p=2) & k_j:=k_0+2j & \text{for } 0\leq j\leq\delta_m,\end{array}\tag{25}$$

as this will give us smallest possible interpolating weights $d(k_0+j(p-1))$ (respectively $d(k_0+2j)$).

Algorithm 3.3. *Our input is:*

- k_0 *- an integer in* $\{2,\dots,p\}$,
- ψ *- a character of* F *of modulus* $\mathfrak{m}$*, with the same parity as* k_0,
- p *- an odd prime number,*
- m *- a natural number.*

[2]This can happen when $\psi\omega^r$ is of *type W*, in the terminology of Greenberg; see [Wil90].

The following algorithm computes the power series $L_p(\psi\omega^{k_0}, s)$ as an element of the ring $\mathcal{O}[\![s]\!]/(p^m)$.

(1) *Let M, Ψ be as in* (15)*, and define k_j as in* (25) *for all $0 \le j \le \delta_m$ with δ_m as in* (24)*. Let S be the Sturm bound for the space of classical modular forms of weight dk_{δ_m} and level $\Gamma_1(M)$. Compute a $\mathbb{Z}$-basis up to precision* $(\mathrm{mod}\ p^{\delta_m+1}, q^S)$ *for each of the classical spaces of modular forms*

$$M_{dk_j}(\Gamma_1(M)), \qquad 0 \le j \le \delta_m.$$

(2) *For all $1 \le n \le S-1$, compute the index sets*

$$X_n = \bigcup_{\mathcal{C} \in \mathrm{Cl}_{\mathfrak{m}}^+} \mathbb{I}(n, \mathcal{C})_{\mathfrak{m}},$$

where $\mathbb{I}(n, \mathcal{C})_{\mathfrak{m}}$ was defined in (18)*.*

(3) *For every k_j compute to precision p^{δ_m+1} the q-series*

$$\Delta_j^{\ge 1}(q) := 2^d \sum_{n=1}^{S-1} \left(\sum_{(\mathfrak{a},\nu) \in X_n} \psi(\mathfrak{a}) \mathrm{Nm}(\mathfrak{a})^{k_j - 1} \right) q^n.$$

(4) *For every k_j find the unique $L_j \in \mathbb{Z}_p/(p^m)$ such that $L_j + \Delta_j^{\ge 1}(q)$ is a linear combination of the basis elements of $M_{dk_j}(\Gamma_1(M))$ modulo (p^{δ_m+1}, q^S). Then compute*

$$L_j^{(p)} = L_j \times \prod_{\mathfrak{p} \mid (p)} (1 - \psi(\mathfrak{p}) \mathrm{Nm}(\mathfrak{p})^{k_j - 1}).$$

(5) *Interpolate the $\delta_m + 1$ values $L_j^{(p)}$, and output the resulting polynomial*

$$L_p(\psi\omega^{k_0}, s) \in \mathcal{O}[s] \bmod p^m.$$

Remark 3.4. There will be a precision loss of $\mathrm{ord}_p(\delta_m!)$ during the interpolation in Step (5), and one observes by the minimality of δ_m that $\delta_m + 1 = m + \mathrm{ord}_p((\delta_m+1)!)$ and so it is sufficient to taking working precision

$$m + \mathrm{ord}_p(\delta_m!) \le m + \mathrm{ord}_p((\delta_m + 1)!) = \delta_m + 1$$

in the earlier steps. Furthermore, it is possible there may be some precision loss during the linear algebra in Step (4), but this seems difficult to quantify in a useful way a priori and did not occur in examples we computed. Such additional loss would be detected during the computation by any computer algebra system that can work with p-adic numbers, and can be clearly indicated alongside the output.

For $p = 2$ the algorithm works as stated, *except* that there is a more dramatic precision loss in the interpolation step. In the examples for $p = 2$ that appear below, we used exact arithmetic instead.

3.3. **An explicit example.** We now illustrate this algorithm on a somewhat arbitrary choice of cubic field F, for the 7-adic L-function of a certain quadratic character of F. Letting $a \in \mathbb{R}$ satisfy the equation

$$a^3 - 3a - 1 = 0, \tag{26}$$

we find $F = \mathbb{Q}(a)$ is a totally real cubic extension of $\mathbb{Q}$. We compute that its ring of integers is $\mathcal{O}_F = \mathbb{Z}[a]$, and its different ideal is $\mathfrak{d} = (3a^2 - 3)$, such that every

element of $\mathfrak{d}^{-1}$ is of the form

$$\nu = \frac{x + ya + za^2}{3a^2 - 3}, \tag{27}$$

for some triple of integers x, y, z. We compute that $\mathrm{Tr}(\nu) = z$, and by calculating all the real embeddings to sufficient accuracy, of which we only include a few digits here for the purpose of readability, it follows that the elements of $\mathfrak{d}_+^{-1}$ of trace $n \geq 1$ are those with $z = n$ and x, y satisfying the conditions

$$\begin{cases} (0.1316\ldots)x & + & (0.2474\ldots)y & > & -n(0.4650\ldots), \\ (-0.3791\ldots)x & + & (0.1316\ldots)y & > & -n(0.0457\ldots), \\ (0.2474\ldots)x & + & (-0.3791\ldots)y & > & n(0.5807\ldots). \end{cases} \tag{28}$$

For any fixed $n \geq 1$, there are a finite number of solutions in $x, y \in \mathbb{Z}$ that may easily be computed by a box search for the smallest box containing the triangle in the (x, y)-plane determined by the inequalities displayed in the system (28).

Since $\mathrm{Cl}_{(5)} \simeq \mathbb{Z}/2\mathbb{Z}$, there is a unique non-trivial totally even character ψ of modulus $\mathfrak{m} = (5)$. We shall compute the p-adic L-series $L_p(\psi\omega^2, s)$ for $p = 7$ using an interpolation corresponding to integer weights k in the residue disk $k \equiv 2 \pmod{p-1}$. Here we note that the prime 7 is inert in K. We take $m := 22$ which gives the precision bound $\delta_m = 24$.

First we compute, for all $k_j = 2 + j(p-1)$ and $0 \leq j \leq 24$, bases for all the classical spaces

$$M_{3k_j}(\Gamma_0(5), \Psi)$$

consisting of q-expansions modulo $(7^{25}, q^{221})$. Here Ψ is the quadratic character of conductor 5. We used methods developed originally in [Lau11, Lau14]. It takes 5 seconds (computing these bases with exact coefficients using built-in Magma functions would take far longer).

Next, using the description of the set $\mathfrak{d}_+^{-1}$ above, we find the diagonal restrictions in weights k_j for $0 \leq j \leq 24$, respectively. We compute each series modulo q^{221} with exact rational coefficients (in time around 20 hours) and find

$$\begin{aligned} \Delta_0 &= L_0 + 8q + 184q^2 - 3472q^3 + 8664q^4 + 2312q^5 + \ldots, \\ \Delta_1 &= L_1 - 17464q + 48344125048q^2 + 77708960940464q^3 + \ldots, \\ \Delta_2 &= L_2 - 12754552q + 7783511850531843064q^2 + \ldots, \\ \Delta_3 &= L_3 - 9298091704q + 13817406003683602595506978 48q^2 + \ldots, \\ \Delta_4 &= L_4 - 6778308875512q + 25817261000989696227095010854660 2744q^2 + \ldots \\ &\vdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \end{aligned} \tag{29}$$

Now with some linear algebra and in around 3 seconds we determine the unknown constant terms L_j modulo 7^{25}.

$$\begin{aligned} L_0 &= -584/5 && \bmod 7^{25}, \\ L_1 &= 644239567957910044930 && \bmod 7^{25}, \\ L_2 &= 225053170195735060254 && \bmod 7^{25}, \\ L_3 &= 1230313269957772629193 && \bmod 7^{25}, \\ L_4 &= 64562798735766423256 && \bmod 7^{25} \\ &\vdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \end{aligned} \tag{30}$$

Interpolating via finite differences, we recover the p-adic L-series, in 0.01 seconds. The (small) loss of precision is kept track of by Magma, and is different for different

coefficients. One obtains a polynomial $L_7(\psi\omega^2, s)$ in s correct modulo 7^{22} and of degree 24, or alternatively

$$L_7(\psi\omega^2, T) = a_0 + a_1 T + a_2 T^2 + \dots$$

in the variable $T = (1+p)^s - 1$, where we find that the coefficients are

n	a_n	n	a_n	n	a_n
0	$64051811381829232449 4 + O(7^{25})$	8	$577517728950 + O(7^{15})$	16	$-6305 \cdot 7 + O(7^6)$
1	$3887031393600245265 + O(7^{23})$	9	$11864601963 + O(7^{13})$	17	$-6919 + O(7^5)$
2	$50242117330833221 + O(7^{21})$	10	$3960164051 + O(7^{12})$	18	$-901 + O(7^4)$
3	$-5393000767479996 + O(7^{19})$	11	$726383669 + O(7^{11})$	19	$108 + O(7^3)$
4	$(27444039407382 + O(7^{18})$	12	$94492019 + O(7^{10})$	20	$-73 + O(7^3)$
5	$12031218045488 + O(7^{17})$	13	$-1830411 \cdot 7 + O(7^9)$	21	$1 + O(7)$
6	$-10194883759927 + O(7^{16})$	14	$1262600 + O(7^9)$		
7	$-2363998044292 + O(7^{15})$	15	$-385206 + O(7^7)$		

Note that this shows in particular that the λ-invariant and the μ-invariant are both zero.

It is evident that all the time in this computation is taken up in computing the higher Fourier coefficients of the modular forms, for which in our cubic example we are using the crudest approach. We solve this algorithmic problem though for quadratic fields in the next section.

3.4. **Comments on implementation.** We now take a more detailed look at the most important steps of the algorithm of the previous section, and their implementation and performance.

a. Bases in high weights. An important step is to compute bases for the classical spaces

$$M_j := M_{d(k_0+j(p-1))}(\Gamma_1(M)) \qquad \bmod (p^{\delta_m+1}, q^s). \tag{31}$$

The practical problem of computing bases for the classical spaces M_j in step (1) has been addressed by the first author [Lau11]; a very similar problem arises when one computes with overconvergent modular forms.

In level 1, corresponding to the case of trivial conductor, it is extremely fast in practice due to the existence of the *Miller basis* [Ste07, Lemma 2.20]. In higher level an elaborate but fast method has been developed and improved over several years, originally for use in the computations underlying [DLR]. We shall not discuss it here except to say it involves computing bases in *low* weight via modular symbols and multiplication of forms. To give a sense of how this part of the algorithm scales, undertaking this step in the cubic example above with working precision increased from 7^{25} to 7^{50} pushes the time up from 5 seconds to around 40 seconds. With precision 7^{75} it is around 200 seconds. The latter computation involves finding bases for 75 different spaces of modular forms of weight up to 1338 working modulo 7^{75} and q^{671}.

Remark 3.5. A more direct computation of the quantities $L_j^{(p)}$ would take place in level Mp, but it is more efficient to work in level M and compute instead L_j. This way, the classical spaces of forms that need computing have dimensions that are smaller by a factor of roughly $(p+1)$.

As seen from the cubic example treated in §3.3, finding the higher Fourier coefficients takes the bulk of the running time in practice in this, most general, version of the algorithm. The total running time in the cubic example was in the order of 20 hours, of which all but a few seconds were spent on this step.

b. The inverse different. Step (2) requires us to find an explicit description of the elements $\nu \in \mathfrak{d}_+^{-1}$ of trace n, for $1 \leq n \leq s-1$. To do this, one first computes a $\mathbb{Z}$-basis of the ring of integers $\mathcal{O}_K$ and its dual basis for $\mathfrak{d}^{-1}$. Then one computes the finite set of elements determined by the condition $\mathrm{Tr}(\nu) = n$ and the system of inequalities obtained from the total positivity conditions, by a simple enumeration just as we did in §3.3. This becomes laborious as $[F : \mathbb{Q}]$ grows, since

$$|\{\nu \in \mathfrak{d}_+^{-1} \,:\, \mathrm{Tr}(\nu) = n\}| \;\sim\; n^{[F:\mathbb{Q}]-1},$$

where the implicit constant depends on the 'shape' of the number field F. Finally, for step (3) we compute $\mathrm{Nm}(I)$ and $\psi(I)$ for the ideal divisors of all the ideals $(\nu)\mathfrak{d}$ using well-established methods. Once this is computed, simple linear algebra determines the constants L_j for all required j in negligible time.

Regarding the complexity, it is difficult to give an overall estimate on this because our algorithm relies in part on methods for computing bases of spaces of modular forms (in low weight) using modular symbols. The complexity of such algorithms does not appear to have been documented in the literature, though they are polynomial-time in input parameters such as the level and q-adic precision required. Our algorithm is certainly though polynomial-time in both the prime p and precision m, as well as the absolute value of the discriminant of the field and norm of the conductor, and exponential in the field degree.

Remark 3.6. The reader may wonder how this general version of the algorithm compares to the work of Roblot [Rob15]. We make a few comments in the following cases:

- $[F : \mathbb{Q}] = 2$: The algorithm of [Rob15] is illustrated with one example in [Rob15, § 6] for $F = \mathbb{Q}(\sqrt{5})$ where the computation of a 7-adic L-function to precision $O(7^{12})$ is reported to take about 35 minutes. Using the most general algorithm in §3.2, not making any of the simplifications for the quadratic case discussed in §4, we obtain the similar running time of 31 minutes.

  However, we give a much more efficient approach in the quadratic case in §4, for arbitrary ring class characters, using reduction theory for binary quadratic forms to efficiently perform step (2). An additional significant advantage is provided by the fact that we can compute directly the sets $\mathbb{I}(n, \mathcal{C})$ for every class $\mathcal{C}$ separately, and not just their union X_n. This then further eliminates the need to evaluate the character ψ on every element of X_n separately in step (3), causing additional savings in running time. To illustrate the scope of the improvement, consider the example

  $$F = \mathbb{Q}(\sqrt{401})$$

  which has class group $\mathrm{Cl}_F = \mathbb{Z}/5\mathbb{Z}$. Computing the 13-adic L-functions to precision $O(13^{45})$ for all the characters of Cl_F, we obtained the following timings for the Fourier coefficients of the diagonal restrictions, which is the bottleneck of our algorithm: **7748.25** seconds with the general degree algorithm of §3.2, versus **9.35** seconds with the real quadratic methods of §4.
- $[F : \mathbb{Q}] > 2$: In this case we could not compare our method to that of Roblot. It is stated in [Rob15, § 1] that the computation of Shintani cone decompositions [Rob15, § 5.4] is at present not practical in general degree,

and no examples are given. A non-constructive proof of the existence of cone decompositions was given by Cassou-Noguès [CN79, Lemma 1], but recently Diaz y Diaz and Friedman [DDF14] and Charollois–Dasgupta–Greenberg [CDG15] explicitly constructed *signed* Shintani cones. It would be very interesting to use these ideas to implement a practical algorithm using the methods of [Rob15], and compare its performance to our algorithm in explicit examples.

4. Real quadratic fields: Ideals and RM points

We now suppose that F is a real quadratic field, and show how we can improve the efficiency of the computations in steps (2) and (3) of Algorithm 3.3 in §3.2. The higher Fourier coefficients (17) will be computed in terms of a certain set of 'RM points' that may be computed efficiently via reduction theory of binary quadratic forms. To this end, we extend some results that are contained in an article of the second named author with Henri Darmon and Alice Pozzi [DPV1].

Notation. Henceforth, F is a real quadratic field, and

$$\psi : \mathrm{Cl}_D^+ \longrightarrow \mathbb{C}_p^\times \tag{32}$$

is a ring class character of discriminant $D > 0$. The *conductor* $f > 0$ is defined by writing $D = f^2 D_0$ where D_0 is a fundamental discriminant. If $\mathcal{C}$ is a class in Cl_D^+, we denote as before

$$\mathbb{I}(n, \mathcal{C})_f := \left\{ (\mathfrak{a}, \nu) \in \mathscr{I}_{F,(f)} \times \mathfrak{d}_+^{-1} \ : \ \begin{array}{ll} \mathrm{Tr}(\nu) = n, & \mathfrak{a} \,|\, (\nu)\mathfrak{d} \\ (\mathfrak{a}, (f)) = 1, & [\mathfrak{a}] = \mathcal{C} \end{array} \right\}. \tag{33}$$

4.1. **The higher coefficients of diagonal restrictions.** We begin by putting the index set $\mathbb{I}(n, \mathcal{C})_f$ in bijection with a certain set of 'RM points' endowed with additional data. We say $\tau \in \mathbb{C}$ is a RM point if it satisfies a primitive quadratic equation

$$a\tau^2 + b\tau + c = 0, \qquad a, b, c \in \mathbb{Z}, \quad b^2 - 4ac = D \tag{34}$$

with positive non-square discriminant $D > 0$. An RM point τ of discriminant D determines the integers a, b, c uniquely if we demand in addition that

$$\tau = \frac{-b + \sqrt{D}}{2a}, \tag{35}$$

i.e. τ is the *stable*[3] root of the quadratic equation. We write $a(\tau)$ for the uniquely determined integer a. Every RM point τ has a unique algebraic conjugate, which we denote by τ'. Finally, if $\mathcal{C} \in \mathrm{Cl}_D^+$ is an ideal class, then it is represented by the fractional ideal $(1, \tau)$ coprime to the conductor f, for some RM point τ. In this case, we write $[\tau] = \mathcal{C}$.

Choose two sets of representatives $M_n \supseteq N_n$ such that

$$\{A \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}) \ : \ \det(A) = n\} = \bigsqcup_{\gamma_n \in M_n} \mathrm{SL}_2(\mathbb{Z}) \cdot \gamma_n \tag{36}$$

$$= \bigsqcup_{\delta_n \in N_n} \mathrm{SL}_2(\mathbb{Z}) \cdot \delta_n \cdot \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\tau). \tag{37}$$

[3]This terminology is explained by the fact that the quadratic equation has a distinguished generator for its stabiliser in $\mathrm{SL}_2(\mathbb{Z})$, which is usually called its *automorph*, for which τ is a stable fixed point.

For instance, it is classical that we may choose the following set M_n

$$M_n = \left\{ \begin{pmatrix} n/d & j \\ 0 & d \end{pmatrix} : \qquad d|n, \quad (d, n/d) = 1, \quad 0 \leq j \leq d-1 \right\}. \tag{38}$$

Now define the set of 'augmented' RM points of discriminant $n^2 D$ by

$$\mathbb{RM}(n,\tau)_f := \left\{ (w, \delta_n) \ : \ \begin{array}{cc} \delta_n \in N_n, & w \in \mathrm{SL}_2(\mathbb{Z})\delta_n \tau \\ w > 0 > w', & (a(w), f) = 1 \end{array} \right\}. \tag{39}$$

Lemma 4.1 appears in [DPV1] in the case $f = 1$, but is easily extended to general, not necessarily fundamental, discriminants D by the same argument.

Lemma 4.1. *Suppose that $[\tau] = \mathcal{C}$; then there exists a bijection*

$$\mathbb{I}(n, \mathcal{C})_f \ \longrightarrow \ \mathbb{RM}(n,\tau)_f$$

such that if $(\mathfrak{a}, \nu)$ corresponds to (w, δ_n), then $\mathrm{Nm}(\mathfrak{a}) = a(w)$.

Proof. Let A, B and $C = (B^2 - D)/4A$ be integers with no common divisor such that

$$\tau = \frac{-B + \sqrt{D}}{2A} \tag{40}$$

and define the integral ideal $I = (A, A\tau)$, whose class in Cl_D^+ is equal to $\mathcal{C}$. Suppose that $(\mathfrak{a}, \nu) \in \mathbb{I}(n, \mathcal{C})_f$; then $\mathfrak{a}\mathfrak{b} = (\nu)\mathfrak{d}$ for some integral ideal $\mathfrak{b} \lhd \mathcal{O}_F$. Define the RM point w by

$$w = \frac{-b + n\sqrt{D}}{2a}, \tag{41}$$

where the integers a, b, c are defined by

$$\left\{ \begin{array}{rcl} a & = & \mathrm{Nm}(\mathfrak{a}), \\ \nu & = & (-b + n\sqrt{D})/2\sqrt{D}, \\ c & = & -\mathrm{Nm}(\mathfrak{b}). \end{array} \right. \tag{42}$$

Then we see that $w > 0 > w'$ and $a = a(w)$ is coprime to f. Note also that $b^2 - 4ac = n^2 D$. Consider the ideal $\mathrm{Nm}(\mathfrak{a})\mathfrak{a}^{-1} I$. It represents the trivial class in Cl_D^+, and is hence generated by an element λ in $\mathbb{Z} + f\mathcal{O}_F$ that is totally positive. Now define the lattice

$$\Lambda = \mathbb{Z}\lambda + \mathbb{Z}w\lambda \tag{43}$$

which is well defined up to multiplication by a totally positive unit in $\mathcal{O}_F^\times \cap (\mathbb{Z} + f\mathcal{O}_F)$, i.e. a unit that is congruent to an integer modulo f. We claim that Λ is a lattice in I of index n. Clearly, $\lambda \in I$. We also have $w\lambda \in I$ since

$$\begin{aligned} (w\lambda) &= (\nu\sqrt{D}/\mathrm{Nm}(\mathfrak{a}))(\mathrm{Nm}(\mathfrak{a})/\mathfrak{a})I \\ &= \mathfrak{b}I. \end{aligned}$$

The quadratic form $\mathrm{Nm}(\lambda x - \lambda w y)/\mathrm{Nm}(I)$ is equal to $ax^2 + bxy + cy^2$, and hence the containment $\Lambda \subseteq I$ must be of index n. Therefore

$$\begin{pmatrix} \lambda w \\ \lambda \end{pmatrix} = N \begin{pmatrix} A\tau \\ A \end{pmatrix}, \qquad \det N = n, \tag{44}$$

and hence there is a unique $\delta_n \in N_n$ such that

$$N \quad \in \quad \mathrm{SL}_2(\mathbb{Z}) \cdot \delta_n \cdot \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\tau). \tag{45}$$

Note δ_n is well-defined: If we multiply λ by a unit in $\mathcal{O}_F^\times \cap (\mathbb{Z} + f\mathcal{O}_F)$ that is totally positive, then N gets multiplied on the right by an element of $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\tau)$. The coset representative δ_n is hence independent of this choice. It is clear that $(w, \delta_n) \in \mathbb{RM}(n, \tau)$.

We now construct an inverse for the map $(\mathfrak{a}, \nu) \mapsto (w, \delta_n)$. Let $ax^2+bxy+cy^2$ be the unique quadratic form of discriminant n^2D whose stable root is w, and define the element $\nu = (-b + n\sqrt{D})/2\sqrt{D} \in \mathfrak{d}_+^{-1}$. Write $w = \gamma\delta_n\tau$, and define λ by

$$\begin{pmatrix} \lambda w \\ \lambda \end{pmatrix} = \gamma\delta_n \begin{pmatrix} A\tau \\ A \end{pmatrix}. \tag{46}$$

Note $\gamma\delta_n$ is only well-defined up to left multiplication by elements in $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(w)$, and up to right multiplication by elements in $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\tau)$, which makes λ well-defined up to totally positive units congruent to an integer modulo f. This makes the integral ideals

$$\mathfrak{a} = \mathrm{Nm}(\lambda I^{-1})/(\lambda I^{-1}), \qquad \mathfrak{b} = (\lambda w)I^{-1} \tag{47}$$

well-defined, and we check easily that $\mathfrak{ab} = (\nu)\mathfrak{d}$ and $\mathfrak{a}$ is coprime to the conductor f. It is easily checked that this defines an inverse to the map defined above. □

4.2. **Reduction theory of binary quadratic forms.** Now that we have established in Lemma 4.1 a bijection between the index set $\mathbb{I}(n, \mathcal{C})_f$ appearing in the expression for the diagonal restrictions of Hilbert Eisenstein series, and an explicit set of 'augmented' RM points $\mathbb{RM}(n, \tau)_f$, it remains to compute the latter. This will be done using classical reduction theory of binary quadratic forms, as we now describe.

Following Gauß, we say that the indefinite binary quadratic form $F = \langle a, b, c\rangle$ of discriminant $\Delta > 0$ is *reduced* if

$$0 < \sqrt{\Delta} - b < 2|a| < \sqrt{\Delta} + b. \tag{48}$$

This condition is equivalent to the following condition on the roots $\lambda^- < \lambda^+$:

$$\begin{cases} \lambda^+ \in (0,1) & \lambda^- \in (-\infty, -1) & \text{if} \quad a > 0, \\ \lambda^+ \in (1,\infty) & \lambda^- \in (-1, 0) & \text{if} \quad a < 0. \end{cases} \tag{49}$$

In general, there are multiple reduced forms in an $\mathrm{SL}_2(\mathbb{Z})$-orbit, though there is clearly a finite number of them. For instance, the two forms of discriminant $\Delta = 2021$ given by

$$\langle 5, 41, -17\rangle \quad \text{and} \quad \langle 19, 11, -25\rangle \tag{50}$$

are $\mathrm{SL}_2(\mathbb{Z})$-equivalent, and are both reduced. There are very efficient algorithms to enumerate all reduced forms in an $\mathrm{SL}_2(\mathbb{Z})$-orbit; see for instance Buchmann–Vollmer [BV07].

As is clear from the description (49), any element $w \in \mathrm{SL}_2(\mathbb{Z})\delta_n\tau$ that satisfies $w > 0 > w'$ is the stable root of an indefinite quadratic form that is a simple translate of a reduced form. Using algorithms for the reduction theory of indefinite binary quadratic forms, we obtain the following algorithm to compute the sets $\mathbb{RM}(n, \tau)$:

(1) Compute the set M_n, defined in (38), and for each $\gamma_n \in M_n$ do the following steps.

(2) For any of the $\gamma_n' \in M_n$ already considered in step (1), test whether
$$\gamma_n' \cdot \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\tau) \cdot \gamma_n^{-1} \subset \mathrm{SL}_2(\mathbb{Z}).$$
If this inclusion holds for some γ_n', do nothing. If it does not hold for any γ_n', let F be the form of discriminant $n^2 D$ whose stable root is $\gamma_n \tau$, and do the following steps.

(3) Run the reduction algorithm outlined in Buchmann–Vollmer [BV07, § 6.4] on the quadratic form F. Specifically, compute the integer s defined in *loc. cit.* and enumerate for $1 \leq i \leq s$ the quadratic forms
$$\begin{array}{ll} \langle a + ib + i^2 c,\ b + 2ic,\ c\rangle & \text{if} \quad a > 0, \\ \langle c,\ -b + 2ic,\ a - ib + i^2 c\rangle & \text{if} \quad a < 0. \end{array}$$
Redefine F to be the (necessarily reduced) last quadratic form in this sequence, and repeat this step until the same reduced form is obtained a second time. Remove the quadratic forms in this list whose first coefficient is not coprime with f.

The set $\mathbb{RM}(n,\tau)_f$ is given by the pairs (w, γ_n) where $\gamma_n \in M_n$, and
$$w = (-b + \sqrt{D})/2a$$
is the stable root of a binary quadratic form $\langle a, b, c\rangle$ obtained from γ_n in the last step.

Remark 4.2. For our application to p-adic L-functions, one needs to compute $\mathbb{RM}(n,\tau)_f$ for all n up to some (Sturm) bound. This allows for an additional speed-up in our implementation. The set $\mathbb{RM}(n,\tau)_f$ may also be computed using double coset representatives in M_d instead of M_n, where d is the smallest divisor of n that is coprime to n/d. For any $\mathrm{SL}_2(\mathbb{Z})$-orbit of elements in $\mathbb{RM}(n/d,\tau)$, which was already computed in the process of determining the (n/d)-th Fourier coefficient, we apply the same algorithm using the coset representatives M_d. This produces the same essential calculations, but eliminates some amount of iterations of step (2) that do not result in step (3). This variant causes a significant speed-up in practice.

4.3. **Examples.** We now illustrate the above methods with some instructive examples.

Example 4.3. As a warm-up, let us first use the above results to compute classical L-values, omitting for now their p-adic interpolation (see Examples 4.6 and 4.7). Let $D = 192$; then we have $f = 4$ and the associated fundamental discriminant is $D_0 = 12$. Set $F = \mathbb{Q}(\sqrt{12})$. We have
$$\mathrm{Cl}_{192}^{+} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \tag{51}$$
and the space of totally even functions on the class group is spanned by the two functions
$$\begin{array}{rcl} \psi_1 & = & \mathbf{1}_{[\mathcal{O}_F]} + \mathbf{1}_{[\mathfrak{d}]} \\ \psi_2 & = & \mathbf{1}_{[\mathfrak{a}]} + \mathbf{1}_{[\mathfrak{a}\mathfrak{d}]} \quad \text{where} \quad \mathfrak{a} = (-3, (12 + \sqrt{192})/2) \end{array} \tag{52}$$
that take values in $\mathbb{Q}$. Using the above algorithm, we compute the first 200 higher Fourier coefficients of the series G_{2,ψ_i} restricted to the diagonal. This took under 4 seconds for each series. As in the previous section, we compute a basis for the

space of forms of level 4 and weight 4, whence we get after a trivial computation the exact special L-values

$$\begin{array}{rcl} L(\psi_1,-1) &=& 35/12, \\ L(\psi_2,-1) &=& -37/12. \end{array} \tag{53}$$

Example 4.4. For a more interesting example, let us take $D = 11^2 \cdot 13$; then we have $f = 11$ and the ring class group of this conductor is isomorphic to

$$\mathrm{Cl}^+_{1573} \simeq \mathbb{Z}/6\mathbb{Z}. \tag{54}$$

The space of totally even functions on this ring class group is spanned by:

$$\begin{array}{rcl} \psi_1 &=& \mathbf{1}_{[\mathcal{O}_F]} + \mathbf{1}_{[\mathfrak{d}]} \\ \psi_2 &=& \mathbf{1}_{[\mathfrak{a}]} + \mathbf{1}_{[\mathfrak{a}\mathfrak{d}]} \qquad \text{where } \mathfrak{a} = (17, (-31+11\sqrt{13})/2). \\ \psi_3 &=& \mathbf{1}_{[\mathfrak{a}^{-1}]} + \mathbf{1}_{[\mathfrak{a}^{-1}\mathfrak{d}]} \end{array} \tag{55}$$

Using the above algorithm, we compute enough higher Fourier coefficients of the series G_{4,ψ_i} restricted to the diagonal to determine that

$$\begin{array}{rcl} L(\psi_1,-3) &=& 17291314/3, \\ L(\psi_2,-3) &=& -9930038/3, \\ L(\psi_3,-3) &=& -9930038/3. \end{array} \tag{56}$$

From this computation, we can deduce the special values of any totally even character. For instance, there is a unique such cubic character ψ whose value on $\mathfrak{a}$ is ζ_3. We find that

$$\begin{aligned} L(\psi,-3) &= 17291314/3 + \zeta_3(-9930038/3) + \zeta_3^2(-9930038/3) \\ &= 9073784. \end{aligned}$$

This entire computation took less than a second, gives the exact L-value, and is provably correct.

Example 4.5. We now combine the above ideas with the algorithms for efficiently computing p-adic bases for classical spaces of modular forms to present a first example of a p-adic L-series. Consider $F = \mathbb{Q}(\sqrt{2})$ and let ψ be the (ramified) character associated to the quadratic extension $\mathbb{Q}(\zeta_8)/F$. Then we compute

$$\begin{aligned} L_5(\psi\omega, s) \equiv\ & -2\cdot 5^9\ s^{11} - 8\cdot 5^8\ s^{10} + 4\cdot 5^8\ s^9 + 9\cdot 5^8\ s^8 \\ & - 18\cdot 5^6\ s^7 - 694\cdot 5^5\ s^6 - 844\cdot 5^4\ s^5 + 1387\cdot 5^5\ s^4 \\ & - 7624\cdot 5^3\ s^3 + 136147\cdot 5^2\ s^2 + 232969\cdot 5\ s, \\ L_7(\psi\omega, s) \equiv\ & 2\cdot 7^9\ s^{10} - 17\cdot 7^8\ s^9 + 114\cdot 7^7\ s^8 \\ & + 618\cdot 7^6\ s^7 + 75\cdot 7^6\ s^6 - 256\cdot 7^6\ s^5 + 5365\cdot 7^4\ s^4 \\ & + 161750\cdot 7^3\ s^3 - 1083083\cdot 7^2\ s^2 - 12676806\cdot 7\ s - 2. \end{aligned}$$

The computations were done modulo 5^{10} and 7^{10} respectively, and took less than a second. Note that the valuations of the coefficients are very close to the predicted estimates in (24). Finally, we note that $L_5(\psi\omega, 0) = 0$ up to the computed precision, as should be the case since 5 is inert in $\mathbb{Q}(\sqrt{2})$ and therefore the L-function has an exceptional zero at $s = 0$. On the other hand, 7 splits into two ideals $\mathfrak{p}_1, \mathfrak{p}_2$ that are not in the kernel of ψ (since 7 does not split completely in $\mathbb{Q}(\zeta_8)/\mathbb{Q}$), and the value at $s = 0$ is equal (up to the computed precision) to

$$-(1-\psi(\mathfrak{p}_1))(1-\psi(\mathfrak{p}_2))L(\psi,0) = -2.$$

Example 4.6. This setting will be revisited in Example 5.4. Let us take $D = 321$, and $F = \mathbb{Q}(\sqrt{321})$. We have

$$\mathrm{Cl}^+_{321} \simeq \mathbb{Z}/6\mathbb{Z}, \tag{57}$$

and the space of odd functions on the class group is spanned by the three functions

$$\begin{array}{rcll} \psi_1 & = & \mathbf{1}_{[\mathcal{O}_F]} - \mathbf{1}_{[\mathfrak{d}]}, & \\ \psi_2 & = & \mathbf{1}_{[\mathfrak{a}]} - \mathbf{1}_{[\mathfrak{a}\mathfrak{d}]} & \text{where } \mathfrak{a} = (4, (-15+\sqrt{321})/2), \\ \psi_3 & = & \mathbf{1}_{[\mathfrak{b}]} - \mathbf{1}_{[\mathfrak{b}\mathfrak{d}]} & \text{where } \mathfrak{b} = (2, (-15+\sqrt{321})/2) \end{array} \tag{58}$$

that take values in $\mathbb{Q}$. Let $p = 7$, which is inert in F. Using the method of this section we can compute that

$$\begin{array}{rcrrr} L_7(\psi_1\omega, T) & \equiv & (3+O(7^2))T^3 & -(10+O(7^3))T^2 & +(913+O(7^4))T, \\ L_7(\psi_2\omega, T) & \equiv & (1+O(7^2))T^3 & +(211+O(7^3))T^2 & +(340\cdot 7+O(7^4))T, \\ L_7(\psi_3\omega, T) & \equiv & -(1+O(7^2))T^3 & -(211+O(7^3))T^2 & -(340\cdot 7+O(7^4))T. \end{array} \tag{59}$$

This took a fraction of a second. In fact, with working precision 7^{60} one computes each of the series $L_7(\psi_j\omega, s)$ mod p^{51} in around 32 seconds (the precision loss during interpolation here is 9, as expected). The resulting series would be too long to reproduce here, but we note that it exhibits $L_7(\psi_1\omega, 0) = 0$ as it should due to the presence of an exceptional zero corresponding to $k = 1$, and it allows us to recover the derivative $L_7'(\psi_1\omega, 0)$ modulo 7^{51} (the derivative here is with respect to s). As we explain in the next section, and will see in Example 5.4, this derivative may also be computed directly in about 4 seconds, and is the logarithm of a p-unit in the Hilbert class field of F by the main result of [DDP11]. Note though this approach to computing the derivative is inferior to that based upon overconvergent forms below: it is slower and suffers from a precision loss during interpolation.

Finally, we note that the method is also practicable for larger primes, e.g. taking $p = 101$ and $m = 15$ the computation of $L_{101}(\psi_1\omega, T)$ runs in 411 seconds, with all but 3 seconds taken up computing higher Fourier coefficients.

Example 4.7. We now compute some Iwasawa invariants for $D = 141 = 3 \cdot 47$ and a variety of small primes p. Let ψ be the genus character of $F = \mathbb{Q}(\sqrt{141})$ corresponding to the biquadratic extension $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-47})$. Then we compute the series

$$L_p(\psi\omega, T) = p^\mu P(T)U(T)$$

for all primes $p \leq 229$, where $U(T) \in \mathbb{Z}_p[\![T]\!]$ is a unit, and $P(T)$ is a distinguished polynomial, i.e.

$$P(T) \equiv T^{\deg(P)} \pmod{p}.$$

We call $\lambda = \deg(P)$. We observe that $\mu = 0$ in each case,[4] which, since $L/\mathbb{Q}$ is abelian, is implied by the main result of Ferrero–Washington [FW79]. The λ-invariants on the other hand exhibit more interesting behaviour, tabulated here:

p	$\left(\frac{D}{p}\right)$	λ	p	$\left(\frac{D}{p}\right)$	λ	p	$\left(\frac{D}{p}\right)$	λ	p	$\left(\frac{D}{p}\right)$	λ	p	$\left(\frac{D}{p}\right)$	λ
2	−1	3	31	−1	1	73	−1	1	127	−1	1	179	1	0
3	0	2	37	1	2	79	1	2	131	−1	1	181	−1	2
5	1	1	41	1	0	83	−1	1	137	1	0	191	−1	1
7	1	2	43	−1	1	89	−1	1	139	−1	1	193	−1	1
11	1	0	47	0	0	97	1	2	149	−1	1	197	−1	1
13	−1	2	53	−1	1	101	−1	1	151	−1	1	199	−1	1
17	−1	2	59	−1	1	103	1	2	157	1	3	211	−1	1
19	−1	1	61	1	2	107	1	0	163	−1	1	223	−1	1
23	1	0	67	−1	1	109	−1	1	167	1	0	227	1	0
29	1	0	71	−1	1	113	1	0	173	−1	1	229	−1	1

At first sight, the number of non-zero values of λ may seem striking, but the bulk of them is explained by exceptional zeroes. More precisely, we have the following possibilities for the splitting behaviour of p in F:

- p is inert in F: In this case, the Euler factor
$$(1 - \psi(p)\mathrm{Nm}(p)^{k-1})$$
vanishes to order one at $k=1$, and therefore the p-adic L-function $L_p(\psi\omega, T)$ must vanish to order at least one at $T = 0$, forcing $\lambda \geq 1$. In the above table, this accounts for all the zeroes, except when $p = 2, 13, 17, 181$.
- p is split in F: Suppose that $(p) = \mathfrak{p}\mathfrak{p}'$; then $\mathfrak{p}$ is necessarily principal. If it is generated by a totally positive element, then $\psi(\mathfrak{p}) = \psi(\mathfrak{p}') = 1$, so the p-adic L-function $L_p(\psi\omega, T)$ has an exceptional zero of order at least two at $T = 0$. In the above table, this again accounts for all the zeroes of the p-adic L-function, except when $p = 5, 157$.

  In those cases, we investigate the zeroes of $L_p(\psi\omega, T)$:
  - $p = 5$: We find that the p-adic L-function has a simple root at
$$T \equiv 1992099 \cdot 5 \pmod{5^{10}}.$$
Note that this is consistent with the fact that $\mathrm{Cl}(L) \simeq \mathbb{Z}/5\mathbb{Z}$, since the 5-divisibility of the class number is equivalent to the existence of a zero in this case.
  - $p = 157$: In this case the distinguished polynomial is $P(T) = T^2(T-a)$ where we computed the value of a to be
$$a = 71 \cdot 157 + 99 \cdot 157^2 + 8 \cdot 157^3 + 115 \cdot 157^4 + \ldots,$$
so the p-adic L-function has a unique root besides its double exceptional zero at $T = 0$, causing the p-part of the class group to grow linearly with slope 3 in the cyclotomic tower over L. Note that unlike the previous case, this does not imply the divisibility of the class number of L by 157 due to the exceptional zero.

[4]Note that when $p = 2$, the L-series always belongs to $4\mathbb{Z}_2[\![T]\!]$ and is hence of valuation at least $2 = d$. In this case, the statement $\mu = 0$ means that we observed coefficients whose valuation was exactly 2.

- p is ramified in F: This is only true for $p = 3, 47$. The 47-adic L-series has no zeroes. When $p = 3$, the character ψ cuts out the extension $F(\sqrt{-3})$, so in fact $\psi\omega$ is trivial. We omitted this case in the above description of the algorithm for simplicity, and now show how to treat it. The series $L_3(1, s)$ has a simple pole at $s = 1$, so we may write

$$L_3(1, T) = F(T)/(T - 3),$$

where $F(T)$ is an element of the Iwasawa algebra that we compute to be

$$F(T) = -539 \cdot 3^2 T + 3929T^2 - 4910T^3 + \dots \pmod{3^{10}}.$$

This power series has $(\lambda, \mu) = (2, 0)$. We note that $L_3(1, T)$ has a simple zero at $T = 0$. This is an exceptional zero caused by the fact that the unique prime above 3 is generated by a totally positive element.

Remark 4.8. If we reverse the above example by fixing a prime and varying ψ over (say) all odd quadratic characters of F, the statistics of the λ-invariant are expected to resemble those of p-adic random matrices. For more on this theme, see Ellenberg–Jain–Venkatesh [EJV11].

5. Real quadratic fields: Overconvergence and derivatives

Algorithm 3.3 in §3.2 can also be recast in terms of overconvergent modular forms. Since the underlying computations that need to be performed are nearly identical to those outlined above in the language of classical modular forms, there seems little advantage in doing so.

However, when the p-adic L-function has an exceptional zero at $k = 1$, its first derivative at $k = 1$ may be computed directly in a way that uses in an essential manner overconvergent modular forms, following recent results of the second author with Henri Darmon and Alice Pozzi [DPV1]. The value of this first derivative in the presence of an exceptional zero is of great interest, and equals the p-adic logarithm of the norm of a Gross–Stark unit; see for instance [DDP11].

Remark 5.1. We note here that a computational approach to the computation of the Gross–Stark unit was developed for real quadratic fields by Dasgupta [Das07] and for cubic fields by Slavov [Sla07] based on the Shintani cone refinements of [Das08]. They are closely related to the definition of the p-adic L-functions by Barsky and Cassou-Noguès, but yield a refinement of it that recovers the Gross–Stark unit (without the norm). It is also possible to obtain a similar refinement in the spirit of Serre and Deligne–Ribet by replacing the p-adic family of Eisenstein series in weight

$$(1 + \varepsilon,\, 1 + \varepsilon)$$

below by a cuspidal family of Hilbert modular forms of *anti-parallel weight*

$$(1 + \varepsilon,\, 1 - \varepsilon)$$

and restricting it to the diagonal. This is the subject of the forthcoming paper [DPV2].

Notation. As before, F is a real quadratic field, and

$$\psi : \mathrm{Cl}_D^+ \longrightarrow \mathbb{C}_p^\times \tag{60}$$

is an *odd* ring class character of discriminant D (not necessarily fundamental), which means that $\psi(\mathfrak{d}) = -1$, where $\mathfrak{d}$ is the different of F. We also choose $p \nmid D$

to be a prime that is inert in F. The vanishing of the Euler factor at p implies that we have an *exceptional zero*, i.e.

$$L_p(\psi\omega, 0) = 0. \tag{61}$$

In this section, we describe a direct way to compute the quantity $L_p'(\psi\omega, 0)$ in this situation.

5.1. **Overconvergent p-adic modular forms.** We now briefly recall the salient points of the algorithms for computing with overconvergent modular forms, as developed in [Lau11].

Let $N \geq 5$ and $p \nmid N$ be a prime. We let $\mathcal{X}/\mathbb{Z}_p$ be the moduli space of generalised elliptic curves with $\Gamma_1(N)$-level structure, and ω the modular line bundle on $\mathcal{X}$. The Hasse invariant A is the unique global section of $\mathbb{F}_p \otimes \omega^{\otimes p-1}$ with q-expansion 1. There is a reduction map

$$\mathrm{red} \ : \ \mathcal{X}(\mathbb{C}_p) \longrightarrow \mathcal{X}_s(\overline{\mathbb{F}}_p), \tag{62}$$

where $\mathcal{X}_s$ is the special fibre of $\mathcal{X}$ over $\mathbb{F}_p$, such that the inverse image $\mathrm{red}^{-1}(x)$ of a closed point is isomorphic to a rigid analytic open disk. The vanishing locus of the Hasse invariant is precisely the supersingular locus of $\mathcal{X}_s$, which consists of a finite set of closed points. Therefore, any lift of the Hasse invariant is invertible on the *ordinary locus* X^{ord}, which is the affinoid whose $\mathbb{C}_p$-points correspond to elliptic curves with ordinary reduction. The ordinary locus X^{ord} is the complement of a finite number of rigid analytic open disks.

Let $r \in \mathbb{C}_p$ such that $0 \leq v_p(r) \leq 1$, and define $X^{\mathrm{ord}} \subset X_r \subset X^{\mathrm{rig}}$ by

$$X_r(\mathbb{C}_p) := \{x \ \in \ X(\mathbb{C}_p) \ : \ v_p(\widetilde{A}_x) \leq v_p(r)\}, \tag{63}$$

where $\widetilde{A}_x$ is a local lift of the Hasse invariant A at x. Note we do not require a global lift of the Hasse invariant to exist, which may fail in general when $p \leq 3$. Katz [Kat73] defines the space of *r-overconvergent modular forms* of integer weight k on $\Gamma_1(N)$ to be

$$M_k^\dagger(r) := H^0(X_r, \omega^{\otimes k}). \tag{64}$$

Now let n be the smallest power of p such that the n-th power of the Hasse invariant A^n lifts to a level 1 Eisenstein series E of weight $k_E = n(p-1)$. Throughout this section, we assume $nv_p(r) \leq 1$. Our notation is summarised in the following table:

p	2	3	≥ 5
E	E_4	E_6	E_{p-1}
n	4	3	1

The p-adic Banach space $M_k^\dagger(r)$ has a basis of *Katz expansions* of the form

$$\left\{ \ r^{ni} \frac{a_{i,j}}{E^i} \ \right\}_{i,j}, \tag{65}$$

where the $a_{i,j}$ are classical modular forms; see [Kat73]. This allows for an efficient explicit computation of spaces of overconvergent modular forms, as described in [Lau11, Von15].

5.2. **Derivatives of families of overconvergent modular forms.** Since p is inert in F, we have an exceptional zero $L_p(\psi, 0) = 0$. In light of the techniques in this paper, this may be interpreted as saying that the diagonal restriction of the Eisenstein series $G_{1,\psi}$ has vanishing constant term at the cusp ∞. Theorem 5.2, proved in Darmon–Pozzi–Vonk [DPV1], states that also its higher Fourier coefficients vanish.

Theorem 5.2. *Suppose that $p \nmid D$ is inert in the real quadratic field F. The diagonal restriction $G_{1,\psi}$ of the Hilbert Eisenstein series vanishes identically.*

The result in *loc. cit.* is stated only for unramified characters, corresponding to the case where D is a fundamental discriminant, but the proof remains valid for ramified characters.

When the p-adic family of Hilbert Eisenstein series $G_{k,\psi}$ restricted to the diagonal vanishes identically at $k = 1$, it becomes natural to consider its first derivative with respect to the weight variable k. The q-expansion of this first derivative is given by

$$H(q) = L_p'(\psi\omega, 0) + 4\sum_{n\geq 1}\left(\sum_{\mathcal{C}\in \mathrm{Cl}_{\mathfrak{m}}^+}\psi(\mathcal{C})\sum_{(\mathfrak{a},\nu)\ \in\ \mathbb{I}(n,\mathcal{C})}\psi(\mathfrak{a})\log_p\left(\mathrm{Nm}(\mathfrak{a})\right)\right)q^n. \tag{66}$$

Note that we are now in a situation very similar to that of the main algorithm above: The constant term $L_p'(\psi\omega, 0)$ is the quantity we wish to compute, and the higher coefficients may be computed very efficiently using the methods from §4. The crucial difference is that the form $H(q)$ is *not* a classical modular form. Lemma 5.3 can be found in [DPV1]:

Lemma 5.3. *The series $H(q)$ is the q-expansion of an element in $M_2^\dagger(r)$, for every $r < p/(p+1)$.*

This leads to a direct algorithm for computing the value $L_p'(\psi\omega, 0)$ that is very similar to the one in §3.2. Indeed, the explicit basis (65) for the spaces $M_2^\dagger(r)$ may be computed efficiently using the algorithms in [Lau11], so we can determine the constant term of $H(q)$ from the higher coefficients as before.

Example 5.4. Let us consider the setting of Example 4.6, and resume the notation introduced there. Let us take $p = 7$, which is inert in F. In this case, there is an exceptional zero, and the diagonal restriction of the Eisenstein family vanishes at $k = 1$ for any odd character. We compute G_{1,ψ_i}' for $i = 1, 2, 3$ and find that

$$\begin{aligned}
L_7'(\psi_1\omega, 0) &= \ 64771969526061725695285078070168228421171131204 51\cdot 7 \pmod{7^{60}},\\
L_7'(\psi_2\omega, 0) &= \ 24000607710173134578660420073909137986735058464 08\cdot 7^2 \pmod{7^{60}},\\
L_7'(\psi_3\omega, 0) &= -24000607710173134578660420073909137986735058464 08\cdot 7^2 \pmod{7^{60}}.
\end{aligned}$$

The first quantity is equal, up to the computed precision, to $\log_7(u)$, where u satisfies the equation

$$7^{16}u^6 - 20976\cdot 7^8u^5 - 270624\cdot 7^4u^4 + 526859689u^3 - 270624u^2 - 20976u + 7^4 = 0 \tag{67}$$

and therefore u is a 7-unit in the narrow Hilbert class field H of $\mathbb{Q}(\sqrt{321})$. This is consistent with the main result of Dasgupta–Darmon–Pollack [DDP11], which predicts the existence of u in $\mathbb{Q}\otimes\mathcal{O}_H[1/7]^\times$. In this case, the Brumer–Stark conjecture, now largely proved by Dasgupta–Kakde [DK], predicts that u is in fact in $\mathcal{O}_H[1/7]^\times$ as we observe. The computations took 13 seconds in total.

Acknowledgments

The authors would like to thank Pierre Charollois for innumerable valuable suggestions and comments, as well as Henri Darmon and Alice Pozzi for many inspiring conversations that shaped the main approach of this paper. We would like to thank the two anonymous referees for providing extremely detailed feedback and many suggestions that greatly improved the paper. All computations were performed using the Magma computer algebra system.

References

[Bar78] Daniel Barsky, *Fonctions zeta p-adiques d'une classe de rayon des corps de nombres totalement réels* (French), Groupe d'Etude d'Analyse Ultramétrique (5e année: 1977/78), Secrétariat Math., Paris, 1978, pp. Exp. No. 16, 23. MR525346

[BV07] Johannes Buchmann and Ulrich Vollmer, *Binary quadratic forms*, Algorithms and Computation in Mathematics, vol. 20, Springer, Berlin, 2007. An algorithmic approach. MR2300780

[CR73] P. Cartier and Y. Roy, *Certains calculs numériques relatifs à l'interpolation p-adique des séries de Dirichlet* (French), Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 269–349. Lecture Notes in Math., Vol. 350. MR0330113

[CN79] Pierrette Cassou-Noguès, *Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques* (French), Invent. Math. **51** (1979), no. 1, 29–59, DOI 10.1007/BF01389911. MR524276

[CD14] Pierre Charollois and Samit Dasgupta, *Integral Eisenstein cocycles on $\mathbf{GL}_n$, I: Sczech's cocycle and p-adic L-functions of totally real fields*, Camb. J. Math. **2** (2014), no. 1, 49–90, DOI 10.4310/CJM.2014.v2.n1.a2. MR3272012

[CDG15] Pierre Charollois, Samit Dasgupta, and Matthew Greenberg, *Integral Eisenstein cocycles on $\mathbf{GL}_n$, II: Shintani's method*, Comment. Math. Helv. **90** (2015), no. 2, 435–477, DOI 10.4171/CMH/360. MR3351752

[Coh76] Henri Cohen, *Variations sur un thème de Seigel et Hecke* (French), Acta Arith. **30** (1976/77), no. 1, 63–93, DOI 10.4064/aa-30-1-63-93. MR422215

[DLR] Henri Darmon, Alan Lauder, and Victor Rotger, *Stark points and p-adic iterated integrals attached to modular forms of weight one*, Forum Math. Pi **3** (2015), e8, 95, DOI 10.1017/fmp.2015.7. MR3456180

[DPV1] Henri Darmon, Alice Pozzi, and Jan Vonk, *Diagonal restrictions of p-adic Eisenstein families*, Math. Ann. **379** (2021), no. 1-2, 503–548, DOI 10.1007/s00208-020-02086-2. MR4211095

[DPV2] H. Darmon, A. Pozzi, and J. Vonk, *The values of the Dedekind-Rademacher cocycle at real multiplication points*, Preprint, 2021.

[Das07] Samit Dasgupta, *Computations of elliptic units for real quadratic fields*, Canad. J. Math. **59** (2007), no. 3, 553–574, DOI 10.4153/CJM-2007-023-0. MR2319158

[Das08] Samit Dasgupta, *Shintani zeta functions and Gross-Stark units for totally real fields*, Duke Math. J. **143** (2008), no. 2, 225–279, DOI 10.1215/00127094-2008-019. MR2420508

[DDP11] Samit Dasgupta, Henri Darmon, and Robert Pollack, *Hilbert modular forms and the Gross-Stark conjecture*, Ann. of Math. (2) **174** (2011), no. 1, 439–484, DOI 10.4007/annals.2011.174.1.12. MR2811604

[DDF14] Francisco Diaz y Diaz and Eduardo Friedman, *Signed fundamental domains for totally real number fields*, Proc. Lond. Math. Soc. (3) **108** (2014), no. 4, 965–988, DOI 10.1112/plms/pdt025. MR3198753

[DK] S. Dasgupta and M. Kakde, *On the Brumer–Stark conjecture*, `arXiv:abs/2010.00657`, 2020.

[DR80] Pierre Deligne and Kenneth A. Ribet, *Values of abelian L-functions at negative integers over totally real fields*, Invent. Math. **59** (1980), no. 3, 227–286, DOI 10.1007/BF01453237. MR579702

[EJV11] Jordan S. Ellenberg, Sonal Jain, and Akshay Venkatesh, *Modeling λ-invariants by p-adic random matrices*, Comm. Pure Appl. Math. **64** (2011), no. 9, 1243–1262, DOI 10.1002/cpa.20375. MR2839300

[FW79] Bruce Ferrero and Lawrence C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), no. 2, 377–395, DOI 10.2307/1971116. MR528968

[Hec24] E. Hecke, *Analytische funktionen und algebraische zahlen* (German), Abh. Math. Sem. Univ. Hamburg **3** (1924), no. 1, 213–236, DOI 10.1007/BF02954625. MR3069428

[Kli62] Helmut Klingen, *Über die Werte der Dedekindschen Zetafunktion* (German), Math. Ann. **145** (1961/62), 265–272, DOI 10.1007/BF01451369. MR133304

[Kat73] Nicholas M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350. MR0447119

[Kat78] Nicholas M. Katz, *p-adic L-functions for CM fields*, Invent. Math. **49** (1978), no. 3, 199–297, DOI 10.1007/BF01390187. MR513095

[Lau11] Alan G. B. Lauder, *Computations with classical and p-adic modular forms*, LMS J. Comput. Math. **14** (2011), 214–231, DOI 10.1112/S1461157011000155. MR2831231

[Lau14] Alan G. B. Lauder, *Efficient computation of Rankin p-adic L-functions*, Computations with modular forms, Contrib. Math. Comput. Sci., vol. 6, Springer, Cham, 2014, pp. 181–200, DOI 10.1007/978-3-319-03847-6_7. MR3381453

[Rob15] Xavier-François Roblot, *Computing p-adic L-functions of totally real number fields*, Math. Comp. **84** (2015), no. 292, 831–874, DOI 10.1090/S0025-5718-2014-02889-5. MR3290966

[Ser73] Jean-Pierre Serre, *Formes modulaires et fonctions zêta p-adiques* (French), Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), Springer, Berlin, 1973, pp. 191–268. Lecture Notes in Math., Vol. 350. MR0404145

[Shi76] Takuro Shintani, *On evaluation of zeta functions of totally real algebraic number fields at non-positive integers*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **23** (1976), no. 2, 393–417. MR427231

[Shi78] Goro Shimura, *The special values of the zeta functions associated with Hilbert modular forms*, Duke Math. J. **45** (1978), no. 3, 637–679. MR507462

[Sie68] Carl Ludwig Siegel, *Berechnung von Zetafunktionen an ganzzahligen Stellen* (German), Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II **1969** (1969), 87–102. MR252349

[Sla07] K. Slavov, *Gross–Stark units for totally real number fields*, Senior thesis, Harvard University, 2007.

[Ste07] William Stein, *Modular forms, a computational approach*, Graduate Studies in Mathematics, vol. 79, American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells, DOI 10.1090/gsm/079. MR2289048

[Von15] Jan Vonk, *Computing overconvergent forms for small primes*, LMS J. Comput. Math. **18** (2015), no. 1, 250–257, DOI 10.1112/S1461157015000042. MR3349318

[Wil90] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. (2) **131** (1990), no. 3, 493–540, DOI 10.2307/1971468. MR1053488

Mathematical Institute, University of Oxford, Woodstock Road, Oxford OX2 6GG, United Kingdom

Email address: lauder@maths.ox.ac.uk

Mathematical Institute (Snellius), University of Leiden, Niels Bohrweg 1, 2333 CA Leiden, The Netherlands

Email address: j.b.vonk@math.leidenuniv.nl