17 Dirichlet characters and primes in arithmetic progressions

Having proved the Prime Number Theorem, we would like to prove an analogous result for primes in arithmetic progressions. We begin with Dirichlet's theorem on primes in arithmetic progressions, a result that predates the prime number theorem by nearly sixty years (indeed Dirichlet died 37 years before the prime number theorem was proved).

Theorem 17.1 (Dirichlet 1837)**.** *For every $a, m \in \mathbb{Z}_{\geq 1}$ with $\gcd(a, m) = 1$ there are infinitely many primes $p \equiv a \bmod m$.*

In fact Dirichlet proved more than this. In a sense that we will make precise below, he proved that for any fixed modulus $m \geq 1$ the primes are equidistributed among the residue classes in $(\mathbb{Z}/m\mathbb{Z})^\times$. The equidistribution statement that Dirichlet was able to prove is a bit weaker than one might like, but it is more than enough to establish Theorem 17.1.

Remark 17.2. Many of the standard tools of complex analysis that we take for granted were not available to Dirichlet in 1837. Riemann was the first to seriously study $\zeta(s)$ as a function of a complex variable, some twenty years after Dirichlet proved his theorem on primes in arithmetic progressions. Rather than retracing Dirichlet's steps exactly, we work in a more modern setting, but our proof is still very much in the spirit of Dirichlet.

17.1 Infinitely many primes

To motivate Dirichlet's method of proof, let us consider the following proof that there are infinitely many primes. To prove this, it suffices to show that the Euler product

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$$

diverges as $s \to 1^+$. Of course we know this to be the case, since $\zeta(s)$ has a pole at $s = 1$, but let us proceed by taking logarithms and showing that the sum

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

diverges as $s \to 1^+$, since we have the asymptotic bounds

$$-\log(1 - x) = x + O(x^2) \quad (\text{as } x \to 0) \qquad \text{and} \qquad \sum_p O(p^{-2s}) = O(1) \quad (\mathrm{Re}(s) > 1/2).$$

We can estimate $\sum_{p \leq x} \frac{1}{p}$ via Mertens' second theorem, one of three he proved in [4].

Theorem 17.3 (Mertens 1874)**.** *As $x \to \infty$ we have*

(1) $\displaystyle\sum_{p \leq x} \frac{\log p}{p} = \log x + R(x)$*, where* $|R(x)| < 2$.[1]

(2) $\displaystyle\sum_{p \leq x} \frac{1}{p} = \log\log x + B + O\big(\tfrac{1}{\log x}\big)$*, where* $B = 0.261497\ldots$ *is Mertens' constant;*

[1] In fact, $R(x) = -B_3 + o(1)$ where $B_3 = 1.332582\ldots$ is an explicit constant.

(3) $\sum_{p\le x} \log\big(1-\frac{1}{p}\big) = -\log\log x - \gamma + O\big(\frac{1}{\log x}\big)$, *where* $\gamma = 0.577216\ldots$ *is Euler's constant.*

Proof. See Problem Set 9. □

Thus not only does $\sum p^{-s}$ diverge as $s \to 1^+$, we can say with a fair degree of precision how quickly this happens. We should note, however, that the estimate provided by Mertens' 2nd theorem is not as strong as that given by the prime number theorem. Indeed, as you will prove on Problem Set 9, the Prime Number Theorem is equivalent to the statement

$$\sum_{p\le x} \frac{1}{p} = \log\log x + B + o\left(\tfrac{1}{\log x}\right),$$

which is (ever so slightly) sharper than Mertens' estimate.[2][3]

17.1.1 Infinitely many primes congruent to 1 modulo 4

To see how the argument above generalizes to primes in arithmetic progressions, let us prove that there are infinitely many primes congruent to 1 mod 4. We might initially consider

$$\prod_{p\,\equiv\,1 \bmod 4} (1-p^{-s})^{-1} = \sum_{\substack{n\ge 1\\ p\mid n \Rightarrow p\,\equiv\,1 \bmod 4}} n^{-s},$$

but the sum on the RHS is a bit awkward. Let us instead define a *Dirichlet character*

$$\chi(n) := \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4,\\ -1 & \text{if } n \equiv -1 \bmod 4,\\ 0 & \text{otherwise,}\end{cases}$$

and consider the *Dirichlet L-function*

$$L(s,\chi) := \prod_p (1-\chi(p)p^{-s})^{-1} = \sum_{n\ge 1} \chi(n) n^{-s} = 1 - 3^{-s} + 5^{-s} - 7^{-s} + 9^{-s} + \cdots.$$

As $s \to 1^+$ we have

$$\begin{aligned}\log L(s,\chi) &= -\sum_p \log(1-\chi(p)p^{-s}) = \sum_p \chi(p)p^{-s} + O(1)\\ &= \sum_{p\,\equiv\,1 \bmod 4} p^{-s} - \sum_{p\,\equiv\,3 \bmod 4} p^{-s} + O(1),\end{aligned}$$

and

$$\log\zeta(s) = \sum_{p\,\equiv\,1 \bmod 4} p^{-s} + \sum_{p\,\equiv\,3 \bmod 4} p^{-s} + O(1),$$

thus

$$\frac{\log\zeta(s) + \log L(s,\chi)}{2} = \sum_{p\,\equiv\,1 \bmod 4} p^{-s} + O(1).$$

[2] In fact the error term in the PNT implies $\sum_{p\le x} \frac{1}{p} = \log\log x + B + O\big(\frac{1}{x}\big)$.

[3] The fact that the difference between a little-o and a big-O is the difference between proving a celebrated theorem and not proving it emphasizes how critical it is to understand error terms.

Provided $\log L(s,\chi) = O(1)$ as $s \to 1^+$, the LHS (and hence the RHS) must tend to infinity as $s \to 1^+$, since $\zeta(s) \to \infty$ as $s \to 1^+$. It thus suffices to show that $L(s,\chi)$ has an analytic continuation to a neighborhood of 1, and that $L(1,\chi) \neq 0$. Assuming this is the case,

$$\sum_{\substack{p \le x \\ p \equiv 1 \bmod 4}} \frac{1}{p} = \frac{1}{2}\log\log x + O(1).$$

and Mertens' 2nd theorem implies that the same holds if we instead sum over $p \equiv 3 \mod 4$. The primes are thus equidistributed modulo 4 in the sense that for $m = 4$ and all integers a coprime to m we have

$$\sum_{\substack{p \le x \\ p \equiv a \bmod m}} \frac{1}{p} \sim \frac{1}{\phi(m)} \sum_{p \le x} \frac{1}{p} \sim \frac{1}{\phi(m)} \log\log x$$

We should note that this statement is weaker than what is known as the "prime number theorem for arithmetic progressions", which states that

$$\pi(x; m, a) \sim \frac{1}{\phi(m)}\pi(x),$$

where $\pi(x; m, a)$ counts the primes $p \le x$ for which $p \equiv a \bmod m$.

Dirichlet did not have Mertens' asymptotic bounds so he stated his results in a different form by defining what is now called the *Dirichlet density* of a set of primes S,

$$d(S) := \lim_{s \to 1^+} \frac{\sum_{p \in S} p^{-s}}{\sum_p p^{-s}},$$

which is defined whenever this limit exists (one can also define notions of lower and upper Dirichlet density using lim inf and lim sup that are always defined). This definition differs from the more common *natural density*

$$\delta(S) := \lim_{x \to \infty} \frac{\#\{p \le x : p \in S\}}{\#\{p \le x\}}.$$

Dirichlet proved that for $m \ge 1$ and a relatively prime to m the set of primes $p \equiv a \bmod m$ has Dirichlet density $1/\phi(m)$, whereas the prime number theorem for arithmetic progressions states that this set has natural density $1/\phi(m)$. One can show that if a set of primes S has a natural density then it has a Dirichlet density and the two are equal, but the converse need not hold: there are sets of primes that have a Dirichlet density but no natural density.

In order to complete our proof that there are infinitely many primes $p \equiv 1 \bmod 4$, we need to show $L(1,\chi) \neq 0$. To do this we need to consider the *Dedekind zeta function* of a number field K,

$$\zeta_K(s) := \sum_I N(I)^{-s} = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1},$$

here the sum ranges over nonzero ideals of the ring of integers $\mathcal{O}_K$, the product ranges over nonzero prime ideals of $\mathcal{O}_K$ (primes of K), and $N(I) := [\mathcal{O}_K : I]$ is the absolute norm.[4] Note that $\zeta_{\mathbb{Q}}(s) = \zeta(s)$, so this is a natural generalization of the Riemann zeta function.

[4]The Dedekind zeta function is named after Richard Dedekind, the last doctoral student of Gauss. He received his Ph.D. in 1854, the same year as Riemann, another student of Gauss; Dedekind and Riemann both studied under Dirichlet as well.

The proof that the Euler product converges for $\mathrm{Re}(s) > 1$ is just a generalization of the proof for $\zeta_{\mathbb{Q}}(s) = \zeta(s)$; we now use unique factorization of ideals in the Dedekind domain O_K to convert the sum over ideals I into a product over prime ideals $\mathfrak{p}$. The number of prime ideals $\mathfrak{p}$ lying above any particular prime p is at most $n = [K : \mathbb{Q}]$, and for $\mathrm{Re}(s) > 1$ we have $|N(\mathfrak{p})^{-s}| \le |p^{-s}|$ for each $\mathfrak{p}|p$. We thus have

$$\sum_{\mathfrak{p}} \left|\log(1 - N(\mathfrak{p})^{-s})\right| \;\le\; n \sum_{p} \left|\log(1 - p^{-s})\right|,$$

and since the later sum converges, so does the former.

We are interested in the case $K = \mathbb{Q}(i)$. We can rewrite the Euler product for $\zeta_K(s)$ as

$$\begin{aligned}
\zeta_K(s) &= \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1} \\
&= \prod_{p} \prod_{\mathfrak{p}|p} (1 - N(\mathfrak{p})^{-s})^{-1} \\
&= (1 - 2^{-s})^{-1} \prod_{p \equiv 1 \bmod 4} (1 - p^{-s})^{-1}(1 - p^{-s})^{-1} \prod_{p \equiv 3 \bmod 4} (1 - p^{-2s})^{-1} \\
&= (1 - 2^{-s})^{-1} \prod_{p \equiv 1 \bmod 4} (1 - p^{-s})^{-1}(1 - p^{-s})^{-1} \prod_{p \equiv 3 \bmod 4} (1 - p^{-s})^{-1}(1 + p^{-s})^{-1} \\
&= \prod_{p} (1 - p^{-s})^{-1} \prod_{p} (1 - \chi(p)p^{-s})^{-1} \\
&= \zeta(s) L(s, \chi).
\end{aligned}$$

In the calculation above we have use the fact that we have

- one prime $\mathfrak{p}$ of norm $N(\mathfrak{p}) = 2$ above the unique prime 2 that ramifies in $\mathbb{Q}(i)$;
- two primes $\mathfrak{p}, \bar{\mathfrak{p}}$ of norm $N(\mathfrak{p}) = N(\bar{\mathfrak{p}}) = p$ above each prime p that spits in $\mathbb{Q}(i)$, equivalently, the primes $p \equiv 1 \bmod 4$;
- one prime $\mathfrak{p}$ of norm $N(\mathfrak{p}) = p^2$ above each prime p that remains inert in $\mathbb{Q}(i)$, equivalently, the primes $p \equiv 3 \bmod 4$.

We now note that $\zeta(s)$ has a simple pole at $s = 1$, so if we can show that $\zeta_K(s)$ extends to a meromorphic function that has a simple pole at $s = 1$ then we will know that (1) $L(s, \chi)$ extends to a meromorphic function on a region that includes $s = 1$ (since it is the ratio of two such functions); and (2) $L(1, \chi) \neq 0$, since we must have $\mathrm{ord}_{s=1} L(s, \chi) = 0$.

In fact $\zeta_K(s)$ does extend to a meromorphic function on $\mathrm{Re}(s) > \frac{1}{2}$ with a simple pole at $s = 1$; this can be proved directly, but it follows from a much more general and striking result, the *analytic class number formula*, which was also proved by Dirichlet (at least for quadratic fields). We will prove the analytic class number formula in the next lecture; in the remainder of this lecture will will focus on generalizing our argument above to arbitrary m.

17.2 Characters of finite abelian groups

Our first step is to generalize the Dirichlet character χ that we defined above; for this we need to recall a few facts about characters of finite abelian groups; the domain $\mathbb{Z}$ of the Dirichlet character χ we used in the case $m = 4$ is not a finite abelian group, but χ restricts to a character of the multiplicative group $(\mathbb{Z}/4\mathbb{Z})^\times$.

Definition 17.4. A *character* of a finite abelian group G is a homomorphism $\chi\colon G \to \mathrm{U}(1)$, where $\mathrm{U}(1) := \{z \in \mathbb{C} : |z| = 1\}$ is the unitary group. The *character group* (or *dual group*) of G is the abelian group

$$G^\wedge := \hom(G, \mathrm{U}(1))$$

under point-wise multiplication: $(\chi_1\chi_2)(g) := \chi_1(g)\chi_2(g)$. The inverse is given by complex conjugation $\chi^{-1}(g) = \overline{\chi}(g) := \overline{\chi(g)}$, and the identity is the *trivial character*, which sends every $g \in G$ to $1 \in \mathrm{U}(1)$.

Proposition 17.5. *Let G be a finite abelian group with character group $G^\wedge$. Then $G \simeq G^\wedge$.*

Proof. Write G as a direct product of cyclic groups $G = \langle g_1\rangle \times \cdots \times \langle g_n\rangle$, so that each element of G can be uniquely represented as $g_1^{e_1} \cdots g_n^{e_n}$ with $e_i \in [0, n_i - 1]$, where $n_i = |g_i|$. For each g_i pick a primitive n_ith root of unity $\alpha_i \in \mathbb{C}^\times$. Define the map $\varphi\colon G \to G^\wedge$ by

$$\varphi(g_1^{e_1} \cdots g_n^{e_n}) := \left((g_1^{f_1}, \ldots, g_n^{f_n}) \mapsto \alpha_1^{e_1 f_1} \cdots \alpha_n^{e_n f_n}\right).$$

We have $\varphi(g)(h_1)\varphi(g)(h_2) = \varphi(g)(h_1h_2)$, so $\varphi(g)$ is a well-defined element of $G^\wedge$, and we also note that $\varphi(g)\varphi(h) = \varphi(gh)$, so $\varphi\colon G \to G^\wedge$ is a homomorphism,

Let μ_{n_i} denote the n_i-torsion subgroup of $\mathrm{U}(1)$ (the group of n_ith roots of unity). Let $\epsilon_i\colon \mu_{n_i} \to \mathbb{Z}/n_i\mathbb{Z}$ be the unique isomorphism for which $\epsilon_i(\alpha_i) = 1$. Define $\psi\colon G^\wedge \to G$ by

$$\psi(\chi) := g_1^{\epsilon_1(\chi(g_1))} \cdots g_n^{\epsilon_n(\chi(g_n))}.$$

We have $\epsilon_i(\chi(g_i^{e_i})) = e_i$, for each $i \in [1, n]$ and $e_i \in [1, n_i]$, thus $\psi \circ \varphi$ and $\varphi \circ \psi$ are both identity maps and φ and ψ are inverse isomorphisms. □

Corollary 17.6. *Let G be a finite abelian group. Then $g \in G$ is the identity if and only if $\chi(g) = 1$ for all $\chi \in G^\wedge$ and $\chi \in G^\wedge$ is the identity if and only if $\chi(g) = 1$ for all $g \in G$.*

Proof. This is clear when g or χ is the identity. If $g \neq 1_G$ then we can choose g_1 with order $n_1 > 1$ as in the proof of the proposition so that $g \in \langle g_1\rangle$, and if we then put $\chi = \psi(g)$ we have $\chi(g) = \alpha_1 \neq 1$. If $\chi \neq 1_{G^\wedge}$ then by definition, $\chi(g) \neq 1$ for some $g \in G$. The second statement is immediate. □

The isomorphism in Proposition 17.5 is not canonical. Indeed, there are $\#\mathrm{Aut}(G)$ distinct ways to choose the α_i used to construct the isomorphism φ. But there is a canonical isomorphism from G to $G^{\wedge\wedge}$ (the character group of $G^\wedge$).

Corollary 17.7. *Let G be a finite abelian group. The evaluation map*

$$g \mapsto (\chi \mapsto \chi(g))$$

is a canonical isomorphism from G to $G^{\wedge\wedge}$.

Proof. If g is in the kernel of this map, then $\chi(g) = 1$ for all $\chi \in G^\wedge$ and therefore $g = 1_G$, by Corollary 17.6, and $G \simeq G^\wedge \simeq G^{\wedge\wedge}$, so it is an isomorphism. □

Corollary 17.7 allows us to view G as the character group of $G^\wedge$ by defining $g(\chi) := \chi(g)$.

Remark 17.8. Corollary 17.7 is a special case of *Pontryagin duality*, which applies to any locally compact abelian group G. In general, the dual group $G^\wedge$ is the group of continuous homomorphisms from G to $\mathrm{U}(1)$; when G is finite with the discrete topology, every homomorphism is continuous so the continuity requirement is superfluous. For infinite groups, G and $G^\wedge$ need not be isomorphic, for example, $\mathbb{Z}^\wedge \simeq \mathrm{U}(1)$ is uncountable, but in some cases they are; this holds for $\mathbb{R}$ and $\mathbb{Q}_p$, and in fact for any local field k; see [3, XV, Lemma 2.2.1]. But in every case, the canonical isomorphism $G \simeq G^{\wedge\wedge}$ always holds.

This is analogous to the situation with vector spaces: finite dimensional vector spaces are isomorphic to their dual, infinite dimensional vector spaces need not be, but every vector space V is canonically isomorphic to its double-dual (and the isomorphism is given by the evaluation map). But we should note that for a locally compact topological vector space V over a field k, the Pontryagin dual is not the same thing as the vector space dual; in the former case we are considering continuous homomorphisms from the additive group of V to $\mathrm{U}(1)$, whereas in the later we are considering linear maps from V to k; for example, the vector space dual $\mathbb{Q}^\vee$ is isomorphic to $\mathbb{Q}$ but the Pontryagin dual of $\mathbb{Q}$ is uncountable.

Proposition 17.9. *Let G be a finite abelian group. For all $g_1, g_2 \in G$ we have*

$$\langle g_1, g_2\rangle := \frac{1}{\#G}\sum_{\chi\in G^\wedge} \chi(g_1)\overline{\chi(g_2)} = \begin{cases} 1 & \text{if } g_1 = g_2,\\ 0 & \text{if } g_1 \neq g_2,\end{cases}$$

and for all $\chi_1, \chi_2 \in G$ we have

$$\langle \chi_1, \chi_2\rangle := \frac{1}{\#G}\sum_{g\in G} \chi_1(g)\overline{\chi_2(g)} = \begin{cases} 1 & \text{if } \chi_1 = \chi_2,\\ 0 & \text{if } \chi_1 \neq \chi_2.\end{cases}$$

Proof. If $g_1 = g_2$ then $\chi(g_1)\overline{\chi(g_2)} = 1$ for all $\chi \in G^\wedge$ and $\langle g_1, g_2\rangle = \#G^\wedge/\#G = 1$; we similarly have $\langle \chi_1, \chi_2\rangle = 1$ whenever $\chi_1 = \chi_2$.

If $g_1 \neq g_2$ then there is a $\chi_0 \in G^\wedge$ for which $\lambda := \chi_0(g_1)\overline{\chi_0(g_2)} = \chi_0(g_1 g_2^{-1}) \neq 1$, by Corollary 17.6. We then have $\lambda\langle g_1, g_2\rangle = \langle g_1, g_2\rangle$, since summing over $\chi_0\chi$ is the same as summing over χ, and $\lambda \neq 1$, so $\langle g_1, g_2\rangle = 0$.

If $\chi_1 \neq \chi_2$ then we can pick $g_0 \in G$ so that $\lambda := \chi_1(g_0)\overline{\chi_2(g_0)} = (\chi_1\overline{\chi_2})(g_0) \neq 1$, since $\chi_1\overline{\chi_2} = \chi_1\chi_2^{-1}$ is not the identity, and we then obtain $\langle \chi_1, \chi_2\rangle = 0$ as above. □

Corollary 17.10. *For $\chi \in G^\wedge$ we have $\sum_{g\in G}\chi(g) \neq 0$ if and only χ is the trivial character.*

Remark 17.11. The *orthogonality of characters* given by Proposition 17.9 is a special case of the orthogonality of characters one encounters in Fourier analysis on compact groups; the weighted sum over G corresponds to integrating against its Haar measure (the counting measure μ normalized so that $\mu(G) = 1$).

Proposition 17.12. *Let G be a finite abelian group. There is an inclusion reversing bijection between subgroups H of G and subgroups K of $G^\wedge$ that sends each order-n subgroup H of G to the index-n subgroup K of $G^\wedge$ consisting of the characters of G that restrict to the trivial character on H. The inverse bijection sends $K \subseteq G^\wedge$ to the subgroup H of G consisting of the element of G that are mapped to 1 by every character in K.*

Proof. Let H be a subgroup of G, let $K = \{\chi \in G^\wedge : \chi(h) = 1 \text{ for all } h \in H\}$, and let $\chi_1 := 1_{G^\wedge}$. We have

$$\#H\#K = \sum_{h\in H}\sum_{\chi\in K}\chi(h) = \sum_{h\in H}\sum_{\chi\in K}\chi(h)\overline{\chi_1(h)} = \sum_{g\in G}\sum_{\chi\in K}\chi(g)\chi_1(g) = \#G,$$

thus the index of K is equal to the order of H. It is clear that the map $H \mapsto K$ is inclusion reversing, and that the inverse bijection is as stated. □

17.3 Dirichlet characters

We now define the notion of a Dirichlet character. Historically, these preceded the notion of a group character; they were introduced by Dirichlet in 1831, at least twenty years before the notion of an abstract group had been formalized (indeed, Galois was still alive).

Definition 17.13. A function $f\colon \mathbb{Z} \to \mathbb{C}$ is called an *arithmetic function*. We say that f is *multiplicative* if $f(mn) = f(m)f(n)$ holds for all relatively prime $m, n \in \mathbb{Z}$, and *totally multiplicative* (or *completely multiplicative*) if this holds for all $m, n \in \mathbb{Z}$. For $m \in \mathbb{Z}_{\geq 1}$ we say that f is *m-periodic* if $f(n+m) = f(n)$ for all $n \in \mathbb{Z}$ and call m the *period* of f it is the least m for which this holds.

Definition 17.14. A *Dirichlet character* χ is an arithmetic function $\chi\colon \mathbb{Z} \to \mathbb{C}$ that is both periodic and totally multiplicative.

The image of a Dirichlet character is a finite subset of $\mathbb{C}$ that is closed under multiplication and not equal to $\{0\}$ and is thus the union of a finite subgroup of the unit circle $\mathrm{U}(1)$ and a subset of $\{0\}$. The constant function $\mathbb{1}$ is the *trivial Dirichlet character*; it is the unique Dirichlet character of period 1. Each m-periodic Dirichlet character χ restricts to a group character χ on $(\mathbb{Z}/m\mathbb{Z})^\times$; conversely, every group character χ of $(\mathbb{Z}/m\mathbb{Z})^\times$ can be extended to a Dirichlet character χ by defining $\chi(n) = 0$ for $n \notin (\mathbb{Z}/m\mathbb{Z})^\times$.

Remark 17.15. Of course when we write $n \notin (\mathbb{Z}/m\mathbb{Z})^\times$ for an integer $n \in \mathbb{Z}$, we are referring to the image of n under the quotient map $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Definition 17.16. A *Dirichlet character of modulus m* is an m-periodic Dirichlet character χ that is the zero-extension of a group character on $(\mathbb{Z}/m\mathbb{Z})^\times$; equivalently, a character for which $n \in (\mathbb{Z}/m\mathbb{Z})^\times \Leftrightarrow \chi(n) \neq 0$.

Remark 17.17. Some authors only define Dirichlet characters of modulus m, thereby baking m into the definition of a Dirichlet character; we will take a more flexible view.

The Dirichlet characters of modulus m form a group under multiplication that is canonically isomorphic to the character group of $(\mathbb{Z}/m\mathbb{Z})^\times$. Not every m-periodic Dirichlet character χ is a Dirichlet character of modulus m, since an m-periodic Dirichlet character need not vanish on $n \in (\mathbb{Z}/m\mathbb{Z})^\times$, but if m is the modulus of χ then this must be the case. More generally, we have the following lemma.

Lemma 17.18. *Let χ be a Dirichlet character of period m. Then χ is a Dirichlet character of modulus m' if and only if $m|m'|m^k$ for some k (which holds in particular for $m' = m$).*

Proof. We first show that χ is a Dirichlet character of modulus m. Suppose for the sake of contradiction that $\chi(n) \neq 0$ and $\gcd(m, n) > 1$ for some $n \in \mathbb{Z}$. Then $\chi(p) \neq 0$ for all primes $p|n$, since $\chi(p)\chi(n/p) = \chi(n) \neq 0$. Fix a prime $p|\gcd(m, n)$. For any $r \in \mathbb{Z}$ we have

$$\chi(r)\chi(p) = \chi(rp) = \chi(rp + m) = \chi(r + m/p)\chi(p),$$

and this implies $\chi(r) = \chi(r + m/p)$, since $\chi(p) \neq 0$. Thus χ is m/p-periodic, but this contradicts the minimality of m (the period of χ). So we must have $\chi(n) = 0$ whenever $\gcd(m, n) > 1$, which implies that χ is a Dirichlet character of modulus m.

If $m|m'|m^k$ then the prime divisors of m' coincide with those of m. It follows that

$$n \in (\mathbb{Z}/m'\mathbb{Z})^\times \iff n \in (\mathbb{Z}/m\mathbb{Z})^\times \iff \chi(n) \neq 0,$$

and χ is clearly m'-periodic (since $m|m'$), so χ is a Dirichlet character of modulus m'.

Conversely, if χ is a Dirichlet character of modulus m', then χ is m'-periodic, and therefore $m|m'$, since m is the period of χ. And since χ is a Dirichlet character of modulus m and of modulus m', for each prime p we have

$$p \notin (\mathbb{Z}/m\mathbb{Z})^\times \iff \chi(p) = 0 \iff p \notin (\mathbb{Z}/m'\mathbb{Z})^\times,$$

thus the prime divisors of m and m' coincide and m' must divide some power m^k of m. □

17.3.1 Primitive Dirichlet characters

Given a Dirichlet character χ_1 of modulus m_1 dividing m_2, we can always create a Dirichlet character χ_2 of modulus m_2 by defining $\chi_2(n) := \chi_1(n)$ for $n \in (\mathbb{Z}/m_2\mathbb{Z})^\times$ and $\chi_2(n) := 0$ otherwise. Provided m_2 is divisible by a prime p that does not divide m_1, the Dirichlet characters χ_1 and χ_2 will not be the same ($\chi_2(p) = 0 \neq \chi_1(p)$, for example), and we can create infinitely many new Dirichlet characters from χ_1 in this way, but they will differ from χ_1 only in a rather trivial sense. We would like to to distinguish the Dirichlet characters that do and do not arise in this way.

Definition 17.19. Let χ_1 and χ_2 be Dirichlet characters of modulus m_1 and m_2, respectively, with $m_1|m_2$. If $\chi_2(n) = \chi_1(n)$ for $n \in (\mathbb{Z}/m_2\mathbb{Z})^\times$ then χ_2 is *induced* by χ_1.

Lemma 17.20. *A Dirichlet character χ_2 of modulus m_2 is induced by a Dirichlet character of modulus $m_1|m_2$ if and only if χ_2 is constant on residue classes in $(\mathbb{Z}/m_2\mathbb{Z})^\times$ that are congruent modulo m_1. When this holds, the Dirichlet character χ_1 of modulus m_1 that induces χ_2 is uniquely determined.*

Proof. If χ_2 is induced by χ_1 then it must be constant on residue classes in $(\mathbb{Z}/m_2\mathbb{Z})^\times$ that are congruent modulo m_1, since χ_1 is. To prove the converse we first show that the surjective ring homomorphism $\mathbb{Z}/m_2\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z}$ given by reduction modulo m_1 induces a surjective homomorphism $(\mathbb{Z}/m_2\mathbb{Z})^\times \to (\mathbb{Z}/m_1\mathbb{Z})^\times$ of unit groups.[5]

Suppose $u_1 \in \mathbb{Z}$ is a unit modulo m_1. Let a be the product of all primes dividing m_2/m_1 but not u_1. Then $u_2 = u_1 + m_1 a$ is not divisible by any prime $p|m_1$ (since u_1 isn't), nor is it divisible by any prime $p|(m_2/m_1)$: by construction, such a p divides exactly one of u_1 and $m_1 a$. Thus u_2 is a unit modulo m_2 that reduces to u_1 modulo m_1.

The surjectivity of the homomorphism $(\mathbb{Z}/m_2\mathbb{Z})^\times \to (\mathbb{Z}/m_1\mathbb{Z})^\times$ induced by reduction modulo m_1 implies that if χ is constant on residue classes of $(\mathbb{Z}/m_2\mathbb{Z})^\times$ that are congruent modulo m_1, then it uniquely determines a group character of $(\mathbb{Z}/m_1\mathbb{Z})^\times$ that can be zero-extended to a Dirichlet character χ_1 of modulus m_1, and χ_1 then induces χ_2. □

Definition 17.21. A Dirichlet character is *primitive* if it is not induced by any Dirichlet character other than itself. A Dirichlet character χ induced by $\mathbb{1}$ is called *principal* (and is primitive only if $\chi = \mathbb{1}$).

[5] In fact, one can show that every surjective homomorphism of finite rings induces a surjective homomorphism of unit groups, but this does not hold in general (consider $\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$, for example).

For each integer $m > 1$ we use $\mathbb{1}_m$ to denote the principal Dirichlet character of modulus m; it corresponds to the identity element under the canonical isomorphism between Dirichlet characters of modulus m and the character group of $(\mathbb{Z}/m\mathbb{Z})^\times$.

Lemma 17.22. *Let χ be a Dirichlet character of modulus m. Then*

$$\sum_{n \in \mathbb{Z}/m\mathbb{Z}} \chi(n) \neq 0 \quad \iff \quad \chi = \mathbb{1}_m.$$

Proof. We have $\chi(n) = 0$ for $n \notin (\mathbb{Z}/m\mathbb{Z})^\times$, and the sum over $(\mathbb{Z}/m\mathbb{Z})^\times$ is nonzero if and only if χ restricts to the trivial character on $(\mathbb{Z}/m\mathbb{Z})^\times$, by Corollary 17.10. □

Note that the principal Dirichlet characters $\mathbb{1}_m$ and $\mathbb{1}_{m'}$ necessarily coincide when $m|m'|m^k$; for example the principal Dirichlet character of modulus 2 (the parity function) is the same as the principal Dirichlet character of modulus 4 (and every power of 2).

Theorem 17.23. *Every Dirichlet character χ is induced by a primitive Dirichlet character $\widetilde{\chi}$ that is uniquely determined by χ.*

Proof. Let us define a partial ordering $\preceq$ on the set of all Dirichlet characters by defining $\chi_1 \preceq \chi_2$ if χ_1 induces χ_2. The relation $\preceq$ is clearly reflexive, and it follows from Lemma 17.20 that it is transitive.

Let χ be a Dirichlet character of period m and consider the set $X = \{\chi' : \chi' \preceq \chi\}$. Each $\chi' \in X$ necessarily has period m' dividing m and there is at most one χ' of period m' for each divisor m' of m, by Lemma 17.20. The set X is thus finite, and it is nonempty, since it contains χ.

Suppose $\chi_1, \chi_2 \in X$ have periods m_1 and m_2, respectively. Then m_1 and m_2 both divide m, as does $m_3 = \gcd(m_1, m_2)$. We have a commutative square of surjective unit group homomorphisms induced by reduction maps:

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^\times & \twoheadrightarrow & (\mathbb{Z}/m_1\mathbb{Z})^\times \\ \downarrow & & \downarrow \\ (\mathbb{Z}/m_2\mathbb{Z})^\times & \twoheadrightarrow & (\mathbb{Z}/m_3\mathbb{Z})^\times \end{array}$$

From Lemma 17.20 we know that χ is constant on residue classes in $(\mathbb{Z}/m\mathbb{Z})^\times$ that are congruent modulo either m_1 or m_2, and therefore χ is constant on residue classes in $(\mathbb{Z}/m\mathbb{Z})^\times$ that are congruent modulo m_3, as are χ_1 and χ_2 (which are determined by χ). It follows that there is a unique Dirichlet character χ_3 of modulus m_3 that induces χ, χ_1, and χ_2.

Thus every pair $\chi_1, \chi_2 \in X$ has a lower bound χ_3 under the partial ordering $\preceq$ that is compatible with the total ordering of X by period. This implies that X contains a unique element $\widetilde{\chi}$ that is minimal, both with respect to the partial ordering $\preceq$ and with respect to the total ordering by period; it must be primitive, by the transitivity of $\preceq$. □

Definition 17.24. The *conductor* of a Dirichlet character χ is the period of the unique primitive Dirichlet character $\widetilde{\chi}$ that induces χ.

Corollary 17.25. *For each integer $m \geq 1$, there is a canonical bijection between the set of Dirichlet characters of modulus m and the set of primitive Dirichlet characters whose conductor divides m. Both sets may be identified with the character group of $(\mathbb{Z}/m\mathbb{Z})^\times$.*

Proof. By Theorem 17.23, we have a canonical injective map $\chi \to \widetilde{\chi}$ from the set of Dirichlet characters χ of modulus m to the set of primitive Dirichlet characters whose conductor divides m. This map is also surjective, since each primitive Dirichlet character $\widetilde{\chi}$ of conductor dividing m can be used to define a Dirichlet character χ of modulus m induced by $\widetilde{\chi}$ by defining $\chi(n) := \widetilde{\chi}(n)$ for $n \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $\chi(n) := 0$ otherwise.

As already noted, there is a canonical bijection between the group of Dirichlet characters of modulus m and the character group of $(\mathbb{Z}/m\mathbb{Z})^\times$: each Dirichlet character of modulus m can be composed with reduction modulo m to obtain a character of $(\mathbb{Z}/m\mathbb{Z})^\times$, and each character of $(\mathbb{Z}/m\mathbb{Z})^\times$ can be zero-extended to a Dirichlet character of modulus m. □

Corollary 17.26. *For a Dirichlet character χ of modulus m we have $\sum_{n\in\mathbb{Z}/m\mathbb{Z}} \chi(n) \neq 0$ if and only if χ has conductor 1.*

Proof. This follows from Lemma 17.22; the principal character $\mathbb{1}_m$ is the unique character of modulus m of conductor 1. □

Example 17.27. 12-periodic Dirichlet characters, ordered by period m and conductor c.

m	c	0	1	2	3	4	5	6	7	8	9	10	11	mod-12	principal	primitive
1	1	1	1	1	1	1	1	1	1	1	1	1	1	no	yes	yes
2	1	0	1	0	1	0	1	0	1	0	1	0	1	no	yes	no
3	1	0	1	1	0	1	1	0	1	1	0	1	1	no	yes	no
3	3	0	1	-1	0	1	-1	0	1	-1	0	1	-1	no	no	yes
4	4	0	1	0	-1	0	1	0	-1	0	1	0	-1	no	no	yes
6	1	0	1	0	0	0	1	0	1	0	0	0	1	yes	yes	no
6	3	0	1	0	0	0	-1	0	1	0	0	0	-1	yes	no	no
12	4	0	1	0	0	0	1	0	-1	0	0	0	-1	yes	no	no
12	12	0	1	0	0	0	-1	0	-1	0	0	0	1	yes	no	yes

17.4 Dirichlet L-functions

Definition 17.28. The *Dirichlet L-function* associated to a Dirichlet character χ is

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

which converges for $\operatorname{Re} s > 1$.

For the trivial Dirichlet character $\mathbb{1}$ have $L(s,\mathbb{1}) = \zeta(s)$. For the principal character $\mathbb{1}_m$ of modulus m induced by $\mathbb{1}$ we have

$$\zeta(s) = L(s,\mathbb{1}_m) \prod_{p|m} \frac{1}{1-p^{-s}}.$$

The product on the right is finite, hence it is bounded and nonzero as $s \to 1^+$, so the L-function $L(s,\mathbb{1}_m)$ has a simple pole at $s = 1$ of residue

$$\operatorname{res}_{s=1} L(s,\mathbb{1}_m) = \prod_{p|m}(1-p^{-1}) = \frac{\phi(m)}{m}.$$

But the L-functions of non-principal Dirichlet characters do not have a pole at $s = 1$.

Proposition 17.29. *Let χ be a non-principal Dirichlet character of modulus m. Then $L(s,\chi)$ extends to a holomorphic function on* $\operatorname{Re} s > 0$.

Proof. Let χ be a non-principal Dirichlet character of modulus m. Define the function $T\colon \mathbb{R}_{\geq 0} \to \mathbb{C}$ by

$$T(x) := \sum_{0<n\leq x} \chi(n).$$

For any $x \in \mathbb{R}_{\geq 0}$ Lemma 17.26 implies

$$T(x+m) - T(x) = \sum_{x<n\leq x+m} \chi(n) = \sum_{n\in\mathbb{Z}/m\mathbb{Z}} \chi(n) = 0,$$

since χ is non-principal. Thus $T(x)$ is periodic modulo m and is therefore bounded.

Writing $L(s,\chi)$ as a Stieltjes integral and integrating by parts yields

$$\begin{aligned} L(s,\chi) &= \sum_{n\geq 1} \chi(n) n^{-s} \\ &= \int_0^\infty x^{-s} dT(x) \\ &= x^{-s}T(x)\Big|_0^\infty - \int_0^\infty T(x) d(x^{-s}) \\ &= 0 - \int_0^\infty T(x)(-sx^{-s-1})dx \\ &= s\int_0^\infty T(x)x^{-s-1}dx. \end{aligned}$$

As a function of s, the RHS extends to a holomorphic function on $\operatorname{Re} s > 0$, since it is the limit of the uniformly converging sequence of functions $\phi_n(s) := s\int_0^n T(x)x^{-s-1}dx$ (here we use the fact that $T(x)$ is bounded). □

Remark 17.30. In fact, $L(s,\chi)$ extends to a holomorphic function on $\mathbb{C}$ whenever χ is non-principal.

17.5 Stieltjes integrals

For the benefit of those who have not seen them before, we recall a few facts about Stieltjes integrals (also called Riemann-Stieltjes integrals), taken from [1, Ch. 7]. These generalize the Riemann integral but are less general than the Lebesgue integral; they provide a handy way for converting sums to integrals that is often used in analytic number theory.

Definition 17.31. Let f and g be (real or complex valued) functions defined on a nonempty real interval $[a,b]$. For any partition $P = (x_0,\dots,x_n)$ of $[a,b]$ and sequence $T = (t_1,\dots,t_k)$ with $t_k \in [x_{k-1},x_k]$, we define the *Riemann-Stieltjes sum*

$$S(P,T,f,g) := \sum_{k=1}^{n} f(t_k)(g(x_k) - g(x_{k-1}))$$

We say that f is *Riemann-Stieltjes integrable with respect to g* and write $f \in S(g)$ if there is a (real or complex) number S such that for every $\epsilon > 0$ there is a partition P_ϵ of $[a,b]$

such that for every refinement $P = (x_0, \dots, x_n)$ of P_ϵ and every sequence $T = (t_1, \dots, t_n)$ with $t_k \in [x_{k-1}, x_k]$ we have $|S(P, T, f, g) - S| < \epsilon$.[6]

When such an S exists it is necessarily unique and we denote it by $\int_a^b f\,dg$, the *Riemann-Stieltjes integral of f with respect to g*. Improper Riemann-Stieltjes integrals are then defined as limits

$$\int_a^\infty f\,dg := \lim_{b\to\infty} \int_a^b f\,dg$$

(and similarly for the lower limit), and we define $\int_b^a f\,dg = -\int_a^b f\,dg$ and $\int_a^a f\,dg = 0$.

The case $g(x) = x$ is the usual Riemann integral. The Riemann-Stieltjes integral satisfies the usual properties of linearity, summability, and integration by parts.

Proposition 17.32. *Let f, g, and h be functions on $[a, b]$ and let c_1 and c_2 be constants. The following hold:*

- *If $f, g \in S(h)$ then $\int_a^b (c_1 f + c_2 g)\,dh = c_1 \int_a^b f\,dh + c_2 \int_a^b g\,dh$.*
- *If $f \in S(g), S(h)$ then $\int_a^b f\,d(c_1 g + c_2 h) = c_i \int_a^b f\,dg + c_2 \int_a^b f\,dh$.*
- *If $f \in S(g)$ then for any $c \in [a, b]$ we have $\int_a^b f\,dg = \int_a^c f\,dg + \int_c^b f\,dg$.*
- *If $f \in S(g)$ then $g \in S(f)$ and $\int_a^b f\,dg + \int_a^b g\,df = f(b)g(b) - f(a)g(a)$.*
- *If $f = f_1 + if_2$ and $g = g_1 + ig_2$ with $f_1, f_2 \in S(g_1), S(g_2)$ then*

$$\int_a^b f\,dg = \left(\int_a^b f_1\,dg_1 - \int_a^b f_2\,dg_2\right) + i\left(\int_a^b f_2\,dg_1 + \int_a^b f_1\,dg_2\right).$$

Proof. See [1, Thm. 7.2-7,7.50]. □

The last identity allows us to reduce complex-valued integrals to real-valued integrals. The following proposition allows us to reduce Stieltjes integrals to Riemann integrals.

Proposition 17.33. *Let f and g be real-valued functions on $[a, b]$ and suppose g has a continuous derivative g' on $[a, b]$. Then*

$$\int_a^b f\,dg = \int_a^b f(x)g'(x)dx.$$

Proof. See [1, Thm. 7.8]. □

A key advantage of the Stieltjes integral $\int_a^b f\,dg$ is that neither the integrand f nor the integrator g is required to be continuous. It suffices for f and g to be of bounded variation and not share any discontinuities (and they can even share certain discontinuities, see Theorem 17.35).

Definition 17.34. Let f be a (real or complex valued) function defined on a nonempty real interval $[a, b]$. Then f is of *bounded variation* if there exists a (real or complex) number M such that

$$\sum_{i=0}^{n-1} |f(x_{i+1}) - f(x_i)| < M$$

[6] This definition (due to Pollard) is more general than that originally given by Stieltjes but is now standard.

for every partition $P = (x_0, \dots, x_n)$ of $[a,b]$. If f has a continuous derivative f' on $[a,b]$ this is equivalent to requiring $\int_a^b |f'(x)|dx < \infty$. Every piecewise monotone function is of bounded variation. In particular, any step function with finitely many discontinuities on $[a,b]$ is of bounded variation.

Theorem 17.35. *Let f and g be functions on $[a,b]$ of bounded variation such that for every $c \in [a,b]$ the function f is continuous from the left at c and the function g is continuous from the right at c. Then $\int_a^b f\,dg$ and $\int_a^b g\,df$ both exist.*

Proof. See [2, Thm. 3.7]. □

Corollary 17.36. *Let f and g be functions on $[a,b]$ such that f and g are not both discontinuous from the left or from the right at integers $n \in [a,b]$, and let $G(x) = \sum_{a<n\le x} g(n)$. Then*

$$\sum_{a<n\le b} f(n)g(n) = \int_a^b f(x)\,dG(x).$$

In particular, the integral on the RHS always exists.

Proof. See [1, Thm. 7.11]. □

As an example of using Stieltjes integrals, let us derive an asymptotic estimate for the the harmonic sum

$$H(x) := \sum_{1\le n\le x} \frac{1}{n}.$$

Theorem 17.37. *For $x \in \mathbb{R}_{\ge 1}$, as $x \to \infty$ we have*

$$H(x) = \log x + \gamma + O\left(\tfrac{1}{x}\right)$$

where $\gamma = \lim_{x\to\infty}(H(x) - \log x) = 0.577216\dots$ is Euler's constant.

Proof. Let $[t]$ denote the greatest integer function. Applying Corollary 17.36 with $g(t) = 1$ and $G(t) = \sum_{1\le n\le x} 1 = [t]$, we have

$$\begin{aligned}
H(x) = \sum_{1\le n\le x} \frac{1}{n} &= \int_{1^-}^{x} \frac{1}{t}\,d[t] \\
&= \frac{[t]}{t}\Big|_{1^-}^{x} - \int_{1^-}^{x} [t]\,d\frac{1}{t} \\
&= \frac{[x]}{x} + \int_{1^-}^{x} \frac{[t]}{t^2}\,dt \\
&= \frac{[x]}{x} + \int_{1^-}^{x} \frac{1}{t}\,dt - \int_{1^-}^{x} \frac{t-[t]}{t^2}\,dt \\
&= \frac{[x]}{x} + \log x - \int_{1^-}^{x} \frac{t-[t]}{t^2}\,dt,
\end{aligned}$$

where we used integration by parts in the second line and applied Proposition 17.33 to get the third line. Now let $\gamma = 1 - \int_{1^-}^{\infty}(t-[t])/t^2\,dt$. Then

$$\begin{aligned}
H(x) &= \frac{[x]}{x} + \log x - 1 + \gamma + \int_x^{\infty} \frac{t-[t]}{t^2}\,dt \\
&= \log x + \gamma + \left(\frac{[x]-x}{x} + \int_x^{\infty} \frac{t-[t]}{t^2}\,dt\right).
\end{aligned}$$

Both summands in the parenthesized quantity on the RHS are clearly $O(\frac{1}{x})$; thus

$$\gamma = \lim_{x\to\infty} (H(x) - \log x),$$

and the theorem follows. □

Remark 17.38. One can further refine this estimate by further analyzing the (exact) error term on the RHS of the expression for $H(x)$. For example, one finds that

$$H(x) = \log x + \gamma + \frac{1}{2x} - \frac{1}{2x^2} + \frac{1}{120x^4} + O\left(\frac{1}{x^6}\right).$$

17.6 Primes in arithmetic progressions

We now return to our goal of proving Dirichlet's theorem on primes in arithmetic progressions. Let a and m be positive integers with $a \perp m$. We want to show that the sum

$$\sum_{p\equiv a \bmod m} p^{-s}$$

is unbounded as $s \to 1^+$. To convert this to a sum over all primes we use Proposition 17.9 to construct the indicator function

$$\frac{1}{\phi(m)} \sum_{\chi} \chi(p/a) = \begin{cases} 1 & \text{if } p \equiv a \bmod m, \\ 0 & \text{otherwise} \end{cases}$$

where p/a is computed modulo m and χ ranges over primitive Dirichlet characters of conductor dividing m (which we identify with the character group of $(\mathbb{Z}/m\mathbb{Z})^\times$ via Corollary 17.25).

As $s \to 1^+$ we then have

$$\begin{aligned}
\sum_{p\equiv a \bmod m} p^{-s} &= \sum_p p^{-s} \frac{1}{\phi(m)} \sum_\chi \chi(p/a) \\
&= \sum_\chi \frac{\chi(1/a)}{\phi(m)} \sum_p \chi(p) p^{-s} \\
&= \sum_\chi \frac{\chi(1/a)}{\phi(m)} \big(\log L(s,\chi) + O(1)\big) \\
&= \frac{\log \zeta(s)}{\phi(m)} + \sum_{\chi\neq\mathbb{1}} \frac{\chi(1/a)}{\phi(m)} \log L(s,\chi) + O(1).
\end{aligned}$$

We now make the key claim that so long as χ is not principal, we have

$$L(1,\chi) \neq 0.$$

This implies that $\log L(1,\chi) = O(1)$ as $s \to 1^+$ and therefore

$$\sum_{p\equiv a \bmod m} p^{-s} = \frac{\log \zeta(s)}{\phi(m)} + O(1)$$

is unbounded as $s \to 1^+$, since $\zeta(s)$ is. Moreover, applying Mertens' second theorem to the estimate (1) for $\log \zeta(s)$ that we derived earlier, we obtain

$$\sum_{\substack{p \le x \\ p \equiv a \bmod m}} \frac{1}{p} \sim \frac{1}{\phi(m)} \log\log x$$

In order to prove the key claim that $L(1,\chi) \neq 0$ when χ is non-principal, we will prove next time that the Dedekind zeta function $\zeta_K(s)$ of the mth cyclotomic field $K = \mathbb{Q}(\zeta_m)$ can be written as

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

where the product ranges over the primitive Dirichlet characters of conductor dividing m. Exactly one of these is principal, namely, $L(s,\mathbb{1}) = \zeta(s)$, and it has a simple pole at $s = 1$. The analytic class formula we will prove in the next lecture implies that $\zeta_K(s)$ extends to a meromorphic function on $\mathrm{Re}(s) > 1 - \frac{1}{\phi(m)}$ with a simple pole at $s = 1$; this implies that $L(1,\chi) \neq 0$ for all non-principal Dirichlet characters.

References

[1] Tom Apostol, *Mathematical analysis*, 2nd edition, Addison-Wesley, 1974.

[2] Paul Bateman and Harold Diamond, *Analytic number theory: An introductory course*, World Scientific, 2004.

[3] J.W.S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, 1967.

[4] Franz Mertenz, *Ein Beitrag zur analytischen Zahlentheorie*, J. reine agnew. Math., **78** (1874), 46–62.