ζ and L functions

Caveat: beginner ← → expert; Me.

Motivation: arithmetic problem (e.g. $\#\{x \in \mathbb{F}_p \mid x^5 + 20x + 16 = 0\}$ $\forall p$) $\rightsquigarrow$ L-function. "character"

We seek an "a priori" for different char. of the L-functions which appear.

Riemann ζ-function:

$$\zeta(s) = \sum_{s \geq 1} n^{-s}$$

by comparison with $\int_1^\infty x^{-s}\,dx \Rightarrow$ converges for real $s > 1$.

$$= \left[\frac{x^{-s+1}}{-s+1} \right]_1^\infty = \frac{1}{s-1}$$

$\Rightarrow$ when viewed as a holomorphic function, absolutely convergent for $\operatorname{Re} s > 1$.

Euler:
- special values, e.g. $\zeta(2) = \pi^2/6$.
- Euler product: $\zeta(s) = \sum (p_1^{n_1} \cdots p_k^{n_k})^{-s} = (1 + 2^{-s} + 2^{-2s} + \dots)(1 + 3^{-s} + 3^{-2s} + \dots)\dots$

$$= \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

Key point seems to be: via Euler product $\sum_{n \geq 1} \frac{1}{n}$ diverges $\Rightarrow \infty$ many primes.
We can use analysis to study the primes: $\Uparrow$ π irrational !!

Riemann:
- ζ admits a meromorphic extension to the whole complex plane.
- ζ has a simple pole at 1, "trivial" zeroes at $-2, -4, \dots$
- $\Lambda(s) := \pi^{-s/2}\,\Gamma\left(\frac{s}{2}\right)\zeta(s)$ satisfies functional equation

$$\Lambda(s) = \Lambda(1-s).$$

critical line

- Riemann hypothesis: all non-trivial zeroes have $\operatorname{Re} z = 1/2$.

(Known that the first 10^{12} zeroes lie on critical line!)

Why do we care?

Roughly: zeroes of ζ are "Fourier modes of primes".

Riemann's motivation:

$$\#\{p \text{ prime} \mid p \leq x\}$$

Prime number theorem: $\pi(x) \sim \dfrac{x}{\log x}$.
(conjecture at Riemann's time)

Why true, and what is the error term?

Instead consider $\Lambda_{VM}(n) = \begin{cases} \log p & \text{if } n = p^k \\ 0 & \text{otherwise.} \end{cases}$ "make $\log p$ noise at prime powers".

$$\psi(x) = \sum_{n \leq x} \Lambda_{VM}(n).$$

Exercise: Show that PNT $\iff$ $\psi(x) \sim x$.

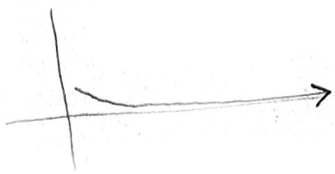
Riemann's explicit formula: if $x \notin \mathbb{Z}$ then

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \log(2\pi)$$

where the sum is over the zeroes of the ζ-function.

i.e. $$x - \psi(x) = \log(2\pi) + \sum_{\rho} \frac{x^{\rho}}{\rho}.$$

Trivial zeroes: $-\dfrac{1}{2n\, x^{2n}}$

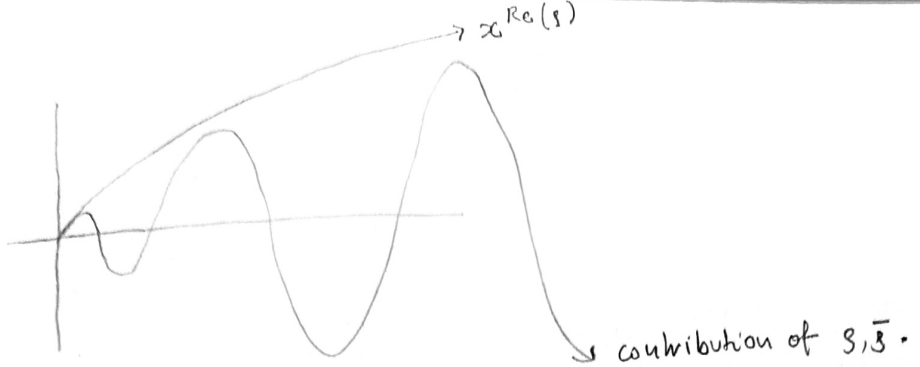


decaying very fast.

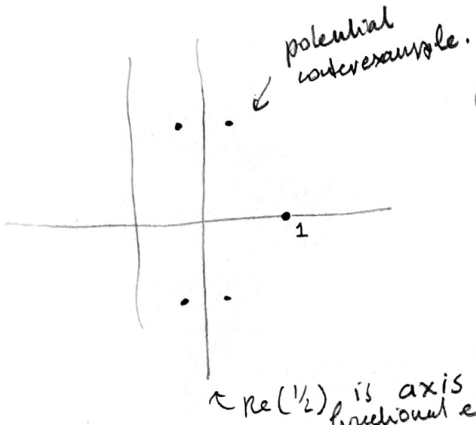
Fix a pair of complex conjugate zeroes, ρ and $\bar{\rho}$:

Combination: $$\lambda \cdot x^{\operatorname{Re}\rho} \cdot \cos(\gamma + \log x)$$

constants depending only on ρ.



<u>Exercise:</u> Show that PNT $\Leftrightarrow$ ζ has no zeroes w/ $\mathrm{Re}\, s = 1$.



<u>Riemann hypothesis</u> $\Leftrightarrow$ $x - \psi(x) \in O(x^{1/2})$.

constant in frequency

As $\mathrm{Im}(s)$ gets bigger, size of λ gets smaller. Thus if RH is true, then small zeroes contribute larger variations.

<u>Rmk:</u> See the website for some approximations to prime counting function via zeroes of ζ.

<u>Dirichlet L-functions:</u> Fix $m \in \mathbb{Z}$ and $a \in (\mathbb{Z}/m\mathbb{Z})^\times$.

What about the set $\{p \mid p \equiv a \bmod m\}$. Is it infinite?

Analogue of PNT:

$$\pi_{a,m}(x) \sim \frac{1}{\phi(m)} \frac{x}{\log x}.$$

<u>Naive:</u>

$$\prod_{p \equiv a (m)} \frac{1}{(1-p^{-s})}$$

no nice properties!

What does representation theory teach us?

functions: $(\mathbb{Z}/m\mathbb{Z})^\times = \cdot \cdot \cdot \cdot \longrightarrow \mathbb{C}$ has two nice bases:

indicator functions: $x \longmapsto \delta_{x,a}$.
$a \in (\mathbb{Z}/m\mathbb{Z})^\times$.

irreducible characters: $x \longrightarrow e^{2\pi i j/\phi(m)}$

for $j = 0, \dots, \phi(m)-1$.

<u>Definition:</u> A <u>Dirichlet character modulo m</u> is a character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ extended by zero to all of $\mathbb{Z}$.

Euler product

Dirichlet L-function: $$L(\chi, s) = \sum_{n \geq 1} \chi(n) n^{-s} = \prod_{p \text{ prime}} \frac{1}{1-\chi(p)p^{-s}}$$

If $\chi =$ trivial, recover ζ-function. $L(\chi, s)$ is (absolutely) convergent on $(\operatorname{Re} s > 1)$ $\operatorname{Re}(s) > 0$. It admits a holomorphic extension to all of $\mathbb{C}$ and satisfies a functional equation.

<u>Dirichlet's theorem</u> is an easy consequence of

$$L(\chi, 1) \neq 0.$$

(GRH) all non-trivial zeroes of $L(\chi, s)$ lie on the critical line.

<u>Dedekind ζ-functions:</u>

$$\begin{array}{ccc} K & \supset & \mathcal{O} \\ | & & | \\ \mathbb{Q} & \supset & \mathbb{Z} \end{array}$$

What about primes in $\mathcal{O}$?

Given $0 \neq I \subset \mathcal{O}$, define $N\mathfrak{p} := |\mathcal{O}/\mathfrak{p}|$. E.g. $N(p) = p$ in $\mathbb{Z}$.

unique factorisation of primes

Dedekind ζ-function:

$$\zeta_K(s) = \sum_{0 \neq I \subset \mathcal{O}} (NI)^{-s} = \prod_{0 \neq \mathfrak{p} \text{ prime}} \frac{1}{(1-(N\mathfrak{p})^{-s})}.$$

Again, meromorphic continuation, functional equation, Riemann hypothesis etc.

<u>Key example:</u> $K = \mathbb{Q}(i) \supset \mathcal{O} = \mathbb{Z}[i]$.

$$\zeta_K(s) = \prod_{\mathfrak{p} \subset \mathcal{O}} \frac{1}{1 - N\mathfrak{p}^{-s}} = \underbrace{\left(\frac{1}{1-2^{-s}}\right)}_{\substack{p=2 \text{ is} \\ \text{ramified}}} \prod_{\substack{p \\ p \text{ splits} \\ \| \\ p=1 \\ \text{mod } 4}} \underbrace{(1-p^{-s})(1-p^{-s})}_{\substack{\text{two primes} \\ \text{lying over } p \\ (\text{e.g. } (5)=(2+i)(2-i))}} \prod_{\substack{p \\ p \text{ inert} \\ \| \\ \text{e.g. } \mathbb{Z}[i]/(3) \cong \mathbb{F}_9 \\ p=3 \text{ mod } 4}} \underbrace{(1-p^{-2s})}_{(1-p^{-s})(1+p^{-s})}$$

$$= \prod_p \frac{1}{(1-p^{-s})} \prod_{p \neq 2} \frac{1}{1-\chi(p)p^{-s}} = \zeta_{\mathcal{O}}(s) \cdot L(\chi, s)$$

where $\chi : (\mathbb{Z}/4\mathbb{Z})^\times : \begin{array}{l} 1 \longmapsto 1 \\ 3 \longmapsto -1 \end{array}$.

<u>Moral:</u> difficulties of $\mathbb{Z}[i]$ are already contained in $\mathbb{Z}$!

<u>Walking across the bridge:</u> ζ-functions of curves$/\mathbb{F}_p$

Remember our analogy:

$$\begin{array}{ccc} \mathcal{O} & & \text{smooth curves.} \\ \cap & \longleftrightarrow & \\ K & & \text{function fields}/\mathbb{F}_p \end{array}$$

<u>Easiest curve</u> $\mathbb{P}^1_{\mathbb{F}_p}$. Instead work with $\mathbb{A}_1$, analogue of $\mathcal{O}$ is $\mathbb{F}_p[x]$.

any non-zero ideal in $\mathcal{O}$ is (f) for some monic polynomial $f \in \mathbb{F}_p[x]$.

$$\zeta_{\mathbb{A}_1}(s) = \sum_{0 \neq I \subset \mathcal{O}} (NI)^{-s} = \sum_{d \geq 0} \left(\begin{array}{c}\text{number of monic} \\ \text{polynomials of degree } n\end{array}\right) \cdot \underbrace{(NI)^{-s}}_{\substack{\| \\ |\mathbb{F}_p[x]/(f)| \\ \| \\ p^d}}$$

$$= \sum_{d \geq 0} \underbrace{p^d (p^d)^{-s}}_{\substack{\| \\ (p^{-s+1})^d}} = \frac{1}{1-p^{-s+1}}$$

simple pole at $s=1$ and no zeroes!

Thus "error term $= 0$". In fact (Gauß):

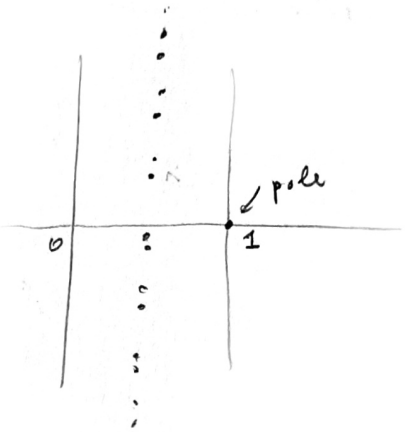
$$\#\text{ irreducible } f \text{ of degree } d = \frac{1}{d} \sum_{m \mid d} \mu\left(\frac{d}{m}\right) p^m .$$

Artin's thesis studied $\mathbb{F}_p[x,y]/(y^2 = f(x))$ (analogue of quadratic fields $\mathbb{Q}(\sqrt{\alpha})$)

$\uparrow$ square-free.

and showed:
$$Z_X(s) = \frac{(1-\alpha p^{-s})(1-\bar{\alpha} p^{-s})}{1-p^{-s+1}}$$
(rational function)

where $\alpha, \bar{\alpha}$ have $|\alpha| = p^{1/2}$.



$\mathbb{A}^1$ is a "little too easy".

Extended to smooth curves $/\mathbb{F}_q$ by Weil, general varieties by Deligne (Weil conjectures).

<u>Artin L-functions:</u>

$$\begin{array}{ll} K & G = \mathrm{Gal}(K/\mathbb{Q}). \\ | & \\ \mathbb{Q} & d_K = \text{discriminant}(K). \end{array}$$

Last time: $p \nmid d_K \iff p$ is unramified

p unramified: Choice of $\mathfrak{p}$ above p $\rightsquigarrow$ Frobenius elt $\mathrm{Frob}_p \in G$.

different choices of $\mathfrak{p}$ over p $\rightsquigarrow$ conjugate Frob_p's

Fix a representation $\rho: G \to GL(V)$ of G.

Artin L-function (first approximation):
$$L_{ur}(V,s) = \prod_{p \nmid d} \det(1 - [\mathrm{Frob}_p]p^{-s} | V)^{-1}.$$

Example: ① Trivial rep $\rightsquigarrow \prod_{p \nmid d} (1-p^{-s})^{-1} = \zeta(s)$ up to finitely many factors.

② Let $\overset{K}{\overset{\shortparallel}{\mathbb{Q}(\sqrt{d})}}$ be a quadratic field and $\mu: G \xrightarrow{\sim} \{\pm 1\}$ viewed as a rep.

For $p \nmid d_K$: $\quad \mathrm{Frob}_p = \begin{cases} 1 & \text{if } p \text{ splits in } K \\ -1 & \text{if } p \text{ is inert.} \end{cases}$

$$L_{vr}(\mu, s) = \prod_{p \nmid d} \left(1 - \left(\tfrac{p}{d}\right) p^{-s}\right) = \prod_{p \nmid d} \left(1 - \chi(d) p^{-s}\right)$$

quadratic reciprocity

for some $\chi: \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}^\times$.

$= L(\chi, s)$ a Dirichlet L-function up to finitely many factors.

Exercise: Suppose K is the splitting field of $f(x) \in \mathbb{Z}[x]$. Let V_{reg} denote the regular rep of G. Find an expression for $L(V_{reg}, s)$ in terms of solutions of $f(x)$ in $\mathbb{F}_p$, $\mathbb{F}_{p^2}$, etc.

What to do at ramified primes?

For p ramified, still have an exact sequence and $\mathfrak{p}$ above p

$$\{1\} \to \underset{\substack{\uparrow \\ \text{inertia}}}{I_{\mathfrak{p}}} \longrightarrow \overset{\text{decomposition group}}{G_{\mathfrak{p}}} \longrightarrow G_{\mathfrak{p}}/I_{\mathfrak{p}} \twoheadrightarrow \{1\}$$

$$G_{\mathfrak{p}}/I_{\mathfrak{p}} = \mathrm{Aut}(\mathbb{O}/\mathfrak{p}) = \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) = \langle \mathrm{Fr} \rangle.$$

$\rightsquigarrow$ have a coset $I_{\mathfrak{p}} \mathrm{Frob}_{\mathfrak{p}}$

General local factor:

$$\det\left(1 - [\mathrm{Frob}_{\mathfrak{p}}]p^{-s} \mid V^{I_{\mathfrak{p}}}\right),$$ independent of choice of $\mathfrak{p}$.

$\Updownarrow$

$L(V,s)$ full <u>Artin L-function</u>.

<u>E.g.</u> ① trivial rep: $I_{\mathfrak{p}}$ acts trivially $\longrightarrow$ $L(\mathrm{triv}, s) = \zeta(s)$.

② $K = \mathbb{Q}(\sqrt{-k})$: if $p \mid d$, $(p) = (\mathfrak{p})^2$, $G = I_{\mathfrak{p}}$.

Hence $L(\mu, s) = L(\chi, s)$.

<u>Exercise:</u> ① (easy!) $L(V_1 \oplus V_2, s) \cong L(V_1, s)\, L(V_2, s)$.

② (do it!) If $\begin{matrix} K \\ | \\ \mathbb{Q} \end{matrix}$ is Galois with group G.

$$L(V_{reg}, s) = \zeta_K(s)$$

regular rep of G — Dedekind ζ-function.

<u>Consequence</u> (Artin) $$\zeta_K(s) = \prod_{V \in \hat{G}} L(V,s)^{\dim V}$$

irreducible reps of G.

Major generalisation of $\zeta_{\mathbb{Q}(i)}(z) = \zeta_{\mathbb{Q}}(s)\, L(\chi, s)$ that we saw earlier.

<u>Moral:</u> the difficulties in K are already contained in the difficulties of $\mathbb{Q}$, if we allow "non-abelian" difficulties.