Computing p-adic L-functions

of Hecke characters

Håvard Damm-Johnsen

October 11, 2021

University of Oxford
Junior number theory seminar

Outline

- L-functions: a 5-min elevator pitch

Outline

- L-functions: a 5-min elevator pitch
- p-adic L-functions: a quick intro

Outline

- L-functions: a 5-min elevator pitch
- p-adic L-functions: a quick intro
- Algorithm: computing p-adic L-functions on a machine

Outline

- L-functions: a 5-min elevator pitch
- p-adic L-functions: a quick intro
- Algorithm: computing p-adic L-functions on a machine
- Data: some explicit p-adic L-functions

Outline

- L-functions: a 5-min elevator pitch
- p-adic L-functions: a quick intro
- Algorithm: computing p-adic L-functions on a machine
- Data: some explicit p-adic L-functions
- Applications & extensions

L-functions

What is an L-function?

What is an L-function?

- Prototype: the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

What is an L-function?

- Prototype: the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.
  - Euler product: $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$

What is an L-function?

- Prototype: the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.
  - Euler product: $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$
  - Functional equation:

$$\xi(s) = \xi(1-s) \quad \text{where} \quad \xi(s) := \pi^{-s/2} \frac{s(s-1)}{2} \Gamma\left(\frac{s}{2}\right) \zeta(s)$$

What is an L-function?

- Prototype: the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.
  - Euler product: $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$
  - Functional equation:

$$\xi(s) = \xi(1-s) \quad \text{where} \quad \xi(s) := \pi^{-s/2} \frac{s(s-1)}{2} \Gamma\left(\frac{s}{2}\right) \zeta(s)$$

  - Meromorphic continuation, $\zeta \colon \mathbb{C} \to \mathbb{C}$

What is an L-function?

- Prototype: the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.
  - Euler product: $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$
  - Functional equation:

$$\xi(s) = \xi(1-s) \quad \text{where} \quad \xi(s) := \pi^{-s/2} \frac{s(s-1)}{2} \Gamma\left(\frac{s}{2}\right) \zeta(s)$$

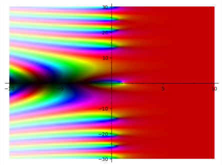
  - Meromorphic continuation, $\zeta : \mathbb{C} \to \mathbb{C}$
  - Fundamental in analytic number theory (eg. PNT)

What is an L-function?

- Prototype: the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.
  - Euler product: $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$
  - Functional equation:

$$\xi(s) = \xi(1-s) \quad \text{where} \quad \xi(s) := \pi^{-s/2} \frac{s(s-1)}{2} \Gamma\left(\frac{s}{2}\right) \zeta(s)$$

  - Meromorphic continuation, $\zeta \colon \mathbb{C} \to \mathbb{C}$
  - Fundamental in analytic number theory (eg. PNT)
- **Selberg class L-function**: Dirichlet series $\sum_n \frac{a_n}{n^s}$ satisfying the above + growth condition on a_n.



Dirichlet L-functions

- Let $\chi\colon \mathbb{Z} \to \mathbb{C}^{\times}$ be a Dirichlet character of modulus N (i.e. a periodic multiplicative function of period N).

Dirichlet L-functions

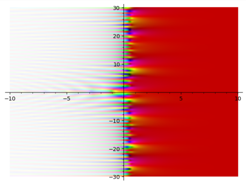
- Let $\chi\colon \mathbb{Z} \to \mathbb{C}^\times$ be a Dirichlet character of modulus N (i.e. a periodic multiplicative function of period N).
- The **Dirichlet L-function** $L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ is Selberg class.

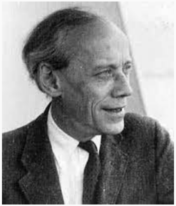
Dirichlet L-functions

- Let $\chi\colon \mathbb{Z} \to \mathbb{C}^\times$ be a Dirichlet character of modulus N (i.e. a periodic multiplicative function of period N).
- The **Dirichlet L-function** $L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ is Selberg class.
- $S := \{a + bn : n \in \mathbb{Z}\}$, $a, b \in \mathbb{N}$; write $\mathbb{1}_S$ as a linear combo of Dirichlet characters to prove that S contains infinitely many primes.

Dirichlet L-functions

- Let $\chi\colon \mathbb{Z} \to \mathbb{C}^\times$ be a Dirichlet character of modulus N (i.e. a periodic multiplicative function of period N).
- The **Dirichlet L-function** $L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ is Selberg class.
- $S := \{a + bn : n \in \mathbb{Z}\}$, $a, b \in \mathbb{N}$; write $\mathbb{1}_S$ as a linear combo of Dirichlet characters to prove that S contains infinitely many primes.
- By viewing χ as a 1-dim. rep. $\mathrm{Gal}(\mathbb{Q}(\zeta_N)) \to \mathbb{C}^\times = \mathrm{Gl}_1(\mathbb{C})$, this generalises to **Artin L-functions** attached to representations.





Zeta functions of number fields

- Fix F a number field with ring of integers $\mathcal{O}_F$.

Zeta functions of number fields

- Fix F a number field with ring of integers $\mathcal{O}_F$.
- e.g. $F = \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$, $\mathcal{O}_F = \mathbb{Z} + \sqrt{3}\mathbb{Z}$.

Zeta functions of number fields

- Fix F a number field with ring of integers $\mathcal{O}_F$.
- e.g. $F = \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$, $\mathcal{O}_F = \mathbb{Z} + \sqrt{3}\mathbb{Z}$.
- "Natural" generalisation of $\mathbb{Q}, \mathbb{Z}$.

Zeta functions of number fields

- Fix F a number field with ring of integers $\mathcal{O}_F$.
- e.g. $F = \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$, $\mathcal{O}_F = \mathbb{Z} + \sqrt{3}\mathbb{Z}$.
- "Natural" generalisation of $\mathbb{Q}, \mathbb{Z}$.
- Dedekind zeta function: $\zeta_F(s) := \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{1}{\mathrm{Nm}(\mathfrak{a})^s}$.

Zeta functions of number fields

- Fix F a number field with ring of integers $\mathcal{O}_F$.
- e.g. $F = \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$, $\mathcal{O}_F = \mathbb{Z} + \sqrt{3}\mathbb{Z}$.
- "Natural" generalisation of $\mathbb{Q}, \mathbb{Z}$.
- Dedekind zeta function: $\zeta_F(s) := \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{1}{\mathrm{Nm}(\mathfrak{a})^s}$.
- Has meromorphic cont., Euler product and functional eqn.

Zeta functions of number fields

- Fix F a number field with ring of integers $\mathcal{O}_F$.
- e.g. $F = \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$, $\mathcal{O}_F = \mathbb{Z} + \sqrt{3}\mathbb{Z}$.
- "Natural" generalisation of $\mathbb{Q}, \mathbb{Z}$.
- Dedekind zeta function: $\zeta_F(s) := \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{1}{\mathrm{Nm}(\mathfrak{a})^s}$.
- Has meromorphic cont., Euler product and functional eqn.
- Dirichlet class number formula:

Zeta functions of number fields

- Fix F a number field with ring of integers $\mathcal{O}_F$.
- e.g. $F = \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$, $\mathcal{O}_F = \mathbb{Z} + \sqrt{3}\mathbb{Z}$.
- "Natural" generalisation of $\mathbb{Q}, \mathbb{Z}$.
- **Dedekind zeta function**: $\zeta_F(s) := \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{1}{\mathrm{Nm}(\mathfrak{a})^s}$.
- Has meromorphic cont., Euler product and functional eqn.
- Dirichlet class number formula:

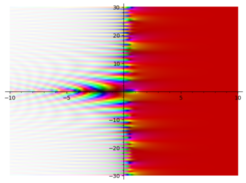
$$\mathrm{Res}_{s=1}\, \zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}\, \mathrm{Reg}_F\, h_F}{w_F\sqrt{|\Delta_F|}}$$

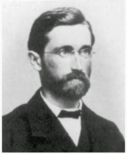
Zeta functions of number fields

- Fix F a number field with ring of integers $\mathcal{O}_F$.
- e.g. $F = \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$, $\mathcal{O}_F = \mathbb{Z} + \sqrt{3}\mathbb{Z}$.
- "Natural" generalisation of $\mathbb{Q}, \mathbb{Z}$.
- Dedekind zeta function: $\zeta_F(s) := \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{1}{\mathrm{Nm}(\mathfrak{a})^s}$.
- Has meromorphic cont., Euler product and functional eqn.
- Dirichlet class number formula:

$$\operatorname{Res}_{s=1} \zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}\,\mathrm{Reg}_F\, h_F}{w_F \sqrt{|\Delta_F|}}$$

- Dedekind's conjecture: given F'/F, the function $\zeta_{F'}(s)/\zeta_F(s)$ is entire





L-functions over number fields

- Generalise Dirichlet L-functions: need “Dirichlet characters of ideals”

L-functions over number fields

- Generalise Dirichlet L-functions: need "Dirichlet characters of ideals"
- Hecke characters: $\chi\colon \mathrm{Cl}_{\mathfrak{m}}(F) \to \mathbb{C}^\times$

L-functions over number fields

- Generalise Dirichlet L-functions: need "Dirichlet characters of ideals"
- Hecke characters: $\chi\colon \mathrm{Cl}_{\mathfrak{m}}(F) \to \mathbb{C}^\times$
- Hecke L-function: $L(\chi, s) := \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{\chi(\mathfrak{a})}{\mathrm{Nm}(\mathfrak{a})^s}$

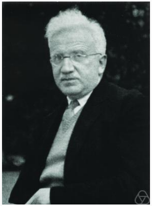
L-functions over number fields

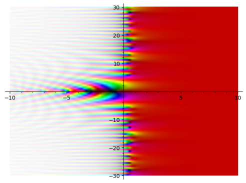
- Generalise Dirichlet L-functions: need "Dirichlet characters of ideals"
- Hecke characters: $\chi\colon \mathrm{Cl}_{\mathfrak{m}}(F) \to \mathbb{C}^\times$
- **Hecke L-function**: $L(\chi, s) := \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{\chi(\mathfrak{a})}{\mathrm{Nm}(\mathfrak{a})^s}$
- Has meromorphic cont., Euler product and functional eqn.

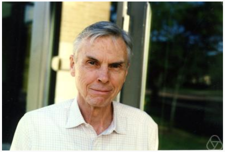
L-functions over number fields

- Generalise Dirichlet L-functions: need “Dirichlet characters of ideals”
- Hecke characters: $\chi\colon \mathrm{Cl}_{\mathfrak{m}}(F) \to \mathbb{C}^\times$
- Hecke L-function: $L(\chi, s) := \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{\chi(\mathfrak{a})}{\mathrm{Nm}(\mathfrak{a})^s}$
- Has meromorphic cont., Euler product and functional eqn.
- Natural interpretation using *adèles*, cf. Tate’s thesis

- Generalise Dirichlet L-functions: need "Dirichlet characters of ideals"
- Hecke characters: $\chi\colon\ \mathrm{Cl}_{\mathfrak{m}}(F) \to \mathbb{C}^\times$
- Hecke L-function: $L(\chi, s) := \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{\chi(\mathfrak{a})}{\mathrm{Nm}(\mathfrak{a})^s}$
- Has meromorphic cont., Euler product and functional eqn.
- Natural interpretation using *adèles*, cf. Tate's thesis







Other L-functions

Can attach L-functions to other objects, e.g. varieties or reps

Other L-functions

Can attach L-functions to other objects, e.g. varieties or reps

- $L(X, s)$ - meromorphic functions "built from local data"

Other L-functions

Can attach L-functions to other objects, e.g. varieties or reps

- $L(X,s)$ - meromorphic functions "built from local data"
- Special value formulae: analogues of Dirichlet class number formula

$$\mathrm{Res}_{s=1}\,\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}\,\mathrm{Reg}_F\,h_F}{w_F\sqrt{|\Delta_F|}}$$

Other L-functions

Can attach L-functions to other objects, e.g. varieties or reps

- $L(X, s)$ - meromorphic functions "built from local data"
- Special value formulae: analogues of Dirichlet class number formula

$$\operatorname{Res}_{s=1} \zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2} \operatorname{Reg}_F h_F}{w_F \sqrt{|\Delta_F|}}$$

  - X = number field: Stark conjectures

Other L-functions

Can attach L-functions to other objects, e.g. varieties or reps

- $L(X, s)$ - meromorphic functions “built from local data”
- Special value formulae: analogues of Dirichlet class number formula

$$\operatorname{Res}_{s=1} \zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2} \operatorname{Reg}_F h_F}{w_F \sqrt{|\Delta_F|}}$$

  - $X =$ number field: Stark conjectures
  - $X =$ elliptic curve: BSD conjecture, Gross-Zagier formula

Other L-functions

Can attach L-functions to other objects, e.g. varieties or reps

- $L(X, s)$ - meromorphic functions "built from local data"
- Special value formulae: analogues of Dirichlet class number formula

$$\mathrm{Res}_{s=1}\, \zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}\, \mathrm{Reg}_F\, h_F}{w_F \sqrt{|\Delta_F|}}$$

  - X = number field: Stark conjectures
  - X = elliptic curve: BSD conjecture, Gross-Zagier formula
  - X = algebraic variety: Conjectures of Bloch, Beilinson, Deligne, ...

Other L-functions

Can attach L-functions to other objects, e.g. varieties or reps

- $L(X, s)$ - meromorphic functions "built from local data"
- Special value formulae: analogues of Dirichlet class number formula

$$\mathrm{Res}_{s=1}\,\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}\,\mathrm{Reg}_F\,h_F}{w_F\sqrt{|\Delta_F|}}$$

  - X = number field: Stark conjectures
  - X = elliptic curve: BSD conjecture, Gross-Zagier formula
  - X = algebraic variety: Conjectures of Bloch, Beilinson, Deligne, ...
- *p-adic L-functions*: $L_p(X, s) : \mathbb{Z}_p \to \mathbb{C}_p$ - interpolates special values of $L(X, s)$

Other L-functions

Can attach L-functions to other objects, e.g. varieties or reps

- $L(X, s)$ - meromorphic functions "built from local data"
- Special value formulae: analogues of Dirichlet class number formula

$$\mathrm{Res}_{s=1}\,\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}\,\mathrm{Reg}_F\,h_F}{w_F\sqrt{|\Delta_F|}}$$

  - X = number field: Stark conjectures
  - X = elliptic curve: BSD conjecture, Gross-Zagier formula
  - X = algebraic variety: Conjectures of Bloch, Beilinson, Deligne, ...
- *p-adic L-functions*: $L_p(X, s) : \mathbb{Z}_p \to \mathbb{C}_p$ - interpolates special values of $L(X, s)$
  - Starting point of Iwasawa theory

Other L-functions

Can attach L-functions to other objects, e.g. varieties or reps

- $L(X,s)$ - meromorphic functions "built from local data"
- Special value formulae: analogues of Dirichlet class number formula

$$\mathrm{Res}_{s=1}\,\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}\,\mathrm{Reg}_F\,h_F}{w_F\sqrt{|\Delta_F|}}$$

    - X = number field: Stark conjectures
    - X = elliptic curve: BSD conjecture, Gross-Zagier formula
    - X = algebraic variety: Conjectures of Bloch, Beilinson, Deligne, ...
- *p-adic L-functions*: $L_p(X,s)\colon \mathbb{Z}_p \to \mathbb{C}_p$ - interpolates special values of $L(X,s)$
    - Starting point of Iwasawa theory
    - Iwasawa main conjectures

Other L-functions

Can attach L-functions to other objects, e.g. varieties or reps

- $L(X,s)$ - meromorphic functions "built from local data"
- Special value formulae: analogues of Dirichlet class number formula

$$\mathrm{Res}_{s=1}\,\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}\,\mathrm{Reg}_F\,h_F}{w_F\sqrt{|\Delta_F|}}$$

  - X = number field: Stark conjectures
  - X = elliptic curve: BSD conjecture, Gross-Zagier formula
  - X = algebraic variety: Conjectures of Bloch, Beilinson, Deligne, ...
- *p-adic L-functions*: $L_p(X,s): \mathbb{Z}_p \to \mathbb{C}_p$ - interpolates special values of $L(X,s)$
  - Starting point of Iwasawa theory
  - Iwasawa main conjectures
  - p-adic BSD conjecture

p-adic L-functions

p-adic L-functions over $\mathbb{Q}$

- **Euler + functional equation:** for k even, $\zeta(1-k) = -B_k/k$.

p-adic L-functions over $\mathbb{Q}$

- **Euler + functional equation:** for k even, $\zeta(1-k) = -B_k/k$.
- **Kummer:** if $k \equiv k' \mod (p-1)p^N$ are even, then

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \mod p^N.$$

p-adic L-functions over $\mathbb{Q}$

- **Euler + functional equation:** for k even, $\zeta(1-k) = -B_k/k$.
- **Kummer:** if $k \equiv k' \mod (p-1)p^N$ are even, then

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \mod p^N.$$

- By p-adic analysis, if $k_0 \equiv k_1 \equiv \dots \mod p-1$, then $(1-p^{k_i-1})\zeta(1-k_i)$ interpolate to $\zeta_p \colon \mathbb{Z}_p \to \mathbb{C}_p$.

p-adic L-functions over $\mathbb{Q}$

- **Euler + functional equation:** for k even, $\zeta(1-k) = -B_k/k$.
- **Kummer:** if $k \equiv k' \mod (p-1)p^N$ are even, then

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \mod p^N.$$

- By p-adic analysis, if $k_0 \equiv k_1 \equiv \dots \mod p-1$, then $(1-p^{k_i-1})\zeta(1-k_i)$ interpolate to $\zeta_p \colon \mathbb{Z}_p \to \mathbb{C}_p$.
- different "branches" corresponding to $\overline{k_0} \in \mathbb{Z}/(p-1)\mathbb{Z}$.

p-adic L-functions over $\mathbb{Q}$

- **Euler + functional equation:** for k even, $\zeta(1-k) = -B_k/k$.
- **Kummer:** if $k \equiv k' \mod (p-1)p^N$ are even, then

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \mod p^N.$$

- By p-adic analysis, if $k_0 \equiv k_1 \equiv \ldots \mod p-1$, then $(1-p^{k_i-1})\zeta(1-k_i)$ interpolate to $\zeta_p \colon \mathbb{Z}_p \to \mathbb{C}_p$.
- different "branches" corresponding to $\overline{k}_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$.
- We can approximate $\zeta_p(s)$ by computing $\zeta(1-k)$ for enough k and use polynomial interpolation:

p-adic L-functions over $\mathbb{Q}$

- **Euler + functional equation:** for k even, $\zeta(1-k) = -B_k/k$.
- **Kummer:** if $k \equiv k' \mod (p-1)p^N$ are even, then

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \mod p^N.$$

- By p-adic analysis, if $k_0 \equiv k_1 \equiv \dots \mod p-1$, then $(1-p^{k_i-1})\zeta(1-k_i)$ interpolate to $\zeta_p \colon \mathbb{Z}_p \to \mathbb{C}_p$.
- different "branches" corresponding to $\overline{k}_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$.
- We can approximate $\zeta_p(s)$ by computing $\zeta(1-k)$ for enough k and use polynomial interpolation:
- given pairs $\{(1-k_i, \zeta_p(1-k_i)) : i = 1, \dots, d\}$, find a polynomial P of degree d such that $P(1-k_i) = \zeta_p(1-k_i)$.

p-adic L-functions over $\mathbb{Q}$

- **Euler + functional equation:** for k even, $\zeta(1-k) = -B_k/k$.
- **Kummer:** if $k \equiv k' \mod (p-1)p^N$ are even, then

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \mod p^N.$$

- By p-adic analysis, if $k_0 \equiv k_1 \equiv \dots \mod p-1$, then $(1-p^{k_i-1})\zeta(1-k_i)$ interpolate to $\zeta_p \colon \mathbb{Z}_p \to \mathbb{C}_p$.
- different "branches" corresponding to $\overline{k}_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$.
- We can approximate $\zeta_p(s)$ by computing $\zeta(1-k)$ for enough k and use polynomial interpolation:
- given pairs $\{(1-k_i, \zeta_p(1-k_i)) : i = 1, \dots, d\}$, find a polynomial P of degree d such that $P(1-k_i) = \zeta_p(1-k_i)$.
- **Eg.** $p = 5, k_i \in \{2, 6, 10\}$, interpolate $\{(k_i, -(1-5^{k_i-1})B_{k_i}/k_i)\}$:

p-adic L-functions over $\mathbb{Q}$

- **Euler + functional equation:** for k even, $\zeta(1-k) = -B_k/k$.
- **Kummer:** if $k \equiv k' \mod (p-1)p^N$ are even, then

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \mod p^N.$$

- By p-adic analysis, if $k_0 \equiv k_1 \equiv \dots \mod p-1$, then $(1-p^{k_i-1})\zeta(1-k_i)$ interpolate to $\zeta_p : \mathbb{Z}_p \to \mathbb{C}_p$.
- different "branches" corresponding to $\overline{k}_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$.
- We can approximate $\zeta_p(s)$ by computing $\zeta(1-k)$ for enough k and use polynomial interpolation:
- given pairs $\{(1-k_i, \zeta_p(1-k_i)) : i = 1, \dots, d\}$, find a polynomial P of degree d such that $P(1-k_i) = \zeta_p(1-k_i)$.
- **Eg.** $p = 5, k_i \in \{2, 6, 10\}$, interpolate $\{(k_i, -(1-5^{k_i-1})B_{k_i}/k_i)\}$:

  $\left(5^2 \cdot 4828 + O(5^8)\right) s^2 + \left(5 \cdot 60514 + O(5^8)\right) s + 51662 + O(5^8)$

- **Euler + functional equation:** for k even, $\zeta(1-k) = -B_k/k$.
- **Kummer:** if $k \equiv k' \mod (p-1)p^N$ are even, then

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_{k'}}{k'} \mod p^N.$$

- By p-adic analysis, if $k_0 \equiv k_1 \equiv \dots \mod p-1$, then $(1-p^{k_i-1})\zeta(1-k_i)$ interpolate to $\zeta_p \colon \mathbb{Z}_p \to \mathbb{C}_p$.
- different "branches" corresponding to $\overline{k}_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$.
- We can approximate $\zeta_p(s)$ by computing $\zeta(1-k)$ for enough k and use polynomial interpolation:
- given pairs $\{(1-k_i, \zeta_p(1-k_i)) : i = 1, \dots, d\}$, find a polynomial P of degree d such that $P(1-k_i) = \zeta_p(1-k_i)$.
- **Eg.** $p = 5, k_i \in \{2, 6, 10\}$, interpolate $\{(k_i, -(1-5^{k_i-1})B_{k_i}/k_i)\}$:

$$\left(5^2 \cdot 4828 + O(5^8)\right) s^2 + \left(5 \cdot 60514 + O(5^8)\right) s + 51662 + O(5^8) \text{ `` } \approx \text{ '' } \zeta_5(s)$$

p-adic L-functions over F

p-adic L-functions over F

- Fix F a *totally real* number field of degree d, ψ a character of $\mathrm{Cl}_{\mathfrak{m}}^{+}$.

p-adic L-functions over F

- Fix F a *totally real* number field of degree d, ψ a character of $\mathrm{Cl}^+_{\mathfrak{m}}$.
- Define $L(\psi, s) := \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{\psi(\mathfrak{a})}{\mathrm{Nm}(\mathfrak{a})^s}$;

p-adic L-functions over F

- Fix F a *totally real* number field of degree d, ψ a character of $\mathrm{Cl}_{\mathfrak{m}}^{+}$.
- Define $L(\psi, s) := \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{\psi(\mathfrak{a})}{\mathrm{Nm}(\mathfrak{a})^s}$; then $L(\psi, 1-k) = -B_{k,\psi}/k \in \overline{\mathbb{Q}}$.

p-adic L-functions over F

- Fix F a *totally real* number field of degree d, ψ a character of $\mathrm{Cl}_{\mathfrak{m}}^{+}$.
- Define $L(\psi, s) \coloneqq \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{\psi(\mathfrak{a})}{\mathrm{Nm}(\mathfrak{a})^s}$; then $L(\psi, 1-k) = -B_{k,\psi}/k \in \overline{\mathbb{Q}}$.
- Interpolation: $L_p(\psi, 1-k) = (1 - \psi(p)p^{k-1})L(\psi, 1-k)$.

p-adic L-functions over F

- Fix F a *totally real* number field of degree d, ψ a character of $\mathrm{Cl}_{\mathfrak{m}}^{+}$.
- Define $L(\psi, s) \coloneqq \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{\psi(\mathfrak{a})}{\mathrm{Nm}(\mathfrak{a})^s}$; then $L(\psi, 1-k) = -B_{k,\psi}/k \in \overline{\mathbb{Q}}$.
- Interpolation: $L_p(\psi, 1-k) = (1 - \psi(p)p^{k-1})L(\psi, 1-k)$.
- However, not obvious how to compute $B_{k,\psi}$ algebraically *quickly*, so we need a new strategy!

p-adic L-functions over F

- Fix F a *totally real* number field of degree d, ψ a character of $\mathrm{Cl}_{\mathfrak{m}}^{+}$.
- Define $L(\psi, s) := \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{\psi(\mathfrak{a})}{\mathrm{Nm}(\mathfrak{a})^s}$; then $L(\psi, 1-k) = -B_{k,\psi}/k \in \overline{\mathbb{Q}}$.
- Interpolation: $L_p(\psi, 1-k) = (1 - \psi(p)p^{k-1})L(\psi, 1-k)$.
- However, not obvious how to compute $B_{k,\psi}$ algebraically *quickly*, so we need a new strategy!
- Serre (Antwerp III): The modular form

$$G_k^* = \frac{1}{2}\zeta_p(1-k) + \sum_{n=1}^{\infty} \left(\sum_{d|n,\, (d,p)=1} d^{k-1} \right) q^n$$

  on $\Gamma_0(p)$ lives in a p-adically continuous family of G_{k_i}.

p-adic L-functions over F

- Fix F a *totally real* number field of degree d, ψ a character of $\mathrm{Cl}_{\mathfrak{m}}^{+}$.
- Define $L(\psi, s) := \sum_{\mathfrak{a} \leqslant \mathcal{O}_F} \frac{\psi(\mathfrak{a})}{\mathrm{Nm}(\mathfrak{a})^s}$; then $L(\psi, 1-k) = -B_{k,\psi}/k \in \overline{\mathbb{Q}}$.
- Interpolation: $L_p(\psi, 1-k) = (1 - \psi(p)p^{k-1})L(\psi, 1-k)$.
- However, not obvious how to compute $B_{k,\psi}$ algebraically *quickly*, so we need a new strategy!
- Serre (Antwerp III): The modular form

$$G_k^* = \frac{1}{2}\zeta_p(1-k) + \sum_{n=1}^{\infty}\left(\sum_{d|n,\,(d,p)=1} d^{k-1}\right)q^n$$

  on $\Gamma_0(p)$ lives in a p-adically continuous family of G_{k_i}.
- Congruences between non-constant terms gives congruences between the constant terms, in fact, the Kummer congruences.

p-adic L-functions from modular forms

- **Idea:** look for modular forms with constant term $L(\psi, 1-k)$.

p-adic L-functions from modular forms

- **Idea:** look for modular forms with constant term $L(\psi, 1-k)$.
- There is a *Hilbert modular form* $G^{(p)}_{k,\psi} : \mathfrak{h}^d \to \mathbb{C}$ defined as

$$G^{(p)}_{k,\psi}(z_1, \ldots, z_d) = L_p(\psi, 1-k) + 2^d \sum_{\nu \in \mathfrak{d}_+^{-1}} \Bigg(\sum_{\substack{\mathfrak{a} | (\nu)\mathfrak{d} \\ (\mathfrak{a}, p) = 1}} \psi(\mathfrak{a}) \operatorname{Nm}(\mathfrak{a})^{k-1} \Bigg) e^{2\pi i (\sigma_1(\nu) z_1 + \ldots \sigma_d(\nu) z_d)}$$

p-adic L-functions from modular forms

- **Idea:** look for modular forms with constant term $L(\psi, 1-k)$.
- There is a *Hilbert modular form* $G^{(p)}_{k,\psi} : \mathfrak{h}^d \to \mathbb{C}$ defined as

$$G^{(p)}_{k,\psi}(z_1, \ldots, z_d) = L_p(\psi, 1-k) + 2^d \sum_{\nu \in \mathfrak{d}^{-1}_+} \Bigg(\sum_{\substack{\mathfrak{a} | (\nu)\mathfrak{d} \\ (\mathfrak{a}, p)=1}} \psi(\mathfrak{a}) \, \mathrm{Nm}(\mathfrak{a})^{k-1} \Bigg) e^{2\pi i (\sigma_1(\nu) z_1 + \ldots \sigma_d(\nu) z_d)}$$

- Setting $z_1 = \ldots = z_d = z$, we get the **diagonal restriction**

$$\Delta_{k,\psi}(z) = L_p(\psi, 1-k) + 2^d \sum_{n>0} \sum_{\substack{\nu \in \mathfrak{d}^{-1}_+ \\ \mathrm{tr}(\nu) = n}} \Bigg(\sum_{\substack{\mathfrak{a} | (\nu)\mathfrak{d} \\ (\mathfrak{a}, p)=1}} \psi(\mathfrak{a}) \, \mathrm{Nm}(\mathfrak{a})^{k-1} \Bigg) q^n$$

p-adic L-functions from modular forms

- **Idea:** look for modular forms with constant term $L(\psi, 1-k)$.
- There is a *Hilbert modular form* $G^{(p)}_{k,\psi} : \mathfrak{h}^d \to \mathbb{C}$ defined as

$$G^{(p)}_{k,\psi}(z_1, \ldots, z_d) = L_p(\psi, 1-k) + 2^d \sum_{\nu \in \mathfrak{d}_+^{-1}} \Big(\sum_{\substack{\mathfrak{a} \mid (\nu)\mathfrak{d} \\ (\mathfrak{a}, p) = 1}} \psi(\mathfrak{a}) \operatorname{Nm}(\mathfrak{a})^{k-1} \Big) e^{2\pi i (\sigma_1(\nu) z_1 + \ldots \sigma_d(\nu) z_d)}$$

- Setting $z_1 = \ldots = z_d = z$, we get the **diagonal restriction**

$$\Delta_{k,\psi}(z) = L_p(\psi, 1-k) + 2^d \sum_{n > 0} \sum_{\substack{\nu \in \mathfrak{d}_+^{-1} \\ \mathrm{tr}(\nu) = n}} \Big(\sum_{\substack{\mathfrak{a} \mid (\nu)\mathfrak{d} \\ (\mathfrak{a}, p) = 1}} \psi(\mathfrak{a}) \operatorname{Nm}(\mathfrak{a})^{k-1} \Big) q^n$$

- This is a classical modular form of weight dk.

p-adic L-functions from modular forms

- **Idea:** look for modular forms with constant term $L(\psi, 1-k)$.
- There is a *Hilbert modular form* $G^{(p)}_{k,\psi} : \mathfrak{h}^d \to \mathbb{C}$ defined as

$$G^{(p)}_{k,\psi}(z_1, \ldots, z_d) = L_p(\psi, 1-k) + 2^d \sum_{\nu \in \mathfrak{d}_+^{-1}} \Bigg(\sum_{\substack{\mathfrak{a} | (\nu)\mathfrak{d} \\ (\mathfrak{a}, p) = 1}} \psi(\mathfrak{a}) \operatorname{Nm}(\mathfrak{a})^{k-1} \Bigg) e^{2\pi i (\sigma_1(\nu) z_1 + \ldots \sigma_d(\nu) z_d)}$$

- Setting $z_1 = \ldots = z_d = z$, we get the **diagonal restriction**

$$\Delta_{k,\psi}(z) = L_p(\psi, 1-k) + 2^d \sum_{n > 0} \sum_{\substack{\nu \in \mathfrak{d}_+^{-1} \\ \operatorname{tr}(\nu) = n}} \Bigg(\sum_{\substack{\mathfrak{a} | (\nu)\mathfrak{d} \\ (\mathfrak{a}, p) = 1}} \psi(\mathfrak{a}) \operatorname{Nm}(\mathfrak{a})^{k-1} \Bigg) q^n$$

- This is a classical modular form of weight dk.
- **Key idea:** knowing a basis for M_{dk} and enough coefficients of $\Delta_{k,\psi}(z)$ lets us solve for $L_p(\psi, 1-k)$!

Algorithm

Algorithm [Lauder-Vonk21]

Algorithm [Lauder-Vonk21]

Input:

Algorithm [Lauder-Vonk21]

Input:

- F totally real number field,

Algorithm [Lauder-Vonk21]

Input:

- F totally real number field,
- p prime,

Algorithm [Lauder-Vonk21]

Input:

- F totally real number field,
- p prime,
- $k_0 \in \mathbb{Z}$ “starting weight”, $m \in \mathbb{N}$ “precision”,

Algorithm [Lauder-Vonk21]

Input:

- F totally real number field,
- p prime,
- $k_0 \in \mathbb{Z}$ "starting weight", $m \in \mathbb{N}$ "precision",
- $\psi\colon\ \mathrm{Cl}^+_{\mathfrak{m}}(F) \to \mathbb{C}^\times$, $(M) := \mathfrak{m} \cap \mathbb{Z}$

Algorithm [Lauder-Vonk21]

Input:

- F totally real number field,
- p prime,
- $k_0 \in \mathbb{Z}$ “starting weight”, $m \in \mathbb{N}$ “precision”,
- $\psi\colon \mathrm{Cl}^+_{\mathfrak{m}}(F) \to \mathbb{C}^\times$, $(M) \coloneqq \mathfrak{m} \cap \mathbb{Z}$

Output: $L_p(\psi, s)$ as an element of $\mathcal{O}_F[s]/(p^m)$.

Algorithm [Lauder-Vonk21]

Input:

- F totally real number field,
- p prime,
- $k_0 \in \mathbb{Z}$ "starting weight", $m \in \mathbb{N}$ "precision",
- $\psi\colon\ \mathrm{Cl}^+_{\mathfrak{m}}(F) \to \mathbb{C}^\times$, $(M) := \mathfrak{m} \cap \mathbb{Z}$

Output: $L_p(\psi, s)$ as an element of $\mathcal{O}_F[s]/(p^m)$.

(I) Set interpolation weights $k_j = k_0 + j(p-1)$,

Algorithm [Lauder-Vonk21]

Input:

- F totally real number field,
- p prime,
- $k_0 \in \mathbb{Z}$ "starting weight", $m \in \mathbb{N}$ "precision",
- $\psi\colon\ \mathrm{Cl}^+_{\mathfrak{m}}(F) \to \mathbb{C}^\times$, $(M) \coloneqq \mathfrak{m} \cap \mathbb{Z}$

Output: $L_p(\psi, s)$ as an element of $\mathcal{O}_F[s]/(p^m)$.

(I) Set interpolation weights $k_j = k_0 + j(p-1)$, compute bases for $M_{dk_j}(\Gamma_0(M), \psi)$ for $j = 1, \ldots, \delta_m \approx m$.

Algorithm [Lauder-Vonk21]

Input:

- F totally real number field,
- p prime,
- $k_0 \in \mathbb{Z}$ "starting weight", $m \in \mathbb{N}$ "precision",
- $\psi\colon\ \mathrm{Cl}^+_{\mathfrak{m}}(F) \to \mathbb{C}^\times$, $(M) := \mathfrak{m} \cap \mathbb{Z}$

Output: $L_p(\psi, s)$ as an element of $\mathcal{O}_F[s]/(p^m)$.

(I) Set interpolation weights $k_j = k_0 + j(p-1)$, compute bases for $M_{dk_j}(\Gamma_0(M), \psi)$ for $j = 1, \ldots, \delta_m \approx m$.

(II) Compute non-constant coefficients of $\Delta_{k_j,\psi}$:

$$a_n = \sum_{\substack{\nu \in \mathfrak{d}_+^{-1} \\ \mathrm{tr}(\nu)=n}} \sum_{\substack{\mathfrak{a} | (\nu)\mathfrak{d} \\ (\mathfrak{a},p)=1}} \psi(\mathfrak{a})\,\mathrm{Nm}(\mathfrak{a})^{k_j-1}, \qquad n > 0.$$

Algorithm [Lauder-Vonk21]

Input:

- F totally real number field,
- p prime,
- $k_0 \in \mathbb{Z}$ "starting weight", $m \in \mathbb{N}$ "precision",
- $\psi\colon \mathrm{Cl}^+_{\mathfrak{m}}(F) \to \mathbb{C}^\times$, $(M) := \mathfrak{m} \cap \mathbb{Z}$

Output: $L_p(\psi, s)$ as an element of $\mathcal{O}_F[s]/(p^m)$.

(I) Set interpolation weights $k_j = k_0 + j(p-1)$, compute bases for $M_{dk_j}(\Gamma_0(M), \psi)$ for $j = 1, \ldots, \delta_m \approx m$.

(II) Compute non-constant coefficients of $\Delta_{k_j,\psi}$:

$$a_n = \sum_{\substack{\nu \in \mathfrak{d}_+^{-1} \\ \mathrm{tr}(\nu) = n}} \sum_{\substack{\mathfrak{a} | (\nu)\mathfrak{d} \\ (\mathfrak{a}, p) = 1}} \psi(\mathfrak{a}) \operatorname{Nm}(\mathfrak{a})^{k_j - 1}, \qquad n > 0.$$

(III) Write $\Delta_{k_j,\psi}$ as linear combination of modular forms in M_{dk_j} and solve for constant term, $L_p(\psi, 1-k_j)$.

Algorithm [Lauder-Vonk21]

Input:

- F totally real number field,
- p prime,
- $k_0 \in \mathbb{Z}$ “starting weight”, $m \in \mathbb{N}$ “precision”,
- $\psi\colon \mathrm{Cl}^+_{\mathfrak{m}}(F) \to \mathbb{C}^\times$, $(M) := \mathfrak{m} \cap \mathbb{Z}$

Output: $L_p(\psi, s)$ as an element of $\mathcal{O}_F[s]/(p^m)$.

(I) Set interpolation weights $k_j = k_0 + j(p-1)$, compute bases for $M_{dk_j}(\Gamma_0(M), \psi)$ for $j = 1, \ldots, \delta_m \approx m$.

(II) Compute non-constant coefficients of $\Delta_{k_j,\psi}$:

$$a_n = \sum_{\substack{\nu \in \mathfrak{d}_+^{-1} \\ \mathrm{tr}(\nu) = n}} \sum_{\substack{\mathfrak{a} | (\nu)\mathfrak{d} \\ (\mathfrak{a}, p) = 1}} \psi(\mathfrak{a}) \,\mathrm{Nm}(\mathfrak{a})^{k_j - 1}, \qquad n > 0.$$

(III) Write $\Delta_{k_j,\psi}$ as linear combination of modular forms in M_{dk_j} and solve for constant term, $L_p(\psi, 1 - k_j)$.

(IV) Interpolate the $\delta_m + 1$ values of $L_p(\psi, 1 - k_j)$ to find $L_p(\psi, s)$.

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

p	$L_p(\chi, s) \in \mathcal{O}_F[s] \pmod{p^m}$, $\chi : \mathrm{Cl}^+_{(4)} \to \mathbb{C}^\times$ unique totally odd char.
3	$\left(3^8 \cdot 1 + O(3^9)\right) s^{12} + \left(3^7 \cdot 19 + O(3^{10})\right) s^{11} + \left(3^7 \cdot 1 + O(3^9)\right) s^{10} + \left(3^5 \cdot 185 + O(3^{10})\right) s^9 + \left(3^7 \cdot 8 + O(3^{10})\right) s^8 + \left(3^5 \cdot 598 + O(3^{11})\right) s^7 + \left(3^6 \cdot 22 + O(3^9)\right) s^6 + \left(3^4 \cdot 182 + O(3^{10})\right) s^5 + \left(3^4 \cdot 194 + O(3^9)\right) s^4 + \left(3^2 \cdot 6025 + O(3^{10})\right) s^3 + \left(3^3 \cdot 5689 + O(3^{11})\right) s^2 + \left(3 \cdot 22742 + O(3^{12})\right) s + 3^{13} \cdot 2 + O(3^{14})$
5	$\left(5^8 \cdot 1 + O(5^9)\right) s^8 + \left(5^6 \cdot 13 + O(5^9)\right) s^7 + \left(5^5 \cdot 401 + O(5^9)\right) s^6 + \left(5^4 \cdot 3069 + O(5^9)\right) s^5 + \left(5^5 \cdot 329 + O(5^9)\right) s^4 + \left(5^3 \cdot 14164 + O(5^9)\right) s^3 + \left(5^2 \cdot 2202 + O(5^9)\right) s^2 + \left(5 \cdot 157656 + O(5^9)\right) s + O(5^{10})$
7	$\left(7^6 \cdot 1 + O(7^7)\right) s^7 + \left(7^6 \cdot 12 + O(7^8)\right) s^6 + \left(7^5 \cdot 220 + O(7^8)\right) s^5 + \left(7^4 \cdot 846 + O(7^8)\right) s^4 + \left(7^3 \cdot 13352 + O(7^8)\right) s^3 + \left(7^2 \cdot 4657 + O(7^8)\right) s^2 + \left(7 \cdot 40340 + O(7^7)\right) s + 3955624 + O(7^8)$
11	$O(11^7) s^6 + \left(11^5 \cdot 42 + O(11^7)\right) s^5 + \left(11^4 \cdot 959 + O(11^7)\right) s^4 + \left(11^3 \cdot 6328 + O(11^7)\right) s^3 + \left(11^2 \cdot 102789 + O(11^7)\right) s^2 + \left(11 \cdot 964668 + O(11^7)\right) s + 11390493 + O(11^7)$
13	$\left(13^6 \cdot 7 + O(13^7)\right) s^6 + \left(13^5 \cdot 62 + O(13^7)\right) s^5 + \left(13^4 \cdot 154 + O(13^7)\right) s^4 + \left(13^3 \cdot 3395 + O(13352^7)\right) s^3 + \left(13^2 \cdot 172247 + O(13^7)\right) s^2 + \left(13^2 \cdot 31667 + O(13^7)\right) s + 26080095 + O(13^7)$
17	$\left(17^6 \cdot 7 + O(17^7)\right) s^6 + \left(17^5 \cdot 159 + O(17^7)\right) s^5 + \left(17^4 \cdot 90 + O(17^7)\right) s^4 + \left(17^3 \cdot 34940 + O(17^7)\right) s^3 + \left(17^2 \cdot 461695 + O(17^7)\right) s^2 + \left(17 \cdot 21148809 + O(17^7)\right) s + 309732348 + O(17^7)$
19	$\left(19^6 \cdot 6 + O(19^7)\right) s^6 + \left(19^5 \cdot 345 + O(19^7)\right) s^5 + \left(19^4 \cdot 1579 + O(19^7)\right) s^4 + \left(19^3 \cdot 98406 + O(19^7)\right) s^3 + \left(19^2 \cdot 645519 + O(19^7)\right) s^2 + \left(19 \cdot 40194503 + O(19^7)\right) s + 354713675 + O(19^7)$

Implementation

Implementation

- Algorithm is polynomial in $p, m, \operatorname{Disc} F$, exponential in $[F : \mathbb{Q}]$.

Implementation

- Algorithm is polynomial in $p, m, \operatorname{Disc} F$, exponential in $[F : \mathbb{Q}]$.
- `sage` has experimental support for Hecke characters via `gp/pari`, but not part of main branch yet

Implementation

- Algorithm is polynomial in $p, m, \operatorname{Disc} F$, exponential in $[F : \mathbb{Q}]$.
- `sage` has experimental support for Hecke characters via `gp/pari`, but not part of main branch yet
- Computational challenges:

Implementation

- Algorithm is polynomial in $p, m, \operatorname{Disc} F$, exponential in $[F : \mathbb{Q}]$.
- `sage` has experimental support for Hecke characters via `gp/pari`, but not part of main branch yet
- Computational challenges:
  - Computing diagonal restriction coefficients

Implementation

- Algorithm is polynomial in $p, m, \operatorname{Disc} F$, exponential in $[F : \mathbb{Q}]$.
- `sage` has experimental support for Hecke characters via `gp/pari`, but not part of main branch yet
- Computational challenges:
  - Computing diagonal restriction coefficients

  -> For ring class characters, reduction theory of quadratic forms

Implementation

- Algorithm is polynomial in $p, m, \operatorname{Disc} F$, exponential in $[F : \mathbb{Q}]$.
- `sage` has experimental support for Hecke characters via `gp/pari`, but not part of main branch yet
- Computational challenges:
    - Computing diagonal restriction coefficients
    - -> For ring class characters, reduction theory of quadratic forms
    - -> Parallelisation, caching makes this somewhat faster

Implementation

- Algorithm is polynomial in $p, m, \operatorname{Disc} F$, exponential in $[F : \mathbb{Q}]$.
- `sage` has experimental support for Hecke characters via `gp/pari`, but not part of main branch yet
- Computational challenges:
  - Computing diagonal restriction coefficients
  - -> For ring class characters, reduction theory of quadratic forms
  - -> Parallelisation, caching makes this somewhat faster
  - -> Fastest method over $\mathbb{Q}$ uses half integer weight MFs; can we generalise this?

Implementation

- Algorithm is polynomial in $p, m, \operatorname{Disc} F$, exponential in $[F : \mathbb{Q}]$.
- `sage` has experimental support for Hecke characters via `gp/pari`, but not part of main branch yet
- Computational challenges:
  - Computing diagonal restriction coefficients
  - -> For ring class characters, reduction theory of quadratic forms
  - -> Parallelisation, caching makes this somewhat faster
  - -> Fastest method over $\mathbb{Q}$ uses half integer weight MFs; can we generalise this?
  - Finding q-expansion bases of modular forms of high weight

Implementation

- Algorithm is polynomial in $p, m, \operatorname{Disc} F$, exponential in $[F : \mathbb{Q}]$.
- `sage` has experimental support for Hecke characters via `gp/pari`, but not part of main branch yet
- Computational challenges:
  - Computing diagonal restriction coefficients
  - -> For ring class characters, reduction theory of quadratic forms
  - -> Parallelisation, caching makes this somewhat faster
  - -> Fastest method over $\mathbb{Q}$ uses half integer weight MFs; can we generalise this?
  - Finding q-expansion bases of modular forms of high weight
  - -> Randomised algorithm due to Lauder, now implemented in `sage`

Implementation

- Algorithm is polynomial in $p, m, \mathrm{Disc}\, F$, exponential in $[F : \mathbb{Q}]$.
- `sage` has experimental support for Hecke characters via `gp/pari`, but not part of main branch yet
- Computational challenges:
  - Computing diagonal restriction coefficients
  - -> For ring class characters, reduction theory of quadratic forms
  - -> Parallelisation, caching makes this somewhat faster
  - -> Fastest method over $\mathbb{Q}$ uses half integer weight MFs; can we generalise this?
  - Finding q-expansion bases of modular forms of high weight
  - -> Randomised algorithm due to Lauder, now implemented in `sage`
  - -> For nontrivial nebentype, this still needs some work (but ok in many cases)

Implementation

- Algorithm is polynomial in $p, m, \operatorname{Disc} F$, exponential in $[F : \mathbb{Q}]$.
- `sage` has experimental support for Hecke characters via `gp/pari`, but not part of main branch yet
- Computational challenges:
  - Computing diagonal restriction coefficients
  - -> For ring class characters, reduction theory of quadratic forms
  - -> Parallelisation, caching makes this somewhat faster
  - -> Fastest method over $\mathbb{Q}$ uses half integer weight MFs; can we generalise this?
  - Finding q-expansion bases of modular forms of high weight
  - -> Randomised algorithm due to Lauder, now implemented in `sage`
  - -> For nontrivial nebentype, this still needs some work (but ok in many cases)
- Roblot '15: Alternative algorithm based on Cassou-Noguès' construction of p-adic L-functions - less efficient in practice.

Applications

- Statistics of λ-invariants à la Ellenberg-Jain-Venkatesh.

Applications

- Statistics of λ-invariants à la Ellenberg-Jain-Venkatesh.
  - $K/\mathbb{Q}_p$ a finite extension with uniformiser ϖ; fix $f \in \mathcal{O}_K[\![T]\!]$.

Applications

- Statistics of λ-invariants à la Ellenberg-Jain-Venkatesh.
  - $K/\mathbb{Q}_p$ a finite extension with uniformiser ϖ; fix $f \in \mathcal{O}_K[[T]]$.
  - **Weierstraß preparation thm**: $f(T) = \varpi^\mu P(T)u(T)$ where $P \in \mathcal{O}_K[T]$, $u \in \mathcal{O}_K[[T]]^\times$.

Applications

- Statistics of λ-invariants à la Ellenberg-Jain-Venkatesh.
  - $K/\mathbb{Q}_p$ a finite extension with uniformiser ϖ; fix $f \in \mathcal{O}_K[\![T]\!]$.
  - **Weierstraß preparation thm**: $f(T) = \varpi^\mu P(T)u(T)$ where $P \in \mathcal{O}_K[T]$, $u \in \mathcal{O}_K[\![T]\!]^\times$.
  - In particular, f has finitely many zeros.

Applications

- Statistics of λ-invariants à la Ellenberg-Jain-Venkatesh.
  - $K/\mathbb{Q}_p$ a finite extension with uniformiser ϖ; fix $f \in \mathcal{O}_K[\![T]\!]$.
  - **Weierstraß preparation thm**: $f(T) = \varpi^\mu P(T)u(T)$ where $P \in \mathcal{O}_K[T]$, $u \in \mathcal{O}_K[\![T]\!]^\times$.
  - In particular, f has finitely many zeros.
  - **Iwasawa invariants:** μ and $\lambda \coloneqq \deg P(T) \in \mathbb{N} \sqcup \{0\}$.

Applications

- Statistics of λ-invariants à la Ellenberg-Jain-Venkatesh.
  - $K/\mathbb{Q}_p$ a finite extension with uniformiser ϖ; fix $f \in \mathcal{O}_K[\![T]\!]$.
  - **Weierstraß preparation thm**: $f(T) = \varpi^{\mu} P(T) u(T)$ where $P \in \mathcal{O}_K[T]$, $u \in \mathcal{O}_K[\![T]\!]^{\times}$.
  - In particular, f has finitely many zeros.
  - **Iwasawa invariants:** μ and $\lambda := \deg P(T) \in \mathbb{N} \sqcup \{0\}$.
  - Conjecture ([EJV11], inspired by p-adic random matrix heuristic):

$$\mathbb{P}(\mathrm{ord}_p \, \lambda(L_p(\chi, T)) = r) = p^{-r} \prod_{t>r} 1 - p^{-r},$$

as χ ranges over quadratic characters $\left(\frac{\bullet}{-D}\right)$ for which $\left(\frac{p}{-D}\right) = -1$.

Applications

- Statistics of λ-invariants à la Ellenberg-Jain-Venkatesh.
  - $K/\mathbb{Q}_p$ a finite extension with uniformiser ϖ; fix $f \in \mathcal{O}_K[\![T]\!]$.
  - **Weierstraß preparation thm**: $f(T) = \varpi^\mu P(T)u(T)$ where $P \in \mathcal{O}_K[T]$, $u \in \mathcal{O}_K[\![T]\!]^\times$.
  - In particular, f has finitely many zeros.
  - **Iwasawa invariants:** μ and $\lambda := \deg P(T) \in \mathbb{N} \sqcup \{0\}$.
  - Conjecture ([EJV11], inspired by p-adic random matrix heuristic):

$$\mathbb{P}(\operatorname{ord}_p \lambda(L_p(\chi, T)) = r) = p^{-r} \prod_{t>r} 1 - p^{-r},$$

  as χ ranges over quadratic characters $\left(\frac{\bullet}{-D}\right)$ for which $\left(\frac{p}{-D}\right) = -1$.
- Over $\mathbb{Q}(\sqrt{D})$ we can compute λ-invariants of $L(\chi, T)$ for $\chi\colon \mathrm{Cl}^+_{(N)} \to \mathbb{C}^\times$ quickly using reduction theory of indefinite binary QFs.

Applications

- Statistics of λ-invariants à la Ellenberg-Jain-Venkatesh.
  - $K/\mathbb{Q}_p$ a finite extension with uniformiser ϖ; fix $f \in \mathcal{O}_K[\![T]\!]$.
  - **Weierstraß preparation thm**: $f(T) = \varpi^\mu P(T)u(T)$ where $P \in \mathcal{O}_K[T]$, $u \in \mathcal{O}_K[\![T]\!]^\times$.
  - In particular, f has finitely many zeros.
  - **Iwasawa invariants:** μ and $\lambda := \deg P(T) \in \mathbb{N} \sqcup \{0\}$.
  - Conjecture ([EJV11], inspired by p-adic random matrix heuristic):

$$\mathbb{P}(\mathrm{ord}_p\, \lambda(L_p(\chi, T)) = r) = p^{-r} \prod_{t>r} 1 - p^{-r},$$

    as χ ranges over quadratic characters $\left(\frac{\bullet}{-D}\right)$ for which $\left(\frac{p}{-D}\right) = -1$.
- Over $\mathbb{Q}(\sqrt{D})$ we can compute λ-invariants of $L(\chi, T)$ for $\chi\colon\ \mathrm{Cl}^+_{(N)} \to \mathbb{C}^\times$ quickly using reduction theory of indefinite binary QFs.
- Some finicky details to work out still.

Thank you!

Questions?