FINITE FOURIER ANALYSIS AND DIRICHLET'S THEOREM

KATHERINE MONSON

Abstract. This is an expository paper on finite Fourier analysis and basic number theory. The focus of the paper is finite Abelian groups and the properties of these groups which are used in the proof of the Dirichlet prime number theorem. We then introduce the specific elements and basic structure of the proof of Dirichlet's theorem.

Contents

1. Introduction

In this paper we will introduce and prove the primary elements in the proof of Dirichlet's theorem of prime numbers. Dirichlet's theorem asserts that for any pair of relatively prime numbers $\ell > m \in \mathbb{Z}$, meaning that the greatest common divisor of ℓ and m is 1, there are infinitely many primes of the form $\ell x + m$. This theorem is based on the work of Euler, Reimann, Fourier, and, of course, Dirichlet himself.

There are many components to Dirichlet's proof that appear through the study of number theory as it relates to prime numbers, Abelian groups and their analysis by Fourier, as well as an analysis of logarithms in the complex plane. This paper will primarily focus on the aspects relating to Abelian groups and their characteristics, with an explanation of how they are used in the components of Dirichlet's final proof.

We assume that the reader knows the definition of an Abelian group and homomorphisms.

The exposition of this paper closely follows the exposition of Stein's introduction to Fourier analysis [1] and Nathonson's Elementary Methods in Number Theory [2], and both offer alternate or more complete proofs of many in this paper.

Date: AUGUST 29, 2015.

2. Preliminary Number Theory

The most important concept in number theory which pertains to Dirichlet's theorem is the infinitude of prime numbers. This theorem is very elegant by Euclid's proof.

Theorem 2.1. *There are infinitely many primes.*

Proof. Suppose for contradiction that there are n prime numbers $p_1, p_2, \ldots, p_n$. Let

$$P = 1 + \prod_{i \leq n} p_i.$$

Then, since $P > p_i$ for all i, P cannot be prime, and thus there exists p_j such that P is divisible by p_j. However, since p_j divides $\prod_{i<n} p_i$, but p_j does not divide 1, as no prime divides 1, then p_j does not divide P. Therefore, since all integers can be uniquely factored by a product of primes, P must be prime. Therefore, there are infinitely many primes. □

What is more interesting than this proof is that not only are there infinitely many primes, but there are infinitely many primes of the form $4x+3$ where $x \in \mathbb{N}$, and furthermore that there are infinitely many primes of the form $4x+1$, which then extends to all relatively prime numbers by Dirichlet's theorem.

One of the foundational elements of Dirichlet's theorem is that it is an extension of Euler's version of the proof of infinite primes, a more difficult approach than Euclid's, but also more illuminating. First, we will introduce Euler's zeta function,

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}, \tag{2.2}$$

and Euler's product formula for the zeta function,

Theorem 2.3. *For all $x \in \mathbb{C}$ with the real part of x is greater than 1,*

$$\zeta(x) = \prod_{p} \left(1 - \frac{1}{p^x}\right)^{-1}$$

This theorem is previously well proven in Elias Stein's book on Fourier Analysis [1], in his introduction to this theorem. Additionally, this text proves the following lemma on the properties of logarithms.

Lemma 2.4. *The exponential and logarithm functions satisfy the following properties:*

(1) $log(1+x) = x + O(x^2)$
(2) If $log(1+x) = y$ and $|x| < \frac{1}{2}$, then $|y| \leq 2|x|$.

With these properties, the following theorem comes about.

Theorem 2.5. *The series*

$$\sum_{p} \frac{1}{p},$$

a sum over all primes, diverges.

Proof. Let $f : \mathbb{N} \longrightarrow \mathbb{Q}$. First we show that the log of a product of f can be written as the sum of logs of f. If the product is finite, this follows from the definition of logarithms. If the product is infinite, then there are two cases.

(1) The product converges.
Let $\lim_{N\longrightarrow\infty}\prod_{n=1}^{N} f(n) = M$. Then

$$\lim_{N\longrightarrow\infty}\log\prod_{n=1}^{N} f(n) = \log(M).$$

Then for all $\epsilon > 0$, there exists $N \in \mathbb{Z}$ such that

$$|\log(M) - \log\prod_{n=1}^{N} f(n)| < \epsilon.$$

Then, since $\log\prod_{n=1}^{N} f(n) = \sum_{n=1}^{N}\log(f(n))$,

$$|\log(M) - \sum_{n=1}^{N}\log(f(n))| < \epsilon.$$

Therefore,

$$\lim_{N\longrightarrow\infty}\sum_{n=1}^{N}\log(f(n)) = \log(M),$$

and thus $\log\prod_{n=1}^{\infty} f(n) = \sum_{n=1}^{\infty}\log(f(n))$.

(2) The product diverges.
Since the definition of convergence for an infinite product is that an infinite product converges if and only if the sum of logs converges, then the sum of logs must diverge if the product diverges, and thus the log of the products is infinite as is the sum of logs, and the two are therefore equivalent.

Then, by taking the logarithm of both sides of Euler's product and using the logarithm equations from lemma 2.4, for $s > 1$, this conclusion holds for $f(n) = \left(1-\frac{1}{p^s}\right)^{-1}$ as follows

$$\log\zeta(s) = \log\prod_{p}\left(1-\frac{1}{p^s}\right)^{-1}$$

$$= \sum_{p}\log\left(1-\frac{1}{p^s}\right)^{-1} = \sum_{p} -\log\left(1-\frac{1}{p^s}\right) = -\sum_{p}\log\left(1-\frac{1}{p^s}\right)$$

$$= -\sum_{p} -\frac{1}{p^s} + O(\frac{1}{p^{2s}}).$$

Then, since all primes $p \in \mathbb{N}$, $\sum_p \frac{1}{p^{2s}} \leq \sum_{n\in\mathbb{N}}\frac{1}{n^{2s}} = O(1)$,

$$\log\zeta(s) = \sum_{p}\frac{1}{p^s} + O(1).$$

Then, since $\sum_{n=1}^{\infty}\frac{1}{n^s} \geq \sum_{n=1}^{M}\frac{1}{n^s}$ for all $M \in \mathbb{Z}$, then $\lim_{s\longrightarrow 1^+}\sum_{n=1}^{\infty}\frac{1}{n^s} \geq \sum_{n=1}^{M}\frac{1}{n}$ for all $M \in \mathbb{Z}$, and therefore $\zeta(s)$ diverges as $s \longrightarrow 1^+$ since similarly $\lim_{s\longrightarrow 1^+}\sum_p\frac{1}{p^s} \geq \sum_{p<M}\frac{1}{p}$ for all $M \in \mathbb{Z}$.

Therefore, $\log\zeta(s) - O(1) \longrightarrow \infty$ as $s \longrightarrow 1^+$, and thus $\sum_p\frac{1}{p^s} \longrightarrow \infty$ as $s \longrightarrow 1^+$. Therefore,

$$\sum_{p}\frac{1}{p} = \infty.$$

□

This theorem then proves by contradiction that there are infinitely many primes, as a finite series must converge. This is the approach then taken by Dirichlet in proving his theorem. First, we must look at Abelian groups and their properties.

3. Basic Properties of Abelian Groups

An example of an infinite Abelian group is $\mathbb{Z}$ with the additive operation. An example of a finite Abelian group, which will be used later on, is $\mathbb{Z}/n\mathbb{Z}$, which is defined as

$$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}^+, a < n\}$$

where $n\mathbb{Z} = \{x \mid \exists z \in \mathbb{Z} \colon x = nz\}$. Thus, $b \in \mathbb{Z}/n\mathbb{Z}$ implies that b is of the form $a + n\mathbb{Z}$. Addition on $\mathbb{Z}/n\mathbb{Z}$ is defined as , with addition defined for all $a, b \in \mathbb{Z}/n\mathbb{Z}$ as

$$a + b = c \pmod{n}.$$

The multiplicative group, $(\mathbb{Z}/n\mathbb{Z})^\times$, is defined as

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{b \in \mathbb{Z}/n\mathbb{Z} \mid \exists b^{-1} \in \mathbb{Z}/n\mathbb{Z} \colon bn^{-1} = 1 + n\mathbb{Z}\}.$$

Now we will define characters of Abelian groups, which are functions with very specific qualities.

Definition 3.1. A character of a finite Abelian group G is a group homomorphism $e \colon G \to \mathbb{C}^\times$, where $\mathbb{C}^\times$ is the group of nonzero complex numbers under multiplication. Characters have the property

$$e(m \cdot n) = e(m)e(n)$$

with $\cdot$ being the operation on G.

Definition 3.2. $\hat{G}$, known as the dual group of G, is the set of the characters of G.

As an example, let $G = \mathbb{Z}/n\mathbb{Z}$. Then, we define $e_l \colon G \longrightarrow \mathbb{C}^\times$ for all $0 \leq l < n$ to map to the nth roots of unity, defined as

$$e_l(a) = e^{2\pi i l a/n} \text{ for all } a \in \mathbb{Z}/n\mathbb{Z}.$$

Then clearly, since the operation on G is addition modulo n,

$$e_l(a + b) = e^{2\pi i l(a+b)/n} = e^{2\pi i l a/n} \cdot e^{2\pi i l b/n} = e_l(a)e_l(b),$$

and thus the characters e_l satisfy the properties of characters of finite Abelian groups.

Definition 3.3. The principal, or trivial, character of a group, denoted e_0, is the character such that

$$\text{For all } a \in G,\ e_0(a) = 1.$$

Lemma 3.4. *Let G be a group. Then the dual group $\hat{G}$ is a finite Abelian group of homomorphisms $e\colon G \longrightarrow A$, where A is a finite Abelian group, such that for $e, f \in \hat{G}$.*

$$(e \cdot f)(a) = e(a)f(a)$$

for all $a \in G$, with the trivial homomorphism e_0 that maps all elements of G to the identity element of A, and with

$$e^{-1}(a) = (e(a))^{-1}$$

This lemma follows directly as the properties of associativity, commutativity, identity and inverses are inherited from the same properties in A.

Additionally, for $e \in \hat{G}$, we define $\overline{e}$ as

$$\overline{e}(a) = \overline{e(a)}$$

for all $a \in G$.

Now we will demonstrate that these characters additionally form an orthonormal basis for complex functions on G. We begin by seeing that only trivial characters or the same $a \in G$ can sum to anything other than 0 over all $a \in G$ and all characters, respectively.

Theorem 3.5 (Orthogonality Relations)**.** *Let G be a finite Abelian group of order n. There are four orthogonality relations.*

(1) Let $e \in \hat{G}$. Then,

$$\sum_{a \in G} e(a) = \begin{cases} n & \text{if } e = e_0, \\ 0 & \text{if } e \neq e_0. \end{cases}$$

(2) Let $a \in G$. Then,

$$\sum_{e \in \hat{G}} e(a) = \begin{cases} n & \text{if } a = 0, \\ 0 & \text{if } a \neq 0. \end{cases}$$

(3) Let $e, f \in \hat{G}$. Then,

$$\sum_{a \in G} e(a)\overline{f}(a) = \begin{cases} n & \text{if } e = f, \\ 0 & \text{if } e \neq f. \end{cases}$$

(4) Let $a, b \in G$. Then,

$$\sum_{e \in \hat{G}} e(a)\overline{e}(b) = \begin{cases} n & \text{if } a = b, \\ 0 & \text{if } a \neq b. \end{cases}$$

Proof. (1) Since $e_0(a) = 1$ for all $a \in G$, and since $|G| = n$,

$$\sum_{a \in G} e_0(a) = n \cdot 1 = n.$$

Let $e \in \hat{G}$ such that $e \neq e_0$. Then there exists $b \in G$ such that $e(b) \neq 1$. Then,

$$e(b) \sum_{a \in G} e(a) = \sum_{a \in G} e(b)e(a) = \sum_{a \in G} e(a \cdot b).$$

Since G is closed under the $\cdot$ operation, $a \cdot b \in G$, and therefore $a \cdot b = c$ where $c \in G$, and thus,

$$\sum_{a \in G} e(a \cdot b) = \sum_{a \in G} e(a).$$

Therefore,

$$e(b) \sum_{a \in G} e(a) = \sum_{a \in G} e(a),$$

and since $e(b) \neq 0$, then $\sum_{a \in G} e(a) = 0$.

(2) Since $e(0) = 1$ for all $e \in \hat{G}$, then since $|\hat{G}| = n$,

$$\sum_{e \in \hat{G}} e(0) = n.$$

Let $a \in G$ such that $a \neq 0$. Then there exists $f \in \hat{G}$ such that $f(a) \neq 1$, since there can only be one identity character. Then,

$$e'(a) \sum_{e \in \hat{G}} e(a) = \sum_{e \in \hat{G}} e'(a)e(a) = \sum_{e \in \hat{G}} (f \cdot e)(a).$$

Since $\hat{G}$ is closed under multiplications, $f \cdot e \in \hat{G}$, and therefore,

$$\sum_{e \in \hat{G}} (f \cdot e)(a) = \sum_{e \in \hat{G}} e(a).$$

Thus,

$$f(a) \sum_{e \in \hat{G}} e(a) = \sum_{e \in \hat{G}} e(a),$$

and since $f(a) \neq 1$, then $\sum_{e \in \hat{G}} e(a) = 0$.

(3) Since by the definition of $\mathbb{C}^\times$, $|e(a)| = 1$ for all $a \in G$, since $\mathbb{C}^\times$ is the unit circle in the complex plane, then

$$e(a)\overline{e}(a) = e(a)\overline{e(a)} = |e(a)|^2 = 1^2 = 1 = e_0(a).$$

Therefore, $\overline{e}(a) = e^{-1}(a)$. Let $e \in \hat{G}$. Then,

$$\sum_{a \in G} e(a)\overline{e}(a) = \sum_{a \in G} e_0(a) = n.$$

Let $e, f \in \hat{G}$ such that $f \neq e$. Then $\overline{f} \neq \overline{e}$, and therefore $e \cdot \overline{f} = h$, where $h \neq e_0$. Then by relation (1),

$$\sum_{a \in G} e(a)\overline{e'}(a) = \sum_{a \in G} e''(a) = 0.$$

(4) Let $a, b \in G$. Then, since $\overline{e}(b) = e^{-1}(b) = e(-b)$, then for all $e \in \hat{G}$,

$$e(a)\overline{e}(b) = e(a)e(-b) = e(a - b).$$

Therefore, if $a = b$,

$$\sum_{e \in \hat{G}} e(a)\overline{e}(b) = \sum_{e \in \hat{G}} e(0) = n.$$

If $a \neq b$, then $a - b = c$ such that $c \in G$ and $c \neq 0$. Therefore,

$$\sum_{e \in \hat{G}} e(a)\overline{e}(b) = \sum_{e \in \hat{G}} e(c) = 0.$$

□

4. Fourier Transform and Series for Abelian Groups

Now we define the Fourier transform and series of complex functions on finite Abelian groups. For a complex function f on a finite Abelian group G of order n, the Fourier coefficient of f with respect to a character $e \in \hat{G}$ is defined as

$$\hat{f}(e) = \frac{1}{n} \sum_{a \in G} f(a)\overline{e}(a).$$

The Fourier series of f is defined as

$$\mathcal{F}[f] = \sum_{e \in \hat{G}} \hat{f}(e)e.$$

Now we will prove that the Fourier series is equal to the function itself. This is known as Fourier inversion, as the function f is defined by its Fourier coefficients, which are themselves defined by f.

Theorem 4.1 (Fourier inversion)**.** *Let G be a finite Abelian group of order n. Let f be a complex function on G. Then,*

$$f = \mathcal{F}[f] = \sum_{e \in \hat{G}} \hat{f}(e)e.$$

Proof. Let $a \in G$. Then, by the definition of the Fourier coefficient of f,

$$\sum_{e \in \hat{G}} \hat{f}(e)e(a) = \sum_{e \in \hat{G}} (\frac{1}{n} \sum_{b \in G} f(b)\overline{e}(b))e(a)$$

$$= \sum_{e \in \hat{G}} \sum_{b \in G} f(b) \left(\frac{1}{n} e(a)\overline{e}(b) \right) = \sum_{b \in G} f(b) \left(\frac{1}{n} \sum_{e \in \hat{G}} e(a)\overline{e}(b) \right).$$

Then, by the orthogonality relations, $\sum_{e \in \hat{G}} e(a)\overline{e}(b) = n$ when $a = b$, and otherwise $\sum_{e \in \hat{G}} e(a)\overline{e}(b) = 0$. Therefore,

$$\sum_{b \in G, b \neq a} f(b) \left(\frac{1}{n} \sum_{e \in \hat{G}} e(a)\overline{e}(b) \right) = 0,$$

and

$$f(a) \left(\frac{1}{n} \sum_{e \in \hat{G}} e(a)\overline{e}(b) \right) = f(a)\frac{1}{n}n = f(a).$$

Therefore,

$$\sum_{e \in \hat{G}} \hat{f}(e)e(a) = \sum_{b \in G} f(b) \left(\frac{1}{n} \sum_{e \in \hat{G}} e(a)\overline{e}(b) \right)$$

$$= \sum_{b \in G, b \neq a} f(b) \left(\frac{1}{n} \sum_{e \in \hat{G}} e(a)\overline{e}(b) \right) + f(a) \left(\frac{1}{n} \sum_{e \in \hat{G}} e(a)\overline{e}(b) \right) = f(a).$$

Therefore,

$$f = \sum_{e \in \hat{G}} \hat{f}(e)e.$$

□

This concludes the necessary elements of finite Fourier analysis for Dirichlet's theorem. We will now apply these definitions and theorems to a specific set of characters and group to focus on prime numbers.

5. Dirichlet Characters and L-Functions

First we are reminded of the group $(\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group of the ring of integers modulo n. Let us define this group as G. We then define the extension for $e \in \hat{G}$, for all $m \in \mathbb{Z}$,

$$\chi(m) = \begin{cases} e(m) & \text{if } m \text{ and } n \text{ are relatively prime,} \\ 0 & \text{if } gcd(m,n) > 1. \end{cases} \tag{5.1}$$

χ is called a Dirichlet character modulo n. This character has the same properties as all other characters of finite Abelian groups, since it is effectively an extension of existing characters. As a standard notation, e is not specified in the character as it is implicitly understood.

Definition 5.2. The principal Dirichlet character χ_0, is defined such that

$$\text{For all } a \in \mathbb{Z} \quad \chi_0(a) = 1.$$

Note that this is the Dirichlet character where e is the trivial character.

Definition 5.3. The Euler φ-function $\varphi(n)$ is the order of the set $N = \{m \mid m \in \mathbb{Z}\setminus\{0\}, m < n, gcd(m,n) = 1\}$. In other words, $\varphi(n)$ defines the number of integers less than n which are relatively prime with n.

For example,

$$\begin{aligned} \varphi(6) &= 2 \quad N = \{1,5\} \\ \varphi(7) &= 6 \quad N = \{1,2,3,4,5,6\} \\ \varphi(8) &= 4 \quad N = \{1,3,5,7\} \end{aligned}$$

Recall that as a character, $\chi(0) = 1$ and $\chi(a+b) = \chi(a)\chi(b)$.

Theorem 5.4. *The Dirichlet characters modulo n are completely multiplicative, meaning that for all Dirichlet characters χ,*

$$\chi(1) = 1 \text{ and } \chi(ab) = \chi(a)\chi(b).$$

Additionally, the following orthogonality relations are true. Let $\sum_{a(mod n)}$ be the sum over all possible remainders of an integer modulo n. Let $\sum_{\chi(mod n)}$ be the sum over all Dirichlet characters modulo n.

(1) Let χ be a Dirichlet character modulo n. Then,

$$\sum_{a(mod\ n)} \chi(a) = \begin{cases} \varphi(n) & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

(2) Let $a \in \mathbb{Z}$. Then,

$$\sum_{\chi(mod\ n)} \chi(a) = \begin{cases} \varphi(n) & \text{if } a \equiv 1 \pmod m \\ 0 & \text{if } a \not\equiv 1 \pmod m. \end{cases}$$

(3) Let χ, χ' be Dirichlet characters modulo n. Then,

$$\sum_{a(mod\ n)} \chi(a)\overline{\chi'}(a) = \begin{cases} \varphi(n) & \text{if } \chi = \chi', \\ 0 & \text{if } \chi \neq \chi'. \end{cases}$$

(4) Let $a, b \in \mathbb{Z}$. Then,

$$\sum_{\chi(mod\ n)} \chi(a)\overline{\chi}(b) = \begin{cases} \varphi(n) & \text{if } gcd(a,n) = gcd(b,m) = 1 \text{ and } a \equiv b \pmod m \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Proving that χ is completely multiplicative is relatively straightforward. $(\mathbb{Z}/n\mathbb{Z})^\times$ is equipped with a multiplicative operation, and 1 is relatively prime to all $n \in \mathbb{Z}$. Then, let χ be the Dirichlet character modulo n for $e \in \hat{G}$. Then

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

Let $a, b \in \mathbb{Z}$ and let χ be a Dirichlet character modulo n. If both a and b are relatively prime to n, then ab is also relatively prime to n. Therefore,

$$\chi(ab) = e(ab) = e(a)e(b) = \chi(a)\chi(b).$$

If a is not relatively prime to n and b is relatively prime to n, then ab is not relatively prime to n. Therefore,

$$\chi(ab) = 0 = 0 \cdot e(b) = \chi(a)\chi(b),$$

and similarly if b is not relatively prime to n and a is relatively prime to n.

If a and b are both not relatively prime to n, then ab is not relatively prime to n, and thus,

$$\chi(ab) = 0 = 0 \cdot 0 = \chi(a)\chi(b).$$

Therefore, χ is completely multiplicative.

Since there are $\varphi(n)$ such $a \pmod n$ such that $\chi_0(a) = 1$, then the first orthogonality relation follows from that for characters of finite Abelian groups (Theorem 2.7).

Similarly, since there are $\varphi(n)$ Dirichlet characters modulo n, and $\chi(a) = 1$ for all χ if and only if $a \equiv 1 \pmod n$, because $(\mathbb{Z}/n\mathbb{Z})^\times$ is a finite Abelian group under multiplication. Thus the second relation follows from that for characters of finite Abelian groups (Theorem 2.7).

The third and fourth relations follow from the first two as they do for characters of finite Abelian groups (Theorem 2.7). □

We now define Dirichlet's L-function as

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \tag{5.5}$$

where $s > 1$ and χ is a Dirichlet character. This function is fundamental in the proof of Dirichlet's theorem.

6. Extension to Dirichlet's Theorem

The following theorems are the tools used in proving Dirichlet's theorem. I will merely sketch them, as they require a greater understanding of logarithms. Both Stein [1] and Nathanson's [2] sections on Dirichlet's theorem prove these theorems thoroughly and explain the intermediate proofs in greater detail.

Theorem 6.1. *Let $s > 1$. Then,*

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

where the product is taken over all primes.

Furthermore, $L(s,\chi) \neq 0$ and

$$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + O(1),$$

with the sum taken over all primes p.

The proof of the product uses the fact that $\left|\frac{\chi(n)}{n^s}\right| \leq \frac{1}{n^{\Re(s)}}$ and the infinite sum of $\frac{1}{n^{\Re(s)}}$ converges, and then using the Fundamental Theorem of Arithmetic one shows that the L function therefore converges to the desired product (see Nathanson's proof [2]).

Then, using the properties of logarithms outlined in Lemma 2.4, and the fact that the log of an infinite product can be substituted by the sum of logs, then taking the log of both sides of the Euler product gives the second result.

Theorem 6.2. *Let χ_0 be the principle Dirichlet character modulo m. Then,*

$$logL(s,\chi_0) = log\left(\frac{1}{s-1}\right) + O(1).$$

First, by taking the log of the Euler product of the zeta function one shows that

$$\log \zeta(r) = \log\left(\frac{1}{r-1}\right) + O(1).$$

Furthermore, one proves that

$$L(s,\chi_0) = \zeta(s) \prod_{p\|m} \left(1 - \frac{1}{p^s}\right),$$

and thus, since $\log \prod_{p\|m}\left(1-\frac{1}{p^s}\right) = \sum_{p\|m} \log\left(1-\frac{1}{p^s}\right)$ and $\sum_p \frac{1}{p^s}$ diverges, then $\log \prod_{p\|m}\left(1-\frac{1}{p^s}\right) = O(1)$, and thus,

$$\log L(r,\chi_0) = \log\zeta(r) + \log \prod_{p\|m}\left(1-\frac{1}{p^s}\right) = \log\left(\frac{1}{r-1}\right) + O(1),$$

since $O(1) + O(1) = O(1)$.

The most crucial, and the most difficult, portion of this proof is the following property of Dirichlet's L functions.

Theorem 6.3. *$L(1,\chi) \neq 0$ for all nonprincipal χ*

This proof takes many different forms and can be approached in many ways, and both Stein [1] and Nathanson [2] are clearer and more concise than can be fairly replicated.

With these properties and theorems, Dirichlet's theorem can be proven.

Theorem 6.4 (Dirichlet's Theorem)**.** *For all relatively prime integers ℓ, m such that $\ell > m$, there exist infinitely many primes p such that*

$$p = \ell x + m.$$

In other words, there are infinitely many primes of the form $p \equiv m \pmod{l}$.

Proof. Let $1 < s < 2$. Then we will examine the following sum,

$$\sum_{\chi \pmod{\ell}} logL(s,\chi)\overline{\chi}(m),$$

where the sum is over Dirichlet characters modulo ℓ. Then, this sum can be split into two parts, $\chi = \chi_0$ and $\chi \neq \chi_0$,

$$logL(s,\chi_0)\overline{\chi_0}(m) + \sum_{\chi \neq \chi_0} logL(s,\chi)\overline{\chi}(m).$$

First we will examine the sum as a whole. Remembering from Theorem 3.6 that

$$log(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + O(1),$$

then,

$$\begin{aligned}\sum_{\chi \pmod{\ell}} logL(s,\chi)\overline{\chi}(m) &= \sum_{\chi \pmod{\ell}} \overline{\chi}(m) \sum_p \frac{\chi(p)}{p^s} + O(1) \\ &= \sum_{\chi \pmod{\ell}} \sum_p \frac{\overline{\chi}(m)\chi(p)}{p^s} + O(1) \\ &= \sum_{\chi \pmod{\ell}} \sum_p \overline{\chi}(m)\chi(p)\frac{1}{p^s} + O(1).\end{aligned}$$

Then, by the orthogonality relations on Dirichlet characters (Theorem 5.4), we know that

$$\sum_{\chi \pmod{\ell}} \overline{\chi}(m)\chi(p) \neq 0$$

only if $p \equiv m \pmod{\ell}$. Therefore, we can reduce the previous sum to

$$\sum_{\chi \pmod{\ell}} \sum_{p \equiv m \pmod{\ell}} \overline{\chi}(m)\chi(p)\frac{1}{p^s} + O(1).$$

Then, by the same orthogonality relation, $\sum_{\chi \pmod{\ell}} \overline{\chi}(m)\chi(p) = \varphi(m)$, and therefore,

$$\sum_{\chi \pmod{\ell}} logL(s,\chi)\overline{\chi}(m) = \varphi(m) \sum_{p \equiv m \pmod{\ell}} \frac{1}{p^s} + O(1).$$

Next, we look at $logL(s,\chi_0)\overline{\chi_0}(m)$, and, as noted above we know that

$$logL(s,\chi_0)\overline{\chi_0}(m) = \left(log\left(\frac{1}{s-1}\right) + O(1)\right)\overline{\chi_0}(m) = log\left(\frac{1}{s-1}\right) + O(1).$$

Then, since we know that for all Dirichlet characters $\chi \neq \chi_0$, $L(1,\chi) \neq 0$, then, as $s \longrightarrow 1^+$, $logL(s,\chi)$ remains bounded. Therefore, $logL(s,\chi) = O(1)$ for $1 \leq s \leq 2$, and therefore for $1 < s < 2$, and thus

$$\sum_{\chi \neq \chi_0} logL(s,\chi)\overline{\chi}(m) = O(1),$$

since $\sum_{\chi\neq\chi_0} \overline{\chi}(m)$ is a constant.

Therefore,

$$\sum_{\chi \pmod{\ell}} logL(s,\chi)\overline{\chi}(m) = logL(s,\chi_0)\overline{\chi_0}(m) + \sum_{\chi\neq\chi_0} logL(s,\chi)\overline{\chi}(m)$$

$$\varphi(m) \sum_{p\equiv m \pmod{\ell}} \frac{1}{p^s} + O(1) = log\left(\frac{1}{s-1}\right) + O(1) + O(1)$$

$$\sum_{p\equiv m \pmod{\ell}} \frac{1}{p^s} = \frac{1}{\varphi(m)} log\left(\frac{1}{s-1}\right) + O(1).$$

Thus, since $\lim_{s\longrightarrow 1^+} log\left(\frac{1}{s-1}\right) = \infty$,

$$\lim_{s\longrightarrow 1^+} \sum_{p\equiv m \pmod{\ell}} \frac{1}{p^s} = \infty,$$

and therefore there are infinite primes p of the form $p \equiv m \pmod{\ell}$. □

Acknowledgments. It is a pleasure to thank my mentors, Gong Chen and Holly Mandel, for their guidance in finding this topic and approaching it in an interesting and effective way. I would also like to thank Peter May for organizing the REU program at the University of Chicago, and Laszlo Babai for teaching the apprentice program and encouraging me to participate and work hard every day of class.

References

[1] Stein, Elias M., and Rami Shakarchi. Fourier Analysis: An Introduction. Princeton: Princeton University Press, 2003.

[2] Nathanson, Melvyn B. (Melvyn Bernard). Elementary Methods in Number Theory. New York: Springer, 2000.