# Appendix C

# Number Theory

We review here the facts of number theory that we use and give references for their proofs.

## C.1 Multiplicative Functions and Euler Products

Analytic number theory frequently deals with functions $f$ defined for integers $n \geqslant 1$ such that $f(mn) = f(m)f(n)$ whenever $m$ and $n$ are coprime. Any such function that is not identically zero is called a *multiplicative* function.[1] A multiplicative function is uniquely determined by the values $f(p^k)$ for primes $p$ and integers $k \geqslant 1$ and satisfies $f(1) = 1$.

We recall that if $f$ and $g$ are functions defined for positive integers, the Dirichlet convolution $f \star g$ is defined by

$$(f \star g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Its key property is that the generating Dirichlet series

$$\sum_{n \geqslant 1} (f \star g)(n) n^{-s}$$

for $f \star g$ is the product of the generating Dirichlet series for $f$ and $g$ (see Proposition A.4.4). In particular, one deduces that the convolution is associative and commutative, and that the function $\delta$ such that $\delta(1) = 1$ and $\delta(n) = 0$ for all $n \geqslant 2$ is a neutral element. In other words, for any arithmetic functions $f$, $g$, and $h$, we have

$$f \star g = g \star f, \quad f \star (g \star h) = (f \star g) \star h, \quad f \star \delta = f.$$

[1] We emphasize that it is not required that $f(mn) = f(m)f(n)$ for *all* pairs of positive integers.



https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

**Lemma C.1.1** *Let $f$ and $g$ be multiplicative functions. Then the Dirichlet convolution $f \star g$ of $f$ and $g$ is multiplicative. Moreover, the function $f \circledcirc g$ defined by*

$$(f \circledcirc g)(n) = \sum_{[a,b]=n} f(a)g(b)$$

*is also multiplicative.*

*Proof* Both statements follow simply from the fact that if $n$ and $m$ are coprime integers, then any divisor $d$ of $nm$ can be uniquely written $d = d'd''$, where $d'$ divides $n$ and $d''$ divides $m$. □

**Example C.1.2** To get an idea of the behavior of a multiplicative function, it is always useful to write down the values at powers of primes. In the situation of the lemma, the Dirichlet convolution satisfies

$$(f \star g)(p^k) = \sum_{j=0}^{k} f(p^j)g(p^{k-j}),$$

whereas

$$(f \circledcirc g)(p^k) = \sum_{j=0}^{k-1} (f(p^j)g(p^k) + f(p^k)g(p^j)) + f(p^k)g(p^k).$$

In particular, suppose that $f$ and $g$ are supported on squarefree integers, so that $f(p^k) = g(p^k) = 0$ for any prime if $k \geqslant 2$. Then $f \circledcirc g$ is also supported on squarefree integers (this is not necessarily the case for $f \star g$) and satisfies

$$(f \circledcirc g)(p) = f(p) + g(p) + f(p)g(p)$$

for all primes $p$.

A very important multiplicative function is the Möbius function.

**Definition C.1.3** The Möbius function $\mu(n)$ is the multiplicative function supported on squarefree integers such that $\mu(p) = -1$ for all primes $p$.

In other words, if we factor

$$n = p_1 \cdots p_j,$$

where each $p_i$ is prime, then we have $\mu(n) = 0$ if there exists $i \neq j$ such that $p_i = p_j$, and otherwise $\mu(n) = (-1)^j$.

A key property of multiplicative functions is their *Euler product* expansion, as a product over primes.

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

**Lemma C.1.4** *Let $f$ be a multiplicative function such that*

$$\sum_{n\geqslant 1} |f(n)| < +\infty.$$

*Then we have*

$$\sum_{n\geqslant 1} f(n) = \prod_p \Big( \sum_{j\geqslant 0} f(p^j) \Big),$$

*where the product on the right is absolutely convergent. In particular, for all $s \in \mathbf{C}$ such that*

$$\sum_{n\geqslant 1} \frac{f(n)}{n^s}$$

*converges absolutely, we have*

$$\sum_{n\geqslant 1} \frac{f(n)}{n^s} = \prod_p (1 + f(p)p^{-s} + \cdots + f(p^k)p^{-ks} + \cdots),$$

*where the right-hand side converges absolutely.*

*Proof* For any prime $p$, the series

$$1 + f(p) + \cdots + f(p^k) + \cdots$$

is a subseries of $\sum f(n)$, so that the absolute convergence of the latter (which holds by assumption) implies that all of these partial series are also absolutely convergent.

We now first assume that $f(n) \geqslant 0$ for all $n$. Then, for any $\mathrm{N} \geqslant 1$, we have

$$\prod_{p\leqslant \mathrm{N}} \sum_{k\geqslant 0} f(p^k) = \sum_{\substack{n\geqslant 1 \\ p|n \Rightarrow p\leqslant \mathrm{N}}} f(n)$$

by expanding the product and using the absolute convergence and the uniqueness of factorization of integers. It follows that

$$\Big| \prod_{p\leqslant \mathrm{N}} \sum_{k\geqslant 0} f(p^k) - \sum_{n\leqslant \mathrm{N}} f(n) \Big| \leqslant \sum_{n>\mathrm{N}} f(n)$$

(since we assume $f(n) \geqslant 0$). This converges to 0 as $\mathrm{N} \to +\infty$, because the series $\sum f(n)$ is absolutely convergent. Thus this case is done.

In the general case, replacing $f$ by $|f|$, the previous argument shows that the product converges absolutely. Then we get in the same manner

$$\Big| \prod_{p\leqslant \mathrm{N}} \sum_{k\geqslant 0} f(p^k) - \sum_{n\leqslant \mathrm{N}} f(n) \Big| \leqslant \sum_{n>\mathrm{N}} |f(n)| \longrightarrow 0$$

as $\mathrm{N} \to +\infty$. □

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

**Corollary C.1.5** *For any $s \in \mathbf{C}$ such that $\mathrm{Re}(s) > 1$, we have*

$$\sum_{n \geqslant 1} n^{-s} = \prod_p \frac{1}{1 - p^{-s}}, \tag{C.1}$$

$$\sum_{n \geqslant 1} \mu(n) n^{-s} = \prod_p (1 - p^{-s}) = \frac{1}{\zeta(s)}. \tag{C.2}$$

**Example C.1.6** The fact that the Dirichlet series for the Möbius function is the inverse of the Riemann zeta function, combined with the link between multiplication and Dirichlet convolution, leads to the so-called *Möbius inversion formula*: for arithmetic functions $f$ and $g$, the relations

$$g(n) = \sum_{d|n} f(d) \quad \text{and} \quad f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$$

(for all $n \geqslant 1$) are equivalent. (Indeed, the first means that $g = f \star 1$, where 1 is the constant function, and the second that $f = g \star \mu$; since $\mu \star 1 = \delta$, which is the multiplicative function version of the identity $\zeta(s)^{-1} \cdot \zeta(s) = 1$, the equivalence of the two follows from the associativity of the convolution.)

**Example C.1.7** Let $f$ and $g$ be multiplicative functions supported on squarefree integers defining absolutely convergent series. Then for $\sigma > 0$, we have

$$\sum_{n \geqslant 1} \frac{f(m)g(n)}{[m,n]^\sigma} = \sum_{d \geqslant 1} \frac{(f \circledcirc g)(d)}{d^\sigma} = \prod_p \left(1 + (f(p) + g(p) + f(p)g(p)) p^{-\sigma}\right).$$

For instance, consider the case where $f$ and $g$ are both the Möbius function $\mu$. Then $\mu \circledcirc \mu$ is supported on squarefree numbers and takes value $-1-1+1 = -1$ at primes and so is in fact equal to $\mu$. We obtain the nice formula

$$\sum_{n \geqslant 1} \frac{\mu(m)\mu(n)}{[m,n]^s} = \sum_{d \geqslant 1} \frac{(f \circledcirc g)(d)}{d^s} = \prod_p \left(1 - \frac{1}{p^s}\right) = \sum_{n \geqslant 1} \mu(n) n^{-s} = \frac{1}{\zeta(s)}$$

for $\mathrm{Re}(s) > 1$.

**Example C.1.8** Another very important multiplicative arithmetic function is the Euler function $\varphi$ defined by $\varphi(q) = |(\mathbf{Z}/q\mathbf{Z})^\times|$ for $q \geqslant 1$. This function is multiplicative, by the Chinese Remainder Theorem, which implies that there exists an isomorphism of groups

$$(\mathbf{Z}/q_1 q_2 \mathbf{Z})^\times \simeq (\mathbf{Z}/q_1\mathbf{Z})^\times \times (\mathbf{Z}/q_2\mathbf{Z})^\times$$

when $q_1$ and $q_2$ are coprime integers. We have $\varphi(p) = p - 1$ if $p$ is prime, and more generally $\varphi(p^k) = p^k - p^{k-1}$ for $p$ prime and $k \geqslant 1$ (since an element $x$ of $\mathbf{Z}/p^k\mathbf{Z}$ is invertible if and only if its unique lift in $\{0, \ldots, p^k - 1\}$ is not divisible by $p$). Hence, by factorization, we obtain the product expansion

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

$$\varphi(n) = \prod_{p|n} (p^{v_p(n)} - p^{v_p(n)-1}) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where $v_p(n)$ is the power $p$-adic valuation of $n$, that is, the exponent of the power of $p$ dividing exactly $n$.

We deduce from Lemma C.1.4 the expression

$$\begin{aligned}\sum_{n\geqslant 1} \varphi(n) n^{-s} &= \prod_p \big(1 + (p-1)p^{-s} + (p^2 - p)p^{-2s} + \cdots + \\ &\qquad (p^k - p^{k-1})p^{-ks} + \cdots\big) \\ &= \frac{\zeta(s-1)}{\zeta(s)},\end{aligned}$$

again valid for $\mathrm{Re}(s) > 1$. This may also be deduced from the formula

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

that is, $\varphi = \mu \star \mathrm{Id}$, where Id is the identity arithmetic function.

## C.2 Additive Functions

We also often encounter *additive functions* (although they are not so important in this book), which are complex-valued functions $g$ defined for integers $n \geqslant 1$ such that $g(nm) = g(n) + g(m)$ for all pairs of coprime integers $n$ and $m$. In particular, we have then $g(1) = 0$.

If $g$ is an additive function, then we can write

$$g(n) = \sum_p g\left(p^{v_p(n)}\right)$$

for any $n \geqslant 1$, where $v_p$ is the $p$-adic valuation (which is zero for all but finitely many $p$). As for multiplicative functions, an additive function is therefore determined uniquely by its values at prime powers.

Some standard examples are given by $g(n) = \log n$, or more generally $g(n) = \log f(n)$, where $f$ is a multiplicative function that is always positive. The arithmetic function $\omega(n)$ that counts the number of prime factors of an integer $n \geqslant 1$ (without multiplicity) is also additive; it is of course the subject of the Erdős–Kac Theorem.

Conversely, if $g$ is an additive function, then for any complex number $s \in \mathbf{C}$, the function $n \mapsto e^{sg(n)}$ is a multiplicative function.

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

## C.3 Primes and Their Distribution

For any real number $x \geqslant 1$, we denote by $\pi(x)$ the prime counting function, that is, the number of prime numbers $p \leqslant x$. This is of course one of the key functions of interest in multiplicative number theory. Except in the most elementary cases, interesting statements require some information on the size of $\pi(x)$.

The first nontrivial quantitative bounds are due to Chebychev, giving the correct order of magnitude of $\pi(x)$, and were elaborated by Mertens to obtain other very useful estimates for quantities involving primes.

**Proposition C.3.1 (Chebychev and Mertens estimates)** (1) *There exist positive constants $c_1$ and $c_2$ such that*

$$c_1 \frac{x}{\log x} \leqslant \pi(x) \leqslant c_2 \frac{x}{\log x}$$

*for all $x \geqslant 2$.*

(2) *For any $x \geqslant 3$, we have*

$$\sum_{p \leqslant x} \frac{1}{p} = \log\log x + \mathrm{O}(1).$$

(3) *For any $x \geqslant 3$, we have*

$$\sum_{p \leqslant x} \frac{\log p}{p} = \log x + \mathrm{O}(1).$$

See, e.g, [59, §2.2] or [52, Th. 7, Th. 414] (resp. [59, (2.15)] or [52, Th. 427]; [59, (2.14)] or [52, Th. 425]) for a proof of the first (resp. second, third) estimate.

**Exercise C.3.2** (1) Show that the first estimate implies that the $n$th prime is of size about $n \log n$ (up to multiplicative constants) and also implies the bounds

$$\log\log x \ll \sum_{p \leqslant x} \frac{1}{p} \ll \log\log x$$

for $x \geqslant 3$.

(2) Let $\pi_2(x)$ be the numbers of integers $n \leqslant x$ such that $n$ is the product of at most two primes (possibly equal). Prove that there exist positive constants $c_3$ and $c_4$ such that

$$c_3 \frac{x \log\log x}{\log x} \leqslant \pi_2(x) \leqslant c_4 \frac{x \log\log x}{\log x}$$

for all $x \geqslant 3$.

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

The real key result in the study of primes is the Prime Number Theorem with a strong error term:

**Theorem C.3.3** *Let* $A > 0$ *be an arbitrary real number. For* $x \geqslant 2$*, we have*

$$\pi(x) = \mathrm{li}(x) + O\left(\frac{x}{(\log x)^A}\right), \tag{C.3}$$

*where* $\mathrm{li}(x)$ *is the logarithmic integral*

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t}$$

*and the implied constant depends only on* A*. More generally, for* $\alpha \geqslant 0$ *fixed, we have*

$$\sum_{p \leqslant x} p^\alpha = \int_2^x t^\alpha \frac{dt}{\log t} + O\left(\frac{x^{1+\alpha}}{(\log x)^A}\right),$$

*where the implied constant depends only on* A*.*

For a proof, see, for instance, [59, §2.4 or Cor. 5.29]. By an elementary integration by parts, we have

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right),$$

for $x \geqslant 2$, hence the "usual" simple asymptotic version of the Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}, \qquad \text{as } x \to +\infty.$$

However, note that if one expresses the main term in the "simple" form $x/\log x$, the error term cannot be better than $x/(\log x)^2$.

The Prime Number Theorem easily implies a stronger form of the Mertens formula:

**Corollary C.3.4** *There exists a constant* $C \in \mathbf{R}$ *such that*

$$\sum_{p \leqslant x} \frac{1}{p} = \log\log x + C + O((\log x)^{-1}). \tag{C.4}$$

**Exercise C.3.5** Show that (C.4) is in fact equivalent with the Prime Number Theorem in the form

$$\pi(x) \sim \frac{x}{\log x}$$

as $x \to +\infty$.

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

Another estimate that will be useful in Chapter 4 is the following:

**Proposition C.3.6** *Let* $A > 0$ *be a fixed real number. For all* $x \geqslant 2$*, we have*

$$\prod_{p \leqslant x} \left(1 + \frac{A}{p}\right) \ll (\log x)^A,$$
$$\prod_{p \leqslant x} \left(1 - \frac{A}{p}\right)^{-1} \ll (\log x)^A,$$

*where the implied constant depends only on* A.

*Proof* In both cases, if we compute the logarithm, we obtain

$$\sum_{p \leqslant x} \left(\frac{A}{p} + O\left(\frac{1}{p^2}\right)\right),$$

where the implied constant depends on A and the result follows from the Mertens formula. □

In Chapter 5, we will also need the generalization of these basic statements to primes in arithmetic progressions. We recall that for $x \geqslant 1$, and any modulus $q \geqslant 1$ and integer $a \in \mathbf{Z}$, we define

$$\pi(x; q, a) = \sum_{\substack{p \leqslant x \\ p \equiv a \pmod q}} 1,$$

the number of primes $p \leqslant x$ that are congruent to $a$ modulo $q$. If $a$ is not coprime to $q$, then $\pi(x; q, a)$ is bounded as $x$ varies; it was one of the first major achievements of analytic number theory when Dirichlet proved that, conversely, there are infinitely many primes $p \equiv a \pmod q$ if $(a, q) = 1$. This was done using the theory of Dirichlet characters and L-functions, which we will survey later (see Section C.5). Here we state the analogue of the Prime Number Theorem, which shows that, asymptotically, all residue classes modulo $q$ are roughly equivalent.

**Theorem C.3.7** *For any fixed* $q \geqslant 1$ *and* $A \geqslant 1$*, and for any* $x \geqslant 2$*, we have*

$$\pi(x; q, a) = \frac{1}{\varphi(q)} \frac{x}{\log x} + O\Big(\frac{x}{(\log x)^A}\Big)$$
$$\sim \frac{1}{\varphi(q)} \pi(x) \sim \frac{1}{\varphi(q)} \operatorname{li}(x).$$

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

## C.4 The Riemann Zeta Function

As recalled in Section 3.1, the Riemann zeta function is defined first for complex numbers $s$ such that $\mathrm{Re}(s) > 1$ by means of the absolutely convergent series

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

By Lemma C.1.4, it has also the Euler product expansion

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

in this region. Using this expression, we can compute the logarithmic derivative of the zeta function, always for $\mathrm{Re}(s) > 1$. We obtain the Dirichlet series expansion

$$-\frac{\zeta'}{\zeta}(s) = \sum_p \frac{(\log p) p^{-s}}{1 - p^{-s}} = \sum_{n \geqslant 1} \frac{\Lambda(n)}{n^s} \tag{C.5}$$

(using a geometric series expansion), where the function $\Lambda$ is called the *von Mangoldt function*, defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and some } k \geqslant 1, \\ 0 & \text{otherwise.} \end{cases} \tag{C.6}$$

In other words, up to the "thin" set of powers of primes with exponent $k \geqslant 2$, the function $\Lambda$ is the logarithm restricted to prime numbers.

Beyond the region of absolute convergence, it is known that the zeta function extends to a meromorphic function on all of $\mathbf{C}$, with a unique pole located at $s = 1$, which is a simple pole with residue 1 (see the argument in Section 3.1 for a simple proof of analytic continuation to $\mathrm{Re}(s) > 0$). More precisely, let

$$\xi(s) = \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s)$$

for $\mathrm{Re}(s) > 1$. Then $\xi$ extends to a meromorphic function on $\mathbf{C}$ with simple poles at $s = 0$ and $s = 1$, which satisfies the functional equation

$$\xi(1 - s) = \xi(s).$$

Because the Gamma function has poles at integers $-k$ for $k \geqslant 0$, it follows that $\zeta(-2k) = 0$ for $k \geqslant 1$ (the case $k = 0$ is special because of the pole at $s = 1$). The negative even integers are called the *trivial zeros* of $\zeta(s)$. Hadamard and de la Vallée Poussin proved (independently) that $\zeta(s) \neq 0$ for $\mathrm{Re}(s) = 1$, and it follows that the nontrivial zeros of $\zeta(s)$ are located in the *critical strip* $0 < \mathrm{Re}(s) < 1$.

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

**Proposition C.4.1** (1) *For* $1/2 < \sigma < 1$, *we have*

$$\frac{1}{2\mathrm{T}}\int_{-\mathrm{T}}^{\mathrm{T}} |\zeta(\sigma+it)|^2 dt \longrightarrow \zeta(2\sigma)$$

*as* $\mathrm{T} \to +\infty$.

(2) *We have*

$$\frac{1}{2\mathrm{T}}\int_{-\mathrm{T}}^{\mathrm{T}} |\zeta(\tfrac{1}{2}+it)|^2 dt \sim \mathrm{T}(\log \mathrm{T})$$

*for* $\mathrm{T} \to +\infty$.

See [117, Th. 7.2] for the proof of the first formula and [117, Th. 7.3] for the second (which is due to Hardy and Littlewood).

**Exercise C.4.2** This exercise explains the proof of the first formula (which is easier than the second one).

(1) Prove that for $\frac{1}{2} \leqslant \sigma \leqslant \sigma' < 1$ and for $\mathrm{T} \geqslant 2$, we have

$$\sum_{1 \leqslant m < n \leqslant \mathrm{T}} \frac{1}{(mn)^\sigma} \frac{1}{\log(n/m)} \ll \mathrm{T}^{2-2\sigma}(\log \mathrm{T}).$$

(Consider separately the sum where $m < \frac{1}{2}n$ and the remainder.)

(2) Prove that

$$\frac{1}{2\mathrm{T}}\int_{-\mathrm{T}}^{\mathrm{T}} \Big| \sum_{n \leqslant |t|} n^{-\sigma-it} \Big|^2 dt \to \zeta(2\sigma)$$

as $\mathrm{T} \to +\infty$. (Expand the square and integrate using (1).)

(3) Conclude using Proposition C.4.5 below.

For much more information concerning the analytic properties of the Riemann zeta function, see [117]. Note however that the deeper *arithmetic* aspects are best understood in the larger framework of L-functions, from Dirichlet L-functions (which are discussed below in Section C.5) to automorphic L-functions (see, e.g, [59, Ch. 5]).

We will also use the *Hadamard factorization* of the Riemann zeta function. This is an analogue of the factorization of polynomials in terms of their zeros, which holds for meromorphic functions on $\mathbf{C}$ with restricted growth.

**Proposition C.4.3** *The zeros* $\varrho$ *of* $\xi(s)$ *all satisfy* $0 < \mathrm{Re}(\varrho) < 1$, *and there exists constants* $\alpha$ *and* $\beta \in \mathbf{C}$ *such that*

$$s(s-1)\xi(s) = e^{\alpha+\beta s} \prod_{\varrho} \left(1 - \frac{s}{\varrho}\right) e^{-s/\varrho}$$

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

*for any $s \in \mathbf{C}$, where the product runs over the zeros of $\xi(s)$, counted with multiplicity, and converges uniformly on compact subsets of $\mathbf{C}$. In fact, we have*

$$\sum_{\varrho} \frac{1}{|\varrho|^2} < +\infty.$$

Given that $s \mapsto s(s-1)\xi(s)$ is an entire function of finite order, this follows from the general theory of such functions (see, e.g, [116, Th. 8.24] for Hadamard's factorization theorem). What is most important for us is the following corollary, which is an analogue of partial fraction expansion for the logarithmic derivative of a polynomial – except that it is most convenient here to truncate the infinite sum.

**Proposition C.4.4** *Let $s = \sigma + it \in \mathbf{C}$ be such that $\frac{1}{2} \leqslant \sigma \leqslant 1$ and $\zeta(s) \neq 0$. Then there are $\ll \log(2+|t|)$ zeros $\varrho$ of $\xi$ such that $|s-\varrho| \leqslant 1$, and we have*

$$-\frac{\zeta'(s)}{\zeta(s)} = \frac{1}{s} + \frac{1}{s-1} - \sum_{|s-\varrho|<1} \frac{1}{s-\varrho} + \mathrm{O}(\log(2+|t|)),$$

*where the sum is over zeros $\varrho$ of $\zeta(s)$ such that $|s-\varrho| < 1$, counted with multiplicity.*

*Sketch of proof* We first claim that the constant $\beta$ in Proposition C.4.3 satisfies

$$\mathrm{Re}(\beta) = -\sum_{\varrho} \mathrm{Re}(\varrho^{-1}), \tag{C.7}$$

where $\varrho$ runs over all the zeros of $\xi(s)$ with multiplicity. Indeed, applying the Hadamard product expansion to both sides of the functional equation $\xi(1-s) = \xi(s)$ and taking logarithms, we obtain

$$2\,\mathrm{Re}(\beta) = \beta + \bar{\beta} = -\sum_{\varrho} \left( \frac{1}{s-\varrho} + \frac{1}{1-s-\bar{\varrho}} + \frac{1}{\varrho} + \frac{1}{\bar{\varrho}} \right).$$

For any fixed $s$ that is not a zero of $\xi(s)$, we have $(s-\varrho)^{-1} - (1-s-\bar{\varrho})^{-1} \ll |\varrho|^{-2}$, where the implied constant depends on $s$. Similarly, $\varrho^{-1} + \bar{\varrho}^{-1} \ll |\varrho|^{-2}$, so the series

$$\sum_{\varrho} \left( \frac{1}{s-\varrho} + \frac{1}{1-s-\bar{\varrho}} \right) \quad \text{and} \quad \sum_{\varrho} \left( \frac{1}{\varrho} + \frac{1}{\bar{\varrho}} \right)$$

are absolutely convergent. So we can separate them; the first one vanishes, because the terms cancel out (both $\varrho$ and $1-\bar{\varrho}$ are zeros of $\zeta(s)$), and we obtain (C.7).

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

Now let $\mathrm{T} \geqslant 2$ and $s = 3 + i\mathrm{T}$. Using the expansion

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{k\geqslant 0} \sum_{p} (\log p) p^{-ks},$$

we get the trivial estimate

$$\left|\frac{\zeta'}{\zeta}(s)\right| \leqslant \zeta'(3).$$

By Stirling's formula (Proposition A.3.3), we have $\frac{\Gamma'}{\Gamma}(s/2) \ll \log(2+\mathrm{T})$, and for any zero $\varrho = \beta + i\gamma$ of $\xi(s)$, we have

$$\frac{2}{9+(\mathrm{T}-\gamma)^2} < \mathrm{Re}\left(\frac{1}{s-\varrho}\right) < \frac{3}{4+(\mathrm{T}-\gamma)^2}.$$

If we compute the real part of the formula

$$-\frac{\zeta'}{\zeta}(s) = \frac{\Gamma'}{\Gamma}(s/2) - \beta + \frac{1}{s} + \frac{1}{s-1} - \sum_{\varrho}\left(\frac{1}{s-\varrho} + \frac{1}{\varrho}\right)$$

and rearrange the resulting absolutely convergent series (using (C.7)), we get

$$\sum_{\varrho} \frac{1}{1+(\mathrm{T}-\gamma)^2} \ll \log(2+\mathrm{T}). \tag{C.8}$$

This convenient estimate implies, as claimed, that there are $\ll \log(2+\mathrm{T})$ zeros $\varrho$ such that $|\mathrm{Im}(\varrho - \mathrm{T})| \leqslant 1$.

Now, finally, let $s = \sigma + it$ such that $\frac{1}{2} \leqslant \sigma \leqslant 1$ and $\xi(s) \neq 0$. We have

$$-\frac{\zeta'}{\zeta}(s) = -\frac{\zeta'}{\zeta}(s) + \frac{\zeta'}{\zeta}(3+it) + \mathrm{O}(\log(2+|t|)),$$

by the previous elementary estimate. Hence (by the Stirling formula again) we have

$$-\frac{\zeta'}{\zeta}(s) = \frac{1}{s} + \frac{1}{s-1} - \sum_{\varrho}\left(\frac{1}{s-\varrho} - \frac{1}{3+it-\varrho}\right) + \mathrm{O}(\log(2+|t|)).$$

In the series, we keep the zeros with $|s-\varrho| < 1$, and we estimate the contribution of the others by

$$\sum_{|s-\varrho|>1}\left|\frac{1}{s-\varrho} - \frac{1}{3+it-\varrho}\right| \leqslant \sum_{|s-\varrho|>1} \frac{3}{1+(\mathrm{T}-\gamma)^2} \ll \log(2+|t|)$$

by (C.8). □

We will use an elementary approximation for $\zeta(s)$ in the strip $\frac{1}{2} < \mathrm{Re}(s) < 1$.

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

**Proposition C.4.5** *Let* $\mathrm{T} \geqslant 1$. *For* $\sigma > 1/2$, *and for any* $s = \sigma + it$ *with* $1/2 \leqslant \sigma < 3/4$ *and* $|t| \leqslant \mathrm{T}$, *we have*

$$\zeta(s) = \sum_{1 \leqslant n \leqslant \mathrm{T}} n^{-s} + \mathrm{O}\left(\frac{\mathrm{T}^{1-\sigma}}{|t|+1} + \mathrm{T}^{-1/2}\right).$$

*Proof* This follows from [117, Th. 4.11] (a result first proved by Hardy and Littlewood) which states that for any $\sigma_0 > 0$, we have

$$\zeta(s) = \sum_{1 \leqslant n \leqslant \mathrm{T}} n^{-s} - \frac{\mathrm{T}^{1-\sigma}}{1-s} + \mathrm{O}(\mathrm{T}^{-1/2})$$

for $\sigma \geqslant \sigma_0$, since $1/(1-s) \ll 1/(|t|+1)$ if $1/2 \leqslant \sigma < 3/4$. □

The last (and most subtle) result concerning the zeta function that we need is an important refinement of (2) in Proposition C.4.1.

**Proposition C.4.6** *Let* $\mathrm{T} \geqslant 1$ *be a real number, and let* $m$, $n$ *be integers such that* $1 \leqslant m, n \leqslant \mathrm{T}$. *Let* $\sigma$ *be a real number with* $\frac{1}{2} \leqslant \sigma \leqslant 1$. *We have*

$$\begin{aligned}\frac{1}{2\mathrm{T}}\int_{-\mathrm{T}}^{\mathrm{T}} \left(\frac{m}{n}\right)^{it} |\zeta(\sigma+it)|^2 dt &= \zeta(2\sigma)\left(\frac{(m,n)^2}{mn}\right)^{\sigma} \\ &\quad + \frac{1}{2\mathrm{T}}\zeta(2-2\sigma)\left(\frac{(m,n)^2}{mn}\right)^{1-\sigma}\int_{-\mathrm{T}}^{\mathrm{T}}\left(\frac{|t|}{2\pi}\right)^{1-2\sigma} dt \\ &\quad + \mathrm{O}(\min(m,n)\mathrm{T}^{-\sigma+\varepsilon}).\end{aligned}$$

This is essentially due to Selberg [110, Lemma 6], and a proof is given by Radziwiłł and Soundararajan [95, §6].

## C.5 Dirichlet L-Functions

Let $q \geqslant 1$ be an integer. The Dirichlet L-functions modulo $q$ are Dirichlet series attached to characters of the group of invertible residue classes modulo $q$. More precisely, for any such character $\chi : (\mathbf{Z}/q\mathbf{Z})^\times \to \mathbf{C}^\times$, we extend it to $\mathbf{Z}/q\mathbf{Z}$ by sending noninvertible classes to 0, and then we view it as a $q$-periodic function on $\mathbf{Z}$. The resulting function on $\mathbf{Z}$ is called a *Dirichlet character modulo* $q$. (See Example B.6.2 (3) for the definition and basic properties of characters of finite abelian groups; an excellent elementary account can also be found in Serre's book [112, §VI.1].)

We denote by $1_q$ the trivial character modulo $q$ (which is identically 1 on all invertible residue classes modulo $q$ and 0 elsewhere). A character $\chi$ such that $\chi(n) \in \{\pm 1\}$ for all $n$ coprime to $q$ is called a *real character*. This condition is equivalent to having $\chi$ real-valued, or to having $\chi^2 = 1_q$.

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

By the duality theorem for finite abelian groups (see Example B.6.2, (3)), the set of Dirichlet characters modulo $q$ is a group under pointwise multiplication with $1_q$ as the identity element, and it is isomorphic to $(\mathbf{Z}/q\mathbf{Z})^\times$; in particular, the number of Dirichlet characters modulo $q$ is $\varphi(q)$. Moreover, the Dirichlet characters modulo $q$ form an orthonormal basis of the space of complex-valued functions on $(\mathbf{Z}/q\mathbf{Z})^\times$.

Let $\chi$ be a Dirichlet character modulo $q$. By construction, the function $\chi$ is multiplicative on $\mathbf{Z}$, in the strong sense that $\chi(nm) = \chi(n)\chi(m)$ for all integers $n$ and $m$ (even if they are not coprime).

The orthonormality property of characters of a finite group implies the following fundamental relation:

**Proposition C.5.1** *Let $q \geqslant 1$ be an integer. For any $x$ and $y$ in $\mathbf{Z}$, we have*

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod q} \chi(x)\overline{\chi(y)} = \begin{cases} 1 & \text{if } x \equiv y \pmod q \text{ and } x, y \text{ are coprime with } q, \\ 0 & \text{otherwise,} \end{cases}$$

*where the sum is over all Dirichlet characters modulo $q$.*

*Proof* If $x$ or $y$ is not coprime with $q$, then the formula is valid because both sides are zero. Otherwise, this is a special case of the general decomposition formula

$$\frac{1}{|\mathrm{G}|} \sum_{\chi \in \widehat{\mathrm{G}}} \chi(x)\overline{\chi(y)} = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x \neq y \end{cases} \tag{C.9}$$

for any finite abelian group G and elements $x$ and $y$ of G. Indeed, if we view $y$ as fixed and $x$ as a variable, this is simply the decomposition of the characteristic function $f_y$ of the element $y \in \mathrm{G}$ in the orthonormal basis of characters: this decomposition is

$$f_y = \sum_{\chi \in \widehat{\mathrm{G}}} \langle f_y, \chi \rangle \chi,$$

which becomes

$$f_y = \sum_{\chi \in \widehat{\mathrm{G}}} \overline{\chi(y)}\chi,$$

from which in turn (C.9) follows by evaluating at $x$. □

Let $q \geqslant 1$ be an integer and $\chi$ a Dirichlet character modulo $q$. One defines

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

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

for all $s \in \mathbf{C}$ such that $\mathrm{Re}(s) > 1$; since $|\chi(n)| \leqslant 1$ for all $n \in \mathbf{Z}$, this series is absolutely convergent and defines a holomorphic function in this region, called the L-*function associated to* $\chi$.

In the region where $\mathrm{Re}(s) > 1$, the multiplicativity of $\chi$ implies that we have the absolutely convergent Euler product expansion

$$\mathrm{L}(s,\chi) = \prod_p (1 - \chi(p)p^{-s})^{-1}$$

(by Lemma C.1.4 applied to $f(n) = \chi(n)n^{-s}$ for any $s \in \mathbf{C}$ such that $\mathrm{Re}(s) > 1$). In particular, we deduce that $\mathrm{L}(s,\chi) \neq 0$ if $\mathrm{Re}(s) > 1$. Moreover, computing the logarithmic derivative, we obtain the formula

$$-\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) = \sum_{n \geqslant 1} \Lambda(n)\chi(n)n^{-s}$$

for $\mathrm{Re}(s) > 1$.

For the trivial character $1_q$ modulo $q$, we have the formula

$$\mathrm{L}(s,1_q) = \prod_{p \nmid q} (1 - p^{-s})^{-1} = \zeta(s) \prod_{p \mid q} (1 - p^{-s}).$$

Since the second factor is a finite product of quite simple form, we see that, when $q$ is fixed, the analytic properties of this particular L-function are determined by those of the Riemann zeta function. In particular, it has meromorphic continuation with a simple pole at $s = 1$, where the residue is

$$\prod_{p \mid q} (1 - p^{-1}) = \frac{\varphi(q)}{q}.$$

For $\chi$ nontrivial, we have the following result (see, e.g., [59, §5.9]):

**Theorem C.5.2** *Let $\chi$ be a nontrivial Dirichlet character modulo $q$. Define $\varepsilon_\chi = 0$ if $\chi(-1) = 1$ and $\varepsilon_\chi = 1$ if $\chi(-1) = -1$. Let*

$$\xi(s,\chi) = \pi^{-(s+\varepsilon_\chi)/2} q^{s/2} \Gamma\left(\frac{s+\varepsilon_\chi}{2}\right) \mathrm{L}(s,\chi)$$

*for* $\mathrm{Re}(s) > 1$. *Furthermore, let*

$$\tau(\chi) = \frac{1}{\sqrt{q}} \sum_{x \in (\mathbf{Z}/q\mathbf{Z})^\times} \chi(x) e\left(\frac{x}{q}\right).$$

*Then $\xi(s,\chi)$ extends to an entire function on* $\mathbf{C}$ *which satisfies the functional equation*

$$\xi(s,\chi) = \tau(\chi)\xi(1-s,\overline{\chi}).$$

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

In Chapter 5, we will require the basic information on the distribution of zeros of Dirichlet L-functions. We summarize it in the following proposition (see, e.g., [59, Th. 5.24]).

**Proposition C.5.3** *Let $\chi$ be a Dirichlet character modulo $q$.*

(1) *For $T \geqslant 1$, the number $N(T;\chi)$ of zeros $\varrho$ of $L(s,\chi)$ such that*

$$\operatorname{Re}(\varrho) > 0, \qquad |\operatorname{Im}(\varrho)| \leqslant T,$$

*satisfies*

$$N(T;\chi) = \frac{T}{\pi}\log\left(\frac{qT}{2\pi}\right) - \frac{T}{\pi} + O(\log q(T+1)), \tag{C.10}$$

*where the implied constant is absolute.*

(2) *For any $\varepsilon > 0$, the series*

$$\sum_{\varrho} |\varrho|^{-1-\varepsilon}$$

*converges, where $\varrho$ runs over zeros of $L(s,\chi)$ such that $\operatorname{Re}(\varrho) > 0$.*

**Remark C.5.4** These two statements are not independent, and in fact the first one implies the second by splitting the partial sum

$$\sum_{|\varrho|\leqslant T} \frac{1}{|\varrho|^{1+\varepsilon}}$$

for $T \geqslant 1$ in terms of zeros in intervals of length 1:

$$\sum_{|\varrho|\leqslant T} \frac{1}{|\varrho|^{1+\varepsilon}} \leqslant \sum_{1\leqslant N\leqslant T} \frac{1}{N^{1+\varepsilon}} \sum_{N-1\leqslant|\varrho|\leqslant N} 1 \ll \sum_{1\leqslant N\leqslant T} \frac{\log N}{N^{1+\varepsilon}}$$

by (1). Since this is uniformly bounded for all T, we obtain (2).

**Corollary C.5.5** *Let $\chi$ be a Dirichlet character modulo $q$.*

(1) *We have*

$$\sum_{\substack{0<\gamma<T\\ L(\frac{1}{2}+i\gamma,\chi)=0}} \frac{1}{|\frac{1}{2}+i\gamma|} \gg (\log T)^2$$

*for $T$ large enough.*

(2) *We have*

$$\sum_{\substack{\gamma>T\\ L(\frac{1}{2}+i\gamma,\chi)=0}} \frac{1}{|\frac{1}{2}+i\gamma|^2} \ll \frac{\log T}{T}$$

*for $T \geqslant 1$.*

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

Finally, we need a form of the *explicit formula* linking zeros of Dirichlet L-functions with the distribution of prime numbers.

**Theorem C.5.6** *Let $q \geqslant 1$ be an integer, and let $\chi$ be a nontrivial Dirichlet character modulo $q$. For any $x \geqslant 2$ and any $\mathrm{X} \geqslant 2$ such that $2 \leqslant x \leqslant \mathrm{X}$, we have*

$$\sum_{n \leqslant x} \Lambda(n)\chi(n) = -\sum_{\substack{\mathrm{L}(\beta+i\gamma)=0 \\ |\gamma| \leqslant \mathrm{X}}} \frac{x^{\beta+i\gamma}}{\beta+i\gamma} + \mathrm{O}\left(\frac{x(\log qx)^2}{\mathrm{X}}\right),$$

*where the sum is over nontrivial zeros of $\mathrm{L}(s,\chi)$, counted with multiplicity, and the implied constant is absolute.*

*Sketch of proof* We refer to, for example, [59, Prop. 5.25] for this result. Here we wish to justify intuitively the existence of such a relation between sums (essentially) over primes and sums over zeros of the associated L-function.

Pick a function $\varphi$ defined on $[0, +\infty[$ with compact support. Using the Mellin inversion formula (see Proposition A.3.1, (3)), we can write

$$\sum_{n \geqslant 1} \Lambda(n)\chi(n)\varphi\left(\frac{n}{x}\right) = \frac{1}{2i\pi}\int_{(2)} -\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\widehat{\varphi}(s)x^s\,ds$$

for all $x \geqslant 1$. Assume (formally) that we can shift the integration line to the left, say, to the line where the real part is $1/4$, where the contribution would be $x^{1/4}$. The contour shift leads to poles located at all the zeros of $\mathrm{L}(s,\chi)$, with residue equal to the opposite of the multiplicity of the zero (since the L-function is entire, there is no contribution from poles). We can therefore expect that

$$\sum_{n \geqslant 1} \Lambda(n)\chi(n)\varphi\left(\frac{n}{x}\right) = -\sum_{\varrho} \widehat{\varphi}(\varrho)x^{\varrho} + (\text{small error}),$$

where $\varrho$ runs over nontrivial zeros of $\mathrm{L}(s,\chi)$, counted with multiplicity.

If such a formula holds for the characteristic function $\varphi$ of the interval $[0,1]$, then since

$$\widehat{\varphi}(s) = \int_0^1 x^{s-1}dx = \frac{1}{s},$$

we would obtain

$$\sum_{n \geqslant 1} \Lambda(n)\chi(n)\varphi\left(\frac{n}{x}\right) = -\sum_{\varrho} \frac{x^{\varrho}}{\varrho} + (\text{small error}).$$

□

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

**Remark C.5.7** There is nontrivial analytic work to do in order to justify the computations in this sketch, because of various convergence issues for instance (which also explains why the formula is most useful in a truncated form involving only finitely many zeros), but this formal outline certainly explains the *existence* of the explicit formula.

This explicit formula explains why the location of zeros of Dirichlet L-functions is so important in the study of prime numbers in arithmetic progressions. This motivates the *Generalized Riemann Hypothesis* modulo $q$:

**Conjecture C.5.8 (Generalized Riemann Hypothesis)** *For any integer $q \geqslant 1$ and for any Dirichlet character $\chi$ modulo $q$ and any zero $\varrho = \beta + i\gamma$ of its* L*-function such that $0 < \beta \leqslant 1$, we have $\beta = \frac{1}{2}$.*

This is the most famous open problem of number theory. In practice, we will also speak of *Generalized Riemann Hypothesis modulo $q$* when considering only the fixed modulus $q$ instead of all moduli. The case $q = 1$ corresponds to the original Riemann Hypothesis for the Riemann zeta function only.

By just applying orthogonality (Proposition C.5.1) and estimating trivially in the explicit formula with the help of Proposition C.5.3, we deduce:

**Proposition C.5.9** *Let $q \geqslant 1$ be an integer. Assume that the Generalized Riemann Hypothesis modulo $q$ holds. Then we have*

$$\sum_{\substack{n\leqslant x\\ n\equiv a \,(\mathrm{mod}\, q)}} \Lambda(n) = \frac{x}{\varphi(q)} + \mathrm{O}(x^{1/2}(\log qx)^2).$$

**Remark C.5.10** Compare the quality of the error term with the (essentially) best known unconditional result of Theorem C.3.7.

Another corollary of the explicit formula that will be helpful in Chapter 5 is the following:

**Corollary C.5.11** *Let $q \geqslant 1$ be an integer and let $\chi$ be a nontrivial Dirichlet character modulo $q$. Assume that the Generalized Riemann Hypothesis holds for* $\mathrm{L}(s, \chi)$*, i.e., that all nontrivial zeros of* $\mathrm{L}(s, \chi)$ *have real part* $1/2$*. For any $x \geqslant 2$, we have*

$$\int_2^x \left(\sum_{n\leqslant t} \Lambda(n)\chi(n)\right) dt \ll x^{3/2},$$

*where the implied constant depends on $q$.*

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

*Proof* Pick $X = x$ in the explicit formula. Using the assumption on the zeros, we obtain by integration the expression

$$\begin{aligned}\int_2^x \Big(\sum_{n\leqslant t}\Lambda(n)\chi(n)\Big)\,dt &= \sum_{\substack{\mathrm{L}(\frac12+i\gamma)=0\\ |\gamma|\leqslant x}} \int_2^x \frac{t^{\frac12+i\gamma}}{\frac12+i\gamma}dt + \mathrm{O}(x(\log qx)^2)\\ &= \sum_{\substack{\mathrm{L}(\frac12+i\gamma)=0\\ |\gamma|\leqslant x}} \frac{x^{\frac12+i\gamma+1}-2^{\frac12+i\gamma+1}}{(\frac12+i\gamma)(\frac12+i\gamma+1)} + \mathrm{O}(x(\log qx)^2) \ll x^{3/2},\end{aligned}$$

where the implied constant depends on $q$, since the series

$$\sum_{\mathrm{L}(\frac12+i\gamma)=0} \frac{1}{(\frac12+i\gamma)(\frac12+i\gamma+1)}$$

converges absolutely by Proposition C.5.3, (2). □

## C.6 Exponential Sums

In Chapter 6, we studied some properties of exponential sums. Although we do not have the space to present a detailed treatment of such sums, we will give a few examples and try to explain some of the reasons why such sums are important and interesting. This should motivate the "curiosity driven" study of the shape of the partial sums. We refer to the notes [75] and to [59, Ch. 11] for more information, including proofs of the Weil bound (6.1) for Kloosterman sums.

In principle, any finite sum

$$\mathrm{S_N} = \sum_{1\leqslant n\leqslant \mathrm{N}} e(\alpha_n)$$

of complex numbers of modulus 1 counts as an exponential sum, and the goal is – given the *phases* $\alpha_n \in \mathbf{R}$ – to obtain a bound on S that improves as much as possible on the "trivial" bound $|\mathrm{S_N}| \leqslant \mathrm{N}$.

On probabilistic grounds, one can expect that for highly oscillating phases, the sum $\mathrm{S_N}$ is of size about $\sqrt{\mathrm{N}}$. Indeed, if we consider $\alpha_n$ to be random variables that are independent and uniformly distributed in $\mathbf{R}/\mathbf{Z}$, then the

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

Central Limit Theorem shows that $S_N/\sqrt{N}$ is distributed approximately like a standard complex Gaussian random variable, so that the "typical" size of $S_N$ is of order of magnitude $\sqrt{N}$. When this occurs also for deterministic sums (up to factors of smaller order of magnitude), one says that the sums have *square-root cancellation*; this usually only makes sense for an infinite sequence of sums where $N \to +\infty$.

**Example C.6.1** For instance, the partial sums

$$M_N = \sum_{1 \leqslant n \leqslant N} \mu(n)$$

of the Möbius function can be seen in this light. Estimating $M_N$ is vitally important in analytic number theory, because it is not very hard to check that the Prime Number Theorem, in the form (C.3), with error term $x/(\log x)^A$ for any $A > 0$, is *equivalent* with the estimate

$$M_N \ll \frac{N}{(\log N)^A}$$

for any $A > 0$, where the implied constant depends on A. Moreover, the best possible estimate is the square-root cancellation

$$M_N \ll N^{1/2+\varepsilon},$$

with an implied constant depending on $\varepsilon > 0$, and this is known to be equivalent to the Riemann Hypothesis for the Riemann zeta function.

The sums that appear in Chapter 6 are, however, of a fairly different nature. They are sums over finite fields (or subsets of finite fields), with summands $e(\alpha_n)$ of "algebraic nature." For a prime $p$ and the finite field $\mathbf{F}_p$ with $p$ elements,[2] the basic examples are of the following types:

**Example C.6.2** (1) [Additive character sums] Fix a rational function $f \in \mathbf{F}_p(T)$. Then for $x \in \mathbf{F}_p$ that is not a pole of $f$, we can evaluate $f(x) \in \mathbf{F}_p$, and $e(f(x)/p)$ is a well-defined complex number. Then consider the sum

$$\sum_{\substack{x \in \mathbf{F}_p \\ f(x) \text{ defined}}} e(f(x)/p).$$

For fixed $a$ and $b$ in $\mathbf{F}_p^\times$, the example $f(T) = aT + bT^{-1}$ gives rise to the *Kloosterman sum* of Section 6.1. If $f(T) = T^2$, we obtain a *quadratic Gauss sum*, namely,

[2] For simplicity, we restrict to these particular finite fields, but the theory extends to all.

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

$$\sum_{x\in\mathbf{F}_p} e\left(\frac{x^2}{p}\right).$$

(2) [Multiplicative character sums] Let $\chi$ be a nontrivial character of the finite multiplicative group $\mathbf{F}_p^\times$; we define $\chi(0) = 0$ to extend it to $\mathbf{F}_p$. Let $f \in \mathbf{F}_p[\mathrm{T}]$ be a polynomial (or a rational function). The corresponding multiplicative character sum is

$$\sum_{x\in\mathbf{F}_p} \chi(f(x)).$$

One may also have finitely many polynomials and characters and sum their products. An important example of these is

$$\sum_{x\in\mathbf{F}_p} \chi_1(x)\chi_2(1-x),$$

for multiplicative characters $\chi_1$ and $\chi_2$, which is called a *Jacobi sum*.

(3) [Mixed sums] In fact, one can mix the two types, obtaining a family of sums that generalize both: fix rational functions $f_1$ and $f_2$ in $\mathbf{F}_p(\mathrm{T})$, and consider the sum

$$\sum_{x\in\mathbf{F}_p} \chi(f_1(x))e(f_2(x)/p),$$

where the summand is defined to be 0 if $f_2(x)$ is not defined, or if $f_1(x)$ is 0 or not defined.

Some of the key examples are obtained in this manner. Maybe the simplest interesting ones are the *Gauss sums* attached to $\chi$, defined by

$$\sum_{x\in\mathbf{F}_p} \chi(x)e(ax/p),$$

where $a \in \mathbf{F}_p$ is a parameter. Others are the sums

$$\sum_{x\in\mathbf{F}_p^\times} \chi(x)e\left(\frac{ax+b\bar{x}}{p}\right)$$

for $a, b$ in $\mathbf{F}_p$, which generalize the Kloosterman sums. When $\chi$ is a character of order 2 (i.e., $\chi(x)$ is either 1 or $-1$ for all $x \in \mathbf{F}_p$), this is called a *Salié sum*.

**Remark C.6.3** We emphasize that the sums that we discuss range over the *whole* finite field (except for values of $x$ where the summand is not defined). Sums over smaller subsets of $\mathbf{F}_p$ (e.g., over a segment $1 \leqslant x \leqslant \mathrm{N} < p$ of

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

integers) are very interesting and important in applications (indeed, they are the topic of Chapter 6!), but behave very differently.

Except for a few special cases (some of which are discussed below in exercises), a simple "explicit" evaluation of exponential sums of the previous types is not feasible. Even deriving nontrivial bounds is far from obvious, and the most significant progress requires input from algebraic geometry. The key result, proved by A. Weil in the 1940s, takes the following form (in a simplified version that is actually rather weaker than the actual statement). It is a special case of the Riemann Hypothesis over finite fields.

**Theorem C.6.4 (Weil)** *Let $\chi$ be a nontrivial multiplicative character modulo $q$. Let $f_1$ and $f_2$ be rational functions in $\mathbf{F}_p[\mathrm{T}]$, and consider the sum*

$$\sum_{x\in\mathbf{F}_p} \chi(f_1(x))e(f_2(x)/p).$$

*Assume that* either *$f_1$ is not of the form $g_1^d$, where $d$ is the order of $\chi$ and $g_1 \in \overline{\mathbf{F}}_p[\mathrm{T}]$,* or *$f_2$ has a pole of order not divisible by $p$, possibly at infinity.*

*Then, there exists an integer $\beta$, depending only on the degrees of the numerator and denominator of $f_1$ and $f_2$, and for $1 \leqslant i \leqslant \beta$, there exist complex numbers $\alpha_i$ such that $|\alpha_i| \leqslant \sqrt{p}$, with the property that*

$$\sum_{x\in\mathbf{F}_p} \chi(f_1(x))e(f_2(x)/p) = -\sum_{i=1}^{\beta} \alpha_i.$$

*In particular, we have*

$$\left|\sum_{x\in\mathbf{F}_p} \chi(f_1(x))e(f_2(x)/p)\right| \leqslant \beta\sqrt{p}.$$

In fact, one can provide formulas for the integer $\beta$ that are quite explicit (in terms of the zeros and poles of the rational functions $f_1$ and $f_2$), and often one knows that $|\alpha_i| = \sqrt{q}$ for all $i$. For instance, if $f_1 = 1$ (so that the sum is an additive character sum) and $f_2$ is a polynomial such that $1 \leqslant \deg(f_2) < p$, then $\beta = \deg(f_2) - 1$, and $|\alpha_i| = \sqrt{p}$ for all $p$.

For more discussion and a proof in either the additive or multiplicative cases, we refer to [75].

The following exercises illustrate this general result in three important cases. Note however, that there is no completely elementary proof in the case of Kloosterman sums, where $\beta = 2$, leading to (6.1).

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

**Exercise C.6.5 (Gauss sums)** Let $\chi$ be a nontrivial multiplicative character of $\mathbf{F}_p^\times$ and $a \in \mathbf{F}_p^\times$. Denote

$$\tau(\chi, a) = \sum_{x \in \mathbf{F}_p} \chi(x) e(ax/p),$$

and put $\tau(\chi) = \tau(\chi, 1)$ (up to normalization, this is the same sum as occurs in the functional equation for the Dirichlet L-function $\mathrm{L}(s, \chi)$, see Theorem C.5.2).

(1) Prove that

$$|\tau(\chi, a)| = \sqrt{p}.$$

(This proves the corresponding special case of Theorem C.6.4 with $\beta = 1$ and $|\alpha_1| = \sqrt{p}$.) [**Hint**: Compute the modulus square, or apply the discrete Parseval identity.]

(2) Prove that for any automorphism $\sigma$ of the field $\mathbf{C}$, we also have

$$|\sigma(\tau(\chi, a))| = \sqrt{p}.$$

(This additional property is also true for all $\alpha_i$ in Theorem C.6.4 in general; it means that each $\alpha_i$ is a so-called $p$-Weil number of weight 1.)

**Exercise C.6.6 (Jacobi sums)** Let $\chi_1$ and $\chi_2$ be nontrivial multiplicative characters of $\mathbf{F}_p^\times$. Denote

$$\mathrm{J}(\chi_1, \chi_2) = \sum_{x \in \mathbf{F}_p} \chi_1(x)\chi_2(1 - x).$$

(1) Prove that

$$\mathrm{J}(\chi_1, \chi_2) = \frac{\tau(\chi_1)\tau(\chi_2)}{\tau(\chi_1\chi_2)},$$

and deduce that Theorem C.6.4 holds for the Jacobi sums $\mathrm{J}(\chi_1, \chi_2)$ with $\beta = 1$ and $|\alpha_1| = 1$. Moreover, show that $\alpha_1$ satisfies the property of the second part of the previous exercise.

(3) Assume that $p \equiv 1 \pmod 4$. Prove that there exist integers $a$ and $b$ such that $a^2 + b^2 = p$ (a result of Fermat). [**Hint**: Show that there are characters $\chi_1$ of order 2 and $\chi_2$ of order 4 of $\mathbf{F}_p^\times$, and consider $\mathrm{J}(\chi_1, \chi_2)$.]

**Exercise C.6.7 (Salié sums)** Assume that $p \geqslant 3$.

(1) Check that there is a unique nontrivial real character $\chi_2$ of $\mathbf{F}_p^\times$. Prove that for any $x \in \mathbf{F}_p$, the number of $y \in \mathbf{F}_p$ such that $y^2 = x$ is $1 + \chi_2(y)$.

(2) Prove that

$$\tau(\chi^2)\tau(\chi_2) = \chi(4)\tau(\chi)\tau(\chi\chi_2)$$

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press

(Hasse–Davenport relation). [**Hint**: Use the formula for Jacobi sums, and compute $J(\chi,\chi)$ in terms of the number of solutions of quadratic equations; express this number of solutions in terms of $\chi_2$.]

For $(a,b) \in \mathbf{F}_p^\times$, define

$$S(a,b) = \sum_{x\in\mathbf{F}_p^\times} \chi_2(x) e\left(\frac{ax+b\bar{x}}{p}\right).$$

(3) Show that for $b \in \mathbf{F}_p^\times$, we have

$$S(a,b) = \sum_{\chi} s(\chi)\chi(a),$$

where

$$s(\chi) = \frac{\chi(b)\chi_2(b)\tau(\bar{\chi})\tau(\bar{\chi}\chi_2)}{q-1}.$$

[**Hint**: Use a discrete multiplicative Fourier expansion.]

(4) Show that

$$s(\chi) = \frac{\chi_2(b)\tau(\chi_2)}{q-1}\chi(4b)\tau(\bar{\chi}^2).$$

(5) Deduce that

$$S(a,b) = \tau(\chi_2) \sum_{ay^2=4b} e\left(\frac{y}{p}\right).$$

(6) Deduce that Theorem C.6.4 holds for $S(a,b)$ with either $\beta = 0$ or $\beta = 2$, in which case, $|\alpha_1| = |\alpha_2| = \sqrt{p}$.

https://doi.org/10.1017/9781108888226.011 Published online by Cambridge University Press