

Dirichlet's Prime Number Theorem: Algebraic and Analytic Aspects

Igor Rapinchuk '07[†]
Harvard University
Cambridge, MA 02138
rapinch@fas.harvard.edu

Abstract

The focus of this paper is the famous theorem on primes in arithmetic progressions due to Dirichlet: *if a and $m > 0$ are relatively prime integers, then there exist infinitely many primes of the form $a + km$ with k a positive integer.* The proof of this theorem in the general case uses analytic techniques, and in fact some key statements heavily rely on complex analysis. The case $a = 1$, however, can be handled by purely algebraic methods as we will show in Section 2.1 following suggestions given in [La]. In Section 2.2, we will outline the idea of the proof of Dirichlet's theorem as it is presented in [IR] and [Kn] for the case $m = 4$. Finally, in Section 2.3, after a brief discussion of characters of finite abelian groups following [Se], we will present the proof of Dirichlet's theorem (cf. [IR, Kn, Se]).

2.1 There are infinitely many primes $p \equiv 1 \pmod{m}$: algebraic proof

Let $P = \{2, 3, 5, \dots\}$ be the set of all primes. For relatively prime integers a and $m > 0$ we let

$$P_{a(m)} = \{p \in P \mid p \equiv a \pmod{m}\}.$$

Dirichlet's Prime Number Theorem states that $P_{a(m)}$ is always infinite. In this section, we will prove this for $a = 1$ by using purely algebraic techniques. It is interesting that the argument can be traced back to Euclid's proof of the fact that P is infinite: if $P = \{p_1, \dots, p_r\}$ then for any prime factor p of $p_1 \cdots p_r + 1$ we have $p \notin \{p_1, \dots, p_r\}$, a contradiction. We will now do a couple of simple examples which demonstrate that suitable modifications of Euclid's method allow one to find infinitely many primes in certain arithmetic progressions.

Proposition 1. *The sets $P_{1(4)}$ and $P_{3(4)}$ are infinite.*

Proof. $P_{1(4)}$: We will use the well-known fact that primes in $P_{1(4)}$ (in other words, primes of the form $4k + 1$) can be characterized as those primes > 2 for which the congruence $x^2 \equiv -1 \pmod{p}$ has a solution. Assume that $P_{1(4)}$ contains only finitely many primes, say, $p_1 = 5, p_2 = 13, \dots, p_n$. Consider $a = 4p_1^2 \cdots p_n^2 + 1$, and let p be a prime factor of a . Then, just as in Euclid's proof, $p \notin \{p_1, \dots, p_n\}$.

[†]Igor Rapinchuk '07 is a mathematics concentrator living in Kirkland House. He came to Harvard from Charlottesville, VA, where he graduated from Albemarle High School. His main mathematical interests are in algebraic geometry and algebraic number theory, with related interests in algebra and complex analysis. Following graduation, Igor plans to pursue graduate studies in mathematics, and will, in particular, be spending the next academic year in the Math Tripos, Part III program at the University of Cambridge as a Gates Cambridge Scholar.

On the other hand, $p|a$ implies that $-1 \equiv (2p_1 \cdots p_n)^2 \pmod{p}$, and therefore $p \in P_{1(4)}$ (as obviously $p > 2$). So, p is a “new” prime in $P_{1(4)}$, contradicting our original assumption. Thus $P_{1(4)}$ is infinite.

$P_{3(4)}$: Again, assume that $P_{3(4)}$ contains only finitely many primes: $p_1 = 3, p_2 = 7, \dots, p_n$. Consider $b = 4p_2 \cdots p_n + 3$. Clearly, b is odd, not divisible by 3, and satisfies $b \equiv 3 \pmod{4}$. Then all prime factors of b cannot belong to $P_{1(4)}$ as otherwise we would have $b \equiv 1 \pmod{4}$. Since $P = \{2\} \cup P_{1(4)} \cup P_{3(4)}$, we conclude that b has a prime factor $p \in P_{3(4)}$. But obviously $p \notin \{p_1, \dots, p_n\}$, which again yields a contradiction. \square

It is important to observe that the above argument for $P_{1(4)}$ already contains the idea that we will use to prove that $P_{1(m)}$ is infinite for any m : show that there exists a polynomial $f(X) \in \mathbb{Z}[X]$ (for $m = 4$ we used $f(X) = X^2 + 1$) such that any prime factor $p \nmid m$ of $f(a)$, where $a \in \mathbb{Z}$, belongs to $P_{1(m)}$, and on the other hand, the values $f(a)$ as a runs through \mathbb{Z} have infinitely many prime divisors. We will show that the latter property holds in fact for any nonconstant integer polynomial (Lemma 2), while the former property holds for the m -th cyclotomic polynomial $\Phi_m(X)$ (see the proof of Theorem 4). This approach to proving that $P_{1(m)}$ is infinite is suggested in Problems 20 and 21 in Ch. VI of [La]. We also notice that our argument for $P_{3(4)}$ depends on the fact that an odd prime can get only in one of the two classes, $P_{1(4)}$ or $P_{3(4)}$, mod 4, and therefore may not be generalizable for $m > 4$.

Lemma 2. (Problem 20 in [La], Ch. VI) *Let*

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$$

be a nonconstant polynomial. Then the nonzero values $f(a)$ with $a \in \mathbb{Z}^+$ are divisible by infinitely many primes.

Proof. We can assume that $a_0 \neq 0$ as otherwise for any prime p , the value $f(pa)$ is divisible by p for any $a \in \mathbb{Z}$, and of course one can pick an a so that $f(pa) \neq 0$. Next, observe that

$$f(a_0 X) = a_0 g(X) \text{ where } g(X) = a_n a_0^{n-1} X^n + \cdots + 1,$$

so it is enough to show that the nonzero values $g(a)$ with $a \in \mathbb{Z}^+$ are divisible by infinitely many primes. In other words, we can assume that $a_0 = 1$. Suppose that the nonzero values $f(a)$ for $a \in \mathbb{Z}$ are divisible only by finitely many primes, say, p_1, \dots, p_r . Consider $F(X) = f(p_1 \cdots p_r X)$. Then $F(X)$ is a nonconstant integer polynomial of degree n , hence assumes each value at not more than n values of the variable. In particular, there exists $a \in \mathbb{Z}^+$ such that $F(a) \neq 0, \pm 1$. Then it follows from our construction that $F(a)$ is divisible by some p_i where $i \in \{1, \dots, r\}$. But

$$F(a) = a_n (p_1 \cdots p_r a)^n + \cdots + a_1 (p_1 \cdots p_r a) + 1,$$

so the fact that $p_i | F(a)$ implies that $p_i | 1$. This is a contradiction, proving the lemma. \square

Obviously, the above proof of Lemma 2 is based on the same idea as Euclid’s proof. We will now give another proof of Lemma 2 which gives some additional quantitative information. For a subset $A \subset \mathbb{Z}$ and a natural number N we let $A(N) = \{a \in A \mid |a| \leq N\}$. We will use the following simple idea: given two subsets $A, B \subset \mathbb{Z}$, to show that $A \not\subset B$ it is enough to find N such that $|A(N)| > |B(N)|$. We will apply this idea to the sets

$$A = \{f(a) \mid a \in \mathbb{Z}^+ \text{ and } f(a) \neq 0\}$$

and, assuming that the numbers in A are divisible only by finitely many primes p_1, \dots, p_r ,

$$B = \{p_1^{\alpha_1} \cdots p_r^{\alpha_r}\}.$$

Let $M = \max\{|a_n|, \dots, |a_0|\}$. Then for any $a \in \mathbb{Z} \setminus \{0\}$ we have

$$|f(a)| \leq |a_n| |a|^n + \cdots + |a_0| \leq M(n+1) |a|^n.$$

It follows that if $d \in \mathbb{N}$ is such that $M(n+1)d^n \leq N$ then all the nonzero numbers among $f(1), \dots, f(d)$ belong to $A(N)$. Since f assumes each value at not more than n different values of the variable, we get that

$$|A(N)| \geq \frac{d-n}{n} = \frac{d}{n} - 1 \geq \frac{1}{n} \left(\left(\frac{N}{M(n+1)} \right)^{1/n} - 1 \right) - 1$$

because for d one can take

$$d = \left\lceil \left(\frac{N}{M(n+1)} \right)^{1/n} \right\rceil > \left(\frac{N}{M(n+1)} \right)^{1/n} - 1. \quad (2.1)$$

Since $(1+n)^{1/n} \leq 2$, we finally get that

$$|A(N)| \geq \frac{N^{1/n}}{2M^{1/n}n} - 2.$$

On the other hand, since $p_i \geq 2$, we see that $p_1^{\alpha_1} \cdots p_r^{\alpha_r} \leq N$ implies that

$$\alpha_1 + \cdots + \alpha_r \leq \log_2 N,$$

and in particular, $\alpha_i \leq \log_2 N$ for all $i = 1, \dots, r$. It follows that

$$|B(N)| \leq (\log_2 N + 1)^r.$$

Since $N^{1/n}/(\log_2 N)^r \rightarrow \infty$ as $N \rightarrow \infty$, we find that

$$|A(N)| > |B(N)|$$

for all sufficiently large N . Thus, $A \not\subset B$, which yields another proof of Lemma 2. In fact, we proved the following.

Proposition 3. *Fix a natural number r and pick N so that*

$$\frac{N^{1/n}}{2M^{1/n}n} - 2 > (\log_2 N + 1)^r.$$

If d is defined by (2.1) then the nonzero numbers among $f(1), f(2), \dots, f(d)$ have at least $(r+1)$ distinct prime divisors.

We are now ready to prove the main result of this section.

Theorem 4. *For any $m > 0$, the set $P_{1(m)}$ is infinite.*

Let $\Phi_m(X)$ denote the m -th cyclotomic polynomial (cf. [Co], Sec. 9.1, or [La], Ch. VI, Sec. 3).

Lemma 5. (Problem 21(a) in [La], Ch. VI) *Let p be a prime, a and $m > 0$ be integers prime to p . Then $p \mid \Phi_m(a)$ if and only if the image \bar{a} of a in $(\mathbb{Z}/p\mathbb{Z})^*$ has order (exactly) m .*

Proof. First, suppose \bar{a} has order m in $(\mathbb{Z}/p\mathbb{Z})^*$. Then $\bar{a}^m = \bar{1}$, or equivalently $p \mid (a^m - 1)$. On the other hand, for any d such that $0 < d < m$, we have $\bar{a}^d \neq \bar{1}$, and therefore $p \nmid (a^d - 1)$. By Proposition 9.1.5 in [Co], we have

$$X^m - 1 = \prod_{d|m} \Phi_d(X) \quad (2.2)$$

and therefore

$$a^m - 1 = \prod_{d|m} \Phi_d(a). \quad (2.3)$$

Let d be a proper divisor of m . Since $\Phi_d(a)|(a^d - 1)$, it follows from the above that $p \nmid \Phi_d(a)$. On the other hand, $p|(a^m - 1)$, so we conclude from (2.3) that $p|\Phi_m(a)$.

Conversely, suppose $p|\Phi_m(a)$. Then it follows from (2.3) that $p|(a^m - 1)$, i.e. $\bar{a}^m = \bar{1}$. This means that the order of \bar{a} divides m . Suppose the exact order of \bar{a} is $m' < m$ (clearly, $m'|m$). Then using a factorization similar to (2.3) in which m is replaced with m' we see that there exist $d|m'$ such that $p|\Phi_d(a)$ (of course, $d < m'$). Then \bar{a} is a root of both reductions $\Phi_n(\bar{X})$ and $\Phi_d(\bar{X}) \pmod{p}$. It follows from (2.2) that \bar{a} is a multiple root of $\bar{X}^m - \bar{1}$. But since $p \nmid m$, the latter has no multiple roots. A contradiction, proving that the order of \bar{a} is exactly m . \square

Proof of Theorem 4. First, let us show that for a prime $p \nmid m$, the conditions $p|\Phi_m(a)$ and $p \equiv 1 \pmod{m}$ are equivalent (Problem 21(b) in [La], Ch. VI). Indeed, if $p|\Phi_m(a)$ then by Lemma 5, the order of \bar{a} is m . Thus, $(\mathbb{Z}/p\mathbb{Z})^*$ contains an element of order m , and therefore its order $p - 1$ is divisible by m , i.e. $p \equiv 1 \pmod{m}$. Conversely, suppose $p \equiv 1 \pmod{m}$. Since the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p - 1$, it contains an element \bar{a} of order m . Then by Lemma 5, $p|\Phi_m(a)$.

Now, by Lemma 2, the values $\Phi_m(a)$ with $a \in \mathbb{Z}$ are divisible by infinitely many primes. As we have seen, all these primes belong to $P_{1(m)}$, implying that $P_{1(m)}$ itself is infinite. \square

Since cyclotomic polynomials can be described explicitly (see [La], pg. 280), one can use Proposition 3 to find, for given m and r , a natural number d such that among prime divisors of the integers $\Phi_m(1), \dots, \Phi_m(d)$ there are at least r distinct primes $\equiv 1 \pmod{m}$. For example, if m is a prime then the cyclotomic polynomial $\Phi_m(X)$ has degree $n = m - 1$ and the maximum of its coefficients is $M = 1$. So, if we choose N so that

$$\frac{N^{1/(m-1)}}{2(m-1)} - 2 > (\log_2 N + 1)^r$$

and define d by (2.1) then the prime divisors $\neq m$ of the numbers $\Phi_m(1), \dots, \Phi_m(d)$ yield at least r distinct primes in $P_{1(m)}$.

2.2 The idea of the proof of Dirichlet's Theorem

The idea of Dirichlet's proof of the Prime Number Theorem can be traced back to Euler's proof of the fact that there exist infinitely many primes. Euler considered the generalized harmonic series

$$\sum \frac{1}{n^s}. \tag{2.4}$$

For $s \in \mathbb{C}$, we have $|n^s| = n^{\operatorname{Re} s}$, so it follows that (2.4) converges whenever $\operatorname{Re} s > 1$. (In fact, it converges absolutely, implying in particular that the series obtained by any permutation of the terms of (2.4) converges to the same number, see [Ru], Theorem 3.55.) The sum of (2.4) for $s \in \mathbb{C}$ such that $\operatorname{Re} s > 1$ is denoted $\zeta(s)$, and the correspondence $s \mapsto \zeta(s)$ is called the **(Riemann) zeta function**. The key step in Euler's proof is the following.

Lemma 6. For $s \in \mathbb{C}$, $\operatorname{Re} s > 1$, we have

$$\zeta(s) = \prod_{p \in P} \frac{1}{1 - p^{-s}}, \tag{2.5}$$

where P is the set of all primes.

Proof. We recall that we write $a = \prod_{n=1}^{\infty} a_n$ if $\lim_{d \rightarrow \infty} \prod_{n=1}^d a_n = a$. In (2.5), we consider the natural order on $P = \{p_1, \dots, p_d, \dots\}$, so that

$$\prod_{p \in P} \frac{1}{1 - p^{-s}} = \prod_{i=1}^{|P|} \frac{1}{1 - p_i^{-s}}$$

where the cardinality $|P|$ is either a finite (natural) number or infinity (in fact, the order on P doesn't matter). Fix $d \geq 1$, and let \mathbb{N}_d denote the set of natural numbers whose prime factors belong to $\{p_1, \dots, p_d\}$. Since

$$\frac{1}{1-p^{-s}} = \sum_{n=0}^{\infty} p^{ns}$$

and the geometric series in the right-hand side is absolutely convergent, we have

$$\prod_{i=1}^d \frac{1}{1-p_i^{-s}} = \sum_{n \in \mathbb{N}_d} \frac{1}{n^s}, \quad (2.6)$$

as absolutely convergent series can be multiplied term-by-term (cf. [Ru], Theorem 3.50). Notice that the order of summation in the right-hand side of (2.6) doesn't matter as the series converges absolutely. Now, we have

$$\zeta(s) - \prod_{i=1}^d \frac{1}{1-p_i^{-s}} = \sum_{n \in \mathbb{N} - \mathbb{N}_d} \frac{1}{n^s}.$$

Clearly, any number in $\mathbb{N} - \mathbb{N}_d$ is strictly greater than $p_d \geq d$, so

$$\left| \sum_{n \in \mathbb{N} - \mathbb{N}_d} \frac{1}{n^s} \right| \leq \sum_{n=d+1}^{\infty} \frac{1}{n^{\operatorname{Re} s}} \rightarrow 0 \text{ as } d \rightarrow \infty,$$

and (2.5) follows. □

Now, suppose that P is finite. Then $\prod_{p \in P} \frac{1}{1-p^{-1}}$ is a finite number, say A . For any $s \in \mathbb{R}$, $s > 1$, we have

$$\zeta(s) = \prod_{p \in P} \frac{1}{1-p^{-s}} \leq \prod_{p \in P} \frac{1}{1-p^{-1}} = A;$$

i.e. $\zeta(s)$ is bounded above by A as $s \rightarrow 1^+$. Let us show that this is not the case. For any $d \in \mathbb{N}$, we have

$$\sum_{n=1}^d \frac{1}{n^s} \leq \zeta(s) \leq A.$$

Taking the limit as $s \rightarrow 1^+$, we get $\sum_{n=1}^d 1/n \leq A$ for all d . This implies that the harmonic series

$\sum_{n=1}^{\infty} 1/n$ converges, a contradiction. Thus, P is infinite. Using a bit more analysis, we can derive the following stronger statement, which is crucial for Dirichlet's Theorem.

Proposition 7. *For $s \in \mathbb{C}$, $\operatorname{Re} s > 1$, let*

$$\lambda(s) = \sum_{p \in P} \frac{1}{p^s}.$$

Then $\lambda(s)$ is unbounded as $s \rightarrow 1^+$ in \mathbb{R} , and consequently the series $\sum_{p \in P} 1/p$ diverges.

Proof. Since $\zeta(s) > 0$ for $s > 1$, we derive from (2.5) that

$$\ln \zeta(s) = \sum_{p \in P} -\ln(1 - p^{-s}). \quad (2.7)$$

Using the expansion

$$\ln(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots \quad \text{for } |x| < 1,$$

we get

$$-\ln(1 - p^{-s}) = \frac{1}{p^s} + \frac{1}{2p^{2s}} + \frac{1}{3p^{3s}} + \dots. \quad (2.8)$$

Let

$$g_p(s) = \frac{1}{2p^{2s}} + \frac{1}{3p^{3s}} + \dots.$$

Clearly, for any $s > 1$ we have

$$0 < g_p(s) \leq \frac{1}{2p^{2s}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots \right) = \frac{1}{p^{2s}} \cdot \frac{1}{2(1 - p^{-s})} \leq \frac{1}{p^{2s}}.$$

It follows that for any d ,

$$\sum_{i=1}^d g_{p_i}(s) \leq \sum_{i=1}^d \frac{1}{p_i^{2s}} \leq \sum_{n=1}^{\infty} \frac{1}{n^2} = \zeta(2).$$

So, for any $s > 1$, the series $\sum_{p \in P} g_p(s)$ converges and its sum $g(s)$ satisfies $0 \leq g(s) \leq \zeta(2)$; in particular $g(s)$ remains bounded as $s \rightarrow 1^+$. On the other hand, by combining (2.7) and (2.8), we obtain

$$\ln \zeta(s) = \lambda(s) + g(s).$$

Since $\zeta(s)$ is unbounded and $g(s)$ is bounded as $s \rightarrow 1^+$, we conclude that $\lambda(s)$ is unbounded.

Now, suppose the series $\sum_{p \in P} 1/p$ converges, say to B . Then for any $s > 1$ and any $m \in \mathbb{N}$ we have

$$\sum_{i=1}^m \frac{1}{p_i^s} \leq \sum_{i=1}^m \frac{1}{p_i} \leq B.$$

Taking the limit as $m \rightarrow \infty$, we get $\lambda(s) \leq B$, a contradiction. \square

The idea of the proof of Dirichlet's Theorem is to establish an analog of Proposition 7 for the function which is defined just like λ , but using, instead of all primes, only those primes that occur in a given arithmetic progression. More precisely, for $s \in \mathbb{C}$, $\text{Re } s > 1$, define

$$\nu_{a(m)}(s) = \sum_{p \in P_{a(m)}} \frac{1}{p^s}.$$

Then to prove that $P_{a(m)}$ is infinite (which is what Dirichlet's theorem claims) it is enough to show that $\nu_{a(m)}(s)$ is unbounded as $s \rightarrow 1^+$. In the remaining part of this section we will show (following [IR], Ch. 16, Sec. 2 and [Kn], Ch. VII, Sec. 1) how this idea can be implemented for $m = 4$; in other words, we will show that $P_{1(4)}$ and $P_{3(4)}$ are infinite.

We obviously have

$$\lambda(s) = 2^{-s} + \nu_{1(4)}(s) + \nu_{3(4)}(s),$$

so it follows from Proposition 7 that the function

$$\lambda_+(s) = \nu_{1(4)}(s) + \nu_{3(4)}(s)$$

is unbounded as $s \rightarrow 1^+$, and therefore at least one of the functions $\nu_{1(4)}(s)$ or $\nu_{3(4)}(s)$ has this property. What we want to show is that *both* functions have this property. For this we need to identify the contributions of $\nu_{1(4)}(s)$ and $\nu_{3(4)}(s)$ to $\lambda_+(s)$ separately. The sets $P_{1(4)}$ and $P_{3(4)}$ can be separated by the following function χ defined on \mathbb{Z} :

$$\chi(n) = \begin{cases} 0 & n \equiv 0 \pmod{2}, \\ 1 & n \equiv 1 \pmod{4}, \\ -1 & n \equiv 3 \pmod{4}. \end{cases}$$

Consider

$$\lambda_-(s) = \sum_{p \in P} \frac{\chi(p)}{p^s}.$$

(Notice that this series absolutely converges for all $s \in \mathbb{C}$, $\operatorname{Re} s > 1$.) Clearly,

$$\nu_{1(4)}(s) = \frac{1}{2}(\lambda_+(s) + \lambda_-(s)) \quad \text{and} \quad \nu_{3(4)}(s) = \frac{1}{2}(\lambda_+(s) - \lambda_-(s)).$$

So, since $\lambda_+(s)$ is unbounded as $s \rightarrow 1^+$, to prove that both $\nu_{1(4)}(s)$ and $\nu_{3(4)}(s)$ have this property, it is enough to show that $\lambda_-(s)$ remains bounded.

Proposition 8. *The function $\lambda_-(s)$ remains bounded as $s \rightarrow 1^+$.*

Proof. Consider the series

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

This series converges absolutely for all $s \in \mathbb{C}$, $\operatorname{Re} s > 1$, but its real advantage over $\lambda_-(s)$ is that it is alternating, and therefore its sum can be easily estimated (notice that $\lambda_-(s) = -3^{-s} + 5^{-s} - 7^{-s} - 11^{-s} + \dots$ is not alternating). We have

$$L_-(s) = 1 - 3^{-s} + 5^{-s} - 7^{-s} + \dots = (1 - 3^{-s}) + (5^{-s} - 7^{-s}) + \dots$$

from which it follows that $L_-(s) > (1 - 3^{-s}) > 2/3$ for all $s > 1$. Similarly, from

$$L_-(s) = 1 - (3^{-s} - 5^{-s}) - (7^{-s} - 9^{-s}) - \dots$$

we conclude that $L_-(s) < 1$ for all $s > 1$. To connect $L_-(s)$ and $\lambda_-(s)$, we observe that the function χ is a multiplicative homomorphism, using which and repeating the proof of Lemma 6 word-for-word, one proves that

$$L_-(s) = \prod_{p \in P} \frac{1}{1 - \chi(p)p^{-s}}$$

(see Proposition 16(i) for a general statement). Then proceeding as in the proof of Proposition 7, we see that

$$\ln L_-(s) = \sum_{p \in P} -\ln(1 - \chi(p)p^{-s})$$

and

$$-\ln(1 - \chi(p)p^{-s}) = \frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{2p^{2s}} + \frac{\chi(p)^3}{3p^{3s}} + \dots$$

It follows that

$$\ln L_-(s) = \lambda_-(s) + h(s)$$

where $h(s)$ is a function that remains bounded as $s \rightarrow 1^+$. We showed above that $2/3 < L_-(s) < 1$ for all $s > 1$, so the boundedness of $\lambda_-(s)$ as $s \rightarrow 1^+$ follows. \square

2.3 The proof of Dirichlet's Theorem

The function χ used in Section 2.2 to separate $P_{1(4)}$ and $P_{3(4)}$ can be viewed as a character of $(\mathbb{Z}/4\mathbb{Z})^*$ extended by 0 on the numbers (or classes of numbers mod 4) that are not relatively prime to 4. So, it is not surprising that the proof of Dirichlet's theorem for arbitrary m uses characters of $(\mathbb{Z}/m\mathbb{Z})^*$ extended to $\mathbb{Z}/m\mathbb{Z}$ by 0 on the classes that are not relatively prime to m . For this reason, we begin with a brief discussion of characters of finite abelian groups, following [Se], Ch. VI, Sec. 1.

Let G be a finite abelian group. By a **character** of G we mean a group homomorphism $\chi: G \rightarrow \mathbb{C}^*$. All characters of G form a group under the operation $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$, which will be denoted \widehat{G} and called the **dual** of G .

Example 2.3.1. Let $G = \mathbb{Z}/n\mathbb{Z}$. Then any $\chi \in \widehat{G}$ is completely determined by its value $\chi(\bar{1})$. Since $\bar{1}$ has order n , we get $\chi(\bar{1})^n = 1$, i.e. $\chi(\bar{1})$ belongs to the group μ_n of n -th roots of unity. Conversely, given any $\zeta \in \mu_n$, the correspondence $\chi: \bar{a} \rightarrow \zeta^a$ is a character of G such that $\chi(\bar{1}) = \zeta$. Thus, the map

$$\widehat{G} \ni \chi \mapsto \chi(\bar{1}) \in \mu_n$$

is a bijection. Moreover, the equation $(\chi_1\chi_2)(\bar{1}) = \chi_1(\bar{1})\chi_2(\bar{1})$ tells us that this map is a group homomorphism, hence in fact a group isomorphism. Thus, in this example $\widehat{G} \simeq \mu_n$ (noncanonically), which means that a finite cyclic group is isomorphic to its group of characters. Furthermore, if $\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n)$ then the corresponding character $\chi(\bar{a}) = \zeta_n^a$ has the property $\chi(\bar{a}) \neq 1$ whenever $\bar{a} \neq \bar{0}$, so for any nontrivial element of a cyclic group there is a character that does not vanish on this element.

We will now extend these observations to arbitrary finite abelian groups.

Proposition 9. *Let G be a finite abelian group. Then*

- (i) $G \simeq \widehat{G}$ (noncanonically), in particular, $|G| = |\widehat{G}|$;
- (ii) for any $g \in G$, $g \neq e$, there exists $\chi \in \widehat{G}$ such that $\chi(g) \neq 1$.

Proof. We first observe that if $G = G_1 \times G_2$ then the correspondence

$$\widehat{G} \xrightarrow{\theta} \widehat{G}_1 \times \widehat{G}_2, \quad \chi \mapsto (\chi|_{G_1}, \chi|_{G_2}),$$

is an isomorphism of groups. Indeed, it follows from the definition of multiplication on the character group that θ is a group homomorphism. Since G_1 and G_2 generate G , θ is injective. Finally, given $(\chi_1, \chi_2) \in \widehat{G}_1 \times \widehat{G}_2$, the map $\chi: G \rightarrow \mathbb{C}^*$ defined by $\chi(g) = \chi_1(g_1)\chi_2(g_2)$ if $g = (g_1, g_2)$ is a character of G which restricts to χ_1 and χ_2 on G_1 and G_2 respectively, proving that θ is surjective.

By the structure theorem for finite abelian groups (see [Ar], Theorem 12.6.4), $G \simeq G_1 \times \cdots \times G_r$, where G_i are cyclic groups. Then it follows by induction from the above remark that the correspondence

$$\widehat{G} \xrightarrow{\iota} \widehat{G}_1 \times \cdots \times \widehat{G}_r, \quad \chi \mapsto (\chi|_{G_1}, \dots, \chi|_{G_r}),$$

is a group isomorphism. According to the example, $\widehat{G}_i \simeq G_i$ for all $i = 1, \dots, r$, yielding (i). If now $g \in G$ is a nontrivial element then $g = (g_1, \dots, g_r)$ and there exists an i such that g_i is nontrivial. As we observed in the example, there exists $\chi_i \in \widehat{G}_i$ such that $\chi_i(g_i) \neq 1$. Then the character $\chi \in \widehat{G}$ corresponding under ι to the r -tuple $(\chi_{01}, \dots, \chi_i, \dots, \chi_{0r})$, where χ_{0j} is the trivial character of G_j , has the property $\chi(g) \neq 1$. \square

Corollary 10. *Let H be a subgroup of G , and let $\widehat{G} \xrightarrow{\rho} \widehat{H}$ be the homomorphism given by restriction. Then ρ is surjective.*

Proof. Assume the contrary. Since $|\widehat{G}| = |G|$ and $|\widehat{H}| = |H|$, this means that $|\ker \rho| > [G : H]$. But any $\chi \in \ker \rho$, having trivial restriction to H , induces a character of $\bar{\chi} \in \widehat{G/H}$ defined by $\bar{\chi}(gH) = \chi(g)$. Clearly, the map $\ker \rho \rightarrow \widehat{G/H}$, $\chi \mapsto \bar{\chi}$, is injective, so we obtain $|G/H| = |\widehat{G/H}| > [G : H]$, a contradiction. \square

For a fixed $g \in G$, the map $\delta_g: \widehat{G} \rightarrow \mathbb{C}^*$, $\delta_g(\chi) = \chi(g)$, is a character of \widehat{G} . Moreover, the map $\varepsilon: G \rightarrow \widehat{\widehat{G}}$, $g \mapsto \delta_g$ is a group homomorphism.

Corollary 11. ε is a group isomorphism. Thus, G is (canonically) isomorphic to its second dual $\widehat{\widehat{G}}$.

Indeed, it follows from (ii) that ε is injective. On the other hand, by (i), $|G| = |\widehat{G}| = |\widehat{\widehat{G}}|$, whence ε is an isomorphism.

The following proposition and especially its corollaries play a crucial role in the proof of Dirichlet's theorem.

Proposition 12. (i) Let $\chi \in \widehat{G}$. Then

$$\sum_{x \in G} \chi(x) = \begin{cases} |G| & \chi \text{ is trivial,} \\ 0 & \text{otherwise.} \end{cases}$$

(ii) Let $x \in G$. Then

$$\sum_{\chi \in \widehat{G}} \chi(x) = \begin{cases} |G| & x = e, \\ 0 & x \neq e. \end{cases}$$

Proof. (i): The first assertion is clear. To prove the second, pick $y \in G$ so that $\chi(y) \neq 1$. Then

$$\sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \left(\sum_{x \in G} \chi(x) \right) \chi(y)$$

It follows that

$$(\chi(y) - 1) \sum_{x \in G} \chi(x) = 0,$$

and therefore $\sum_{x \in G} \chi(x) = 0$.

(ii): In the notations introduced prior to Corollary 11,

$$\sum_{\chi \in \widehat{G}} \chi(x) = \sum_{\chi \in \widehat{G}} \delta_x(\chi).$$

Since $\delta_x = 1 \Leftrightarrow x = 1$, our claim follows from part (i) applied to \widehat{G} . \square

Corollary 13. For $x, y \in G$ we have

$$\sum_{\chi \in \widehat{G}} \chi(x)^{-1} \chi(y) = \begin{cases} |G| & x = y, \\ 0 & x \neq y. \end{cases}$$

Indeed, $\sum_{\chi \in \widehat{G}} \chi(x)^{-1} \chi(y) = \sum_{\chi \in \widehat{G}} \chi(x^{-1}y)$, so we can apply (ii).

Now, fix $m \geq 1$ and let $G_m = (\mathbb{Z}/m\mathbb{Z})^*$; clearly, $|G_m| = \varphi(m)$. Given $\chi \in \widehat{G_m}$, we extend it to a function on all of $\mathbb{Z}/m\mathbb{Z}$ by defining its value to be 0 on classes mod m that are not relatively prime to

m . Composing this function with the canonical homomorphism $\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ we obtain a function on \mathbb{Z} that will be denoted by the same letter χ . Notice that $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}$. A special role in the proof is played by (the function on \mathbb{Z} obtained from) the trivial character χ_0 which in this context is called the **principal character**. Thus, $\chi_0(a) = 1$ if a is relatively prime to m , and 0 otherwise. For each $\chi \in \widehat{G_m}$, we define

$$\lambda(s, \chi) = \sum_{p \in P} \frac{\chi(p)}{p^s}.$$

Since $|\chi(a)| \leq 1$ for all $a \in \mathbb{Z}$, the series in the right-hand side absolutely converges for all $s \in \mathbb{C}$, $\operatorname{Re} s > 1$.

Corollary 14. *In the notations introduced in Section 2.2, for any integer a prime to m we have*

$$\nu_{a(m)}(s) = \frac{1}{\varphi(m)} \sum_{\chi \in \widehat{G_m}} \chi(a)^{-1} \lambda(s, \chi)$$

for any $s \in \mathbb{C}$, $\operatorname{Re} s > 1$.

Indeed, using the definition of $\lambda(s, \chi)$ we obtain

$$\begin{aligned} \sum_{\chi \in \widehat{G_m}} \chi(a)^{-1} \lambda(s, \chi) &= \sum_{\chi \in \widehat{G_m}} \chi(a)^{-1} \sum_{p \in P} \frac{\chi(p)}{p^s} \\ &= \sum_{p \in P} \frac{\sum_{\chi \in \widehat{G_m}} \chi(a)^{-1} \chi(p)}{p^s} \\ &= \sum_{p \in P_{a(m)}} \frac{\varphi(m)}{p^s} = \varphi(m) \cdot \nu_{a(m)}(s) \end{aligned}$$

as

$$\sum_{\chi \in \widehat{G_m}} \chi(a)^{-1} \chi(p) = \begin{cases} \varphi(m) & p \equiv a \pmod{m}, \\ 0 & x \neq \text{otherwise.} \end{cases}$$

according to Corollary 13.

The following theorem comprises the most technically complicated part of the proof of Dirichlet's theorem.

Theorem 15. (i) *The function $\lambda(s, \chi_0)$ is unbounded as $s \rightarrow 1^+$.*

(ii) *For $\chi \neq \chi_0$, the function $\lambda(s, \chi)$ remains bounded as $s \rightarrow 1^+$.*

Theorem 15 in conjunction with Corollary 14 immediately implies Dirichlet's theorem. Indeed, Theorem 15 implies that the function

$$\nu_{a(m)}(s) = \frac{1}{\varphi(m)} \sum_{\chi \in \widehat{G_m}} \chi(a)^{-1} \lambda(s, \chi)$$

is unbounded as $s \rightarrow 1^+$. Since

$$\nu_{a(m)}(s) = \sum_{p \in P_{a(m)}} \frac{1}{p^s},$$

this implies that the set $P_{a(m)}$ is infinite.

The remaining part of this section is devoted to proving Theorem 15. Assertion (i) is easy: we obviously have

$$\lambda(s) = \sum_{p|m} \frac{1}{p^s} + \lambda(s, \chi_0),$$

so the required fact immediately follows from Proposition 7. On the contrary, assertion (ii) is very difficult. First, as we have already seen in the proof of Proposition 8, it may be easier to work instead of $\lambda(s, \chi)$ with a similar expression in which the summation runs over all natural numbers instead of just primes:

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

This series absolutely converges for $s \in \mathbb{C}$, $\operatorname{Re} s > 1$ and defines a function in this domain which is called the **Dirichlet L -function** corresponding to the character χ . The following proposition relates $L(s, \chi)$ and $\lambda(s, \chi)$.

Proposition 16. *For any character $\chi \bmod m$ and any $s \in \mathbb{C}$, $\operatorname{Re} s > 1$, we have the following:*

$$(i) L(s, \chi) = \prod_{p \in P} \frac{1}{1 - \chi(p)p^{-s}};$$

(ii) $\ln L(s, \chi) = \lambda(s, \chi) + g(s, \chi)$ where $g(s, \chi)$ is bounded as $s \rightarrow 1^+$.

Proof. (i): We will imitate the proof of Lemma 6. Again, let \mathbb{N}_d denote the set of natural numbers whose prime factors are among the first d primes p_1, \dots, p_d . For a fixed prime p we have

$$\begin{aligned} \frac{1}{1 - \chi(p)p^{-s}} &= 1 + \frac{\chi(p)}{p^s} + \left(\frac{\chi(p)}{p^s}\right)^2 + \dots \\ &= 1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \dots \end{aligned}$$

It follows that

$$\begin{aligned} \prod_{i=1}^d \frac{1}{1 - \chi(p_i)p_i^{-s}} &= \prod_{i=1}^d \left(1 + \frac{\chi(p_i)}{p_i^s} + \frac{\chi(p_i^2)}{p_i^{2s}} + \dots\right) \\ &= \sum_{n \in \mathbb{N}_d} \frac{\chi(n)}{n^s} \end{aligned}$$

because

$$\frac{\chi(p_1)^{\alpha_1}}{p_1^{\alpha_1}} \dots \frac{\chi(p_d)^{\alpha_d}}{p_d^{\alpha_d}} = \frac{\chi(p_1^{\alpha_1} \dots p_d^{\alpha_d})}{p_1^{\alpha_1} \dots p_d^{\alpha_d}}.$$

Now,

$$L(s, \chi) - \prod_{i=1}^d \frac{1}{1 - \chi(p_i)p_i^{-s}} = \sum_{n \in \mathbb{N} - \mathbb{N}_d} \frac{\chi(n)}{n^s}.$$

Since any $n \in \mathbb{N} - \mathbb{N}_d$ is $\geq d$, we have

$$\left| \sum_{n \in \mathbb{N} - \mathbb{N}_d} \frac{\chi(n)}{n^s} \right| \leq \sum_{n=d+1}^{\infty} \frac{1}{n^{\operatorname{Re} s}} \rightarrow 0 \text{ as } d \rightarrow \infty,$$

proving (i).

(ii): Here the argument is similar to the proof of Proposition 7. From (i) we derive that

$$\ln L(s, \chi) = \sum_{p \in P} -\ln(1 - \chi(p)p^{-s})$$

On the other hand,

$$-\ln(1 - \chi(p)p^{-s}) = \frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{2p^{2s}} + \frac{\chi(p)^3}{3p^{3s}} + \dots = \frac{\chi(p)}{p^s} + g_p(s, \chi)$$

where

$$g_p(s, \chi) := \frac{\chi(p)^2}{2p^{2s}} + \frac{\chi(p)^3}{3p^{3s}} + \cdots.$$

Then

$$|g_p(s, \chi)| \leq \frac{1}{2p^{2s}} + \frac{1}{3p^{3s}} + \cdots \leq \frac{1}{p^{2s}}$$

as we have seen in the proof of Proposition 7. Then for any d ,

$$\sum_{i=1}^d |g_{p_i}(s, \chi)| \leq \sum_{i=1}^d \frac{1}{p_i^{2s}} \leq \sum_{n=1}^{\infty} \frac{1}{n^2} = \zeta(2).$$

This means that for any $s > 1$, the series $\sum_{p \in P} g_p(s, \chi)$ absolutely converges, and its sum $g(s, \chi)$ satisfies $|g(s, \chi)| \leq \zeta(2)$, hence remains bounded as $s \rightarrow 1^+$. Since $\ln L(s, \chi) = \lambda(s, \chi) + g(s, \chi)$, (ii) is proven. \square

It follows from Proposition 16(ii) that to complete the proof of Theorem 15 one needs to show that if $\chi \neq \chi_0$, $L(s, \chi)$ approaches some *nonzero* number as $s \rightarrow 1^+$. This part of the argument heavily relies on complex analysis. Let

$$\zeta_m(s) = \prod_{\chi \in \widehat{G}_m} L(s, \chi).$$

Proposition 17. (i) $L(s, \chi_0)$ extends meromorphically to the domain $D = \{s \in \mathbb{C} \mid \operatorname{Re} s > 0\}$ with the only pole at $s = 1$, and this pole is simple.

(ii) For $\chi \neq \chi_0$, $L(s, \chi)$ extends holomorphically to D .

(iii) $\zeta_m(s)$ extends meromorphically to D with a pole at $s = 1$.

Assume for now Proposition 17. Then for $\chi \neq \chi_0$,

$$\lim_{s \rightarrow 1^+} L(s, \chi) = L(1, \chi),$$

which is a finite number. Suppose $L(1, \chi) = 0$ for at least one character $\chi \neq \chi_0$. Then in the product $L(s, \chi_0)L(s, \chi)$ the zero of $L(s, \chi)$ would annihilate the pole of $L(s, \chi_0)$ at $s = 1$, implying that the product is actually holomorphic at $s = 1$. Since the L -functions for all other characters are also holomorphic at $s = 1$, we would get that $\zeta_m(s)$ is holomorphic at $s = 1$, which contradicts Proposition 17(iii).

Analyticity in parts (i) and (ii) is derived from the following general statement.

Lemma 18. Let U be an open set of \mathbb{C} and let $\{f_n\}$ be a sequence of holomorphic functions on U which converges uniformly on every compact subset of U to a function f . Then f is holomorphic in U .

Proof. See [Se], pg. 64-65. \square

Proof of Proposition 17(i). First, we will show $\zeta(s)$ extends to a meromorphic function on D with a simple pole at $s = 1$. For $s > 1$ we have

$$\frac{1}{s-1} = \int_1^{\infty} t^{-s} dt = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s} dt.$$

Hence we can write

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \left(\frac{1}{n^s} - \int_n^{n+1} t^{-s} dt \right) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - t^{-s}) dt.$$

Set now

$$\phi_n(s) = \int_n^{n+1} (n^{-s} - t^{-s})dt \text{ and } \phi(s) = \sum_{n=1}^{\infty} \phi_n(s).$$

Our goal is to show that $\phi(s)$ is defined and analytic in D ; then $1/(s-1) + \phi(s)$ will be the required meromorphic extension of $\zeta(s)$. Since each of the functions $\phi_n(s)$ is analytic in D , the analyticity of ϕ will follow from Lemma 18 if we can show that the series $\sum \phi_n(s)$ converges uniformly on every compact subset of D . But any compact subset of D is contained in

$$K_{\sigma,c} = \{s \in \mathbb{C} \mid \operatorname{Re} s \geq \sigma, |s| \leq c\}$$

for some $c, \sigma > 0$. Let $\psi_{n,s}(t) = n^{-s} - t^{-s}$. Then for any $t_0 \in [n, n+1]$ we have

$$\begin{aligned} |\psi_{n,s}(t_0)| &= |\psi_{n,s}(t_0) - \psi_{n,s}(n)| \\ &\leq \max_{t \in [n, n+1]} |\psi'_{n,s}(t)| \cdot |t_0 - n| \\ &\leq \max_{t \in [n, n+1]} \left| \frac{s}{t^{s+1}} \right| = \frac{|s|}{n^{\operatorname{Re} s + 1}}. \end{aligned}$$

So, for $s \in K_{\sigma,c}$, we have

$$|\phi_n(s)| \leq \max_{t \in [n, n+1]} |\psi_{n,s}(t)| \leq \frac{|s|}{n^{\operatorname{Re} s + 1}} \leq \frac{c}{n^{\sigma + 1}}.$$

Since the series $\sum \frac{c}{n^{\sigma+1}}$ converges, the series $\sum \phi_n(s)$ uniformly converges on $K_{\sigma,c}$ by the Weierstrass M -test (cf. [Ru], Theorem 7.10).

Now, it remains to relate $\zeta(s)$ and $L(s, \chi_0)$. Suppose $m = q_1^{\alpha_1} \cdots q_r^{\alpha_r}$. Let \mathbb{N}' be the set of all natural numbers of the form $q_1^{\beta_1} \cdots q_r^{\beta_r}$, and let \mathbb{N}'' be the set of all natural numbers that are relatively prime to m . Then any $n \in \mathbb{N}$ can be uniquely written in the form $n = n'n''$ with $n' \in \mathbb{N}'$, $n'' \in \mathbb{N}''$. It follows that

$$\zeta(s) = \sum_{n \in \mathbb{N}} \frac{1}{n^s} = \left(\sum_{n \in \mathbb{N}'} \frac{1}{n^s} \right) \left(\sum_{n \in \mathbb{N}''} \frac{1}{n^s} \right)$$

But

$$\sum_{n \in \mathbb{N}'} \frac{1}{n^s} = L(s, \chi_0)$$

and

$$\sum_{n \in \mathbb{N}''} \frac{1}{n^s} = \left(1 + \frac{1}{q_1^s} + \frac{1}{q_1^{2s}} + \cdots \right) \cdots \left(1 + \frac{1}{q_r^s} + \frac{1}{q_r^{2s}} + \cdots \right) = \prod_{i=1}^r \frac{1}{1 - q_i^{-s}}.$$

So, $L(s, \chi_0) = \zeta(s)F(s)$, where $F(s) = \prod_{i=1}^r (1 - q_i^{-s})$. Since $F(s)$ is holomorphic and has no zeroes in D , we obtain our claim. \square

Proof of Proposition 17(ii). We will prove analyticity of $L(s, \chi)$ in D for $\chi \neq \chi_0$ by showing that the series

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

converges uniformly on compact subsets of D . The proof imitates the proof of Abel's and Dirichlet's test for convergence of series of the form $\sum a_n b_n$ (cf. [Ru], Theorem 3.41). Let $a_n = \chi(n)$, $b_n = n^{-s}$. To apply the Cauchy criterion, we need to show that $|\sum_{n=M}^N a_n b_n|$ becomes arbitrarily small uniformly on $K_{\sigma,c}$ for $M < N$ if M is large enough. Let $A_n = \sum_{k=1}^n a_k$. The crucial thing is that the assumption

$\chi \neq \chi_0$ implies that $|A_n| \leq C$ for some constant C independent of n (which, of course, is false for $\chi = \chi_0$!). Indeed, for any $a \in \mathbb{Z}$ we have $\chi(a) = \chi(a + m)$, and besides it follows from Proposition 12(i) that

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

Thus, if $n = dm + r$ where $0 \leq r < m$ then

$$A_n = \sum_{k=1}^n \chi(k) = \sum_{k=dm+1}^{dm+r} \chi(k) = \sum_{k=1}^r \chi(k) = A_r$$

where by convention $A_0 = 0$. So, $C = \max\{|A_1|, \dots, |A_{m-1}|\}$ will work.

Substituting $a_n = A_n - A_{n-1}$, we get

$$\sum_{n=M}^N a_n b_n = \sum_{n=M}^{N-1} A_n (b_n - b_{n+1}) + A_N b_N - A_{M-1} b_M. \quad (2.9)$$

We have seen in the proof of part (i) that

$$|n^{-s} - (n+1)^{-s}| \leq \frac{|s|}{n^{\operatorname{Re} s + 1}}.$$

So it follows from (2.9) that

$$\left| \sum_{n=M}^N a_n b_n \right| \leq \sum_{n=M}^{N-1} \frac{C|s|}{n^{\operatorname{Re} s + 1}} + \frac{C}{M^{\operatorname{Re} s}} + \frac{C}{N^{\operatorname{Re} s}}.$$

Thus, if $s \in K_{\sigma, c}$ then

$$\left| \sum_{n=M}^N a_n b_n \right| \leq Cc \sum_{n=M}^{N-1} \frac{1}{n^{\sigma+1}} + \frac{2C}{M^\sigma}.$$

Since the series $\sum \frac{1}{n^{\sigma+1}}$ converges, we see that $|\sum_{n=M}^N a_n b_n|$ becomes arbitrarily small uniformly on $K_{\sigma, c}$ if M is large enough, completing the proof. \square

Proof of Proposition 17(iii). We only need to show that $\zeta_m(s)$ cannot be holomorphic at $s = 1$.

Lemma 19. For an integer a prime to m , let $f(a)$ denote the order of \bar{a} in G_m , and let $g(a) = \varphi(m)/f(a)$. If T is a variable then

$$\prod_{\chi \in \widehat{G_m}} (1 - \chi(a)T) = (1 - T^{f(a)})^{g(a)}.$$

Proof. Let H be the cyclic subgroup of G_m generated by \bar{a} ; $|H| = f(a)$. Then the set $\{\chi(\bar{a}) \mid \chi \in \widehat{H}\}$ is precisely the set of all $f(a)$ -th roots of unity. It follows that

$$\prod_{\chi \in \widehat{H}} (X - \chi(a)) = X^{f(a)} - 1.$$

Substituting $X = T^{-1}$ and multiplying by $T^{f(a)}$, we get

$$\prod_{\chi \in \widehat{H}} (1 - \chi(a)T) = 1 - T^{f(a)}.$$

Now, the homomorphism of restriction $\widehat{G}_m \rightarrow \widehat{H}$ is surjective (Corollary 11) and its kernel has order $g(a)$. It follows that

$$\prod_{\chi \in \widehat{G}_m} (1 - \chi(a)T) = \left(\prod_{\chi \in \widehat{H}} (1 - \chi(a)T) \right)^{g(a)} = (1 - T^{f(a)})^{g(a)}.$$

□

Using Lemma 19, we can transform the expression for $\zeta_m(s)$:

$$\zeta_m(s) = \prod_{\chi \in \widehat{G}_m} L(s, \chi) = \prod_{p \in P} \left(\prod_{\chi \in \widehat{G}_m} \frac{1}{1 - \chi(p)p^{-s}} \right) = \prod_{(p,m)=1} \frac{1}{(1 - p^{-f(p)s})^{g(p)}}. \quad (2.10)$$

Since

$$\frac{1}{(1 - p^{-f(p)s})} = 1 + \frac{1}{p^{f(p)s}} + \frac{1}{p^{2f(p)s}} + \dots,$$

it follows from (2.10) that $\zeta_m(s)$ can be written in the form

$$\zeta_m(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s} \quad (2.11)$$

(a **Dirichlet series**) with $c_n \geq 0$, and the series converges for $|s| > 1$. Assume now that $\zeta_m(s)$ is holomorphic at $s = 1$. Then $\zeta_m(s)$ is holomorphic everywhere in D . By applying [Se], Prop. 7, Ch. VI, we conclude that the series in (2.11) converges everywhere in D . To see that this is false, we observe that

$$\begin{aligned} \frac{1}{(1 - p^{-f(p)s})^{g(p)}} &= (1 + p^{-f(p)s} + p^{-2f(p)s} + \dots)^{g(p)} \\ &\geq 1 + p^{-\varphi(m)s} + p^{-2\varphi(m)s} + \dots = \frac{1}{1 - p^{-\varphi(m)s}}. \end{aligned}$$

So,

$$\sum_{n=1}^{\infty} \frac{c_n}{n^s} \geq \prod_{(p,m)=1} \frac{1}{1 - p^{-\varphi(m)s}} = \sum_{(n,m)=1} n^{-\varphi(m)s} = L(\varphi(m)s, \chi_0).$$

But we already know that $L(\varphi(m)s, \chi_0)$ diverges for $s = \varphi(m)^{-1}$, so $\sum \frac{c_n}{n^s}$ cannot converge for the same value of s . A contradiction. □

This concludes the proof of Dirichlet's theorem.

References

- [Ar] Michael Artin: *Algebra*. Englewood Cliffs, N.J.: Prentice Hall, 1991.
- [Co] David A. Cox: *Galois Theory*. Hoboken, N.J.: Wiley-Interscience, 2004.
- [IR] Kenneth Ireland and Michael Rosen: *A Classical Introduction to Modern Number Theory*. New York: Springer, 1990 (Graduate Texts in Math. **84**).
- [Kn] Anthony W. Knap: *Elliptic Curves*. Princeton, N.J.: Princeton Univ. Press, 1992 (Mathematical Notes **40**).
- [La] Serge Lang: *Algebra*. New York: Springer, 2002 (Graduate Texts in Math. **211**).
- [Ru] Walter Rudin: *Principles of Mathematical Analysis*. New York: McGraw-Hill Book Co., 1976.
- [Se] Jean-Pierre Serre: *A Course in Arithmetic*. New York: Springer, 1973 (Graduate Texts in Math. **7**).