Lecture 15.1

Last time:

- A **character mod b** is an arithmetic function $\chi : \mathbb{Z} \to \mathbb{C}$ satisfying:
  - $\chi(n) = \chi(n+b)$
  - $\chi(n) = 0 \iff \gcd(n,b) > 1$
  - χ is completely multiplicative.

- **Theorem** For any $b \geq 2$,
  (1) $\chi(1) = 1$ for any character χ.
  (2) For any character χ and any n with $\gcd(n,b) = 1$, $\chi(n)$ is a dth

root of unity for some $d \mid \phi(b)$,

i.e. $\chi(n)^d = 1$.

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

Pf of (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 $k = p$ 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

$$z^d - 1 = 0$$

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

Then χ_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 $\chi(g) = e^{2\pi ij/d}$ for some j, but $p-1 = dk$ for some m, so

$$\chi(g) = e^{2\pi ij/d} = e^{2\pi ijk/(p-1)}$$

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

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

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, Φ is also surjective, hence a bijection. $\square$

Def The **L-function** of a character χ 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

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

Returning to our arithmetic function

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

we know f is not completely multiplicative, so its Dirichlet series

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

$a \equiv a \pmod b$

does not have a product formula.

However, f <u>is</u> periodic with period b and

$f(n) = 0$ when $\gcd(n,b) > 1$.

Theorem Any arithmetic function f which is periodic with period b and satisfies $f(n) = 0$ when $\gcd(n,b) > 1$ can be expressed as a $\mathbb{C}$-linear combination of characters mod b:

$$f = m_0 \chi_0 + m_1 \chi_1 + \dots + m_r \chi_r, \quad m_j \in \mathbb{C}$$

(χ_0: trivial)

$$= \sum_{\chi \in X(b)} m_\chi \chi.$$

In particular, our $f = f_{a,b}$ is such a function, and its explicit decomposition as a sum of characters is a little easier to prove than the general case above.

Prop For any a relatively prime to b,

$$f_{a,b}(n) = \sum_{\chi \in X(b)} \frac{\chi(a)^{-1}}{\phi(b)} \chi(n).$$

Pf: Since characters are completely multiplicative,

$$\sum_{\chi \in X(b)} \frac{\chi(a)^{-1}}{\phi(b)} \chi(n) = \frac{1}{\phi(b)} \sum_{\chi \in X(b)} \chi(a^{-1}) \chi(n)$$

$$= \frac{1}{\phi(b)} \sum_{\chi \in X(b)} \chi(a^{-1}n).$$

$\chi \in X(b)$

Here, a^{-1} means the unique solution to

$$ax \equiv 1 \pmod{b}.$$

Claim: For any $a \in \mathbb{Z}$,

$$\sum_{\chi \in X(b)} \chi(a) = \begin{cases} \phi(b), & a \equiv 1 \pmod{b} \\ 0, & a \equiv 1 \pmod{b}. \end{cases}$$

If $\gcd(a,b) > 1$, each $\chi(a) = 0$ so the formula holds in that case.

If $a \equiv 1 \pmod{b}$, by periodicity,

$$\sum_{\chi \in X(b)} \chi(a) = \sum_{\chi \in X(b)} \chi(1) = \sum_{\chi \in X(b)} 1 = \phi(b).$$

Otherwise $a \not\equiv 1 \pmod{b}$ and for some $\chi(1)$

Otherwise, $\psi \neq 1$ (that is) and for some $\psi \in X(b)$,

$\psi(a) \neq 1$. (i.e. ψ is not the trivial char.)

Then

$$\psi(a) \sum_{\chi} \chi(a) = \sum_{\chi} \psi(a)\chi(a)$$

$$= \sum_{\chi} (\psi\chi)(a)$$

$$= \sum_{\chi} \chi(a)$$

since every character in $X(b)$ can be written as $\psi\chi$ for some χ.

But this can be rewritten as

$$(\psi(a) - 1) \sum_{\chi \in X(b)} \chi(a) = 0$$

and since $\psi(a) \neq 1$, $\sum_{\chi \in X(b)} \chi(a) = 0$.

This finishes proving the claim.

Returning to the expression

$$\frac{1}{\phi(b)} \sum_{\chi \in X(b)} \chi(a^{-1}n)$$

the claim says this evaluates to

$$\begin{cases} \frac{1}{\phi(b)}\phi(b), & \text{if } a^{-1}n \equiv 1 \pmod{b} \\ 0, & \text{if } a^{-1}n \not\equiv 1 \pmod{b} \end{cases}$$

but $a^{-1}n \equiv 1 \pmod{b}$ is equivalent to

$n \equiv a \pmod{b}$, so this is just our

original arithmetic function $f_{a,b}(n)$. □

We'd like to relate $\sum_{p \equiv a \pmod b} \frac{1}{p^s}$ to the

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

$\chi \in X(b)$.

Consider the product of L-functions

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

Since each χ is completely multiplicative, each

L-function has a product formula:

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

Applying log, we get:

$$\log\left(\prod_{\chi} L(\chi,s)\right) = \sum_{\chi}\sum_{p} -\log\left(1-\chi(p)p^{-s}\right)$$

$$= \sum_{\chi}\sum_{p}\sum_{k=1}^{\infty} \frac{\chi(p)^k}{k} p^{-sk}$$

$$= \sum_{k=1}^{\infty}\sum_{\chi}\sum_{p} \frac{\chi(p)^k}{k} p^{-sk}$$

$$= \underbrace{\sum_{\chi}\sum_{p} \frac{\chi(p)}{p^s}}_{H(\chi,s)} + \underbrace{\sum_{k=2}^{\infty}\sum_{\chi}\sum_{p} \frac{\chi(p)^k}{k} p^{-sk}}_{G(s)}.$$

The $H(\chi,s)$ relate to our sum $\sum_{p\equiv a \pmod b} \frac{1}{p^s}$ as follows:

$$\sum_{p \equiv a \pmod b} \frac{1}{p^s} = \sum_p f_{a,b}(p)\, p^{-s}$$

$$= \sum_p \sum_\chi \frac{\chi(a)^{-1}}{\phi(b)} \chi(p)\, p^{-s}$$

$$= \frac{1}{\phi(b)} \sum_p \sum_\chi \chi(a)^{-1} \chi(p)\, p^{-s}$$

$$= \frac{1}{\phi(b)} \sum_\chi \chi(a)^{-1} \sum_p \chi(p)\, p^{-s}$$

$$= \frac{1}{\phi(b)} \sum_\chi \chi(a)^{-1} H(\chi, s).$$

Goal: Show $\prod_\chi L(\chi, s)$ diverges and $G(s)$ converges as $s \to 1^+$, which will imply $\sum_\chi H(\chi, s)$ diverges as $s \to 1^+$.

Next time: Analyzing $\log L(X, s)$.