Selberg class and Langlands reciprocity

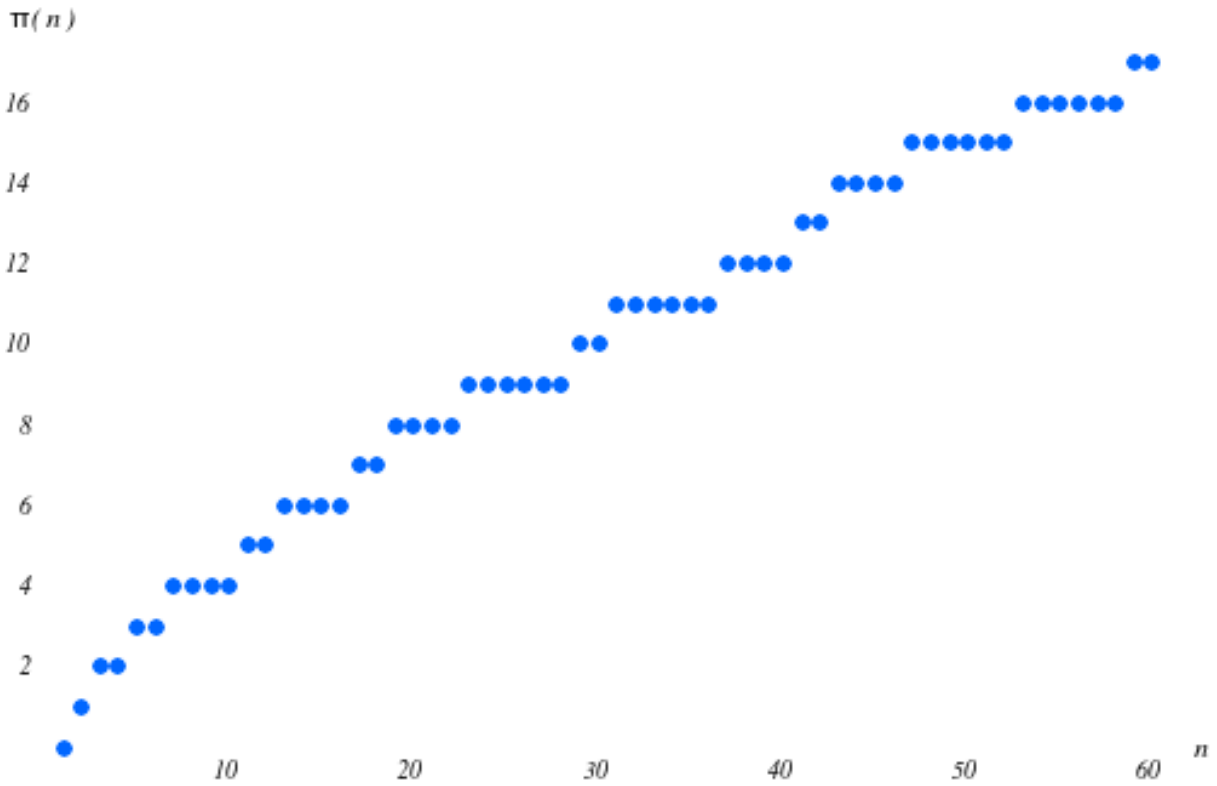
How they describe the same L-functions

Guo Liang Oon

May 8, 2026

Arithmetic randomness vs. Analytic order

$$\pi(x) = \#\{p \text{ prime} : p \leq x\}$$



[1]

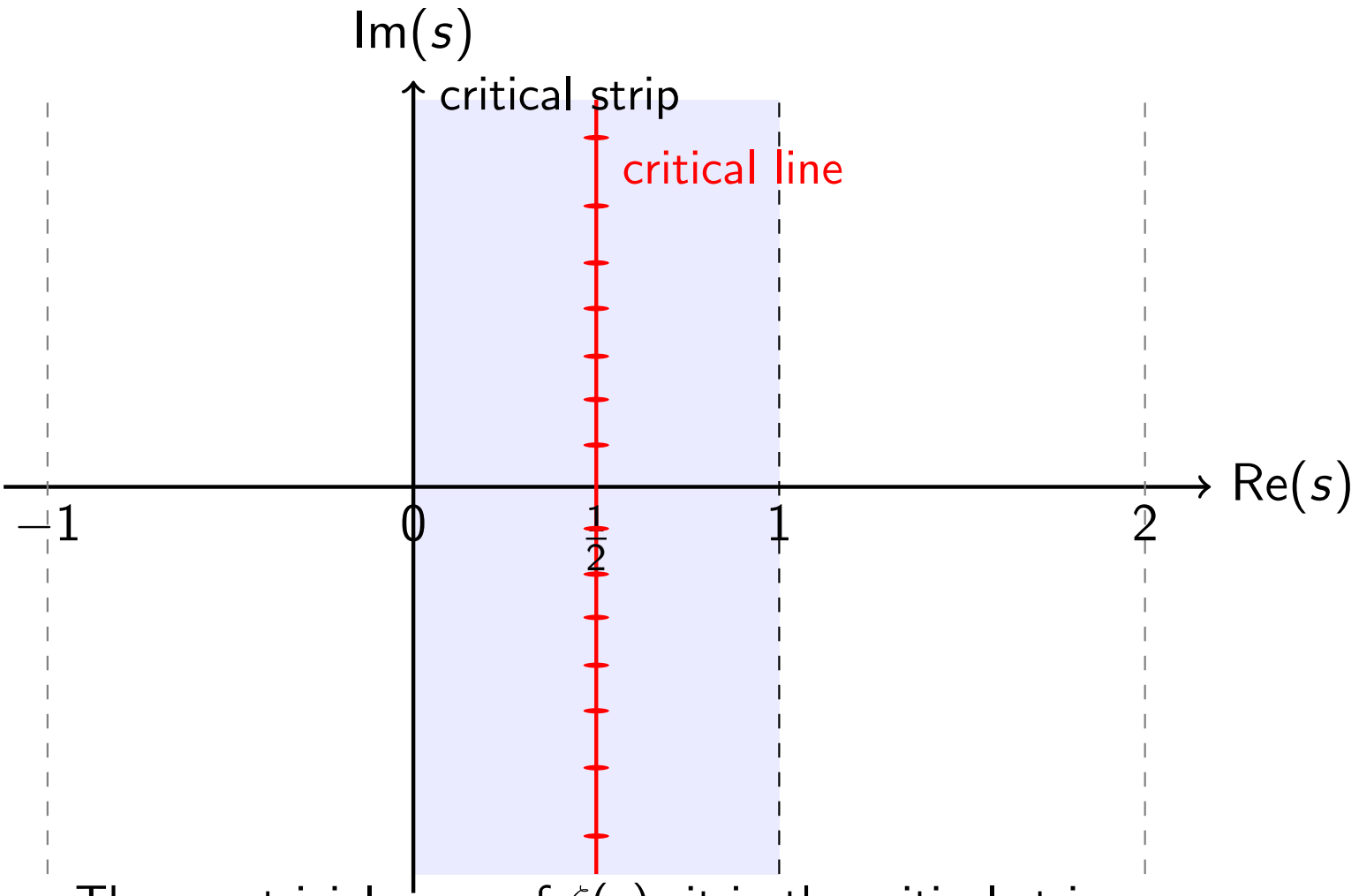
The distribution of primes

Prime number theorem:

$$\pi(x) = \underbrace{\mathrm{Li}(x)}_{\text{trend}} + \underbrace{O(x \exp(-c\sqrt{\ln x}))}_{\text{error term}}$$

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln t}$$

Zeros and primes



The non-trivial zeros of $\zeta(s)$ sit in the critical strip; their locations control the prime-counting error term.

L-function

Riemann zeta function:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

It is a Dirichlet L-**function**:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

with $\chi(n) = 1$.

What is an L-function?

Two questions, one answer

What is an L-function?

Selberg (1989)

What analytic properties must an L-function have?

Axiomatise them.

$= ?$

Langlands (1967)

Where do L-functions come from?

Build them from symmetry.

The **Automorphy Conjecture**: the two collections are identical.

Selberg's answer: an analytic fingerprint

Five tests for being an L-function

Dirichlet series	coefficients
Analytic continuation	global function
Functional equation	symmetry $s \mapsto 1 - s$
Ramanujan	controlled growth
Euler product	primes

analytic
axioms

$\Longleftrightarrow$?

arithmetic
origin

Strong enough for analytic number theory; broad enough to include the intended arithmetic examples.

Too weak: fake L-functions? Too strong: missing arithmetic ones?

Langlands: Let's build L-functions

A simple question: **When is -1 a square mod p?**

For an odd prime p:

$$x^2 \equiv -1 \pmod{p} \quad \text{has a solution iff} \quad p \equiv 1 \pmod{4}$$

Proof sketch.

Euler's criterion: -1 is a square mod p iff $(-1)^{(p-1)/2} = 1$, iff $p \equiv 1 \pmod{4}$. □

Langlands: Let's build L-functions

A simple question: **When is -1 a square mod p?**

For an odd prime p:

$$x^2 \equiv -1 \pmod{p} \quad \text{has a solution iff} \quad p \equiv 1 \pmod{4}$$

Proof sketch.

Euler's criterion: -1 is a square mod p iff $(-1)^{(p-1)/2} = 1$, iff $p \equiv 1 \pmod{4}$. □

Question

Why should a *quadratic residue* question have a *congruence* answer?

The Galois side: prime splitting

Adjoin $\sqrt{-1}$: work in the Gaussian integers $\mathbb{Z}[i]$.

The ring isomorphism

$$\mathbb{F}_p[x]/(x^2+1) \cong \mathbb{Z}[i]/(p)$$

turns the quadratic residue question into a **splitting question**:

$$\begin{aligned} & -1 \text{ is a square mod } p \\ \iff \quad & x^2+1 \text{ has a root mod } p \\ \iff \quad & p \text{ splits in } \mathbb{Z}[i]. \end{aligned}$$

Prime splitting: examples

By the Dedekind–Kummer theorem, how p splits in $\mathbb{Z}[i]$ is read off from $x^2 + 1 \bmod p$:

p		$x^2 + 1 \bmod p$	behaviour
2		$(x+1)^2$	ramifies
3		irreducible	inert
5		$(x-2)(x+2)$	splits: $(5) = (2+i)(2-i)$
7		irreducible	inert
13		$(x-5)(x+5)$	splits: $(13) = (3+2i)(3-2i)$

Prime splitting: examples

By the Dedekind–Kummer theorem, how p splits in $\mathbb{Z}[i]$ is read off from $x^2 + 1 \bmod p$:

p	$p \bmod 4$	$x^2 + 1 \bmod p$	behaviour
2	$-$	$(x+1)^2$	ramifies
3	3	irreducible	inert
5	1	$(x-2)(x+2)$	splits: $(5) = (2+i)(2-i)$
7	3	irreducible	inert
13	1	$(x-5)(x+5)$	splits: $(13) = (3+2i)(3-2i)$

The splitting behaviour is entirely determined by $p \bmod 4$ – a **congruence condition**.

The Frobenius element

Each prime p determines a canonical element of $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$ — the **Frobenius**:

$$\mathrm{Fr}_p : i \mapsto i^p$$

Then:

$$p \text{ splits} \iff \mathrm{Fr}_p = \mathrm{id}.$$

Since $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$, the Frobenius acts on a **root of unity**, so i^p depends only on p mod 4:

$$\mathrm{Fr}_p(i) = i^p = \begin{cases} i & p \equiv 1 \pmod 4 \\ -i & p \equiv 3 \pmod 4 \end{cases}$$

This is why the splitting pattern is **periodic**.

Artin reciprocity

The Frobenius map $p \mapsto \mathrm{Fr}_p$ is an isomorphism:

$$\boxed{(\mathbb{Z}/4\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})} \qquad [p \bmod 4] \mapsto \mathrm{Fr}_p$$

Composing with $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \{\pm 1\}$ gives the **Dirichlet character**:

$$\chi_{-4} : (\mathbb{Z}/4\mathbb{Z})^\times \to \{\pm 1\}, \qquad \chi_{-4}(p) = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$$

Artin reciprocity is Langlands in degree 1:
abelian Galois characters correspond to Hecke characters.

Representations

Lift to representations on absolute Galois group and idelè class group:

Galois side		**Automorphic side**
$\rho_{\chi_{-4}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_1(\mathbb{C})$	$\longleftrightarrow$	$\chi_{-4} : \mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \to GL_1(\mathbb{C})$
factors through $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$		a Hecke character; on primes, it is the same $\chi_{-4}(p)$

One encodes symmetry via Galois groups; the other via harmonic analysis on $\mathbb{A}_{\mathbb{Q}}^{\times}$.

Langlands reciprocity: same L-functions!

The same arithmetic question, seen from two sides:

	Galois	**Automorphic**
arithmetic	p splits in $\mathbb{Z}[i]$	$p \equiv 1 \pmod 4$
character	$\mathrm{Fr}_p = \mathrm{id}$ in $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$	$\chi_{-4}(p) = 1$

Lift both sides to L-functions — **Langlands reciprocity**:

$$L(s, \rho_{\chi_{-4}}) = L(s, \chi_{-4})$$

$\rho_{\chi_{-4}}$ cuts out $\mathbb{Q}(i)$ $\quad$ χ_{-4} has conductor $4 = |\Delta_{\mathbb{Q}(i)}|$

How far does this go?

Degree	Statement	Status
1	Dirichlet and Hecke characters	class field theory
2 family	elliptic curves over $\mathbb{Q}$	modularity theorem
2 general	many deep cases	still open
n general	Galois reps. vs. automorphic forms	mostly open

Langlands Reciprocity Conjecture:

$$\rho \longleftrightarrow \pi$$
$$L(s, \rho) = L(s, \pi)$$

Selberg Automorphy Conjecture:

primitive Selberg L-functions = automorphic L-functions

References I



Wikipedia contributors.
Plot of the prime-counting function $\pi(x)$.
https://en.wikipedia.org/wiki/Prime-counting_function, 2024.
Accessed: April 18, 2026.

Backup Slides

Backup: Frobenius in $\mathbb{Q}(i)$

For $p \neq 2$, Frobenius is the element satisfying

$$\mathrm{Fr}_p(\alpha) \equiv \alpha^p \pmod{\mathfrak{p}}$$

for a prime $\mathfrak{p}$ above p.

p	factorisation of x^2+1	residue degree	Fr_p
5	$(x-2)(x+2)$	1	id
3	irreducible	2	complex conjugation

If p splits, the residue field above either prime is $\mathbb{F}_p$, so the residue-field Frobenius is trivial. If p is inert, the residue field is $\mathbb{F}_{p^2}$, and Frobenius has order 2.

Backup: What does Frobenius generate?

For a prime $\mathfrak{p}$ of K above an unramified prime p of F:

$$D_{\mathfrak{p}} \longrightarrow \mathrm{Gal}\big(k_{\mathfrak{p}}/k_p\big)$$

is an isomorphism.

The residue-field Galois group is cyclic, generated by

$$x \longmapsto x^{|k_p|}.$$

So $\mathrm{Fr}_{\mathfrak{p}}$ is the unique element of the decomposition group whose action on the residue field is this generator.

In a Galois extension, changing $\mathfrak{p}$ conjugates Frobenius. Thus the invariant object is usually a conjugacy class:

$$\mathrm{Frob}_p \subset \mathrm{Gal}(K/F).$$

Backup: What about ramified primes?

At a ramified prime, the inertia group is nontrivial:

$$1 \longrightarrow I_{\mathfrak{p}} \longrightarrow D_{\mathfrak{p}} \longrightarrow \mathrm{Gal}(k_{\mathfrak{p}}/k_p) \longrightarrow 1.$$

The quotient still has a Frobenius generator, but it no longer lifts canonically to a single element of $D_{\mathfrak{p}}$.

For $K = \mathbb{Q}(i)$:

$$2\mathbb{Z}[i] = (1+i)^2.$$

So 2 is ramified. This is why the clean formula

$$\mathrm{Fr}_p(i) = i^p$$

is used only for $p \neq 2$.

Backup: Dirichlet vs Hecke characters

A Dirichlet character is a character on congruence classes:

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times.$$

A Hecke character does two upgrades at once:

1. replace $\mathbb{Q}$ by a number field F;
2. package all local conditions at all places simultaneously.

Conceptually:

$$\text{Dirichlet character} \quad \rightsquigarrow \quad \chi : \mathbb{A}_F^\times / F^\times \to \mathbb{C}^\times.$$

For $F = \mathbb{Q}$ and finite-order characters, this recovers ordinary Dirichlet characters.

Backup: What exactly is matched?

At almost every prime, Langlands reciprocity matches local prime data:

$$\rho(\mathrm{Frob}_p) \quad \longleftrightarrow \quad \text{Satake parameter of } \pi_p \quad \longleftrightarrow \quad p\text{-th Euler factor.}$$

The equality of L-functions is therefore not just a global coincidence. It says that the same prime-by-prime data is being read in two languages:

Galois side	automorphic side
Frobenius conjugacy classes	local representations π_p
characteristic polynomials	Euler factors

Backup: Degree 2 status

The slogan "degree 2 is modular" is true only in important cases, not in complete generality.

case	status
elliptic curves over $\mathbb{Q}$	modularity theorem
many 2-dimensional Galois representations	proved under hypotheses
general degree 2 Langlands reciprocity	still open

So the safe statement is: degree 1 is class field theory; degree 2 contains the modularity theorem; the general Langlands correspondence is much broader.

Backup: GRH and error terms

Prime-counting error terms measure how quickly primes equidistribute.

For a conjugacy class $C \subset G = \mathrm{Gal}(K/F)$, Chebotarev predicts

$$\pi_C(x) = \frac{|C|}{|G|}\mathrm{Li}(x) + E_C(x).$$

The main term comes from the trivial representation. The error term is controlled by zeros of the nontrivial Artin L-functions appearing when one decomposes class functions on G into characters.

GRH predicts these zeros lie on the critical line, giving square-root-size cancellation. Langlands organizes the relevant L-functions, but does not by itself prove GRH.