Math 680 Fall 2017

Primes in an Arithmetic Progression

In order to prove Dirichlet's theorem on primes in an arithmetic progression, we need to look at characters and L-series.

Definition : Fix a modulus $m > 1$. A *Dirichlet character* modulo m is a totally multiplicative function χ that satisfies the two properties:

i) $\chi(a) = \chi(b)$ whenever $a \equiv b \mod m$,

ii) $\chi(a) \neq 0$ if and only if a is relatively prime to m.

Such a character naturally associates to a unique function on the group $\left(\mathbb{Z}/m\mathbb{Z}\right)^{\times}$, and vice-versa.

Example 1: For any modulus m, the *principal character* χ_0 is

$$\chi_0(a) = \begin{cases} 1 & \text{if } a \text{ is relatively prime to } m, \\ 0 & \text{otherwise.} \end{cases}$$

Example 2: For $m = 3$, set

$$\chi_1(a) = \begin{cases} 1 & \text{if } a \equiv 1 \mod 3, \\ -1 & \text{if } a \equiv 2 \mod 3, \\ 0 & \text{if } a \equiv 3 \mod 3. \end{cases}$$

Example 3: The above example is actually a particular case of a more generic situation. Set m to be a prime p. Choose a $(p-1)^{\text{th}}$ root of unity ξ and a primitive root (modulo p) r. In other words, as an element of $(\mathbb{Z}/p\mathbb{Z})^{\times}$, r generates the entire cyclic group. We then have the character

$$\chi(a) = \begin{cases} \xi^n & \text{if } a \equiv r^n \mod p \text{ for some } n, \\ 0 & \text{if } a \equiv 0 \mod p. \end{cases}$$

Given a Dirichlet character χ, we get the L-series

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

This is a Dirichlet series with an Euler product by a previous Proposition/exercise:

$$L(s, \chi) = \prod_{p \text{ prime}} \left(1 - \chi(p) p^{-s}\right)^{-1}.$$

We need to determine some elementary properties of these L-series.

For the principal character, we have

$$
\begin{aligned}
L(s,\chi_0) &= \prod_{p \text{ prime}} \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} \\
&= \prod_{\substack{p \text{ prime} \\ p \nmid m}} \left(1 - \frac{1}{p^s}\right)^{-1} \\
&= \frac{\prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}}{\prod_{\substack{p \text{ prime} \\ p \mid m}} \left(1 - \frac{1}{p^s}\right)^{-1}} \\
&= \zeta(s) \prod_{\substack{p \text{ prime} \\ p \mid m}} (1 - p^{-s}).
\end{aligned} \tag{1}
$$

Since the product on the right is finite, we clearly see that $L(s,\chi_0)$ has the same abscissa of convergence as the zeta function. Further, it has a simple pole at $s = 1$.

For other characters, we will need a bit more background.

Definition : A *character* on a finite abelian group G is a group homomorphism $\chi\colon G \to \mathbb{C}^\times$. The set of all characters on G itself forms a group under point-wise multiplication; this group is called the *dual* of G and is denoted $G^\perp$.

Note that Dirichlet characters are essentially group characters on $(\mathbb{Z}/m\mathbb{Z})^\times$. Also, the image of such a character must lie on the unit circle.

Proposition 1: For any finite abelian group G we have $G \cong G^\perp$. Further,

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\sum_{\chi \in G^\perp} \chi(g) = \begin{cases} |G| & \text{if } g = e, \\ 0 & \text{otherwise.} \end{cases}$$

Proof: Suppose first that G is cyclic with generator g. Then any character χ is completely determined by $\chi(g)$. Since the order of the image must divide the order of the group, $\chi(g)$ must be an m^{th} root of unity, where m is the order of g. Any such root of unity is possible here, and we thus see that $\chi(g) = \exp(k2\pi i/m)$ for some $k = 1, \ldots, m$. This shows that $G^\perp \cong (\mathbb{Z}/m\mathbb{Z}) \cong G$.

In general, G is isomorphic to a direct product of cyclic groups: $G \cong G_1 \times G_2 \times \cdots \times G_l$. One easily verifies that $G^\perp \cong G_1^\perp \times G_2^\perp \times \cdots \times G_l^\perp$ since any $\chi \in G^\perp$ is uniquely determined by its image on the generators of the various cyclic subgroups G_i. Therefore the general case follows from the cyclic case.

We obviously have $\sum_{g \in G} \chi_0(g) = |G|$, so suppose $\chi \neq \chi_0$. Choose an $h \in G$ such that $\chi(h) \neq 1$. Then as g runs through all elements of G, so does hg and thus

$$\begin{aligned}\sum_{g\in G}\chi(g) &= \sum_{g\in G}\chi(hg)\\ &= \sum_{g\in G}\chi(h)\chi(g)\\ &= \chi(h)\sum_{g\in G}\chi(g).\end{aligned}$$

Since we are assuming that $\chi(h) \neq 1$, we must have $\sum_{g\in G}\chi(g) = 0$.

The same argument works for the dual sums. We clearly have $\sum_{\chi\in G^\perp}\chi(e) = |G^\perp| = |G|$, so suppose that $g \neq e$. Choose a $\chi_1 \in G^\perp$ with $\chi_1(g) \neq 1$. This is possible since otherwise the dual of the cyclic subgroup generated by g is trivial, contradicting what we have already shown and the assumption that $g \neq e$. As χ runs through all elements of $G^\perp$, so does $\chi_1\chi$ and thus

$$\begin{aligned}\sum_{\chi\in G^\perp}\chi(g) &= \sum_{\chi\in G^\perp}\chi_1(g)\chi(g)\\ &= \chi_1(g)\sum_{\chi\in G^\perp}\chi(g).\end{aligned}$$

Since $\chi_1(g) \neq 1$, we must have $\sum_{\chi\in G^\perp}\chi(g) = 0$.

Applying this proposition to the case where $G = (\mathbb{Z}/m\mathbb{Z})^\times$, we see that for Dirichlet characters modulo m

$$\begin{aligned}\sum_{\substack{1\le n\le m\\ \gcd(n,m)=1}}\chi(n) &= \begin{cases}\phi(m) & \text{if } \chi=\chi_0,\\ 0 & \text{otherwise,}\end{cases}\\ \sum_{\chi}\chi(n) &= \begin{cases}\phi(m) & \text{if } n\equiv 1 \mod m,\\ 0 & \text{otherwise.}\end{cases}\end{aligned} \tag{2}$$

(The second sum here is over all Dirichlet characters modulo m.)

Proposition 2: Suppose χ is a non-principal Dirichlet character modulo m. Then $L(s,\chi)$ has abscissa of convergence 0.

Proof: Set $A(x) = \sum_{n\le x}\chi(n)$. Since χ is non-principal, (2) implies that $|A(x)| \le \phi(m)$ always. By Theorem 2 from the Dirichlet Series handout, this implies that $\sigma_c \le 0$. On the other hand, we clearly see from (2) that $\sum_{n\ge 1}\chi(n)$ diverges, so that $\sigma_c \ge 0$.

Theorem 1: Suppose $m > 1$ and for all non-principal Dirichlet characters χ modulo m we have $L(1,\chi) \neq 0$. Then for all integers a relatively prime to m we have

$$\sum_{\substack{n\ge 1\\ n\equiv a \mod m}}\frac{\Lambda(n)}{n^\sigma} \to \infty$$

as $\sigma \to 1^+$. In particular, there are infinitely many primes $p \equiv a \mod m$.

Proof: Fix an integer b such that $ab \equiv 1 \mod m$. Then for any Dirichlet character χ modulo m we have $\chi(a)\chi(b) = \chi(ab) = \chi(1) = 1 = \chi_0(a)$. Now by (2)

$$\frac{1}{\phi(m)} \sum_{\chi} \chi(b)\chi(n) = \begin{cases} 1 & \text{if } bn \equiv 1 \mod m, \\ 0 & \text{otherwise,} \end{cases} = \begin{cases} 1 & \text{if } n \equiv a \mod m, \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

Here the sum is over all Dirichlet characters modulo m.

Arguing exactly as in the proof of the Euler product for the zeta function, we have

$$\frac{L'(s,\chi)}{L(s,\chi)} = -\sum_{n\geq 1} \frac{\Lambda(n)\chi(n)}{n^s},$$

which is valid if $\Re(s) > 1$. Using this together with (3) yields

$$\begin{aligned} \sum_{\chi} \frac{L'(s,\chi)}{L(s,\chi)}\chi(b) &= -\sum_{\chi} \chi(b) \sum_{n\geq 1} \frac{\Lambda(n)\chi(n)}{n^s} \\ &= -\sum_{n\geq 1} \frac{\Lambda(n)}{n^s} \sum_{\chi} \chi(b)\chi(n) \\ &= -\phi(m) \sum_{\substack{n\geq 1 \\ n\equiv a \mod m}} \frac{\Lambda(n)}{n^s}. \end{aligned} \tag{4}$$

Now by (1), $L'(s,\chi_0)/L(s,\chi_0)$ has a simple pole at $s=1$ and $-L'(\sigma,\chi_0)/L(\sigma,\chi_0) \to \infty$ as $\sigma \to 1^+$. On the other hand, by Proposition 2 and the hypothesis that $L(1,\chi) \neq 0$ for all non-principal characters χ, we see that $L'(1,\chi)/L(1,\chi)$ exists for all non-principal characters. Since $\chi_0(b) = 1$, all of this together with (4) proves the first part of the theorem.

Finally, we note that

$$\begin{aligned} \sum_{\substack{n=p^k \\ p \text{ prime} \\ k>1}} \frac{\Lambda(n)}{n} &= \sum_{p \text{ prime}} \log p \sum_{k>1} \frac{1}{p^k} \\ &= \sum_{p \text{ prime}} \frac{\log p}{p(p-1)} \\ &< \sum_{n>1} \frac{\log n}{n(n-1)} \\ &< \infty. \end{aligned}$$

This together with the first part of the theorem shows that

$$\sum_{\substack{p \text{ prime} \\ p\equiv a \mod m}} \frac{\Lambda(p)}{p^\sigma} \to \infty$$

as $\sigma \to 1^+$. In particular, there are infinitely many primes $p \equiv a \mod m$.

Theorem 2: Suppose $m > 1$ and χ is a non-principal Dirichlet character modulo m. Then $L(1,\chi) \neq 0$.

Proof: Consider the product over all Dirichlet L-series modulo m:

$$P(s) := \prod_{\chi} L(s,\chi) = \prod_{\chi} \prod_{p \text{ prime}} \left(1 - \chi(p)p^{-s}\right)^{-1}.$$

This product converges when $\Re(s) > 1$, certainly. Assuming $\Re(s) > 1$, we have by (2)

$$\begin{aligned}
\log P(s) &= -\sum_{\chi} \sum_{p \text{ prime}} \log\left(1 - \chi(p)p^{-s}\right) \\
&= \sum_{\chi} \sum_{p \text{ prime}} \sum_{k \geq 1} \frac{\chi(p)^k}{p^{sk}k} \\
&= \sum_{p \text{ prime}} \sum_{k \geq 1} \frac{1}{p^{sk}k} \sum_{\chi} \chi(p^k) \\
&= \sum_{p \text{ prime}} \sum_{\substack{k \geq 1 \\ p^k \equiv 1 \mod m}} \frac{\phi(m)}{p^{sk}k}.
\end{aligned}$$

Set

$$a(n) := \begin{cases} \frac{\phi(m)}{k} & \text{if } n = p^k \equiv 1 \mod m \text{ for some prime } p, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$D(s) := \log P(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$$

is a Dirichlet series with $\sigma_c \leq 1$ and $a_n \geq 0$ for all n. We need a positive lower bound for the abscissa of convergence.

Suppose p is a prime that doesn't divide m. Then by Euler's extension of Fermat's "little" theorem, $p^{\phi(m)} \equiv 1 \mod m$. Now just using the $k = \phi(m)$ term we have

$$\begin{aligned}
D(\sigma) = \sum_{n \geq 1} \frac{a_n}{n^\sigma} &= \sum_{k \geq 1} \sum_{\substack{p \text{ prime} \\ p^k \equiv 1 \mod m}} \frac{\phi(m)}{p^{\sigma k}k} \\
&> \sum_{\substack{p \text{ prime} \\ p \nmid m}} \frac{1}{p^{\sigma\phi(m)}} \\
&= \sum_{p \text{ prime}} \frac{1}{p^{\sigma\phi(m)}} - \sum_{\substack{p \text{ prime} \\ p \mid m}} \frac{1}{p^{\sigma\phi(m)}}.
\end{aligned}$$

The second sum on the right is finite and depends only on m and σ. However, we've seen that $\sum_p \frac{\log p}{p}$ diverges. In particular, $D\big(1/2\phi(m)\big)$ diverges so that $\sigma_c \geq 1/2\phi(m) > 0$. (In fact, using Chebyshev's inequalities we see that $\sum_p \frac{1}{p}$ diverges and that $\sigma_c \geq 1/\phi(m)$. But that is of no consequence here; we simply need to demonstrate that the abscissa of convergence is strictly positive.)

We may write

$$P(s) = 1 + \frac{D(s)}{1!} + \frac{D(s)^2}{2!} + \cdots + \frac{D(s)^n}{n!} + \cdots$$

As above, $D(s)$ may be expressed as a Dirichlet series with absissa of convergence $\sigma_c \geq 1/2\phi(m)$ *and* all of the coefficients are non-negative. Thus any convergence along the real axis is absolute convergence. This implies that each $D(s)^n/n!$ may be expressed as a Dirichlet series with non-negative coefficients and the same abscissa of convergence. And now the same argument applies to $P(s)$ via the infinite series representation above. We therefore may conclude by Landau's Theorem that $P(s)$ is *not* analytic on the right half-plane $\{s = \sigma + it \colon \sigma > 0\}$.

To complete the proof, suppose by contradiction that some $L(1, \chi_1) = 0$. By (1), $L(s, \chi_0)$ is analytic on the right half-plane except for a simple pole at $s = 1$. Since all other L-series here are analytic on the entire right half-plane by Proposition 2, our simple pole at $s = 1$ from $L(s, \chi_0)$ is canceled out by the zero from the factor $L(1, \chi_1)$ in $P(s)$, implying that the product $P(s)$ of our L-series is analytic on the entire right half-plane.