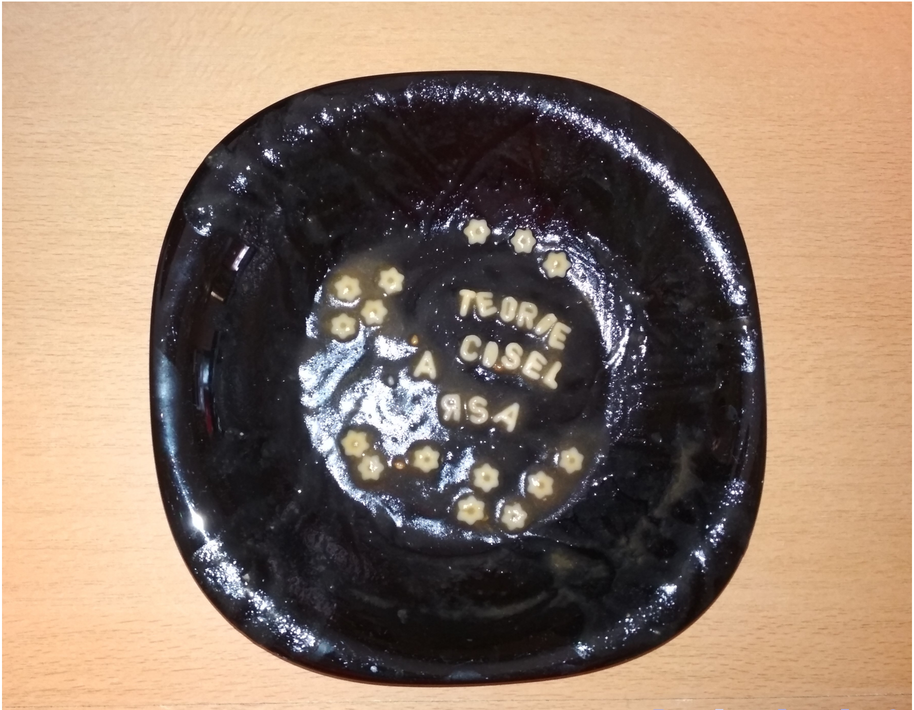
TEORIE
CISEL
A
RSA

Introduction to L-functions and Langlands program I

Vita Kala

Charles University, Prague

sites.google.com/site/vitakala/

May 17, 2020

Outline

Existence of primes

Euclid: There are infinitely many primes

How many are there?

$\pi(x)$ = number of primes $p \leq x$

Theorem (Prime number theorem, Hadamard, de la Vallée Poussin 1896)

$$\pi(x) \sim \frac{x}{\log x}, \text{ i.e.,}$$

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1$$

Proof based on idea of Riemann (1859) to study zeta-function

Existence of primes

Euclid: There are infinitely many primes
How many are there?
$\pi(x)$ = number of primes $p \leq x$

Theorem (Prime number theorem, Hadamard, de la Vallée Poussin 1896)

$$\pi(x) \sim \frac{x}{\log x}, \text{ i.e.,}$$

$$\lim_{x \to \infty} \frac{\pi(x)}{x / \log x} = 1$$

Proof based on idea of Riemann (1859) to study zeta-function

Definition

Definition (Riemann ζ-function)

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

s real: converges for $s > 1$
Studied by Euler
Well-known special values

$$\sum \frac{1}{n^2} = \zeta(2) = \frac{\pi^2}{6}$$

More useful to take s complex (Riemann 1859)

Absolutely convergent for $\mathrm{Re}(s) > 1$
$\Rightarrow \zeta(s)$ is *holomorphic* for $\mathrm{Re}(s) > 1$, i.e., has complex derivative

Definition

Definition (Riemann ζ-function)

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

s real: converges for $s > 1$

Studied by Euler

Well-known special values

$$\sum \frac{1}{n^2} = \zeta(2) = \frac{\pi^2}{6}$$

More useful to take s complex (Riemann 1859)

Absolutely convergent for $\mathrm{Re}(s) > 1$

$\Rightarrow \zeta(s)$ is *holomorphic* for $\mathrm{Re}(s) > 1$, i.e.,
has complex derivative

WHY: Euler product

What has $\zeta(s)$ to do with primes?!

Euler product

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}},$$

for $\mathrm{Re}(s) > 1$,
p runs over all primes.

Proof: Geometric series

$$\prod_p \frac{1}{1 - \frac{1}{p^s}} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right)$$

Multiply out and rearrange RHS to get

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{2^{2s}} + \frac{1}{5^s} + \frac{1}{2^s} \cdot \frac{1}{3^s} + \cdots .$$

WHY: Euler product

What has $\zeta(s)$ to do with primes?!

Euler product

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}},$$

for $\mathrm{Re}(s) > 1$,
p runs over all primes.

Proof: Geometric series

$$\prod_p \frac{1}{1 - \frac{1}{p^s}} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right)$$

Multiply out and rearrange RHS to get

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{2^{2s}} + \frac{1}{5^s} + \frac{1}{2^s} \cdot \frac{1}{3^s} + \cdots .$$

Euler product and primes

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

$\Rightarrow$ there are infinitely many primes:
If finitely many, then RHS at $s = 1$ converges $\prod_p \frac{1}{1-\frac{1}{p}} < \infty$
But harmonic series $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges, i.e., $\zeta(1) = \infty$.

First indication that understanding $\zeta(s)$ around $s = 1$ is useful for number of primes $\pi(x)$

Euler product and primes

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

$\Rightarrow$ there are infinitely many primes:
If finitely many, then RHS at $s = 1$ converges $\prod_p \frac{1}{1-\frac{1}{p}} < \infty$
But harmonic series $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges, i.e., $\zeta(1) = \infty$.

First indication that understanding $\zeta(s)$ around $s = 1$ is useful for number of primes $\pi(x)$

Meromorphic continuation

Second key property of ζ-function

Definition/Theorem: Meromorphic continuation

$\zeta(s)$ has *meromorphic continuation*, i.e.,
there is meromorphic function $\tilde{\zeta}(s)$ that extends $\tilde{\zeta}(s) = \zeta(s)$ for $\mathrm{Re}(s) > 1$.

Recall $f : \mathbb{C} \to \mathbb{C}$ is *meromorphic*,
if defined and has complex derivative for all points $s \in \mathbb{C}$
EXCEPT for a discrete set of *poles* s_0
at which behaves as $\frac{a}{(s-s_0)^k}$ for some $k \in \mathbb{N}$ and $a \in \mathbb{C}$.

Continuation of Riemann zeta-function has only one pole of order $k = 1$ (with residue $a = 1$):
Well-known $s_0 = 1$.
Meromorphic continuation is unique (if exists), so let's not distinguish $\zeta(s) := \tilde{\zeta}(s)$.

Meromorphic continuation

Second key property of ζ-function

Definition/Theorem: Meromorphic continuation

$\zeta(s)$ has *meromorphic continuation*, i.e.,
there is meromorphic function $\tilde{\zeta}(s)$ that extends $\tilde{\zeta}(s) = \zeta(s)$ for $\mathrm{Re}(s) > 1$.

Recall $f : \mathbb{C} \to \mathbb{C}$ is *meromorphic*,
if defined and has complex derivative for all points $s \in \mathbb{C}$
EXCEPT for a discrete set of *poles* s_0
at which behaves as $\frac{a}{(s-s_0)^k}$ for some $k \in \mathbb{N}$ and $a \in \mathbb{C}$.
Continuation of Riemann zeta-function has only one pole of order $k = 1$
(with residue $a = 1$):
Well-known $s_0 = 1$.
Meromorphic continuation is unique (if exists), so let's not distinguish $\zeta(s) := \tilde{\zeta}(s)$.

Meromorphic continuation

Second key property of ζ-function

Definition/Theorem: Meromorphic continuation

$\zeta(s)$ has *meromorphic continuation*, i.e.,
there is meromorphic function $\tilde{\zeta}(s)$ that extends $\tilde{\zeta}(s) = \zeta(s)$ for $\mathrm{Re}(s) > 1$.

Recall $f : \mathbb{C} \to \mathbb{C}$ is *meromorphic*,
if defined and has complex derivative for all points $s \in \mathbb{C}$
EXCEPT for a discrete set of *poles* s_0
at which behaves as $\frac{a}{(s-s_0)^k}$ for some $k \in \mathbb{N}$ and $a \in \mathbb{C}$.
Continuation of Riemann zeta-function has only one pole of order $k = 1$
(with residue $a = 1$):
Well-known $s_0 = 1$.
Meromorphic continuation is unique (if exists), so let's not distinguish
$\zeta(s) := \tilde{\zeta}(s)$.

Functional equation

Theorem (Functional equation)

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s),$$

where

$$\Gamma(z) = \int_0^\infty x^{z-1} e^{-x} dx$$

is usual Γ*-function that extends factorial:* $\Gamma(n) = (n-1)!$ *for* $n \in \mathbb{N}$.

LOOKS VERY COMPLICATED, SHOULD I STOP WATCHING?

NOT YET! Key: gives explicit relation between $\zeta(s)$ and $\zeta(1-s)$.
Ramanujan's "identity"

$$1+2+3+4+5+\cdots = \zeta(-1) = 2^{-1}\pi^{-2} \sin\left(-\frac{\pi}{2}\right) \Gamma(2)\zeta(2) = -\frac{1}{12}.$$

Functional equation

Theorem (Functional equation)

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s),$$

where

$$\Gamma(z) = \int_0^\infty x^{z-1} e^{-x} dx$$

is usual Γ*-function that extends factorial:* $\Gamma(n) = (n-1)!$ *for* $n \in \mathbb{N}$*.*

LOOKS VERY COMPLICATED, SHOULD I STOP WATCHING?

NOT YET! Key: gives explicit relation between $\zeta(s)$ and $\zeta(1-s)$.
Ramanujan's "identity"

$$1 + 2 + 3 + 4 + 5 + \cdots = \zeta(-1) = 2^{-1}\pi^{-2} \sin\left(-\frac{\pi}{2}\right) \Gamma(2)\zeta(2) = -\frac{1}{12}.$$

Functional equation

Theorem (Functional equation)

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s),$$

where

$$\Gamma(z) = \int_0^\infty x^{z-1} e^{-x} dx$$

is usual Γ*-function that extends factorial:* $\Gamma(n) = (n-1)!$ *for* $n \in \mathbb{N}$*.*

LOOKS VERY COMPLICATED, SHOULD I STOP WATCHING?

NOT YET! Key: gives explicit relation between $\zeta(s)$ and $\zeta(1-s)$.
Ramanujan's "identity"

$$1 + 2 + 3 + 4 + 5 + \cdots = \zeta(-1) = 2^{-1}\pi^{-2} \sin\left(-\frac{\pi}{2}\right) \Gamma(2)\zeta(2) = -\frac{1}{12}.$$

Critical strip

Functional equation $\zeta(s) = \mathrm{blabla} \cdot \zeta(1-s)$,
$\Rightarrow$ can use $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ for $\mathrm{Re}(s) > 1$ to compute values for $\mathrm{Re}(s) < 0$.

Between is *critical strip* $0 < \mathrm{Re}(s) < 1$.
Very mysterious behavior of zeta

Riemann hypothesis

s is zero of ζ-function in critical strip, i.e.,
$\zeta(s) = 0$ for $0 < \mathrm{Re}(s) < 1$.
Then s lies on the center line $\mathrm{Re}(s) = \frac{1}{2}$.

Riemann hypothesis

s is zero of ζ-function in critical strip, i.e.,
$\zeta(s) = 0$ for $0 < \mathrm{Re}(s) < 1$.
Then s lies on the center line $\mathrm{Re}(s) = \frac{1}{2}$.

WHY PROVE?

1. get famous and rich
2. understand asymptotics of primes:

get precise error terms for PNT $\pi(x) \sim \frac{x}{\log x}$

$$\pi(x) = \frac{x}{\log x} + \frac{1!x}{(\log x)^2} + \frac{2!x}{(\log x)^3} + \cdots + O(\sqrt{x}\log x)$$

Already $\zeta(s) \neq 0$ for $\mathrm{Re}(s) = 1 \Leftrightarrow$ PNT

3. develop tools that generalize to other L-functions

Riemann hypothesis

Riemann hypothesis

s is zero of ζ-function in critical strip, i.e.,
$\zeta(s) = 0$ for $0 < \mathrm{Re}(s) < 1$.
Then s lies on the center line $\mathrm{Re}(s) = \frac{1}{2}$.

WHY PROVE?

1. get famous and rich
2. understand asymptotics of primes:
get precise error terms for PNT $\pi(x) \sim \frac{x}{\log x}$

$$\pi(x) = \frac{x}{\log x} + \frac{1!x}{(\log x)^2} + \frac{2!x}{(\log x)^3} + \cdots + O(\sqrt{x}\log x)$$

Already $\zeta(s) \neq 0$ for $\mathrm{Re}(s) = 1 \Leftrightarrow$ PNT
3. develop tools that generalize to other L-functions

Riemann hypothesis

Riemann hypothesis

s is zero of ζ-function in critical strip, i.e.,
$\zeta(s) = 0$ for $0 < \mathrm{Re}(s) < 1$.
Then s lies on the center line $\mathrm{Re}(s) = \frac{1}{2}$.

WHY PROVE?

1. get famous and rich
2. understand asymptotics of primes:

get precise error terms for PNT $\pi(x) \sim \frac{x}{\log x}$

$$\pi(x) = \frac{x}{\log x} + \frac{1!x}{(\log x)^2} + \frac{2!x}{(\log x)^3} + \cdots + O(\sqrt{x}\log x)$$

Already $\zeta(s) \neq 0$ for $\mathrm{Re}(s) = 1 \Leftrightarrow$ PNT

3. develop tools that generalize to other L-functions

Riemann hypothesis

Riemann hypothesis

s is zero of ζ-function in critical strip, i.e.,
$\zeta(s) = 0$ for $0 < \mathrm{Re}(s) < 1$.
Then s lies on the center line $\mathrm{Re}(s) = \frac{1}{2}$.

WHY PROVE?

1. get famous and rich
2. understand asymptotics of primes:

get precise error terms for PNT $\pi(x) \sim \frac{x}{\log x}$

$$\pi(x) = \frac{x}{\log x} + \frac{1!x}{(\log x)^2} + \frac{2!x}{(\log x)^3} + \cdots + O(\sqrt{x}\log x)$$

Already $\zeta(s) \neq 0$ for $\mathrm{Re}(s) = 1 \Leftrightarrow$ PNT

3. develop tools that generalize to other L-functions

Outline

Primes in arithmetic progressions

Theorem (Dirichlet's theorem on arithmetic progressions, 1837)

There are infinitely many primes of the form $nt + a$ for every coprime $n, a \in \mathbb{N}$.

Some cases, e.g., $4t - 1$ or $nt + 1$ elementary (using cyclotomic polynomials)

In general requires L-functions

Even stronger

Theorem (PNT for arithmetic progressions)

$$(\text{Number of primes } p = nt + a \leq x) \sim \frac{1}{\varphi(n)} \cdot \frac{x}{\log x}$$

Primes in arithmetic progressions

Theorem (Dirichlet's theorem on arithmetic progressions, 1837)

There are infinitely many primes of the form $nt + a$ for every coprime $n, a \in \mathbb{N}$.

Some cases, e.g., $4t - 1$ or $nt + 1$ elementary (using cyclotomic polynomials)

In general requires L-functions

Even stronger

Theorem (PNT for arithmetic progressions)

$$(\text{Number of primes } p = nt + a \leq x) \sim \frac{1}{\varphi(n)} \cdot \frac{x}{\log x}$$

Characters

Definition

Dirichlet character modulo n is a map $\chi : \mathbb{N} \to \mathbb{C}$ such that for all positive integers u, v and k:

- χ is periodic modulo n: $\chi(u + kn) = \chi(u)$,
- χ is multiplicative: $\chi(uv) = \chi(u)\chi(v)$,
- $\chi(u) \neq 0$ iff u is coprime with n.

Exercise: All non-zero values of a character χ lie on the unit circle $|z| = 1$ and are $\varphi(n)$-th roots of one $e^{2\pi ir/\varphi(n)}$ (with some $r \in \mathbb{Z}$).

Dirichlet characters are suitable for capturing information modulo n

Examples:

- Trivial character modulo n

$$\chi(u) = \begin{cases} 1 & \text{if } \gcd(u, n) = 1, \\ 0 & \text{if } \gcd(u, n) > 1. \end{cases}$$

- Non-trivial character modulo 5

$$\chi(u) = \begin{cases} 1 & \text{if } u \equiv 1 \pmod 5, \\ i & \text{if } u \equiv 2 \pmod 5, \\ -i & \text{if } u \equiv 3 \pmod 5, \\ -1 & \text{if } u \equiv 4 \pmod 5, \\ 0 & \text{if } u \equiv 0 \pmod 5. \end{cases}$$

- Legendre symbol $\left(\frac{u}{p}\right)$ modulo primes p.

Dirichlet L-functions

Riemann $\zeta(s)$ good to study primes, characters χ good for arithmetic progressions $\Rightarrow$ let's combine them!

Definition (Dirichlet 1837)

Dirichlet L-function

$$L(s,\chi) = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}},$$

absolutely convergent for $\mathrm{Re}(s) > 1$.

Notation by L already used by Dirichlet – apparently quite randomly

Examples:

$\chi =$ trivial character modulo 1: $L(s,\chi) = \zeta(s)$

$\chi =$ trivial character modulo p_0: $L(s,\chi) = \prod_{p \neq p_0} \frac{1}{1-\frac{1}{p^s}}$

Dirichlet L-functions

Riemann $\zeta(s)$ good to study primes, characters χ good for arithmetic progressions $\Rightarrow$ let's combine them!

Definition (Dirichlet 1837)

Dirichlet L-function

$$L(s,\chi) = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}},$$

absolutely convergent for $\mathrm{Re}(s) > 1$.

Notation by L already used by Dirichlet – apparently quite randomly

Examples:

$\chi =$ trivial character modulo 1: $L(s,\chi) = \zeta(s)$

$\chi =$ trivial character modulo p_0: $L(s,\chi) = \prod_{p \neq p_0} \frac{1}{1-\frac{1}{p^s}}$

Functional equation

$$L(s,\chi) = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}},$$

Many analogies with Riemann ζ-function:

- Euler product of *degree 1*, i.e.,
  we multiply $\frac{1}{P_{p,\chi}(p^{-s})}$, where $P_{p,\chi}(X) = 1 - \chi(p)X$ is polynomial of degree 1 (depending on χ and the prime p).
- Meromorphic continuation of $L(s,\chi)$ to $s \in \mathbb{C}$,
  in fact holomorphic (i.e., no poles) if χ is non-trivial
- Functional equation,
  that relates $L(s,\chi)$ and $L(1-s,\overline{\chi})$
  where $\overline{\chi}$ is conjugate character $\overline{\chi}(u) := \overline{\chi(u)}$.
  (even more technical than FE for $\zeta(s0)$)

Functional equation

$$L(s,\chi) = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}},$$

Many analogies with Riemann ζ-function:

- Euler product of *degree 1*, i.e., we multiply $\frac{1}{P_{p,\chi}(p^{-s})}$, where $P_{p,\chi}(X) = 1 - \chi(p)X$ is polynomial of degree 1 (depending on χ and the prime p).
- Meromorphic continuation of $L(s,\chi)$ to $s \in \mathbb{C}$, in fact holomorphic (i.e., no poles) if χ is non-trivial
- Functional equation, that relates $L(s,\chi)$ and $L(1-s,\overline{\chi})$ where $\overline{\chi}$ is conjugate character $\overline{\chi}(u) := \overline{\chi(u)}$. (even more technical than FE for $\zeta(s0)$)

Proof of Dirichlet's theorem on arithmetic progressions

Theorem

There are infinitely many primes $nt + a$ for every coprime $n, a \in \mathbb{N}$.

Idea of proof: consider

$$S_{n,a}(s) = \sum_{p \equiv a \pmod{n}} \frac{1}{p^s}$$

if we prove a pole at $s = 1$, there are infinitely many $p \equiv a \pmod{n}$

To isolate AP, use identity

$$\frac{1}{\varphi(n)} \sum_{\chi \bmod n} \chi(a)^{-1} \cdot \chi(u) = \begin{cases} 1 & \text{if } u \equiv a \pmod{n}, \\ 0 & \text{else,} \end{cases}$$

where sum is over all characters modulo n.

Proof of Dirichlet's theorem on arithmetic progressions

Theorem

There are infinitely many primes $nt + a$ for every coprime $n, a \in \mathbb{N}$.

Idea of proof: consider

$$S_{n,a}(s) = \sum_{p \equiv a \pmod{n}} \frac{1}{p^s}$$

if we prove a pole at $s = 1$, there are infinitely many $p \equiv a \pmod{n}$

To isolate AP, use identity

$$\frac{1}{\varphi(n)} \sum_{\chi \bmod n} \chi(a)^{-1} \cdot \chi(u) = \begin{cases} 1 & \text{if } u \equiv a \pmod{n}, \\ 0 & \text{else,} \end{cases}$$

where sum is over all characters modulo n.

Proof of Dirichlet's theorem on arithmetic progressions 2

$$\log L(s,\chi) = \log\left(\prod_p \frac{1}{1-\frac{\chi(p)}{p^s}}\right) = -\sum_p \log\left(1-\frac{\chi(p)}{p^s}\right)$$

Taylor expansion $-\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \dots$

$$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + \text{small rest}$$

$$\frac{1}{\varphi(n)} \sum_{\chi \mod n} \chi(a)^{-1} \log L(s,\chi) \approx \sum_p \frac{1}{\varphi(n)p^s} \sum_{\chi \mod n} \chi(a)^{-1}\chi(p) =$$

$$= \sum_{p \equiv a \mod n} \frac{1}{p^s} = S_{n,a}(s)$$

Want pole at $s = 1 \Rightarrow$ study LHS, key is $L(1,\chi) \neq 0$

Proof of Dirichlet's theorem on arithmetic progressions 2

$$\log L(s,\chi) = \log\left(\prod_p \frac{1}{1-\frac{\chi(p)}{p^s}}\right) = -\sum_p \log\left(1-\frac{\chi(p)}{p^s}\right)$$

Taylor expansion $-\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \dots$

$$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + \text{small rest}$$

$$\frac{1}{\varphi(n)} \sum_{\chi \mod n} \chi(a)^{-1} \log L(s,\chi) \approx \sum_p \frac{1}{\varphi(n)p^s} \sum_{\chi \mod n} \chi(a)^{-1}\chi(p) =$$

$$= \sum_{p\equiv a \mod n} \frac{1}{p^s} = S_{n,a}(s)$$

Want pole at $s=1 \Rightarrow$ study LHS, key is $L(1,\chi) \neq 0$

Outline

Langlands program

Vast web of conjectures

emerging and developing since 1960's

connections between number theory and representation theory

2018 Abel prize for Langlands

Broad goal: understand general L-functions

that encode algebraic or geometric information

(primes or solutions to diophantine equations)

want Euler Product, Meromorphic Continuation, Functional Equation

hard to prove directly

$\Rightarrow$ define analytic L-functions, for which FE easier

For now: what algebraic L-functions?

Cyclotomic fields

$K = \mathbb{Q}(e^{2\pi i/m})$ for some $m \in \mathbb{N}$.
E.g., $m = 4 \Rightarrow e^{2\pi i/4} = e^{\pi i/2} = i \Rightarrow K = \mathbb{Q}(i)$

Key property:
Galois group $Gal(\mathbb{Q}(e^{2\pi i/m})/\mathbb{Q})$, i.e.,
group of all automorphisms of the field $\mathbb{Q}(e^{2\pi i/m})$,
is isomorphic to

$$\mathbb{Z}_m^* = \{u \in \mathbb{Z} | 0 < u < m, \gcd(u, m) = 1\}$$

Easy to describe: $u \in \mathbb{Z}_m^*$ corresponds to

$$\varphi_u : \mathbb{Q}\left(e^{\frac{2\pi i}{m}}\right) \to \mathbb{Q}\left(e^{\frac{2\pi i}{m}}\right),$$

$$\varphi_u\left(e^{\frac{2\pi i}{m}}\right) = e^{\frac{2\pi i u}{m}}.$$

Cyclotomic fields

$K = \mathbb{Q}(e^{2\pi i/m})$ for some $m \in \mathbb{N}$.
E.g., $m = 4 \Rightarrow e^{2\pi i/4} = e^{\pi i/2} = i \Rightarrow K = \mathbb{Q}(i)$

Key property:
Galois group $Gal(\mathbb{Q}(e^{2\pi i/m})/\mathbb{Q})$, i.e.,
group of all automorphisms of the field $\mathbb{Q}(e^{2\pi i/m})$,
is isomorphic to

$$\mathbb{Z}_m^* = \{u \in \mathbb{Z} | 0 < u < m, \gcd(u, m) = 1\}$$

Easy to describe: $u \in \mathbb{Z}_m^*$ corresponds to

$$\varphi_u : \mathbb{Q}\left(e^{\frac{2\pi i}{m}}\right) \to \mathbb{Q}\left(e^{\frac{2\pi i}{m}}\right),$$

$$\varphi_u\left(e^{\frac{2\pi i}{m}}\right) = e^{\frac{2\pi iu}{m}}.$$

Galois representations

In general have Galois extension $K = \mathbb{Q}(\alpha) \supset \mathbb{Q}$
(Galois $\Leftrightarrow$ all roots of minimal polynomial of α lie in K)
Galois group $Gal(K/\mathbb{Q})$ = all field automorphisms

To understand $Gal(K/\mathbb{Q})$, consider its *Galois representations*, i.e., group homs

$$\rho : Gal(K/\mathbb{Q}) \to GL_n(\mathbb{C}),$$

where $GL_n(\mathbb{C})$ is group of $n \times n$ invertible matrices.

Motivation: $Gal(K/\mathbb{Q})$ is quite abstract group, but ρ realizes its elements as specific matrices $\Rightarrow$ can take determinant, eigenvalues, etc.

Galois representations

In general have Galois extension $K = \mathbb{Q}(\alpha) \supset \mathbb{Q}$
(Galois $\Leftrightarrow$ all roots of minimal polynomial of α lie in K)
Galois group $Gal(K/\mathbb{Q})$ = all field automorphisms

To understand $Gal(K/\mathbb{Q})$, consider its *Galois representations*, i.e., group homs

$$\rho : Gal(K/\mathbb{Q}) \to GL_n(\mathbb{C}),$$

where $GL_n(\mathbb{C})$ is group of $n \times n$ invertible matrices.

Motivation: $Gal(K/\mathbb{Q})$ is quite abstract group, but ρ realizes its elements as specific matrices $\Rightarrow$ can take determinant, eigenvalues, etc.

Artin L-function

General definition harder, so now only for cyclotomic $K = \mathbb{Q}(e^{2\pi i/m})$ and 1-dimensional representations $\rho : Gal(K/\mathbb{Q}) \to \mathbb{C}^* = GL_1(\mathbb{C})$

Recall $\mathbb{Z}_m^* \simeq Gal(K/\mathbb{Q}) \Rightarrow$
Associate to ρ Dirichlet character modulo m

$$\chi(u) = \begin{cases} \rho(\varphi_u) & \text{if } \gcd(u,m) = 1, \\ 0 & \text{if } \gcd(u,m) > 1. \end{cases}$$

Artin L-function then equals Dirichlet L-function for character χ

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

This general correspondence of Artin "algebraic" and Dirichlet "analytic" L-functions was one of keystones on which Langlands built his program

Class field theory

$L(s,\rho) = L(s,\chi)$ holds for all 1-d representations $\rho : Gal(K/\mathbb{Q}) \to \mathbb{C}^*$ (for any number field K)

Follows from *Class Field Theory*

Emil Artin, Helmut Hasse, John Tate $\sim$ 1900 – 1950

describe all K with *commutative* Galois group similarly as

$Gal(\mathbb{Q}(e^{2\pi i/m})/\mathbb{Q}) \simeq \mathbb{Z}_m^*$.

Special case: *quadratic reciprocity*

- relation between Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ for primes p, q,
- i.e., solvability of congruences $x^2 \equiv p \pmod q$ and $x^2 \equiv q \pmod p$.

Even implies higher reciprocity laws for congruences of n-th degree

$\Rightarrow$ main theorem is called Artin reciprocity law

$\Rightarrow$ hypothetical, much more general Langlands reciprocity law

Class field theory

$L(s,\rho) = L(s,\chi)$ holds for all 1-d representations $\rho : Gal(K/\mathbb{Q}) \to \mathbb{C}^*$
(for any number field K)

Follows from *Class Field Theory*

Emil Artin, Helmut Hasse, John Tate $\sim$ 1900 – 1950

describe all K with *commutative* Galois group similarly as

$Gal(\mathbb{Q}(e^{2\pi i/m})/\mathbb{Q}) \simeq \mathbb{Z}_m^*$.

Special case: *quadratic reciprocity*

- relation between Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ for primes p, q,
- i.e., solvability of congruences $x^2 \equiv p \pmod{q}$ and $x^2 \equiv q \pmod{p}$.

Even implies higher reciprocity laws for congruences of n-th degree

$\Rightarrow$ main theorem is called Artin reciprocity law

$\Rightarrow$ hypothetical, much more general Langlands reciprocity law

Recap

Studied Riemann zeta $\zeta(s)$,
Dirichlet $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\frac{\chi(p)}{p^s}}$,
Artin $L(s,\rho)$
all L-functions of degree 1

Next:

- Elliptic curves: diophantine equations $y^2 = x^3 + ax + b$, give algebraic L-functions of degree 2
- Modular forms: corresponding analytic L-functions of degree 2
- Their correspondence $\Rightarrow$ FLT
- Langlands program: Artin representations correspond to automorphic representations

Recap

Studied Riemann zeta $\zeta(s)$,
Dirichlet $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}$,
Artin $L(s, \rho)$
all L-functions of degree 1

Next:

- Elliptic curves: diophantine equations $y^2 = x^3 + ax + b$, give algebraic L-functions of degree 2
- Modular forms: corresponding analytic L-functions of degree 2
- Their correspondence $\Rightarrow$ FLT
- Langlands program: Artin representations correspond to automorphic representations

Recap

Studied Riemann zeta $\zeta(s)$,
Dirichlet $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\frac{\chi(p)}{p^s}}$,
Artin $L(s,\rho)$
all L-functions of degree 1

Next:

- Elliptic curves: diophantine equations $y^2 = x^3 + ax + b$, give algebraic L-functions of degree 2
- Modular forms: corresponding analytic L-functions of degree 2
- Their correspondence $\Rightarrow$ FLT
- Langlands program: Artin representations correspond to automorphic representations

Thanks

Thanks for your attention!