[Hint: Consider the map $\mathbb{Z}(nm) \to \mathbb{Z}(n) \times \mathbb{Z}(m)$ given by $k \mapsto (k \bmod n, k \bmod m)$, and use the fact that there exist integers x and y such that $xn + ym = 1$.]

2.* Every finite abelian group G is isomorphic to a direct product of cyclic groups. Here are two more precise formulations of this theorem.

- If $p_1, \ldots, p_s$ are the distinct primes appearing in the factorization of the order of G, then

$$G \approx G(p_1) \times \cdots \times G(p_s),$$

where each $G(p)$ is of the form $G(p) = \mathbb{Z}(p^{r_1}) \times \cdots \times \mathbb{Z}(p^{r_\ell})$, with $0 \leq r_1 \leq \cdots \leq r_\ell$ (this sequence of integers depends on p of course). This decomposition is unique.

- There exist unique integers $d_1, \ldots, d_k$ such that

$$d_1 | d_2, \quad d_2 | d_3, \quad \cdots, \quad d_{k-1} | d_k$$

and

$$G \approx \mathbb{Z}(d_1) \times \cdots \times \mathbb{Z}(d_k).$$

Deduce the second formulation from the first.

3. Let $\hat{G}$ denote the collection of distinct characters of the finite abelian group G.

(a) Note that if $G = \mathbb{Z}(N)$, then $\hat{G}$ is isomorphic to G.

(b) Prove that $\widehat{G_1 \times G_2} = \hat{G}_1 \times \hat{G}_2$.

(c) Prove using Problem 2 that if G is a finite abelian group, then $\hat{G}$ is isomorphic to G.

4.* When p is prime the group $\mathbb{Z}^*(p)$ is cyclic, and $\mathbb{Z}^*(p) \approx \mathbb{Z}(p-1)$.

8 Dirichlet's Theorem

> Dirichlet, Gustav Lejeune (Düren 1805-Göttingen 1859), German mathematician. He was a number theorist at heart. But, while studying in Paris, being a very likeable person, he was befriended by Fourier and other like-minded mathematicians, and he learned analysis from them. Thus equipped, he was able to lay the foundation for the application of Fourier analysis to (analytic) theory of numbers.
>
> *S. Bochner*, 1966

As a striking application of the theory of finite Fourier series, we now prove Dirichlet's theorem on primes in arithmetic progression. This theorem states that if q and ℓ are positive integers with no common factor, then the progression

$$\ell, \ \ell + q, \ \ell + 2q, \ \ell + 3q, \ldots, \ell + kq, \ldots$$

contains infinitely many prime numbers. This change of subject matter that we undertake illustrates the wide applicability of ideas from Fourier analysis to various areas outside its seemingly narrower confines. In this particular case, it is the theory of Fourier series on the finite abelian group $\mathbb{Z}^*(q)$ that plays a key role in the solution of the problem.

1 A little elementary number theory

We begin by introducing the requisite background. This involves elementary ideas of divisibility of integers, and in particular properties regarding prime numbers. Here the basic fact, called the fundamental theorem of arithmetic, is that every integer is the product of primes in an essentially unique way.

1.1 The fundamental theorem of arithmetic

The following theorem is a mathematical formulation of long division.

Theorem 1.1 (Euclid's algorithm) *For any integers a and b with $b > 0$, there exist unique integers q and r with $0 \leq r < b$ such that*

$$a = qb + r.$$

Here q denotes the quotient of a by b, and r is the remainder, which is smaller than b.

Proof. First we prove the existence of q and r. Let S denote the set of all non-negative integers of the form $a - qb$ with $q \in \mathbb{Z}$. This set is non-empty and in fact S contains arbitrarily large positive integers since $b \neq 0$. Let r denote the smallest element in S, so that

$$r = a - qb$$

for some integer q. By construction $0 \leq r$, and we claim that $r < b$. If not, we may write $r = b + s$ with $0 \leq s < r$, so $b + s = a - qb$, which then implies

$$s = a - (q + 1)b.$$

Hence $s \in S$ with $s < r$, and this contradicts the minimality of r. So $r < b$, hence q and r satisfy the conditions of the theorem.

To prove uniqueness, suppose we also had $a = q_1 b + r_1$ where $0 \leq r_1 < b$. By subtraction we find

$$(q - q_1)b = r_1 - r.$$

The left-hand side has absolute value 0 or $\geq b$, while the right-hand side has absolute value $< b$. Hence both sides of the equation must be 0, which gives $q = q_1$ and $r = r_1$.

An integer a **divides** b if there exists another integer c such that $ac = b$; we then write $a|b$ and say that a is a **divisor** of b. Note that in particular 1 divides every integer, and $a|a$ for all integers a. A **prime number** is a positive integer greater than 1 that has no positive divisors besides 1 and itself. The main theorem in this section says that any positive integer can be written uniquely as the product of prime numbers.

The **greatest common divisor** of two positive integers a and b is the largest integer that divides both a and b. We usually denote the greatest common divisor by $\gcd(a, b)$. Two positive integers are **relatively prime** if their greatest common divisor is 1. In other words, 1 is the only positive divisor common to both a and b.

Theorem 1.2 *If $\gcd(a, b) = d$, then there exist integers x and y such that*

$$ax + by = d.$$

Proof. Consider the set S of all positive integers of the form $ax + by$ where $x, y \in \mathbb{Z}$, and let s be the smallest element in S. We claim that $s = d$. By construction, there exist integers x and y such that

$$ax + by = s.$$

Clearly, any divisor of a and b divides s, so we must have $d \leq s$. The proof will be complete if we can show that $s|a$ and $s|b$. By Euclid's algorithm, we can write $a = qs + r$ with $0 \leq r < s$. Multiplying the above by q we find $qax + qby = qs$, and therefore

$$qax + qby = a - r.$$

Hence $r = a(1 - qx) + b(-qy)$. Since s was minimal in S and $0 \leq r < s$, we conclude that $r = 0$, therefore s divides a. A similar argument shows that s divides b, hence $s = d$ as desired.

In particular we record the following three consequences of the theorem.

Corollary 1.3 *Two positive integers a and b are relatively prime if and only if there exist integers x and y such that $ax + by = 1$.*

Proof. If a and b are relatively prime, two integers x and y with the desired property exist by Theorem 1.2. Conversely, if $ax + by = 1$ holds and d is positive and divides both a and b, then d divides 1, hence $d = 1$.

Corollary 1.4 *If a and c are relatively prime and c divides ab, then c divides b. In particular, if p is a prime that does not divide a and p divides ab, then p divides b.*

Proof. We can write $1 = ax + cy$, so multiplying by b we find $b = abx + cby$. Hence $c|b$.

Corollary 1.5 *If p is prime and p divides the product $a_1 \cdots a_r$, then p divides a_i for some i.*

Proof. By the previous corollary, if p does not divide a_1, then p divides $a_2 \cdots a_r$, so eventually $p|a_i$.

We can now prove the main result of this section.

Theorem 1.6 *Every positive integer greater than 1 can be factored uniquely into a product of primes.*

Proof. First, we show that such a factorization is possible. We do so by proving that the set S of positive integers > 1 which do not have a factorization into primes is empty. Arguing by contradiction, we assume that $S \neq \emptyset$. Let n be the smallest element of S. Since n cannot be a prime, there exist integers $a > 1$ and $b > 1$ such that $ab = n$. But then $a < n$ and $b < n$, so $a \notin S$ as well as $b \notin S$. Hence both a and b have prime factorizations and so does their product n. This implies $n \notin S$, therefore S is empty, as desired.

We now turn our attention to the uniqueness of the factorization. Suppose that n has two factorizations into primes

$$\begin{aligned} n &= p_1 p_2 \cdots p_r \\ &= q_1 q_2 \cdots q_s. \end{aligned}$$

So p_1 divides $q_1 q_2 \cdots q_s$, and we can apply Corollary 1.5 to conclude that $p_1 | q_i$ for some i. Since q_i is prime, we must have $p_1 = q_i$. Continuing with this argument we find that the two factorizations of n are equal up to a permutation of the factors.

We briefly digress to give an alternate definition of the group $\mathbb{Z}^*(q)$ which appeared in the previous chapter. According to our initial definition, $\mathbb{Z}^*(q)$ is the multiplicative group of units in $\mathbb{Z}(q)$: those $n \in \mathbb{Z}(q)$ for which there exists an integer m so that

$$nm \equiv 1 \mod q. \tag{1}$$

Equivalently, $\mathbb{Z}^*(q)$ is the group under multiplication of all integers in $\mathbb{Z}(q)$ that are relatively prime to q. Indeed, notice that if (1) is satisfied, then automatically n and q are relatively prime. Conversely, suppose we assume that n and q are relatively prime. Then, if we put $a = n$ and $b = q$ in Corollary 1.3, we find

$$nx + qy = 1.$$

Hence $nx \equiv 1 \mod q$, and we can take $m = x$ to establish the equivalence.

1.2 The infinitude of primes

The study of prime numbers has always been a central topic in arithmetic, and the first fundamental problem that arose was to determine whether

there are infinitely many primes or not. This problem was solved in Euclid's *Elements* with a simple and very elegant argument.

Theorem 1.7 *There are infinitely many primes.*

Proof. Suppose not, and denote by $p_1, \ldots, p_n$ the complete set of primes. Define

$$N = p_1 p_2 \cdots p_n + 1.$$

Since N is larger than any p_i, the integer N cannot be prime. Therefore, N is divisible by a prime that belongs to our list. But this is also an absurdity since every prime divides the product, yet no prime divides 1. This contradiction concludes the proof.

Euclid's argument actually can be modified to deduce finer results about the infinitude of primes. To see this, consider the following problem. Prime numbers (except for 2) can be divided into two classes depending on whether they are of the form $4k + 1$ or $4k + 3$, and the above theorem says that at least one of these classes has to be infinite. A natural question is to ask whether both classes are infinite, and if not, which one is? In the case of primes of the form $4k + 3$, the fact that the class is infinite has a proof that is similar to Euclid's, but with a twist. If there are only finitely many such primes, enumerate them in increasing order omitting 3,

$$p_1 = 7, \quad p_2 = 11, \quad \ldots, \quad p_n,$$

and let

$$N = 4p_1 p_2 \cdots p_n + 3.$$

Clearly, N is of the form $4k + 3$ and cannot be prime since $N > p_n$. Since the product of two numbers of the form $4m + 1$ is again of the form $4m + 1$, one of the prime divisors of N, say p, must be of the form $4k + 3$. We must have $p \neq 3$, since 3 does not divide the product in the definition of N. Also, p cannot be one of the other primes of the form $4k + 3$, that is, $p \neq p_i$ for $i = 1, \ldots n$, because then p divides the product $p_1 \cdots p_n$ but does not divide 3.

It remains to determine if the class of primes of the form $4k + 1$ is infinite. A simple-minded modification of the above argument does not work since the product of two numbers of the form $4m + 3$ is never of the form $4m + 3$. More generally, in an attempt to prove the law of quadratic reciprocity, Legendre formulated the following statement:

If q and ℓ are relatively prime, then the sequence

$$\ell + kq, \qquad k \in \mathbb{Z}$$

contains infinitely many primes (hence at least one prime!).

Of course, the condition that q and ℓ be relatively prime is necessary, for otherwise $\ell + kq$ is never prime. In other words, this hypothesis says that any arithmetic progression that could contain primes necessarily contains infinitely many of them.

Legendre's assertion was proved by Dirichlet. The key idea in his proof is Euler's analytical approach to prime numbers involving his product formula, which gives a strengthened version of Theorem 1.7. This insight of Euler led to a deep connection between the theory of primes and analysis.

The zeta function and its Euler product

We begin with a rapid review of infinite products. If $\{A_n\}_{n=1}^{\infty}$ is a sequence of real numbers, we define

$$\prod_{n=1}^{\infty} A_n = \lim_{N\to\infty} \prod_{n=1}^{N} A_n$$

if the limit exists, in which case we say that the product converges. The natural approach is to take logarithms and transform products into sums. We gather in a lemma the properties we shall need of the function $\log x$, defined for positive real numbers.

Lemma 1.8 *The exponential and logarithm functions satisfy the following properties:*

(i) $e^{\log x} = x$.

(ii) $\log(1+x) = x + E(x)$ *where* $|E(x)| \le x^2$ *if* $|x| < 1/2$.

(iii) *If* $\log(1+x) = y$ *and* $|x| < 1/2$, *then* $|y| \le 2|x|$.

In terms of the O notation, property (ii) will be recorded as $\log(1+x) = x + O(x^2)$.

Proof. Property (i) is standard. To prove property (ii) we use the power series expansion of $\log(1+x)$ for $|x| < 1$, that is,

$$\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n. \tag{2}$$

Then we have

$$E(x) = \log(1+x) - x = -\frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots,$$

and the triangle inequality implies

$$|E(x)| \le \frac{x^2}{2}\left(1 + |x| + |x|^2 + \cdots\right).$$

Therefore, if $|x| \le 1/2$ we can sum the geometric series on the right-hand side to find that

$$\begin{aligned} |E(x)| &\le \frac{x^2}{2}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right) \\ &\le \frac{x^2}{2}\left(\frac{1}{1-1/2}\right) \\ &\le x^2. \end{aligned}$$

The proof of property (iii) is now immediate; if $x \neq 0$ and $|x| \le 1/2$, then

$$\begin{aligned} \left|\frac{\log(1+x)}{x}\right| &\le 1 + \left|\frac{E(x)}{x}\right| \\ &\le 1 + |x| \\ &\le 2, \end{aligned}$$

and if $x = 0$, (iii) is clearly also true.

We can now prove the main result on infinite products of real numbers.

Proposition 1.9 *If* $A_n = 1 + a_n$ *and* $\sum |a_n|$ *converges, then the product* $\prod_n A_n$ *converges, and this product vanishes if and only if one of its factors* A_n *vanishes. Also, if* $a_n \neq 1$ *for all* n, *then* $\prod_n 1/(1-a_n)$ *converges.*

Proof. If $\sum |a_n|$ converges, then for all large n we must have $|a_n| < 1/2$. Disregarding finitely many terms if necessary, we may assume that this inequality holds for all n. Then we may write the partial products as follows:

$$\prod_{n=1}^{N} A_n = \prod_{n=1}^{N} e^{\log(1+a_n)} = e^{B_N},$$

where $B_N = \sum_{n=1}^{N} b_n$ with $b_n = \log(1+a_n)$. By the lemma, we know that $|b_n| \le 2|a_n|$, so that B_N converges to a real number, say B. Since

the exponential function is continuous, we conclude that e^{B_N} converges to e^B as N goes to infinity, proving the first assertion of the proposition. Observe also that if $1 + a_n \neq 0$ for all n, the product converges to a non-zero limit since it is expressed as e^B.

Finally observe that the partial products of $\prod_n 1/(1-a_n)$ are $1/\prod_{n=1}^N (1-a_n)$, so the same argument as above proves that the product in the denominator converges to a non-zero limit.

With these preliminaries behind us, we can now return to the heart of the matter. For s a real number (strictly) greater than 1, we define the **zeta function** by

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

To see that the series defining ζ converges, we use the principle that whenever f is a decreasing function one can compare $\sum f(n)$ with $\int f(x)\,dx$, as is suggested by Figure 1. Note also that a similar technique was used in Chapter 3, that time bounding a sum from below by an integral.

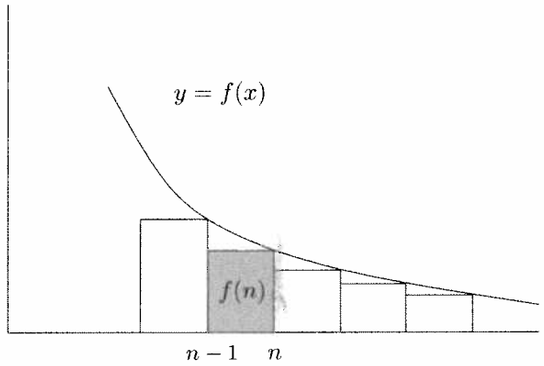

Figure 1. Comparing sums with integrals

Here we take $f(x) = 1/x^s$ to see that

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \leq 1 + \sum_{n=2}^{\infty} \int_{n-1}^{n} \frac{dx}{x^s} = 1 + \int_1^{\infty} \frac{dx}{x^s},$$

and therefore,

$$\zeta(s) \leq 1 + \frac{1}{s-1}. \tag{3}$$

Clearly, the series defining ζ converges uniformly on each half-line $s > s_0 > 1$, hence ζ is continuous when $s > 1$. The zeta function was already mentioned earlier in the discussion of the Poisson summation formula and the theta function.

The key result is Euler's product formula.

Theorem 1.10 *For every $s > 1$, we have*

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

where the product is taken over all primes.

It is important to remark that this identity is an analytic expression of the fundamental theorem of arithmetic. In fact, each factor of the product $1/(1-p^{-s})$ can be written as a convergent geometric series

$$1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots + \frac{1}{p^{Ms}} + \cdots.$$

So we consider

$$\prod_{p_j} \left(1 + \frac{1}{p_j^s} + \frac{1}{p_j^{2s}} + \cdots + \frac{1}{p_j^{Ms}} + \cdots\right),$$

where the product is taken over all primes, which we order in increasing order $p_1 < p_2 < \cdots$. Proceeding formally (these manipulations will be justified below), we calculate the product as a sum of terms, each term originating by picking out a term $1/p_j^{ks}$ (in the sum corresponding to p_j) with a k, which of course will depend on j, and with $k = 0$ for j sufficiently large. The product obtained this way is

$$\frac{1}{(p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m})^s} = \frac{1}{n^s},$$

where the integer n is written as a product of primes $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$. By the fundamental theorem of arithmetic, each integer ≥ 1 occurs in this way uniquely, hence the product equals

$$\sum_{n=1}^{\infty} \frac{1}{n^s}.$$

We now justify this heuristic argument.

Proof. Suppose M and N are positive integers with $M > N$. Observe now that any positive integer $n \leq N$ can be written uniquely as a product of primes, and that each prime must be less than or equal to N and repeated less than M times. Therefore

$$\begin{aligned}\sum_{n=1}^{N} \frac{1}{n^s} &\leq \prod_{p \leq N} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots + \frac{1}{p^{Ms}}\right) \\ &\leq \prod_{p \leq N} \left(\frac{1}{1 - p^{-s}}\right) \\ &\leq \prod_{p} \left(\frac{1}{1 - p^{-s}}\right).\end{aligned}$$

Letting N tend to infinity now yields

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

For the reverse inequality, we argue as follows. Again, by the fundamental theorem of arithmetic, we find that

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

Letting M tend to infinity gives

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

Hence

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

and the proof of the product formula is complete.

We now come to Euler's version of Theorem 1.7, which inspired Dirichlet's approach to the general problem of primes in arithmetic progression. The point is the following proposition.

Proposition 1.11 *The series*

$$\sum_{p} 1/p$$

diverges, when the sum is taken over all primes p.

Of course, if there were only finitely many primes the series would converge automatically.

Proof. We take logarithms of both sides of the Euler formula. Since $\log x$ is continuous, we may write the logarithm of the infinite product as the sum of the logarithms. Therefore, we obtain for $s > 1$

$$-\sum_{p} \log(1 - 1/p^s) = \log \zeta(s).$$

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

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

which gives

$$\sum_{p} 1/p^s + O(1) = \log \zeta(s).$$

The term $O(1)$ appears because $\sum_p 1/p^{2s} \leq \sum_{n=1}^{\infty} 1/n^2$. Now we let s tend to 1 from above, namely $s \to 1^+$, and note that $\zeta(s) \to \infty$ since $\sum_{n=1}^{\infty} 1/n^s \geq \sum_{n=1}^{M} 1/n^s$, and therefore

$$\liminf_{s \to 1^+} \sum_{n=1}^{\infty} 1/n^s \geq \sum_{n=1}^{M} 1/n \quad \text{for every } M.$$

We conclude that $\sum_p 1/p^s \to \infty$ as $s \to 1^+$, and since $1/p > 1/p^s$ for all $s > 1$, we finally have that

$$\sum_{p} 1/p = \infty.$$

In the rest of this chapter we see how Dirichlet adapted Euler's insight.

2 Dirichlet's theorem

We remind the reader of our goal:

Theorem 2.1 *If q and ℓ are relatively prime positive integers, then there are infinitely many primes of the form $\ell + kq$ with $k \in \mathbb{Z}$.*

Following Euler's argument, Dirichlet proved this theorem by showing that the series

$$\sum_{p \equiv \ell \mod q} \frac{1}{p}$$

diverges, where the sum is over all primes congruent to ℓ modulo q. Once q is fixed and no confusion is possible, we write $p \equiv \ell$ to denote a prime congruent to ℓ modulo q. The proof consists of several steps, one of which requires Fourier analysis on the group $\mathbb{Z}^*(q)$. Before proceeding with the theorem in its complete generality, we outline the solution to the particular problem raised earlier: are there infinitely many primes of the form $4k+1$? This example, which consists of the special case $q = 4$ and $\ell = 1$, illustrates all the important steps in the proof of Dirichlet's theorem.

We begin with the character on $\mathbb{Z}^*(4)$ defined by $\chi(1) = 1$ and $\chi(3) = -1$. We extend this character to all of $\mathbb{Z}$ as follows:

$$\chi(n) = \begin{cases} 0 & \text{if } n \text{ is even,} \\ 1 & \text{if } n = 4k+1, \\ -1 & \text{if } n = 4k+3. \end{cases}$$

Note that this function is multiplicative, that is, $\chi(nm) = \chi(n)\chi(m)$ on *all* of $\mathbb{Z}$. Let $L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)/n^s$, so that

$$L(s,\chi) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \cdots.$$

Then $L(1,\chi)$ is the convergent series given by

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots.$$

Since the terms in the series are alternating and their absolute values decrease to zero we have $L(1,\chi) \neq 0$. Because χ is multiplicative, the Euler product generalizes (as we will prove later) to give

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

Taking the logarithm of both sides, we find that

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

Letting $s \to 1^+$, the observation that $L(1,\chi) \neq 0$ shows that $\sum_p \chi(p)/p^s$ remains bounded. Hence

$$\sum_{p \equiv 1} \frac{1}{p^s} - \sum_{p \equiv 3} \frac{1}{p^s}$$

is bounded as $s \to 1^+$. However, we know from Proposition 1.11 that

$$\sum_p \frac{1}{p^s}$$

is unbounded as $s \to 1^+$, so putting these two facts together, we find that

$$2 \sum_{p \equiv 1} \frac{1}{p^s}$$

is unbounded as $s \to 1^+$. Hence $\sum_{p \equiv 1} 1/p$ diverges, and as a consequence there are infinitely many primes of the form $4k+1$.

We digress briefly to show that in fact $L(1,\chi) = \pi/4$. To see this, we integrate the identity

$$\frac{1}{1+x^2} = 1 - x^2 + x^4 - x^6 + \cdots,$$

and get

$$\int_0^y \frac{dx}{1+x^2} = y - \frac{y^3}{3} + \frac{y^5}{5} - \cdots, \qquad 0 < y < 1.$$

We then let y tend to 1. The integral can be calculated as

$$\int_0^1 \frac{dx}{1+x^2} = \arctan u \Big|_0^1 = \frac{\pi}{4},$$

so this proves that the series $1 - 1/3 + 1/5 - \cdots$ is Abel summable to $\pi/4$. Since we know the series converges, its limit is the same as its Abel limit, hence $1 - 1/3 + 1/5 - \cdots = \pi/4$.

The rest of this chapter gives the full proof of Dirichlet's theorem. We begin with the Fourier analysis (which is actually the last step in the example given above), and reduce the theorem to the non-vanishing of L-functions.

2.1 Fourier analysis, Dirichlet characters, and reduction of the theorem

In what follows we take the abelian group G to be $\mathbb{Z}^*(q)$. Our formulas below involve the order of G, which is the number of integers $0 \leq n < q$ that are relatively prime to q; this number defines the **Euler phi-function** $\varphi(q)$, and $|G| = \varphi(q)$.

Consider the function δ_ℓ on G, which we think of as the characteristic function of ℓ; if $n \in \mathbb{Z}^*(q)$, then

$$\delta_\ell(n) = \begin{cases} 1 & \text{if } n \equiv \ell \mod q, \\ 0 & \text{otherwise.} \end{cases}$$

We can expand this function in a Fourier series as follows:

$$\delta_\ell(n) = \sum_{e \in \hat{G}} \hat{\delta}_\ell(e) e(n),$$

where

$$\hat{\delta}_\ell(e) = \frac{1}{|G|} \sum_{m \in G} \delta_\ell(m) \overline{e(m)} = \frac{1}{|G|} \overline{e(\ell)}.$$

Hence

$$\delta_\ell(n) = \frac{1}{|G|} \sum_{e \in \hat{G}} \overline{e(\ell)} e(n).$$

We can extend the function δ_ℓ to all of $\mathbb{Z}$ by setting $\delta_\ell(m) = 0$ whenever m and q are not relatively prime. Similarly, the extensions of the characters $e \in \hat{G}$ to all of $\mathbb{Z}$ which are given by the recipe

$$\chi(m) = \begin{cases} e(m) & \text{if } m \text{ and } q \text{ are relatively prime} \\ 0 & \text{otherwise,} \end{cases}$$

are called the **Dirichlet characters** modulo q. We shall denote the extension to $\mathbb{Z}$ of the trivial character of G by χ_0, so that $\chi_0(m) = 1$ if m and q are relatively prime, and 0 otherwise. Note that the Dirichlet characters modulo q are multiplicative on all of $\mathbb{Z}$, in the sense that

$$\chi(nm) = \chi(n)\chi(m) \quad \text{for all } n, m \in \mathbb{Z}.$$

Since the integer q is fixed, we may without fear of confusion, speak of "Dirichlet characters" omitting reference to q.[1]

With $|G| = \varphi(q)$, we may restate the above results as follows:

[1] We use the notation χ instead of e to distinguish the Dirichlet characters (defined on $\mathbb{Z}$) from the characters e (defined on $\mathbb{Z}^*(q)$).

Lemma 2.2 *The Dirichlet characters are multiplicative. Moreover,*

$$\delta_\ell(m) = \frac{1}{\varphi(q)} \sum_\chi \overline{\chi(\ell)} \chi(m),$$

where the sum is over all Dirichlet characters.

With the above lemma we have taken our first step towards a proof of the theorem, since this lemma shows that

$$\begin{aligned} \sum_{p \equiv \ell} \frac{1}{p^s} &= \sum_p \frac{\delta_\ell(p)}{p^s} \\ &= \frac{1}{\varphi(q)} \sum_\chi \overline{\chi(\ell)} \sum_p \frac{\chi(p)}{p^s}. \end{aligned}$$

Thus it suffices to understand the behavior of $\sum_p \chi(p) p^{-s}$ as $s \to 1^+$. In fact, we divide the above sum in two parts depending on whether or not χ is trivial. So we have

$$\begin{aligned} \sum_{p \equiv \ell} \frac{1}{p^s} &= \frac{1}{\varphi(q)} \sum_p \frac{\chi_0(p)}{p^s} + \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_0} \overline{\chi(\ell)} \sum_p \frac{\chi(p)}{p^s} \\ &= \frac{1}{\varphi(q)} \sum_{p \text{ not dividing } q} \frac{1}{p^s} + \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_0} \overline{\chi(\ell)} \sum_p \frac{\chi(p)}{p^s}. \end{aligned} \tag{4}$$

Since there are only finitely many primes dividing q, Euler's theorem (Proposition 1.11) implies that the first sum on the right-hand side diverges when s tends to 1. These observations show that Dirichlet's theorem is a consequence of the following assertion.

Theorem 2.3 *If χ is a nontrivial Dirichlet character, then the sum*

$$\sum_p \frac{\chi(p)}{p^s}$$

remains bounded as $s \to 1^+$.

The proof of Theorem 2.3 requires the introduction of the L-functions, to which we now turn.

2.2 Dirichlet L-functions

We proved earlier that the zeta function $\zeta(s) = \sum_n 1/n^s$ could be expressed as a product, namely

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

Dirichlet observed an analogue of this formula for the so-called **L-functions** defined for $s > 1$ by

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

where χ is a Dirichlet character.

Theorem 2.4 *If $s > 1$, then*

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

where the product is over all primes.

Assuming this theorem for now, we can follow Euler's argument formally: taking the logarithm of the product and using the fact that $\log(1 + x) = x + O(x^2)$ whenever x is small, we would get

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

If $L(1, \chi)$ is finite and non-zero, then $\log L(s, \chi)$ is bounded as $s \to 1^+$, and we can conclude that the sum

$$\sum_p \frac{\chi(p)}{p^s}$$

is bounded as $s \to 1^+$. We now make several observations about the above formal argument.

First, we must prove the product formula in Theorem 2.4. Since the Dirichlet characters χ can be complex-valued we will extend the logarithm to complex numbers w of the form $w = 1/(1 - z)$ with $|z| < 1$. (This will be done in terms of a power series.) Then we show that with this definition of the logarithm, the proof of Euler's product formula given earlier carries over to L-functions.

Second, we must make sense of taking the logarithm of both sides of the product formula. If the Dirichlet characters are real, this argument works

and is precisely the one given in the example corresponding to primes of the form $4k + 1$. In general, the difficulty lies in the fact that $\chi(p)$ is a complex number, and the complex logarithm is not single valued; in particular, the logarithm of a product is not the sum of the logarithms.

Third, it remains to prove that whenever $\chi \neq \chi_0$, then $\log L(s, \chi)$ is bounded as $s \to 1^+$. If (as we shall see) $L(s, \chi)$ is continuous at $s = 1$, then it suffices to show that

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

This is the non-vanishing we mentioned earlier, which corresponds to the alternating series being non-zero in the previous example. The fact that $L(1, \chi) \neq 0$ is the most difficult part of the argument.

So we will focus on three points:

1. Complex logarithms and infinite products.
2. Study of $L(s, \chi)$.
3. Proof that $L(1, \chi) \neq 0$ if χ is non-trivial.

However, before we enter further into the details, we pause briefly to discuss some historical facts surrounding Dirichlet's theorem.

Historical digression

In the following list, we have gathered the names of those mathematicians whose work dealt most closely with the series of achievements related to Dirichlet's theorem. To give a better perspective, we attach the years in which they reached the age of 35:

Euler 1742
Legendre 1787
Gauss 1812
Dirichlet 1840
Riemann 1861

As we mentioned earlier, Euler's discovery of the product formula for the zeta function is the starting point in Dirichlet's argument. Legendre in effect conjectured the theorem because he needed it in his proof of the law of quadratic reciprocity. However, this goal was first accomplished by Gauss who, while not knowing how to establish the theorem about primes in arithmetic progression, nevertheless found a number of different proofs of quadratic reciprocity. Later, Riemann extended the study of the zeta function to the complex plane and indicated how properties

related to the non-vanishing of that function were central in the further understanding of the distribution of prime numbers.

Dirichlet proved his theorem in 1837. It should be noted that Fourier, who had befriended Dirichlet when the latter was a young mathematician visiting Paris, had died several years before. Besides the great activity in mathematics, that period was also a very fertile time in the arts, and in particular music. The era of Beethoven had ended only ten years earlier, and Schumann was now reaching the heights of his creativity. But the musician whose career was closest to Dirichlet was Felix Mendelssohn (four years his junior). It so happens that the latter began composing his famous violin concerto the year after Dirichlet succeeded in proving his theorem.

3 Proof of the theorem

We return to the proof of Dirichlet's theorem and to the three difficulties mentioned above.

3.1 Logarithms

The device to deal with the first point is to define two logarithms, one for complex numbers of the form $1/(1-z)$ with $|z|<1$ which we denote by $\log_1$, and one for the function $L(s,\chi)$ which we will denote by $\log_2$.

For the first logarithm, we define

$$\log_1\left(\frac{1}{1-z}\right)=\sum_{k=1}^{\infty}\frac{z^k}{k} \quad \text{for } |z|<1.$$

Note that $\log_1 w$ is then defined if $\mathrm{Re}(w)>1/2$, and because of equation (2), $\log_1 w$ gives an extension of the usual $\log x$ when x is a real number $>1/2$.

Proposition 3.1 *The logarithm function* $\log_1$ *satisfies the following properties:*

(i) *If* $|z|<1$, *then*

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

(ii) *If* $|z|<1$, *then*

$$\log_1\left(\frac{1}{1-z}\right)=z+E_1(z),$$

where the error E_1 *satisfies* $|E_1(z)|\le|z|^2$ *if* $|z|<1/2$.

(iii) *If* $|z|<1/2$, *then*

$$\left|\log_1\left(\frac{1}{1-z}\right)\right|\le 2|z|.$$

Proof. To establish the first property, let $z=re^{i\theta}$ with $0\le r<1$, and observe that it suffices to show that

$$(1-re^{i\theta})\,e^{\sum_{k=1}^{\infty}(re^{i\theta})^k/k}=1. \tag{5}$$

To do so, we differentiate the left-hand side with respect to r, and this gives

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

The term in brackets equals

$$-e^{i\theta}+(1-re^{i\theta})e^{i\theta}\left(\sum_{k=1}^{\infty}(re^{i\theta})^{k-1}\right)=-e^{i\theta}+(1-re^{i\theta})e^{i\theta}\frac{1}{1-re^{i\theta}}=0.$$

Having found that the left-hand side of the equation (5) is constant, we set $r=0$ and get the desired result.

The proofs of the second and third properties are the same as their real counterparts given in Lemma 1.8.

Using these results we can state a sufficient condition guaranteeing the convergence of infinite products of complex numbers. Its proof is the same as in the real case, except that we now use the logarithm $\log_1$.

Proposition 3.2 *If* $\sum|a_n|$ *converges, and* $a_n\neq 1$ *for all* n, *then*

$$\prod_{n=1}^{\infty}\left(\frac{1}{1-a_n}\right)$$

converges. Moreover, this product is non-zero.

Proof. For n large enough, $|a_n|<1/2$, so we may assume without loss of generality that this inequality holds for all $n\ge 1$. Then

$$\prod_{n=1}^{N}\left(\frac{1}{1-a_n}\right)=\prod_{n=1}^{N}e^{\log_1\left(\frac{1}{1-a_n}\right)}=e^{\sum_{n=1}^{N}\log_1\left(\frac{1}{1-a_n}\right)}.$$

But we know from the previous proposition that

$$\left|\log_1\left(\frac{1}{1-z}\right)\right| \leq 2|z|,$$

so the fact that the series $\sum |a_n|$ converges, immediately implies that the limit

$$\lim_{N\to\infty} \sum_{n=1}^{N} \log_1\left(\frac{1}{1-a_n}\right) = A$$

exists. Since the exponential function is continuous, we conclude that the product converges to e^A, which is clearly non-zero.

We may now prove the promised Dirichlet product formula

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

For simplicity of notation, let L denote the left-hand side of the above equation. Define

$$S_N = \sum_{n\leq N} \chi(n)n^{-s} \quad \text{and} \quad \Pi_N = \prod_{p\leq N}\left(\frac{1}{1-\chi(p)p^{-s}}\right).$$

The infinite product $\Pi = \lim_{N\to\infty}\Pi_N = \prod_p\left(\frac{1}{1-\chi(p)p^{-s}}\right)$ converges by the previous proposition. Indeed, if we set $a_n = \chi(p_n)p_n^{-s}$, where p_n is the n^{th} prime, we note that if $s > 1$, then $\sum |a_n| < \infty$.

Also, define

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

Now fix $\epsilon > 0$ and choose N so large that

$$|S_N - L| < \epsilon \quad \text{and} \quad |\Pi_N - \Pi| < \epsilon.$$

We can next select M large enough so that

$$|S_N - \Pi_{N,M}| < \epsilon \quad \text{and} \quad |\Pi_{N,M} - \Pi_N| < \epsilon.$$

To see the first inequality, one uses the fundamental theorem of arithmetic and the fact that the Dirichlet characters are multiplicative. The

second inequality follows merely because each series $\sum_{n=1}^{\infty}\frac{\chi(p^n)}{p^{ns}}$ converges.

Therefore

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

as was to be shown.

3.2 *L*-functions

The next step is a better understanding of the L-functions. Their behavior as functions of s (especially near $s = 1$) depends on whether or not χ is trivial. In the first case, $L(s, \chi_0)$ is up to some simple factors just the zeta function.

Proposition 3.3 *Suppose χ_0 is the trivial Dirichlet character,*

$$\chi_0(n) = \begin{cases} 1 & \text{if } n \text{ and } q \text{ are relatively prime,} \\ 0 & \text{otherwise,} \end{cases}$$

and $q = p_1^{a_1}\cdots p_N^{a_N}$ is the prime factorization of q. Then

$$L(s,\chi_0) = (1-p_1^{-s})(1-p_2^{-s})\cdots(1-p_N^{-s})\zeta(s).$$

Therefore $L(s, \chi_0) \to \infty$ as $s \to 1^+$.

Proof. The identity follows at once on comparing the Dirichlet and Euler product formulas. The final statement holds because $\zeta(s) \to \infty$ as $s \to 1^+$.

The behavior of the remaining L-functions, those for which $\chi \neq \chi_0$, is more subtle. A remarkable property is that these functions are now defined and continuous for $s > 0$. In fact, more is true.

Proposition 3.4 *If χ is a non-trivial Dirichlet character, then the series*

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

converges for $s > 0$, and we denote its sum by $L(s, \chi)$. Moreover:

(i) *The function $L(s, \chi)$ is continuously differentiable for $0 < s < \infty$.*

(ii) *There exists constants $c, c' > 0$ so that*

$$L(s,\chi) = 1 + O(e^{-cs}) \quad \text{as } s \to \infty, \text{ and}$$

$$L'(s,\chi) = O(e^{-c's}) \quad \text{as } s \to \infty.$$

We first isolate the key cancellation property that non-trivial Dirichlet characters possess, which accounts for the behavior of the L-function described in the proposition.

Lemma 3.5 *If χ is a non-trivial Dirichlet character, then*

$$\left|\sum_{n=1}^{k}\chi(n)\right| \leq q, \quad \text{for any } k.$$

Proof. First, we recall that

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

In fact, if S denotes the sum and $a \in \mathbb{Z}^*(q)$, then the multiplicative property of the Dirichlet character χ gives

$$\chi(a)S = \sum \chi(a)\chi(n) = \sum \chi(an) = \sum \chi(n) = S.$$

Since χ is non-trivial, $\chi(a) \neq 1$ for some a, hence $S = 0$. We now write $k = aq + b$ with $0 \leq b < q$, and note that

$$\sum_{n=1}^{k}\chi(n) = \sum_{n=1}^{aq}\chi(n) + \sum_{aq<n\leq aq+b}\chi(n) = \sum_{aq<n\leq aq+b}\chi(n),$$

and there are no more than q terms in the last sum. The proof is complete once we recall that $|\chi(n)| \leq 1$.

We can now prove the proposition. Let $s_k = \sum_{n=1}^{k}\chi(n)$, and $s_0 = 0$. We know that $L(s,\chi)$ is defined for $s > 1$ by the series

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

which converges absolutely and uniformly for $s > \delta > 1$. Moreover, the differentiated series also converges absolutely and uniformly for $s > \delta > 1$, which shows that $L(s,\chi)$ is continuously differentiable for $s > 1$. We

sum by parts[2] to extend this result to $s > 0$. Indeed, we have

$$\begin{aligned}\sum_{k=1}^{N}\frac{\chi(k)}{k^s} &= \sum_{k=1}^{N}\frac{s_k - s_{k-1}}{k^s}\\ &= \sum_{k=1}^{N-1}s_k\left[\frac{1}{k^s} - \frac{1}{(k+1)^s}\right] + \frac{s_N}{N^s}\\ &= \sum_{k=1}^{N-1}f_k(s) + \frac{s_N}{N^s},\end{aligned}$$

where $f_k(s) = s_k\left[k^{-s} - (k+1)^{-s}\right]$. If $g(x) = x^{-s}$, then $g'(x) = -sx^{-s-1}$, so applying the mean-value theorem between $x = k$ and $x = k+1$, and the fact that $|s_k| \leq q$, we find that

$$|f_k(s)| \leq qsk^{-s-1}.$$

Therefore, the series $\sum f_k(s)$ converges absolutely and uniformly for $s > \delta > 0$, and this proves that $L(s,\chi)$ is continuous for $s > 0$. To prove that it is also continuously differentiable, we differentiate the series term by term, obtaining

$$\sum(\log n)\frac{\chi(n)}{n^s}.$$

Again, we rewrite this series using summation by parts as

$$\sum s_k\left[-k^{-s}\log k + (k+1)^{-s}\log(k+1)\right],$$

and an application of the mean-value theorem to the function $g(x) = x^{-s}\log x$ shows that the terms are $O(k^{-\delta/2-1})$, thus proving that the differentiated series converges uniformly for $s > \delta > 0$. Hence $L(s,\chi)$ is continuously differentiable for $s > 0$.

Now, observe that for all s large,

$$\begin{aligned}|L(s,\chi) - 1| &\leq 2q\sum_{n=2}^{\infty}n^{-s}\\ &\leq 2^{-s}O(1),\end{aligned}$$

and we can take $c = \log 2$, to see that $L(s,\chi) = 1 + O(e^{-cs})$ as $s \to \infty$. A similar argument also shows that $L'(s,\chi) = O(e^{-c's})$ as $s \to \infty$ with in fact $c' = c$, and the proof of the proposition is complete.

[2]For the formula of summation by parts, see Exercise 7 in Chapter 2.

With the facts gathered so far about $L(s,\chi)$ we are in a position to define the logarithm of the L-functions. This is done by integrating its logarithmic derivative. In other words, if χ is a non-trivial Dirichlet character and $s > 1$ we define[3]

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

We know that $L(t,\chi) \neq 0$ for every $t > 1$ since it is given by a product (Proposition 3.2), and the integral is convergent because

$$\frac{L'(t,\chi)}{L(t,\chi)} = O(e^{-ct}),$$

which follows from the behavior at infinity of $L(t,\chi)$ and $L'(t,\chi)$ recorded earlier.

The following links the two logarithms.

Proposition 3.6 *If $s > 1$, then*

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

Moreover

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

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

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

So $e^{-\log_2 L(s,\chi)}L(s,\chi)$ is constant, and this constant can be seen to be 1 by letting s tend to infinity. This proves the first conclusion.

To prove the equality between the logarithms, we fix s and take the exponential of both sides. The left-hand side becomes $e^{\log_2 L(s,\chi)} = L(s,\chi)$, and the right-hand side becomes

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

[3]The notation $\log_2$ used in this context should not be confused with the logarithm to the base 2.

by (i) in Proposition 3.1 and the Dirichlet product formula. Therefore, for each s there exists an integer $M(s)$ so that

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

As the reader may verify, the left-hand side is continuous in s, and this implies the continuity of the function $M(s)$. But $M(s)$ is integer-valued so we conclude that $M(s)$ is constant, and this constant can be seen to be 0 by letting s go to infinity.

Putting together the work we have done so far gives rigorous meaning to the formal argument presented earlier. Indeed, the properties of $\log_1$ show that

$$\begin{aligned}\sum_p \log_1\left(\frac{1}{1-\chi(p)/p^s}\right) &= \sum_p \frac{\chi(p)}{p^s} + O\left(\sum_p \frac{1}{p^{2s}}\right)\\ &= \sum_p \frac{\chi(p)}{p^s} + O(1).\end{aligned}$$

Now if $L(1,\chi) \neq 0$ for a non-trivial Dirichlet character, then by its integral representation $\log_2 L(s,\chi)$ remains bounded as $s \to 1^+$. Thus the identity between the logarithms implies that $\sum_p \chi(p)p^{-s}$ remains bounded as $s \to 1^+$, which is the desired result. Therefore, to finish the proof of Dirichlet's theorem, we need to see that $L(1,\chi) \neq 0$ when χ is non-trivial.

3.3 Non-vanishing of the L-function

We now turn to a proof of the following deep result:

Theorem 3.7 *If $\chi \neq \chi_0$, then $L(1,\chi) \neq 0$.*

There are several proofs of this fact, some involving algebraic number theory (among them Dirichlet's original argument), and others involving complex analysis. Here we opt for a more elementary argument that requires no special knowledge of either of these areas. The proof splits in two cases, depending on whether χ is complex or real. A Dirichlet character is said to be **real** if it takes on only real values (that is, $+1$, -1, or 0) and **complex** otherwise. In other words, χ is real if and only if $\chi(n) = \overline{\chi(n)}$ for all integers n.

Case I: complex Dirichlet characters

This is the easier of the two cases. The proof is by contradiction, and we use two lemmas.

Lemma 3.8 *If $s > 1$, then*

$$\prod_{\chi} L(s,\chi) \geq 1,$$

where the product is taken over all Dirichlet characters. In particular the product is real-valued.

Proof. We have shown earlier that for $s > 1$

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

Hence,

$$\begin{aligned}\prod_{\chi} L(s,\chi) &= \exp\left(\sum_{\chi}\sum_p \log_1\left(\frac{1}{1-\chi(p)p^{-s}}\right)\right)\\ &= \exp\left(\sum_{\chi}\sum_p\sum_{k=1}^{\infty}\frac{1}{k}\frac{\chi(p^k)}{p^{ks}}\right)\\ &= \exp\left(\sum_p\sum_{k=1}^{\infty}\sum_{\chi}\frac{1}{k}\frac{\chi(p^k)}{p^{ks}}\right).\end{aligned}$$

Because of Lemma 2.2 (with $\ell = 0$) we have $\sum_\chi \chi(p^k) = \varphi(q)\delta_0(p^k)$, and hence

$$\prod_{\chi} L(s,\chi) = \exp\left(\varphi(q)\sum_p\sum_{k=1}^{\infty}\frac{1}{k}\frac{\delta_0(p^k)}{p^{ks}}\right) \geq 1,$$

since the term in the exponential is non-negative.

Lemma 3.9 *The following three properties hold:*

(i) *If $L(1,\chi) = 0$, then $L(1,\overline{\chi}) = 0$.*

(ii) *If χ is non-trivial and $L(1,\chi) = 0$, then*

$$|L(s,\chi)| \leq C|s-1| \quad \text{when } 1 \leq s \leq 2.$$

(iii) *For the trivial Dirichlet character χ_0, we have*

$$|L(s,\chi_0)| \leq \frac{C}{|s-1|} \quad \text{when } 1 < s \leq 2.$$

Proof. The first statement is immediate because $L(1,\overline{\chi}) = \overline{L(1,\chi)}$. The second statement follows from the mean-value theorem since $L(s,\chi)$ is continuously differentiable for $s > 0$ when χ is non-trivial. Finally, the last statement follows because by Proposition 3.3

$$L(s,\chi_0) = (1-p_1^{-s})(1-p_2^{-s})\cdots(1-p_N^{-s})\zeta(s),$$

and ζ satisfies the similar estimate (3).

We can now conclude the proof that $L(1,\chi) \neq 0$ for χ a non-trivial complex Dirichlet character. If not, say $L(1,\chi) = 0$, then we also have $L(1,\overline{\chi}) = 0$. Since $\chi \neq \overline{\chi}$, there are at least two terms in the product

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

that vanish like $|s-1|$ as $s \to 1^+$. Since only the trivial character contributes a term that grows, and this growth is no worse than $O(1/|s-1|)$, we find that the product goes to 0 as $s \to 1^+$, contradicting the fact that it is ≥ 1 by Lemma 3.8.

Case II: real Dirichlet characters

The proof that $L(1,\chi) \neq 0$ when χ is a non-trivial real Dirichlet character is very different from the earlier complex case. The method we shall exploit involves summation along hyperbolas. It is a curious fact that this method was introduced by Dirichlet himself, twelve years after the proof of his theorem on arithmetic progressions, to establish another famous result of his: the average order of the divisor function. However, he made no connection between the proofs of these two theorems. We will instead proceed by proving first Dirichlet's divisor theorem, as a simple example of the method of summation along hyperbolas. Then, we shall adapt these ideas to prove the fact that $L(1,\chi) \neq 0$. As a preliminary matter, we need to deal with some simple sums, and their corresponding integral analogues.

Sums vs. Integrals

Here we use the idea of comparing a sum with its corresponding integral, which already occurred in the estimate (3) for the zeta function.

Proposition 3.10 *If N is a positive integer, then:*

(i) $$\sum_{1\le n\le N}\frac{1}{n}=\int_1^N\frac{dx}{x}+O(1)=\log N+O(1).$$

(ii) *More precisely, there exists a real number γ, called Euler's constant, so that*

$$\sum_{1\le n\le N}\frac{1}{n}=\log N+\gamma+O(1/N).$$

Proof. It suffices to establish the more refined estimate given in part (ii). Let

$$\gamma_n=\frac{1}{n}-\int_n^{n+1}\frac{dx}{x}.$$

Since $1/x$ is decreasing, we clearly have

$$0\le\gamma_n\le\frac{1}{n}-\frac{1}{n+1}\le\frac{1}{n^2},$$

so the series $\sum_{n=1}^{\infty}\gamma_n$ converges to a limit which we denote by γ. Moreover, if we estimate $\sum f(n)$ by $\int f(x)\,dx$, where $f(x)=1/x^2$, we find

$$\sum_{n=N+1}^{\infty}\gamma_n\le\sum_{n=N+1}^{\infty}\frac{1}{n^2}\le\int_N^{\infty}\frac{dx}{x^2}=O(1/N).$$

Therefore

$$\sum_{n=1}^{N}\frac{1}{n}-\int_1^N\frac{dx}{x}=\gamma-\sum_{n=N+1}^{\infty}\gamma_n+\int_N^{N+1}\frac{dx}{x},$$

and this last integral is $O(1/N)$ as $N\to\infty$.

Proposition 3.11 *If N is a positive integer, then*

$$\begin{aligned}\sum_{1\le n\le N}\frac{1}{n^{1/2}}&=\int_1^N\frac{dx}{x^{1/2}}+c'+O(1/N^{1/2})\\&=2N^{1/2}+c+O(1/N^{1/2}).\end{aligned}$$

The proof is essentially a repetition of the proof of the previous proposition, this time using the fact that

$$\left|\frac{1}{n^{1/2}}-\frac{1}{(n+1)^{1/2}}\right|\le\frac{C}{n^{3/2}}.$$

This last inequality follows from the mean-value theorem applied to $f(x)=x^{-1/2}$, between $x=n$ and $x=n+1$.

Hyperbolic sums

If F is a function defined on pairs of positive integers, there are three ways to calculate

$$S_N=\sum\sum F(m,n),$$

where the sum is taken over all pairs of positive integers (m,n) which satisfy $mn\le N$.

We may carry out the summation in any one of the following three ways. (See Figure 2.)

(a) Along hyperbolas:

$$S_N=\sum_{1\le k\le N}\left(\sum_{nm=k}F(m,n)\right)$$

(b) Vertically:

$$S_N=\sum_{1\le m\le N}\left(\sum_{1\le n\le N/m}F(m,n)\right)$$

(c) Horizontally:

$$S_N=\sum_{1\le n\le N}\left(\sum_{1\le m\le N/n}F(m,n)\right)$$

It is a remarkable fact that one can obtain interesting conclusions from the obvious fact that these three methods of summation give the same sum. We apply this idea first in the study of the divisor problem.

Intermezzo: the divisor problem

For a positive integer k, let $d(k)$ denote the number of positive divisors of k. For example,

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$d(k)$	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4	5	2

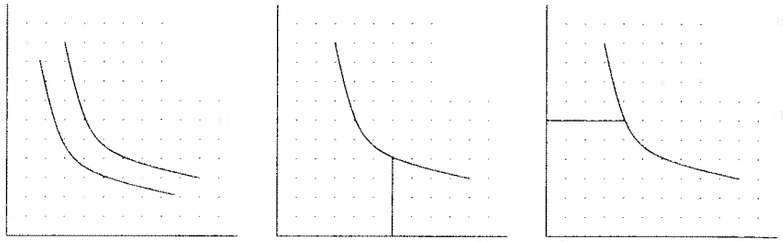

Figure 2. The three methods of summation

One observes that the behavior of $d(k)$ as k tends to infinity is rather irregular, and in fact, it does not seem possible to approximate $d(k)$ by a simple analytic expression in k. However, it is natural to inquire about the average size of $d(k)$. In other words, one might ask, what is the behavior of

$$\frac{1}{N}\sum_{k=1}^{N} d(k) \quad \text{as } N \to \infty?$$

The answer was provided by Dirichlet, who made use of hyperbolic sums. Indeed, we observe that

$$d(k) = \sum_{nm=k,\ 1\le n,m} 1.$$

Theorem 3.12 *If k is a positive integer, then*

$$\frac{1}{N}\sum_{k=1}^{N} d(k) = \log N + O(1).$$

More precisely,

$$\frac{1}{N}\sum_{k=1}^{N} d(k) = \log N + (2\gamma - 1) + O(1/N^{1/2}),$$

where γ is Euler's constant.

Proof. Let $S_N = \sum_{k=1}^{N} d(k)$. We observed that summing $F = 1$ along hyperbolas gives S_N. Summing vertically, we find

$$S_N = \sum_{1\le m\le N}\ \sum_{1\le n\le N/m} 1.$$

But $\sum_{1\le n\le N/m} 1 = [N/m] = N/m + O(1)$, where $[x]$ denote the greatest integer $\le x$. Therefore

$$S_N = \sum_{1\le m\le N} (N/m + O(1)) = N\left(\sum_{1\le m\le N} 1/m\right) + O(N).$$

Hence, by part (i) of Proposition 3.10,

$$\frac{S_N}{N} = \log N + O(1)$$

which gives the first conclusion.

For the more refined estimate we proceed as follows. Consider the three regions I, II, and III shown in Figure 3. These are defined by

$$I = \{1 \le m < N^{1/2},\ N^{1/2} < n \le N/m\},$$
$$II = \{1 \le m \le N^{1/2},\ 1 \le n \le N^{1/2}\},$$
$$III = \{N^{1/2} < m \le N/n,\ 1 \le n < N^{1/2}\}.$$

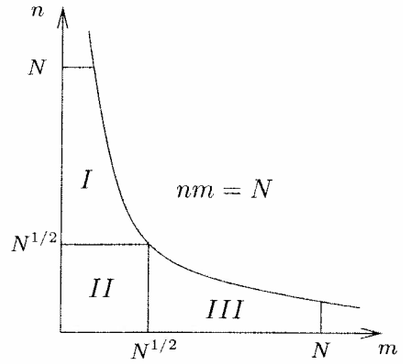

Figure 3. The three regions I, II, and III

If S_I, S_{II}, and S_{III} denote the sums taken over the regions I, II, and III, respectively, then

$$\begin{aligned} S_N &= S_I + S_{II} + S_{III} \\ &= 2(S_I + S_{II}) - S_{II}, \end{aligned}$$

since by symmetry $S_I = S_{III}$. Now we sum vertically, and use (ii) of Proposition 3.10 to obtain

$$\begin{aligned} S_I + S_{II} &= \sum_{1\le m\le N^{1/2}} \left(\sum_{1\le n\le N/m} 1 \right) \\ &= \sum_{1\le m\le N^{1/2}} [N/m] \\ &= \sum_{1\le m\le N^{1/2}} (N/m + O(1)) \\ &= N\left(\sum_{1\le m\le N^{1/2}} 1/m \right) + O(N^{1/2}) \\ &= N\log N^{1/2} + N\gamma + O(N^{1/2}). \end{aligned}$$

Finally, S_{II} corresponds to a square so

$$S_{II} = \sum_{1\le m\le N^{1/2}} \sum_{1\le n\le N^{1/2}} 1 = [N^{1/2}]^2 = N + O(N^{1/2}).$$

Putting these estimates together and dividing by N yields the more refined statement in the theorem.

Non-vanishing of the L-function

Our essential application of summation along hyperbolas is to the main point of this section, namely that $L(1,\chi) \neq 0$ for a non-trivial real Dirichlet character χ.

Given such a character, let

$$F(m,n) = \frac{\chi(n)}{(nm)^{1/2}},$$

and define

$$S_N = \sum\sum F(m,n),$$

where the sum is over all integers $m, n \geq 1$ that satisfy $mn \leq N$.

Proposition 3.13 *The following statements are true:*

(i) $S_N \geq c\log N$ *for some constant* $c > 0$.

(ii) $S_N = 2N^{1/2}L(1,\chi) + O(1)$.

It suffices to prove the proposition, since the assumption $L(1,\chi) = 0$ would give an immediate contradiction.

We first sum along hyperbolas. Observe that

$$\sum_{nm=k} \frac{\chi(n)}{(nm)^{1/2}} = \frac{1}{k^{1/2}} \sum_{n|k} \chi(n).$$

For conclusion (i) it will be enough to show the following lemma.

Lemma 3.14 $\sum_{n|k} \chi(n) \geq \begin{cases} 0 & \text{for all } k \\ 1 & \text{if } k = \ell^2 \text{ for some } \ell \in \mathbb{Z}. \end{cases}$

From the lemma, we then get

$$S_N \geq \sum_{k=\ell^2,\ \ell\le N^{1/2}} \frac{1}{k^{1/2}} \geq c\log N,$$

where the last inequality follows from (i) in Proposition 3.10.

The proof of the lemma is simple. If k is a power of a prime, say $k = p^a$, then the divisors of k are $1, p, p^2, \dots, p^a$ and

$$\begin{aligned} \sum_{n|k} \chi(n) &= \chi(1) + \chi(p) + \chi(p^2) + \cdots + \chi(p^a) \\ &= 1 + \chi(p) + \chi(p)^2 + \cdots + \chi(p)^a. \end{aligned}$$

So this sum is equal to

$$\begin{cases} a+1 & \text{if } \chi(p) = 1, \\ 1 & \text{if } \chi(p) = -1 \text{ and } a \text{ is even}, \\ 0 & \text{if } \chi(p) = -1 \text{ and } a \text{ is odd}, \\ 1 & \text{if } \chi(p) = 0, \text{ that is } p|q. \end{cases}$$

In general, if $k = p_1^{a_1}\cdots p_N^{a_N}$, then any divisor of k is of the form $p_1^{b_1}\cdots p_N^{b_N}$ where $0 \leq b_j \leq a_j$ for all j. Therefore, the multiplicative property of χ gives

$$\sum_{n|k} \chi(n) = \prod_{j=1}^{N} \left(\chi(1) + \chi(p_j) + \chi(p_j^2) + \cdots + \chi(p_j^{a_j}) \right),$$

and the proof is complete.

To prove the second statement in the proposition, we write

$$S_N = S_I + (S_{II} + S_{III}),$$

where the sums S_I, S_{II}, and S_{III} were defined earlier (see also Figure 3). We evaluate S_I by summing vertically, and $S_{II} + S_{III}$ by summing horizontally. In order to carry this out we need the following simple results.

Lemma 3.15 *For all integers $0 < a < b$ we have*

$$\text{(i)} \quad \sum_{n=a}^{b} \frac{\chi(n)}{n^{1/2}} = O(a^{-1/2}),$$

$$\text{(ii)} \quad \sum_{n=a}^{b} \frac{\chi(n)}{n} = O(a^{-1}).$$

Proof. This argument is similar to the proof of Proposition 3.4; we use summation by parts. Let $s_n = \sum_{1 \le k \le n} \chi(k)$, and remember that $|s_n| \le q$ for all n. Then

$$\begin{aligned} \sum_{n=a}^{b} \frac{\chi(n)}{n^{1/2}} &= \sum_{n=a}^{b-1} s_n \left[n^{-1/2} - (n+1)^{-1/2} \right] + O(a^{-1/2}) \\ &= O\left(\sum_{n=a}^{\infty} n^{-3/2} \right) + O(a^{-1/2}). \end{aligned}$$

By comparing the sum $\sum_{n=a}^{\infty} n^{-3/2}$ with the integral of $f(x) = x^{-3/2}$, we find that the former is also $O(a^{-1/2})$.

A similar argument establishes (ii).

We may now finish the proof of the proposition. Summing vertically we find

$$S_I = \sum_{m < N^{1/2}} \frac{1}{m^{1/2}} \left(\sum_{N^{1/2} < n \le N/m} \chi(n)/n^{1/2} \right).$$

The lemma together with Proposition 3.11 shows that $S_I = O(1)$. Finally

we sum horizontally to get

$$\begin{aligned} S_{II} + S_{III} &= \sum_{1 \le n \le N^{1/2}} \frac{\chi(n)}{n^{1/2}} \left(\sum_{m \le N/n} 1/m^{1/2} \right) \\ &= \sum_{1 \le n \le N^{1/2}} \frac{\chi(n)}{n^{1/2}} \left\{ 2(N/n)^{1/2} + c + O((n/N)^{1/2}) \right\} \\ &= 2N^{1/2} \sum_{1 \le n \le N^{1/2}} \frac{\chi(n)}{n} + c \sum_{1 \le n \le N^{1/2}} \frac{\chi(n)}{n^{1/2}} \\ &\qquad + O\left(\frac{1}{N^{1/2}} \sum_{1 \le n \le N^{1/2}} 1 \right) \\ &= A + B + C. \end{aligned}$$

Now observe that the lemma, together with the definition of $L(s, \chi)$, implies

$$A = 2N^{1/2} L(1, \chi) + O(N^{1/2} N^{-1/2}).$$

Moreover, part (i) of the lemma gives $B = O(1)$, and we also clearly have $C = O(1)$. Thus $S_N = 2N^{1/2} L(1, \chi) + O(1)$, which is part (ii) in Proposition 3.13.

This completes the proof that $L(1, \chi) \neq 0$, and thus the proof of Dirichlet's theorem.

4 Exercises

1. Prove that there are infinitely many primes by observing that if there were only finitely many, $p_1, \ldots, p_N$, then

$$\prod_{j=1}^{N} \frac{1}{1 - 1/p_j} \ge \sum_{n=1}^{\infty} \frac{1}{n}.$$

2. In the text we showed that there are infinitely many primes of the form $4k + 3$ by a modification of Euclid's original argument. Adapt this technique to prove the similar result for primes of the form $3k + 2$, and for those of the form $6k + 5$.

3. Prove that if p and q are relatively prime, then $\mathbb{Z}^*(p) \times \mathbb{Z}^*(q)$ is isomorphic to $\mathbb{Z}^*(pq)$.

4. Let $\varphi(n)$ denote the number of positive integers $\leq n$ that are relatively prime to n. Use the previous exercise to show that if n and m are relatively prime, then

$$\varphi(nm) = \varphi(n)\varphi(m).$$

One can give a formula for the Euler phi-function as follows:

(a) Calculate $\varphi(p)$ when p is prime by counting the number of elements in $\mathbb{Z}^*(p)$.

(b) Give a formula for $\varphi(p^k)$ when p is prime and $k \geq 1$ by counting the number of elements in $\mathbb{Z}^*(p^k)$.

(c) Show that

$$\varphi(n) = n \prod_i \left(1 - \frac{1}{p_i}\right),$$

where p_i are the primes that divide n.

5. If n is a positive integer, show that

$$n = \sum_{d|n} \varphi(d),$$

where φ is the Euler phi-function.

[Hint: There are precisely $\varphi(n/d)$ integers $1 \leq m \leq n$ with $\gcd(m,n) = d$.]

6. Write down the characters of the groups $\mathbb{Z}^*(3)$, $\mathbb{Z}^*(4)$, $\mathbb{Z}^*(5)$, $\mathbb{Z}^*(6)$, and $\mathbb{Z}^*(8)$.

(a) Which ones are real, or complex?

(b) Which ones are even, or odd? (A character is even if $\chi(-1) = 1$, and odd otherwise).

7. Recall that for $|z| < 1$,

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

We have seen that

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

(a) Show that if $w = 1/(1-z)$, then $|z| < 1$ if and only if $\mathrm{Re}(w) > 1/2$.

(b) Show that if $\mathrm{Re}(w) > 1/2$ and $w = \rho e^{i\varphi}$ with $\rho > 0$, $|\varphi| < \pi$, then

$$\log_1 w = \log \rho + i\varphi.$$

[Hint: If $e^\zeta = w$, then the real part of ζ is uniquely determined and its imaginary part is determined modulo 2π.]

8. Let ζ denote the zeta function defined for $s > 1$.

(a) Compare $\zeta(s)$ with $\int_1^\infty x^{-s}\,dx$ to show that

$$\zeta(s) = \frac{1}{s-1} + O(1) \quad \text{as } s \to 1^+.$$

(b) Prove as a consequence that

$$\sum_p \frac{1}{p^s} = \log\left(\frac{1}{s-1}\right) + O(1) \quad \text{as } s \to 1^+.$$

9. Let χ_0 denote the trivial Dirichlet character mod q, and $p_1, \ldots, p_k$ the distinct prime divisors of q. Recall that $L(s,\chi_0) = (1 - p_1^{-s}) \cdots (1 - p_k^{-s})\zeta(s)$, and show as a consequence

$$L(s,\chi_0) = \frac{\varphi(q)}{q}\frac{1}{s-1} + O(1) \quad \text{as } s \to 1^+.$$

[Hint: Use the asymptotics for ζ in Exercise 8.]

10. Show that if ℓ is relatively prime to q, then

$$\sum_{p\equiv\ell} \frac{1}{p^s} = \frac{1}{\varphi(q)} \log\left(\frac{1}{s-1}\right) + O(1) \quad \text{as } s \to 1^+.$$

This is a quantitative version of Dirichlet's theorem.

[Hint: Recall (4).]

11. Use the characters for $\mathbb{Z}^*(3)$, $\mathbb{Z}^*(4)$, $\mathbb{Z}^*(5)$, and $\mathbb{Z}^*(6)$ to verify directly that $L(1,\chi) \neq 0$ for all non-trivial Dirichlet characters modulo q when $q = 3, 4, 5,$ and 6.

[Hint: Consider in each case the appropriate alternating series.]

12. Suppose χ is real and non-trivial; assuming the theorem that $L(1,\chi) \neq 0$, show directly that $L(1,\chi) > 0$.

[Hint: Use the product formula for $L(s,\chi)$.]

13. Let $\{a_n\}_{n=-\infty}^{\infty}$ be a sequence of complex numbers such that $a_n = a_m$ if $n = m \bmod q$. Show that the series

$$\sum_{n=1}^{\infty} \frac{a_n}{n}$$

converges if and only if $\sum_{n=1}^{q} a_n = 0$.

[Hint: Sum by parts.]

14. The series

$$F(\theta) = \sum_{|n|\neq 0} \frac{e^{in\theta}}{n}, \qquad \text{for } |\theta| < \pi,$$

converges for every θ and is the Fourier series of the function defined on $[-\pi,\pi]$ by $F(0) = 0$ and

$$F(\theta) = \begin{cases} i(-\pi-\theta) & \text{if } -\pi \leq \theta < 0 \\ i(\pi-\theta) & \text{if } 0 < \theta \leq \pi, \end{cases}$$

and extended by periodicity (period 2π) to all of $\mathbb{R}$ (see Exercise 8 in Chapter 2).

Show also that if $\theta \neq 0 \bmod 2\pi$, then the series

$$E(\theta) = \sum_{n=1}^{\infty} \frac{e^{in\theta}}{n}$$

converges, and that

$$E(\theta) = \frac{1}{2}\log\left(\frac{1}{2-2\cos\theta}\right) + \frac{i}{2}F(\theta).$$

15. To sum the series $\sum_{n=1}^{\infty} a_n/n$, with $a_n = a_m$ if $n = m \bmod q$ and $\sum_{n=1}^{q} a_n = 0$, proceed as follows.

(a) Define

$$A(m) = \sum_{n=1}^{q} a_n \zeta^{-mn} \qquad \text{where } \zeta = e^{2\pi i/q}.$$

Note that $A(q) = 0$. With the notation of the previous exercise, prove that

$$\sum_{n=1}^{\infty} \frac{a_n}{n} = \frac{1}{q}\sum_{m=1}^{q-1} A(m)E(2\pi m/q).$$

[Hint: Use Fourier inversion on $\mathbb{Z}(q)$.]

(b) If $\{a_m\}$ is odd, $(a_{-m} = -a_m)$ for $m \in \mathbb{Z}$, observe that $a_0 = a_q = 0$ and show that

$$A(m) = \sum_{1\leq n<q/2} a_n(\zeta^{-mn} - \zeta^{mn}).$$

(c) Still assuming that $\{a_m\}$ is odd, show that

$$\sum_{n=1}^{\infty} \frac{a_n}{n} = \frac{1}{2q}\sum_{m=1}^{q-1} A(m)F(2\pi m/q).$$

[Hint: Define $\tilde{A}(m) = \sum_{n=1}^{q} a_n\zeta^{mn}$ and apply the Fourier inversion formula.]

16. Use the previous exercises to show that

$$\frac{\pi}{3\sqrt{3}} = 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \frac{1}{7} - \frac{1}{8} + \cdots,$$

which is $L(1,\chi)$ for the non-trivial (odd) Dirichlet character modulo 3.

5 Problems

1.* Here are other series that can be summed by the methods in Exercise 15.

(a) For the non-trivial Dirichlet character modulo 6, $L(1,\chi)$ equals

$$\frac{\pi}{2\sqrt{3}} = 1 - \frac{1}{5} + \frac{1}{7} - \frac{1}{11} + \frac{1}{13} + \cdots.$$

(b) If χ is the odd Dirichlet character modulo 8, then $L(1,\chi)$ equals

$$\frac{\pi}{2\sqrt{2}} = 1 + \frac{1}{3} - \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \frac{1}{11}\cdots.$$

(c) For an odd Dirichlet character modulo 7, $L(1,\chi)$ equals

$$\frac{\pi}{\sqrt{7}} = 1 + \frac{1}{2} - \frac{1}{3} + \frac{1}{4} - \frac{1}{5} - \frac{1}{6}\cdots.$$

(d) For an even Dirichlet character modulo 8, $L(1,\chi)$ equals

$$\frac{\log(1+\sqrt{2})}{\sqrt{2}} = 1 - \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} \cdots .$$

(e) For an even Dirichlet character modulo 5, $L(1,\chi)$ equals

$$\frac{2}{\sqrt{5}} \log\left(\frac{1+\sqrt{5}}{2}\right) = 1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{4} + \frac{1}{6} - \frac{1}{7} - \frac{1}{8} + \frac{1}{9} + \frac{1}{11} \cdots .$$

2. Let $d(k)$ denote the number of positive divisors of k.

(a) Show that if $k = p_1^{a_1} \cdots p_n^{a_n}$ is the prime factorization of k, then

$$d(k) = (a_1 + 1) \cdots (a_n + 1).$$

Although Theorem 3.12 shows that on "average" $d(k)$ is of the order of $\log k$, prove the following on the basis of (a):

(b) $d(k) = 2$ for infinitely many k.

(c) For any positive integer N, there is a constant $c > 0$ so that $d(k) \geq c(\log k)^N$ for infinitely many k. [Hint: Let $p_1, \ldots, p_N$ be N distinct primes, and consider k of the form $(p_1 p_2 \cdots p_N)^m$ for $m = 1, 2, \ldots$.]

3. Show that if p is relatively prime to q, then

$$\prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right) = \left(\frac{1}{1 - p^{fs}}\right)^g,$$

where $g = \varphi(q)/f$, and f is the order of p in $\mathbb{Z}^*(q)$ (that is, the smallest n for which $p^n \equiv 1 \mod q$). Here the product is taken over all Dirichlet characters modulo q.

4. Prove as a consequence of the previous problem that

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

where $a_n \geq 0$, and the product is over all Dirichlet characters modulo q.

Appendix : Integration

This appendix is meant as a quick review of the definition and main properties of the Riemann integral on $\mathbb{R}$, and integration of appropriate continuous functions on $\mathbb{R}^d$. Our exposition is brief since we assume that the reader already has some familiarity with this material.

We begin with the theory of Riemann integration on a closed and bounded interval on the real line. Besides the standard results about the integral, we also discuss the notion of sets of measure 0, and give a necessary and sufficient condition on the set of discontinuities of a function that guarantee its integrability.

We also discuss multiple and repeated integrals. In particular, we extend the notion of integration to the entire space $\mathbb{R}^d$ by restricting ourselves to functions that decay fast enough at infinity.

1 Definition of the Riemann integral

Let f be a *bounded* real-valued function defined on the closed interval $[a,b] \subset \mathbb{R}$. By a **partition** P of $[a,b]$ we mean a finite sequence of numbers $x_0, x_1, \ldots, x_N$ with

$$a = x_0 < x_1 < \cdots < x_{N-1} < x_N = b.$$

Given such a partition, we let I_j denote the interval $[x_{j-1}, x_j]$ and write $|I_j|$ for its length, namely $|I_j| = x_j - x_{j-1}$. We define the upper and lower sums of f with respect to P by

$$\mathcal{U}(P,f) = \sum_{j=1}^{N} [\sup_{x \in I_j} f(x)]\,|I_j| \quad \text{and} \quad \mathcal{L}(P,f) = \sum_{j=1}^{N} [\inf_{x \in I_j} f(x)]\,|I_j|.$$

Note that the infimum and supremum exist because by assumption, f is bounded. Clearly $\mathcal{U}(P,f) \geq \mathcal{L}(P,f)$, and the function f is said to be **Riemann integrable**, or simply **integrable**, if for every $\epsilon > 0$ there exists a partition P such that

$$\mathcal{U}(P,f) - \mathcal{L}(P,f) < \epsilon.$$

To define the value of the integral of f, we need to make a simple yet important observation. A partition P' is said to be a **refinement** of the partition P if P' is obtained from P by adding points. Then, adding one