p-adic L-functions à la Klingen-Siegel

Håvard Damm-Johnsen

September 2021

Contents

1 Introduction

L-functions are ubiquitous in modern number theory, and their behaviour is described by a number of important conjectures which have been verified in only a very limited number of cases. While computer calculation might be considered a good tool for testing the conjectures, historically some of their formulations – most notably the Birch–Swinnerton-Dyer conjecture – were directly inspired by numerical observations.

1.1 Historical background

The history of p-adic L-function can arguably be traced to Kummer's work on Fermat's last theorem. By studying class groups of cyclotomic fields, he found the surprising congruence

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \mod p^{m+1} \tag{1.1}$$

when k and k' are even integers satisfying $k \equiv k' \mod (p-1)p^m$. On the other hand, by Euler's solution to the Basel problem and the functional equation for the Riemann zeta function, we have

$$\zeta(1-k) = -\frac{B_k}{k}, \qquad k \text{ even}, \tag{1.2}$$

leading Kubota and Leopoldt to interpret eq. (3.5) as a congruence between special values of ζ. A density argument then gives a p-adic analytic function $\zeta_p \colon \mathbb{Z}_p \to \mathbb{C}_p$ which "interpolates" ζ in the sense that

$$\zeta_p(1-k) = (1-p^{1-k})\zeta(1-k), \qquad k \text{ even}. \tag{1.3}$$

The appearance of the factor $(1-p^{1-k})$ is conceptually explained as dividing out by the p-th Euler factor in the Euler product of ζ.

To be precise, we actually obtain a *collection* of analytic functions $\zeta_{p,i}(s)$ where $i \in (\mathbb{Z}/p\mathbb{Z})^\times$ is the congruence class of the integers k from which $\zeta_{p,i}$ is interpolated. This is often referred to as the i-th Iwasawa branch of ζ_p.

It is worth briefly mentioning a more conceptual construction of ζ_p: recall from the proof of the functional equation of ζ that ζ is, up to a factor of $(s-1)$, the *Mellin transform* of $f(t) = \frac{t}{e^t-1}$. This is the so-called "exponential generating function" of the Bernoulli numbers, meaning we have a formal expansion

$$\frac{t}{e^t-1} = \sum_{k=1}^{\infty} \frac{B_k t^k}{k!}. \tag{1.4}$$

Analogously we can define ζ_p as a "p-adic Mellin transform" of a suitably chosen "pseudo-measure". This ties into the interesting philosophy of treating analysis over the various completions of $\mathbb{Q}$ on equal footing, in contrast with the historical preference for the archimedean completions.

Dirichlet defined, as part of his work on primes in arithmetic progressions, L-functions attached to Dirichlet characters[1]. More precisely, let $\chi \colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a group homomorphism and extend to $\mathbb{Z}$ by the rule $\chi(p) = 0$ for $p \mid N$. Then we can define the *Dirichlet L-function*

$$L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^{-s}}, \qquad \Re(s) > 1, \tag{1.5}$$

[1] Of course, the name came later.

and in a manner similar to ζ show that L admits an Euler product and a functional equation. In particular, $L(\chi, s)$ is the Mellin transform of $\sum_{a=1}^{N} \frac{te^{at}}{e^{Nt}-1}$, which is the generating function of the so-called *generalised Bernoulli numbers*, $B_{k,\chi}$.

It is natural to ask whether these give rise to a p-adic analytic function like ζ_p, and indeed we can construct the p-adic L-function $L_p(\chi, s)$ simply by twisting the measure defining ζ_p by χ. In particular, $\zeta_{p,i}(s) = L_p(\omega^i, s)$ where $\omega\colon \mathbb{Z}/(p-1)\mathbb{Z} \to \mathbb{Z}_p$ is the Teichmüller character. This also features in the special value formula

$$L_p(\chi, 1-k) = (1-\chi\omega^{-k}(p)p^{k-1})L(\chi\omega^{-k}, 1-k), \qquad k \geq 1. \tag{1.6}$$

1.2 Overview

In XYZ we do ABC etc.

2 Theory

2.1 Hecke characters

The main reference for this section is [Miy89].

When extending the definition of the Riemann zeta function ζ to general number fields F, i.e. the Dedekind zeta function ζ_F, one immediately finds that the correct generalisation is to replace the summation over the integers in ζ to summation over integral ideals in $\mathcal{O}_F$, and then taking norms. If we would like to define an analogue of the Dirichlet L-functions to F, then it is necessary to define characters whose domain is the set of (integral) ideals of F, which is precisely what lead Hecke to define his Grössencharaktere:

Let $\mathfrak{m}$ be an integral ideal of F and set

$$J_{\mathfrak{m}} := \{\mathfrak{a} \leq \mathcal{O}_F : (\mathfrak{a}, \mathfrak{m}) = 1\} \quad \text{and} \quad P_{\mathfrak{m}} := \{(a) \leq \mathcal{O}_F : F^\times \ni a \equiv 1 \mod^\times \mathfrak{m}\}. \tag{2.1}$$

Here $a \equiv 1 \mod^\times$ means that we can find $b, c \in \mathcal{O}_F^\times$ coprime to $\mathfrak{m}$ such that $a = b/c$ and $b \equiv c \mod \mathfrak{m}$. Enumerate the r_1 real embeddings of F into $\mathbb{C}$ up to conjugation as σ_ν for $1 \leq \nu \leq r_1$ and the r_2 imaginary embeddings modulo conjugation as σ_ν for $r_1 \leq \nu \leq r_1 + r_2$.

Definition 2.1. A **Hecke character modulo** $\mathfrak{m}$ is a group homomorphism $\chi\colon J_{\mathfrak{m}} \to \mathbb{C}^\times$ satisfying for any $(a) \in P_{\mathfrak{m}}$,

$$\chi((a)) = \prod_{\nu=1}^{r_1+r_2} \left(\frac{\sigma_\nu(a)}{|\sigma_\nu(a)|}\right)^{u_\nu} |\sigma_\nu|^{iv_\nu}, \tag{2.2}$$

where $u_\nu \in \{0,1\}$ for $1 \le \nu \le r_1$ and $u_\nu \in \mathbb{Z}$ otherwise, and $v_\nu \in \mathbb{R}$ satisfy

$$\sum_{\nu=1}^{r_1+r_2} u_\nu = 0. \tag{2.3}$$

The tuple (u_ν) is called the **infinity-type** of χ.

Suppose χ is a Hecke character of modulus $\mathfrak{m}$. If $\mathfrak{m} \mid \mathfrak{m}'$, then χ is naturally a Hecke character of modulus $\mathfrak{m}'$ by restricting its domain to $J_{\mathfrak{m}'}$.

Definition 2.2. The minimal $\mathfrak{m}$ for which χ is a Hecke character of modulus $\mathfrak{m}$ is called the **conductor of** χ.

Definition 2.3. If $u_\nu = 0$ for all $r_1 + 1 \le \nu \le r_2$ and $v_\nu = 0$ for all ν, in other words, if χ has infinity-type $(u_1, \dots, u_{r_1}, 0, \dots, 0)$ then χ is called a **ray class character**.

Since χ is then trivial on the *principal ray* $P_{\mathfrak{m}'}$ corresponding to some modulus $\mathfrak{m}' = \mathfrak{m}\mathfrak{m}_\infty$, where $\mathfrak{m}_\infty$ is determined by $\{u_\nu : 1 \le \nu \le r_1\}$, χ descends to a character on the ray class group, $\overline{\chi} \colon \mathrm{Cl}_{\mathfrak{m}'} \to \mathbb{C}^\times$. We will later restrict our attention to Hecke characters of this type.

Example 2.4. Let χ be any Dirichlet character. Then $\chi \circ \mathrm{Nm}_{F/\mathbb{Q}}$ is a Hecke character of F, called the *base change of* χ *to* F.

Example 2.5. Fix $m \in \mathbb{N}_{>1}$. For a non-zero prime ideal $\mathfrak{p}$ in $\mathbb{Q}(\zeta_m)$ coprime to m with $p := \mathrm{Nm}\,\mathfrak{p}$, and fixing $x \notin \mathfrak{p}$, let $\chi_\mathfrak{p}(x)$ be the root of unity in $\mathbb{Q}(\zeta_m)$ satisfying

$$\chi_\mathfrak{p}(x) \equiv x^{\frac{p-1}{m}} \mod \mathfrak{p}. \tag{2.4}$$

If $a = (a_j) \in (\mathbb{Z}/m\mathbb{Z})^r$ is any non-zero vector, then we can define

$$J_a(\mathfrak{p}) := (-1)^{r+1} \sum_{\substack{x_1,\dots,x_r \bmod \mathfrak{p} \\ \sum x_j \equiv -1 \bmod \mathfrak{p}}} \chi_\mathfrak{p}(x_k)^{a_j}. \tag{2.5}$$

Weil showed in [Wei52] that J_a is in fact a Hecke character modulo (m^2) on $\mathbb{Q}(\zeta_m)$.

As with Dirichlet characters, we extend χ to ideals $\mathfrak{a}$ not coprime to $\mathfrak{m}$ by setting $\chi(\mathfrak{a}) = 0$.

The observation leading to the perhaps strange-looking definition of a Hecke character was the following: if $F = \mathbb{Q}(\sqrt{D})$ with class number h and $\mathfrak{a} \le \mathcal{O}_F$ is an integral ideal, then we can fix $\alpha \in F^\times$ such that $(\alpha) = \mathfrak{a}^h$. Then

$$\chi(\mathfrak{a}) := \begin{cases} \exp\left(\frac{\pi i}{\log|\epsilon|} \left|\frac{\alpha}{\alpha'}\right|\right) & \text{if } D > 0, \\ \left(\frac{\alpha}{|\alpha|}\right)^2 & \text{if } D < 0, \end{cases} \tag{2.6}$$

where ϵ is a fundamental unit of F and α' is the conjugate of α, defines a character on the set of ideals of $\mathcal{O}_F$. Hecke proved that these admit L-functions which behave like Dirichlet L-functions.

Definition 2.6. Fix a Hecke character χ. The **Hecke L-function** attached to χ is given by the Dirichlet series

$$L(\chi, s) := \sum_{\mathfrak{a} \leq \mathcal{O}_F} \chi(\mathfrak{a}) \operatorname{Nm}(\mathfrak{a})^{-s}. \tag{2.7}$$

Example 2.7. If χ is the trivial character of modulus $\mathfrak{m} = (1)$, then $L(\chi, s) = \zeta_F(s)$.

Example 2.8. Returning to example 2.5, Weil proved that the L-functions $L(J_a, s)$ agree with the Hasse-Weil L-functions of a family of hyperelliptic curves, establishing a special case of the Hasse-Weil conjecture. This strategy of proving meromorphy of Hasse-Weil L-functions was later adopted by Deuring to CM elliptic curves, and by Shimura and Taniyama to CM abelian varieties. Some explicit examples are worked out in [IR90, Ch.18].

A key aspect of the characters (pun intended) appearing in this story is that they are *algebraic*, which means they naturally occur as one-dimensional complex representations of the absolute Galois group of a number field. The so-called *Weil group*, an "enlargement", seems to encompass also the non-algebraic ones.

There seems to be an analogy between Hecke characters of "complicated" infinity-type (i.e. non-algebraic, or perhaps even non-ray class characters) and Maaß forms; perhaps ask James about this? Related: SO post – the answer says non-alg Hecke chars are analogous to non-alg Maaß forms, i.e. those of eigenvalue $> 1/4$.

Proposition 2.9. *Let χ be a Hecke character, and $L(\chi, s)$ the associated Hecke L-function.*

(i) *$L(\chi, s)$ converges uniformly and absolutely on the half-plane $\Re(s) > 1 + \epsilon$ for any $\epsilon > 0$;*

(ii) *$L(\chi, s)$ has an Euler product*

$$L(\chi, s) = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p}) \operatorname{Nm}(\mathfrak{p})^{-s}}, \tag{2.8}$$

where $\mathfrak{p}$ runs over prime ideals of $\mathcal{O}_F$.

(iii) *Let*

$$\Lambda(\chi, s) := \left(\frac{2^{r_1} |\Delta_F| \operatorname{Nm}(\mathfrak{m})}{(2\pi)^g}\right) \prod_{\nu=1}^{r_1+r_2} \Gamma\left(\frac{n_\nu s + |u_\nu| + i v_\nu}{2}\right) L(\chi, s), \tag{2.9}$$

where $n_\nu = 1$ if $1 \leq \nu \leq r_1$ and $n_\nu = 2$ otherwise. Then Λ extends to a meromorphic on $\mathbb{C}$, and satisfies

$$\Lambda(\chi, 1 - s) = T(\chi) \Lambda(\overline{\chi}, s), \tag{2.10}$$

for some $T(\chi) \in \mathbb{C}$ depending only on χ which satisfies $|T(\chi)| = 1$.

(iv) *If χ is trivial, then Λ is holomorphic except for poles at $s = 0$ and $s = 1$; otherwise Λ is entire.*

Proof. See [Miy89, §3.3]. □

(iii) was originally proved using a method similar to Riemann's, namely by realising $L(\chi, s)$ as the Mellin transform of some theta function attached to χ, generalising the classical theta function $\theta(x) := \sum_{n\in\mathbb{Z}} e^{2\pi i n^2}$. This was recast more conceptually in the language of adèles by Tate in his famous PhD thesis, see [CF67, Ch.XV].

In the language of adèles, a Hecke character is nothing but a character on the idèle class group.

2.2 *L*-functions of totally real fields

It is natural to try to extend the constructions of the previous section from $\mathbb{Q}$ to a general number field F. Suppose χ is a ray class character over a field which admits both a real and a complex embedding. By eq. (2.9), the functional equation then has the form fix this

$$\Lambda(chi, s) = \epsilon\Lambda(\overline{\chi}, 1-s), \qquad \Lambda(\chi, s) = C(\chi)^s \Gamma\left(\frac{s}{2}\right)^a \Gamma\left(\frac{s+1}{2}\right)^b L(\chi, s), \tag{2.11}$$

where $|\epsilon| = 1$, $C(\chi)$ is some constant depending on χ, and $a, b \in \mathbb{Q}$. Here $a = 0$ (resp. b) is non-zero iff F has a real (resp. imaginary) embedding into $\mathbb{C}$. We can rearrange this to obtain an expression for $L(chi, 1-s)$ in terms of $L(\chi, s)$. For $k \gg 0$, the values $L(\chi, k)$ are finite and easily seen to be non-zero. However, since Γ has poles at the negative integers, the occurrence of both real and complex embeddings implies that the values $L(\chi, 1-k)$ all vanish unless F has either only real or only non-real embeddings into $\mathbb{C}$. Accordingly we can only hope to p-adically interpolate L-functions attached to totally real or totally imaginary number fields. cf Cassels Frollick? Probably Tate's thesis

Fix F a totally real field, $\psi\colon \mathrm{Cl}_{\mathfrak{m}}(F) \to \mathbb{C}^\times$ a ray class character and p a prime. We define the *Hecke L-function associated to* ψ by

$$L(\psi, s) := \sum_{\substack{\mathfrak{a}\leq\mathcal{O}_F \\ (\mathfrak{a},\mathfrak{m})=1}} \psi(\mathfrak{a})\,\mathrm{Nm}(\mathfrak{a})^{-s}, \tag{2.12}$$

where by $\psi(\mathfrak{a})$ we mean ψ evaluated at the class of $\mathfrak{a}$ in $\mathrm{Cl}_{\mathfrak{m}}$. Hecke showed that $L(\psi, s)$ has an Euler product. It was possibly known to Hecke, and at any rate to Siegel and Klingen, that the special values $L(\psi, 1-k)$ are rational when k is an even integer. TODO: Write out the argument maybe? This was later proved

by Shintani using analytical methods. Removing the Euler factors above p, the resulting special values

$$L_p(\psi, 1-k) := \prod_{\mathfrak{p}|(p)} (1 - \psi(\mathfrak{p}) \operatorname{Nm}(\mathfrak{p})^{k-1}) L(\psi, 1-k) \tag{2.13}$$

interpolate p-adically by the work of Deligne-Ribet [DR80] to a p-adic analytic function $L_p(\psi, s) \colon \mathbb{Z}_p \to \mathbb{C}_p$, or alternatively by the work of Barsky and Cassou-Nogues [Cas79], which is based on Shintani's method.

Example 2.10. Perhaps it's better to write this out in detail?

Taking $F = \mathbb{Q}$, $\mathfrak{m} = (1)$ and ψ trivial recovers the construction of the Kubota-Leopoldt p-adic L-function ζ_p, which interpolates $(1 - p^{k-1})\zeta(1-k)$.

2.3 p-adic interpolation

The main way of representing $L_p(\psi, s)$ is as a power series over $\mathbb{Q}_p$. From a computational point of view, it is natural to approximate this by polynomials. To avoid heavy arithmetic over $\mathbb{Q}_p$, it is convenient to use Newton's divided differences method; Lagrange interpolation would require divison by elements of $\mathbb{Z}_p$, which could lead to precision loss.

2.4 The algorithm

We now describe the algorithm for computing a polynomial approximation of $L_p(\psi, s)$.

Algorithm 1: Compute $L_p(\psi, s)$

Input:

- F a totally real number field of degree d,
- p an odd prime,
- $\psi\colon \mathrm{Cl}_{\mathfrak{m}} \to \mathbb{C}^\times$ a totally odd or even Hecke character of F of modulus $\mathfrak{m}$,
- $k_0 \in [2, p]$ with same parity as ψ,
- $m \in \mathbb{N}$.

Output: $P(s) \in \mathbb{Z}_p[q]/(p^{\delta_m}, q^m)$ approximating $L_p(\psi, s)$

$\Psi, M \leftarrow$ `Diricihlet`(ψ) `// Described in subroutine X`

$\delta_m \leftarrow m\frac{p-1}{p-2}$
$S \leftarrow$ Sturm bound for $M_{dk_j}(\Gamma_0(\Psi))$

for $j = 0, \ldots, \delta_m$ **do**
  $k_j \leftarrow k_0 + j(p-1)$
  $M_{dk_j} \leftarrow$ basis for $M_{dk_j}(\Gamma_1(M))$ mod q^S
  `/* Described in subroutine Y */`
  $\Delta_j(q) \leftarrow 2^d \sum_{n=1}^{S-1} \sum_{\nu \in \mathfrak{d}_+^{-1}} \sum_{\mathfrak{a} \mid (\nu)\mathfrak{d}} \psi(\mathfrak{a}) \mathrm{Nm}(\mathfrak{a})^{k_j - 1} q^n$
  `/* Described in subroutine Z */`

  $L(\psi, 1-k_j) \leftarrow$`find_const_term`$(\Delta_j, M_{dk_j})$
  $L_p(\psi, 1-k_j) \leftarrow L(\psi, 1-k_j) \cdot \prod_{\mathfrak{p} \mid (p)} (1 - \psi(\mathfrak{p}) \mathrm{Nm}(\mathfrak{p})^{k_j - 1})$

$P(s) \leftarrow$ `Newton_poln`$\{(1-k_j, L_p(\psi, 1-k_j)) : j = 0, \ldots \delta_m\}$

Example 2.11. Let $F = \mathbb{Q}(\sqrt{5})$, $p = 3$ and $\mathfrak{m} = (4)$. Then $\mathrm{Cl}_{\mathfrak{m}}^+ \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, with generators $\mathfrak{a} = (41, \frac{13+\sqrt{5}}{2})$ and $\mathfrak{b} = (11, \frac{15+\sqrt{5}}{2})$. We fix the totally odd character ψ on $\mathrm{Cl}_{\mathfrak{m}}^+$ defined by $\psi(\mathfrak{a}) = 1$ and $\psi(\mathfrak{b}) = -1$. Running the algorithm above with $m = 8$ and $k_0 = 3$ then gives

$$\begin{aligned} P(s) = \ldots &+ \left(3^{11} \cdot 2 + O(3^{12})\right)s^{16} + \left(3^9 \cdot 22 + O(3^{12})\right)s^{15} + \left(3^{10} \cdot 2 + O(3^{12})\right)s^{14} + \left(3^8 \cdot 10 + O(3^{12})\right)s^{13} \\ &+ \left(3^9 \cdot 5 + O(3^{12})\right)s^{12} + \left(3^7 \cdot 97 + O(3^{12})\right)s^{11} + \left(3^7 \cdot 157 + O(3^{12})\right)s^{10} + \left(3^5 \cdot 914 + O(3^{12})\right)s^9 \\ &+ \left(3^7 \cdot 98 + O(3^{12})\right)s^8 + \left(3^5 \cdot 976 + O(3^{12})\right)s^7 + \left(3^6 \cdot 598 + O(3^{12})\right)s^6 + \left(3^4 \cdot 20 + O(3^{12})\right)s^5 \\ &+ \left(3^4 \cdot 19067 + O(3^{13})\right)s^4 + \left(3^2 \cdot 369067 + O(3^{14})\right)s^3 + \left(3^3 \cdot 185023 + O(3^{15})\right)s^2 \\ &+ \left(3 \cdot 1380869 + O(3^{16})\right)s + 3^{17} \cdot 2 + O(3^{18}) \end{aligned}$$

We note 1) that the 3-adic valuation of the n-th coefficient of $P(s)$ is roughly n so the general term tends to zero in 3-adic absolute value, and 2) that the high power

of 3 dividing the constant term is likely explained by $L_3(\psi, 0) = 0$. As in [LV21, Example 3.4], this simply reflects the fact that 3 is inert in $\mathbb{Q}(\sqrt{5})$, so $\psi(3) = 1$ as ψ is trivial on principal ideals. The Euler factor at p is $(1 - 1 * \mathrm{Nm}(p)^{1-1}) = 0$, and so $L_p(\psi, 0) = 0$. The branch of $k_0 = 1$ similarly gives

$$P(s) = ... + \left(3^2 \cdot 191920 + O(3^{14})\right) s^3 + \left(3^3 \cdot 185023 + O(3^{15})\right) s^2 + \left(3 \cdot 10946807 + O(3^{16})\right) s$$

with a clear zero at $s = 0$.[2]

Similarly, for $p = 5$ which is ramified in F, we see that

$$P(s) = ... + \left(5^3 \cdot 142289 + O(5^{11})\right) s^3 + \left(5^2 \cdot 1002202 + O(5^{11})\right) s^2 + \left(5 \cdot 19298281 + O(5^{12})\right) s + O(5^{13})$$

2.5 Lambda-invariants

2.5.1 A quick summary of EJV

Here we should talk about [EJV11]. Also mentioned by [Rob13], better check this out

2.5.2 Mention results of Santato?

Let $K/\mathbb{Q}_p$ be a finite extension, and $\mathcal{O}_K$ its ring of integers, with uniformiser ϖ. The structure of power series over K is well-understood by the following theorem:

Theorem 2.12 (Weierstraß preparation theorem)**.** *Let $f \in \mathcal{O}_K[[T]]$ be a power series. Then f factors as*

$$f(T) = \varpi^{\mu} P(T) u(T), \tag{2.14}$$

where $\mu \in \mathbb{Z}_{\geq 0}$, $P(T) \in \mathcal{O}_K[T]$ and $u(T) \in \mathcal{O}_K[[T]]^{\times}$.

The number μ is called the *(Iwasawa) μ-invariant* of f, and $\lambda := \deg P(T)$ its *λ-invariant*.

The λ-invariants of p-adic L-functions are particularly interesting because of their connection to Iwasawa theory. For the μ-invariant, we have the following theorem:

Theorem 2.13 (Ferrero-Washington)**.** *Suppose F is a totally real abelian number field, p is prime and χ a ring class character of F. Then the μ-invariant of the associated p-adic L-function $L_p(\chi, s)$ is* 0.

[2] The omission of $O(3^{18})$ in the branch at 1 comes from the fact that the special value at 1 is 0, whereas for the branch at 3 we didn't actually compute this value.

For a reference, see [Lan90, §10].

Give some examples of non-abelian extensions with non-zero μ?

The theorem was conjectured by Iwasawa, and he also gave a counterexample to show that we cannot expect the result to hold for arbitrary fields:

Example 2.14.

3 Implementation

We now describe how to interpolate $L_p(\psi, s)$ (somewhat) efficiently, at least in the case of $F = \mathbb{Q}(\sqrt{D})$ a real quadratic field. The ticket "Ray class groups and Hecke characters " brings experimental support for Hecke characters to `sage`, allowing us in particular to evaluate Hecke characters at ideals explicitly. However, this remains inefficient in practice, since in the computation of the higher Fourier coefficients of the diagonal restriction we need to perform this evaluation a very large number of times. For real quadratic fields, we can circumvent this with a method described in section 3.2.

3.1 An algorithm for quadratic fields

3.2 The quadratic forms method

If we take ψ to be a *ring class character*, i.e. a character of $\mathrm{Cl}^+_{(f)}(F)$, then we can use the classical reduction theory of indefinite quadratic forms to find the coefficients of the diagonal restrictions much more efficiently.

One can show that if ψ is totally even (resp. odd), then ψ is a linear combination of functions $\mathbb{1}_{\mathfrak{a}} + \mathbb{1}_{\mathfrak{b}}$ (resp. $\mathbb{1}_{\mathfrak{a}} - \mathbb{1}_{\mathfrak{b}}$) where

$$\mathbb{1}_{\mathfrak{a}} \colon \mathrm{Cl}^+_{(f)} \to \{\pm 1\}, \qquad \mathbb{1}_{\mathfrak{a}}(\mathscr{C}) = \begin{cases} 1 & \text{if} \quad [\mathfrak{a}] = \mathscr{C}, \\ 0 & \text{otherwise.} \end{cases} \tag{3.1}$$

If we have a decomposition $\psi = \sum_{\mathfrak{a},\mathfrak{b}} \mathbb{1}_{\mathfrak{a}} \pm \mathbb{1}_{\mathfrak{b}}$ for some fixed sign $\pm$, then we can compute Δ_j by splitting the sum into partial sums corresponding to fixed classes in the narrow class group.

[[[Can we do this automatically?]]]

Example 3.1. Let $F = \mathbb{Q}(\sqrt{5})$

3.2.1 Computing sets of nearly reduced forms

Compute $\mathbb{I}(n, \mathscr{C})$ *using* $\mathbb{I}(d, \mathscr{C})$ *for some* $d|n$: Input: - n a positive integer.

(i) For $m = n/d$, compute matrices of the form

$$\begin{pmatrix} m & j \\ 0 & m/d' \end{pmatrix}, \qquad 0 < j < d', \tag{3.2}$$

for all $d' || m$.
(ii) For each

Finding nearly reduced forms: This step has a natural interpretation in terms of the so-called Conway polytope: given our indefinite quadratic form $Q_0 = Q|_\gamma$, we first perform Gaussian reduction to obtain a reduced form, which necessarily lies on the *river*. Now we apply translation and add each translate to our list of nearly reduced forms iteratively, until we reach another reduced form. When this happens, we reflect, and then continue translating. We continue the process of translating and reflecting until we return to our first reduced form, at which point the algorithm terminates, and we return the list nearly reduced forms.

If $F = \mathbb{Q}(\sqrt{D})$, $Q = \langle a, b, c\rangle$ is an indefinite quadratic form with positive root $\tau = \frac{-b+\sqrt{D}}{2a}$ for some integers $a, b, c \in \mathbb{Z}$, then Q determines an embedding of $\mathcal{O}_F$ into $M_2(\mathbb{Z})$ by $\alpha(\sqrt{D}) = \begin{pmatrix} -b & -2c \\ 2a & a \end{pmatrix}$; indeed,

$$\begin{pmatrix} -b & -2c \\ 2a & a \end{pmatrix}^2 = \begin{pmatrix} b^2 - 4ac & 2bc - 2bc \\ -2ab + 2ab & -4ac + b^2 \end{pmatrix} = D\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We view this as an embedding of the quadratic order $\mathcal{O}_F$ into the maximal order $M_2(\mathbb{Z})$ of the split quaternion algebra $M_2(\mathbb{Q})$. For any $x \in F$, the action

$$x \cdot M = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} M \cdot \alpha(x) + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} M \cdot \alpha(\overline{x}), \tag{3.3}$$

makes $M_2(\mathbb{Q})$ a 2-dimensional vector space over F.

Lemma 3.2. *There is a natural decomposition $M_2(F) = M_+ \oplus M_-$, where*

$$M_+ = \{M \in M_2(F) : x \cdot M = xM\} \quad \textit{and} \quad M_- = \{M \in M_2(F) : x \cdot M = \overline{x}M\}.$$

(Q: is this just the eigenspace decomposition?) Now let $B : M_2(\mathbb{Q}) \to F$ be composition $M_2(\mathbb{Q}) \hookrightarrow M_2(F) \xrightarrow{\mathrm{pr}_+} M_+ \xrightarrow{\det} F$.

Proposition 3.3. *The map $B : M_2(\mathbb{Q}) \to F$ satisfies*

(i) $B(x \cdot M) = x^2 B(M)$,
(ii) $\mathrm{tr}_{F/\mathbb{Q}} B(M) = \det M$,

and is uniquely characterised by these properties.

Recall that for $\alpha \in F$, we write $\alpha \gg 0$ if α is *totally positive*, that is, if $\sigma(\alpha) > 0$ for all embeddings $\sigma\colon F \hookrightarrow \mathbb{R}$.

Proposition 3.4. *Let $F = \mathbb{Q}(\sqrt{D})$ be a real quadratic field and $\mathscr{C} \in \mathrm{Cl}^+$ a fixed class in its narrow class group. Let*

$$\mathbb{I}(n,\mathscr{C}) := \left\{ (\mathfrak{a},\nu) : \begin{array}{l} \nu \in \mathfrak{d}^{-1},\ \nu \gg 0, \\ \mathrm{tr}(\nu) = n \\ \mathfrak{a} \mid (\nu)\mathfrak{d},\ [\mathfrak{a}] = \mathscr{C} \end{array} \right\} \tag{3.4}$$

and

$$M(n,\mathscr{C}) := \left\{ \gamma \in M_2(\mathbb{Z})/\alpha(\mathcal{O}_F^\times) : \begin{array}{l} \det\gamma = n \\ \det_F(\gamma) \gg 0 \end{array} \right\}. \tag{3.5}$$

Then there is a bijection $\mathbb{I}(n,\mathscr{C}) \leftrightarrow M(n,\mathscr{C})$.

3.3 Optimisations of the naïve algorithm

- Parallelising the Δ-step
- Randomised bases in sage
- Storing values of $\psi(\mathfrak{p})$ in a dictionary (introduces additional complexity of shared memory between processes)
- Compare with magma algorithm?
- Speed up computations by working mod p^N; should actually matter once we go big
- Discussion of why this isn't good enough for statistics:
  - computing mfs with large level on Γ_1 is still very inefficient in `sage` because Sturm bound gets large; forces computation of MANY coeffs
  -

4 Future investigations

Bibliography

[Cas79] Pierrette Cassou-Nogues. Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques. *Inventiones mathematicae*, 51(1):29–59, 1979. 7

[CF67] John William Scott Cassels and Albrecht Fröhlich. *Algebraic Number Theory: Proceedings of an Instructional Conference*. Academic press, 1967. 6

[DR80] Pierre Deligne and Kenneth A. Ribet. Values of abelian L-functions at negative integers over totally real fields. *Inventiones Mathematicae*, 59(3):227–286, October 1980. 7

[EJV11] Jordan S Ellenberg, Sonal Jain, and Akshay Venkatesh. Modeling λ-invariants by p-adic random matrices. *Communications on pure and applied mathematics*, 64(9):1243–1262, 2011. 9

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1990. 5

[Lan90] Serge Lang. *Cyclotomic Fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer New York, New York, NY, 1990. 10

[LV21] Alan Lauder and Jan Vonk. Computing p-adic L-functions of totally real fields. *Mathematics of Computation*, page 1, June 2021. 9

[Miy89] Toshitsune Miyake. *Modular Forms*. Springer Monographs in Mathematics. Springer-Verlag, Berlin Heidelberg, 1989. 3, 6

[Rob13] Xavier-François Roblot. Computing p-adic L-functions of totally real number fields. *Mathematics of Computation*, 84(292):831–874, 2013. 9

[Wei52] Andre Weil. Jacobi Sums as "Grossencharaktere". *Transactions of the American Mathematical Society*, 73(3):487–495, 1952. 4