MTH 391A Project Report
Dirichlet's Theorem

Anurag Sahay
Roll No. 11141
Department of Mathematics and Statistics
IIT Kanpur

16th November, 2013

Abstract

We present a proof of Dirichlet's theorem on the infinitude of primes in arithmetic progressions. This report was submitted as part of the course MTH 391A (Undergraduate Project I) at IIT Kanpur in the 2013-14/Ist Semester, under the supervision of Prof. Shobha Madan.

Contents

1 Introduction

In 1837, Peter Gustav Lejeune Dirichlet, a German mathematician proved that there exists infinitely many prime numbers in any arithmetic progression of integers such that the first term and the common difference of the progression are coprime. In other words, Dirichlet showed that for any integers a and d with $(a, d) = 1$, the sequence

$$a, a + d, a + 2d, a + 3d, \cdots, a + nd \cdots$$

contains infinitely many prime numbers. This theorem is a generalization of Euclid's theorem that there are infinitely many prime numbers (Euclid's theorem is the case $a = d = 1$), and can historically be considered the first result of analytic number theory.

In this note, we provide a proof of Dirichlet's theorem, adapted from [1], with some modifications taken from [2]. We have simplified some of the steps, and have added our commentary with the goal of highlighting the main ideas behind the proof by simplifying the exposition. Several things that are needed for this proof, but do not fit with the rest of the note have been relegated to the appendices. We have assumed basic mathematical maturity, such as familiarity with groups (in particular, we assume the fundamental theorem of finite abelian groups), modular arithmetic, vector spaces over $\mathbb{C}$, basic number theory and uniform convergence.

2 Fourier Analysis on Finite Abelian Groups

The proof of Dirichlet's theorem uses fourier analysis on finite abelian groups, or more particular, fourier analysis on the multiplicative group of integers modulo q, $(\mathbb{Z}/q\mathbb{Z})^\times$. In this section, we shall develop the theory for a general group G, and then apply these to $(\mathbb{Z}/q\mathbb{Z})^\times$ to get the particular results we shall need.

2.1 The Circle Group

Any circle can be endowed with a group structure that is compatible with its geometric and analytic structure (transforming it into what is called a

Lie group). In particular, if we note that the unit circle on the Argand Plane is the set

$$\{z \in \mathbb{C} : |z| = 1\}$$

we see that in fact this subset of the complex numbers is actually a subgroup of $\mathbb{C}$ under multiplication[1]. This circle is denoted by S^1 or $\mathbb{T}$, and is called the circle group.

The fourier analysis of a finite abelian group G is done by studying homomorphisms from G to $\mathbb{T}$.

2.2 Characters of a Group

Suppose $(G, \cdot)$ is a finite abelian group. Then a function $e : G \to \mathbb{T}$ is called a character if, for all $a, b \in G$

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

or, in other words, e is a group homomorphism from G to $\mathbb{T}$. The character given by $e(a) = 1$ for all $a \in G$ is called the "trivial character".

Let us denote the set of all characters of G by $\widehat{G}$. Then $\widehat{G}$ inherits a natural group operation given by

$$(e_1 \cdot e_2)(a) = e_1(a)e_2(a)$$

for all $a \in G$, with the identity given by the trivial character, and the inverse of e given by its conjugate function, $e^{-1}(a) = \overline{e(a)}$ for all $a \in G$.

2.3 The Function Space of G

Let V_G be the set of all functions $f : G \to \mathbb{C}$. V_G is naturally a vector space over $\mathbb{C}$ with the operations of pointwise addition and scalar multiplication. When G is finite, this vector space is finite-dimensional, with dimension $n = |G|$. Furthermore, for any ordering of elements of G, say $a_1, a_2, \cdots, a_n$,

[1]Since $|z_1 z_2| = |z_1||z_2|$ and $|\frac{1}{z}| = \frac{1}{|z|}$.

the space V_G can be naturally identified with the vector space of n-tuples $\mathbb{C}^n$ by associating the function f with the tuple $(f(a_1), f(a_2), \cdots, f(a_n))$. Thus, the space V_G inherits a basis from this identification given by the function f_a for $a \in G$, defined as

$$f_a(x) = \delta_{a,x} = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{if } x \neq a \end{cases}$$

Note that there is no use for the group structure on G in the above, and that in fact, G could be replaced by an arbitrary set S. However, consider the following form on V_G

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{a \in G} f(a)\overline{g(a)}$$

where the sum is over all elements a of G. This can be easily seen to be a positive-definite, conjugate-symmetric and bilinear form, thus defining a Hermitian inner product on V_G. The crucial facts about V_G as an inner product space that we shall need for our proof of Dirichlet's theorem are recorded in the following theorems.

Theorem 2.1. *If h is a non-trivial character of a finite abelian group, then $\sum_{a \in G} h(a) = 0$.*

Proof. As h is non-trivial, there must be some $b \in G$ such that $h(b) \neq 1$. Hence,

$$h(b) \sum_{a \in G} h(a) = \sum_{a \in G} h(b)h(a) = \sum_{a \in G} h(ab) = \sum_{a \in G} h(a)$$

where the last equality follows from the fact that when a ranges over all elements of G, then so does ab. Hence, since $h(b)$ is not 1, the theorem follows. □

Theorem 2.2. *The set of characters forms an orthonormal family for V_G under the above inner product.*

Proof. Clearly, for any character $e \in \widehat{G}$ and any $a \in G$, $|e(a)| = 1$. Hence, $e(a)\overline{e(a)} = |e(a)|^2 = 1$. It thus follows that

$$\langle e, e\rangle = \frac{1}{|G|}\sum_{a\in G} e(a)\overline{e(a)} = \frac{1}{|G|}\sum_{a\in G} 1 = 1$$

Also, suppose $e_1(\neq e)$ is a character, then $h = e\cdot\overline{e_1}$ is a non-trivial character. Applying the previous theorem to h, we get

$$\langle e, e_1\rangle = \frac{1}{|G|}\sum_{a\in G} e(a)\overline{e_1(a)} = 0$$

Hence,

$$\langle e, e_1\rangle = \begin{cases} 1 & \text{if } e = e_1 \\ 0 & \text{if } e \neq e_1 \end{cases}$$

or,

$$\frac{1}{|G|}\sum_{a\in G} e(a)\overline{e_1(a)} = \begin{cases} 1 & \text{if } e = e_1 \\ 0 & \text{if } e \neq e_1 \end{cases}$$

□

Since the characters form an orthonormal family, they must be linearly independent, and hence their cardinality$(=\widehat{G})$ is $\leq |G|$, the dimension of V_G. We can show in fact that they form a basis by showing that $|\widehat{G}| = |G|$. This can be done easily by explicitly noting that for the additive group of integers modulo q, $|\widehat{G}| = |G|$, noting that $\widehat{G_1 \times G_2}$ is isomorphic to $\widehat{G_1} \times \widehat{G_2}$ and invoking the fundamental theorem of finite abelian groups. We omit the details of this proof, see the Chapter 7 Problems of [1] for more information.

Now, since the characters form an orthonormal basis for V_G, for any function $f \in V_G$, we can write it uniquely as

$$f = \sum_{e\in\widehat{G}} \langle f, e\rangle e$$

Now consider the functions f_a we had considered earlier. Clearly,

$$\langle f_a, e\rangle = \frac{1}{|G|}\sum_{b\in G} f_a(b)\overline{e(b)} = \frac{\overline{e(a)}}{|G|}$$

Hence,

$$f_a(b) = \sum_{e\in\widehat{G}} \langle f_a, e\rangle e(b) = \sum_{e\in\widehat{G}} \frac{\overline{e(a)}}{|G|} e(b)$$

Or, in other words,

$$\frac{1}{|G|}\sum_{e\in\widehat{G}} e(a)\overline{e(b)} = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{if } a \neq b \end{cases}$$

We note the similarity between this identity and the orthogonality of characters.

3 Euclid's Theorem

We now move to a proof of Euclid's theorem due to Euler that encapsulate many ideas that shall be used in our proof of Dirichlet's theorem. Euclid's theorem, which states that there are infinitely many prime numbers has a elementary proof known since classical times. However, Euler provided an "analytical" proof of the theorem. He considered the limit

$$\lim_{s\to 1^+}\sum_p \frac{1}{p^s}$$

where the sum is over all primes p, and showed that this limit is ∞. If there were only finitely many primes, then this would not be possible, hence proving the infinitude of primes.

We will now prove that the limit above is actually ∞.

3.1 The Riemann Zeta Function

For any real number $s > 1$, we define the Riemann zeta function,

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

We can see this function converges by noting that

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \sum_{n=2}^{\infty} \int_{n-1}^{n} \frac{dx}{n^s} \leq 1 + \sum_{n=2}^{\infty} \int_{n-1}^{n} \frac{dx}{x^s} = 1 + \int_{1}^{\infty} \frac{dx}{x^s}$$

Thus,

$$\zeta(s) \leq 1 + \frac{1}{s-1}$$

is convergent for all $s > 1$.

The zeta function encodes in it a lot of information about the distribution of primes among the integers. In particular, it can be extended to a holomorphic function on the entire complex plane except for $s = 1$, where it has a simple pole. The distribution of zeroes of this extensison is intimately connected to the distribution of primes and the Riemann Hypothesis, one of the biggest unsolved problems in mathematics is a statement about these zeroes.

3.2 Euler Product

Notwithstanding the holomorphic extension, the zeta function we have defined itself encodes a lot about the primes. In particular, the zeta function admits a product formula which is essentially an analytic statement of the fundamental theorem of arithmetic. This product formula, known as the Euler product of $\zeta(s)$ is given in the following theorem.

Theorem 3.1. *For every $s > 1$,*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - 1/p^s}$$

where the product is over all primes p.

Proof. Suppose M and N are positive integers such that $M > N$. Every $n \leq N$ can be uniquely written as a product of primes. These primes shall obviously be $\leq N$, and cannot occur more than M times in the product. Hence, it follows that every term in the left of the following inequality shall also be in the right of the inequality. That is,

$$\sum_{n=1}^{N} \frac{1}{n^s} \leq \prod_{p \leq N} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots + \frac{1}{p^{Ms}}\right)$$

Taking first $M \to \infty$ and then $N \to \infty$ in the left, we get

$$\sum_{n=1}^{N} \frac{1}{n^s} \leq \prod_{p} \left(\frac{1}{1 - p^{-s}}\right)$$

Finally, taking $N \to \infty$,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \leq \prod_{p} \left(\frac{1}{1 - p^{-s}}\right)$$

For the reverse inequality, note that if we consider all products of primes such that each prime is $\leq N$ and does not occur more than M times, we shall get finitely many distinct integers. Thus,

$$\prod_{p \leq N} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots + \frac{1}{p^{Ms}}\right) \leq \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Again, taking $M \to \infty$ and then $N \to \infty$, we obtain

$$\prod_{p} \left(\frac{1}{1 - p^{-s}}\right) \leq \sum_{n=1}^{\infty} \frac{1}{n^s}$$

The equality follows from these two inequalites. $\square$

3.3 Proof of Euclid's Theorem

We are now in a position to prove Euclid's theorem.

Theorem 3.2. *We have,*

$$\lim_{s\to 1^+} \sum_p \frac{1}{p^s} = \infty$$

where the sum is taken over all primes p.

Proof. Taking the natural logarithm of both sides of the Euler product, and using the continuity of logarithms,

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

Since $\log(1+x) = x + O(x^2)$, we get,

$$-\sum_p \left[-\frac{1}{p^s} + O\left(\frac{1}{p^{2s}}\right)\right] = \log\zeta(s)$$

Thus, since $\sum_p 1/p^{2s} \leq \sum_n 1/n^{2s}$, which is convergent, and hence bounded,

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

Now, $\zeta(s) \geq \sum_{n=1}^M 1/n^s$ for every M. Hence,

$$\liminf_{s\to 1^+} \zeta(s) \geq \sum_{n=1}^M \frac{1}{n}$$

for every M. Clearly, since the harmonic series diverges, the right side is unbounded. Thus, $\lim_{s\to 1^+} \zeta(s) = \infty$.

Combining this with the earlier estimate on $\sum_p 1/p^s$, we get that

$$\lim_{s \to 1^+} \sum_p \frac{1}{p^s} = \infty$$

$\square$

4 Dirichlet Characters

In this section, we will connect the previous two sections to give a sketch of our proof of Dirichlet's theorem.

Fix a positive integer q and Consider the group $(\mathbb{Z}/q\mathbb{Z})^\times$. Our aim is to show that every congruence class modulo q that is coprime to q contains infinitely many prime numbers. Clearly, this will imply the infinitude of primes in arithmetic progressions.

The basic tool in the proof shall be the so-called "Dirichlet characters" modulo q, which are a generalization of characters of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$. Let e be a character of $(\mathbb{Z}/q\mathbb{Z})^\times$. We define $\chi : \mathbb{Z} \to \mathbb{C}$ as

$$\chi(n) = \begin{cases} e([n]) & \text{if } (n,q) = 1 \\ 0 & \text{if } (n,q) > 1 \end{cases}$$

Hence, wherever it makes meaningful sense to assign $e(n)$, we use $e(n)$ and everywhere else we use 0. This χ is called a Dirichlet character modulo q.

If e is the trivial character, it gives rise to the principal Dirichlet character χ_0

$$\chi_0(n) = \begin{cases} 1 & \text{if } (n,q) = 1 \\ 0 & \text{if } (n,q) > 1 \end{cases}$$

All other characters are called non-principal Dirichlet characters.

It is trivially seen that $\chi(n)$ is periodic, with period q. Furthermore, for any $m, n \in \mathbb{Z}$, we have

$$\chi(mn) = \chi(m)\chi(n)$$

as can be verified.

Now, we shall adapt our theorems for groups characters to Dirichlet characters.

Theorem 4.1. *For any non-trivial Dirichlet character modulo q, we have*

$$\sum_{n=1}^{q} \chi(n) = 0$$

Proof. Since $\chi(n) = 0$ if $(n, q) > 1$, we have

$$\sum_{n=1}^{q} \chi(n) = \sum_{\substack{1 \le n \le q \\ (a,q)=1}} \chi(n) = \sum_{\substack{1 \le n \le q \\ (a,q)=1}} e([n]) = \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^{\times}} e(a)$$

Where the last equality follows from the fact that n varies over the given domain, $[n]$ goes traverses all the elements of $(\mathbb{Z}/q\mathbb{Z})^{\times}$. Thus invoking the fact about group characters that $\sum_{a \in G} e(a) = 0$, we get

$$\sum_{n=1}^{q} \chi(n) = 0$$

□

Theorem 4.2. *For any $m, n \in \mathbb{Z}$,*

$$\sum_{\chi} \chi(m)\overline{\chi(n)} = \begin{cases} \phi(q) & \text{if } m \equiv n \pmod{q} \text{ and } (n,q) = 1 \\ 0 & \text{otherwise} \end{cases}$$

where the sum is over all Dirichlet characters modulo q.

Proof. First, note that if $(n, q) > 1$, $\chi(n) = 0$ for all χ. Hence, the sum clearly equals 0. Similarly, we see that if $(m, q) > 1$, the sum is 0. Hence, suppose that $(n, q) = (m, q) = 1$.

Thus, we can go from Dirichlet characters to group characters as

$$\sum_{\chi} \chi(m)\overline{\chi(n)} = \sum_{e \in \widehat{G}} e([m])\overline{e([n])}$$

By the previously proven results, the last sum is 0 unless $[m] = [n]$, or in other words, $m \equiv n \pmod q$. In that case, the sum is $|(\mathbb{Z}/q\mathbb{Z})^\times| = \phi(q)$. Hence the theorem follows. $\square$

At this point, we would like to note the use of this theorem. In essence, this theorem states that if $(n, q) = 1$, we can pick out the congruence class containing n by doing a sum over all Dirichlet characters. This shall be useful later, as it shall let us convert intractable sums over integers in a congruence class into double sums over characters and *all* integers. Sums of this type are easier to handle when we have information about the Dirichlet characters (as shall be seen in this proof).

We now state and prove the final property of Dirichlet characters that we shall need.

Theorem 4.3. *For any non-principal Dirichlet character χ, and any integer k, we have*

$$\left| \sum_{n \le k} \chi(n) \right| \le q$$

Proof. Clearly, by previous theorems and the periodicity of χ, if we write $k = aq + b$, with $b < q$

$$\sum_{n \le k} \chi(n) = \sum_{n \le aq} \chi(n) + \sum_{aq < n \le aq+b} \chi(n) = \sum_{n \le b} \chi(n)$$

Thus, by the triangle inequality,

$$\left| \sum_{n \le k} \chi(n) \right| \le \sum_{n \le b} |\chi(n)| \le b \le q$$

$\square$

4.1 Adapting Euler's Proof of Euclid's Theorem

We can now see how Euler's proof for Eulcid's theorem may be adapted here. Fix integers q and a such that $(a, q) = 1$. We consider the following limit

$$\lim_{s\to 1^+} \sum_{p\equiv a \pmod q} \frac{1}{p^s}$$

where the sum is now only over all primes in the same congruence class as a modulo q. Our attempt shall be to show that this limit is ∞, which would, analogous to Euclid's theorem, show that there are infinitely many primes in that congruence class.

As stated before, sums over elements in a particular congruence class are normally intractable. However, using a trick, we can reduce these sums to over all prime p.

Now, since $(a, q) = 1$, we have that

$$\frac{1}{\phi(q)} \sum_{\chi} \chi(p)\overline{\chi(a)} = \begin{cases} 1 & \text{if } p \equiv a \pmod q \\ 0 & \text{otherwise} \end{cases}$$

Hence, we can rewrite the sum as

$$\sum_{p\equiv a \pmod q} \frac{1}{p^s} = \sum_{p} \frac{1}{\phi(q)} \sum_{\chi} \frac{\chi(p)\overline{\chi(a)}}{p^s}$$

Since everything converges uniformly and absolutely for $s > s_0 > 1$, we can rewrite this as

$$\sum_{p\equiv a \pmod q} \frac{1}{p^s} = \frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)} \sum_{p} \frac{\chi(p)}{p^s}$$

Hence, it suffices to study the behaviour of $\sum_p \chi(p)/p^s$ as $s \to 1^+$.

Now, the sum can be rewritten as

$$\sum_{p\equiv a \pmod q} \frac{1}{p^s} = \frac{1}{\phi(q)} \sum_{p} \frac{\chi_0(p)}{p^s} + \frac{1}{\phi(q)} \sum_{\chi\neq\chi_0} \overline{\chi(a)} \sum_{p} \frac{\chi(p)}{p^s}$$

where the second sum is over non-prinicipal characters.

Clearly,

$$\sum_p \frac{\chi_0(p)}{p^s} = \sum_{p \nmid q} \frac{1}{p^s}$$

Since there are only finitely many primes dividing q, this last sum goes to infinity as $s \to 1^+$, as in the proof of Euclid's theorem. Thus, if we show that as $s \to 1^+$, the non-principal part is bounded (that is, $\sum_p \chi(p)/p^s = O(1)$),the theorem is proved.

Hence, we see that by careful use of Dirichlet characters, we have reduced our problem to a sum over all primes p.

4.2 Sketch of the Proof

We shall now sketch a proof of the fact that for non-principal characters, $\sum_p \chi(p)/p^s = O(1)$ as $s \to 1^+$. This shall be similar to the proof of Euclid's theorem, using the zeta function.

In place of $\zeta(s)$, we will consider a generalization associated with each character χ called the Dirichlet L-function, $L(s,\chi)$, given by

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

wherever the series converges.

Similar to $\zeta(s)$, there exists an Euler product formula for $L(s,\chi)$ viz.

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)/p^s}$$

Taking logarithms on both sides, we get

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

Using $\log(1+x) = x + O(x^2)$,

$$\log L(s,\chi) = -\sum_p \left[-\frac{\chi(p)}{p^s} + O\left(\frac{1}{p^{2s}}\right) \right]$$

Thus, we get

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

Hence, if $L(1,\chi)$ is finite and non-zero, and $L(s,\chi)$ is continuous, then the left of this equation will be bounded as $s \to 1^+$, and hence $\sum_p \chi(p)/p^s$ is bounded.

In the above argument, there are several holes we need to fill to make the argument rigorous. Firstly, we need to prove the product formula for $L(s,\chi)$; secondly, since the numbers involved may, in general, be complex numbers, we need to clearly define the branch of the logarithm we are using and its properties; thirdly, we need to show that $L(s,\chi)$ is continuous at $s=1$; and finally, we need to show that $L(1,\chi) \neq 0$.

5 Reducing Dirichlet's Theorem to $L(1,\chi) \neq 0$

We shall first fill in the other holes in the argument. By doing this, we are essentially saying proving that Dirichlet's theorem follows from the non-vanishing of $L(1,\chi)$ for any character χ. We shall deal with the problem of logarithms by defining two logarithms, one for the function $L(s,\chi)$, and the other for elements of the form $\frac{1}{1-z}$.

5.1 The First Logarithm

We define our first logarithm, $\log_1$ as

$$\log_1\left(\frac{1}{1-z}\right) = \sum_{k=1}^{\infty} \frac{z^k}{k}$$

for $|z| < 1$. Clearly in the chosen domain, this function converges absolutely.

Theorem 5.1. *If* $|z| < 1$*, then*

$$e^{\log_1\left(\frac{1}{1-z}\right)} = \frac{1}{1-z}$$

Proof. Let $z = re^{i\theta}$. Note that it is sufficient to show that $(1-re^{i\theta})e^{\sum_{k=1}^{\infty}(re^{i\theta})^k/k}$ is constant (since putting $r = 0$ gives 1, as it should).

Thus, differentiating this we get

$$\left[-e^{i\theta} + (1-re^{i\theta})e^{i\theta}\left(\sum_{k=1}^{\infty}(re^{i\theta})^{k-1}\right)\right]e^{\sum_{k=1}^{\infty}(re^{i\theta})^k/k}$$

A quick calculation using the sum of an infinite geometric series shows that the term in the square brackets is zero, hence we are done. □

5.2 Euler Product

We now prove the Euler product for $L(s, \chi)$.

Theorem 5.2. *For any character* χ *and* $s > 1$*,*

$$L(s, \chi) = \sum_n \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)/p^s}$$

Proof. Clearly, the product converges since $\sum_p \chi(p)/p^s$ converges. Let us represent the sum over positive integeres by Σ and the product as Π. Further, define

$$\Sigma_N = \sum_{n \le N} \frac{\chi(n)}{n^s}$$

$$\Pi_N = \prod_{p \le N}\left(\frac{1}{1-\chi(p)/p^s}\right)$$

$$\Pi_{N,M} = \prod_{p \le N}\left(1 + \frac{\chi(p)}{p^s} + \cdots + \frac{\chi(p^M)}{p^{Ms}}\right)$$

Now, fix $\epsilon > 0$. Clearly, since the product is finite, $\lim_{M\to\infty} \Pi_{N,M} = \Pi_N$. Furthermore, since the sum and product converge, $\lim_{N\to\infty} \Pi_N = \Pi$ and $\lim_{N\to\infty} \Sigma_N = \Sigma$. Hence, we can choose N and M large enough that

$$|\Pi_{N,M} - \Pi_N| < \epsilon$$

$$|\Pi_N - \Pi| < \epsilon$$

$$|\Sigma_N - \Sigma| < \epsilon$$

Furthermore, by the fundamental theorem of arithmetic, and the multiplicativity of the Dirichlet characters, for large enough M, $\Pi_{M,N} - \Sigma_N$ is the tail end of a convergent series, and can thus be made $< \epsilon$.

Hence,

$$|\Sigma - \Pi| \leq |\Sigma_N - \Sigma| + |\Pi_{M,N} - \Sigma_N| + |\Pi_{N,M} - \Pi_N| + |\Pi_N - \Pi| < 4\epsilon$$

for any $\epsilon > 0$. Thus, clearly $\Sigma = \Pi$. □

5.3 Behaviour of $L(s, \chi)$

In this section, we examine the behaviour of $L(s, \chi)$.

Theorem 5.3. *If χ_0 is the principal character modulo q, then*

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

where the product is over all primes p dividing q.

Proof. This trivially follows from the Euler products of the two sides.

□

Thus, in some sense, the behaviour of the L-function associated with the principal Dirichlet character is the same as the zeta function. For non-principal characters, the situation is very different.

Theorem 5.4. *If χ is a non-principal character, then $L(s,\chi)$ exists for $s>0$. Moreover, it is continuously differentiable for $0<s<\infty$, and there exists constants $c,c'>0$ such that as $s\to\infty$*

$$L(s,\chi) = 1 + O(e^{-cs})$$

$$L'(s,\chi) = O(e^{-c's})$$

Proof. Suppose $s>0$. Using summation by parts[2]

$$\sum_{n\le N}\frac{\chi(n)}{n^s} = \frac{1}{N^s}\sum_{n\le N}\chi(n) + \int_0^N \left(\sum_{n\le x}\chi(n)\right)\left(\frac{-s}{x^{s+1}}\right)dx$$

Note that since $\left|\sum_{n\le N}\chi(n)\right| \le q$, the first term goes to zero as $N\to\infty$. Furthermore, the integral is bounded above by the integral $\int \frac{qs}{x^{s+1}}dx$, which clearly converges for $s+1>1$ (that is $s>0$) when $N\to\infty$. Hence, the partial sums of the series converges, and hence $L(s,\chi)$ exists for $s>0$. Furthermore, the series converges uniformly for $s>\sigma>0$. We can apply a similar argument to show that the term-wise derivative also converges uniformly for $s>\sigma>0$, proving that $L(s,\chi)$ is continuously differentiable.

□

With this, we can now define our second logarithm.

5.4 The Second Logarithm

We define our second logarithm, $\log_2$ as

$$\log_2 L(s,\chi) = -\int_s^\infty \frac{L'(t,\chi)}{L(t,\chi)}dt$$

[2]See appendices

Theorem 5.5. *If $s > 1$,*

$$e^{\log_2 L(s,\chi)} = L(s,\chi)$$

Proof. Differentiating $e^{-\log_2 L(s,\chi)} L(s,\chi)$ with respect to s, we get

$$-\frac{L'(s,\chi)}{L(s,\chi)} e^{-\log_2 L(s,\chi)} L(s,\chi) + e^{-\log_2 L(s,\chi)} L'(s,\chi) = 0$$

Hence $e^{-\log_2 L(s,\chi)} L(s,\chi)$ is constant. Taking $s \to \infty$, this is easily seen to be 1. $\square$

We can now connect our two logarithms to show that we can meaningfully "take logarithms on both sides" of the Euler product for $L(s,\chi)$.

Theorem 5.6. *If $s > 1$,*

$$\log_2 L(s,\chi) = \sum_p \log_1 \left(\frac{1}{1 - \chi(p)/p^s} \right)$$

Proof. We see that

$$e^{\sum_p \log_1 \left(\frac{1}{1-\chi(p)/p^s} \right)} = \prod_p e^{\log_1 \left(\frac{1}{1-\chi(p)/p^s} \right)} = \prod_p \left(\frac{1}{1 - \chi(p)/p^s} \right)$$

The right most quantity is, by the Euler product, $L(s,\chi)$.

Also,

$$e^{\log_2 L(s,\chi)} = L(s,\chi)$$

Hence, since their exponential is the same, they must differ by some integer multiple of 2π. That is,

$$\log_2 L(s,\chi) - \sum_p \log_1 \left(\frac{1}{1 - \chi(p)/p^s} \right) = 2\pi M(s)$$

Now, clearly, the left side of the equality is a continuous function of s. Hence, $M(s)$ is an integer valued continuous function, and thus constant. Taking $s \to \infty$, this is clearly 0.

$\square$

Putting all of this together, the proof sketch given earlier can be formalized by filling the holes in the argument with these patches.

Therefore, to prove this theorem, we need to establish that $L(1, \chi) \neq 0$.

6 The Non-vanishing of the L-function

We shall now prove that $L(1, \chi) \neq 0$ for all non-principal Dirichlet characters. We shall distinguish between two types of characters. If a character χ is always real, (that is $\chi(n) = 0, +1, -1$ or, to put it another way $\chi(n) = \overline{\chi(n)}$), we call it a real character. A character which is not a real character is called a complex character. We shall treat these two separately.

6.1 Complex Characters

Suppose χ_1 is a complex Dirichlet character such that $L(1, \chi_1) = 0$. We will now derive a contradiction.

For $s > 1$, define f as follows

$$f(s) = \prod_{\chi} L(s, \chi)$$

where the product is taken over all Dirichlet characters modulo q.

Theorem 6.1. *If $s > 1$, $f(s)$ is real-valued, and furthermore*

$$f(s) \geq 1$$

Proof. We know that

$$L(s,\chi) = \exp\left(\sum_p \log_1\left(\frac{1}{1-\chi(p)p^{-s}}\right)\right)$$

Hence,

$$\prod_\chi L(s,\chi) = \exp\left(\sum_\chi \sum_p \log_1\left(\frac{1}{1-\chi(p)p^{-s}}\right)\right)$$

Now, using the definition of $\log_1$ and the multiplicativity of χ,

$$\prod_\chi L(s,\chi) = \exp\left(\sum_\chi \sum_p \sum_{k=1}^{\infty} \frac{1}{k}\frac{\chi(p^k)}{p^{ks}}\right)$$

Now, we can rearrange the summation to get

$$\prod_\chi L(s,\chi) = \exp\left(\sum_p \sum_{k=1}^{\infty} \frac{1}{kp^{ks}} \sum_\chi \chi(p^k)\right)$$

However, from a previous theorem we know that $\sum_\chi \chi(n)$ is either 0 or $\phi(q)$, and thus is a real non-negative quantity. Hence, the term in the exponential shall be a sum over non-negative quantities and, thus non-negative. This implies that its exponential shall be real and greater than 1.

$\square$

Now we know that $L(1,\chi_1) = 0$, that is $L(s,\chi_1)$ has a zero of order at least 1. Hence, to compensate for that, some other L-function in the product must be diverging to infinity. We know that $L(s,\chi_0)$ has a pole of order 1 at $s = 1$, since $\zeta(s)$ has a pole of order 1. However, if $L(1,\chi_1) = 0$, then $L(1,\overline{\chi_1}) = \overline{L(1,\chi_1)} = 0$, and hence, $L(1,\overline{\chi_1})$ also has a zero of order at least 1 at $s = 1$. However, these are all distinct terms in the product, and no other term in the product can diverge to infinity (since we have show that for non-principal characters, their L-functions are well-defined and bounded at $s = 1$). Hence, the product $f(s)$ has a zero of at least order 1 at $s = 1$, contradicting the above theorem.

The above contradiction shall yield that no complex character can satisfy $L(1,\chi_1) = 0$. Note that the above proof does not work for real characters as for them $\chi = \overline{\chi}$, and thus we can only show that one L-function in the product vanishes, which is not sufficient to make the entire product vanish.

We formalize the above argument in the following theorems.

Theorem 6.2. *If* $L(1, \chi_1) = 0$ *then* $L(1, \overline{\chi_1}) = 0$.

Proof. It is easy to see from their definitions that $L(1, \overline{\chi_1}) = \overline{L(1, \chi_1)}$, from which the claim follows.

□

Theorem 6.3. *If* χ *is a non-principal character, such that* $L(1, \chi) = 0$, *then*

$$L(s, \chi) = O(s - 1)$$

as $s \to 1$.

Proof. Applying the mean-value theorem on $L(s, \chi)$ in $1 \leq s \leq 2$, we get that for some $t \in (1, s)$

$$L(s, \chi) - L(1, \chi) = L'(t, \chi)\,(s - 1)$$

Now note that $|L'(s, \chi)|$ is continuos and thus has a maximum (say C) on $[1, 2]$. Furthermore, $L(1, \chi) = 0$.

Hence for $1 \leq s \leq 2$,

$$|L(s, \chi)| \leq C|s - 1|$$

proving the claim.

□

Theorem 6.4. *For the principal Dirichlet character* χ_0, *we have*

$$L(s, \chi_0) = O\left(\frac{1}{s - 1}\right)$$

as $s \to 1$.

Proof. We know that

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

Also, clearly as $s \to 1$, the terms in the product are $O(1)$.

However, we have shown earlier that for $s > 1$

$$\zeta(s) < 1 + \frac{1}{s-1}$$

Putting this together, clearly $L(s,\chi_0) = O(1/(s-1))$.

□

Theorem 6.5. *For any complex character χ_1, $L(1,\chi_1) \neq 0$.*

Proof. We know that for χ $(\neq \chi_0, \chi_1, \overline{\chi_1})$, $L(s,\chi)$ exists and is bounded. That is $L(s,\chi) = O(1)$ as $s \to 1$. Now,

$$f(s) = \prod_{\chi} L(s,\chi) = L(s,\chi_0)L(s,\chi_1)L(s,\overline{\chi_1}) \prod_{\chi \neq \chi_0,\chi_1,\overline{\chi_1}} L(s,\chi)$$

Therefore, by our theorems

$$f(s) = O\left(\frac{1}{s-1}\right) \times O(s-1) \times O(s-1) \times O(1) = O(s-1)$$

Therefore, at $s = 1$, $f(s) = 0 < 1$, contradicting our previous theorem.

□

6.2 Real Characters

We now move on to the final, and the deepest part of this theorem, the proof that for real characters χ, $L(1,\chi) \neq 0$.

Define $S(x)$ as follows

$$S(x) = \sum_{mn \leq x} \frac{\chi(n)}{(mn)^{1/2}}$$

We will obtain two different asymptotic formulae for $S(x)$ which shall establish our theorem.

Before that, we shall prove the facts we need to establish the formulae.

Theorem 6.6. *Suppose that χ is a real Dirichlet character and n is any positive integer. Then,*

$$\sum_{d|n} \chi(d) \geq \begin{cases} 0 & \textit{for all } n \\ 1 & \textit{if } n = t^2, t \in \mathbb{Z} \end{cases}$$

Proof. Note that since χ is multiplicative absolutely,

$$\sum_{d|n} \chi(d) = \prod_{p^a || n} \left(\sum_{k=0}^{a} \chi(p^a) \right)$$

Where $p^a || n$ denotes that p is a prime dividing n such that a is the largest exponent for which p^a divides n.

Hence, clearly, it is sufficient to establish this fact for prime powers, to establish it in general.

Now for $n = p^a$, clearly,

$$\sum_{d|n} \chi(d) = \chi(1) + \chi(p) + \chi(p^2) + \cdots + \chi(p^a) = \chi(1) + \chi(p) + \chi(p)^2 + \cdots + \chi(p)^a$$

Clearly, since $\chi(p)$ is $0, 1, -1$,

$$\sum_{d|n} \chi(d) = \begin{cases} a+1 & \text{if } \chi(p) = 1 \\ 0 & \text{if } \chi(p) = -1 \text{ and } a \text{ is odd} \\ 1 & \text{if } \chi(p) = -1 \text{ and } a \text{ is even} \\ 1 & \text{if } \chi(p) = 0 \end{cases}$$

Thus, we see that this sum satisfies the inequality for prime powers, and thus for all positive integers.

□

With this, we can establish a lower bound on the growth rate of $S(x)$.

Theorem 6.7. *We have,*

$$S(x) \gg \log x$$

In particular $S(x) \to \infty$ as $x \to \infty$.

Proof. The defining formula of $S(x)$ can clearly be rewritten the following way,

$$S(x) = \sum_{n \leq x} \sum_{d|n} \frac{\chi(d)}{n^{1/2}}$$

where we have replaced mn by n and n by d.

Hence, clearly

$$S(x) = \sum_{n \leq x} \frac{1}{n^{1/2}} \sum_{d|n} \chi(d)$$

Now, using the bound earlier established, we know the inner sum is greater than 0 always, and greater than 1 for square n. Hence,

$$S(x) \geq \sum_{\substack{n \leq x \\ n = t^2, t \in \mathbb{Z}}} \frac{1}{n^{1/2}}$$

Or, in other words,

$$S(x) \geq \sum_{t^2 \leq x} \frac{1}{t} = \sum_{t \leq x^{1/2}} \frac{1}{t} \gg \log x$$

□

We shall now use Dirichlet's hyperbola method[3] to prove an asymptotic formula for $S(x)$.

Theorem 6.8.
$$S(x) = 2x^{1/2}L(1,\chi) + O(1)$$

Proof. Note that the defining formula for $S(x)$ can be written as follows

$$S(x) = \sum_{n\leq x}\sum_{d|n} \frac{\chi(d)}{d^{1/2}} \frac{1}{\left(\frac{n}{d}\right)^{1/2}}$$

Thus, taking $g(n) = \chi(n)/\sqrt{n}$, $h(n) = 1/\sqrt{n}$ and $y = \sqrt{x}$, in Dirichlet's hyperbola method,

$$S(x) = \sum_{d\leq\sqrt{x}} \frac{\chi(d)}{d^{1/2}} H\left(\frac{x}{d}\right) + \sum_{d\leq\sqrt{x}} \frac{1}{d^{1/2}} G\left(\frac{x}{d}\right) - G(\sqrt{x})H(\sqrt{x})$$

Where by partial summation[4],

$$G(x) = \sum_{n\leq x} \frac{\chi(n)}{n^{1/2}} = O\left(\frac{1}{x^{1/2}}\right)$$

and

$$H(x) = \sum_{n\leq x} \frac{1}{n^{1/2}} = 2\sqrt{x} + O\left(\frac{1}{x^{1/2}}\right) = O(x^{1/2})$$

Therefore, $G(\sqrt{x})H(\sqrt{x}) = O(1)$. Furthermore,

$$\sum_{d\leq\sqrt{x}} \frac{1}{d^{1/2}} G\left(\frac{x}{d}\right) = \sum_{d\leq\sqrt{x}} \frac{1}{d^{1/2}} \times O\left(\frac{1}{(x/d)^{1/2}}\right) = O\left(\sum_{d\leq\sqrt{x}} \frac{1}{d^{1/2}} \frac{d^{1/2}}{x^{1/2}}\right) = O(1)$$

Hence the main term comes from the first part of the sum. That is,

[3] See appendix
[4] See appendix

$$\sum_{d\le\sqrt{x}} \frac{\chi(d)}{d^{1/2}} H\left(\frac{x}{d}\right) = \sum_{d\le\sqrt{x}} \frac{\chi(d)}{d^{1/2}} \left(2\frac{x^{1/2}}{d^{1/2}} + O\left(\frac{d^{1/2}}{x^{1/2}}\right)\right)$$

Now, note that the error term, when multiplied out evaluates to $O(\sum_{d\le\sqrt{x}} \chi(d)) = O(1)$, by the previous bound on character sums.

Further, the main term evaluates to

$$2x^{1/2} \sum_{d\le\sqrt{x}} \frac{\chi(d)}{d}$$

Now,

$$\sum_{d\le\sqrt{x}} \frac{\chi(d)}{d} = \sum_{d=1}^{\infty} \frac{\chi(d)}{d} - \sum_{d>\sqrt{x}} \frac{\chi(d)}{d} = L(1,\chi) + O\left(\frac{1}{x^{1/2}}\right)$$

where the error term is obtained by partial summation. Thus,

$$2x^{1/2} \sum_{d\le\sqrt{x}} \frac{\chi(d)}{d} = 2x^{1/2} L(1,\chi) + O(1)$$

Putting all the estimates together, we get

$$S(x) = 2\sqrt{x} L(1,\chi) + O(1)$$

□

This, estimate, together with the previously obtained lower bound are sufficient to establish the theorem. To see this, note that by the lower bound, $S(x)$ is unbounded as x goes to infinity. Suppose $L(1,\chi) = 0$. The estimate we have obtained then reduces to $S(x) = O(1)$, contradicting the unboundedness of $S(x)$.

Putting all of this together, we have obtained Dirichlet's theorem.

A Appendix

In the appendix, we shall collect a few facts and definitions that are needed for the note but do not fit in the body.

A.1 Asymptotic Notation

In this note, we have used two asymptotic notations. The first one, called the big O notation is as follows

$$f(x) = O(g(x))$$

if for some constant C,

$$|f(x)| \leq C|g(x)|$$

for x close to the limiting point (which can be infinity, 0 or 1 in this note).

We also use $f(x) \ll g(x)$ for the same purpose.

A.2 $(\mathbb{Z}/q\mathbb{Z})^\times$

We shall elaborate on how we define our group $(\mathbb{Z}/q\mathbb{Z})^\times$. In this note, we define $\mathbb{Z}/q\mathbb{Z}$ as the quotient ring formed by quotienting $\mathbb{Z}$ by the ideal $q\mathbb{Z}$. For any $n \in \mathbb{Z}$, we denote by $[n]$ the equivalence class in $\mathbb{Z}/q\mathbb{Z}$ containing n. That is, $[n] = n + q\mathbb{Z}$. $(\mathbb{Z}/q\mathbb{Z})^\times$ is then the group of units of this ring.

It is easy to see that the size of this group is equal to Euler's totient function, $\phi(q)$.

A.3 Logarithm

We shall prove a property of the logarithm we frequently used in the note.

Theorem A.1. *For $x > 0$, we have*

$$\log(1 + x) = x + O(x^2)$$

as $x \to 0$.

Proof. Suppose $|x| < 1/2$. Therefore, we can use the power series of $\log(1+x)$ around zero. That is

$$\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}x^n}{n}$$

Therefore,

$$|\log(1+x) - x| \leq \frac{x^2}{2}(1 + |x| + |x|^2 + \cdots)$$

Hence, since $|x| < 1/2$,

$$|\log(1+x) - x| \leq \frac{x^2}{2}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right) = \frac{x^2}{2}\left(\frac{1}{1 - 1/2}\right) = x^2$$

Hence, we get

$$\log(1+x) = x + O(x^2)$$

□

Note that this same proof shall work for the first logarithm defined for complex numbers.

A.4 Partial Summation

We now give an account for partial summation, which is used liberally in this note. In general, partial summation or summation by parts is an identity similar to integration by parts, which relates the sum of the product of two functions with the sum of one function, and the difference of the other. However, for our purposes we shall need the following, much weaker version.

Theorem A.2 (Partial Summation)**.** *Suppose $a_1, a_2, a_3 \cdots$ is a sequence of complex numbers, $A(x) = \sum_{n \le x} a_n$ and $f(x)$ is some differentiable function on $(1, \infty)$. Then*

$$\sum_{n \le x} a_n f(n) = A(x) f(x) - \int_1^x A(t) f'(t) dt$$

Proof. Suppose x is a natural number. Therefore,

$$\sum_{n \le x} a_n f(n) = \sum_{n \le x} \{A(n) - A(n-1)\} f(n) = A(x) f(x) - \sum_{n \le x-1} A(n) \{f(n+1) - f(n)\}$$

Now, using the fact that f is differentiable,

$$\sum_{n \le x} a_n f(n) = A(x) f(x) - \sum_{n \le x-1} A(n) \int_n^{n+1} f'(t) dt$$

Now, $A(x)$ is a step function changing values at positive integers. Hence $A(n)$ can be taken inside and replaced by $A(t)$.

$$\sum_{n \le x} a_n f(n) = A(x) f(x) - \sum_{n \le x-1} \int_n^{n+1} A(t) f'(t) dt$$

and thus

$$\sum_{n \le x} a_n f(n) = A(x) f(x) - \int_1^{\infty} A(t) f'(t) dt$$

proving our theorem for integers. For non-integers, note that the theorem holds $\lfloor x \rfloor$ the greates integer less than x, and that

$$A(x) \{f(x) - f(\lfloor x \rfloor)\} - \int_{\lfloor x \rfloor}^x A(t) f'(t) dt = 0$$

$\square$

This identity is a powerful tool for obtaining elementary estimates for many sums that arise in number theory. In particular, we shall use it to obtain the following identities that we have used in the note without proof.

Theorem A.3. *For $x > 0$,*

$$\sum_{n \leq x} \frac{1}{x} = \log x + O(1)$$

Proof. Putting $a_n = 1$ and $f(t) = 1/t$ in the partial summation identity, we see that $A(x) = \sum_{n \leq x} 1 = \lfloor x \rfloor$ and thus,

$$\sum_{n \leq x} \frac{1}{x} = \frac{\lfloor x \rfloor}{x} + \int_1^x \frac{\lfloor t \rfloor}{t^2} dt$$

Now, using $\lfloor x \rfloor = x - \{x\} = x + O(1)$,

$$\sum_{n \leq x} \frac{1}{x} = \frac{x + O(1)}{x} + \int_1^x \frac{t + O(1)}{t^2} dt$$

Thus, the first term is clearly $O(1)$. Furthermore, the error term in the integral evaluates to

$$\int_1^x \frac{dt}{t^2} = 1 - \frac{1}{x}$$

which contributes $O(1)$. Hence, the main term is

$$\int_1^x \frac{dt}{t} = \log x + O(1)$$

Hence our claim follows.

□

Theorem A.4. *For $x > 0$,*

$$\sum_{n \leq x} \frac{1}{\sqrt{x}} = 2\sqrt{x} + O\left(\frac{1}{\sqrt{x}}\right)$$

Proof. Taking $a_n = 1$, $f(x) = 1/\sqrt{x}$, we see that $A(x) = \lfloor x \rfloor$. Thus,

$$\sum_{n \leq x} \frac{1}{\sqrt{x}} = \frac{\lfloor x \rfloor}{\sqrt{x}} + \frac{1}{2} \int_1^x \frac{\lfloor t \rfloor}{t^{3/2}} dt$$

Again, using the estimate $\lfloor x \rfloor = x + O(1)$, we get a contribution of $\sqrt{x} + O(1/x^{1/2})$ from the first term. From the integral again, we get a contribution of $\sqrt{x} + O(1/x^{1/2})$. Thus, we obtain the estimate

$$\sum_{n \leq x} \frac{1}{\sqrt{x}} = 2\sqrt{x} + O\left(\frac{1}{\sqrt{x}}\right)$$

□

Now, using analogous techniques to the previous two theorems, in particular taking $a_n = \chi(n)$ and noting that then $|A(x)| \leq q$, we can prove the following

Theorem A.5. *For* $x > 0$

$$\sum_{n > x} \frac{\chi(n)}{n} = O\left(\frac{1}{x^{1/2}}\right)$$

and

$$\sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} = O\left(\frac{1}{x^{1/2}}\right)$$

The proof of this claim is left as an exercise to the reader.

A.5 Dirichlet's Hyperbola Method

We differ greatly from [1] in our treatment of Dirichlet' Hyperbola Method. For us, the method is an easily proven identity. We now prove the identity and expound on its importance.

Theorem A.6 (Dirichlet's Hyperbola Method)**.** *Suppose $g(n)$ and $h(n)$ are functions on the natural numbers such that*

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

$$F(x) = \sum_{n \le x} f(n)$$

$$G(x) = \sum_{n \le x} g(n)$$

$$H(x) = \sum_{n \le x} h(n)$$

then for any real number $y > 0$ we have the following identity

$$F(x) = \sum_{d \le y} g(d) H\left(\frac{x}{d}\right) + \sum_{d \le \frac{x}{y}} g(d) H\left(\frac{x}{d}\right) - G(y) H\left(\frac{x}{y}\right)$$

Proof. We have

$$\sum_{n \le x} f(n) = \sum_{n \le x} \sum_{de=n} g(d)h(e) = \sum_{de \le x} g(d)h(e)$$

Pick a $y > 0$. Hence,

$$\sum_{n \le x} = \sum_{\substack{de \le x \\ d \le y}} g(d)h(e) + \sum_{\substack{de \le x \\ d > y}} g(d)h(e)$$

On, in other words,

$$\sum_{n \le x} = \sum_{d \le y} \sum_{e \le x/d} g(d)h(e) + \sum_{e \le x/y} \sum_{y < d \le x/e} g(d)h(e)$$

Hence, recalling the definition of G and H,

$$\sum_{n\leq x} = \sum_{d\leq y} g(d)H\left(\frac{x}{d}\right) + \sum_{e\leq x/y} h(e)\left\{G\left(\frac{x}{e}\right) - G(y)\right\}$$

and thus,

$$F(x) = \sum_{d\leq y} g(d)H\left(\frac{x}{d}\right) + \sum_{e\leq \frac{x}{y}} g(d)H\left(\frac{x}{d}\right) - G(y)H\left(\frac{x}{y}\right)$$

as desired.

□

This identity is an important one, as it gives the summatory function of the Dirichlet convolution of two number-theoretic functions in terms of the summatory functions of those number-theoretic functions. Both summatory functions and Dirichlet convolutions are commonly occurring in number theory. Furthermore, the freedom to choose the parameter y allows one to choose the optimal y to obtain the asymptotic behaviour we wish to prove. We typically choose y so that two of the terms become negligible, while the third contains the main term.

References

[1] Elias M. Stein and Rami Shakarchi, *Fourier Analysis: An Introduction* (Princeton Lectures in Analysis Vol. 1). Princeton University Press, Princeton, NJ, 2003.

[2] M. Ram Murty, *Problems in Analytic Number Theory*. Springer-Verlag, New York, NY, 2001.