COMPUTING p-ADIC L-FUNCTIONS OF TOTALLY REAL FIELDS

ALAN LAUDER AND JAN VONK

Contents

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, which 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.

2010 *Mathematics Subject Classification.* 11R42,11F41,11Y40.

[1] We mention also the unpublished algorithm of Charollois, based on cocycle relations for GL_n as in [CD14, CDG15] which is inspired by the approach via explicit formulae of Shintani which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

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 [Das07, Sla07]. A notable difference is that we obtain such an explicit formula numerically through linear algebra in spaces of modular forms. 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 Cohen [Coh76] for the trivial character. 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 [DPV] 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 [DPV] for more details.

1.1. **Acknowledgements.** The authors would like to thank Pierre Charollois, Henri Darmon, and Alice Pozzi for many useful comments and suggestions. 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, during various stages of this project. All computations were performed using the Magma computer algebra system.

1.2. **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 $\{\sigma_1, \ldots, \sigma_d\}$ 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 quotient of $\mathscr{I}_{F,\mathfrak{m}}$ by the relation

$$\mathfrak{a} \sim \mathfrak{b} \text{ if and only if } \mathfrak{a}\mathfrak{b}^{-1} = (\alpha) \text{ for some totally positive } \alpha \in 1 + \mathfrak{m}$$

is the *narrow ray class group* $\mathrm{Cl}_{\mathfrak{m}}^{+}$. We will consider ray class characters

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

which are either *totally odd* or *totally even.* This means that for any element $\alpha \in 1 + \mathfrak{m}$ such that $\sigma_i(\alpha) < 0$ for some i and $\sigma_j(\alpha) > 0$ for all $j \neq i$, we have $\psi(\alpha) = -1$, respectively 1.

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

$$L(\psi, s) = \sum_{\mathfrak{a} \lhd \mathcal{O}_F} \psi(\mathfrak{a}) \mathrm{Nm}(\mathfrak{a})^{-s} \tag{3}$$

which analytically continues to $\mathbb{C}$ when $\psi \neq 1$. If p is 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

$$L_p(\psi\omega, n) = \sum_{(\mathfrak{a},p)=1} \psi\omega^n(\mathfrak{a}) \mathrm{Nm}(\mathfrak{a})^{-n} \tag{4}$$

for all integers $n < 0$, where ω is the p-adic Teichmüller character. For non-trivial characters, the function $L_p(\psi, s)$ defines an element of the Iwasawa algebra $\Lambda_{\mathcal{O}}$, see § 2.2. It is this p-adic L-function whose explicit computation is the subject of the rest of this article.

2. Hilbert Eisenstein series and p-adic L-functions

In this section, we describe Hilbert Eisenstein series, their p-stabilisations, and their diagonal restrictions, which are central to our approach. A general algorithm, described in § 2.4, reduces the computation of $L_p(\psi\omega, s)$ to a computation of the higher Fourier coefficients of these diagonal restrictions, which have a much more elementary nature.

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 Darmon–Dasgupta–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

$$M_k(\mathfrak{m}, \psi) \tag{5}$$

of Hilbert modular forms of (parallel) weight k, level $\mathfrak{m}$ and character ψ. It consists of tuples of holomorphic functions on the d-fold product of upper half-planes $\mathcal{H}^d$, indexed by the narrow class group of F, satisfying various conditions. We content ourselves by mentioning that the data for each element includes a holomorphic function $f : \mathcal{H}^d \to \mathbb{C}$ associated to the class of $\mathfrak{d}^{-1}$, which satisfies

$$(\mathrm{c}_1 z_1 + \mathrm{d}_1)^{-k} \cdots (\mathrm{c}_d z_d + \mathrm{d}_d)^{-k} f\left(\frac{\mathrm{a}_1 z_1 + \mathrm{b}_1}{\mathrm{c}_1 z_1 + \mathrm{d}_1}, \ldots, \frac{\mathrm{a}_d z_d + \mathrm{b}_d}{\mathrm{c}_d z_d + \mathrm{d}_d}\right) = \psi(\mathrm{a}) f(z), \tag{6}$$

for all matrices

$$\gamma = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} \in \mathbf{SL}_2(\mathcal{O}_F) \quad \text{such that } \mathrm{c} \in \mathfrak{m}, \tag{7}$$

where $z = (z_1, \ldots, z_d)$ is the variable in $\mathcal{H}^d$. The transformation law (6) implies that every form has a q-expansion, indexed by the totally positive elements $\mathfrak{d}_+^{-1}$ of the inverse different.

In this paper, we are only concerned with Hilbert Eisenstein series, whose basic properties are discussed in Katz [Kat78]. More precisely, there exists a Hilbert modular form

$$G_{k,\psi} \in M_k(\mathfrak{m}, \psi) \tag{8}$$

whose q-expansion is given by

$$G_{k,\psi}(z) = L(\psi, 1-k) + 2^d \sum_{\nu \in \mathfrak{d}_+^{-1}} \left(\sum_{\mathfrak{a} | (\nu)\mathfrak{d}} \psi(\mathfrak{a}) \mathrm{Nm}(\mathfrak{a})^{k-1} \right) q^\nu \tag{9}$$

where we use the notation

$$q^\nu = \exp\left(2\pi i(\nu_1 z_1 + \nu_2 z_2 + \ldots + \nu_d z_d)\right) \tag{10}$$

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 (9) must be modified, but since we will not need this case, we refer the interested reader to Darmon–Dasgupta–Pollack [DDP11, Proposition 2.11].

2.2. **p-Adic Hilbert Eisenstein series.** 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 $\mathbb{Z}_p^\times$, which is cyclic of order $\phi(q)$, where $q = 4$ if $p = 2$, and $q = p$ 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

$$\begin{array}{ccccccc} \mathbb{Z}_p^\times & \xrightarrow{\sim} & \Delta \times (1 + p\mathbb{Z}_p), & & a & \longmapsto & (\omega(a), \langle a \rangle), \\ \Lambda & \xrightarrow{\sim} & \mathbb{Z}_p[\Delta][\![T]\!], & & 1+q & \longmapsto & 1+T. \end{array} \tag{11}$$

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

$$\mathfrak{I}_k = \left(1 + T - (1+q)^{1-k}\right) \tag{12}$$

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 $\mathfrak{I}_{k,\psi}$ is the Eisenstein series

$$G^{(p)}_{k,\psi}(z) = L_p(\psi, 1-k) + 2^d \sum_{\nu \in \mathfrak{d}_+^{-1}} \left(\sum_{\substack{\mathfrak{a} | (\nu)\mathfrak{d} \\ (\mathfrak{a}, p) = 1}} \psi(\mathfrak{a}) \langle \mathrm{Nm}(\mathfrak{a}) \rangle^{k-1} \right) q^\nu \tag{13}$$

which is called the *ordinary p-stabilisation* of the Eisenstein series $G_{k,\psi}$ from § 2.1.

2.3. **Diagonal restrictions.** The *diagonal restriction* of a Hilbert modular form $f : \mathcal{H}^d \to \mathbb{C}$ is the restriction of f to the diagonally embedded copy of the upper half plane in $\mathcal{H}^d$. By the transformation property (6), this procedure yields a one-variable (i.e. elliptic) modular form of weight dk. Its level M is the positive generator of $\mathbb{Z} \cap \mathfrak{m}$, and its character Ψ is obtained by restriction of the character $\psi\omega^{1-k}$:

$$\Psi : (\mathbb{Z}/M\mathbb{Z})^\times \hookrightarrow (\mathscr{I}_{F,\mathfrak{m}}/\mathfrak{m})^\times \longrightarrow \mathbb{C}_p^\times. \tag{14}$$

The diagonal restriction $\Delta_{k,\psi}^{(p)}$ of the Eisenstein series $G_{k,\psi}^{(p)}$ introduced in § 2.2 is a modular form of level Mp, nebentypus Ψ, and weight dk. Its q-expansion is given by

$$\Delta_{k,\psi}^{(p)}(q) \;=\; L_p(\psi, 1-k) + 2^d \sum_{n \geq 1} \left(\sum_{\substack{\nu \in \mathfrak{d}_+^{-1} \\ \mathrm{Tr}(\nu) = n}} \; \sum_{\substack{\mathfrak{a} \mid (\nu)\mathfrak{d} \\ (\mathfrak{a}, \mathfrak{m}(p)) = 1}} \psi(\mathfrak{a}) \langle \mathrm{Nm}(\mathfrak{a}) \rangle^{k-1} \right) q^n. \tag{15}$$

The n-th Fourier coefficient a_n of the diagonal restriction (15) may be written as

$$a_n = 2^d \sum_{\mathcal{C} \in \mathrm{Cl}_{\mathfrak{m}}^+} \psi(\mathcal{C}) \sum_{(\mathfrak{a},\nu) \,\in\, \mathbb{I}(n,\mathcal{C})_{\mathfrak{m}(p)}} \langle \mathrm{Nm}(\mathfrak{a}) \rangle^{k-1} \tag{16}$$

where we define the index set by

$$\mathbb{I}(n, \mathcal{C})_{\mathfrak{b}} := \left\{ (\mathfrak{a}, \nu) \in \mathscr{I}_{F,\mathfrak{m}} \times \mathfrak{d}_+^{-1} \;:\; \begin{array}{ll} \mathrm{Tr}(\nu) = n, & \mathfrak{a} \mid (\nu)\mathfrak{d} \\ (\mathfrak{a}, \mathfrak{b}) = 1, & [\mathfrak{a}] = \mathcal{C} \end{array} \right\}. \tag{17}$$

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 (16) 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 multitude of different weights k, once the sets $\mathbb{I}(n, \mathcal{C})$ have been computed.

2.4. An algorithm to compute p-adic L-functions.

Following an idea of Hecke [Hec24, Satz 3], Klingen–Siegel [Kli62, Sie68] use the diagonal restrictions discussed above 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

$$\zeta_F(-1) = \frac{1}{60} \sum_{\substack{b < \sqrt{D} \\ b \equiv D \pmod 2}} \sigma_1\left(\frac{D - b^2}{4}\right) \tag{18}$$

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

$$\mathrm{Cl}_{\mathfrak{p}}^+ \simeq \mathbb{Z}/4\mathbb{Z} \tag{19}$$

so there is a unique quadratic character ψ of conductor $\mathfrak{p}$, which 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

$$M_4\left(\Gamma_1(5), \left(\frac{5}{\cdot}\right)\right) \tag{20}$$

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

$$\begin{cases} f_1 = 1 \qquad - 14q^2 - 52q^3 + \dots \\ f_2 = \qquad q + 7q^2 + 26q^3 + \dots \end{cases} \tag{21}$$

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

$$\Delta_{2,\psi} = L(\psi, -1) + 24q - 168q^2 - 624q^3 + \dots \tag{22}$$

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 $L(\psi, -1) = 24$.

To compute the p-adic L-series $L_p(\psi, T)$ we use the above idea of Siegel to find its value at sufficiently many weights k and then use interpolation. We now outline the main algorithm, and in the next section we discuss some economical methods for carrying out the various steps.

Remark 2.2. For simplicity, we will not include the special case $\psi\omega^{2-k} = 1$ in this discussion, when, due to the presence of a simple pole, one needs to modify the statements below. Since this modification is straightforward, and would only cloud the explanation of the algorithm, we thought it appropriate to omit this case from the discussion, see Example 3.6.

We use finite differences to interpolate values at integer weights, to compute the p-adic L-series $L_p(\psi, s)$ as a power series in $\mathcal{O}[\![s]\!]/(p^m)$ for some required p-adic precision m, with respect to the variable $s = 1 - k$ in $\mathbb{Z}_p$. For a discussion of this interpolation step in the same context, see Cartier–Roy [CR73]. Note that we obtain a different power series for each residue class in $\mathbb{Z}/(p-1)\mathbb{Z}$, and interpolation should be done over weights in this residue class. Since $L_p(\psi, T)$ belongs to $\mathcal{O}[\![T]\!]$ and $T = (1+q)^s - 1$, the series $L_p(\psi, s) \bmod p^m$ is in fact a polynomial of degree at most δ_m, where δ_m is the smallest integer such that

$$\begin{array}{lll} (p \neq 2) & i - v_p(i!) \geq m & \text{for all } i \geq \delta_m + 1, \\ (p = 2) & 2i - v_p(i!) \geq m & \text{for all } i \geq \delta_m + 1, \end{array} \tag{23}$$

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 $\delta_m + 1$ points and use interpolation. For each fixed $2 \leq k_0 \leq p$, we shall choose interpolation points

$$\begin{array}{lll} (p \neq 2) & k_j := k_0 + j(p-1) & \text{for } 0 \leq j \leq \delta_m, \\ (p = 2) & k_j := k_0 + 2j & \text{for } 0 \leq j \leq \delta_m, \end{array} \tag{24}$$

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

Algorithm 2.3. *Our input is:*

- k_0 *- an integer in* $[2, p]$,
- 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.*

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

(1) *Let M, Ψ be as in (14), and define k_j as in (24) for all $0 \le j \le \delta_m$ with δ_m as in (23). Let S be the Sturm bound for the space of classical modular forms of weight dk_{δ_m}, level $\Gamma_0(M)$, and nebentypus Ψ. Compute a basis for each of the classical spaces*

$$M_{dk_j}(\Gamma_0(M), \Psi) \qquad (\mathrm{mod}\ p^{\delta_m+1}, q^S), \qquad 0 \le j \le \delta_m.$$

(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 (17)*.*

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

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

(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 $M_{dk_j}(\Gamma_0(M), \Psi)$ modulo (p^{δ_m+1}, q^S). Then compute*

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

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

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

Remark 2.4. 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 which can work with p-adic numbers.

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 the steps above, using exact arithmetic instead, for simplicity.

As an illustration, we now run this algorithm for a totally real cubic field F.

Example 2.5. Letting $a \in \mathbb{R}$ satisfy the equation

$$a^3 - 3a - 1 = 0, \tag{25}$$

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 $\mathfrak{d} = (3a^2 - 3)$, so that every element of $\mathfrak{d}^{-1}$ is of the form

$$\nu = \frac{x + ya + za^2}{3a^2 - 3}, \tag{26}$$

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

$$\left\{ \begin{array}{rcrcr} (0.1316\ldots)x & + & (0.2474\ldots)y & > & -n(0.4650\ldots) \\ (-0.3791\ldots)x & + & (0.1316\ldots)y & > & -n(0.0457\ldots) \\ (0.2474\ldots)x & + & (-0.3791\ldots)y & > & n(0.5807\ldots). \end{array} \right. \tag{27}$$

For any fixed $n \geq 1$, there are a finite number of solutions in $x, y \in \mathbb{Z}$ which 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 (27).

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 $L_p(\psi, s)$ for $p = 7$ in the residue disk $s \equiv -1 \pmod{p-1}$. Here the prime 7 is inert in K. We take $m := 22$ which gives $\delta_m = 24$.

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 9 seconds (computing these bases with exact coefficients using in-built 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

$$\begin{aligned} \Delta_0 &= L_0 + 8q + 184q^2 - 3472q^3 + 8664q^4 + 2312q^5 + \ldots \\ \Delta_1 &= L_1 - 17464q + 48344125048q^2 + 77708960940464q^3 + \ldots \\ \Delta_2 &= L_2 - 12754552q + 778351185053184306 4q^2 + \ldots \\ \Delta_3 &= L_3 - 9298091704q + 1381740600368360259550697848q^2 + \ldots \\ \Delta_4 &= L_4 - 6778308875512q + 25817261000989696227095010854660 2744q^2 + \ldots \\ &\ \ \vdots \qquad\qquad \vdots \end{aligned} \tag{28}$$

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

$$\begin{array}{lcll} L_0 & = & -584/5 & \mathrm{mod} 7^{25} \\ L_1 & = & 644239567957910044930 & \mathrm{mod} 7^{25} \\ L_2 & = & 225053170195735060254 & \mathrm{mod} 7^{25} \\ L_3 & = & 1230313269957772629193 & \mathrm{mod} 7^{25} \\ L_4 & = & 645623798735766423256 & \mathrm{mod} 7^{25} \\ \vdots & & \vdots & \end{array} \tag{29}$$

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 $L_p(\psi, s)$ in s correct modulo 7^{22} and of degree 24, or alternatively

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

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	$640518113818292324494 + O(7^{25})$	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.

Remark 2.6. We note the striking similarity between the system of inequalities (27), and the Shintani cones appearing in the approach of Barsky and Cassou-Noguès [Bar78, CN79]. It is likely that the above computations can be made more efficient in cases where one can compute appropriate explicit Shintani cone decompositions, similar to those in Roblot [Rob15]. For the case of quadratic fields, which we turn to next, such cone considerations are made obsolete using results from [DPV] and computationally efficient routines for reduced cycles of indefinite quadratic forms.

2.5. **Comments on implementation.**

We now take a more detailed look at some of the steps of the algorithm of the previous section.

First we need to compute bases for the classical spaces

$$M_j := M_{d(k_0 + j(p-1))}(M, \Psi) \qquad \mathrm{mod}\ (p^{\delta_m + 1}, q^s). \tag{30}$$

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 which are smaller by a factor of roughly $(p+1)$. The practical problem of computing bases for the classical spaces M_j in step (1) has already been addressed by the first author; a very similar problem arises when one computes with overconvergent modular forms. In level 1 it is very easy and extremely fast in practice (this corresponds to the case of trivial conductor), and in higher level an elaborate but fast method has been developed and improved over several years. (We shall not discuss it here except to say it involves computing bases in *low* weight via modular symbols and multiplication of forms.)

As seen from the cubic example, finding the higher Fourier coefficients takes the bulk of the running time in practice. A much more efficient approach in the case where F is real quadratic is given in the next section. In that case, reduction theory for binary quadratic forms can be used to perform step (2) very efficiently. One additional advantage in the setting of real quadratic fields F 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 as in the algorithm. This then further eliminates the need to evaluate the character ψ on every element of X_n separately, causing additional savings in running time. In the general case, step (2) requires us to find an explicit description of the elements $\nu \in \mathfrak{d}_+^{-1}$ of trace n, for $1 \leq n \leq s-1$. In practice, one can compute generators for the principal ideal $\mathfrak{d}^{-1}$, and compute numerically the finite set of elements determined by the condition $\mathrm{Tr}(\nu) = n$ and the system of inequalities obtained from the total positivity conditions. Then we compute $\mathrm{Nm}(I)$ and $\psi(I)$ for the ideal divisors of all the ideals $(\nu)\mathfrak{d}$ thus obtained. Once this set is computed, simple linear algebra determines the constants L_j for all required j.

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.

3. 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 the algorithm in § 2.4. Its higher Fourier coefficients will be computed in terms of a certain set of 'RM points', which may be computed more efficiently via reduction theory of binary quadratic forms. We use some results that are contained in the forthcoming paper of the second author with Henri Darmon and Alice Pozzi [DPV].

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

$$\psi : \mathrm{Cl}_D^+ \longrightarrow \mathbb{C}_p^\times \tag{31}$$

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.

3.1. **The higher coefficients of diagonal restrictions.** We begin by putting the index set $\mathbb{I}(n, \mathcal{C})$ appearing in the expression (16) 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

$$a\tau^2 + b\tau + c = 0, \qquad a, b, c \in \mathbb{Z}, \quad b^2 - 4ac = D \tag{32}$$

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

$$\tau = \frac{-b + \sqrt{D}}{2a} \tag{33}$$

i.e. τ is the *stable* 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, suppose that $\mathcal{C} \in \mathrm{Cl}_D^+$ 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

$$\{A \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}) \ : \ \det(A) = n\} \quad = \quad \bigsqcup_{\gamma_n \in M_n} \mathbf{SL}_2(\mathbb{Z}) \cdot \gamma_n \tag{34}$$

$$= \quad \bigsqcup_{\delta_n \in N_n} \mathbf{SL}_2(\mathbb{Z}) \cdot \delta_n \cdot \mathrm{Stab}_{\mathbf{SL}_2(\mathbb{Z})}(\tau). \tag{35}$$

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

$$M_n = \left\{ \begin{pmatrix} n/d & j \\ 0 & d \end{pmatrix} : \qquad d | n, \quad (d, n/d) = 1, \quad 0 \leq j \leq d-1 \right\}. \tag{36}$$

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

$$\mathbb{RM}(n, \tau)_f := \left\{ (w, \delta_n) \ : \ \begin{matrix} \delta_n \in N_n, & w \in \mathbf{SL}_2(\mathbb{Z})\delta_n\tau \\ w > 0 > w', & (a(w), f) = 1 \end{matrix} \right\}. \tag{37}$$

The following lemma appears in [DPV] in the case $f = 1$, but is easily extended to general, not necessarily fundamental, discriminants D by the same argument.

Lemma 3.1. *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

$$\tau = \frac{-B + \sqrt{D}}{2A} \tag{38}$$

and define the integral ideal $I = (A, A\tau)$, whose class 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

$$w = \frac{-b + n\sqrt{D}}{2a} \tag{39}$$

where the integers a, b, c are defined by

$$\left\{\begin{array}{rcl} a & = & \mathrm{Nm}(\mathfrak{a}) \\ \nu & = & (-b + n\sqrt{D})/2\sqrt{D} \\ c & = & -\mathrm{Nm}(\mathfrak{b}). \end{array}\right. \tag{40}$$

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

$$\Lambda = \mathbb{Z}\lambda + \mathbb{Z}w\lambda \tag{41}$$

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 which 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

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

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

$$\begin{pmatrix} \lambda w \\ \lambda \end{pmatrix} = N \begin{pmatrix} A\tau \\ A \end{pmatrix}, \qquad \det N = n, \tag{42}$$

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

$$N \quad \in \quad \mathbf{SL}_2(\mathbb{Z}) \cdot \delta_n \cdot \mathrm{Stab}_{\mathbf{SL}_2(\mathbb{Z})}(\tau). \tag{43}$$

Note that δ_n is well-defined: If we multiply λ by a unit in $\mathcal{O}_F^\times \cap (\mathbb{Z} + f\mathcal{O}_F)$ which is totally positive, then N gets multiplied on the right by an element of $\mathrm{Stab}_{\mathbf{SL}_2(\mathbb{Z})}(\tau)$. 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

$$\begin{pmatrix} \lambda w \\ \lambda \end{pmatrix} = \gamma\delta_n \begin{pmatrix} A\tau \\ A \end{pmatrix}. \tag{44}$$

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

$$\mathfrak{a} = \mathrm{Nm}(\lambda I^{-1})/(\lambda I^{-1}), \qquad \mathfrak{b} = (\lambda w)I^{-1} \tag{45}$$

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

3.2. **Reduction theory of binary quadratic forms.** Now that we have established in Lemma 3.1 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 $\mathbb{RM}(n, \mathcal{C})_f$, 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

$$0 < \sqrt{\Delta} - b < 2|a| < \sqrt{\Delta} + b. \tag{46}$$

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

$$\begin{cases} \lambda^+ \in (0,1) & \lambda^- \in (-\infty, -1) & \text{if} \quad a > 0 \\ \lambda^+ \in (1,\infty) & \lambda^- \in (-1, 0) & \text{if} \quad a < 0. \end{cases} \tag{47}$$

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

$$\langle 5, 41, -17\rangle \qquad \text{and} \qquad \langle 19, 11, -25\rangle \tag{48}$$

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

As is clear from the description (47), any element $w \in \mathbf{SL}_2(\mathbb{Z})\delta_n\tau$ which 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 (36), and for each $\gamma_n \in M_n$ do the following steps.

(2) For any of the previously considered γ_n', test whether

$$\gamma_n' \cdot \mathrm{Stab}_{\mathbf{SL}_2(\mathbb{Z})}(\tau) \cdot \gamma_n^{-1} \subset \mathbf{SL}_2(\mathbb{Z}).$$

If it is for some γ_n', do nothing. If it is not 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 $1 \le i \le s$ the quadratic forms

$$\begin{array}{ll} \langle a + ib + i^2c,\ b + 2ic,\ c\rangle & \text{if} \quad a > 0 \\ \langle c,\ -b + 2ic,\ a - ib + i^2c\rangle & \text{if} \quad a < 0. \end{array}$$

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.

To increase efficiency, the sets $\mathbb{RM}(n,\tau)_f$ may be constructed inductively, by letting n_0 be the largest divisor of n, and computing it starting from $\mathbb{RM}(n_0,\tau)$, using the appropriate coset representatives of level (n/n_0). This variant causes a significant speed-up in practice.

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

Example 3.2. 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 3.5 and 3.6). 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

$$\mathrm{Cl}^+_{192} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \tag{49}$$

and the space of totally even functions on the class group is spanned by the two functions

$$\begin{array}{rcll} \psi_1 & = & \mathbf{1}_{[\mathcal{O}_F]} + \mathbf{1}_{[\mathfrak{d}]} & \\ \psi_2 & = & \mathbf{1}_{[\mathfrak{a}]} \quad + \mathbf{1}_{[\mathfrak{a}\mathfrak{d}]} & \text{where } \mathfrak{a} = (-3, (12+\sqrt{192})/2) \end{array} \tag{50}$$

which 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

$$\begin{array}{rcr} L(\psi_1,-1) & = & 35/12 \\ L(\psi_2,-1) & = & -37/12. \end{array} \tag{51}$$

Example 3.3. 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

$$\mathrm{Cl}^+_{1573} \simeq \mathbb{Z}/6\mathbb{Z}. \tag{52}$$

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

$$\begin{array}{rcll} \psi_1 & = & \mathbf{1}_{[\mathcal{O}_F]} + \mathbf{1}_{[\mathfrak{d}]} & \\ \psi_2 & = & \mathbf{1}_{[\mathfrak{a}]} \quad + \mathbf{1}_{[\mathfrak{a}\mathfrak{d}]} & \text{where } \mathfrak{a} = (17, (-31+11\sqrt{13})/2). \\ \psi_3 & = & \mathbf{1}_{[\mathfrak{a}^{-1}]} + \mathbf{1}_{[\mathfrak{a}^{-1}\mathfrak{d}]} & \end{array} \tag{53}$$

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

$$\begin{array}{rcl} L(\psi_1,-3) & = & 17291314/3 \\ L(\psi_2,-3) & = & -9930038/3 \\ L(\psi_3,-3) & = & -9930038/3. \end{array} \tag{54}$$

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

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

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

Example 3.4. 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

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

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 (23). Finally, we note that $L_5(\psi, 0) = 0$ 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 $\mathfrak{p}_1, \mathfrak{p}_2$ which 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 3.5. This setting will be revisited in Example 4.4 below. Let us take $D = 321$, and $F = \mathbb{Q}(\sqrt{321})$. We have

$$\mathrm{Cl}^+_{321} \simeq \mathbb{Z}/6\mathbb{Z}, \tag{55}$$

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

$$\begin{array}{rcll} \psi_1 & = & \mathbf{1}_{[\mathcal{O}_F]} - \mathbf{1}_{[\mathfrak{d}]} & \\ \psi_2 & = & \mathbf{1}_{[\mathfrak{a}]} \quad - \mathbf{1}_{[\mathfrak{a}\mathfrak{d}]} & \text{where } \mathfrak{a} = (4, (-15 + \sqrt{321})/2) \\ \psi_3 & = & \mathbf{1}_{[\mathfrak{b}]} \quad - \mathbf{1}_{[\mathfrak{b}\mathfrak{d}]} & \text{where } \mathfrak{b} = (2, (-15 + \sqrt{321})/2) \end{array} \tag{56}$$

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

$$\begin{array}{rcrrr} L_7(\psi_1, T) & \equiv & (3 + O(7^2))T^3 & -(10 + O(7^3))T^2 & +(913 + O(7^4))T \\ L_7(\psi_2, T) & \equiv & (1 + O(7^2))T^3 & +(211 + O(7^3))T^2 & +(340\cdot 7 + O(7^4))T \\ L_7(\psi_3, T) & \equiv & -(1 + O(7^2))T^3 & -(211 + O(7^3))T^2 & -(340\cdot 7 + O(7^4))T \end{array} \tag{57}$$

Which took a fraction of a second. In fact, with working precision 7^{60} one computes each of the series $L_7(\psi_j, s) \bmod p^{51}$ 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 $L_7(\psi_1, 0) = 0$ as it should due to the presence of an exceptional zero corresponding to $k = 1$, and it allows us to recover the derivative $L_7'(\psi_1, 0)$ modulo 7^{51} (the derivative here is with respect to s). As we explain in the next section, and will see in Example 4.4, 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. 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 $L_{101}(\psi_1, T)$ runs in 411 seconds, with all but 3 seconds taken up computing higher Fourier coefficients.

Example 3.6. 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

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

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

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

We call $\lambda = \deg(P)$. We observe that $\mu = 0$ in each case[2], which, since $L/\mathbb{Q}$ is abelian, is predicted 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 amount 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 that the p-adic L-function $L_p(\psi, T)$ 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 $L_p(\psi, T)$:

[2] 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.

- $p = 5$: 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
$$a = 71 \cdot 157 + 99 \cdot 157^2 + 8 \cdot 157^3 + 115 \cdot 157^4 + \dots$$
so that the p-adic L-function has 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.

- 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 that 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 that we may write
$$L_3(1, T) = F(T)/(T - 3)$$
where $F(T)$ is an element of the Iwasawa algebra which we compute to be
$$F(T) = -539 \cdot 3^2 T + 3929T^2 - 4910T^3 + \dots \qquad \pmod{3^{10}}.$$
and which is a power series with $(\lambda, \mu) = (2, 0)$. We note that $L_3(1, T)$ has a simple zero at $T = 0$, which is an exceptional zero caused by the fact that the unique prime above 3 is generated by a totally positive element.

Remark 3.7. 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].

4. Real quadratic fields: Overconvergence and derivatives

The algorithm in § 2.4 can also be recast in terms of overconvergent modular forms. Since the underlying computations which 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 which uses in an essential manner overconvergent modular forms, following recent results of the second author with Henri Darmon and Alice Pozzi [DPV]. 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 4.1. 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].

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

$$\psi : \mathrm{Cl}_D^+ \longrightarrow \mathbb{C}_p^\times \tag{58}$$

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. If $p \nmid D$ is a prime which is inert in F, then the vanishing of the Euler factor implies that we have an *exceptional zero*, i.e.

$$L_p(\psi, 0) = 0. \tag{59}$$

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

4.1. 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 $\omega^{\otimes p-1}$ with q-expansion 1. There is a reduction map

$$\mathrm{red}\ :\ \mathcal{X}(\mathbb{C}_p) \longrightarrow \mathcal{X}_s(\overline{\mathbb{F}}_p), \tag{60}$$

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 set of $\mathbb{C}_p$-points correspond to elliptic curves with ordinary reduction. It 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

$$X_r(\mathbb{C}_p) := \{x \in X(\mathbb{C}_p) \ :\ v_p(\widetilde{A}_x) \leq v_p(r)\}, \tag{61}$$

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

$$M_k^\dagger(r) := H^0(X_r, \omega^{\otimes k}). \tag{62}$$

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

$$\left\{ r^{ni}\frac{a_{i,j}}{E^i} \right\}_{i,j} \tag{63}$$

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].

4.2. **Derivatives of families of overconvergent modular forms.** In the situation considered above, we know that for trivial reasons, we must have $L_p(\psi, 0) = 0$ when p is inert in F. In light of the techniques in this paper, this may be interpreted as saying that the diagonal restriction of the Eisenstein series $G_{1,\psi}$ vanishes at the cusp ∞. The following theorem, proved in Darmon–Pozzi–Vonk [DPV], states that also its higher Fourier coefficients vanish.

Theorem 4.2. *Suppose that $p \nmid D$ is inert in the real quadratic field F, then the diagonal restriction of the Hilbert Eisenstein series $G_{1,\psi}$ 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

$$H(q) = L_p'(\psi, 0) + 4\sum_{n\geq 1}\left(\sum_{\mathcal{C}\in \mathrm{Cl}_{\mathfrak{m}}^+} \psi(\mathcal{C}) \sum_{(\mathfrak{a},\nu)\,\in\,\mathbb{I}(n,\mathcal{C})} \psi(\mathfrak{a}) \log_p\left(\mathrm{Nm}(\mathfrak{a})\right)\right) q^n. \tag{64}$$

Note that we are now in a situation very similar to that of the main algorithm above: The constant term $L_p'(\psi, 0)$ is the quantity we wish to compute, and the higher coefficients may be computed very efficiently using the methods from § 3. The crucial difference is that the form $H(q)$ is *not* a classical modular form. The following lemma can be found in [DPV]:

Lemma 4.3. *The series $H(q)$ is the q-expansion of an element in $M_2^\dagger(r)$, for every $r < p/(p+1)$.*

The above observations now lead to an algorithm very similar to the one in § 2.4, which computes the value $L_p'(\psi, p)$ directly. Indeed, having an explicit orthonormal basis (63) for the spaces $M_2^\dagger(r)$, which may be computed very efficiently using the algorithms in [Lau11], we can determine the constant term of $H(q)$ from the higher coefficients as before.

Example 4.4. Let us consider the setting of Example 3.5, 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

$$\begin{array}{rcrr} L_7'(\psi_1, 0) & = & 6477196952606172569528507807016822842117113120451 \cdot 7 & \pmod{7^{60}} \\ L_7'(\psi_2, 0) & = & 2400060771017313457866042007390913798673505846408 \cdot 7^2 & \pmod{7^{60}} \\ L_7'(\psi_3, 0) & = & -2400060771017313457866042007390913798673505846408 \cdot 7^2 & \pmod{7^{60}}. \end{array}$$

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

$$7^{16}u^6 - 20976 \cdot 7^8u^5 - 270624 \cdot 7^4u^4 + 526859689u^3 - 270624u^2 - 20976u + 7^4 = 0 \tag{65}$$

and is therefore a 7-unit in the narrow Hilbert class field of $\mathbb{Q}(\sqrt{321})$, as predicted by the main result of Darmon–Dasgupta–Pollack [DDP11]. The computations took 13 seconds in total.

References

[Bar78] D. Barsky. *Fonctions zêta padiques d'une classe de rayon des corps totalement réels*, Groupe d'études d'analyse ultramétrique, 1977-1978; errata 1978-1979. ↑1, 9.

[BV07] J. Buchmann, U. Vollmer. *Binary Quadratic Forms*, Springer-Verlag, Berlin; Algorithms and Computation in Mathematics **20** (2007) ↑13.

[CR73] P. Cartier, Y. Roy, *Certains calculs numériques relatifs à l'interpolation p-adique des séries de Dirichlet.* (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 269–349. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973. ↑2, 6.

[CN79] P. Cassou-Noguès, *Valeurs aux entiers négatifs des fonctions zeta et fonctions zeta p-adiques*, Invent. Math., **51** (1979), 29–60. ↑1, 9.

[CD14] P. Charollois, S. Dasgupta. *Integral Eisenstein cocycles on GL_n, I : Sczech's cocycle and p-adic L-functions of totally real fields* Cambridge J. of Mathematics, Vol 2.1 (2014), 49-90. ↑1.

[CDG15] P. Charollois, S. Dasgupta, and M. Greenberg *Integral Eisenstein cocycles on GL_n, II : Shintani's method* Commentarii Math. Helv. , Vol. 90.2 (2015), 435-477. ↑1.

[Coh76] H. Cohen, *Variations sur un thème de Siegel et Hecke.* Acta Arith. 30 (1976/77), no. 1, 63–93. ↑2.

[DPV] H. Darmon, A. Pozzi, J. Vonk. *Gross–Stark units, Stark–Heegner points, and derivatives of p-adic Eisenstein families*, preprint. ↑2, 9, 10, 11, 17, 19.

[DPV2] H. Darmon, A. Pozzi, J. Vonk. *On the RM values of the Dedekind–Rademacher cocycle*, in preparation. ↑18.

[Das07] S. Dasgupta. *Computations of Elliptic Units for Real Quadratic Fields*, Canadian Journal of Mathematics, 59 (2007), 553-574. ↑2, 17.

[Das08] S. Dasgupta. *Shintani Zeta Functions and Gross-Stark Units for Totally Real Fields*, Duke Mathematical Journal, 143 (2008), no. 2, 225-279. ↑17.

[DDP11] S. Dasgupta, H. Darmon, and R. Pollack. *Hilbert modular forms and the Gross–Stark conjecture.* Ann. of Math. (2) **174** (2011), no. 1, 439–484. ↑3, 4, 17, 20.

[DR80] P. Deligne, K. Ribet. *Values of abelian L-functions at negative integers over totally real fields.* Inventiones Mathematicae **59** (1980) 227–286. ↑1.

[EJV11] J.S. Ellenberg, S. Jain, A. Venkatesh. *Modeling λ-invariants by p-adic random matrices.* Comm. Pure Appl. Math. 64 (2011), no. 9, 1243–1262. ↑17.

[FW79] B. Ferrero, L.C. Washington. *The Iwasawa invariant μ_p vanishes for abelian number fields.* Ann. of Math. (2) 109 (1979), no. 2, 377–395. ↑16.

[Hec24] E. Hecke. *Analytische Funktionen und Algebraische Zahlen. Zweiter Teil.* Abhandlungen aus dem Mathematischen Universität Bd. 3 (1924) 213–236. ↑1, 5.

[Kli62] H. Klingen. *Über die Werte der Dedekindschen Zetafunktion.* Math. Annalen 145 (1962), 265–272. ↑5.

[Kat73] N. Katz, *p-Adic properties of modular schemes and modular forms*, in "Modular Forms in One Variable III", P. Deligne and W. Kuyk (eds), LNM **350**, Springer-Verlag, 69-190 (1973). ↑18, 19.

[Kat78] N. Katz, *p-Adic L-functions for CM fields*, Invent. Math. **49**, 199–297 (1978). ↑3.

[Lau11] A. Lauder, *Computations with classical and p-adic modular forms*, LMS J. Comput. Math. **14**, 214–231 (2011). ↑1, 2, 8, 18, 19.

[Lau14] A. Lauder, *Efficient computation of Rankin p-adic L-functions*, in "Computations with Modular Forms", Böckle G. and Wiese G. (eds), Springer Verlag (2014). ↑2, 8.

[Rob15] X.-F. Roblot, *Computing p-adic L-functions of totally real number fields*, Math. Comp. **84** (2015), no. 292, 831–874. ↑1, 2, 9.

[Ser73] J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques.* Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 191–268. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973. ↑1, 6.

[Shi76] T. Shintani. *An evaluation of zeta-functions of totally real algebraic fields at non-positive integers.* J. Fac. Sci., Univ. Tokyo, Sect. IA 23 (1976), 393–417 ↑1, 2.

[Shi78] G. Shimura. *The special values of the zeta functions associated with Hilbert modular forms.* Duke Math. J. **45** (1978) 637–678. ↑3.

[Sie68] C.L. Siegel. *Berechnung von Zetafunktionen an ganzzahlingen Stellen.* Nachr. Akad. Wiss. Göttingen, Math.-Phys. Klasse **2** (1968) 7–38. ↑1, 5.

[Sla07] K. Slavov. *Gross–Stark units for totally real number fields*, Senior thesis, Harvard University (2007). ↑2, 17.

[Von15] J. Vonk. *Computing overconvergent forms for small primes.* LMS J. Comp. Math., 18(1):250–257, 2015. ↑1, 2, 19.

Alan Lauder, Mathematical Institute, University of Oxford, Woodstock Road, Oxford OX2 6GG, UK

E-mail address: lauder@maths.ox.ac.uk

Jan Vonk, Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540, USA

E-mail address: vonk@ias.edu