ANALYTIC NUMBER THEORY AND DIRICHLET'S THEOREM

JOHN BINDER

Abstract. In this paper, we prove Dirichlet's theorem that, given any pair h, k with $(h, k) = 1$, there are infinitely many prime numbers congruent to $h \pmod{k}$. Although this theorem lies strictly within the realm of number theory, its proof employs a range of tools from other branches of mathematics, most notably characters from group theory and holomorphic functions from complex analysis.

Contents

1. Arithmetic Functions

Analytic number theory is best described as the study of number theory through the use of functions, whose properties can be examined using analytic techniques. The most basic tool of analytic number theory is the arithmetic function.

Definition 1.1. A function $f : \mathbb{N} \to \mathbb{C}$ is called an arithmetic function.

Example 1.2. Any function $f : \mathbb{C} \to \mathbb{C}$ defines an arithmetic function when its domain is restricted to the natural numbers.

Examples 1.3. The following arithmetic functions are central to the study of number theory:

Date: August 22, 2008.

1). The divisor function $d(n)$, which counts the number of divisors of a natural number n.

2). The divisor sum function $\sigma(n)$, which takes the sum of the factors of a natural number n.

3). Euler's totient function $\phi(n)$, which counts the numbers $k < n$ such that $(n, k) = 1$.

4). Von Mangoldt's function $\Lambda(n)$, where

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^m \text{ for some prime } p, \\ 0 & \text{otherwise} \end{cases} \tag{1.4}$$

A subset of arithmetic functions is especially useful to number theorists. These are the multiplicative functions.

Definition 1.5. An arithmetic function f is called a multiplicative function if, for all m, n with $(m, n) = 1$, we have $f(mn) = f(m)f(n)$. Moreover, f is called completely multiplicative if $f(mn) = f(m)f(n)$ for all integers m and n.

Example 1.6. The function $f(n) = n^\alpha$ is completely multiplicative for any α.

Examples 1.7. The functions $d(n)$, $\sigma(n)$, and $\phi(n)$ are all multiplicative, but not completely multiplicative.

2. Dirichlet Products and Mobius Inversion

Definition 2.1. Let f and g be arithmetic functions. We define the Dirichlet product of f and g by

$$(f \star g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right) \tag{2.2}$$

It should be noted that, though the Dirichlet product uses the same symbol that typically signifies a convolution, the Dirchlet product is not a convolution in the strict sense since 'convolution' requires a group action, and the natural numbers do not form a group under multiplication.

However, as seen in the following theorem, the Dirichlet product is itself a group operation on a subset of arithmetic functions, as seen below:

Theorem 2.3. *Let S be the set of arithmetic functions f such that $f(1) \neq 0$. Then $(S, \star)$ forms an abelian group.*

Proof. Since $f \star g(1) = f(1)\, g(1)$, then S is closed under Dirichlet multiplication. Furthermore, simple algebraic manipulation shows $\star$ to be both commutative and associative.

Let

$$e(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise} \end{cases} \tag{2.4}$$

It is clear that $e \star f = f$ for all arithmetic functions f, so that e is the identity element. Finally, we must show that, given $f \in S$, there exists an $f^{-1} \in S$ such that $f \star f^{-1} = e$. Given f, we will construct f^{-1} inductively. First, we need $f \star f^{-1}(1) = e(1)$, which occurs if and only if $f(1)\, f^{-1}(1) = 1$. Since $f(1) \neq$

0, $f^{-1}(1)$ is uniquely determined. Now, assume that $n > 1$ and f^{-1} has been determined for all $k < n$. Then we have

$$f \star f^{-1}(n) = \sum_{d|n} f(d) f^{-1}\left(\frac{n}{d}\right) \Rightarrow -f(1) f^{-1}(n) = \sum_{d|n,\ d>1} f(d) f^{-1}\left(\frac{n}{d}\right) \tag{2.5}$$

This uniquely determines $f^{-1}(n)$. Thus, we may uniquely determine an f^{-1} for all $f \in S$. □

One important application of Dirichlet multiplication involves recovering a function from a piecewise sum. For instance, given f, we wish to find a function g such that:

$$f(n) = \sum_{d|n} g(d) \tag{2.6}$$

We may solve this problem using Dirichlet multiplication. First, we write $f = g \star \mathbf{1}$, where $\mathbf{1}(n) = 1$ for all n. Then $\mathbf{1}$ has an inverse function; call it μ. We then have

$$g = g \star (\mathbf{1} \star \mu) = (g \star \mathbf{1}) \star \mu = f \star \mu$$

Given the importance of μ, we will construct it from the definition. We begin with a lemma.

Lemma 2.7. *Let f, g, $h \in S$, with $h = f \star g$. If both h and f are multiplicative, then so is g.*

Proof. We must show that, for all m, n, with $(m,n) = 1$, we have $g(mn) = g(m) g(n)$. We will show this by inducting upwards on the quantity mn. Since f is multiplicative, we have $f(1) = f(1 \cdot 1) = f(1)^2 \Rightarrow f(1) = 0$ or 1. Since f has an inverse, we must have $f(1) = 1$. Similarly, we have $h(1) = 1$. Therefore, $g(1) = 1$, so that $g(1 \cdot 1) = g(1) \cdot g(1)$. This proves the base case.

Now for our inductive step. Pick m, n so that $mn > 1$. By definition, we have

$$h(mn) = \sum_{d|mn} f(d) g\left(\frac{mn}{d}\right) \tag{2.8}$$

For all d, we may decompose d into $d_m \cdot d_n$, where $d_m | m$ and $d_n | n$. Moreover, since $(m,n) = 1$, this decomposition is unique. Therefore, we have

$$h(mn) = \sum_{d_m|m,\ d_n|n} f(d_m \cdot d_n) g\left(\frac{m}{d_m} \cdot \frac{n}{d_n}\right) \tag{2.9}$$

Since $(m,n) = 1$, then $(d_m, d_n) = \left(\frac{m}{d_m}, \frac{n}{d_n}\right) = 1$. Since f is multiplicative we have $f(d_m \cdot d_n) = f(d_m) \cdot f(d_n)$, and by our inductive hypothesis we have $g\left(\frac{m}{d_m} \cdot \frac{n}{d_n}\right) = g\left(\frac{m}{d_m}\right) g\left(\frac{n}{d_n}\right)$ so long as $d_m \cdot d_n < mn$. Therefore, we may write.

(2.10)

$$h(mn) = \left(\sum_{d_m|m,\ d_n|n} f(d_m) f(d_n) g\left(\frac{m}{d_m}\right) g\left(\frac{n}{d_n}\right)\right) - g(m) g(n) + g(mn)$$

$$= \left(\sum_{d_m|m} f(d_m)\, g\left(\frac{m}{d_m}\right) \right) \left(\sum_{d_n|n} f(d_n)\, g\left(\frac{n}{d_n}\right) \right) - g(m)\, g(n) + g(mn) \tag{2.11}$$

$$= h(m)\, h(n) - g(m)\, g(n) + g(mn) \tag{2.12}$$

Since h is multiplicative, we must have $g(m)\, g(n) = g(mn)$. This completes the inductive step and therefore the proof. □

Since e is multiplicative, we have the following corollary:

Corollary 2.13. *If f is multiplicative, then so is f^{-1}.*

Using lemma 2.7, we can construct μ, the Dirichlet inverse of $\mathbf{1}$.

Theorem 2.14. *Let*

$$\mu(n) = \begin{cases} 0 & \text{if } \exists k > 1 : k^2 | n, \\ (-1)^m & \text{if } n = p_1 \cdot p_2 \cdot \ldots \cdot p_m \end{cases} \tag{2.15}$$

Then $\mu = \mathbf{1}^{-1}$

Proof. Since $\mathbf{1}$ is multiplicative, then so too must be its inverse. Therefore, by determining $\mu(p^m)$ for each prime power p^m, we determine μ.

It is clear that we must have $\mu(1) = 1$. Consider $\mu(p)$, for p prime. Then

$$e(p) = 0 = \mathbf{1} \star \mu(p) = \mu(1) + \mu(p) \Rightarrow \mu(p) = -1 \tag{2.16}$$

Next, consider p^2. We have

$$0 = \mathbf{1} \star \mu\left(p^2\right) = \mu(1) + \mu(p) + \mu\left(p^2\right) = 1 + -1 + \mu\left(p^2\right) \Rightarrow \mu\left(p^2\right) = 0 \tag{2.17}$$

Finally, assume $\mu\left(p^k\right) = 0$ for all $2 \leq k \leq m-1$. Then we have

$$0 = \mathbf{1} \star \mu(p^m) = \mu(1) + \mu(p) + \mu\left(p^2\right) + \ldots + \mu\left(p^{m-1}\right) + \mu(p^m) \tag{2.18}$$

$$= 1 + -1 + 0 + \ldots + 0 + \mu(p^m) \Rightarrow \mu(p^m) = 0$$

This shows μ to be as stated in equation 2.15 for all prime powers. Because we know μ to be multiplicative, then 2.15 correctly states μ for all natural numbers. □

This function μ is called the Mobius function.

Remark 2.19. One should note that, even though $\mathbf{1}$ is completely multiplicative, its inverse μ is not. In general, the inverse of a completely multiplicative function is not completely multiplicative. If we examine the proof of lemma 2.7, we see that we cannot uniquely decompose a divisor d of mn into a divisor of m and a divisor of n unless m and n are relatively prime. Therefore, proof of lemma 2.7 fails when $(m, n) \neq 1$ at equation 2.11.

3. Dirichlet Characters

Recall the definition of a character on an abelian group.

Definition 3.1. Let G be a finite abelian group. We call $\tau : G \to \mathbb{C}$ a character on G if for all $g \in G$, $\tau(g) \neq 0$ and for all $g,\, h \in G$, we have $\tau\,(gh) = \tau\,(g)\,\tau\,(h)$.

Remark 3.2. For a finite abelian group G, $\tau\,[G] \subset \mathbb{T}$, since for each $g \in G$, there is an $m > 0$ such that $g^m = 1$.

Let τ be a character on the multiplicative group $(\mathbb{Z}/k\mathbb{Z})^*$. We may extend the domain of this character to the entire set of natural numbers in the following manner: first, let $\bar{h} \in \mathbb{Z}/k\mathbb{Z}$ be the equivalence class modulo k containing h. We extend the domain of τ to the entire set of natural numbers in the most obvious way possible: let

$$\chi(n) = \begin{cases} \tau(\bar{n}) & \text{if } (n,k) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Note that $\bar{n} \in (\mathbb{Z}/k\mathbb{Z})^*$ if and only if $(n,k) = 1$. Therefore, this function is well-defined.

We call χ a Dirichlet character modulo k. To formalize:

Definition 3.3. A function $\chi : \mathbb{N} \to \mathbb{C}$ is called a Dirichlet character modulo k if there exists a character τ on the group $(\mathbb{Z}/k\mathbb{Z})^*$ such that

$$\chi(n) = \begin{cases} \tau(\bar{n}) & \text{if } (n,k) = 1 \\ 0 & \text{otherwise} \end{cases}$$

It is easy to see that χ has two important properties: first, it is k-periodic (that is, $\chi(a+k) = \chi(a)$ for all a); and second, it is completely multiplicative (that is, $\chi(m \cdot n) = \chi(m)\chi(n)$ for all m and n).

The figures below show the Dirichlet characters modulo 5 and modulo 8. It is simple to check that no more exist, though we will prove this fact as a more general statement later.

$x \pmod 5$	0	1	2	3	4
χ_1	0	1	1	1	1
χ_2	0	1	-1	-1	1
χ_3	0	1	i	$-i$	-1
χ_4	0	1	$-i$	i	-1

$x \pmod 8$	0	1	2	3	4	5	6	7
χ_1	0	1	0	1	0	1	0	1
χ_2	0	1	0	-1	0	-1	0	1
χ_3	0	1	0	-1	0	1	0	-1
χ_4	0	1	0	1	0	-1	0	-1

Remark 3.4. In both of the above tables, we have defined χ_1 as the Dirichlet character modulo k that satisfies $\chi_1\,(h) = 1$ if $(h,k) = 1$ and 0 otherwise. This character is called the trivial (or principle) character modulo k. The trivial character is denoted by χ_1 solely from convention, though this specific character will play a special role later.

On the one hand, all Dirichlet characters are periodic, completely multiplicative per the definition. However, interestingly, all nontrivial functions that have both of these properties are Dirichlet characters:

Theorem 3.5. *If χ is an arithmetic function that is both periodic and completely multiplicative, and it is not universally* 0*, then it is a Dirichlet character.*

Proof. Let k be the minimal period of χ. Since χ is k-periodic, it is constant in each equivalence class modulo k. Moreover, since it is completely multiplicative, its values on $(\mathbb{Z}/k\mathbb{Z})^*$ make it a character. Therefore, we need to show that $\chi(n) = 0$ if and only if $(n, k) \neq 1$.

First, assume $(n, k) = 1$; then we have $n^{\phi(k)} \equiv 1 \pmod{k}$. Since χ is completely multiplicative and k-periodic, we have $\chi(n)^{\phi(k)} = \chi\left(n^{\phi(k)}\right) = \chi(1)$. Thus, if $\chi(n) = 0$, then $\chi(1) = 0$. However, if $\chi(1) = 0$, then we have $\chi(m) = \chi(1)\chi(m) = 0$ for all m. Hence, if $(n, k) = 1$ and $\chi(n) = 0$, then χ is universally 0.

On the other hand, assume there is an n such that $(n, k) > 1$ and $\chi(n) \neq 0$. Then there is at least one prime p such that $p|k$ and $\chi(p) \neq 0$. Consider this p, and let m be any natural number. Because χ is k-periodic and completely multiplicative, we have

$$\chi(m)\chi(p) = \chi(mp) = \chi(mp + k) = \chi(p)\chi\left(m + \frac{k}{p}\right)$$

Since $\chi(p) \neq 0$, we must have $\chi(m) = \chi(m + k/p)$ for all m. But this means that χ is $\frac{k}{p}$-periodic. This violates the stipulation that k is the minimal period of χ. $\square$

It should be remarked that the function $\mathbf{1}(n) = 1$ is technically a Dirichlet character modulo 1.

Proposition 3.6. *There are $\phi(k)$ Dirichlet characters modulo k.*

Proof. We prove a more general proposition: let G be an abelian group with $|G| = N$. Then there are N characters on G.

First, since G is finite and abelian, we may decompose it into the direct product of groups C_{a_i}, where C_{a_i} are cyclic groups of order a_i. Consider the cyclic group C_{a_i} with generator x_i. Then, since $x_i^{a_i} = 1$, we have $\tau(x_i)^{a_i} = 1$, this leaves a_i possibilities for $\tau(x_i)$, and each choice determines a character on C_{a_i}. Moreover, since x_i is a generator, the choice of $\tau(x_i)$ uniquely determines τ.

Consider the decomposition of G into cyclic groups; write $G = C_{a_1} \times \ldots \times C_{a_m}$. That is, there are elements $x_i \in G$ such that $x_i^{a_i} = 1$ and each $g \in G$ can be expressed uniquely as $\prod_i x_i^{t_i}$, with $0 \leq t_i < a_i$. Let τ_i be a character on the subgroup generated by x_i. Then it is clear that the function defined by $\tau(g) = \prod_i \tau_i(x_i^{t_i})$ is a character on G, and that $\prod_i \tau_i = \prod_i \tau_i'$ if and only if $\tau_i = \tau_i'$ for all i.

We must now show that each character on G can be expressed as a product of τ_i's. Let x_i be as above.. Then, given $g \in G$, we may express g uniquely as $g = \prod_i x_i^{t_i}$ with $0 \leq t_i < a_i$. Thus, for all $g \in G$, we have $\tau(g) = \prod_i \tau(x_i)^{p_i}$. Moreover, the restriction of τ to the subgroup generated by x_i is itself a character on that subgroup. Therefore, we may express any character τ on G as a product of characters τ_i, where τ_i is a character on the subgroup generated by x_i. But this subgroup is isomorphic to C_{a_i}, so there are a_i characters on that subgroup.

Hence, the number of characters on G is equal to $\prod_i a_i = |G|$. Since each Dirichlet character modulo k is uniquely determined by a character on $(\mathbb{Z}/k\mathbb{Z})^*$, the number of Dirichlet characters modulo k is $|(\mathbb{Z}/k\mathbb{Z})^*| = \phi(k)$. $\square$

Proposition 3.7. *The $\phi(k)$ Dirichlet characters modulo k form a group under multiplication.*

Proof. We see that the trivial character is the identity element of the group. If χ is a Dirichlet character, then its inverse is $\overline{\chi}$, the complex conjugate of χ. Moreover, the set of characters modulo k is closed under multiplication, since $(\chi \cdot \chi')(gh) = \chi(gh)\chi'(gh) = \chi(g)\chi(h)\chi'(g)\chi'(h) = (\chi \cdot \chi')(g)(\chi \cdot \chi')(h)$, $(\chi \cdot \chi')(n) = 0$ if and only if $(n, k) \neq 1$, and since the product of two k-periodic functions is itself k-periodic. $\square$

4. Orthogonality Relations of Characters

In this section, we will prove the following identity, which will be useful in our proof of Dirichlet's theorem.

Theorem 4.1. *Let $\chi_1, \ldots, \chi_{\phi(k)}$ be the Dirichlet characters modulo k. Then we have*

$$\sum_{i=1}^{\phi(k)} \overline{\chi_i(h)}\chi_i(p) = \begin{cases} \phi(k) & \text{if } h \equiv p \pmod{k} \text{ and } (h,k) = 1, \\ 0 & \text{otherwise} \end{cases} \tag{4.2}$$

We will prove this theorem in general, for any Abelian group. Since a Dirichlet character is simply an extension of a character on $(\mathbb{Z}/k\mathbb{Z})^*$, the theorem will follow.

Lemma 4.3. *Let G be an abelian group, where $|G| = N$, and let $\tau_1, \ldots, \tau_N$ be the characters on G. Then we have*

$$\sum_{g \in G} \tau(g) = \begin{cases} N & \text{if } \tau(g) = 1 \text{ for all } g, \\ 0 & \text{otherwise} \end{cases}$$

Proof. Obviously, the sum of the trivial character on this group is the size of the group, N.

Otherwise, assume χ is not the trivial character, and pick b such that $\tau(b) \neq 1$. Moverover, the group G is invariant under multiplication by any of its elements. We therefore have

$$\sum_{g \in G} \tau(g) = \sum_{g} \tau(b \cdot g) = \sum_{g} \tau(b) \cdot \tau(g) = \tau(b) \sum_{g} \tau(g) \tag{4.4}$$

Since $\tau(b) \neq 1$, we must have $\sum \tau(g) = 0$. $\square$

From here, we have another lemma:

Lemma 4.5. *Let A be the $N \times N$ matrix $[\tau_i(g_j)]_{i,j \leq N}$ and let A^* denote the conjugate transpose of of A. Then we have $AA^* = NI$.*

Proof. Consider the i, j coordinate of AA^*. If v_i denotes the vector of row i in A, then this quantity is equal to $v_i \cdot \overline{v_j} = \sum_g \tau_i(g) \cdot \overline{\tau_j(g)}$. But $\tau_i \overline{\tau_j}$ is itself a character, and is the trivial character if and only if $i = j$. Therefore, we have $(AA^*)_{ij} = N$ if $i = j$ and 0 otherwise; that is, $AA^* = NI$. $\square$

From here, we prove the generalization of theorem 4.1.

Proposition 4.6. *Given g_i, $g_j \in G$ and $\tau_1, \ldots, \tau_N$ the characters on G, we have*

$$\sum_{l=1}^{N} \overline{\tau_l(g_i)} \cdot \tau_l(g_j) = \begin{cases} N & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

Proof. Since $AA^* = NI$, we have $A^*A = NI$; this implies $(A^*A)_{ij} = N$ if $i = j$ and 0 otherwise. Moreover, we can examine this quantity via matrix multiplication. Let w_i signify a column vector of A; then we have

$$(A^*A)_{ij} = \overline{w_i} \cdot w_j = \sum_{l=1}^{N} \overline{\tau_l(g_i)} \cdot \tau_l(g_j)$$

.

Given what we know about A^*A, this proves the proposition. □

Theorem 4.1 follows as an immediate corollary, since χ is an extension of a character on $(\mathbb{Z}/k\mathbb{Z})^*$ and vanishes on those n not relatively prime to k.

5. An Analytic Proof of the Infinitude of Primes

Almost two and a half millennia ago, Euclid gave the first, and most standard, proof of the infinitude of primes. The argument is simple enough: assume there are finitely many; multiply them all together and add one; the new quantity is not divisible by any prime in the list; contradiction.

This argument, however, cannot be generalized to prove that there are infinitely many primes congruent to $h \pmod{k}$, because numbers from one equivalence class may have divisors from a different class. Therefore, a different type of argument is necessary to prove Dirichlet's theorem on primes in arithmetic progressions.

We will summarize an analytic proof of the infinitude of primes due to Euler; this proof will act as a starting point for the proof of Dirichlet's theorem.

Theorem 5.1. *There are infinitely many primes.*

Proof. Define the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{5.2}$$

This sum converges for all $s > 1$. However, as $s \to 1^+$, we have $\zeta(s) \to \infty$.

Consider the product

$$\left(1 + \frac{1}{2^s} + \frac{1}{4^s} + \ldots\right)\left(1 + \frac{1}{3^s} + \frac{1}{9^s} + \ldots\right)\left(1 + \frac{1}{5^s} + \frac{1}{25^s} + \ldots\right)\ldots$$

where the product extends over all primes. Because each natural number has a unique prime factorization, this product 'covers' every natural number exactly once: i.e, we have

$$\zeta(s) = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots\right) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \tag{5.3}$$

Taking the logarithm of both sides and applying the Taylor expansion for $\log(1 + x)$ yields

$$\log \zeta(s) = \sum_p -\log\left(1 - \frac{1}{p^s}\right) = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{ns}} = \sum_p \frac{1}{p^s} + \sum_p \sum_{n=2}^{\infty} \frac{1}{np^{ns}} \tag{5.4}$$

(we may separate this sum as above since it is absolutely convergent for $s > 1$).

Since $\zeta(s) \to \infty$ as $s \to 1^+$, so does its logarithm. Therefore, if we can show that the second sum is bounded as $s \to 1^+$, we will show that $\sum_p 1/p^s$ is unbounded as s approaches 1. Fortunately, for all $s \geq 1$ we have

$$\sum_p \sum_{n=2}^{\infty} \frac{1}{np^{ns}} < \sum_p \sum_{n=2}^{\infty} \frac{1}{p^n} = \sum_p \frac{1}{p^2} \cdot \frac{1}{1-1/p} < \sum_{m=2}^{\infty} \frac{1}{m(m-1)} = 1 \tag{5.5}$$

Hence, we must have $\sum_p 1/p^s$ unbounded as s approaches 1. This is only possible if there are infinitely many primes. □

Remark 5.6. In the above proof, the logarithm function was well-defined because our domain was restricted to the real numbers. However, the logarithm of a complex number is not well-defined. Instead, we define the logarithm of a complex number by its Taylor series; that is

$$\log(1-z) = -\sum_{n=1}^{\infty} \frac{z^n}{n} \tag{5.7}$$

The identity $\log(ab) = \log(a) + \log(b)$ still holds under this definition of the logarithm.

6. Dirichlet Series and L-functions

Unfortunately, the zeta function by itself is insufficient to attack Dirichlet's theorem because it leaves no means for distinguishing between the residue classes modulo k. For this, we need a more general class of functions.

Definition 6.1. Let a_n and λ_n be two sequences of complex numbers. For all $s \in \mathbb{C}$, we define the function

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{e^{\lambda_n s}}$$

Such a series is called a Dirichlet series.

Examples 6.2. The zeta function is defined by a Dirichlet series, where $a_n = 1$ and $\lambda_n = \log(n)$. In fact, any series of the form $\sum a_n/n^s$ is a Dirichlet series where $\lambda_n = \log(n)$.

The nice properties of Dirichlet characters (they are both periodic and multiplicative and interact nicely with one another) will be of great use in our attack on Dirichlet's theorem. Dirichlet series whose coefficients are given by Dirichlet characters are called L-functions.

Definition 6.3. Let χ be a Dirichlet character modulo k, and let s be a complex number. Then we define the function

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \tag{6.4}$$

Such a function is called an L-function.

Example 6.5. Let χ be the nontrivial character modulo 4. Then we have $L(s,\chi) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \ldots$. Specifically, we have $L(1,\chi) = \frac{\pi}{4}$.

We now have all the conceptual tools in place to move on to the final stage of this paper: the proof itself.

7. The Proof of Dirichlet's Theorem

All necessary apparatus is now in place to complete the proof of Dirichlet's theorem. The thrust of the proof is similar to that of the proof of the infinitude of the primes given in section 5. However, we will employ L-functions in place of the zeta function to isolate primes in a residue class modulo k.

The proof will consist of two parts: first, we will show that if $L(s, \chi)$ is bounded and nonzero as $s \to 1^+$ for nontrivial χ, then Dirichlet's theorem holds. The second, and more challenging part, is to show that $L(1, \chi)$ is, in fact, bounded and nonzero for nontrvial χ.

We will prove the easier step first. This requires a small lemma.

Lemma 7.1. *Let χ_1 denote the trivial character modulo k. Then $L(s, \chi_1)$ is unbounded as $s \to 1^+$*

Proof. We have

$$L(s, \chi_1) = \sum_{(n,k)=1} \frac{1}{n^s} > \sum_{q=1}^{\infty} \frac{1}{(qk)^s} = \frac{1}{k^s} \sum_{q=1}^{\infty} \frac{1}{q^s}$$

Since the sum on the right approaches infinity as s approaches 1, and the term $1/k^s$ approaches $1/k$, this quantity must diverge. □

Theorem 7.2. *If $L(s, \chi)$ is bounded and nonzero as $s \to 1$ for nontrivial χ, then we have*

$$\lim_{s \to 1^+} \sum_{p \equiv h \pmod{k}} \frac{1}{p^s} = \infty$$

This fact implies Dirichlet's theorem.

Proof. We will examine $L(s, \chi)$ as $s \to 1^+$. Because χ is completely multiplicative, we may 'factor' an L-function just as we did the zeta function (see equation 5.3). That is

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \dots\right) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \tag{7.3}$$

Recall from remark 5.6 that, although the logarithm function is not well-defined on the complex plane, we may still define the logarithm by its Taylor series, which retains the property that $\log(a) + \log(b) = \log(ab)$. Taking the logarithm of $L(s, \chi)$ yields

$$\log(L(s, \chi)) = \sum_p -\log\left(1 - \frac{\chi(p)}{p^s}\right) = \sum_p \sum_{n=1}^{\infty} \frac{\chi(p)^n}{np^{ns}} \tag{7.4}$$

Since this sum is absolutely convergent for $s > 1$, we may break it into two parts as shown:

$$\sum_p \sum_{n=1}^{\infty} \frac{\chi(p)}{np^{ns}} = \sum_p \frac{\chi(p)}{p^s} + \sum_p \sum_{n=2}^{\infty} \frac{\chi(p)}{np^{ns}}$$

We see that the second sum is bounded for $s > 1$, since

$$\left| \sum_p \sum_{n=2}^{\infty} \frac{\chi(p)}{np^{ns}} \right| \leq \sum_p \sum_{n=2}^{\infty} \frac{1}{np^{n \cdot \Re(s)}} < \sum_p \sum_{n=2}^{\infty} \frac{1}{p^n} = \sum_p \frac{1}{p^2} \cdot \frac{1}{1 - 1/p} < \sum_{m=2}^{\infty} \frac{1}{m(m-1)} = 1$$

Hence, we have $\log\left(L\left(s,\chi\right)\right)=\sum_p \frac{\chi(p)}{p^s}+O\left(1\right)$.

So far, we have worked only with a general Dirichlet character χ. We will now pick a k, and let $\chi_1,\chi_2,\ldots\chi_{\phi(k)}$ be the Dirichlet characters modulo k. Pick h such that $(h,k)=1$, and consider the sum

$$\frac{1}{\phi\left(k\right)}\sum_{i=1}^{\phi(k)}\overline{\chi_i\left(h\right)}\cdot\log\left(L\left(s,\chi\right)\right)=\frac{1}{\phi\left(k\right)}\left(\sum_{i=1}^{\phi(k)}\overline{\chi_i\left(h\right)}\sum_p\frac{\chi_i\left(p\right)}{p^s}\right)+O\left(1\right)$$

Again, for $s>1$, this sum is absolutely convergent. We may therefore rearrange the summations to yield

$$\frac{1}{\phi\left(k\right)}\sum_{i=1}^{\phi(k)}\overline{\chi_i\left(h\right)}\cdot\log\left(L\left(s,\chi\right)\right)=\frac{1}{\phi\left(k\right)}\sum_p\frac{1}{p^s}\sum_{i=1}^{\phi(k)}\overline{\chi_i\left(h\right)}\cdot\chi\left(p\right)+O\left(1\right)$$

However, recall from theorem 4.1 that

$$\sum_{i=1}^{\phi(k)}\overline{\chi_i\left(h\right)}\cdot\chi\left(p\right)=\begin{cases}\phi\left(k\right) & \text{if } p\equiv h \pmod{k},\\ 0 & \text{otherwise}\end{cases}$$

Since $(h,k)=1$.

Hence, we have

$$\sum_{p\equiv h \pmod{k}}\frac{1}{p^s}=\frac{1}{\phi\left(k\right)}\sum_{i=1}^{\phi(k)}\overline{\chi_i\left(h\right)}\cdot\log\left(L\left(s,\chi_i\right)\right)+O\left(1\right)$$

We know that $L\left(s,\chi_1\right)\to\infty$ as $s\to 1$; thus, so too does $\log\left(L\left(s,\chi_1\right)\right)$. Consider the other characters modulo k: if $L\left(s,\chi_i\right)$ is both bounded and nonzero as $s\to 1$, then its logarithm will be bounded. Moreover, if $\log\left(L\left(s,\chi_i\right)\right)$ is bounded for all nontrivial characters χ_i, we must have $\sum_{i=1}^{\phi(k)}\overline{\chi_i\left(h\right)}\cdot\log\left(L\left(s,\chi_i\right)\right)$, and therefore $\sum_{p\equiv h \pmod{k}}1/p^s$, unbounded. Hence, if we can show $L\left(s,\chi_i\right)$ to be bounded and nonzero at $s=1$ for nontrivial χ, then Dirichlet's theorem will follow. □

8. The Boundedness of $\log\left(L\left(s,\chi\right)\right)$ for Nontrivial χ

We now have the more difficult part of the proof: showing that $\log\left(L\left(s,\chi\right)\right)$ is bounded as s approaches 1 for nontrivial Dirichlet characters χ. In order to do this, we must show that $L\left(1,\chi\right)$ is both convergent and nonzero.

We will prove this in six steps.

1). We will show that, for nontrivial χ, $\sum_n \chi\left(n\right)/n^s$ converges for all s in the half-plane $\Re\left(s\right)>0$. This not only shows $L\left(1,\chi\right)$ to be finite, but will also aid us in showing that $L\left(1,\chi\right)\neq 0$.

2). We will use step 1 to show that $L\left(s,\chi\right)$ is holomorphic in this domain.

3). We will show that $L\left(s,\chi_1\right)$ is holomorphic except for a simple pole at $s=1$.

4). Consider the function $\zeta_k\left(s\right)=\prod_\chi L\left(s,\chi\right)$. From steps 2 and 3, we see that if there is a χ such that $L\left(1,\chi\right)=0$, then $\zeta_k\left(s\right)$ is holomorphic for all $\Re\left(s\right)>0$. We will show that, in the domain $\Re\left(s\right)>1$, we can express ζ_k as a convergent Dirichlet series with nonnegative real coefficients.

5). We will show that, if there is a χ such that $L\left(1,\chi\right)=0$, then the Dirichlet series defining ζ_k is convergent for all s in the domain $\Re\left(s\right)>0$.

6). Finally, we will use our findings in step 4 to show that the Dirichlet series defining ζ_k is unbounded at $s = \phi(k)^{-1}$. This will contradict our assumption that there exists a χ so that $L(1, \chi) = 0$, completing the proof.

8.1. **Step 1: The Convergence of $L(s, \chi)$ for $\Re(s) > 0$.** We will prove a generalized version of the needed result.

Lemma 8.1. *Let a_n be a sequence of complex numbers so that the function $S(x) = \sum_{n \leq x} a_n$ is bounded (say by J). Then the Dirichlet series*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

converges for all s in the domain $\Re(s) > 0$.

Proof. We will show this sum to be Cauchy. By Abel's summation formula, we have

$$\sum_{n=m+1}^{M} \frac{a_n}{n^s} = \frac{S(M)}{M^s} - \frac{S(m)}{m^s} + s \int_m^M \frac{S(t)}{t^{s+1}} dt$$

Let σ denote the real part of s. Taking absolute values in the above equation yields

$$\left| \sum_{n=m+1}^{M} \frac{a_n}{n^s} \right| \leq \frac{|S(M)|}{M^\sigma} + \frac{|S(m)|}{m^\sigma} + |s| \int_m^M \frac{|S(t)|}{t^{\sigma+1}} dt \tag{8.2}$$

$$\leq J \left(\frac{2}{m^\sigma} + |s| \int_m^M \frac{dt}{t^{\sigma-1}} \right) \leq J \left(\frac{2}{m^\sigma} + \frac{|s|}{\sigma} \left| \frac{1}{M^\sigma} - \frac{1}{m^\sigma} \right| \right) \leq \frac{2J}{m^\sigma} \left(1 + \frac{|s|}{\sigma} \right)$$

For a given s where $\sigma > 0$, this quantity approaches 0 as m approaches ∞. This shows the sum $\sum_n a_n/n^s$ to be Cauchy, and therefore convergent, for all s in the domain $\Re(s) > 0$. □

The same logic can be used to prove a slightly more general version:

Corollary 8.3. *Consider a_n so that the sum $\sum_n a_n/n^{s_0}$ is bounded. Then the Dirichlet series*

$$\sum_{n=0}^{\infty} \frac{a_n}{n^s}$$

converges for all s in the domain $\Re(s) > \Re(s_0)$.

Geometrically, this corollary shows that a Dirichlet series converges in a half-plane (where we count both $\emptyset$ and $\mathbb{C}$ as half-planes).

Using lemma 8.1, we prove the convergence of $L(s, \chi)$ in the desired domain for nontrivial χ.

Proposition 8.4. *If χ is a nontrivial character modulo k, then we have $L(s, \chi)$ finite for all s with real part greater than 0. Specifically, $L(1, \chi)$ is finite.*

Proof. By lemma 8.1, it is sufficient to show that the sum

$$S(x) = \sum_{n \leq x} \chi(n)$$

is bounded.

If χ is nontrivial, we have $S(l \cdot k) = 0$ for all $l = 1, 2, \ldots$. Moreover, we have

$$|\chi(n)| = \begin{cases} 1 & \text{if } (n,k) = 1 \\ 0 & \text{otherwise} \end{cases}$$

We therefore have $|S(n)| \le \phi(k)$. $\square$

8.2. **Step 2: $L(s,\chi)$ is holomorphic for $\Re(s) > 0$.** We wish to show that $L(s,\chi)$ is holomorphic in the domain $\Re(s) > 0$. To do this, we make use of a well-known lemma from complex analysis.

Lemma 8.5. *Let f_n be a sequence of functions, holomorphic in some subset A of $\mathbb{C}$, that converge uniformly on A to a function f. Then f is holomorphic on A, and $\frac{d}{dz} f = \lim_{n\to\infty} \frac{d}{dz} f_n$.*

Furthermore, it is sufficient to show that f_n converges to f uniformly in each compact subset of A.

Proposition 8.6. *Let K be a compact subset of $\{s \in \mathbb{C} \mid \Re(s) > 0\}$, and let the sum $\sum_n a_n$ be bounded (again by J). Then the Dirichlet series $F(s) = \sum_n \chi(n)/n^s$ converges uniformly on K for all nontrivial characters χ. It follows that F is holomorphic in the given half-plane.*

Proof. We will use equation 8.2, which states

$$\left| \sum_{n=m+1}^{M} \frac{a_n}{n^s} \right| \le \frac{2J}{m^\sigma} \left(1 + \frac{|s|}{\sigma} \right)$$

where σ denotes the real part of s, for all nontrivial χ. In particular, we will use this to show that the Dirichlet series is uniformly Cauchy on K.

Let $\alpha = \inf_{z \in K} \Re(z)$. Since K is compact, we must have $\alpha > 0$. Furthermore, let $\beta = \sup_{z\in K} |z|$. Again, since K is compact, β is well-defined and finite. Therefore, for all $s \in K$, we have

$$\left| \sum_{n=m+1}^{M} \frac{a_n}{n^s} \right| \le \frac{2J}{m^\alpha} \left(1 + \frac{\beta}{\alpha} \right)$$

This quantity approaches 0 as $m \to \infty$. Moreover, the constants α and β depend only on K and are independent of the individual elements of K. Therefore, the Dirichlet series defining L is uniformly Cauchy, and therefore uniformly convergent, on K. Thus, $F(s)$ is holomorphic in its domain of convergence. $\square$

Again, the same logic shows that if $\sum_n a_n/n^{s_0}$ is bounded, then the function $F(s)$ defined by the Dirichlet series $\sum_n a_n/n^s$ is holomorphic in the domain $\Re(s) > \Re(s_0)$. Specifically, a Dirichlet series is holomorphic in its half-plane of convergence.

Of course, since the partial sums of nontrivial Dirichlet characters are bounded, we have the following corollary:

Corollary 8.7. *For nontrivial χ, we have $L(s,\chi)$ holomorphic in the domain $\Re(s) > 0$.*

In step 5, we will make use of the derivative of a function defined by a Dirichlet series. Fortunately, lemma 8.5 tells us that we may differentiate a Dirichlet series termwise in its domain of convergence.

Corollary 8.8. *Let* $F(s) = \sum_n f(n)/n^s$ *be a Dirichlet series that converges for* $\Re(s) > 0$. *Then*

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

Proof. Termwise differentiation yields $\frac{d}{ds}F(s) = -\sum_n f(n)\log(n)/n^s$. The corollary follows inductively. $\square$

8.3. **Step 3: $L(s,\chi_1)$ has a simple pole at $s = 1$.**

Proposition 8.9. *The function* $L(s,\chi_1)$ *is holomorphic in the entire domain* $\Re(s) > 0$ *except for a simple pole at* $s = 1$.

Proof. We have $L(s,\chi_1) = \sum_{(n,k)=1} 1/n^s$. Factoring this sum yields

$$L(s,\chi_1) = \prod_{p\nmid k}\left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s)\prod_{p|k}\left(1 - \frac{1}{p^s}\right)$$

The zeta function is holomorphic for $\Re(s)$ except for a simple pole at $s = 1$. Moreover, for a given p, we have $1 - 1/p^s$ holomorphic everywhere and nonzero at $s = 1$. Since there are only finitely many p to consider, we must have $L(s,\chi)$ holomorphic except for a simple pole at $s = 1$. $\square$

8.4. **Step 4: The function $\zeta_k(s)$ and its Dirichlet Series.** We consider the function

$$\zeta_k(s) = \prod_\chi L(s,\chi)$$

where the product is taken over all Dirichlet characters modulo k. Since we know $L(s,\chi_1)$ has a simple pole at $s = 1$ and that $L(s,\chi)$ is holomorphic for all s with $\Re(s) > 0$, then this function will be holomorphic in this domain if $L(s,\chi) = 0$ for some χ. Therefore, examination of this function is sufficient to prove Dirichlet's theorem.

Fortunately, this function has some nice properties.

Proposition 8.10. *For* $\Re(s) > 1$, $\zeta_k(s)$ *is defined by a convergent Dirichlet series with positive integer coefficients.*

Proof. We have

$$\zeta_k(s) = \prod_\chi L(s,\chi) = \prod_\chi \prod_{p\nmid k}\left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \prod_{p\nmid k}\prod_\chi\left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \tag{8.11}$$

Consider $\prod_\chi (1 - \chi(p)p^{-s})^{-1}$. Let $f(p)$ be the order of p modulo k; then the values $\chi(p)$ are the $f(p)^{\text{th}}$ roots of unity. Moreover, if we consider the character group, the set of characters χ such that $\chi(p) = w$ (where w is a root of unity for $f(p)$) is a coset of the subgroup $\{\chi \mid \chi(p) = 1\}$. Hence, there are exactly $g(p) = \phi(k)/f(p)$ characters that attain each w. We therefore have

$$\prod_\chi\left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \prod_{w^{f(p)}=1}\left(\left(1 - \frac{w}{p^s}\right)^{-1}\right)^{g(p)} = \left(\left(1 - \frac{1}{p^{sf(p)}}\right)^{-1}\right)^{g(p)} \tag{8.12}$$

Therefore, when we take the product over all primes, we have

$$\zeta_k(s) = \prod_{p \nmid k} \left(1 - \frac{1}{p^{sf(p)}}\right)^{-g(p)}$$

For $\Re(s) > 1$, each term in the product is equal to $(1 + 1/p^{s \cdot f(p)} + 1/p^{2s \cdot f(p)} + \ldots)^{g(p)}$. Thus, in this domain, we may express ζ_k as a Dirichlet series with positive integer coefficients. □

8.5. **Step 5: $L(1, \chi) = 0$ implies the convergence of ζ_k for $\Re(s) > 0$.** We have shown that ζ_k is defined by a Dirichlet series with nonnegative real coefficients in the domain $\Re(s) > 1$. We now wish to show that if it is holomorphic in the half plane $\Re(s) > 0$, then the series defining it is convergent in the same domain. We will prove a lemma; the proposition will immediately follow.

Lemma 8.13. *Let $F(s)$ be a function defined in the half-plane $\Re(s) > c$ by the convergent Dirichlet series*

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

where $f(n)$ is real and nonnegative. Moreover, let F be holomorphic in the domain $\Re(s) > c'$, with $c' < c$. Then the Dirichlet series defining F converges for all $\Re(s) > c'$.

Proof. Consider some point $a > c$. Then F is holomorphic, and therefore analytic, at a, and therefore we may define F by its power series

$$F(s) = \sum_{k=0}^{\infty} \frac{F^{(k)}(a)}{k!} (s-a)^k$$

Moreover, from step 3, we know that

$$F^{(k)}(a) = (-1)^k \sum_{n=1}^{\infty} \frac{f(n) \log(n)^k}{n^s}$$

We may therefore write the Taylor series in this form:

$$F(s) = \sum_{k=0}^{\infty} \sum_{n=1}^{\infty} \frac{(a-s)^k f(n) \log(n)^k}{k! \cdot n^s}$$

Pick $b > c'$. Then there is a neighborhood O of a that both contains b and lies entirely in the set $\{z \mid \Re(z) > c'\}$. Therefore, F is holomorphic in the entirety of O, so that the power series representation for F is valid for b. Moreover, since each term in this double-sum is real and nonnegative, we may rearrange the order of summation, giving

$$F(b) = \sum_{n=1}^{\infty} \frac{f(n)}{n^a} \sum_{k=0}^{\infty} \frac{((a-b)\log(n))^k}{k!} = \sum_{n=1}^{\infty} \frac{f(n)}{n^a} e^{(a-b)\log(n)}$$

$$= \sum_{n=1}^{\infty} \frac{f(n)}{n^{a-(a-b)}} = \sum_{n=1}^{\infty} \frac{f(n)}{n^b}$$

Thus, the Dirichlet series converges at b for any $b > c'$, and therefore in the entire half-plane $\Re(s) > c'$. □

Corollary 8.14. *If ζ_k is holomorphic at $s = 1$, the Dirichlet series defining it is convergent in the entire domain where $\Re(s) > 0$.*

Proof. Recall from step 4 that if ζ_k is holomorphic at $s = 1$, it is holomorphic in the entire half-plane where $\Re(s) > 0$. Also recall that the Dirichlet series defining it is convergent for $\Re(s) > 1$. Therefore, by lemma 8.13, this Dirichlet series must converge for $\Re(s) > 0$. □

8.6. **Step 6: The divergence of ζ_k at $s = \phi(k)^{-1}$.**

Proposition 8.15. *The Dirichlet series defining $\zeta_k(s)$ diverges at $s = \frac{1}{\phi(k)}$.*

Proof. Recall from step 4 that we have

$$\zeta_k(s) = \prod_{p \nmid k} \left(1 - \frac{1}{p^{sf(p)}}\right)^{-g(p)}$$

and consider the factor corresponding to p. We have

$$\left(1 - \frac{1}{p^{sf(p)}}\right)^{-g(p)} = \left(1 + p^{-sf(p)} + p^{-2sf(p)} + \dots\right)^{g(p)}$$

Since $f(p) \leq \phi(k)$ and $g(p) \geq 1$, this sum dominates the sum

$$1 + p^{-s\phi(k)} + p^{-2s\phi(k)} + \dots$$

Therefore, the series defining $\zeta_k(s)$ dominates the series $\sum_{(n,k)=1} n^{-s\phi(k)}$. However, this sum diverges at $s = 1/\phi(k)$. □

We have shown that, if there is a χ so that $L(1, \chi) = 0$, then the function $\zeta_k(s)$ is holomorphic in the entire half-plane $\Re(s) > 0$. This would imply that the Dirichlet series defining ζ_k converges in this domain. However, we have just found at least one s for which this Dirichlet series does not converge. Therefore, there cannot exist a χ so that $L(1, \chi) = 0$, which in turn implies the boundedness of $\log(L(1, \chi)) = 0$ for nontrivial χ. Theorem 7.2 shows that this fact implies Dirichlet's theorem. Hence, the proof is complete.

References

[1] J. P. Serre. Course in Arithmetic. Springer-Verlag, 1973.
[2] Tom M. Apostol. Introduction to Analytic Number Theory. Springer-Verlag, 1976.