DIRICHLET'S THEOREM ON ARITHMETIC PROGRESSIONS

by

JOSEPH TOMCAL

A THESIS

Presented to the Department of Mathematics
and the Robert D. Clark Honors College
in partial fulfillment of the requirements for the degree of
Bachelor of Arts

June, 2014

An Abstract of the Thesis of

Joseph Tomcal for the degree of Bachelor of Arts
in the Department of Mathematics to be taken June 2014

Title: Dirichlet's Theorem on Arithmetic Progressions

Approved: _____

Peter B. Gilkey

The intent of this paper is to give a proof of Dirichlet's Theorem on Arithmetic Progressions, provide a brief history of the area, explain the mathematical concepts used in the theorem, and to expound upon the significance of the theorem. The statement of the Theorem is as follows: Given two coprime integers k and n, there exist an infinite number of primes congruent to k mod n.

Acknowledgements

I wish to thank my advisor, Professor Peter B. Gilkey, and all his associates at the Krill Institute of Technology. This project would not have been possible without their generous help and support.

DIRICHLET'S THEOREM ON ARITHMETIC PROGRESSIONS

J. TOMCAL

Abstract. The intent of this paper is to give a proof of Dirichlet's Theorem on Arithmetic Progressions, provide a brief history of the area, explain the mathematical concepts used in the theorem, and to expound upon the significance of the theorem. The statement of the Theorem is as follows: Given two coprime integers k and n, there exist an infinite number of primes congruent to k mod n.

1. Introduction

Whereas it is easy to state Dirichlet's Theorem [2], the proof is surpisingly difficult (as is often the case for theorems in number theory). The proof we shall present (there are several quite different proofs in the literature) uses both representation theory and complex variables; this is often the case in analytic number theory. We shall use infinite sums and products, the Riemann Zeta function, Dirichlet L-Series, and Dirichlet characters.

2. History

We begin by reviewing a bit of the history of the subject; we have used [9] as our primary reference. We start our review with Pythagoras of Samos (circa 569 B.C.E - 475 B.C.E.), who is most known for the Pythagorean Theorem: If (a, b, c) are 3 sides in a right triangle where c is the hypotenuse, then $a^2 + b^2 = c^2$; if (a, b, c) are integers, then this is called a Pythagorean triple. While Pythagoras is credited with the discovery, evidence suggests that the Babylonians had the result almost one thousand years earlier. Pythagoras's life remains ambiguous as historians do not have any sources written by Pythagoras himself. In other sources, Pythagoras was said to have established a school around 518 B.C.E. in Croton, located in modern day Italy. The school of Pythagoras was philosophical, religious, and secretive in nature (the secretivity contributes to issues in researching Pythagoras himself). While the contributions of Pythagoras to number theory and geometry may seem elementary today, they are nevertheless important building blocks to a deeper understanding of mathematics. [9]

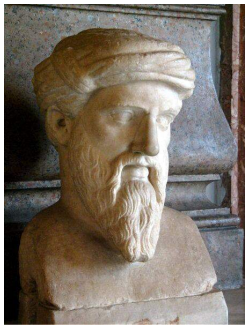

Figure 1. Bust of Pythagoras

The first results concerning prime numbers are reported in Euclid of Alexandria's treatise on mathematics known as "Elements," circa 300 B.C.E. (see, for example, the English translation by Heath [5]). Little is known about Euclid's life, despite the fact that he was one of the most prominent mathematicians of the ancient world. Euclid is credited with the discovery of the Fundamental Theorem of Arithmetic (which we will discuss presently in Theorem 3.3), the division algorithm (also known as the Euclidean algorithm), and the existence of infinitely many prime numbers. [9]

FIGURE 2. A 1500s depiction of Euclid

Leonhard Euler (1707-1783) was the first known mathematician to conjecture that every arithmetic progression beginning with 1 contained infinitely many primes. He was born in Basel Switzerland and was the son of a Protestant minister. His father sent him to the University of Basel in 1720 to prepare him for a career as a minister. However, Johann Bernoulli recognized Euler's potential in mathematics, who then convinced Euler to devote his studies to the topic. Euler discovered the identity $e^{ix} = cos(x) + isin(x)$, Theorem 3.7, and many other important mathematical results. [9]

FIGURE 3. Euler by Emanuel Handmann

Carl Friedrich Gauss (1777-1855) proposed the theorem to be proven in this thesis (see, for example, the discussion in [6]). Gauss was born in Brunswick, located in modern day Germany. Gauss's potential in mathematics was first recognized in elementary school at the age of seven when he was able to instantly sum the numbers from 1 to 100 by using 50 pairs of numbers summing to 101 [9]. Gauss attended the Brunswick Collegium Carolinum in 1792. There, he discovered Bode's law, the binomial theorem, and investigated arithmetic and geometric means. Later in his life, Gauss made several important contributions to number theory, and differential geometry. [9]

FIGURE 4. Gauss by Christian Albrecht Jensen

The theorem we intend to establish in this paper was first proved by Johann Peter Gustav Lejeune Dirichlet (1805-1859) in the year 1837 [2]. Dirichlet was born in Dren, which is located in modern day Germany. Dirichlet was the son of the postmaster of Dren. Dirichlet attended the Jesuit College in Cologne at the age of 14. There, he was taught by Georg Simon Ohm, who is renowned for his law on electrical resistance. In addition to the Theorem we intend to prove in this document, Dirichlet proved the case of $n = 5$ of Fermat's Last Theorem. Dirichlet is also credited with first proposing the modern definition of a function, and with important work on units in algebraic number theory. [9]

FIGURE 5. A Sketch of Dirichlet

We shall also give mention to Georg Friedrich Bernhard Riemann (1826-1866), who was a contemporary of Dirichlet. Riemann was the son of a Lutheran minister in Hannover, which is located in modern day Germany. Riemann attended the University of Berlin in the spring of 1847; there he was taught by Steiner, Jacobi, Dirichlet and Eisenstein. During his career, Riemann made several important contributions to complex analysis, differential geometry, and analytic number theory. An important discovery of Riemann was the Riemann-Zeta function over the complex numbers, which we shall make use of in our analysis. Riemann conjectured that the function had infinitely many nontrivial zeros that all have $\Re(s) = \frac{1}{2}$. This is known as the Riemann hypothesis, which is currently a Millenium prize problem. [9]

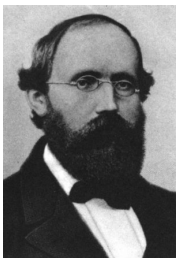

FIGURE 6. A Photograph of Riemann

As a final remark, the above listed accomplishments of Pythagoras, Euclid, Euler, Gauss, Dirichlet and Riemann do not comprise the complete body of each mathematician's respective work.

3. Preliminary Material

We begin with some preliminaries and some basic definitions.

3.1. **Character theory.** We first review some elementary results from *character theory*. Let G be a finite Abelian group. A *character* on G is a multiplicative group homomorphism from G to $\mathbb{C}$; necessarily such a map takes values in the unit complex numbers. We let $\hat{G}$ be the set of all characters; function multiplication gives $\hat{G}$ the structure of an Abelian group; this is called the *dual Abelian group*. Let $L^2(G)$ be the set of all maps from G to $\mathbb{C}$. We define a positive definite Hermitian inner-product on $L^2(G)$ by setting:

$$\ll f_1, f_2 \gg_G := \frac{1}{|G|} \sum_{g \in G} f_1(g) \bar{f}_2(g)\,.$$

L3.1 **Lemma 3.1.** *Adopt the notation established above. Then $|\hat{G}| = |G|$ and the elements of $\hat{G}$ form an orthonormal basis for $L^2(G)$.*

Proof. Suppose first that $G = \mathbb{Z}_k$ is cyclic. The map $n \to e^{2\pi i n j/k}$ defines a character $\rho_j \in \hat{G}$. Suppose $\lambda^k = 1$ but $\lambda \neq 1$. We compute

$$0 = 1 - \lambda^k = (1-\lambda)(1 + \lambda + \cdots + \lambda^{k-1})$$

and thus $1 + \lambda + \cdots + \lambda^{k-1} = 0$. Let $\lambda_0 := e^{2\pi\sqrt{-1}/k}$. Then $\lambda = \lambda_0^{(a-b)}$ satisfies $\lambda^k = 1$; $\lambda = 1$ if and only if $a \equiv b \mod k$. Thus:

$$\ll \rho_a, \rho_b \gg_{\mathbb{Z}_k} = \frac{1}{k} \sum_{j=0}^{k-1} \lambda_0^{j(a-b)} = \left\{ \begin{array}{l} 0 \text{ if } a \not\equiv b \mod k \\ 1 \text{ if } a \equiv b \mod k \end{array} \right\}.$$

This proves the Lemma if G is cyclic. More generally, the fundamental theorem of Abelian groups yields $G = \mathbb{Z}_{k_1} \oplus \cdot \oplus \mathbb{Z}_\ell$ and dually $\hat{G} = \hat{\mathbb{Z}}_{k_1} \oplus \cdots \oplus \hat{\mathbb{Z}}_{k_\ell}$. The result in general follows; we refer to Apostol [1] for further details. □

3.2. **The Theorem of Euclid.**

Definition 3.2.

(1) *An integer $a > 1$ is said to be* **prime** *if the only positive divisors of a are 1 and a.*

(2) *Two positive integers a and b are said to be* ***coprime*** *if* 1 *is the only positive integer which divides both a and b.*
(3) *A sequence of positive integers $b_n = b_1 + d(n-1)$ is said to be in arithmetic progression.*

The fact that there exist infinitely many primes plays a key role. We refer to Heath [5] for an English translation of the **Elements** of Euclid which contains the following result:

T3.3 **Theorem 3.3** (Euclid)**.**

(1) *There are infinitely many prime numbers.*
(2) *Every positive integer $n \geq 2$ can be represented uniquely as a product $n = p_1 p_2 \dots p_k$ where each p_i is prime and $1 < p_1 \leq p_2 \leq \dots \leq p_k$.*

Proof. Suppose to the contrary that there are but a finite number of primes. We argue for a contradiction. Let $\{p_1, \dots, p_n\}$ be enumeration of the primes. Let $A = p_1 \dots p_n + 1$ and let p be a prime dividing A. If $p = p_k$ for some k, then p divides $A - p_1 \dots p_n = 1$ which is false. Thus there must be infinitely many primes. This establishes Assertion (1); we shall omit the proof of (2) as the proof is quite lengthy and instead refer the reader to **Elements**. [5] □

3.3. **Infinite sums and infinite products.** We now turn to the discussion of infinite sums and infinite products. Since 0 plays a distinguished role with respect to multiplication, there are some subtleties in considering infinite products. The distinction between convergence and absolute convergence will play a crucial role in our analysis. Let log be the principal branch of the Logarithm function; $\log(1+p)$ is defined for $|p| < 1$ and $\log(1) = 0$. Let $\{a_n\}$ be a sequence of complex numbers. We recall some basic notation and results in the area; a good auxiliary reference would be Marsden and Hoffman [7].

(1) Let $s_k := a_1 + \dots + a_k$ be the partial sums of $\{a_n\}$. If $\lim_{n\to\infty} s_k$ exists, then the infinite series is said to converge and we write:

$$\sum_{n=1}^{\infty} a_n := \lim_{k\to\infty} s_k\,.$$

If the series converges, then the $a_n \to 0$; the converse can fail. If the series $\sum_n |a_n| < \infty$, then the series is said to converge absolutely. Note that there exist conditionally convergent series. If the series converges absolutely, any rearrangement of the series converges to the same limit; this fails for series which are conditionally but not absolutely convergent.

(2) We suppose that $a_n \neq -1$ for $n \geq N$ and let $p_n = (1+a_N)\dots(1+a_n)$ be the partial product. The infinite product is said to converge if $\lim_{n\to\infty} p_n \neq 0$ and we set

$$\prod_{n=1}^{\infty}(1+p_n) = (1+a_1)\dots(1+a_{N-1}) \lim_{n\to\infty} p_n\,.$$

The infinite product is zero if and only if one of the $a_n = -1$. If the infinite product converges, then the $a_n \to 0$; the converse can fail. We suppose $|a_n| < 1$ for $n \geq N$. The infinite product is convergent if and only the infinite series $\sum_{n\geq N} \log(1+a_n)$ is convergent. If $\sum_{n\geq N} |\log(1+a_n)| < \infty$, then the infinite product is said to be absolutely convergent. If the infinite product converges absolutely, any rearrangement of the product converges to the same limit; this fails for products which are conditionally but not absolutely convergent.

The following provides a useful criteria for the absolute convergence of an infinite product by relating the condition $\sum_n |\log(1+a_n)|$ to a more familiar condition:

L3.4 **Lemma 3.4.** *Let a_n be a sequence of complex numbers with $|a_n| < 1$ for all n. The following conditions are equivalent:*

(1) $\sum_{n\geq 1} |\log(1+a_n)| < \infty$.
(2) $\sum_{n\geq 1} |a_n| < \infty$.

Proof. We may expand log in a Taylor series about 1 to see

$$\log(1+p) = p - \tfrac{1}{2}p^2 + \tfrac{1}{3}p^3 - \dots .$$

We suppose $|a| < \frac{1}{2}$. We may estimate:

$$\begin{aligned} & |\log(1+a)| \leq |a| + \tfrac{1}{2}|a|^2 + \tfrac{1}{3}|a|^3 + \dots \leq |a| + \tfrac{1}{2}(|a|^2 + |a|^3 + \dots) \\ = \;& |a| + \tfrac{1}{2}|a|^2(1-|a|)^{-1} \leq |a| + \tfrac{1}{4}|a|(1-\tfrac{1}{2})^{-1} \leq |a| + \tfrac{1}{2}|a| = \tfrac{3}{2}|a| . \end{aligned}$$

Consequently, we may show that Assertion (2) implies Assertion (1) by estimating:

$$\sum_{n=1}^{\infty} |\log(1+a_n)| \leq \frac{3}{2}\sum_{n=1}^{\infty} |a_n| .$$

Conversely, we may estimate:

$$\begin{aligned} & |a| \leq |\log(1+a)| + \tfrac{1}{2}|a|^2 + \tfrac{1}{3}|a|^3 + \dots \\ \leq \;& |\log(1+a)| + \tfrac{1}{2}(|a|^2 + |a|^3) + \dots \leq |\log(1+a)| + \tfrac{1}{2}|a| . \end{aligned}$$

We subtract $\frac{1}{2}|a|$ from both sides to see $\frac{1}{2}|a| \leq |\log(1+a)|$. We show that Assertion (1) implies Assertion (2) and complete the proof by computing:

$$\sum_{n=0}^{\infty} |a_n| \leq 2\sum_{n=1}^{\infty} |\log(1+a_n)|. \qquad \square$$

3.4. **Holomorphic functions with specified zeros.** Let

$$T_n(z) := z + \frac{1}{2}z^2 + \frac{1}{3}z^3 + \dots + \frac{1}{n}z^n ;$$

$-T_n(z)$ is the tail in the Taylor series for $\log(1-z)$. Consequently, given $\epsilon > 0$, there exists $m(\epsilon)$ so that

$$|\log(1-z) + T_{m(\epsilon)}(z)| \leq \epsilon \text{ for } |z| \leq \tfrac{1}{2} .$$

We say that a function is **entire** if it is complex differentiable and if it is defined on the entire complex plane. The following is a lovely result which illustrates the use of infinite products.

Proposition 3.5. *Let a_n be a sequence of distinct complex numbers with $a_0 = 0$ and $\lim_{n\to\infty} |a_n| = \infty$. Let k_n be a sequence of non-negative integers. Let m_n be chosen so $k_n|\log(1-z) + T_{m_n}(z)| < 2^{-n}$ for $|z| \leq \frac{1}{2}$.*

(1) *The following infinite product converges absolutely:*

$$F(z) = z^{k_0}\prod_{n=1}^{\infty}(1-\frac{z}{a_n})^{k_n}e^{k_n T_{m_n}(\frac{z}{a_n})}$$

(2) *The function F is entire and has zeros of order k_n at the points a_n.*
(3) *The function F has no other zeros.*
(4) *Let $f(z)$ be an entire function with zeros of order k_n the points a_n. Then there exists an entire function g so that $f(z) = e^g F$.*

Proof. Choose R. Find N so $n \geq N$ implies $|a_n| \geq 2R$. If $n \geq N$ and if $|z| \leq R$, then $|\frac{z}{a_n}| \leq \frac{1}{2}$. We may therefore estimate:

$$\begin{aligned} &\sum_{n=N}^{\infty} \left|\log\left((1-\tfrac{z}{a_n})^{k_n} e^{k_n T_{m(n)}(\frac{z}{a_n})}\right)\right| \\ = \quad &\sum_{n=N}^{\infty} k_n \left|\log\left(1-\tfrac{z}{a_n}\right) + T_{m(n)}(\tfrac{z}{a_n})\right| \leq \sum_{n=N}^{\infty} 2^{-n} < 1\,. \end{aligned}$$

This shows that the series converges uniformly for $|z| \leq R$ and hence the infinite product converges uniformly on compact subsets of $\mathbb{C}$. Assertion (1) now follows; Assertions (2) and (3) follow from Assertion (1). Since $\frac{f(z)}{F(z)}$ is nowhere vanishing and since $\mathbb{C}$ is simply connected, we can conclude that there is a function $g(z)$ that is analytic on $\mathbb{C}$ and unique up to the addition of a constant multiple of $2\pi i$ where $e^{g(z)} = \frac{f(z)}{F(z)}$ for all z in $\mathbb{C}$. □

3.5. **The Riemann Zeta function.** We now turn to the Riemann Zeta function; this function will play a central role in our analysis. Set

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}\,. \tag{1}$$ E1a

T3.6 **Theorem 3.6.** *The series of Equation (1) defining the Riemann zeta function converges absolutely to a holomorphic function of s for $\Re(s) > 1$. There is a meromorphic extension of ζ to $\mathbb{C}$ with a simple isolated pole at $s = 1$ with residue 1.*

Proof. We begin by recalling some facts about the classical Γ function and refer to [7] for further details. Recall that the Γ function is given for $s > 0$ by:

$$\Gamma(s) := \int_0^{\infty} t^{s-1} e^{-t} dt\,. \tag{2}$$ E1

Integration by parts yields the functional equation

$$s\Gamma(s) = \Gamma(s+1)$$

which permits us to extend Γ to be a meromorphic function on $\mathbb{C}$ with simple poles at the non-positive integers $s = 0,\ s = -1, \ldots$. Since $\Gamma(n) = n!$, $\operatorname{Res}_{s=0}\Gamma = 1$. The infinite product formula

$$\Gamma(t) = e^{-\gamma t} t^{-1} \prod_{n=1}^{\infty} \left(1 + \frac{t}{n}\right)^{-1} e^{\frac{t}{n}}$$

where γ is the Euler-Maascheroni constant shows that Γ never vanishes. We use the Mellin transform. For $t > 0$, set

$$h(t) := \sum_{n=1}^{\infty} e^{-tn} = \frac{1}{1-e^{-t}} \text{ for } t > 0\,. \tag{3}$$ E2

For $\Re(s) > 1$, since the convergence in

$$\sum_{n=1}^{\infty} \int_0^{\infty} e^{-nt} t^{s-1} dt$$

is uniform, we can interchange the order of integration and summation and then make a change of variables to see:

$$\begin{aligned}\int_0^\infty t^{s-1}h(t)dt &= \sum_{n=1}^\infty \int_0^\infty e^{-nt}t^{s-1}dt = \sum_{n=1}^\infty n^{-s}\int_0^\infty e^{-nt}(nt)^{s-1}d(nt)\\ &= \sum_{n=1}^\infty n^{-s}\int_0^\infty e^{-\tau}\tau^{s-1}d\tau = \Gamma(s)\zeta(s)\,.\end{aligned}$$

This gives an integral representation of η. Decompose $\zeta(s) = \zeta_1(s) + \zeta_2(s)$ for:

$$\begin{aligned}\zeta_1(s) &:= \Gamma(s)^{-1}\int_0^1 t^{s-1}\frac{1}{1-e^{-t}}dt,\\ \zeta_2(s) &:= \Gamma(s)^{-1}\int_1^\infty t^{s-1}\frac{1}{1-e^{-t}}dt\end{aligned}$$

The integral series defining $\zeta_2(s)$ converges absolutely and uniformly on compact s subsets of $\mathbb{C}$ to a holomorphic function of s which is defined on the whole complex plane. To examine $\zeta_1(s)$, we expand

$$\frac{1}{1-e^{-t}} = t^{-1} + \sum_{n=0}^\infty a_n t^n$$

in a Laurent series about the origin; the positive term series converges for $|t| < 2\pi$. Let $\mathcal{E}_N$ be the remainder in the series; $|\mathcal{E}_N| \le C_N t^N$ for $|t| \le 1$. We may therefore expand

$$\begin{aligned}\zeta_1(s) &= \Gamma(s)^{-1}\int_0^1 t^{s-1}\left\{t^{-1} + \sum_{n\le N} a_n t^n + \mathcal{E}_N\right\}dt\\ &= \Gamma(s)^{-1}\left\{\frac{1}{s-1} + \sum_{n\le N} a_n\frac{1}{n+s} + \int_0^1 t^{s-1}\mathcal{E}_N(t)dt\right\}.\end{aligned}$$

The integral $t^{s-1}\mathcal{E}_N dt$ converges to a holomorphic function of s for $\Re(s) > -N$. The remaining series is defined for all s. This gives the desired meromorphic extension to $\mathbb{C}$; the apparent additional poles when $n + s = 0$ are cancelled by the zeros of $\Gamma(s)^{-1}$ there. Since Γ is never zero, $\Gamma(s)^{-1}$ does not create any additional poles. Hence, when $s = 1$, at $\Gamma(1) = 1$, we have the desired residue of 1. □

3.6. **An infinite product formula for the zeta function.** Let $\mathcal{P}$ be the collection of prime numbers. Euler (see the discussion in [8]) established that:

T3.7 **Theorem 3.7.** *If $\Re(s) > 1$, then*

$$\zeta(s) = \prod_{p\in\mathcal{P}}\left(\frac{1}{1-p^{-s}}\right).$$

where the infinite product converges absolutely.

Proof. We shall establish this identity for s real; the general case will then follow by the identity theorem. Let $\{p_k\}$ be an enumeration of the primes in increasing order. Fix (k, ℓ, ν) and let:

$$\alpha_{k,\ell}(s) := \prod_{j=1}^k (1 + p_j^{-s} + \cdots + p_j^{-\ell s}) \text{ and } \beta_\nu(s) := \sum_{n=1}^\nu n^{-s}\,.$$

If $\nu > p_1^\ell \cdot \cdots \cdot p_k^\ell$, Then

$$\{p_1^{\ell_1} \cdot \cdots \cdot p_k^{\ell_k}\}_{1 \le \ell_1 \le \ell, \ldots 1 \le \ell_k \le \ell} \subset \{1, \ldots, \nu\}\,.$$

Consequently

$$\alpha_{k,\ell}(s) \le \beta_\nu(s) \le \sum_{n=1}^{\infty} n^{-s} = \eta(s)\,.$$

We may now take the limit as $\ell \to \infty$ to see

$$\prod_{j=1}^{k} \frac{1}{1-p^{-s}} = \prod_{j=1}^{k} \left(\lim_{\ell \to \infty} 1 + p_k^{-s} + \cdots + p_k^{-s\ell} \right)$$

$$= \lim_{\ell \to \infty} \prod_{j=1}^{k} \left(1 + p_k^{-s} + \cdots + p_k^{-s\ell}\right) = \lim_{\ell \to \infty} \alpha_{k,\ell}(s) \le \zeta(s)\,.$$

We now take the limit as $k \to \infty$ to obtain the estimate:

$$\prod_{j=1}^{\infty} \frac{1}{1-p^{-s}} = \lim_{k \to \infty} \prod_{j=1}^{k} \frac{1}{1-p^{-s}} \le \zeta(s)\,.$$

We complete the proof by deriving the reverse inequality. Fix N. Let $n \le N$. We use the unique factorization into primes to express $n = p_1^{j_1} \ldots p_N^{j_N}$ where of course many of the j_N will be zero. This permits us to estimate:

$$\beta_N(s) = \sum_{n=1}^{N} n^{-s} \le \prod_{j=1}^{N} (1 + p_j^{-s} + \cdots + p_j^{-Ns}) = \alpha_{N,N}(s)\,.$$

Since $\alpha_{N,N}(s) \le \alpha_{k,\ell}(s)$ for $k \ge N$ and $\ell \ge N$, we may take the limit as $\ell \to \infty$ and apply the argument given above interchanging finite products and the limiting process to see

$$\beta_N(s) \le \prod_{j=1}^{k} \frac{1}{1-p_j^{-s}}\,.$$

Since this holds for j arbitrary, we can again take the limit as $k \to \infty$ to see

$$\beta_N(s) \le \prod_{j=1}^{\infty} \frac{1}{1-p_j^{-s}}\,.$$

Since this holds for N arbitrary, we complete the proof by showing

$$\sum_{n=1}^{\infty} n^{-s} = \lim_{N \to \infty} \beta_N(s) \le \prod_{j=1}^{\infty} \frac{1}{1-p_j^{-s}}. \qquad \square$$

Remark 3.8. We can use Theorem 3.7 to show there are an infinite number of primes as follows. Assume to the contrary that there are only a finite number of primes. If the set $\mathcal{P}$ was finite, then the infinite product $\prod_{p \in \mathcal{P}}$ would converge for $\Re(s) > 0$ and provide an analytic extension of $\zeta(s)$ near $s = 1$. This is not possible since $\zeta(s)$ has a simple pole at $s = 1$.

This is, of course, not the argument given by Euclid as we gave earlier. It is, however, the sort of argument we are going to use to show there are an infinite number of primes in any arithmetic progression. To do this, we must generalize the Riemann zeta function, which we shall do presently.

3.7. **Summation by parts.**

L3.9 **Lemma 3.9.** *Let C be a compact subset of $\mathbb{C}$. Let $b_n(x)$ be positive continuous real valued functions on C with $b_1(x) \geq b_2(x) \geq \dots$ so that $b_n(x)$ converges uniformly to 0 on C. Let $a_n(x)$ be continuous complex valued functions on C so that $\sum_n |a_n(x)|$ is uniformly bounded on C. Then $\sum_n a_n(x)b_n(x)$ converges uniformly to a continuous function on C.*

Proof. We set $s_n = a_1 + \dots + a_n$. Choose K so $|s_n| \leq K$ for all n. We use Cauchy's criteria and compute:

$$\begin{aligned}
& |a_n b_n + a_{n+1}b_{n+1} + \dots + a_m b_m| \\
= \; & |(s_{n+1} - s_n)b_n + (s_{n+2} - s_{n+1})b_{n+1} + \dots \\
& + (s_m - s_{m-1})b_{m-1} + (s_{m+1} - s_m)b_m| \\
= \; & | - s_n b_n + s_{n+1}(b_n - b_{n+1}) + \dots + s_m(b_{m-1} - b_m) + s_{m+1}b_m| \\
\leq \; & |s_n b_n| + |s_{m+1}b_m| + K(b_n - b_{n+1}) + \dots + K(b_{m-1} - b_m) \\
\leq \; & K b_n + K b_m + K(b_n - b_m) \leq 2K b_n \,.
\end{aligned}$$

Since $b_n \to 0$ uniformly as $n \to \infty$, we can use Cauchy's criteria to derive the desired result; the uniform limit of continuous functions being continuous. □

3.8. **Generalized zeta functions.** We consider the following subsets:

$$\begin{aligned}
\mathcal{O}_1 &:= \{(s,\lambda) \in \mathbb{C} \times \mathbb{C} : \Re(s) > 1 \text{ and } |\lambda| \leq 1\}, \\
\mathcal{O}_2 &:= \{(s,\lambda) \in \mathbb{R} \times \mathbb{C} : s > 0, |\lambda| \leq 1, \lambda \neq 1\} \,.
\end{aligned}$$

T3.10 **Theorem 3.10.** *Consider the infinite series $\zeta_\lambda(s) := \sum_{n=1}^{\infty} \lambda^n n^{-s}$.*

1. *The series converges absolutely on $\mathcal{O}_1$ and the convergence is uniform on compact subsets of $\mathcal{O}_1$. Thus $\zeta_\lambda(s)$ is continuous on $\mathcal{O}_1$. The function $\zeta_\lambda(s)$ is holomorphic in s and holomorphic in λ for $|\lambda| < 1$.*
2. *The series converges conditionally on $\mathcal{O}_2$ and the convergence is uniform on compact subsets of $\mathcal{O}_2$. Thus $\zeta_\lambda(s)$ is continuous on $\mathcal{O}_2$. The function $\zeta_\lambda(s)$ is holomorphic in s and holomorphic in λ for $|\lambda| < 1$.*

Proof. Since $|\lambda^n| \leq 1$ and $\Re(s) > 1$, Assertion (1) follows since

$$|\lambda^n n^{-s}| \leq |n^{-s}| = n^{-\Re(s)}$$

and $\Re(s) > 1$. If $\lambda \neq 1$, then we set $a_n = \lambda^n$ and $b_n = n^{-s}$. The series b_n is monotonically decreasing and the convergence to zero is uniform on compact subsets of $s > 0$. We have

$$|1 + \lambda + \dots + \lambda^n| = \left| \frac{1 - \lambda^{n+1}}{1 - \lambda} \right| \leq 2(|1 - \lambda|)^{-1} \,.$$

This can be uniformly bounded on compact subsets of the λ domain and the desired result now follows from Lemma 3.9. □

We say that a map $\chi : \mathbb{N} \to \mathbb{C}$ is *multiplicative* if $\chi(n)\chi(m) = \chi(mn)$. We suppose $|\chi(n)| \leq 1$ for all n. We may then define

$$\zeta_\chi(s) = \sum_{n=0}^{\infty} \chi(n) n^{-s} \,.$$

This converges uniformly for $\Re(s) > 1$ to a holomorphic function of s. Theorem 3.7 extends to this situation to yield an infinite product formula

$$\zeta_\chi(s) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \chi(p)p^{-s}} \,.$$

This is considerably more delicate and requires more careful estimates which we omit in the interests of brevity.

3.9. **Regularity of Dirichlet zeta functions.**

T3.11 **Theorem 3.11.**

(1) *Let $\chi:\mathbb{N}\to\mathbb{C}$ be multiplicative. If $\chi(n)=\chi(n+k)$ for all n, then χ arises from a map of $\mathbb{Z}_k\to\mathbb{C}$. The function ζ_χ is regular at $s=1$ if and only if $\langle\rho_0,\chi\rangle=0$.*

(2) *A multiplicative map χ from $\mathbb{Z}_k\to\mathbb{C}$ is said to be a Dirichlet character if $\chi(a)=0$ whenever a and k are not coprime. We say that χ is principal if $\chi(a)=1$ for a and k coprime. If χ is a Dirichlet character, then $\zeta_\chi(s)$ is regular at $s=1$ if and only if χ is not principal.*

Proof. Recall that we defined the characters $\rho_j(n)=e^{2\pi ijn/k}$ and showed these formed an orthonormal basis for $L^2(\mathbb{Z}_k)$. If $\chi:\mathbb{Z}_k\to\mathbb{C}$ is a multiplicative complex function, then we may decompose $\chi=c_0\rho_0+\cdots+c_{k-1}\rho_{k-1}$. This decomposes

$$\zeta_\chi(s)=\sum_{j=0}^{k-1}c_j\zeta_{e^{2\pi ja/k}}(s)\,.$$

Since ζ_λ is regular at $s=1$ for $\lambda\neq1$ whilst ζ_1 has a simple pole at $s=1$, Assertion (2) follows. Let Z_k^* be the set of integers mod k which are coprime to k; this forms a group under multiplication. Suppose χ is a Dirichlet character and suppose that $\chi(a)\neq1$ for some a coprime to 1. We then have

$$\langle\rho_0,\chi\rangle=\frac{1}{k}\sum_{(b,k)=1}\chi(b)=\frac{1}{k}\sum_{(ab,k)=1}\chi(ab)=\chi(a)\langle\rho_0,\chi\rangle\,.$$

This show $(1-\chi(a))\langle\rho_0,\chi\rangle=0$ and hence $\langle\rho_0,\chi\rangle=0$. Thus $\zeta_\chi(s)$ is regular at $s=0$. Conversely, suppose that χ is a principal character. Then

$$\zeta_\chi(s)=\prod_{(p,k)=1}\frac{1}{1-p^{-s}}\text{ so}$$

$$\zeta(s)=\prod_{(p,k)\neq1}\frac{1}{1-p^{-s}}\prod_{(p,k)=1}\frac{1}{1-p^{-s}}=\prod_{(p,k)\neq1}\zeta_\chi(s)\,.$$

Since there are only a finite number of primes dividing k, $\prod_{(p,k)\neq1}\frac{1}{1-p^{-s}}$ is regular for $s\neq0$. Since $\zeta(s)$ has a pole at $s=1$, $\zeta_\chi(s)$ has a pole at $s=1$. □

4. The proof of Dirichlet's Theorem

We break the proof up into a number of steps.

Step 1. Let $\mathcal{O}_2:=\{(s,\lambda)\in[0,\infty)\times\mathbb{C}:|\lambda|\leq1,\lambda\neq1\}$. We have defined

$$\eta_\lambda(s):=\sum_{n=1}^{\infty}\lambda^n n^{-s}\,.$$

We showed in Theorem 3.10 that series converges uniformly on compact subsets of $\mathcal{S}_1$ to a continuous function of (s,λ). Thus if $\lambda^k=1$ and $\lambda\neq1$, then $\lim_{s\to1}\zeta(s,\lambda)$ exists and is finite. Note that the convergence is conditional and not absolute. We also defined

$$\zeta(s)=\sum_{n=1}^{\infty}n^{-s}\,.$$

We showed in Theorem 3.6 that this series converged uniformly on compact subsets of the half-plane $\Re(s)>1$ to a holomorphic function which had a simple pole at $s=1$ with residue 1. In particular $\lim_{s\to1}\zeta(s)=\infty$.

Step 2. Let $\mathbb{Z}_k$ be the ring of integers mod k. Let $\rho_j(a) := e^{2\pi\sqrt{-1}ja/k}$. This defines a group homomorphism from $\mathbb{Z}_k$ to $\mathbb{C}$ and $\tilde{\mathbb{Z}}_k = \{\rho_0, \ldots, \rho_{k-1}\}$. Let $\mathbb{Z}_k^*$ be the subgroup elements coprime to k. We have $\mathbb{Z}_k^*$ is a group under multiplication. Let $\chi \in \hat{\mathbb{Z}}_k^*$. We extend χ to be zero on $\mathbb{Z}_k - \mathbb{Z}_k^*$. Such an element is called a *Dirichlet character*. We say that χ is the *principal Dirichlet character* if and only if $\chi \equiv 1$ on $\mathbb{Z}_k^*$. We defined

$$\zeta_\chi(s) = \sum_{n=1}^{\infty} \chi(n) n^{-s} .$$

We may expand $\chi = \sum_j \ll \chi, \rho_j \gg_{\mathbb{Z}_k} \cdot \rho_j$ and thereby expand

$$\zeta_\chi(s) = \sum_j \ll \chi, \rho_j \gg_{\mathbb{Z}_k} \cdot \zeta(s, \rho_j) .$$

Thus this is regular at $s = 1$ if and only if $\ll \chi, \rho_0 \gg_{\mathbb{Z}_k} = 0$. We showed in Theorem 3.11 that this happens if and only if χ is principal. Thus $\zeta_\chi(s)$ is regular at $s = 1$ if and only if χ is not principal.

Step 3. Let χ be a Dirichlet character. Let $\mathcal{P}$ be the collection of prime numbers ordered in increasing order. If $f : \mathbb{Z}_k \to \mathbb{C}$, define:

$$\zeta_{\mathcal{P}}(s, f) := \sum_{p \in \mathcal{P}} f(p) p^{-s} .$$

If χ is a Dirichlet character, we have the infinite product formula which generalizes the infinite product formula for the Rieman zeta function (and which is proved in a fashion similar to that used to prove Theorem 3.7)

$$\zeta_\chi(s) = \sum_{n=1}^{\infty} \chi(n) n^{-s} = \prod_{p \in \mathcal{P}} \left(\frac{1}{1 - \chi(p) p^{-s}} \right) .$$

We take the log:

$$\log(\zeta_\chi(s)) = -\sum_{p \in \mathcal{P}} \log(1 - \chi(p) p^{-s}) .$$

This shows that $\zeta_{\mathcal{P}}(s, \chi)$ is regular at $s = 1$ if and only if $\zeta_\chi(s)$ is regular at $s = 1$, i.e. χ is not principal. An argument similar to that given to prove Lemma 3.4 then shows this condition is equivalent to the condition

$$\sum_{p \in \mathcal{P}} \chi(p) p^{-s}$$

is regular at $s = 1$.

Step 4. Let a and k have no common divisors. Let

$$f_a(j) = \left\{ \begin{array}{l} 1 \text{ if } j \equiv a \mod k \\ 0 \text{ otherwise} \end{array} \right\} .$$

This is the *skyscraper function* based at a. Note that f_a is supported on $\mathbb{Z}_k^*$. Thus we may use Lemma 3.1 to expand

$$f_a = \sum_{\chi \in \mathbb{Z}_k^*} \ll f_a, \chi \gg_{\mathbb{Z}_k^*} \cdot \chi,$$

$$\sum_{p \in \mathcal{P}, p \equiv a \mod k} p^{-s} = \sum_{\chi \in \hat{\mathbb{Z}}_k^*} \ll f_a, \chi \gg_{\mathbb{Z}_k^*} \cdot \zeta_{\mathcal{P}}(s, \chi) \text{ where}$$

$$\ll f_a, \chi \gg_{\mathbb{Z}_k^*} = \frac{1}{|\mathbb{Z}_k^*|} \chi(a) .$$

Consequently the coefficient of the principal Dirichlet character is non-zero. Since all the other Dirichlet characters are regular at $s = 1$ and the Dirichlet character is not regular at $s = 1$, we conclude $\zeta_{\mathcal{P}}(s, f_a)$ is not regular at $s = 1$. Thus, the sum defining $\zeta_{\mathcal{P}}(s, f_a)$ could not be finite and there are an infinite number of primes congruent to a mod k.

5. Acknowledgements

I wish to thank my advisor, Professor Peter B. Gilkey, and all his associates at the Krill Institute of Technology. This project would not have been possible without their generous help and support.

References

A76 [1] T. Apostol, "Introduction to analytic number theory", Undergraduate Texts in Mathematics, New York-Heidelberg: Springer-Verlag, 1976.

D37 [2] L. Dirichlet, "There are infinitely many prime numbers in all arithmetic progressions with first term and a difference prime", Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1837, 45–81. English translation by Ralf Stephan. Available at arXiv:0808.1408v1.

L75 [3] L. Euler "On the sum of the series formed from the prime numbers where the prime numbers of the form 4n1 have a positive sign and those of the form 4n+1 a negative sign" Opuscula Analytica 2, 1785, 240–256. English translation by Jordan Bell. Available at arXiv:0708.2564

HW [4] G. H. Hardy and E. M. Wright, "An introduction to the theory of numbers. 3rd ed.", Oxford, at the Clarendon Press, 1954.

H56 [5] T. L. Heath, "The thirteen books of Euclid's Elements", Dover Publ., New York, 1956.

H74 [6] C. Hooley "The distribution of sequences in arithmetic progressions." In Proceedings of the International Congress of Mathematicians, vol. 1, 1974, 357-364.

M99 [7] J. E. Marsden and M. J. Hoffman, "Baisc Complex Analysis: Third Edition", W. H. Freeman and Company, 1999.

N00 [8] W. Narkiewicz "The Development of Prime Number Theory: From Euclid to Hardy and Littlewood" Springer., 2000.

BIO [9] J. J. O'Connor and E. F. Robertson "Biographies of Mathematicians", University of Saint Andrew's, Scotland, 1999 Available at http://www-groups.dcs.st-and.ac.uk/

University of Oregon, Eugene OR 97403, USA
E-mail address: jtomcal@uoregon.edu