# Lecture 14.1

## Last time:

- The **Riemann zeta function** is the complex function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad Re(s) > 1.$$

- It has a product formula

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}.$$

- By expanding $\log \zeta(s)$, we can write

$$\log \zeta(s) = \sum \frac{1}{\ }$$

$$\log \zeta(s) = \sum_{p \text{ prime}} \frac{1}{p^s} + G(s)$$

where $G(s)$ converges for all $s$.

- Since $\log \zeta(1)$ diverges, $\sum_p \frac{1}{p}$ does too.

- A Dirichlet series is an expression of the form

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

for some arithmetic function $f$.

---

To prove that the sum

$$\sum_{p \equiv a \pmod{b}} \frac{1}{p^s}$$

diverges at $s = 1$, we considered the following Dirichlet series last time:

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

$$f(n) = f_{a,b}(n) = \begin{cases} 1, & n \equiv a \pmod{b} \\ 0, & n \not\equiv a \pmod{b}. \end{cases}$$

**Prop** Let $f(n)$ be an arithmetic function with Dirichlet series

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

If $f$ is multiplicative, i.e.

$$f(jk) = f(j)f(k) \quad \text{when} \quad \gcd(j,k) = 1,$$

then $F(s)$ has a product formula

$$F(s) = \prod_p \frac{1}{1 - f(p)p^{-s}}.$$

Exercise 1: Prove it!

If $f_{a,b}(n)$ were multiplicative, then we could write

$$F(s) = \sum^{\infty} \frac{f_{a,b}(n)}{} = \prod \frac{1}{}$$

$$F(s) = \sum_{n=1}^{\infty} \frac{f_{a,b}(n)}{n^s} = \prod_p \frac{1}{1-f_{a,b}(p)p^{-s}}$$

$$\log F(s) = \log\left(\prod_p \left(1-f_{a,b}(p)p^{-s}\right)^{-1}\right)$$

$$= \sum_p -\log\left(1-f_{a,b}(p)p^{-s}\right)$$

$$= \sum_p \sum_{n=1}^{\infty} \frac{f_{a,b}(p)}{n} p^{-sn}$$

$$= \sum_{n=1}^{\infty} \frac{1}{n} \sum_p \frac{f_{a,b}(p)}{p^{sn}}$$

$$= \sum_{p \equiv a \pmod b} \frac{1}{p^s} + G(s).$$

BUT $f_{a,b}(n)$ is not multiplicative!

e.g. $f_{3,4}(3) = 1 \qquad (3 \equiv 3 \pmod 4))$

$f_{3,4}(5) = 0 \qquad (5 \not\equiv 3 \pmod 4))$

and $f_{3,4}(5) = 0$ $\quad (5 \not\equiv 3 \pmod 4)$

but $f_{3,4}(15) = 1$ $\quad (15 \equiv 3 \pmod 4)$

To get around this, we will show how to decompose $f_{a,b}(n)$ into multiplicative functions called characters.

---

## Characters and L-Functions

**Def** A **Dirichlet character mod $b$** is a function $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ satisfying:

(1) $\chi(n+b) = \chi(n)$ for all $n \in \mathbb{Z}$,

i.e. $\chi$ is periodic with period $b$.

(2) $\chi(n) = 0$ if and only if $\gcd(n, b) > 1$.

(3) $\chi$ is completely multiplicative:

$$\chi(mn) = \chi(m)\chi(n) \text{ for all } m, n \in \mathbb{Z}.$$

$\boxed{\text{Ex}}$ For any fixed $b$, the trivial character mod $b$ is

$$\chi_0(n) = \begin{cases} 1, & \gcd(n, b) = 1 \\ 0, & \gcd(n, b) > 1. \end{cases}$$

This is sometimes called the principal character mod $b$.

$\boxed{\text{Ex}}$ For $b=4$, a nontrivial character mod 4 is

$$\chi(n) = \begin{cases} 1, & n \equiv 1 \pmod 4 \\ -1, & n \equiv 3 \pmod 4 \\ 0, & n \text{ is even.} \end{cases}$$

$\boxed{\text{Ex}}$ For $b=p$ an odd prime, define a character $\chi(n)$ by

$$\chi(n) = \begin{cases} 1, & n \text{ is a QR mod } p \\ -1, & n \text{ is a NR mod } p \\ 0, & p \mid n. \end{cases}$$

Then $\chi(n)$ is just the quadratic residue symbol $\left(\frac{n}{\ }\right)$

Let's check that it's a character mod $p$:

- $\left(\frac{n+p}{n}\right) = \left(\frac{n}{p}\right)$ since $n+p \equiv n \pmod p$

- $\left(\frac{n}{p}\right) = 0$ if and only if $p \mid n$

- $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$ by a theorem in Lecture 8.1

So residue symbols are characters!

$\boxed{\text{Ex}}$ An example of a character mod 5 is

$$\chi(n) = \begin{cases} 0, & n \equiv 0 \pmod 5 \\ 1, & n \equiv 1 \pmod 5 \end{cases}$$

$$\chi(n) = \begin{cases} i, & n \equiv 2 \pmod 5 \\ -i, & n \equiv 3 \pmod 5 \\ -1, & n \equiv 4 \pmod 5 \end{cases}$$

More generally, it is possible to construct characters mod $p$ using a primitive root mod $p$ and the index function $I(n)$ from Lecture 13.1.

Here are all the properties of characters we will need though.

$\boxed{\text{Theorem}}$ Fix $b \geq 2$.

(1) Any character $\chi$ mod $b$ satisfies $\chi(1) = 1$.

(2) For every character $\chi$ mod $b$ and every $n$ with $\gcd(n, b) = 1$, $\chi(n)$ is a complex root

of $z^d - 1$ for some $d \mid \phi(b)$, called a dth root of unity.

(3) There are exactly $\phi(b)$ characters mod $b$.

Pf: (1) Write

$$\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1).$$

Since $\gcd(1,b) = 1$, $\chi(1) \neq 0$, so we can cancel it from both sides, giving $\chi(1) = 1$.

(2) By Euler's theorem, $n^{\phi(b)} \equiv 1 \pmod{b}$

so $n^{\phi(b)} = 1 + bk$ for some $k \in \mathbb{Z}$. Then

$$\chi(n)^{\phi(b)} = \chi(n^{\phi(b)})$$

$$= \chi(1+bk)$$

$$= \chi(1) = 1.$$

So $z = \chi(n)$ satisfies the equation

$$z^{\phi(b)} - 1 = 0$$

and in particular must satisfy

$$z^d - 1 = 0$$

for some $d \mid \phi(b)$.

(3) Let $\mathbb{Z}/b\mathbb{Z} = \{0, 1, \ldots, b-1\}$

and $(\mathbb{Z}/b\mathbb{Z})^\times = \{r \in \mathbb{Z}/b\mathbb{Z} \mid \gcd(r,b) = 1\}.$

Then $\#(\mathbb{Z}/b\mathbb{Z})^\times = \phi(b)$ by definition, so

our goal is to construct a bijection between

$(\mathbb{Z}/b\mathbb{Z})^\times$ and the set

$$X(b) = \{\chi : \mathbb{Z} \to \mathbb{C} \mid \chi \text{ is a char. mod } b\}.$$

We illustrate the proof for $b = p$ prime and

leave the full version as an exercise.

Choose a primitive root $g$ mod $p$ and

define $\chi_g \in X(p)$ by

$$\chi_g(n) = \begin{cases} 0, & (n,p) > 1 \\ \omega^{I(n)}, & (n,p) = 1 \end{cases}$$

where $I(n)$ is the index of $n$ mod $p$, i.e.

the unique number mod $p-1$ satisfying

$$g^{I(n)} \equiv n \pmod p$$

and $\omega = e^{2\pi i/(p-1)}$, which is a solution to

$$z^{p-1} - 1 = 0$$

but not of

$$z^d - 1 = 0 \text{ for any } d < p-1.$$

Then $\chi_g$ is a character mod $p$: (assume $(n,p) = 1$)

- $\chi_g(n+p) = \omega^{I(n+p)} = \omega^{I(n)} = \chi_g(n)$

  since $I(n)$ is only dependent on the residue class of $n$ mod $p$

- $\chi_g(n) \neq 0$ since $\omega \neq 0$

- $\chi_g(mn) = \omega^{I(mn)} = \omega^{I(m)+I(n)}$

$$= \omega^{I(m)} \omega^{I(n)} = \chi_g(m)\chi_g(n).$$

Next, we define a map

$$\Phi : (\mathbb{Z}/b\mathbb{Z})^\times \longrightarrow X(b)$$
$$g^k \longmapsto \chi_g^k$$

where $\chi_g^k(n) = \chi_g(n)^k$. One can check that this map is one-to-one.

(Hint: check the values $\chi_g^k(g)$ for different $k$.)

On the other hand, for any $\chi \in X(p)$, $\chi(g)$ satisfies

$$\chi(g)^d - 1 = 0$$

for some $d \mid p-1$, by part (2).

Then $\chi(g) = e^{2\pi i j/d}$ for some $j$, but

$p-1 = dk$ for some $m$, so

$$\chi(g) = e^{2\pi i j/d} = e^{2\pi i jk/(p-1)}$$

$$= \left(e^{2\pi i/(p-1)}\right)^{jk}$$

$$= \chi_g^{jk}(g).$$

But since any $n \in (\mathbb{Z}/p\mathbb{Z})^\times$ is congruent to $g^{I(n)}$, it follows that

$$\chi(n) = \chi_g^{jk}(n).$$

That is, $\Phi$ is also surjective, hence a bijection. $\square$

**Def** The L-function of a character $\chi$ mod $b$ is the Dirichlet series

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

Since every character is multiplicative:

**Corollary** Every L-function has a product formula

$$L(\chi, s) = \prod_{p} \frac{1}{1 - \chi(p) p^{-s}}.$$

Next time: more on characters and their

L-functions.

L-functions.