PARI/GP, playing the L-functions game of number theorists

Aurel Page

RTCA, ENS Lyon
Inria / Université de Bordeaux

27/06/2023

The Riemann zeta function

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \text{ for } \Re(s) > 1.$$

Important properties:

- Euler product: $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$;
- Meromorphic continuation to $\mathbb{C}$, simple pole at $s = 1$;
- Functional equation: $\Lambda(s) = \Gamma_{\mathbb{R}}(s)\zeta(s)$ satisfies $\Lambda(s) = \Lambda(1 - s)$;

where $\Gamma_{\mathbb{R}}(s) = \pi^{s/2}\Gamma(s/2)$.

L-functions

An **L-function** $L(s)$ of degree d and conductor N (integers ≥ 1) is a series

$$L(s) = \sum_{n \geq 1} \frac{a_n}{n^s} \text{ converging for } \Re(s) \text{ large enough}$$

satisfying the properties:

- Euler product: $L(s) = \prod_p F_p(p^{-s})^{-1}$ where $F_p(x) \in \mathbb{C}[x]$ satisfies $F_p(0) = 1$, and for $p \nmid N$ all roots of F_p have absolute value 1 and $\deg F_p = d$;
- Meromorphic continuation to $\mathbb{C}$, finite number of poles;
- Functional equation: $\Lambda(s) = N^{s/2} \prod_{i=1}^{d} \Gamma_{\mathbb{R}}(s + \alpha_i) L(s)$ satisfies $\Lambda(s) = \epsilon \overline{\Lambda(1 - \bar{s})}$.

Note: sometimes we make a shift, so the functional equation relates s to some $k - s$.

Example: elliptic curve

Consider the curve

$$E\colon y^2 + y = x^3 + x^2 - 2x.$$

For each prime p, let $a_p = p - n_p$ where n_p is the number of solutions mod p and define

$$F_p(x) = 1 - a_p x + p x^2.$$

Then $\prod_p F_p(p^{-s})^{-1}$ can be modified at finitely many primes into an L-function $L(E, s)$ such that

- $d = 2$,
- $N = 389$,
- $(\alpha_1, \alpha_2) = (0, 1)$.

The number theorists game

1. For various arithmetic objects X, construct an L-function $L(X,s)$.
2. Find equalities $L(X_1,s) = L(X_2,s)$ for seemingly unrelated X_1 and X_2.

It even has a name: the ”Langlands programme”!

The number theorists game

More precisely, you are supposed to match ”motivic” L-functions and ”automorphic” L-functions.

Motivic:

- Consider polynomial equations;
- Build $F_p(x)$ from mod p point counts.

Automorphic:

- Consider (finite-dimensional) spaces of automorphic forms: functions satisfying some functional equations + some differential equations;
- Build $F_p(x)$ from the eigenvalues of some operators (Hecke operators).

Example: modular forms

To match our motivic L-function $L(E, s)$, we need an automorphic object: a modular form f.

- $f\colon \mathbb{C} \setminus \mathbb{R} \to \mathbb{C}$;
- Functional equations: $f(\frac{az+b}{cz+d}) = (cz+d)^2 f(z)$ for every $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in some subgroup $\Gamma \subset \mathrm{GL}_2(\mathbb{Z})$;
- Differential equations: f is holomorphic.
- Eigenvalue of Hecke operators: $T_p f = a_p f$ gives $F_p(x) = 1 - a_p x + p x^2$.

Dedekind zeta function

Consider $P(x) \in \mathbb{Z}[x]$ irreducible of degree d.
For each prime p, let

$$F_p(x) = \prod_{j=1}^{s} (1 - x^{d_j})$$

where $(d_1, \ldots, d_s)$ are the degrees of the irreducible factors of $P \bmod p$.
After modifying finitely many F_p, this gives an L-function $\zeta_K(s)$ (where $K = \mathbb{Q}(\alpha)$ with $P(\alpha) = 0$) with

- degree d,
- $N =$ the absolute value of the discriminant of K,
- $\alpha_1 = \cdots = \alpha_d = 0$.

Dirichlet characters

We will describe automorphic objects matching Dedekind zeta functions in some simple cases.

Let $N \geq 1$ be an integer and $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ a character. Set

$$F_p(x) = 1 - \chi(p)x \text{ for all but finitely many } p.$$

These are the Euler factors of an L-function $L(\chi, s)$.

For suitable K, we have $\zeta_K(s) = \prod_k L(\chi_k, s)$ for some χ_k.

Ray class groups

We can also play the game in reverse!

Let $K = \mathbb{Q}(\alpha)$ be a number field with ring of algebraic integers $\mathbb{Z}_K$. We want an analogue of $(\mathbb{Z}/N\mathbb{Z})^\times$ for K. Define the **ray class group**

$$\mathrm{Cl}_K(N) = \frac{\{\text{ideals of } \mathbb{Z}_K \text{ coprime to } N\}}{\{\text{ideals generated by some } \beta \equiv 1 \bmod N\}}.$$

For every character $\chi\colon \mathrm{Cl}_K(N) \to \mathbb{C}^\times$, we get an L-function $L(\chi, s)$.

There exists a number field H (a **class field**) such that $\zeta_H(s) = \prod_\chi L(\chi, s)$.

Hecke characters

Let $K = \mathbb{Q}(\alpha)$ be a number field with ring of algebraic integers $\mathbb{Z}_K$, where $P(\alpha) = 0$. Let r_1 be the number of real roots of P and r_2 the number of pairs of conjugate complex roots. Let's upgrade the previous construction and define the **idèle class group**

$$\mathcal{C}_K(N) = \frac{(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \times \{\text{ideals of } \mathbb{Z}_K \text{ coprime to } N\}}{\{\text{elements } \beta \equiv 1 \bmod N\}}.$$

For every continuous character $\chi\colon \mathcal{C}_K(N) \to \mathbb{C}^\times$, we get an L-function $L(\chi, s)$.

Example: a genus 2 curve

We consider $P(x) = x^4 - x^3 + 2x^2 + 4x + 3$ and a specific infinite order Hecke character χ.

Corresponding motivic object? The curve

$$C\colon y^2 + x^3y = -2x^4 - 2x^3 + 2x^2 + 3x - 2$$

has an attached L-function $L(C, s)$, and we have

$$L(\chi, s) = L(C, s).$$

Transcendental Hecke characters

Sometimes we fail at the game!

Some Hecke characters (transcendental) cannot correspond to a motivic object.

In PARI/GP, the Hecke characters package broke the L-functions package!

- large α_i
- nonreal α_i
- approximate α_i.

Hypergeometric motives

We can also fail in the other direction.

Consider equations

$$H\colon \prod_{i=1}^{n} x_i^{\gamma_i} = t,\ \sum_{i=1}^{n} x_i = 0,\ x_i \neq 0.$$

for some integers γ_i and $t \in \mathbb{Q}$. We can efficiently compute most coefficients of $L(H, s)$, but not the corresponding automorphic object.

Often one object is harder than the other one.

In progress: weight 1 modular forms

Often one object is easier than the other one, and we can take advantage of this!

All modular forms of weight 1 and level $N \leq X$:

- $X = 1500$ (Buzzard–Lauder)
- $X = 4000$ (PARI/GP, Belabas–Cohen)
- $X = 10^4$ (Child, 1TB of memory)
  Time complexity $O(X^4)$, memory $O(X^2)$.
- $X = 10^6$ (new algorithm in PARI/GP, Allombert–P.).
  Time complexity $O(X^\alpha)$ for $2.5 \leq \alpha \leq 4$, low memory.

In progress: Hilbert modular forms

Currently being integrated into PARI/GP: fundamental domains for Fuchsian groups by James Rickards.

Area	Magma (s)	PARI/GP (s)	speedup
20.943	13	0.022	600
571.770	4200	3.1	1300
4490.383	2700000	1200	2200

This will allow us to compute Hilbert modular forms.

Projects

We plan to compute more automorphic objects:

- higher dimensional arithmetic manifolds,
- numerical methods,
- lattice-based methods
- ...

Questions ?

Thank you !