Dirichlet Characters

Where we left off from Tuesday (Liang).

Want to show for $(a,b)=1$

\[ \sum_{\chi \in \chi(a,b)} \frac{1}{p^s} \sim \frac{1}{\phi(b)} \log \frac{1}{s-1} \quad \text{as } s \to 1. \]

Goal today is to show \( \exists \) a func. \( \Psi(n) = \begin{cases} 1 & \text{if } n \equiv a(b) \\ 0 & \text{else.} \end{cases} \)

Then could write LHS of the above as \( \sum \frac{\Psi(p)}{p^s} \), and hope this is easier to deal with.

In order to do this or construct \( \Psi \), we need to seemingly shift gears and construct functions from \( \mathbb{Z} \) to \( \mathbb{C}^* \) which has the properties. For \( \chi : \mathbb{Z} \to \mathbb{C}^* \)

1. \( \exists \, N \in \mathbb{N} \), s.t. \( \chi(x+N) = \chi(x) \) (periodic in \( N \))
2. \( \chi(1) = 1 \) then \( \chi(x) = 0 \) if \( (x,N) = 1 \) then \( \chi(x) \neq 1 \). (Non-zero on relatively prime \( \#s \))
3. \( \chi(mn) = \chi(m) \chi(n) \) for any \( m,n \in \mathbb{Z} \).
Can prove \( \chi(1) = 1 \) from these properties, likewise if \( a \equiv b \pmod{\phi(N)} \)

then \( \chi(a) = \chi(b) \).

Euler's Theorem: If \( (a, N) = 1 \) then \( a^{\phi(N)} \equiv 1 \pmod{N} \).

**Proof:**

So \( \chi(a^{\phi(N)}) = \chi(1 + k\phi(N)) = \chi(1) \), but also \( \chi(a^{\phi(N)}) = \chi(a)^{\phi(N)} \).

So \( \chi(a) = 1 \), or \( \chi(a) \) is a \( \phi(N) \)th root of unity.

Do these exist? Yes, but need a new object.

**Definition:**

Set \( (a, N) = 1 \) then \( g \) modulo \( N \) is called a primitive root modulo \( N \) if \( \exists \ k \in \mathbb{Z} \) s.t. \( a \equiv g^k \pmod{N} \).

In other words, given any element \( a \) modulo \( N \), you can "get to it" by a sufficient power of your primitive root \( g \).

As \( \phi(N) \) is the \( \phi(N) \)th root of unity, \( g^k \equiv 1 \pmod{N} \), \( g \) is a primitive root if \( \nexists \ k \) with \( k < \phi(N) \) s.t. \( g^k \equiv 1 \pmod{N} \).

**Example:**

\( N = 5 \), \( g = 2 \), then \( g^2 = 4, g^3 = 3, g^4 = 1 \).

\( g = 3 \), then \( g^2 = 4, 2^3 = 2, 1 \).

\( \exists k \) in interval \( 0 \leq k < \phi(n) - 1 \) s.t. \( a \equiv g^k \pmod{N} \), we label it \( k = \text{ind}_g a \) and call it the index of \( a \) to base \( g \mod N \).
Remark: The index of a relative to \( g \) should immediately remind you of the logarithm and its relationship with exponentiation.

Then let \( g \) be a primitive root mod \( N \). If \( (a, N) = (b, N) = 1 \) then

1. \( \text{Ind}_g(ab) \equiv \text{Ind}_g(a) + \text{Ind}_g(b) \pmod{\phi(N)} \)
2. \( \text{Ind}_g(a^N) \equiv N \cdot \text{Ind}_g(a) \pmod{\phi(N)} \)
3. If \( g' \) is another primitive root then \( \text{Ind}_g = \text{Ind}_{g'} \).

Pt. HW

So for a given \( N \) do primitive roots exist? Not always.

Thus for \( N = 1, 2, 4, p^x \), or \( 2p^x \), where \( p \) is an odd prime and \( x \geq 1 \), \( \exists \) a primitive root.

Pt. Will not show. Perhaps if time show for \( p^x \), \( x \geq 1 \).

Construction of \( \chi \)

If \( p \) odd

Let \( g \) be a primitive root of \( p^x \), \( x \geq 1 \). Set \( b(n) = \text{Ind}_g n \pmod{\phi(p^x)} \)

so \( n \equiv g(b(n)) (p^x) \). For \( h = 0, 1, \ldots, \phi(p^x) - 1 \), define

\[
\chi_h(n) = \begin{cases} 
\frac{2\pi i h b(n)}{\phi(p^x)} & \text{if } (n, p^x) = 1 \\
0 & \text{else}
\end{cases}
\]
Note \( \chi_h(n) = e^{2\pi i h(n)} = 1 \) as well \( \chi_h(n+k^\alpha) \).

\[
\chi_h(n) = \chi_h(n+k^\alpha) = \chi_h(n) \quad \text{as} \quad n+k^\alpha \equiv s \pmod{p^\alpha} \implies n \equiv s \pmod{p^\alpha}.
\]

Also, \( \chi_{nm} = \chi_h(n)\chi_h(m) \).

As there are \( \phi(p) \) h's, there are \( \phi(p^\alpha) \) distinct Dirichlet characters \( \chi \pmod{p^\alpha} \). This construction works also for moduli \( 2^\alpha \) if \( \alpha = 1 \) or \( \alpha = 2 \) with \( q=3 \) (check HWW). However, \( \not\exists \) no primitive root for \( 2^\alpha \), \( \alpha \geq 3 \)

and one constructs Dirichlet characters mod \( 2^\alpha \) by a different method.

Now if \( N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \) and if \( \chi_i \) is a Dirichlet character mod \( p_i^{\alpha_i} \), then \( \chi = \chi_1 \chi_2 \ldots \chi_r \) is a Dirichlet character mod \( N \).

How many \( \alpha \) are there in this construction, there are \( \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\ldots\phi(p_r^{\alpha_r}) \) of them.

Then \( \phi(c,b) = \phi(a)\phi(b) = \phi(ab) \).

If HWW (Give steps toward proof)

by Then \( \phi(p_1^{\alpha_1})\ldots\phi(p_r^{\alpha_r}) = \phi(N) \), with some group theory

one can show this is all of the Dirichlet characters modulo \( N \).

Why do we care about Dirichlet characters?
Easy to check if $\chi \cdot \psi$ are Dirichlet character mod $N$. Then $\chi \cdot \psi$ is also. (Check HW). Take $x \in \mathbb{Z}$ s.t. $x \not\equiv 1 (N)$.

Consider $\sum \chi(x)$. If we multiply it by $\psi(x)$ with $\psi(x) \neq 1$, $\chi(x)$

then $\psi(x) \cdot \sum \chi(x) = \sum \psi(x) \chi(x)$. Can check by def'n of Dirichlet character that $\psi$ acting by multiplication on $\{\chi_1, \ldots, \chi_{\phi(N)}\}$ permutes the set of $\phi(N)$, so $\sum (\psi \cdot \chi)(x) = \sum \chi(x)$. Then $(1 - \psi(x)) \sum \chi(x) = 0$, $\chi(x)$

so $\sum \chi(x) = 0$. If $x \not\equiv 1 (N)$ then by def'n $\sum \chi(x) = \sum \chi(1(N)) = \Phi(N)$.

We have then $\frac{1}{\psi} \sum \chi(x) = \left\{ \begin{array}{ll} 1, & x \equiv 1 (N) \\ 0, & \text{else} \end{array} \right.$

Back to our original problem with $(a,b) = 1$.

$$\sum \frac{1}{\rho s} = \sum \frac{1}{\rho s} \quad \text{where} \quad \sum_{\rho \in \mathbb{Z} / \mathbb{Z}} \rho \not\equiv 1 (b),$$

Using Dirichlet characters

$$\sum_{\rho \in \mathbb{Z} / \mathbb{Z}} \frac{1}{\varphi(b)} \sum_{\chi(c)} \chi(p \rho) = \frac{1}{\varphi(b)} \sum_{\rho \in \mathbb{Z} / \mathbb{Z}} \chi(p \rho),$$

is our $\tau$ we desired to construct! What have we gained from this?
Can write as

\[
\frac{1}{\phi(b)} \sum_{\pi(b)} \frac{\pi(p)}{p^s},
\]

Similar to Tuesday adding \( \frac{\log \zeta(s)}{s} \) to \( \sum_{\pi(b)} \frac{\pi(p)}{p^s} \), and ask

\[
\sum_{\text{prime}} \frac{1}{p^s}
\]

we define

\[
L(s, x) := \sum_{\pi(b)} \frac{\pi(p)}{p^s},
\]

what are its analytic properties and relate \( \log L(s, x) \sim \sum_{\pi(b)} \frac{\pi(p)}{p^s} \), for any \( \pi(N) \).
Homework Problems

1. Define the function \( \mu \) as follows: \( \mu(1) = 1 \); \( \mu(n) = (-1)^r \) if \( n = p_1^a_1 \cdots p_r^a_r \) and \( q = a_1 = \cdots = a_r = 1 \); \( \mu(n) = 0 \) otherwise.

2. Show \( \sum \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = 1 \) if \( n = 1 \); \( 0 \) if \( n > 1 \). Here \( \lfloor x \rfloor \) is the floor function.

3. Use this to prove \( \left( \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \right) \cdot \zeta(s) = 1 \), for \( \Re(s) > 1 \).

4. What does this say about the Euler product of \( \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \)?

2. Prove if \( n \neq 1 \) then \( \phi(n) = \sum_{d|n} \mu(d) \frac{n}{d} \).

   Hint: Write \( \phi(n) = \sum_{j=1}^{n} \left\lfloor \frac{n}{\gcd(n,j)} \right\rfloor \), where \( \gcd(n,j) \) is GCD of \( n \) and \( j \).

3. Prove for \( n \neq 1 \) \( \phi(n) = n \prod_{p|n} \left( 1 - \frac{1}{p} \right) \).

   Hint: Expand the product into a sum and use (2).

4. Conclude from (3) that if \( (m,n) = 1 \) then \( \phi(mn) = \phi(m) \phi(n) \).

   Remark: There are other (possibly easier) proofs of this using the Chinese Remainder Theorem.