Dirichlet's Theorem on Arithmetic Progressions*

Thai Pham
Massachusetts Institute of Technology

May 21, 2012

Abstract

In this paper, we derive a proof of Dirichlet's theorem on primes in arithmetic progressions. We try to motivate each step in the proof in a natural way, so that readers can have a sense of how mathematics works.

1 Introduction

Number theory is the queen of mathematics, and Dirichlet's theorem on arithmetic progressions has been considered a gem of that queen. The significance of this theorem lies not only in its simple statement, but also in the beautiful proof given by Dirichlet, which in fact set a background for the study of group theory and representation theory later on. Our main purpose in this paper is to discuss this theorem and its proof.

Theorem 1. (Dirichlet) *Given* $a, m \in \mathbb{N}^*$ *with* $\gcd(a, m) = 1$*, there are infinitely many prime numbers in the arithmetic progression* $\{a + km\}_{k \in \mathbb{N}}$.

One can easily show this theorem for $m = 4$ and $a \in \{1, 3\}$ (See Shi & Xie [9]). However, the proof for the general case is much more complicated and requires many deep algebraic and analytical ideas. Even though Selberg was able to give an elementary proof in 1949 (See [7]), his proof is rather tedious and unmotivated. In this paper, we will follow Dirichlet's method with some possible modifications to simplify the original proof.

We organize the rest of the paper as follows. Section 2 discusses the motivation for the proof of the theorem. Section 3 reviews background needed for the proof: *group characters*, *Dirichlet series*, and *Euler products*. Section 4 is dedicated to the proof of Dirichlet's theorem.

2 Motivation

In this section, we talk about the motivation for Dirichlet's proof of the theorem. Rigorous treatments are presented in the later sections.

*I am grateful to Sigurdur Helgason and Susan Ruff for their invaluable help in commenting on the earlier version of the paper in terms of both content and exposition.

We first observe that Dirichlet's theorem is in fact an extension of Euclid's theorem, which states that there are infinitely many prime numbers. Specifically, for $(a = 1, m = 2)$ the two theorems are equivalent since all the primes greater than two are odd. Our purpose is to use a similar technique to that in the proof of Euclid's theorem to prove Dirichlet's theorem.

Actually, what interests us the most is the stronger version of Euclid's theorem, also known as Euler's theorem on the sum of the reciprocals of the prime numbers (See Dunham's paper [3]):

$$\sum_p \frac{1}{p} = \infty. \tag{1}$$

(Throughout the paper, we write p to denote a prime number, unless otherwise specified). Motivated by this theorem, we desire to prove a stronger result than Dirichlet's original theorem:

$$\sum_{p \equiv a (\bmod m)} \frac{1}{p} = \infty. \tag{2}$$

We recall the proof of Euler's theorem to grasp the ideas behind it. In his proof, Euler took advantage of the *product formula*:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}} \text{ for all } s \in \mathbb{C} \text{ with Re(s)} > 1. \tag{3}$$

The left hand side of (3) is known as the *Riemann zeta function* $\zeta(s)$. Euler proceeded in his proof by writing

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + g(s), \tag{4}$$

where $g(s)$ is bounded as $s \to 1$. The fact that $\zeta(s) \to \infty$ as $s \to 1$ would then imply the result.

To prove Dirichlet's theorem, we want the sum $\displaystyle\sum_{p \equiv a (\bmod m)} \frac{1}{p^s}$ to appear in a similar sense. To do this, we need a good trick to 'filter out' the primes congruent to a modulo m from all other primes. The zeta function needs to be modified, and the *Dirichlet series* appears naturally; it has the form $\displaystyle\sum_{n=1}^{\infty} a(n) n^{-s}$, where $s, a(n) \in \mathbb{C}$ for all $n \in \mathbb{N}^*$. A random choice of $a(n)$ would yield nothing. However, when $a(n)$ is chosen to be a *completely multiplicative function* (i.e. $a(1) = 1$ and $a(mn) = a(m)a(n)$ for all $m, n \in \mathbb{N}^*$), we obtain an equation similar to (3), known as the *Euler product*:

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_p \frac{1}{1 - a(p)p^{-s}} \text{ for all } s \in \mathbb{C} \text{ with Re(s)} > 1. \tag{5}$$

Taking the natural logarithm of both sides of (5), we can write the right hand side in the form $\displaystyle\sum_p \frac{a(p)}{p^s} + h(s, a)$. The choice of $a(n)$ is not good enough nevertheless, as we have not reached the sum we desire. We need to fine-tune $a(n)$ to help in the filtering process. The breakthrough point here is Dirichlet's use of *group characters*. With this tool in hand, Dirichlet's theorem is no longer far away. Now, we come to the rigorous treatment for the theorem.

3 Background

In this section, we present the important notions which were mentioned earlier and which are necessary for the proof of Dirichlet's theorem. The notions include group characters, Dirichlet series, and Euler products.

3.1 Group Characters

To understand this part well, readers should have a sufficient knowledge of abstract algebra, specifically group theory. As a reference, the author recommends Artin's book (See [2]) and Serre's book (See [8]). About particular group characters, readers should consult Apostol's book (See [1]).

Definition 2. *Let G be an abelian group. A function $\chi : G \to \mathbb{C}\backslash\{0\}$ mapping G to the set of non-zero complex numbers is called a* character *of G if it is a group homomorphism, that is $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)\ \forall g_1, g_2 \in G$.*

We restrict our attention to the finite group G. In this case, the set of characters χ_i of G forms an abelian group under multiplication $(\chi_j \chi_k)(g) = \chi_j(g)\chi_k(g)\ \forall g \in G$ with *principal character* χ_0 such that $\chi_0(g) = 1\ \forall g \in G$. This group is called the *dual* of G and is usually denoted by $\widehat{G}$.

We now turn to one important property of the dual group.

Proposition 3. *Any abelian group G is isomorphic to its dual $\widehat{G}$.*

Proof. For a cyclic group G, the result is straightforward. Since G can be written as a product of cyclic groups, it holds in general. □

We now consider an important property of group characters, which will help us filter out the primes we want in the above discussion: the orthogonality property of characters.

Proposition 4. *If $\chi \in \widehat{G}$, then*

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

Also, if $g \in G$ then

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |\widehat{G}| & \text{if } g = 1 \text{ (the identity element of } G\text{)}, \\ 0 & \text{otherwise.} \end{cases} \tag{7}$$

Proof. We can easily see (7) is a corollary of (6) thanks to Proposition 3. So, it is sufficient to prove only (6).

To this end, we observe that if $\chi = \chi_0$ then $\chi(g) = 1 \ \forall g \in G$. Then, $\sum_{g \in G} \chi(g) = |G|$. If $\chi \neq \chi_0$, there exists some $h \in G$ such that $\chi(h) \neq 1$. We have

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(gh) = \sum_{g \in G} \chi(g). \tag{8}$$

Thus $\sum_{g \in G} \chi(g) = 0$, and this ends the proof. $\square$

We observe that, if $\chi, \varphi \in \widehat{G}$ then $\chi\varphi^{-1} \in \widehat{G}$. Moreover, $\sum_{g \in G} (\chi\varphi^{-1})(g) = \sum_{g \in G} \chi(g)\overline{\varphi(g)}$. Similarly, if $g, h \in G$, then $gh^{-1} \in G$. We have $\sum_{\chi \in \widehat{G}} \chi(gh^{-1}) = \sum_{\chi \in \widehat{G}} \chi(g)\overline{\chi(h)}$. Then by Proposition 4, we get the following corollary.

Corollary 5. *If $\chi, \varphi \in \widehat{G}$, then*

$$\sum_{g \in G} \chi(g)\overline{\varphi(g)} = \begin{cases} |G| & \text{if } \chi = \varphi, \\ 0 & \text{otherwise.} \end{cases} \tag{9}$$

Also, if $g, h \in G$ then

$$\sum_{\chi \in \widehat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} |\widehat{G}| & \text{if } g = h, \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

The above result is quite impressive, but it is not the end of the story. We need something more specific, more directly applicable to our theorem. Again, Dirichlet made a big jump in introducing the *Dirichlet character*. This notion will reappear later on when we talk about Dirichlet series and Euler products.

Definition 6. *A Dirichlet character is any function $\chi : \mathbb{Z} \to \mathbb{C}$ which satisfies the following properties:*

(a) There exists $m \in \mathbb{Z}_+$ such that $\chi(n) = \chi(n+m)$ for all $n \in \mathbb{Z}$.

(b) If $\gcd(n, m) > 1$, then $\chi(n) = 0$; if $\gcd(n, m) = 1$, then $\chi(n) \neq 0$.

(c) $\chi(nk) = \chi(n)\chi(k)$ for all $n, k \in \mathbb{Z}$.

From this definition, we can deduce other properties. From (b) and (c), $\chi(1) = 1$. Combining this with (c), we conclude that χ is a completely multiplicative function. Besides, (a) implies that χ is periodic with period m. This is why we also call χ the *Dirichlet character modulo* m.

We make two remarks here. First, according to Definition 2 a character cannot have zero value; however, a Dirichlet character can take the value zero. Second, if $\gcd(a, m) = 1$ then by Euler's theorem $a^{\phi(m)} \equiv 1 \pmod{m}$, where ϕ is the *totient function*. Hence, $\chi(a^{\phi(m)}) = \chi(1) = 1$ which implies that $\chi(a)^{\phi(m)} = 1$. Thus, $\chi(a)$ is a $\phi(m)$-th root of unity for all a such that $\gcd(a, m) = 1$.

Thanks to these two points, Dirichlet characters can be viewed in terms of the character group of the unit group of the ring $\mathbb{Z}/m\mathbb{Z}$.

Specifically, let $G = (\mathbb{Z}/m\mathbb{Z})^*$ (so $|G| = \phi(m)$) with the principal character χ_0 such that $\chi_0(a) = 1$ if $\gcd(a, m) = 1$ and 0 otherwise. Then, the Dirichlet character modulo m is informally considered the extension of G to $\mathbb{Z}$. We obtain the following important formulas.

Corollary 7. *Let χ and φ be Dirichlet characters modulo m. Then*

$$\sum_{g=0}^{m-1} \chi(g)\overline{\varphi(g)} = \begin{cases} \phi(m) & \text{if } \chi = \varphi, \\ 0 & \text{otherwise.} \end{cases} \tag{11}$$

Similarly, let g and h be integers. Then

$$\sum_{\chi} \chi(g)\overline{\chi(h)} = \begin{cases} \phi(m) & \text{if } g \equiv h \ (\text{mod } m), \\ 0 & \text{otherwise.} \end{cases} \tag{12}$$

With this corollary in hand, we can begin to sense how we may obtain the sum $\displaystyle\sum_{p \equiv a (\operatorname{mod} m)} \frac{1}{p^s}$. However, the tools we have covered so far are not enough. We now turn to the next critical point in the proof of the theorem: the Dirichlet series.

3.2 Dirichlet series

Our main purpose in this section is to review one important property of the Dirichlet series, and we incorporate it into a theorem.

Theorem 8. **(Cohen)** *Let $D = \displaystyle\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ be a Dirichlet series. If D converges for some $s = s_0$, then it converges uniformly on each compact set of the half-plane $Re(s) > Re(s_0)$. Moreover, the sum is analytic in this region.*

The proof of this theorem is quite simple; but as it is not central to the purpose of this paper, we refer interested readers to Titchmarsh's book, Chapter IX (See [10]).

We discussed in section 2 that $a(n)$ in the Dirichlet series being completely multiplicative is not good enough. Moreover, in equations (11) and (12) we used the Dirichlet characters χ and φ and mentioned that they will help in the filtering process. Dirichlet was very clever in using such χ in the Dirichlet series and created the Dirichlet L-series:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{13}$$

The use of $L(s, \chi)$ is in fact not so important when we study the Dirichlet series here or the Euler products in the next part; but as it is essential for completing the proof of Dirichlet's theorem, we bring it along in these discussions.

One not-so-direct corollary of theorem 8 is concerned with $L(s, \chi)$.

Corollary 9. *Let χ be a Dirichlet character modulo m different from the principal character. Then $L(s, \chi)$ converges and is analytic in $Re(s) > 0$.*

Proof. For any $a \in \mathbb{Z}$, proposition 4 implies

$$\sum_{n=1}^{m} \chi(n+a) = \sum_{n=0}^{m-1} \chi(n) = 0. \tag{14}$$

Let $s \in \mathbb{R}_+$. Let $U_n = \sum_{i=1}^{n} \chi(i)$. By (14), $\{U_n\}_n$ is bounded. So there is some constant $C \in \mathbb{R}_+$ such that $|U_n| < C \; \forall n \in \mathbb{N}$. For any $M \in \mathbb{Z}_+$, applying Abel's summation formula (See Rudin [6] p. 79) we get

$$\left| \sum_{n=M}^{\infty} \frac{\chi(n)}{n^s} \right| = \left| \sum_{n=M}^{\infty} U_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) \right| \leq C \sum_{n=M}^{\infty} \left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right| = \frac{C}{M^s}. \tag{15}$$

Since $\lim_{M \to \infty} \frac{C}{M^s} = 0$, then $\lim_{M \to \infty} \sum_{n=M}^{\infty} \frac{\chi(n)}{n^s} = 0$ which implies $L(s, \chi)$ converges for $s \in \mathbb{R}_+$. By theorem 8, we conclude that $L(s, \chi)$ converges and is analytic in $Re(s) > 0$. $\square$

We make two remarks here. First, corollary 9 is apparently unnecessary now but it will definitely be useful when we prove Dirichlet's theorem. Second, we defer some properties of $L(s, \chi)$ until they become relevant with the context of the proof. Next, we discuss another important notion: the Euler products.

3.3 Euler products

This section serves to introduce two important results related to Euler products. The first one is similar to equation (5).

Theorem 10. *$L(s, \chi)$ converges absolutely for $Re(s) > 1$. Moreover in this region,*

$$L(s, \chi) = \prod_{p} \frac{1}{1 - \chi(p) p^{-s}}. \tag{16}$$

Proof. First, notice that χ is bounded; therefore, $L(s, \chi)$ converges absolutely for $Re(s) > 1$. Now, for each prime p we have: $\left(1 - \chi(p)p^{-s}\right)^{-1} = \sum_{n=0}^{\infty} \chi(p)^n p^{-ns} = \sum_{n=0}^{\infty} \chi(p^n) p^{-ns}$. This implies, for any fixed prime q, that $\prod_{p \leq q} \frac{1}{1 - \chi(p)p^{-s}} = \sum_{n \in T_q} \frac{\chi(n)}{n^s}$, where T_q is the set of all natural numbers whose prime factors are less than or equal to q. Then, for any natural number N we have

$$\sum_{n=1}^{N} \frac{\chi(n)}{n^s} = \prod_{p \leq r} \frac{1}{1 - \chi(p)p^{-s}} - \sum_{n \in T_r, n > N} \frac{\chi(n)}{n^s}, \tag{17}$$

where r is the largest prime less than or equal to N, and T_r is defined in the same way as T_q. Letting N approach infinity, we obtain the desirable result. □

The second result is concerned only with $L(s, \chi_0)$.

Proposition 11. *$L(s, \chi_0)$ extends to a meromorphic function in $Re(s) > 0$ with the only pole at $s = 1$.*

Proof. By theorem 10, we get

$$L(s, \chi_0) = \prod_{p \nmid m} \frac{1}{1 - p^{-s}}. \tag{18}$$

We proceed by presenting an important result about the Riemann zeta function $\zeta(s)$.

Lemma 12. *Let ζ be the Riemann zeta function. Then,*
(a) $\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}$ for $Re(s) > 1$, and
(b) $\zeta(s) - \frac{1}{s-1}$ extends to a holomorphic function in $Re(s) > 0$.

We will not prove this lemma, as it is very famous in the literature (See e.g. Rudin [6] p. 141). Now, we come back to our proposition 11. By lemma $12(a)$, we can write

$$L(s, \chi_0) = \zeta(s) \prod_{p \mid m} (1 - p^{-s}) \ \text{ for } Re(s) > 1. \tag{19}$$

Note that $\prod_{p \mid m} (1 - p^{-s})$ is finite. Combining this fact with lemma $12(b)$, we conclude that $L(s, \chi_0)$ can extend to a meromorphic function in $Re(s) > 0$ and its only pole is at $s = 1$. □

Now, we have enough tools to prove Dirichlet's theorem.

4 Dirichlet's Theorem

We want to prove theorem 1 in a way suggested in section 2 of the paper. We start by taking the natural logarithm of the Euler product (equation (16)):

$$\log L(s, \chi) = \sum_{p} \left[-\log\left(1 - \chi(p) p^{-s}\right) \right] \ \text{ for Re(s)} > 1. \tag{20}$$

We will show that the right hand side of (20) can be written in the form $\sum_{p} \frac{\chi(p)}{p^s} + h(s, \chi)$, where $h(s, \chi)$ is bounded as $s \to 1$.

To this end, we fix p and use the Taylor's expansion for $-\log(1 - x)$ at $x = \chi(p) p^{-s}$:

$$-\log\left(1 - \chi(p) p^{-s}\right) = \frac{\chi(p)}{p^s} + \sum_{n=2}^{\infty} \frac{\chi(p)^n}{n p^{ns}} \ \text{ for } Re(s) > 1. \tag{21}$$

Moreover, $|\chi(p)| = 0$ or 1 so $|\chi(p)p^{-s}| \le |p^{-s}| \le 2^{-1}$. Then for $Re(s) > 1$, we get

$$\left|\sum_{n=2}^{\infty} \frac{\chi(p)^n}{np^{ns}}\right| \le \left|\frac{\chi(p)}{p^s}\right|^2 \sum_{n=2}^{\infty} \frac{1}{n}\left|\frac{\chi(p)}{p^s}\right|^{n-2} \le \left|\frac{\chi(p)}{p^s}\right|^2 \sum_{n=2}^{\infty} \frac{1}{2}\frac{1}{2^{n-2}} = \left|\frac{\chi(p)}{p^s}\right|^2 \le \frac{1}{p^2}. \tag{22}$$

Let $h(s,\chi) = \sum_p \sum_{n=2}^{\infty} \frac{\chi(p)^n}{np^{ns}}$. Then

$$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + h(s,\chi), \text{where} \tag{23}$$

$$|h(s,\chi)| \le \sum_p \left|\sum_{n=2}^{\infty} \frac{\chi(p)^n}{np^{ns}}\right| \le \sum_p \frac{1}{p^2} < \sum_{n=1}^{\infty} \frac{1}{n^2} < \infty \text{ for } Re(s) > 1. \tag{24}$$

Thus, $h(s,\chi)$ is bounded as $s \to 1$ as desired.

The next step is the filtering process. We recall the orthogonality property that given group $G = (\mathbb{Z}/m\mathbb{Z})^*$,

$$\sum_\chi \chi(g)\overline{\chi(h)} = \begin{cases} \phi(m) & \text{if } g \equiv h \ (mod\ m), \\ 0 & \text{otherwise.} \end{cases} \tag{25}$$

(We write the sum over χ to indicate the sum over all $\chi \in \widehat{G}$). By multiplying both sides of (23) by $\overline{\chi(a)}$ and summing over all χ, we obtain

$$\sum_\chi \overline{\chi(a)} \log L(s,\chi) = \sum_\chi \overline{\chi(a)} \sum_p \frac{\chi(p)}{p^s} + \sum_\chi \overline{\chi(a)} h(s,\chi). \tag{26}$$

Hence,

$$\sum_\chi \overline{\chi(a)} \log L(s,\chi) - \sum_\chi \overline{\chi(a)} h(s,\chi) = \sum_p \frac{1}{p^s} \sum_\chi \chi(p)\overline{\chi(a)} = \phi(m) \sum_{p \equiv a (\text{mod}\, m)} \frac{1}{p^s}. \tag{27}$$

The sum we want finally appears. Now notice that $|\widehat{G}| = \phi(m)$. Because $h(s,\chi)$ is bounded as $s \to 1$, $\sum_\chi \overline{\chi(a)} h(s,\chi)$ is bounded as $s \to 1$.

Our goal is to show that the right hand side of (27) diverges to infinity as $s \to 1$. To do this, we need to show $\sum_\chi \overline{\chi(a)} \log L(s,\chi) \to \infty$ as $s \to 1$.

By proposition 11, we know that $L(s,\chi_0) \to +\infty$ as $s \to 1$ and thus, so does $\log L(s,\chi_0)$. Since $\overline{\chi(a)} \neq 0$ and is bounded, to obtain the desired result it is enough to show $\log L(1,\chi)$ is bounded below for all $\chi \neq \chi_0$. This is equivalent to showing $L(1,\chi) \neq 0 \ \forall \chi \neq \chi_0$. Once this statement is proved, we are done with the proof of Dirichlet's theorem. Thus, it is sufficient to prove the following proposition.

Proposition 13. *For all $\chi \neq \chi_0$, $L(1,\chi) \neq 0$.*

It is interesting to note that, in the proof of the Prime Number Theorem (See Zagier's paper [11]) the analogous statement for $\zeta(s)$ is also a major step.

Back to our proposition, there are at least two ways to show it. One method is quick but not very illuminating; interested readers can see it in Garrett's paper (See [4]). Here, we provide a much more interesting proof, though it is more complicated. Another note is that this proof was modified from Dirichlet's original proof.[1]

Proof. The key to the proof is the function $\zeta_m(s)$, which is defined as

$$\zeta_m(s) = \prod_{\chi} L(s, \chi). \tag{28}$$

We observe that for all $\chi \neq \chi_0$, $L(s, \chi)$ is analytic in $Re(s) > 0$ by corollary 9. Moreover, $L(s, \chi_0)$ extends to a holomorphic function in $Re(s) > 0$ with the only pole at $s = 1$ by proposition 11. Suppose that there is some $\chi \neq \chi_0$ such that $L(1, \chi) = 0$ then $\zeta_m(s)$ would be analytic in $Re(s) > 0$ (since the zero value at $s = 1$ of $L(s, \chi)$ will cancel the pole of $L(s, \chi_0)$). We will show that $\zeta_m(s)$ cannot be analytic in $Re(s) > 0$ to obtain a contradiction, through which we prove proposition 13.

To this end, we denote by $ord(p)$ the order of the image $\overline{p}$ of p in $G = (\mathbb{Z}/m\mathbb{Z})^*$ for any prime $p \nmid m$. We proceed with the following lemma.

Lemma 14. *If* $Re(s) > 1$, *then*

$$\zeta_m(s) = \prod_{p \nmid m} \left(\frac{1}{1 - p^{-ord(p)s}} \right)^{\frac{\phi(m)}{ord(p)}}. \tag{29}$$

Proof. To prove this lemma, we first note that if $p \nmid m$ then

$$\prod_{\chi} \left(1 - \frac{\chi(p)}{p^s} \right) = \left(1 - \frac{1}{p^{ord(p)s}} \right)^{\frac{\phi(m)}{ord(p)}}. \tag{30}$$

To see why (28) is true, we start from the identity

$$1 - x^{ord(p)} = \prod_{\omega \in U_{ord(p)}} (1 - \omega x), \tag{31}$$

where U_n denotes the set of all n-th roots of unity. Notice that for each $\omega \in U_{ord(p)}$, there are exactly $\phi(m)/ord(p)$ Dirichlet characters χ such that $\chi(p) = \omega$. Hence

$$\prod_{\chi} (1 - \chi(p)x) = \left(1 - x^{ord(p)}\right)^{\frac{\phi(m)}{ord(p)}}. \tag{32}$$

[1]We cannot find any official document saying who was the first to modify Dirichlet's proof; among the possible contributors is Edmund Landau.

Let $x = p^{-s}$ we obtain (28). From here, we have for $Re(s) > 1$

$$\zeta_m(s) = \prod_{\chi} L(s,\chi) = \prod_{\chi}\prod_{p\nmid m} \frac{1}{1-\chi(p)p^{-s}} = \prod_{p\nmid m}\left(\frac{1}{1-p^{-ord(p)s}}\right)^{\frac{\phi(m)}{ord(p)}}, \tag{33}$$

as desired. So, lemma 14 is proved.

□

The key here is to observe that $\dfrac{1}{1-p^{-ord(p)s}}$ is a Dirichlet series with non-negative real coefficients. Hence, by lemma 14, $\zeta_m(s)$ is also a Dirichlet series with non-negative real coefficients. To come up with a contradiction, we need to use the following result, known as *Landau's theorem.*

Theorem 15. ***(Landau)*** *Let $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ be a Dirichlet series with real coefficients $a_n \geq 0$. Suppose that the series defining $f(s)$ converges for $Re(s) > s_0$ for some real s_0. Suppose further that the function f extends to a holomorphic function in a neighborhood of s_0, to say $(s_0 - \epsilon, s_0)$ for some $\epsilon > 0$. Then, the series defining $f(s)$ converges for $Re(s) > s_0 - \epsilon$.*

We will not prove this theorem here. Instead, we refer interested readers to Garrett's paper (See [4]).

Coming back to proposition 13, the proof is now at hand. Our goal is to show that $\zeta_m(s)$ cannot be analytic in $Re(s) > 0$. Assume the contrary is true. Recall that $\zeta_m(s)$ is a Dirichlet series whose coefficients are real and non-negative. Moreover, $L(s,\chi)$ converges for $Re(s) > 1$ for all χ so $\zeta_m(s)$ also converges for $Re(s) > 1$. By Landau's theorem with $s_0 = \epsilon = 1$, $\zeta_m(s)$ converges for $Re(s) > 0$.

However, for $Re(s) > 1$, we have

$$\left(\frac{1}{1-p^{-ord(p)s}}\right)^{\frac{\phi(m)}{ord(p)}} = \left(1 + p^{-ord(p)s} + p^{-2ord(p)s} + \cdots\right)^{\frac{\phi(m)}{ord(p)}}, \tag{34}$$

which dominates the series $1 + p^{-\phi(m)s} + p^{-2\phi(m)s} + \cdots = \dfrac{1}{1-p^{-\phi(m)s}}$.

Then for $s > 1$, all the coefficients of $\zeta_m(s) = \prod_{p\nmid m}\left(\frac{1}{1-p^{-ord(p)s}}\right)^{\frac{\phi(m)}{ord(p)}}$ are greater than those of $\prod_{p\nmid m} \frac{1}{1-p^{-\phi(m)s}} = \sum_{n\in\mathbb{Z}_+,\, \gcd(n,m)=1} \frac{1}{n^{\phi(m)s}}$. Hence,

$$\zeta_m\left(\phi(m)^{-1}\right) \geq \sum_{n\in\mathbb{Z}_+,\, \gcd(n,m)=1} \frac{1}{n}, \tag{35}$$

which is divergent to infinity.

So $\zeta_m(s)$ diverges at $s = \phi(m)^{-1} > 0$, which is a contradiction! So proposition 13 is proved, and we are done with the proof of Dirichlet's theorem. □

References

[1]. **Apostol, Tom M.** (1976), *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, New York-Heidelberg: Springer-Verlag.
[2]. **Artin, Michael**, *Algebra*, Prentice Hall, 1991.
[3]. **Dunham, William** (1999). *Euler: The Master of Us All*. The Mathematical Association of America, Dolciani Mathematical Expositions, Vol. 22, 1999.
[4]. **Garrett, Paul**, *Primes in arithmetic progressions*, 2011.
$http://www.math.umn.edu/\sim garrett/m/mfms/notes\_c/dirichlet.pdf$
[5]. **Knapp, A.**, *Elliptic Curves*. Princeton UP, New Jersey, 1992.
[6]. **Rudin, W.** *Principles of Mathematical Analysis*. 3rd ed. New York, NY: McGraw-Hill, 1976.
[7]. **Selberg, Atle**, *An Elementary Proof of Dirichlet's Theorem About Primes in an Arithmetic Progression*, The Annals of Mathematics, 2nd Series, Vol.50, No.2 (Apr., 1949), pp.$297-304$.
[8]. **Serre, J.-P.**, *A Course in Arithmetic*, Springer-Verlag, New York, 1973.
[9]. **Shi, Meiyi & Xie, Tessa**, *Prime, Modular Arithmetic, and Squares*. SWIM 2010, Princeton.
[10]. **Titchmarsh, E. C.**, *The Theory of Functions*, Oxford University Press, 1932.
[11]. **Zagier, D.**, *Newman's short proof of the Prime Number Theorem*. The American Mathematical Monthly, 104(1997), $705-708$.