Dirichlet Characters

Where we left off from Tuesday (Liang).

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

$$\sum_{p \equiv a(b)} \frac{1}{p^s} \sim \frac{1}{\phi(b)} \log \frac{1}{s-1} \text{ as } s \to 1.$$

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

Then could write LHS of the above as $\sum_{p \text{ prime}} \mathbb{1}(p) \frac{1}{p^s}$, and hope this is easier to deal with.

In order to do this or construct $\mathbb{1}$, 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. If $(x,N) > 1$ 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 $a\equiv b(N)$ ②

then $\chi(a)=\chi(b)$. ~~[illegible]~~ Need a theorem to get a crucial property of χ.

Euler's Theorem ~~[illegible]~~ If $(a,N)=1$ then $a^{\phi(N)}\equiv 1\,(N)$.

Pf HW.

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

so $\chi(a)^{\phi(N)}=1$, or $\chi(a)$ is a $\phi(N)$-th root of unity.

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

Def'n Let $(a,N)=1$, then g modulo N is called a primitive root modulo N if $\exists\ k\in\mathbb{N}$ s.t. $a\equiv g^k(N)$.

In other words, given any element ~~[illegible]~~ a modulo N, you can "get to it" by a sufficient power of our primitive root g. ~~[illegible]~~ As $g^{\phi(N)}\equiv 1\,(N)$, $\forall\, g\,(\mathrm{mod}\,N)$, g is a primitive root if $\nexists\, k$ with $k<\phi(N)$ s.t. $g^k\equiv 1\,(N)$.

Example $N=5$, $g=2$, then $g^2=4$, $g^3=3$, $g^4=1$

$g=3$, then $g^2=4$, $g^3=2$, 1.

$\exists!\ k$ in interval $0\le k<\phi(m)-1$ s.t. $a\equiv g^k(N)$. We label it $k=\mathrm{ind}_g a$ and call it the index of a to base $g\,(\mathrm{mod}\,N)$.

Remark: The index of a relative to g should immediately remind you of the logarithm and its relationship with exponential.

Thm: Let g be a primitive root mod N. If $(a,N)=(b,N)=1$ then

① $\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g(a) + \operatorname{ind}_g(b) \pmod{\phi(N)}$

② $\operatorname{ind}_g(a^N) \equiv N \operatorname{ind}_g(a) \pmod{\phi(N)}$

③ If g' is another primitive root then $\operatorname{ind}_g a \equiv \operatorname{ind}_{g'} a \cdot \operatorname{ind}_g g' \pmod{\phi(N)}$

Pf. HW

So for a general N do primitive roots exists? Not always.

Thm: For $N = 1, 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime and $\alpha \geq 1$, $\exists$ a primitive root.

Pf: Will not show. Perhaps if time show for p^α, $\alpha \geq 1$.

Construction of χ.

Let g be a primitive root of $\overset{p \text{ odd}}{p^\alpha}$, $\alpha \geq 1$. Let $b(n) := \operatorname{ind}_g n \pmod{p^\alpha}$

So $n \equiv g^{b(n)} \ (p^\alpha)$. For $h = 0, 1, \ldots, \phi(p^\alpha)-1$, define

$$\chi_h(n) := \begin{cases} e^{\frac{2\pi i h b(n)}{\phi(p^\alpha)}} & \text{if } (n, p^\alpha) = 1 \\ 0 & \text{else} \end{cases}$$

Note $\chi_h(n)^{\phi(p^\alpha)} = e^{2\pi i h b(n)} = 1$. As well $\chi_h(n+kp^\alpha)$

$= \chi_h(n)$ as $n+kp^\alpha \equiv g^j (p^\alpha) \Rightarrow n \equiv g^j (p^\alpha)$. Also, for $(nm, p^\alpha) = 1$

$$\chi_h(nm) = e^{\frac{2\pi i h\, b(nm)}{\phi(p^\alpha)}} = e^{\frac{2\pi i h(b(n)+b(m))}{\phi(p^\alpha)}} = \chi_h(n)\chi_h(m).$$

As there are $\phi(p^\alpha)$ h's, there are $\phi(p^\alpha)$ distinct Dirichlet characters $\chi (\bmod p^\alpha)$. This construction works also for modulus 2^α if $\alpha=1$ or $\alpha=2$ with $g=3$, (check, HW). However, $\nexists$ no primitive root for 2^α, $\alpha \geq 3$ and one constructs Dirichlet characters mod 2^α by another method.

Now if $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ and if χ_i is a Dirichlet character mod $p_i^{\alpha_i}$ then $\chi = \chi_1 \cdot \chi_2 \cdots \chi_r$ is a Dirichlet character mod N.

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

<u>Thm</u> If $(a,b)=1$ $\phi(a)\phi(b) = \phi(ab)$.

<u>Pf</u>. HW (Give steps toward proof)

by Thm $\phi(p_1^{\alpha_1})\cdots\phi(p_r^{\alpha_r}) = \phi(N)$. With some group theory one can show this is <u>all</u> of the Dirichlet characters modulo N.

Why do we care about Dirichlet characters?

Easy to check if χ, ψ are Dirichlet character mod N (5)

then $\chi \cdot \psi$ is also. (Check, HW). Take $x \in \mathbb{Z}$ s.t. $x \not\equiv 1\,(N)$.

Consider $\sum_{\chi(N)} \chi(x)$. If we multiply it by $\psi(x)$ with $\psi(x) \neq 1$,

then $\psi(x) \sum_{\chi(N)} \chi(x) = \sum_{\chi(N)} \underbrace{\psi(x)\chi(x)}_{=(\psi\cdot\chi)(x)}$. Can check by def'n of Dirichlet

character that ψ acting by multiplication on $\{\chi_1, \ldots \chi_{\phi(N)}\}$ permutes the set, (HW). So $\sum_{\chi(N)} (\psi\cdot\chi)(x) = \sum_{\chi(N)} \chi(x)$. Then $(1-\psi(x)) \sum_{\chi(N)} \chi(x) = 0$,

so $\sum_{\chi(N)} \chi(x) = 0$. If $x \equiv 1\,(N)$ then by def'n $\sum \chi(x) = \sum \chi(1) = \phi(N)$.

We have then $\frac{1}{\phi(N)} \sum_{\chi(N)} \chi(x) = \begin{cases} 1 & \text{if } x \equiv 1\,(N) \\ 0 & \text{else} \end{cases}$.

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

$$\sum_{p \equiv a(b)} \frac{1}{p^s} = \sum_{p\bar{a} \equiv 1(b)} \frac{1}{p^s}$$ where $\bar{a} \in \mathbb{Z}$ s.t. $a\bar{a} \equiv 1\,(b)$, unique modulo b.

Using Dirichlet characters $\sum_{p \text{ prime}} \left[\frac{1}{\phi(b)} \sum_{\chi(b)} \chi(p\bar{a})\right] \frac{1}{p^s}$, so $\Pi(p) = \frac{1}{\phi(b)} \sum_{\chi(b)} \chi(p\bar{a})$

is our fcn we desired to construct! What have we gained from this?

Can write as

$$\frac{1}{\phi(b)} \sum_{\chi} \chi(\bar{a}) \sum_{p \text{ prime}} \frac{\chi(p)}{p^s}.$$

Similar to Tuesday where we related $\log \zeta(s)$ to $\sum_{p \text{ prime}} \frac{1}{p^s}$ we define $L(s,\chi) := \sum \frac{\chi(n)}{n^s}$, and ask what are its analytic properties and relate $\log L(s,\chi) \sim \sum_{p} \frac{\chi(p)}{p^s}$, for any $\chi(N)$.

Homework Problems

① Define the function μ as follows: $\mu(1)=1$;

If $n>1$, write $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Then $\mu(n) = (-1)^r$ if $\alpha_1 = \alpha_2 = \cdots = \alpha_r = 1$,

$\mu(n) = 0$ otherwise.

ⓐ Show $\displaystyle\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1. \end{cases}$ Here $[x]$ is the floor function.

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

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

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

Hint: Write $\displaystyle\phi(n) = \sum_{j=1}^{n} \left[\frac{1}{(n,j)}\right]$, where (n,j) is GCD of n & j.

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

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

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

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