Introduction to Analytic Number Theory

Math 531 Lecture Notes, Fall 2005

A.J. Hildebrand
Department of Mathematics
University of Illinois

http://www.math.uiuc.edu/~hildebr/ant

Version 2013.01.07

Chapter 6

Primes in arithmetic progressions: Dirichlet's Theorem

6.1 Introduction

The main goal of this chapter is a proof of Dirichlet's theorem on the existence of primes in arithmetic progressions, a result that predates the prime number theorem by about 50 years, and which has had an equally profound impact on the development of analytic number theory. In its original version this result is the following.

Theorem 6.1 (Dirichlet's Theorem)**.** *Given any positive integers q and a with $(a,q)=1$, there exist infinitely many primes congruent to a modulo q. In other words, each of the arithmetic progressions*

$$\{qn+a: \quad n=0,1,2,\dots\}, \quad q,a\in\mathbb{N},\ (a,q)=1, \tag{6.1}$$

contains infinitely many primes.

The above form of Dirichlet's theorem is the analog of Euclid's theorem on the infinitude of primes. Our proof will in fact give a stronger result, namely an analog of Mertens' estimate for primes in arithmetic progressions.

Theorem 6.2 (Dirichlet's Theorem, quantitative version)**.** *Given any positive integers q and a with $(a,q)=1$, we have*

$$\sum_{\substack{p\le x\\ p\equiv a \bmod q}} \frac{1}{p} = \frac{1}{\phi(q)}\log\log x + O_q(1) \quad (x\ge 3). \tag{6.2}$$

This is still short of an analog of the PNT for primes in arithmetic progressions, which would be an asymptotic formula for the counting functions $\pi(x; q, a) = \#\{p \leq x : p \equiv a \bmod q\}$. Such estimates are indeed known, but the proofs are rather technical, so we will not present them here. (Essentially, one has to combine Dirichlet's method for the proof of Theorem 6.1 with the analytic argument we used in the previous chapter to prove the PNT with error term.)

We note that the condition $(a, q) = 1$ in Dirichlet's theorem is necessary, for if $(a, q) = d > 1$, then any integer congruent to a modulo q is divisible by d, and hence there can be at most one prime in the residue class a modulo q. Thus, for given q, all but finitely many exceptional primes fall into one of the residue classes a mod q, with $(a, q) = 1$. By the definition of the Euler phi function, there are $\phi(q)$ such residue classes, and if we assume that the primes are distributed approximately equally among these residue classes, then a given class a modulo q, with $(a, q) = 1$, can be expected to contain a proportion $1/\phi(q)$ of all primes. Thus, the factor $1/\phi(q)$ in (6.2) is indeed the "correct" factor here.

A natural attempt to prove Dirichlet's theorem would be to try to mimick Euclid's proof of the infinitude of primes. In certain special cases, this does indeed succeed. For example, to show that there are infinitely many primes congruent to 3 modulo 4, assume there are only finitely many, say $p_1, \ldots, p_n$, and consider the number $N = p_1^2 \ldots p_n^2 + 2$. Since $p_i^2 \equiv 3^2 \equiv 1 \bmod 4$ for each i, N must be congruent to 3 modulo 4. Now note that, since N is odd, all its prime factors are odd, and so congruent to either 1 or 3 modulo 4. Moreover, N must be divisible by at least one prime congruent to 3 modulo 4, and hence by one of the primes p_i, since otherwise N would be a product of primes congruent to 1 modulo 4 and thus itself congruent to 1 modulo 4. But this is impossible, since then p_i would divide both N and $N - 2$, and hence also $N - (N - 2) = 2$.

Similar, though more complicated, elementary arguments can be given for some other special arithmetic progressions, but the general case of Dirichlet's theorem cannot be proved by these methods.

As was the case with the PNT, the breakthrough that led to a proof of Dirichlet's theorem in its full generality came with the introduction of analytic tools. The key tools that Dirichlet introduced and which are now named after him, are the *Dirichlet characters* and *Dirichlet L-functions*. Dirichlet characters are certain arithmetic functions that are used to extract terms belonging to a given arithmetic progression from a summation. Dirichlet L-functions are the Dirichlet series associated with these functions. The analytic properties of these Dirichlet series, and in particular the loca-

tion of their zeros, play a key role in the argument. In fact, the most difficult part of the proof consists in showing that the single point $s = 1$ is not a zero for a Dirichlet L-function.

6.2 Dirichlet characters

The basic definition of a character is as follows.

Definition (Dirichlet characters)**.** Let q be a positive integer. A **Dirichlet character modulo** q is an arithmetic function χ with the following properties:

(i) χ is periodic modulo q, i.e., $\chi(n+q) = \chi(n)$ for all $n \in \mathbb{N}$.

(ii) χ is completely multiplicative, i.e., $\chi(nm) = \chi(n)\chi(m)$ for all $n, m \in \mathbb{N}$ and $\chi(1) = 1$.

(iii) $\chi(n) \neq 0$ if and only if $(n, q) = 1$.

The arithmetic function $\chi_0 = \chi_{0,q}$ defined by $\chi_0(n) = 1$ if $(n, q) = 1$ and $\chi_0(n) = 0$ otherwise (i.e., the characteristic function of the integers coprime with q) is called the **principal character modulo** q.

Remarks. (i) That the principal character χ_0 is, in fact, a Dirichlet character can be seen as follows: condition (i) follows from the relation $(n, q) = (n + q, q)$, (ii) follows from the fact that $(nm, q) = 1$ holds if and only if $(n, q) = 1$ and $(m, q) = 1$, and (iii) holds by the definition of χ_0.

(ii) The notation χ_0 has become the standard notation for the principal character. In using this notation, one must keep in mind that χ_0 depends on q, even though this is not explicitly indicated in the notation.

(iii) In analogy with the residue class notation "$a \bmod q$", the notation "$\chi \bmod q$" is used to indicate that χ is a Dirichlet character modulo q. In a summation condition this notation denotes a sum over all characters χ modulo q.

Examples

(1) **Characters modulo** 1**.** The constant function 1 clearly satisfies the conditions of the above definition with $q = 1$. Moreover, since any character modulo 1 must be periodic modulo 1 and equal to 1 at 1, $\chi \equiv 1$ is the only Dirichlet character modulo 1. Note that this character is the principal character modulo 1.

(2) **Characters modulo 2.** The coprimality condition forces any character modulo 2 to be 0 at even integers, and the periodicity condition along with the requirement $\chi(1) = 1$ then forces $\chi(n)$ to be equal to 1 at odd integers. Thus, as in the case $q = 1$, there is only one character modulo 2, namely the principal character χ_0 defined by $\chi_0(n) = 1$ if $(n, 2) = 1$ and $\chi_0(n) = 0$ otherwise.

(3) **Characters modulo 3.** We have again the principal character $\chi_0(n)$, defined by $\chi_0(n) = 1$ if $(n, 3) = 1$ and $\chi_0(n) = 0$ otherwise. We will show that there is exactly one other character modulo 3.

Suppose χ is a character modulo 3. Then properties (i)–(iii) force $\chi(1) = 1$, $\chi(3) = 0$, and $\chi(2)^2 = \chi(4) = \chi(1) = 1$, so that $\chi(2) = \pm 1$. If $\chi(2) = 1$, then χ is equal to χ_0 since both functions are periodic modulo 3 and have the same values at $n = 1, 2, 3$. If $\chi(2) = -1$, then $\chi = \chi_1$, where χ_1 is the unique periodic function modulo 3 defined by $\chi_1(1) = 1$, $\chi_1(2) = -1$, and $\chi_1(3) = 0$. Clearly χ_1 satisfies properties (i) and (iii). The complete multiplicativity is not immediately obvious, but can be seen as follows:

Define a completely multiplicative function f by $f(3) = 0$, $f(p) = -1$ if $p \equiv -1 \bmod 3$ and $f(p) = 1$ if $p \equiv 1 \bmod 3$. Then $f(n) = \chi_1(n)$ for $n = 1, 2, 3$, so to show that $f = \chi_1$ (and hence that χ_1 is completely multiplicative) it suffices to show that f is periodic with period 3.

To this end, note first that if $n \equiv 0 \bmod 3$, then $f(n) = 0$. Otherwise $n \equiv \pm 1 \bmod 3$, and in this case n can be written as $n = \prod_{i \in I} p_i \prod_{j \in J} p_j$, where the products over $i \in I$ and $j \in J$ are finite (possibly empty), and the primes p_i, $i \in I$, and p_j, $j \in J$, are congruent to 1, resp. -1, modulo 3. We then have $f(n) = \prod_{i \in I} f(p_i) \prod_{j \in J} f(p_j) = (-1)^{|J|}$. On the other hand, since $p_i \equiv 1 \bmod 3$ and $p_j \equiv -1 \bmod 3$, we have $n \equiv (-1)^{|J|} \bmod 3$. Hence, if $|J|$ is even, then $n \equiv 1 \bmod 3$, and $f(n) = 1 = f(1)$, and if $|J|$ is odd, then $n \equiv 2 \bmod 3$, and $f(n) = -1 = f(2)$. Thus, f is periodic with period 3, as we wanted to show.

(4) **Legendre symbols as characters.** Let q be an odd prime, and let $\chi(n) = \left(\frac{n}{q}\right)$ denote the Legendre symbol modulo q, defined as 0 if $(n, q) > 1$, 1 if $(n, q) = 1$ and $n \equiv x^2 \bmod q$ has a solution (i.e., if n is a quadratic residue modulo q), and -1 otherwise (i.e., if n is a quadratic non-residue modulo q). Then $\chi(n)$ is a character modulo q. Indeed, properties (i) (periodicity) and (iii) (coprimality) follow immediately

from the definition of the Legendre symbol, while (ii) (complete multiplicativity) amounts to the identity $\left(\frac{nm}{q}\right) = \left(\frac{n}{q}\right)\left(\frac{m}{q}\right)$, which is a known result from elementary number theory.

A character χ derived from a Legendre symbol in this way takes on only the values $0, \pm 1$, and thus satisfies $\chi^2 = \chi_0$, but $\chi \neq \chi_0$. Characters with the latter two properties are called **quadratic characters**. Note that a character taking on only real values (such a character is called **real character**) necessarily has all its values in $\{0, \pm 1\}$, and so is either a principal character or a quadratic character.

We will later describe a systematic method for constructing all Dirichlet characters to a given modulus q.

We next deduce some simple consequences from the definition of a character.

Theorem 6.3 (Elementary properties of Dirichlet characters)**.** *Let q be a positive integer.*

(i) The values of a Dirichlet character χ modulo q are either 0, or $\phi(q)$-th roots of unity; i.e., for all n, we have either $\chi(n) = 0$ or $\chi(n) = e^{2\pi i\nu/\phi(q)}$ for some $\nu \in \mathbb{N}$.

(ii) The characters modulo q form a group with respect to pointwise multiplication, defined by $(\chi_1\chi_2)(n) = \chi_1(n)\chi_2(n)$. The principal character χ_0 is the neutral element of this group, and the inverse of a character χ is given by the character $\overline{\chi}$ defined by $\overline{\chi}(n) = \overline{\chi(n)}$.

Proof. (i) If $\chi(n) \neq 0$, then $(n, q) = 1$. By Euler's generalization of Fermat's Little Theorem we then have $n^{\phi(q)} \equiv 1 \bmod q$. By the complete multiplicativity and periodicity of χ this implies $\chi(n)^{\phi(q)} = \chi\left(n^{\phi(q)}\right) = \chi(1) = 1$, as claimed.

(ii) The group properties follow immediately from the definition of a character. □

In order to derive further information on the properties of the group of characters, we need a well-known result from algebra, which we state here without proof.

Lemma 6.4 (Basis theorem for finite abelian groups)**.** *Every finite abelian group is a direct product of cyclic groups. That is, for every finite abelian group G there exist elements $g_1, \ldots, g_r \in G$ of respective orders $h_1, \ldots, h_r$, such that every element $g \in G$ has a unique representation $g = \prod_{i=1}^{r} g_i^{\nu_i}$ with $0 \leq \nu_i < h_i$. Moreover, we have $\prod_{i=1}^{r} h_i = |G|$.*

We note that in case the group is trivial, i.e., consists of only the identity element, the result remains valid with an empty set as "basis" if the product representation $g = \prod_i g_i^{\nu_i}$ is interpreted as the empty product whose value is the identity element.

If we specialize the group G in Lemma 6.4 as the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^*$ of reduced residue classes modulo q, this result becomes:

Lemma 6.5 (Basis theorem for reduced residue classes modulo q)**.** *Let q be a positive integer. Then there are positive integers $g_1, \ldots, g_r$, all relatively prime to q and of respective orders $h_1, \ldots, h_r$ modulo q (i.e., h_i is the least positive integer h such that $g_i^h \equiv 1 \bmod q$), with the following property: For every integer n with $(n, q) = 1$ there exist unique integers ν_i with $0 \le \nu_i < h_i$, such that $n \equiv \prod_{i=1}^r g_i^{\nu_i} \bmod q$. Moreover, we have $\prod_{i=1}^r h_i = \phi(q)$.*

Examples

(1) If $q = p^m$ is a prime power, with p an *odd* prime, then, by a result from elementary number theory, there exists a *primitive root* g modulo p^m, i.e., an element g that generates the multiplicative group modulo p^m. Thus, this group is itself cyclic, and the basis theorem therefore holds with $r = 1$ and $g_1 = g$. (For powers of 2 the situation is slightly more complicated, as the corresponding residue class groups are in general not cyclic.)

(2) Let $q = 15 = 3 \cdot 5$. We claim that $(g_1, g_2) = (2, 11)$ is a basis. It is easily checked that the orders of g_1 and g_2 are $h_1 = 4$ and $h_2 = 2$, respectively. Note also that $h_1 h_2 = 4 \cdot 2 = \phi(5)\phi(3) = \phi(15)$, in agreement with the theorem. A simple case-by-case check then shows that the congruence classes $2^{\nu_1} 11^{\nu_2}$ with $0 \le \nu_1 < 4$ and $0 \le \nu_2 < 2$ cover every residue class $a \bmod q$ with $(a, 15) = 1$ exactly once.

Our main application of the basis theorem is given in the following lemma.

Lemma 6.6 (Number of characters modulo q)**.** *Let q be a positive integer. Then exist exactly $\phi(q)$ Dirichlet characters modulo q. Moreover, for any integer a with $(a, q) = 1$ and $a \not\equiv 1 \bmod q$ there exists a character χ with $\chi(a) \neq 1$.*

Proof. Let $g_1, \dots, g_r$ and $h_1, \dots, h_r$ be as in Lemma 6.5, and set $\omega_j = e^{2\pi i/h_j}$. Thus ω_j^ν, $\nu = 0, 1, \dots, h_j$, are distinct h_j-th roots of unity. We claim that there is a one-to-one correspondence between the tuples

$$\nu = (\nu_1, \dots, \nu_r), \quad 0 \le \nu_i < h_i, \tag{6.3}$$

and the characters modulo q.

To show this, suppose first that χ is a character modulo q. Then $\chi(n) = 0$ for $(n, q) > 1$, by the definition of a character. On the other hand, if $(n, q) = 1$, then, by the basis theorem, we have $n \equiv \prod_{i=1}^r g_i^{\mu_i} \bmod q$ with a unique tuple $\mu = (\mu_1, \dots, \mu_r)$ with $0 \le \mu_i < h_i$. The periodicity and complete multiplicativity properties of a character then imply

$$\chi(n) = \chi\left(\prod_{i=1}^r g_i^{\mu_i}\right) = \prod_{i=1}^r \chi(g_i)^{\mu_i}, \text{ if } n \equiv \prod_{i=1}^r g_i^{\mu_i} \bmod q. \tag{6.4}$$

Thus, χ is uniquely specified by its values on the generators g_i. Moreover, since g_i has order h_i, we have

$$\chi(g_i)^{h_i} = \chi(g_i^{h_i}) = \chi(1) = 1,$$

so $\chi(g_i)$ must be an h_i-th root of unity; i.e., setting $\omega_j = \exp(2\pi i/h_j)$, we have

$$\chi(g_i) = \omega_i^{\nu_i} \quad (i = 1, \dots, r), \tag{6.5}$$

for a unique tuple $\nu = (\nu_1, \dots, \nu_r)$ of the form (6.3). Thus, every character χ modulo q gives rise to a unique tuple ν of the above form.

Conversely, given a tuple ν of this form, we define an arithmetic function $\chi = \chi_\nu$ by setting $\chi(n) = 0$ if $(n, q) > 1$ and defining $\chi(n)$ via (6.4) and (6.5) otherwise. By construction, this function $\chi(n)$ is periodic modulo q and satisfies $\chi(n) \ne 0$ if and only if $(n, q) = 1$, and one can verify that χ is also completely multiplicative. Thus χ is indeed a Dirichlet character modulo q.

We have thus shown that the characters modulo q are in one-to-one correspondence with tuples ν of the form (6.3). Since by Lemma 6.5 there are $h_1 \dots h_r = \phi(q)$ such tuples, it follows that there are $\phi(q)$ characters modulo q. This establishes the first part of the Lemma 6.6.

For the proof of the second part, let an integer a be given with $(a, q) = 1$ and $a \not\equiv 1 \bmod q$. By the basis theorem, we have $a \equiv \prod_{i=1}^r g_i^{\mu_i} \bmod q$ with suitable exponents μ_i of the form (6.3). Since $a \not\equiv 1 \bmod q$, at least one

of the exponents μ_i must be non-zero. Without loss of generality, suppose that $\mu_1 \neq 0$. Define a character χ by setting $\chi(g_1) = \omega_1$ and $\chi(g_i) = 1$ for $i = 2, \ldots, r$. Then

$$\chi(a) = \chi(g_i^{\mu_1}) = \chi(g_i)^{\mu_1} = \exp\left\{\frac{2\pi i \mu_1}{h_1}\right\} \neq 1,$$

since $0 < \mu_1 < h_1$. □

Example: Characters modulo 15

We illustrate the construction of characters in the case of the modulus $q = 15$ considered in the example following Lemma 6.5. There we had obtained $g_1 = 2$ and $g_2 = 11$ as generators with respective orders $h_1 = 4$ and $h_2 = 2$. The corresponding roots of unity ω_i in (6.5) are $\omega_1 = e^{2\pi i/4} = i$ and $\omega_2 = e^{2\pi i/2} = -1$. Thus there are 8 characters χ_{ν_1,ν_2} modulo 15, corresponding to the pairs (ν_1, ν_2) with $0 \leq \nu_1 < 4$ and $0 \leq \nu_2 < 2$, and defined by setting $\chi_{\nu_1,\nu_2}(2) = i^{\nu_1}$ and $\chi_{\nu_1,\nu_2}(11) = (-1)^{\nu_2}$. The corresponding values of $\chi_{\nu_1,\nu_2}(a)$ at all integers $1 \leq a \leq q$ with $(a, 15) = 1$ can be calculated by representing a in the form $a \equiv 2^{\mu_1}11^{\mu_2} \bmod 15$ with $0 \leq \mu_1 < 4$, $0 \leq \mu_2 < 2$, and then using the formula $\chi(a) = \chi(2^{\mu_1}11^{\mu_2}) = \chi(2)^{\mu_1}\chi(11)^{\mu_2}$. The result is given in Table 6.1:

(μ_1, μ_2)	$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$
a	1	2	4	8	11	7	14	13
$\chi_{0,0}(a)$	1	1	1	1	1	1	1	1
$\chi_{0,1}(a)$	1	1	1	1	-1	-1	-1	-1
$\chi_{1,0}(a)$	1	i	-1	$-i$	1	i	-1	$-i$
$\chi_{1,1}(a)$	1	i	-1	$-i$	-1	$-i$	1	i
$\chi_{2,0}(a)$	1	-1	1	-1	1	-1	1	-1
$\chi_{2,1}(a)$	1	-1	1	-1	-1	1	-1	1
$\chi_{3,0}(a)$	1	$-i$	-1	i	1	$-i$	-1	i
$\chi_{3,1}(a)$	1	$-i$	-1	i	-1	i	1	$-i$

Table 6.1: Table of all Dirichlet characters modulo 15. The integers a in the second row are the values of $2^{\mu_1}11^{\mu_2}$ modulo 15.

The main result of this section is the following.

Theorem 6.7 (Orthogonality relations for Dirichlet characters)**.** *Let q be a positive integer.*

(i) For any Dirichlet character χ modulo q we have

$$\sum_{a=1}^{q} \chi(a) = \begin{cases} \phi(q) & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise,} \end{cases}$$

where χ_0 is the principal character modulo q.

(ii) For any integer $a \in \mathbb{N}$ we have

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

where the summation runs over all Dirichlet characters modulo q.

(iii) For any Dirichlet characters χ_1, χ_2 modulo q we have

$$\sum_{a=1}^{q} \chi_1(a)\overline{\chi_2(a)} = \begin{cases} \phi(q) & \text{if } \chi_1 = \chi_2, \\ 0 & \text{otherwise.} \end{cases}$$

(iv) For any integers $a_1, a_2 \in \mathbb{N}$ we have

$$\sum_{\chi \bmod q} \chi(a_1)\overline{\chi(a_2)} = \begin{cases} \phi(q) & \text{if } a_1 \equiv a_2 \bmod q \text{ and } (a_1, q) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

where the summation runs over all Dirichlet characters modulo q.

Proof. (i) Let S denote the sum on the left. If $\chi = \chi_0$, then $\chi(a) = 1$ if $(a, q) = 1$, and $\chi(a) = 0$ otherwise, so $S = \phi(q)$.

Suppose now that $\chi \neq \chi_0$. Then there exists a number a_1 with $(a_1, q) = 1$ such that $\chi(a_1) \neq 1$. Note that, since $\chi(a) = 0$ if $(a, q) > 1$, the sum in (i) may be restricted to terms with $(a, q) = 1$, $1 \leq a \leq q$. Also, observe that, if a runs through these values, then so does $b = aa_1$, after reducing modulo q. Therefore,

$$\chi(a_1)S = \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} \chi(a_1)\chi(a) = \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} \chi(a_1 a) = \sum_{\substack{1 \leq b \leq q \\ (b,q)=1}} \chi(b) = S.$$

Since $\chi(a_1) \neq 1$, this implies $S = 0$. This completes the proof of part (i).

(ii) Let S denote the sum on the left. If $(a, q) > 1$, then all terms in this sum are 0, so $S = 0$. If $(a, q) = 1$ and $a \equiv 1 \bmod q$, then $\chi(a) = \chi(1) = 1$ for all characters χ modulo q, and since by Lemma 6.6 there exist exactly $\phi(q)$ such characters, we have $S = \phi(q)$ in this case.

Now suppose that $(a, q) = 1$ and $a \not\equiv 1 \bmod q$. By Lemma 6.6, there exists a character χ_1 modulo q with $\chi_1(a) \neq 1$. Since the characters modulo q form a group, if χ runs through all characters modulo q, then so does $\chi_1\chi$. We therefore have

$$\chi_1(a)S = \sum_{\chi \bmod q} \chi_1(a)\chi(a) = \sum_{\chi \bmod q} (\chi_1\chi)(a) = \sum_{\psi \bmod q} \psi(a) = S,$$

where in the last sum ψ runs through all characters modulo q. Since $\chi_1(a) \neq 1$, this implies $S = 0$, as desired.

(iii) This follows by applying (i) with the character $\chi = \chi_1\overline{\chi_2}$ and noting that $\chi = \chi_0$ if and only if $\chi_1 = \chi_2$.

(iv) We may assume that $(a_1, q) = (a_2, q) = 1$ since otherwise the sum is 0 and the result holds trivially. Therefore, a_2 has a multiplicative inverse $\overline{a_2}$ modulo q. We now apply (ii) with $a = a_1\overline{a_2}$. Noting that

$$\chi(a_2)\chi(a) = \chi(a_2a) = \chi(a_2a_1\overline{a_2}) = \chi(a_1)$$

and hence

$$\chi(a) = \frac{\chi(a_1)}{\chi(a_2)} = \chi(a_1)\overline{\chi(a_2)},$$

and that $a = a_1\overline{a_2} \equiv 1 \bmod q$ if and only $a_1 \equiv a_2 \bmod q$, we obtain the desired relation. □

The last part, (iv), is by far the most important, and it is key to Dirichlet's argument. This identity allows one to extract terms satisfying a given congruence from a sum. We will apply it with a_2 a fixed congruence class $a \bmod q$ and with a_1 running through primes p, in order to extract those primes that fall into the congruence class $a \bmod q$. This identity alone is often referred to as the orthogonality relation for Dirichlet characters.

We record one simple, but useful consequence of part (i) of the above theorem.

Corollary 6.8 (Summatory function of characters)**.** *Let q be a positive integer and χ a character modulo q.*

(i) If χ is not the principal character χ_0 modulo q, then

$$\left|\sum_{n\le x}\chi(n)\right| \le \phi(q) \quad (x \ge 1).$$

(ii) If $\chi = \chi_0$, then

$$\left|\sum_{n\le x}\chi(n) - \frac{\phi(q)}{q}x\right| \le 2\phi(q) \quad (x \ge 1).$$

Proof. Since χ is periodic modulo q, we have, for any $x \ge 1$,

$$\sum_{n\le x}\chi(n) = [x/q]S + R,$$

where

$$S = \sum_{a=1}^{q}\chi(a), \quad |R| \le \sum_{a=1}^{q}|\chi(n)|.$$

Clearly, $|R| \le \phi(q)$, and by part (i) of Theorem 6.7 we have $S = 0$ if $\chi \ne \chi_0$, and $S = \phi(q)$ if $\chi = \chi_0$. The asserted bounds follow from these remarks. □

6.3 Dirichlet L-functions

Given a Dirichlet character χ, its Dirichlet series, i.e., the function

$$L(s,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}, \tag{6.6}$$

is called the *Dirichlet L-function*, or *Dirichlet L-series*, associated with the character χ.

The analytic behavior of Dirichlet L-functions plays a crucial role in the proof of Dirichlet's theorem. The following theorem collects the main analytic properties of L-functions that we will need for the proof of Dirichlet's theorem. The key property, upon which the success of the argument hinges, is the last one, which asserts that L-functions do not have a zero at the point $s = 1$. This is also the most difficult property to establish, and we therefore defer its proof to a later section.

Theorem 6.9 (Analytic properties of L-functions)**.** *Let χ be a Dirichlet character modulo q, and let $L(s,\chi)$ denote the associated Dirichlet L-function, defined by* (6.6)*.*

(i) If $\chi \neq \chi_0$, where χ_0 is the principal character modulo q, then $L(s,\chi)$ is analytic in the half-plane $\sigma > 0$.

(ii) If $\chi = \chi_0$, then $L(s,\chi)$ has a simple pole at $s = 1$ with residue $\phi(q)/q$, and is analytic at all other points in the half-plane $\sigma > 0$.

(iii) If $\chi \neq \chi_0$, then $L(1,\chi) \neq 0$.

Proof. As mentioned above, we defer the proof of (iii) to a later section, and only prove (i) and (ii) in this section.

By Corollary 6.8 the summatory function $M(\chi,x) = \sum_{n\le x}\chi(n)$ satisfies, for $x \ge 1$,

$$M(\chi,x) = \begin{cases} O_q(1) & \text{if } \chi \neq \chi_0, \\ \dfrac{\phi(q)}{q}x + O_q(1) & \text{if } \chi = \chi_0, \end{cases} \tag{6.7}$$

where the O-constant depends only on q. Parts (i) and (ii) then follow as special cases of Theorem 4.13.

Alternatively, one can obtain (i) and (ii) as follows:

If $\chi \neq \chi_0$, then using partial summation and the fact that the partial sums $\sum_{n\le x}\chi(n)$ are bounded in this case, one can easily see that the Dirichlet series (6.6) converges in the half-plane $\sigma > 0$. Since a Dirichlet series represents an analytic function in its half-plane of convergence, this shows that $L(s,\chi)$ is analytic in $\sigma > 0$ when $\chi \neq \chi_0$.

In the case $\chi = \chi_0$ one can argue similarly with the arithmetic function $f(n) = \chi_0(n) - \phi(q)/q$. By (6.7), the partial sums $\sum_{n\le x} f(n)$ are bounded, so the Dirichlet series $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ converges in the half-plane $\sigma > 0$ and is therefore analytic in this half-plane. On the other hand, writing $\chi_0(n) = f(n) + \phi(q)/q$, we see that $L(s,\chi_0) = F(s) + (\phi(q)/q)\zeta(s)$ for $\sigma > 1$. Since $F(s)$ is analytic in $\sigma > 0$ and $\zeta(s)$ is analytic in $\sigma > 0$ with the exception of a pole at $s = 1$ with residue 1, we conclude that $L(s,\chi_0)$ is analytic in $\sigma > 0$ with the exception of a pole at $s = 1$ with residue $\phi(q)/q$. □

6.4 Proof of Dirichlet's Theorem

In this section we prove Dirichlet's theorem in the quantitative version given in Theorem 6.2, modulo the nonvanishing result for $L(1,\chi)$ stated in part

(iii) of Theorem 6.9. The latter result which will be established in the next section.

We fix positive integers a and q with $(a,q) = 1$, and we define the functions

$$S_{a,q}(x) = \sum_{\substack{p \le x \\ p \equiv a \bmod q}} \frac{1}{p} \quad (x \ge 2),$$

$$F_{a,q}(s) = \sum_{\substack{p \\ p \equiv a \bmod q}} \frac{1}{p^s} \quad (\sigma > 1),$$

$$F_\chi(s) = \sum_p \frac{\chi(p)}{p^s} \quad (\sigma > 1).$$

Note that the Dirichlet series $F_{a,q}(s)$ and $F_\chi(s)$ are absolutely convergent in $\sigma > 1$. We will use these series only in this half-plane.

In the above notation, the estimate of Theorem 6.2 takes the form

$$S_{a,q}(x) = \frac{1}{\phi(q)} \log\log x + O_q(1) \quad (x \ge 3). \tag{6.8}$$

We will establish this estimate by a sequence of steps that reduce the estimation of $S_{a,q}(x)$ in turn to that of the functions $F_{a,q}(s)$, $F_\chi(s)$, $L(s,\chi)$, and ultimately to the non-vanishing of $L(1,\chi)$ for $\chi \ne \chi_0$.

To ease the notation, we will not explicitly indicate the dependence of error terms on q. *Through the remainder of the proof, all O-constants are allowed to depend on q.*

Reduction to $F_{a,q}(s)$. We first show that (6.8) follows from

$$F_{a,q}(\sigma) = \frac{1}{\phi(q)} \log \frac{1}{\sigma - 1} + O(1) \quad (\sigma > 1). \tag{6.9}$$

To see this, let $x \ge 3$ and take $\sigma = \sigma_x = 1 + 1/\log x$ in (6.9). Then the main term on the right of (6.9) is equal to the main term on the right of (6.8), and the error term in (6.9) is of the desired order $O(1)$. Thus, it suffices to show that the left-hand sides of these relations, i.e., $S_{a,q}(x)$ and $F_{a,q}(\sigma_x)$, differ by at most $O(1)$.

To show this, we write

$$S_{a,q}(x) - F_{a,q}(\sigma_x) = \sum_{\substack{p \le x \\ p \equiv a \bmod q}} \frac{1 - p^{1-\sigma_x}}{p} - \sum_{\substack{p > x \\ p \equiv a \bmod q}} \frac{1}{p^{\sigma_x}} = \sum\nolimits_1 - \sum\nolimits_2, \tag{6.10}$$

say. Since

$$1 - p^{1-\sigma_x} = 1 - \exp\left\{-\frac{\log p}{\log x}\right\} \ll \frac{\log p}{\log x} \quad (p \le x),$$

we have

$$\sum\nolimits_1 \ll \frac{1}{\log x} \sum_{p \le x} \frac{\log p}{p} \ll 1,$$

by Mertens' estimate. Moreover, by partial summation and Chebyshev's estimate,

$$\begin{aligned} \sum\nolimits_2 &\le \sum_{p > x} \frac{1}{p^{\sigma_x}} = -\frac{\pi(x)}{x^{\sigma_x}} + \sigma_x \int_x^\infty \frac{\pi(u)}{u^{\sigma_x + 1}} du \\ &\ll \frac{1}{\log x} + \int_x^\infty \frac{1}{u^{\sigma_x} \log u} du \\ &\le \frac{1}{\log x} + \frac{x^{1-\sigma_x}}{(\sigma_x - 1)(\log x)} \ll 1. \end{aligned}$$

Thus, both terms on the right-hand side of (6.10) are of order $O(1)$, which is what we wanted to show.

Reduction to $F_\chi(s)$. Next, let $\sigma > 1$, so that the series $F_{a,q}(\sigma)$ and $F_\chi(\sigma)$ are absolutely convergent. By the orthogonality relation for characters (part (iv) of Theorem 6.7) we have

$$\begin{aligned} F_{a,q}(\sigma) &= \sum_p \frac{1}{p^\sigma} \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \chi(p) \\ &= \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \sum_p \frac{\chi(p)}{p^\sigma} = \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} F_\chi(\sigma). \end{aligned} \tag{6.11}$$

Reduction to Dirichlet L-functions. Since a Dirichlet character is completely multiplicative and of absolute value at most 1, the associated L-function $L(s,\chi)$ has an Euler product representation in the half-plane $\sigma > 1$, given by

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

Taking logarithms on both sides (using the principal branch of the logarithm) we get, for $\sigma > 1$,

$$\begin{aligned}\log L(s,\chi) &= -\sum_p \log\left(1 - \frac{\chi(p)}{p^s}\right) \\ &= \sum_p \sum_{m=1}^{\infty} \frac{\chi(p)^m}{mp^{ms}} = F_\chi(s) + R_\chi(s),\end{aligned}$$

where $F_\chi(s) = \sum_p \chi(p)p^{-s}$ is the function defined above and

$$|R_\chi(s)| \le \sum_p \sum_{m=2}^{\infty} \frac{1}{mp^{m\sigma}} \le \sum_p \sum_{m=2}^{\infty} \frac{1}{mp^m} \ll \sum_p \frac{1}{p^2} < \infty.$$

Thus, we have

$$F_\chi(s) = \log L(s,\chi) + O(1) \quad (\sigma > 1). \tag{6.12}$$

Contribution of the principal character. If $\chi = \chi_0$, then, by part (ii) of Theorem 6.9, $L(s,\chi_0)$ has a pole with residue $\phi(q)/q$ at $s = 1$ and is analytic elsewhere in the half-plane $\sigma > 0$. Thus, in $\sigma > 0$ we have

$$L(s,\chi_0) = \frac{\phi(q)}{q}\frac{1}{\sigma - 1} + H(s),$$

where $H(s) = H_{\chi_0}(s)$ is analytic in $\sigma > 0$. In particular, $H(s)$ is bounded in any compact set contained in this half-plane, and hence satisfies

$$|H(\sigma)| \le \frac{\phi(q)}{2q(\sigma - 1)} \quad (1 < \sigma \le \sigma_0) \tag{6.13}$$

with a suitable constant $\sigma_0 > 1$ (depending on q). Thus

$$\begin{aligned}\log L(\sigma,\chi_0) &= \log\left(\frac{\phi(q)/q}{\sigma - 1}\left(1 + H(\sigma)(\sigma - 1)\frac{q}{\phi(q)}\right)\right) \\ &= \log(\phi(q)/q) + \log\frac{1}{\sigma - 1} + \log\left(1 + H(\sigma)(\sigma - 1)\frac{q}{\phi(q)}\right) \\ &= \log\frac{1}{\sigma - 1} + O(1) \quad (1 < \sigma \le \sigma_0),\end{aligned}$$

where in the last step we used (6.13). By (6.12) it follows that

$$F_{\chi_0}(\sigma) = \log \frac{1}{\sigma - 1} + O(1), \tag{6.14}$$

initially only in the range $1 < \sigma \leq \sigma_0$, but in view of the trivial bound

$$|F_{\chi_0}(\sigma)| \leq \sum_p \frac{1}{p^\sigma} \leq \sum_p \frac{1}{p^{\sigma_0}} < \infty \quad (\sigma > \sigma_0),$$

in the full range $\sigma > 1$.

Contribution of the non-principal characters. If $\chi \neq \chi_0$, then, by part (i) of Theorem 6.9, $L(s, \chi)$ is analytic in $\sigma > 0$, and thus, in particular, continuous at $s = 1$. Moreover, by the last part of this result, $L(1, \chi) \neq 0$. Hence, $\log L(s, \chi)$ is analytic and thus continuous in a neighborhood of $s = 1$. In particular, there exists $\sigma_0 > 1$ such that $\log L(\sigma, \chi)$ is bounded in $1 < \sigma \leq \sigma_0$. In view of (6.12), this implies

$$F_\chi(\sigma) = O(1) \quad (\chi \neq \chi_0), \tag{6.15}$$

first for $1 < \sigma \leq \sigma_0$, and then, since as before $F_\chi(\sigma)$ is bounded in $\sigma \geq \sigma_0$, for the full range $\sigma > 1$.

Proof of Dirichlet's theorem. Substituting the estimates (6.14) and (6.15) into (6.11), we obtain

$$\begin{aligned} F_{a,q}(\sigma) &= \frac{1}{\phi(q)} \overline{\chi_0(a)} F_{\chi_0}(\sigma) + O(1) \\ &= \frac{1}{\phi(q)} \log \frac{1}{\sigma - 1} + O(1) \quad (1 < \sigma \leq 2), \end{aligned}$$

since $\chi_0(a) = 1$ by the definition of a principal character and the assumption $(a, q) = 1$. This proves (6.9), and hence the asserted estimate (6.8).

6.5 The non-vanishing of $L(1, \chi)$

We now prove part (iii) of Theorem 6.9, which we restate in the following theorem.

Theorem 6.10 (Non-vanishing of $L(1, \chi)$)**.** *Let q be a positive integer and χ a non-principal character modulo q. Then $L(1, \chi) \neq 0$.*

The proof requires several auxiliary results, which we state as lemmas. The first lemma is reminiscent of the "3-4-1 inequality" of the previous chapter (Lemma 5.9), which was key to obtaining a zero-free region for the zeta function.

Lemma 6.11. *Let*

$$P(s) = P_q(s) = \prod_{\chi \bmod q} L(s, \chi).$$

Then, for $\sigma > 1$,

$$P(\sigma) \geq 1.$$

Proof. Expanding the Dirichlet series $L(s, \chi)$ into Euler products and taking logarithms, we obtain, for $\sigma > 1$,

$$\begin{aligned} \log P(\sigma) &= \sum_{\chi \bmod q} \log L(\sigma, \chi) = \sum_{\chi \bmod q} \sum_{p} \log \left(1 - \frac{\chi(p)}{p^\sigma}\right)^{-1} \\ &= \sum_{\chi \bmod q} \sum_{p} \sum_{m=1}^{\infty} \frac{\chi(p)^m}{p^{m\sigma}} \\ &= \sum_{p} \sum_{m=1}^{\infty} \frac{1}{p^{m\sigma}} \sum_{\chi \bmod q} \chi(p)^m. \end{aligned}$$

Since

$$\sum_{\chi \bmod q} \chi(p)^m = \sum_{\chi \bmod q} \chi(p^m) = \begin{cases} \phi(q) & \text{if } p^m \equiv 1 \bmod q, \\ 0 & \text{else,} \end{cases}$$

by the complete multiplicativity of χ and the orthogonality relation for characters (part (ii) of Theorem 6.7), the right-hand side above is a sum of nonnegative terms, and the assertion of the lemma follows. □

Proof of Theorem 6.10 for complex characters χ. We will use the above lemma to show that $L(1, \chi) \neq 0$ in the case χ is a *complex* character modulo q, i.e., if χ takes on non-real values. The argument is similar to that used in the proof of the non-vanishing of $\zeta(s)$ on the line $\sigma = 1$ (see Theorem 5.7).

We assume that $L(1, \chi_1) = 0$ for some complex character χ_1 modulo q. We shall derive a contradiction from this assumption.

We first note that, since χ_1 is a complex character, the characters χ_1 and $\overline{\chi_1}$ are distinct, and neither character is equal to the principal character

χ_0. Hence, χ_0, χ_1, and $\overline{\chi_1}$ each contribute a factor to the product $P(\sigma)$ in Lemma 6.11. Splitting off these three factors, we obtain, for $\sigma > 1$,

$$P(\sigma) = L(\sigma, \chi_0)L(\sigma, \chi_1)L(\sigma, \overline{\chi_1})Q(\sigma), \tag{6.16}$$

where

$$Q(\sigma) = \prod_{\substack{\chi \bmod q \\ \chi \neq \chi_0, \chi_1, \overline{\chi_1}}} L(\sigma, \chi).$$

We now examine the behavior of each term on the right of (6.16) as $\sigma \to 1+$. First, by part (ii) of Theorem 6.9, $L(s, \chi_0)$ has a simple pole at $s = 1$, so we have $L(\sigma, \chi_0) = O(1/(\sigma - 1))$ as $\sigma \to 1+$. Next, our assumption $L(1, \chi_1) = 0$ and the analyticity of $L(s, \chi_1)$ at $s = 1$ imply $L(\sigma, \chi_1) = O(\sigma - 1)$, and since

$$L(\sigma, \overline{\chi_1}) = \sum_{n=1}^{\infty} \frac{\overline{\chi_1(n)}}{n^\sigma} = \overline{\sum_{n=1}^{\infty} \frac{\chi_1(n)}{n^\sigma}} = \overline{L(\sigma, \chi_1)},$$

we also have $L(\sigma, \overline{\chi_1}) = O(\sigma - 1)$. Finally, by part (i) of Theorem 6.9, $Q(\sigma)$ is bounded as $\sigma \to 1+$.

It follows from these estimates that $P(\sigma) = O(\sigma - 1)$ as $\sigma \to 1+$. This contradicts the bound $P(\sigma) \geq 1$ of Lemma 6.11. Thus $L(1, \chi_1)$ cannot be equal to 0, and the proof of Theorem 6.10 for complex characters is complete. □

The above argument breaks down in the case of a real character χ_1, since then $\overline{\chi_1} = \chi_1$ and in the above factorization of the product $P(\sigma)$ only one L-function corresponding to χ_1 would appear, so the assumption $L(1, \chi_1) = 0$ would only give an estimate $P(\sigma) = O(1)$, which is not enough to obtain a contradiction. To prove the non-vanishing of $L(1, \chi)$ for real characters, a completely different, and more complicated, argument is needed. We prove several auxiliary results first.

Lemma 6.12. *Let χ be a real character and let $f = 1 * \chi$. Then*

$$f(n) \begin{cases} \geq 1 & \text{if } n \text{ is a square,} \\ \geq 0 & \text{otherwise.} \end{cases}$$

Proof. Since χ is multiplicative, so is f. Since χ is a real character modulo q, we have $\chi(p) = \pm 1$ if $p \nmid q$, and $\chi(p) = 0$ if $p|q$. Thus, at prime powers

p^m we have

$$f(p^m) = 1 + \sum_{k=1}^{m} \chi(p)^k = \begin{cases} 1 & \text{if } p|q, \\ m+1 & \text{if } p \nmid q \text{ and } \chi(p) = 1, \\ 0 & \text{if } p \nmid q,\ \chi(p) = -1, \text{ and } m \text{ is odd}, \\ 1 & \text{if } p \nmid q,\ \chi(p) = -1, \text{ and } m \text{ is even} \end{cases}$$

It follows that

$$f(p^m) \begin{cases} \geq 1 & \text{if } m \text{ is even}, \\ \geq 0 & \text{if } m \text{ is odd}. \end{cases}$$

By the multiplicativity of f this yields the assertion of the lemma. □

Lemma 6.13. *We have*

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

where A is a constant.

Proof. By Euler's summation formula, we have

$$\begin{aligned} \sum_{n \leq x} \frac{1}{\sqrt{n}} &= 1 - \{x\}x^{-1/2} + \int_1^x u^{-1/2} du + \int_1^x \{u\}(-1/2)u^{-3/2} du \\ &= 1 + O\left(\frac{1}{\sqrt{x}}\right) + 2(\sqrt{x} - 1) \\ &\quad - \frac{1}{2}\int_1^\infty \{u\}u^{-3/2} du + O\left(\int_x^\infty u^{-3/2} du\right) \\ &= 2\sqrt{x} + A + O\left(\frac{1}{\sqrt{x}}\right) \end{aligned}$$

with $A = -1 - (1/2)\int_1^\infty \{u\}u^{-3/2} du$. □

Lemma 6.14. *Let χ be a non-principal character modulo q and s a complex number in the half-plane $\sigma > 0$. Then*

$$\sum_{n \leq x} \frac{\chi(n)}{n^s} = L(s, \chi) + O_{q,s}(x^{-\sigma}) \quad (x \geq 1). \tag{6.17}$$

Proof. Let $M(u) = M(\chi, u) = \sum_{n \le u} \chi(n)$. By partial summation we have, for $y > x$,

$$\sum_{x < n \le y} \frac{\chi(n)}{n^s} = \frac{M(y)}{y^s} - \frac{M(x)}{x^s} + s \int_x^y M(u) u^{-s-1} du.$$

Since χ is non-principal, we have $M(u) = O_q(1)$ by Corollary 6.8, so the right-hand side above is bounded by

$$\ll_q x^{-\sigma} + |s| \int_x^y u^{-\sigma-1} du \ll_{q,s} x^{-\sigma}.$$

Letting $y \to \infty$, the left-hand side tends to $L(s, \chi) - \sum_{n \le x} \chi(n) n^{-s}$, and the result follows. □

Proof of Theorem 6.10 for real characters χ. We fix a real, non-principal character χ modulo q. Throughout the proof, we let constants in O-estimates depend on χ, and hence also on q, without explicitly indicating this dependence.

We let f be defined as in Lemma 6.12 and consider the sum

$$S(x) = \sum_{n \le x} \frac{f(n)}{\sqrt{n}}.$$

On the one hand, by Lemma 6.12 we have

$$S(x) \ge \sum_{m^2 \le x} \frac{f(m^2)}{\sqrt{m^2}} \ge \sum_{m \le \sqrt{x}} \frac{1}{m} \gg \log x \quad (x \ge 2). \tag{6.18}$$

On the other hand, we can estimate $S(x)$ by writing $f(n) = \sum_{d|n} \chi(d) = \sum_{dm=n} \chi(d)$ and splitting up the resulting double sum according to the Dirichlet hyperbola method:

$$S(x) = \sum_{\substack{d,m \le x \\ dm \le x}} \frac{\chi(d) \cdot 1}{\sqrt{d} \cdot \sqrt{m}} = \sum\nolimits_1 + \sum\nolimits_2 - \sum\nolimits_3, \tag{6.19}$$

where

$$\sum\nolimits_1 = \sum_{d \le \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{m \le x/d} \frac{1}{\sqrt{m}},$$

$$\sum\nolimits_2 = \sum_{m \le \sqrt{x}} \frac{1}{\sqrt{m}} \sum_{d \le x/m} \frac{\chi(d)}{\sqrt{d}},$$

$$\sum\nolimits_3 = \sum_{d \le \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{m \le \sqrt{x}} \frac{1}{\sqrt{m}}.$$

The last three sums can be estimated using Lemmas 6.13 and 6.14: We obtain

$$\begin{aligned}
\sum\nolimits_1 &= \sum_{d\le\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \left(2\sqrt{x/d} + A + O\left(\frac{1}{\sqrt{x/d}}\right)\right) \\
&= 2\sqrt{x} \sum_{d\le\sqrt{x}} \frac{\chi(d)}{d} + A \sum_{d\le\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} + O\left(\sum_{d\le\sqrt{x}} \frac{1}{\sqrt{x}}\right) \\
&= 2\sqrt{x}\left(L(1,\chi) + O\left(\frac{1}{\sqrt{x}}\right)\right) + A\left(L(1/2,\chi) + O\left(\frac{1}{x^{1/4}}\right)\right) + O(1) \\
&= 2\sqrt{x}L(1,\chi) + O(1), \\
\sum\nolimits_2 &= \sum_{m\le\sqrt{x}} \frac{1}{\sqrt{m}} \left(L(1/2,\chi) + O\left(\frac{1}{\sqrt{x/m}}\right)\right) \\
&= L(1/2,\chi)\left(2x^{1/4} + O(1)\right) + O\left(\sum_{m\le\sqrt{x}} \frac{1}{\sqrt{x}}\right) \\
&= L(1/2,\chi)2x^{1/4} + O(1), \\
\sum\nolimits_3 &= \left(L(1/2,\chi) + O\left(\frac{1}{x^{1/4}}\right)\right)\left(2x^{1/4} + O(1)\right) \\
&= L(1/2,\chi)2x^{1/4} + O(1).
\end{aligned}$$

Substituting these estimates into (6.19), we get

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

If now $L(1,\chi) = 0$, then we would have $S(x) = O(1)$, contradicting (6.18). Hence $L(1,\chi) \neq 0$, and the proof of Theorem 6.10 is complete. □

6.6 Exercises

6.1 Show that if every arithmetic progression a mod q with $(a,q)=1$ contains at least one prime, then every such progression contains *infinitely* many primes.

6.2 Show that if f is a periodic, completely multiplicative arithmetic function, then f is a Dirichlet character to some modulus q.

6.3 Let χ be a nonprincipal character mod q. Show that for all positive integers $a<b$ we have $\left|\sum_{n=a}^{b}\chi(n)\right| \le (1/2)\phi(q)$.

6.4 Given a rational number a with $0<a\le 1$, define $\zeta(s,a)=\sum_{n=0}^{\infty}(n+a)^{-s}$. Show that any Dirichlet L-function can be expressed in terms of the functions $\zeta(s,a)$, and that, conversely, any such function $\zeta(s,a)$ with rational a can be expressed in terms of Dirichlet L-functions.

6.5 Let a and q be positive integers with $(a,q)=1$. Express the Dirichlet series $\sum_{n\equiv a \bmod q}\mu(n)n^{-s}$ in the half-plane $\sigma>1$ in terms of Dirichlet L-functions.

6.6 Given an arithmetic function f, and a real number α, let $f_\alpha(n)=f(n)e^{2\pi i\alpha n}$, and let $F_\alpha(s)$ be the corresponding Dirichlet series. For the case when α is rational and $f=\mu$ or $f=\Lambda$, express $F_\alpha(s)$ in terms of Dirichlet L-functions.

6.7 Let $f(n)$ denote the remainder of n modulo 5 (so that $f(n)\in\{0,1,2,3,4\}$ for each n), and let $F(s)=\sum_{n=1}^{\infty}f(n)n^{-s}$ be the Dirichlet series of f.

(i) Express $F(s)$ in the half-plane $\sigma>1$ in terms of Dirichlet L-functions.

(ii) Show that $F(s)$ has a merophorphic continuation to the half-plane $\sigma>0$ and find all poles (if any) of $F(s)$ in this half-plane, and their residues.

6.8 Suppose χ is a non-principal character modulo q. We know (from the general theory of L-series) that the Dirichlet L-series $L(s,\chi)=\sum_{n=1}^{\infty}\chi(n)n^{-s}$ converges at $s=1$. Obtain an explicit estimate (i.e., one with numerical constants, rather than O's) for the "speed of convergence", i.e., a bound for the tails $\sum_{n>x}\chi(n)n^{-1}$.

6.9 Given a positive integer a with decimal representation $a = a_1 \dots a_k$ (so that $a_i \in \{0, 1, \dots, 9\}, a_1 \neq 0$), let P_a denote the set of primes whose decimal representation *begins* with the string $a_1 \dots a_k$, and let Q_a denote the set of primes whose decimal representation *ends* with this string. Let $S_a(x) = \sum_{p \leq x, p \in P_a} 1/p$ and $T_a(x) = \sum_{p \leq x, p \in Q_a} 1/p$. Obtain asymptotic estimates for $S_a(x)$ and $T_a(x)$ with error term $O_a(1)$. Which of these two functions is asymptotically larger?