Classical Algebraic and Analytic Number Theory

Henry Twiss

2025

Contents

Part I

Multiplicative Number Theory

Chapter 1

Arithmetic Functions

1.1 Multiplicative and Additive Functions

Any function

$$f : \mathbb{Z}_{\geq 1} \to \mathbb{C},$$

is said to be *arithmetic*. That is, arithmetic functions are maps from the positive integers to the complex numbers. If an arithmetic function f satisfies

$$f(nm) = f(n)f(m) \quad \text{or} \quad f(nm) = f(n) + f(m),$$

whenever n and m are relatively prime, we say f is *multiplicative* or *additive* respectively. If either condition holds for all n and m then we say f is *completely multiplicative* or *completely additive*. If f is additive or multiplicative then f is uniquely determined by its values on prime powers and if f is completely additive or completely multiplicative then it is uniquely determined by its values on primes. Moreover, we have

$$f(1) = 1 \quad \text{or} \quad f(1) = 0,$$

according to if f is multiplicative or additive. Most important arithmetic functions are either multiplicative or additive. Below is a list of the most important arithmetic functions (some of these functions are restrictions of common functions but we define them here as arithmetic functions for completeness):

(i) The *constant function*: The function $\mathbf{1}(n)$. This function is neither additive nor multiplicative.

(ii) The *indicator function*: The function $\varepsilon(n)$ defined by

$$\varepsilon(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \geq 2. \end{cases}$$

This function is completely multiplicative.

(iii) The *identity function*: The function $\mathrm{id}(n)$. This function is completely multiplicative.

(iv) The *logarithm*: The function $\log(n)$. This function is completely additive.

(v) The *Möbius function*: The function $\mu(n)$ defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n \text{ is square-free with an even number of prime factors,} \\ -1 & \text{if } n \text{ is square-free with an odd number of prime factors,} \\ 0 & \text{if } n \text{ is not square-free.} \end{cases}$$

This function is multiplicative.

(vi) The *characteristic function of square-free integers*: The square of the Möbius function $\mu^2(n)$. This function is multiplicative.

(vii) *Liouville's function*: The function $\lambda(n)$ defined by

$$\lambda(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is composed of } k \text{ not necessarily distinct prime factors.} \end{cases}$$

This function is completely multiplicative.

(viii) *Euler's totient function*: The function $\varphi(n)$ defined by

$$\varphi(n) = \sum_{\substack{a \pmod n \\ (a,n)=1}} 1.$$

This function is multiplicative.

(ix) The *divisor function*: The function $\sigma_0(n)$ defined by

$$\sigma_0(n) = \sum_{d|n} 1.$$

This function is multiplicative.

(x) The *sum of divisors function*: The function $\sigma_1(n)$ defined by

$$\sigma_1(n) = \sum_{d|n} d.$$

This function is multiplicative.

(xi) The *generalized sum of divisors function*: The function $\sigma_s(n)$ defined by

$$\sigma_s(n) = \sum_{d|n} d^s,$$

for any $s \in \mathbb{C}$. This function is multiplicative.

(xii) The *number of distinct prime factors function*: The function $\omega(n)$ defined by

$$\omega(n) = \sum_{p|n} 1.$$

This function is additive.

(xiii) The *total number of prime divisors function*: The function $\Omega(n)$ defined by

$$\Omega(n) = \sum_{p^m|n} 1.$$

This function is completely additive.

(xiv) The *von Mangoldt function*: The function $\Lambda(n)$ defined by

$$\Lambda(n) = \begin{cases} 0 & \text{if } n \text{ is not a prime power,} \\ \log(p) & \text{if } n = p^m \text{ for some prime } p \text{ and positive integer } m. \end{cases}$$

This function is neither additive or multiplicative.

1.2 Dirichlet Convolution and Möbius Inversion

If f and g are two arithmetic functions then we can define a new arithmetic function $f * g$ called their *Dirichlet convolution* defined by

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

As the sum is over all divisors, Dirichlet convolution is a symmetric operation. Dirichlet convolution preserves multiplicative functions.

Proposition 1.2.1. *If f and g are multiplicative arithmetic functions then so is their Dirichlet convolution $f * g$.*

Proof. Let n and m be relatively prime positive integers. Every divisor d of nm is of the form $d = d'd''$ with d' a divisor of n, d'' a divisor of m, and d' and d'' relatively prime. A short computation shows

$$\sum_{d|nm} f(d) g\left(\frac{nm}{d}\right) = \left(\sum_{d'|n} f(d') g\left(\frac{n}{d'}\right)\right) \left(\sum_{d''|m} f(d'') g\left(\frac{m}{d''}\right)\right),$$

which is equivalent to the claim. $\square$

This result makes the set of multiplicative functions into a commutative semigroup under Dirichlet convolution. It is actually a commutative monoid since the indicator function ε acts as an identity. This means

$$f * \varepsilon = f.$$

A certain case of interest for Dirichlet convolution is when the Möbius function is convolved with the constant function.

Proposition 1.2.2. *We have*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \geq 2. \end{cases}$$

In particular,

$$\mu * \mathbf{1} = \varepsilon.$$

Proof. The first statement is equivalent to the second, so it suffices to prove the first. The sum $\sum_{d|n} \mu(d)$ is multiplicative by Proposition 1.2.1 so we may assume $n = p^r$ is a nonnegative power of a prime. When $r = 0$, $d = 1$ and the sum is 1. When $r \geq 1$, d runs over $1, p, \ldots, p^r$. Every value is zero except $\mu(1) = 1$ and $\mu(p) = -1$. This proves that the sum is zero. $\square$

With this result we can prove *Möbius inversion*:

Theorem (Möbius inversion). *If f and g are arithmetic functions, then*

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

In particular,

$$g = f * \mathbf{1} \quad \text{if and only if} \quad f = g * \mu.$$

Proof. As the first statement is equivalent to the second, we will prove the second statement. Convolving $g = f * \mathbf{1}$ with μ gives $f = g * \mu$ in view of Proposition 1.2.2. This proves the forward implication. The reverse implication follows by convolving $f = g * \mu$ with $\mathbf{1}$ and arguing analogously. $\square$

Chapter 2

Todo: [Ditributions and Asymptotics]

Chapter 3

Dirichlet Characters and Exponential Sums

3.1 Dirichlet Characters

Let m be a positive integer. A multiplicative homomorphism

$$\chi : \mathbb{Z} \to \mathbb{C},$$

is said to be a *Dirichlet character* modulo m if it is m-periodic and such that $\chi(a) = 0$ if and only if $(a, m) > 1$. We call m the *modulus* of χ. A Dirichlet character is necessarily a completely multiplicative arithmetic function when restricted to the positive integers.

We say a Dirichlet character χ is *principal* if it only takes values 0 or 1. There is always a unique principal Dirichlet character modulo m, denoted $\chi_{m,0}$, defined by

$$\chi_{m,0}(a) = \begin{cases} 1 & (a, m) = 1, \\ 0 & (a, m) > 1. \end{cases}$$

When the modulus is 1, the principal Dirichlet character is identically 1 and we call this the *trivial Dirichlet character*. This is the only Dirichlet character modulo 1.

By Euler's little theorem, $a^{\varphi(m)} \equiv 1 \pmod{m}$ whenever $(a, m) = 1$. This forces $\chi(a)^{\varphi(m)} = 1$ and so the nonzero values of any Dirichlet character modulo m are $\varphi(m)$-th roots of unity. This implies that there are only finitely many Dirichlet characters of any fixed modulus. Given two Dirichlet character χ and ψ modulo m, the functions

$$\chi\psi : \mathbb{Z} \to \mathbb{C} \quad \text{and} \quad \overline{\chi} : \mathbb{Z} \to \mathbb{C},$$

are also Dirichlet characters modulo m. This turns the set of such Dirichlet characters into an abelian group denote by X_m where the identity is the principal Dirichlet character modulo m and the inverse is given by the conjugate as the nonzero values of Dirichlet characters are roots of unity.

This is all strikingly similar to characters on $(\mathbb{Z}/m\mathbb{Z})^*$ and there is indeed a connection. By the multiplicativity and m-periodicity of χ, it induces a character of

$(\mathbb{Z}/m\mathbb{Z})^*$. Conversely, if we are given a character on $(\mathbb{Z}/m\mathbb{Z})^*$ we can extend it to a Dirichlet character χ by defining it to be m-periodic with $\chi(a) = 0$ if $(a, m) > 1$. We call this extension a *zero extension*. This argument shows that Dirichlet characters modulo m are exactly the zero extensions of characters on $(\mathbb{Z}/m\mathbb{Z})^*$. As abelian groups are isomorphic to their character groups, we deduce that the group of Dirichlet characters modulo m is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$. Therefore there are $\varphi(m)$ Dirichlet characters modulo m and we identify them with the characters on $(\mathbb{Z}/m\mathbb{Z})^*$. Just as for characters of abelian groups, we have orthogonality relations called the *Dirichlet orthogonality relations*.

Proposition (Dirichlet orthogonality relations). *Let χ and ψ be Dirichlet characters modulo m and let $a, b \in (\mathbb{Z}/m\mathbb{Z})^*$. Then*

$$\sum_{a \pmod m} (\chi\overline{\psi})(a) = \varphi(m)\delta_{\chi,\psi} \quad \text{and} \quad \sum_{\chi \pmod m} \chi(a\overline{b}) = \varphi(m)\delta_{a,b}.$$

In particular,

$$\sum_{a \pmod m} \chi(a) = \varphi(m)\delta_{\chi,\chi_{m,0}} \quad \text{and} \quad \sum_{\chi \pmod m} \chi(a) = \varphi(m)\delta_{a,1}.$$

Proof. If $\chi = \psi$ then the first sum is clearly $\phi(m)$. If not, let $b \in (\mathbb{Z}/m\mathbb{Z})^*$ be such that $(\chi\overline{\psi})(b) \neq 1$. A short computation shows

$$(\chi\overline{\psi})(b) \sum_{a \pmod m} (\chi\overline{\psi})(a) = \sum_{a \pmod m} (\chi\overline{\psi})(a),$$

in which case the sum vanishes. This proves the first identity. For the second, if $a = b$ then the second sum is clearly $\varphi(m)$. If $a \neq b$, we claim that there exists a Dirichlet character ψ modulo m with $\psi(a\overline{b}) \neq 1$. Set $g = a\overline{b}$. The cyclic subgroup $\langle g \rangle$ of $(\mathbb{Z}/m\mathbb{Z})^*$ has some order $d > 1$. Consider the homomorphism

$$\psi_d : \langle g \rangle \to \mathbb{C} \qquad g^k \mapsto e^{\frac{2\pi i k}{d}}.$$

By the structure theorem for finite abelian groups, $(\mathbb{Z}/m\mathbb{Z})^* \cong \langle g \rangle \times H$ for some subgroup H. Whence we define a Dirichlet character ψ modulo m by

$$\psi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C} \qquad g^k h \mapsto e^{\frac{2\pi i k}{d}}.$$

This ψ is the desired Dirichlet character, A short computation shows

$$\psi(a\overline{b}) \sum_{\chi \pmod m} \chi(a\overline{b}) = \sum_{\chi \pmod m} \chi(a\overline{b}),$$

in which case the sum vanishes. This proves the second identity and the first statement in its entirety. The second statement follows from the first upon taking $\psi = \chi_{m,0}$ and $b = 1$ respectively. $\square$

It it possible for Dirichlet characters of a fixed modulus to arise from Dirichlet characters of a smaller modulus. Suppose χ and χ^* are Dirichlet characters modulo m and d respectively with $d \mid m$. We say χ is induced *induced* from χ^* (or χ^* *induces* χ) if

$$\chi(a) = \begin{cases} \chi^*(a) & \text{if } (a,m) = 1, \\ 0 & \text{if } (a,m) > 1. \end{cases}$$

This means χ is a Dirichlet character whose values are given by those of χ^*. Necessarily χ is d-periodic and its nonzero values are $\varphi(d)$-th roots of unity. We say a Dirichlet character is *primitive* if it is not induced by any Dirichlet character other than itself and *imprimitive* otherwise. The principal Dirichlet characters are precisely those induced from the trivial Dirichlet character and the only primitive one is the trivial Dirichlet character itself. Moreover, a Dirichlet character is primitive if and only if its conjugate is. Our primary aim will be to show that every Dirichlet character is induced from a unique primitive Dirichlet character.

Theorem 3.1.1. *Suppose χ is a Dirichlet character modulo m. There exists a unique primitive Dirichlet character $\widetilde{\chi}$ such that χ is induced from $\widetilde{\chi}$.*

Proof. Let q be the positive integer given by

$$q = \min\{d \mid m : \chi(a) = \chi(b) \text{ for all } a \equiv b \pmod{d} \text{ with } (ab,m) = 1\},$$

and let $\widetilde{\chi} : \mathbb{Z} \to \mathbb{C}$ be defined by

$$\widetilde{\chi}(a) = \begin{cases} \chi(a) & \text{if } (a,q) = 1, \\ 0 & \text{if } (a,q) > 1. \end{cases}$$

The definition of q implies $\widetilde{\chi}$ is well-defined and hence q-periodic. In fact, $\widetilde{\chi}$ is a Dirichlet character modulo q and minimality forces $\widetilde{\chi}$ to be primitive. By construction χ is indued from $\widetilde{\chi}$ and this proves existence. Now suppose $\widetilde{\chi}_1$ and $\widetilde{\chi}_2$ are two primitive Dirichlet characters modulo q_1 and q_2 respectively both of which induce χ. Then $\widetilde{\chi}_1(a) = \widetilde{\chi}_2(a)$ whenever $(a,m) = 1$. Setting $q = (q_1, q_2)$, we also have $\widetilde{\chi}_1(a) = \widetilde{\chi}_2(a)$ whenever $(a,q) = 1$. Hence $\widetilde{\chi}_1$ and $\widetilde{\chi}_2$ are both induced from the same Dirichlet character modulo q. Primitivity implies $q_1 = q_2$ and $\widetilde{\chi}_1 = \widetilde{\chi}_2$. This proves uniqueness. $\square$

In light of this result, we define the *conductor* q of a Dirichlet character χ modulo m to be the modulus of the unique primitive Dirichlet character $\widetilde{\chi}$ inducing χ. By the proof, the conductor is given by

$$q = \min\{d \mid m : \chi(a) = \chi(b) \text{ for all } a \equiv b \pmod{d} \text{ with } (ab,m) = 1\}.$$

Also observe that χ is q-periodic, q is the minimal period of χ, and the nonzero values of χ are $\varphi(q)$-th roots of unity. Moreover,

$$\chi = \widetilde{\chi}\chi_{\frac{m}{q},0},$$

and χ is primitive if and only if its conductor and modulus are equal.

As not every Dirichlet character of a fixed modulus is primitive, it is natural to ask how many primitive Dirichlet characters there are for a given modulus. Let $N(m)$ be the number of primitive Dirichlet characters modulo m. Then $N(m)$ is easily determined via Möbius inversion.

Proposition 3.1.2. *For any positive integer m, we have*

$$\phi(m) = \sum_{d|m} N(d),$$

where $N(d)$ be the number of primitive Dirichlet characters modulo d. In particular, $N(m)$ is given by

$$N(m) = \sum_{d|m} \phi(d)\mu\left(\frac{m}{d}\right)$$

Proof. To prove the first formula, the right-hand side counts the number of Dirichlet characters modulo m since every such Dirichlet character is induced from a unique primitive Dirichlet character whose modulus divides m by Theorem 3.1.1. The left hand side also counts the number of Dirichlet characters modulo m as are $\phi(m)$ many. This proves the first formula. The second follows by Möbius inversion. □

Primitive Dirichlet characters also behave well with respect to multiplication if the conductors are relatively prime as the following proposition shows:

Proposition 3.1.3. *Suppose χ_1 and χ_2 are Dirichlet characters modulo m_1 and m_2 respectively with $(m_1, m_2) = 1$. Set $\chi = \chi_1\chi_2$. Then χ is a primitive if and only if χ_1 and χ_2 both are.*

Proof. By construction, χ is a Dirichlet character modulo m_1m_2. Let q_1 and q_2 be the conductors of χ_1 and χ_2 respectively and let q be the conductor of χ. Then χ is q_1q_2-periodic and $q \mid q_1q_2$.

For the forward implication, suppose χ is primitive so that $q = m_1m_2$ whence $m_1m_2 \mid q_1q_2$. This forces $m_1 = q_1$ and $m_2 = q_2$ proving χ_1 and χ_2 are both primitive. For the reverse implication, suppose χ_1 and χ_2 are both primitive so that $q_1 = m_1$ and $q_2 = m_2$. Then $(q_1, q_1) = 1$ and the Chinese remainder theorem implies that χ is q_1-periodic on those integers that are congruent to 1 modulo q_2 and q_2-periodic on those integers that are congruent to 1 modulo q_1. This forces $q_1 \mid q$ and $q_2 \mid q$ which together imply $q = q_1q_2$ and thus χ is primitive. □

We would now like to distinguish Dirichlet characters based on their nonzero values. We say χ is *real* if it is real-valued. This means the nonzero values of χ are 1 or -1 since they are the only real roots of unity. We say χ is *complex* if it is not real. More commonly, we distinguish Dirichlet characters by the roots of unity that their nonzero values take. We say χ is of *order n* if the nonzero values of χ are all n-th roots of unity. In the cases of small order we will often use the latin derived names *quadratic*, *cubic*, etc. To connect these two naming conventions observe that a nontrivial Dirichlet character is quadratic if and only if it is real and an other nontrivial Dirichlet character is necessarily complex. Also note that quadratic Dirichlet characters are their own conjugates.

We will also distinguish Dirichlet characters by their parity. By multiplicativity, we must have $\chi(-1) = \pm 1$. Accordingly, we say χ is *even* if $\chi(-1) = 1$ and *odd* if $\chi(-1) = -1$. Then even Dirichlet characters are even functions while odd Dirichlet characters are odd functions. Note that conjugate and induced Dirichlet characters necessarily have the same parity. The parity is also expressed via the formula

$$\frac{\chi(1) - \chi(-1)}{2} = \begin{cases} 0 & \text{if } \chi \text{ is even}, \\ 1 & \text{if } \chi \text{ is odd}. \end{cases}$$

3.2 Quadratic Dirichlet Characters

Quadratic Dirichlet characters deserve special attention as it is possible to classify all of them explicitly. This is due to the fact that they arise from Jacobi and Kronecker symbols. For a positive odd integer m, define

$$\chi_m(a) = \left(\frac{a}{m}\right).$$

By definition of the Jacobi symbol, χ_m becomes a quadratic Dirichlet character modulo m. Unfortunately, the quadratic Dirichlet characters constructed in this manner do not exhaust all possible examples. To accomplish this we need to use Kronecker symbols. An integer D is said to be a *fundamental discriminant* if it is of the form

$$D = \begin{cases} d & \text{if } D \equiv 1 \pmod{4}, \\ 4d & \text{if } D \equiv 8, 12 \pmod{16}, \end{cases}$$

for some square-free integer d. Necessarily $d \equiv 1 \pmod{4}$ or $d \equiv 2, 3 \pmod{4}$ respectively and thus is nonzero. We define $\chi_D : \mathbb{Z} \to \mathbb{C}$ by

$$\chi_D(a) = \left(\frac{D}{a}\right).$$

It turns out that χ_D defines a primitive quadratic Dirichlet character modulo $|D|$, provided $D \neq 1$, and exhausts all such possibilities.

Theorem 3.2.1. *If D is a fundamental discriminant and $D \neq 1$ then χ_D is a primitive quadratic Dirichlet character of conductor $|D|$. Moreover, all primitive quadratic Dirichlet characters are of this form.*

Proof. We first show that χ_D is a primitive quadratic Dirichlet character modulo $|D|$. If $D \equiv 1 \pmod{4}$, the sign in quadratic reciprocity is always 1. Then

$$\chi_D(a) = \left(\frac{a}{|D|}\right),$$

which is a Dirichlet character modulo $|D|$. If $D \equiv 12 \pmod{16}$ then $\frac{D}{4} \equiv 3 \pmod 4$ and the sign in quadratic reciprocity is $\left(\frac{-1}{a}\right)$ which is the primitive quadratic Dirichlet character modulo 4 as there are only two such Dirichlet characters and $\left(\frac{-1}{a}\right)$ is not principal. Whence

$$\chi_D(a) = \left(\frac{-1}{a}\right)\left(\frac{a}{\left|\frac{D}{4}\right|}\right),$$

which is a Dirichlet character modulo $|D|$. If $D \equiv 8 \pmod{16}$ first observe that $\left(\frac{D}{a}\right) = \left(\frac{8}{a}\right)\left(\frac{\frac{D}{8}}{a}\right)$ where $\left(\frac{8}{a}\right)$ is one of the two primitive quadratic Dirichlet character modulo 8 (the other is $\left(\frac{-8}{a}\right)$). As $\frac{D}{8} \equiv 1, 3 \pmod 4$, the sign in quadratic reciprocity is either 1 or $\left(\frac{-1}{a}\right)$ according to these two cases. Thus

$$\chi_D(a) = \left(\frac{8}{a}\right)\left(\frac{a}{\left|\frac{D}{8}\right|}\right) \quad \text{or} \quad \chi_D(a) = \left(\frac{-8}{a}\right)\left(\frac{a}{\left|\frac{D}{8}\right|}\right),$$

according to if $\frac{D}{8} \equiv 1, 3 \pmod 4$ respectively, and in either case is a Dirichlet character modulo $|D|$. We can compactly express all of these cases as follows:

$$\chi_D(a) = \begin{cases} \left(\frac{a}{|D|}\right) & \text{if } D \equiv 1 \pmod 4, \\ \left(\frac{-1}{a}\right)\left(\frac{a}{\left|\frac{D}{4}\right|}\right) & \text{if } \frac{D}{4} \equiv 3 \pmod 4, \\ \left(\frac{8}{a}\right)\left(\frac{a}{\left|\frac{D}{8}\right|}\right) & \text{if } \frac{D}{8} \equiv 1 \pmod 4, \\ \left(\frac{-8}{a}\right)\left(\frac{a}{\left|\frac{D}{8}\right|}\right) & \text{if } \frac{D}{8} \equiv 3 \pmod 4. \end{cases}$$

This proves χ_D is a Dirichlet characters modulo $|D|$. It is not hard to see that χ_D is primitive. Indeed, we have already mentioned that the characters $\left(\frac{-1}{a}\right)$, $\left(\frac{8}{a}\right)$, and $\left(\frac{-8}{a}\right)$ are all primitive. Since D, $\frac{D}{4}$, and $\frac{D}{8}$ are square-free according to their equivalences modulo 4 and $D \neq 1$, it suffices to show that χ_p is primitive for all primes p with $p \neq 2$ by Proposition 3.1.3. This is immediate since p is prime and χ_p is not principal.

We now show that every primitive quadratic Dirichlet character is of the form χ_D for some fundamental discriminant D. By Proposition 3.1.3 again, it suffices to consider primitive quadratic Dirichlet character modulo a prime power p^m.

First suppose $p \neq 2$. Then $(\mathbb{Z}/p^m\mathbb{Z})^*$ is cyclic, generated by say g, and every $a \in (\mathbb{Z}/p^m\mathbb{Z})^*$ is of the form $a = g^\nu$ for some $\nu \in (\mathbb{Z}/\varphi(p^m)\mathbb{Z})$. It follows that every corresponding Dirichlet character χ is of the form

$$\chi(a) = e^{\frac{2\pi i k\nu}{\varphi(p^m)}},$$

for an integer k modulo $\varphi(p^m)$. Moreover, χ is primitive if and only if $k \not\equiv 0 \pmod p$ for otherwise χ is a Dirichlet character modulo p^{m-1}. Similarly, χ is quadratic if and only if $k \equiv \frac{\varphi(p^m)}{2} \pmod{\varphi(p^m)}$. Such a k exists and is unique because $p \neq 2$. We also see that if χ is quadratic then it is imprimitive unless $m = 1$ for then $\varphi(p) = p - 1$ which is not a multiple of p. To summarized, there is a unique quadratic Dirichlet character modulo p^m and it is primitive if and only if $m = 1$. Necessarily, this unique primitive quadratic Dirichlet character modulo p is given by χ_D for the fundamental discriminant $D = p$ if $p \equiv 1 \pmod 4$ and $D = -p$ if $p \equiv 3 \pmod 4$.

Now suppose $p = 2$ so that $p^m = 2^m$. If $m = 1$ then $\varphi(2) = 1$ and there are no primitive quadratic Dirichlet characters as the only Dirichlet character is principal. If $m = 2$ then $\varphi(4) = 2$ so that there are two Dirichlet characters. They are both quadratic but only one is primitive namely the aforementioned $\left(\frac{-1}{a}\right)$. This primitive quadratic Dirichlet character is given by χ_D for the fundamental discriminant $D = -4$. For $m \geq 3$ there is an isomorphism $(\mathbb{Z}/2^m\mathbb{Z})^* \cong C_2 \times C_{2^{m-2}}$ where C_2 and $C_{2^{m-2}}$ are the cyclic groups of order 2 and 2^{m-2} respectively. Therefore every $a \in (\mathbb{Z}/2^m\mathbb{Z})^*$ is of the form $a = (-1)^\mu 5^\nu$ for some $\mu \in \mathbb{Z}/2\mathbb{Z}$ and $\nu \in \mathbb{Z}/2^{m-2}\mathbb{Z}$. Then every corresponding Dirichlet character χ is of the form

$$\chi(a) = e^{\frac{2\pi i j\mu}{2}} e^{\frac{2\pi i k\nu}{2^{m-2}}},$$

for integers j modulo 2 and k modulo 2^{m-2}. Similarly to the case for $p \neq 2$, χ is primitive if and only if $k \not\equiv 0 \pmod{2^{m-2}}$. Moreover, χ is quadratic if and only if $k \equiv 0 \pmod{2^{m-3}}$. These congruences together imply that a primitive quadratic Dirichlet character exists if and only if $m = 3$. In this case there are four Dirichlet characters. They are all quadratic but only two are primitive, namely the aforementioned $\left(\frac{8}{a}\right)$ and $\left(\frac{-8}{a}\right)$. These two primitive quadratic Dirichlet characters are given by χ_D for the fundamental discriminants $D = 8$ and $D = -8$ respectively. $\square$

It follows from Theorem 3.2.1 that all quadratic Dirichlet characters are induced from some χ_D including $D = 1$ since this corresponds to the trivial Dirichlet character. In particular, so too are the quadratic Dirichlet characters given by Jacobi symbols.

3.3 Ramanujan and Gauss Sums

For integers b and m with m positive, the *Ramanujan sum* $r(b, m)$ is defined by

$$r(b, m) = \sum_{\substack{a \pmod m \\ (a,m)=1}} e^{\frac{2\pi i ab}{m}}.$$

The Ramanujan sum is a finite sum of m-th roots of unity. When $b \mid m$ the summands are all 1 and the Ramanujan sum has the simple evaluation

$$r(b, m) = \varphi(m).$$

For a general idex the Ramanujan sums can be computed explicitly by means of the Möbius function.

Proposition 3.3.1. *For integers b and m with m positive, we have*

$$r(b, m) = \sum_{d \mid (b,m)} d\mu\left(\frac{m}{d}\right).$$

Proof. The identity is obvious if $m = 1$ since the Ramanujan sum is 1. So assume $m > 1$. Every a modulo m is of the form $a = a'd$ for some divisor d of m and a' modulo $\frac{m}{d}$ with $\left(a', \frac{m}{d}\right) = 1$. So summing $r(b,d)$ over the divisors d of m gives

$$\sum_{d|m} r(b,d) = \sum_{a \pmod m} e^{\frac{2\pi iab}{m}},$$

If $m \mid b$ the latter sum is m while if $m \nmid b$ the sum vanishes as it is the sum of all m-th roots of unity. Thus

$$\sum_{d|m} r(b,d) = \begin{cases} m & \text{if } m \mid b, \\ 0 & \text{if } m \nmid b. \end{cases}$$

Now apply Möbius inversion. □

More general Ramanujan sums can be constructed by introducing a Dirichlet character. Let χ be a Dirichlet character modulo m. For any integer b, the *Ramanujan sum* $\tau(n,\chi)$ associated to χ is given by

$$\tau(b,\chi) = \sum_{a \pmod m} \chi(a)e^{\frac{2\pi iab}{m}}.$$

This generalizes the previous Ramanujan sum as

$$r(b,m) = \tau(b, \chi_{m,0}).$$

When $b \mid m$ the summands are all 1 and the Dirichlet orthogonality relations imply

$$\tau(b,\chi) = \varphi(m)\delta_{\chi,\chi_{m,0}}.$$

When $b = 1$ we simply write $\tau(\chi) = \tau(1,\chi)$ and call $\tau(\chi)$ the *Gauss sum* associated to χ. The following proposition develops the basic properties of these Ramanujan sums:

Proposition 3.3.2. *Let χ and ψ be nontrivial Dirichlet characters modulo m and n respectively and let b be an integer. Then the following properties hold:*

(i) $\overline{\tau(b,\overline{\chi})} = \chi(-1)\tau(b,\chi)$.

(ii) If $(b,m) = 1$ then $\tau(b,\chi) = \overline{\chi}(b)\tau(\chi)$.

(iii) If $(b,m) > 1$ and χ is primitive then $\tau(b,\chi) = 0$.

(iv) If $(m,n) = 1$ then $\tau(b,\chi\psi) = \chi(n)\psi(m)\tau(b,\chi)\tau(b,\psi)$.

(v) If $\widetilde{\chi}$ is the primitive Dirichlet character of conductor q inducing χ, then

$$\tau(\chi) = \mu\left(\frac{m}{q}\right)\widetilde{\chi}\left(\frac{m}{q}\right)\tau(\widetilde{\chi}).$$

Proof. We will prove the properties separately.

(i) This follows by direct computation.

(ii) This follows by direct computation.

(iii) Let c be an integer with $(c, m) = 1$ and satisfying $\chi(c) \neq 1$. Such a c exists because otherwise χ the principal Dirichlet character modulo m and thus imprimitive. A short computation shows

$$\chi(c)\tau(b, \chi) = \tau(b, \chi),$$

whence $\tau(b, \chi) = 0$.

(iv) Since $(m, n) = 1$, the Chinese remainder theorem implies that any a modulo mn is of the form $a = a'n + a''m$ with a' modulo m and a'' modulo n. Whence

$$(\chi\psi)(a) = \chi(a'n)\psi(a''m).$$

Using this fact, a short computation shows

$$\sum_{a \pmod{mn}} (\chi\psi)(a)e^{\frac{2\pi iab}{mn}} = \chi(n)\psi(m)$$

$$\cdot \left(\sum_{a' \pmod{m}} \chi(a')e^{\frac{2\pi iab}{m}} \right) \left(\sum_{a'' \pmod{n}} \psi(a'')e^{\frac{2\pi ia''b}{n}} \right),$$

which is equivalent to the claim.

(v) First consider the case when $\left(\frac{m}{q}, q\right) = 1$. In view of $\chi = \widetilde{\chi}\chi_{\frac{m}{q},0}$, we use (iv) to obtain

$$\tau(\chi) = \tau(\chi_{\frac{m}{q},0})\widetilde{\chi}\left(\frac{m}{q}\right)\tau(\widetilde{\chi}).$$

As $\tau(\chi_{\frac{m}{q},0}) = r\left(1, \frac{m}{q}\right)$, we use Proposition 3.3.1 to compute $\tau(\chi_{\frac{m}{q},0}) = \mu\left(\frac{m}{q}\right)$. Whence

$$\tau(\chi) = \mu\left(\frac{m}{q}\right)\widetilde{\chi}\left(\frac{m}{q}\right)\tau(\widetilde{\chi}).$$

Now suppose $\left(\frac{m}{q}, q\right) > 1$. In this case the right-hand side is zero because $\widetilde{\chi}\left(\frac{m}{q}\right) = 0$. So we must show $\tau(\chi) = 0$. Now there exists a prime p with $p \mid \frac{m}{q}$ and $p \mid q$. For any a modulo m write $a = a'\frac{m}{p} + a''$ with a' modulo p and a'' modulo $\frac{m}{p}$. Moreover, as $p \mid \frac{m}{q}$ we know $q \mid \frac{m}{p}$. These two facts and a short computation together show

$$\tau(\chi) = \left(\sum_{a' \pmod{p}} e^{\frac{2\pi ia'}{p}} \right) \left(\sum_{a'' \pmod{\frac{m}{p}}} \widetilde{\chi}(a'')e^{\frac{2\pi ia''}{m}} \right).$$

The first sum vanishes since it is the sum of all p-th roots of unity. This proves $\tau(\chi) = 0$. $\square$

These properties help to reduce the evaluation of Ramanujan and Gauss sums. However, even evaluating Gauss sums for arbitrary primitive Dirichlet characters is a very difficult problem much of which is still open. Yet it is not difficult to determine the modulus of the Gauss sum when χ is primitive.

Theorem 3.3.3. *Let χ be a primitive Dirichlet character of conductor q. Then*

$$|\tau(\chi)| = \sqrt{q}.$$

Proof. If χ is the trivial Dirichlet character the claim is obvious since the Gauss sum is 1. So assume χ is nontrivial whence $q > 1$. Consider instead $|\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)}$. Expanding the Gauss sum $\overline{\tau(\chi)}$ and invoking Proposition 3.3.2 (ii), a short computation shows

$$|\tau(\chi)|^2 = \sum_{a \pmod q} \tau(a, \chi) e^{-\frac{2\pi i a}{q}}.$$

Upon expanding the Ramanujan sum, another short computation gives

$$|\tau(\chi)|^2 = \sum_{a' \pmod q} \chi(a') \left(\sum_{a \pmod q} e^{\frac{2\pi i a(a'-1)}{q}} \right).$$

If $a' \equiv 1 \pmod q$ the inner sum is q and otherwise vanishes as it is the sum of all q-th roots of unity. It follows that the double sum is q whence $|\tau(\chi)|^2 = q$. This is equivalent to the claim. $\square$

As an almost immediate corollary, we deduce a useful expression for primitive Dirichlet characters as exponential sums.

Corollary 3.3.4. *Let χ be a primitive Dirichlet character of conductor q. Then for any integer b, we have*

$$\tau(b, \chi) = \overline{\chi}(b)\tau(\chi).$$

In particular,

$$\chi(b) = \frac{1}{\tau(\overline{\chi})} \sum_{a \pmod q} \overline{\chi}(a) e^{\frac{2\pi i a b}{q}}.$$

Proof. For the first statement, the identity is obvious if χ is the trivial character as the Ramanujan sum is 1. So assume χ is nontrivial. If $(b, q) = 1$ then this is exactly Proposition 3.3.2 (ii). If $(b, q) > 1$ then the identity follows from Proposition 3.3.2 (iii) and that $\overline{\chi}(b) = 0$. This proves the first statement in full. For the second statement, observe that $\tau(\chi) \neq 0$ by Theorem 3.3.3. The second identity follows upon replacing χ with $\overline{\chi}$, dividing by $\tau(\chi)$, and expanding the Ramanujan sum. $\square$

For a Dirichlet character χ modulo m, we define the *epsilon factor* ε_χ by

$$\varepsilon_\chi = \frac{\tau(\chi)}{\sqrt{m}}.$$

When χ is primitive, the epsilon factor lies on the unit circle by Theorem 3.3.3. The question of the evaluation of Gauss sums, and hence Ramanujan sums, boils down to determining what value the epsilon factor is. This is the real difficultly in evaluating Gauss sums. However, when χ is primitive there is a simple relationship between the epsilon factors ε_χ and $\varepsilon_{\overline{\chi}}$:

Proposition 3.3.5. *Let χ be a primitive Dirichlet character of conductor q. Then*

$$\varepsilon_\chi \varepsilon_{\overline{\chi}} = \chi(-1).$$

Proof. If χ is trivial this is obvious since both epsilon factors are 1. So assume χ is nontrivial. On the one hand, $\varepsilon_{\overline{\chi}}$ lies on the unit circle so that

$$\varepsilon_{\overline{\chi}}^{-1} = \frac{\overline{\tau(\chi)}}{\sqrt{q}}.$$

On the other hand, Proposition 3.3.2 (i) implies

$$\varepsilon_\chi = \chi(-1)\frac{\overline{\tau(\chi)}}{\sqrt{q}}.$$

Combining these identities gives the result. □

3.4 Quadratic Gauss Sums

Our primary aim will be to evaluate the epsilon factor of the Gauss sum for quadratic Dirichlet characters defined by Jacobi symbols. To accomplish this we will study and auxiliary exponential sum. For integers b and m with m positive, the *quadratic Gauss sum* $g(b, m)$ is defined by

$$g(b, m) = \sum_{a \pmod{m}} e^{\frac{2\pi i a^2 b}{m}}.$$

When $b \mid m$ the summands are all 1 and the quadratic Gauss sum evaluates to

$$g(b, m) = m.$$

If $b = 1$ we write $g(m) = g(1, m)$. It turns out that for square-free m the Ramanujan sum attached to the quadratic Dirichlet character modulo m given by the Jacobi symbol is precisely the quadratic Gauss sum. This takes some work to prove. The first step is to reduce to the case when $(b, m) = 1$.

Proposition 3.4.1. *Let b and m be integers with m positive. Then*

$$g(b, m) = (b, m)g\left(\frac{b}{(b, m)}, \frac{m}{(b, m)}\right).$$

Proof. Any a modulo m is of the form $a = a'\frac{m}{(b,m)} + a''$ with a' modulo (b,m) and a'' modulo $\frac{m}{(b,m)}$. A short computation shows

$$\sum_{a \pmod m} e^{\frac{2\pi i a^2 b}{m}} = (b,m) \sum_{a'' \pmod{\frac{m}{(b,m)}}} e^{\frac{2\pi i (a'')^2 \frac{b}{(b,m)}}{\frac{m}{(b,m)}}}.$$

The remaining sum is exactly $g\left(\frac{b}{(b,m)}, \frac{m}{(b,m)}\right)$ and the desired identity follows. $\square$

The second step is to deduce an equivalent formulation of the Ramanujan sum associated to quadratic Dirichlet characters given by Jacobi symbols. This will imply equivalence between the aforementioned exponential sums when the modulus is an odd prime.

Proposition 3.4.2. *Let b and m be integers with m positive, odd, and such that $(b,m) = 1$. Let χ_m be the quadratic Dirichlet character modulo m given by the Jacobi symbol. Then*

$$\tau(b, \chi_m) = \sum_{a \pmod m} \left(1 + \left(\frac{a}{m}\right)\right) e^{\frac{2\pi i ab}{m}}.$$

When $m = p$ is prime,

$$\tau(b, \chi_p) = g(b,p).$$

Proof. The first statement is obvious when $m = 1$ since the Ramanujan sum is 1. So assume $m > 1$. Now write the sum as

$$\sum_{a \pmod m} e^{\frac{2\pi i ab}{m}} + \sum_{a \pmod m} \left(\frac{a}{m}\right) e^{\frac{2\pi i ab}{m}}.$$

The first sum vanishes as it is the sum of all m-th roots of unity. This proves the first identity. Now let $m = p$ be an odd prime. Then

$$1 + \left(\frac{a}{p}\right) = \begin{cases} 2 & \text{if } a \text{ is a quadratic residue modulo } p, \\ 0 & \text{if } a \text{ is not quadratic residue modulo } p, \\ 1 & \text{if } p \mid a. \end{cases}$$

Moreover, when a is a quadratic residue modulo p there exists an a' modulo p with $a \equiv (a')^2 \pmod p$. As there are $\frac{p-1}{2}$ such residues, the first statement implies

$$\tau(b, \chi_p) = 1 + \sum_{\substack{a' \pmod p \\ a \nmid 0}} e^{\frac{2\pi i (a')^2 b}{p}}.$$

This is exactly $g(b,p)$ which proves the second statement. $\square$

The third step is to generalize the second statement in Proposition 3.4.2 for square-free m. To accomplish this we will need to develop some properties of quadratic Gauss sums.

Proposition 3.4.3. *Let b, m, and n be integers with m and n positive and let p be an odd prime Then the following properties hold:*

(i) *If $(b,p)=1$ then $g(b,p^r)=pg(b,p^{r-2})$ provided $r\geq 2$.*

(ii) *If $(m,n)=1$ and $(b,mn)=1$ then $g(b,mn)=g(bn,m)g(bm,n)$.*

(iii) *If m is odd and $(b,m)=1$ then $g(b,m)=\left(\frac{b}{m}\right)g(m)$ where $\left(\frac{b}{m}\right)$ is the Jacobi symbol.*

Proof. We will prove the properties separately.

(i) Every a modulo p satisfies $(a,p)=1$ or is a multiple of p. Whence

$$g(b,p^r)=\sum_{\substack{a \pmod{p^r}\\(a,p)=1}} e^{\frac{2\pi i a^2 b}{p^r}}+\sum_{a \pmod{p^{r-1}}} e^{\frac{2\pi i a^2 b}{p^{r-2}}},$$

since every a modulo p satisfies $(a,p)=1$ or not. Every a modulo p^{r-1} is of the form $a=a'p^{r-2}+a''$ with a' modulo p and a'' modulo p^{r-2}. A short computation shows

$$\sum_{a \pmod{p^{r-1}}} e^{\frac{2\pi i a^2 b}{p^{r-2}}}=p\sum_{a'' \pmod{p}} e^{\frac{2\pi i (a'')^2 b}{p^{r-2}}}.$$

The remaining sum is exactly $g(b,p^{r-2})$. So it suffices to show that the first sum vanishes. This sum is exactly $r(b,p^r)$ and Proposition 3.3.1 implies $r(b,p^r)=\mu(p^r)$ which is zero as $r\geq 2$.

(ii) Since $(m,n)=1$, the Chinese remainder theorem implies that any a modulo mn is of the form $a=a'n+a''m$ with a' modulo m and a'' modulo n. Whence

$$\left(\sum_{a' \pmod{m}} e^{\frac{2\pi i (a')^2 bn}{m}}\right)\left(\sum_{a'' \pmod{n}} e^{\frac{2\pi i (a'')^2 bm}{n}}\right)=\sum_{a \pmod{mn}} e^{\frac{2\pi i a^2 b}{mn}}.$$

This is equivalent to the claim.

(iii) The claim is obvious if $m=1$ because the quadratic Gauss sum is 1. So assume $m>1$. By multiplicativity of the Jacobi symbol and (ii), it suffices to prove the claim when $m=p^r$ is an odd prime power. The case when $r=1$ follows from Proposition 3.4.2, Proposition 3.3.2 (ii), and that quadratic Dirichlet characters are their own conjugates. The case when $r\geq 2$ follows by induction using (i). $\square$

At last we can prove our Ramanujan and quadratic Gauss sums agree.

Theorem 3.4.4. *Suppose m is a square-free positive odd integer and let χ_m be the quadratic Dirichlet character modulo m given by the Jacobi symbol. Then for any integer b with $(b,m)=1$, we have*

$$\tau(b,\chi_m)=g(b,m).$$

Proof. The claim is obvious if $m = 1$ because the Ramanujan and Gauss sums are both 1. So suppose $m > 1$. It suffices to assume $b = 1$ by Proposition 3.3.2 (ii), Proposition 3.4.3 (iii), and that quadratic Dirichlet characters are their own conjugates. Let $m = p_1 p_2 \cdots p_k$ be the prime decomposition of m. Repeated application of Proposition 3.3.2 (iv) shows

$$\tau(\chi) = \left(\prod_{i<j} \chi_{p_j}(p_i)\chi_{p_i}(p_j)\right)\left(\prod_i \tau(\chi_{p_i})\right).$$

By Proposition 3.4.2, we may write

$$\left(\prod_{i<j} \chi_{p_j}(p_i)\chi_{p_i}(p_j)\right)\left(\prod_i \tau(\chi_{p_i})\right) = \left(\prod_{i<j} \left(\frac{p_i}{p_j}\right)\left(\frac{p_j}{p_i}\right)\right)\left(\prod_i g(p_i)\right).$$

Repeated application of Proposition 3.4.3 (ii) gives

$$\left(\prod_{i<j} \left(\frac{p_i}{p_j}\right)\left(\frac{p_j}{p_i}\right)\right)\left(\prod_i g(p_i)\right) = g(m).$$

This completes the proof. □

The properties in Proposition 3.4.3 help to reduce the evaluation of quadratic Gauss sums. Thankfully, it is possible to completely evaluate quadratic Gauss sums when $b = 1$ and therefore even some Ramanujan sums. As with the Gauss sum, we first deduce a fact about the modulus.

Theorem 3.4.5. *Let m be a positive odd integer. Then*

$$|g(m)| = \sqrt{m}.$$

Proof. The claim is obvious if $m = 1$ because the quadratic Gauss sum is 1. So assume $m > 1$. By Proposition 3.4.3 (ii) and (iii), it suffices to prove the claim when $m = p^r$ is an odd prime power. The case when $r = 1$ follows from Theorems 3.3.3 and 3.4.4. The case when $r \geq 2$ is proved by induction and Proposition 3.4.3 (i). □

For any integer m, we define the *epsilon factor* ε_m by

$$\varepsilon_m = \frac{g(m)}{\sqrt{m}}.$$

Theorem 3.4.5 says that this value lies on the unit circle when m is odd. This evaluation of these epsilon factors was completely resolved by Gauss in 1808. Modern proofs use analytic techniques by expressing $g(m)$ in a form where Poisson summation can be applied.

Theorem 3.4.6. *Let $m \geq 1$. Then*

$$\varepsilon_m = \begin{cases} (1+i) & \text{if } m \equiv 0 \pmod 4, \\ 1 & \text{if } m \equiv 1 \pmod 4, \\ 0 & \text{if } m \equiv 2 \pmod 4, \\ i & \text{if } m \equiv 3 \pmod 4. \end{cases}$$

Proof. The aim is to express $g(m)$ as a periodic sum over $\mathbb{Z}$ whose summands are compactly supported functions of bounded variation. For then we can apply Poisson summation to evaluate the sum in an alternative manner. To this end, consider the function

$$f(x) = \begin{cases} e^{\frac{2\pi i x^2}{m}} & \text{if } x \in [0, m], \\ 0 & \text{if } x \notin [0, m]. \end{cases}$$

Then $f(x)$ is of bounded variation with compact support and has jump discontinuities only at $x = 0$ and $x = m$. Therefore Poisson summation applies where $f(n)$ is understood to be the average of the left-hand and right-hand limits at points of discontinuity and the sums are ordered symmetrically with respect to the size of the index. On the one hand, this means

$$\sum_{n \in \mathbb{Z}} f(n) = g(m).$$

On the other hand, Poisson summation gives

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{t \in \mathbb{Z}} \sqrt{m} e^{-\frac{2\pi i t^2 m}{4}} \int_{\frac{t\sqrt{m}}{2}}^{\sqrt{m} + \frac{t\sqrt{m}}{2}} e^{2\pi i x^2} \, dx.$$

As $t \equiv 0, 1 \pmod 4$ according to if t is even or odd, the subsums according to this parity are

$$\sqrt{m} \int_{-\infty}^{\infty} e^{2\pi i x^2} \, dx \quad \text{and} \quad \sqrt{m} e^{-\frac{2\pi i m}{4}} \int_{-\infty}^{\infty} e^{2\pi i x^2} \, dx,$$

respectively. As the sum is ordered with respect to this parity, we have

$$\sum_{n \in \mathbb{Z}} f(n) = \sqrt{m} \left(1 + e^{-\frac{2\pi i m}{4}}\right) \int_{-\infty}^{\infty} e^{2\pi i x^2} \, dx.$$

Equating our two expressions gives

$$g(m) = \sqrt{m} \left(1 + e^{-\frac{2\pi i m}{4}}\right) \int_{-\infty}^{\infty} e^{2\pi i x^2} \, dx.$$

To compute the remaining integral we take $m = 1$. As the Gauss sum is 1 and $e^{-\frac{2\pi i}{4}} = -i$, we find that

$$\int_{-\infty}^{\infty} e^{2\pi i x^2} \, dx = \frac{1}{1-i}.$$

Therefore

$$\varepsilon_m = \frac{1+e^{-\frac{2\pi i m}{4}}}{1-i} = \begin{cases} (1+i) & \text{if } m \equiv 0 \pmod 4, \\ 1 & \text{if } m \equiv 1 \pmod 4, \\ 0 & \text{if } m \equiv 2 \pmod 4, \\ i & \text{if } m \equiv 3 \pmod 4, \end{cases}$$

as desired. □

As an immediate corollary, we can evaluate the epsilon factor ε_{χ_p} for the quadratic Dirichlet character χ_p modulo p given by the Jacobi symbol when p is an odd prime.

Corollary 3.4.7. *Let p be an odd prime and χ_p be the quadratic Dirichlet character modulo p given by the Jacobi symbol. Then*

$$\varepsilon_{\chi_p} = \begin{cases} 1 & \textit{if } p \equiv 1 \pmod 4, \\ i & \textit{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. The claim follows immediately from Theorem 3.4.6 and Proposition 3.4.2. □

Part II

Algebraic Number Theory

Chapter 4

Todo: [Algebraic Integers]

Chapter 5

Todo: [Ramification]

Chapter 6

Todo: [Geometry of Numbers]

Part III

Analytic Number Theory

Chapter 7

Dirichlet Series

Throughout, $s = \sigma + it$ and $s_0 = \sigma_0 + it_0$ will stand for complex variables with σ, σ_0, t, and t_0 real.

7.1 Convergence Properties

A *Dirichlet series* $D(s)$ is a sum of the form

$$D(s) = \sum_{n\geq 1} \frac{a(n)}{n^s},$$

with $a(n) \in \mathbb{C}$. Our first aim is to understand where Dirichlet series converge and where they converge absolutely. It does not take much for $D(s)$ to converge uniformly in a sector.

Theorem 7.1.1. *Suppose $D(s)$ is a Dirichlet series that converges at $s_0 = \sigma_0 + it_0$. Then for any $H > 0$, $D(s)$ converges uniformly in the sector*

$$\{s \in \mathbb{C} : \sigma \geq \sigma_0 \text{ and } |t - t_0| \leq H(\sigma - \sigma_0)\}.$$

In particular, $D(s)$ converges in the half-plane $\sigma > \sigma_0$.

Proof. Write $R(u) = \sum_{n\geq u} \frac{a(n)}{n^{s_0}}$ for the tail of $D(s_0)$ so that

$$\frac{a(n)}{n^{s_0}} = (R(n) - R(n+1)).$$

Then for positive integers N and M with $M \leq N$, summation by parts implies

$$\sum_{M\leq n\leq N} \frac{a(n)}{n^s} = R(M)M^{s_0-s} - R(N+1)(N+1)^{s_0-s} - \sum_{M\leq n\leq N} R(n+1)(n^{s_0-s} - (n+1)^{s_0-s}).$$

We will express the sum on the right-hand side as an integral. To do this, observe that

$$n^{s_0-s} - (n+1)^{s_0-s} = -(s_0 - s) \int_n^{n+1} u^{s_0-s-1}\, du.$$

As $R(u)$ is constant on the interval $(n, n+1]$ a short computation shows

$$\sum_{M \leq n \leq N} R(n+1)(n^{s_0-s} - (n+1)^{s_0-s}) = -(s_0 - s)\int_M^{N+1} R(u)u^{s_0-s-1}\,du,$$

Whence

$$\sum_{M \leq n \leq N} \frac{a(n)}{n^s} = R(M)M^{s_0-s} - R(N+1)(N+1)^{s_0-s} + (s_0 - s)\int_M^{N+1} R(u)u^{s_0-s-1}\,du.$$

As $D(s)$ converges at $s = s_0$, we can choose M sufficiently large such that $|R(u)| < \varepsilon$ for all $u \geq M$. It follows that $|R(u)u^{s_0-s}| < \varepsilon$ for all such u provided s in the desired sector. For such s, we have

$$|s - s_0| \leq (\sigma - \sigma_0) + |t - t_0| \leq (H+1)(\sigma - \sigma_0).$$

These estimates together imply

$$\sum_{M \leq n \leq N} \frac{a(n)}{n^s} = O\left(2\varepsilon + \varepsilon(H+1)(\sigma - \sigma_0)\int_M^{N+1} u^{\sigma_0-\sigma-1}\,du\right).$$

Since the integral is $O\left(\frac{1}{\sigma - \sigma_0}\right)$, the sum is $o(1)$ for s in the desired sector. The first statement follows by uniform Cauchy's criterion. Taking the limit as $H \to \infty$ proves the second statement. $\square$

We will want to keep track of where Dirichlet series converge absolutely. Let σ_c be the infimum of all σ for which $D(s)$ converges. We call σ_c the *abscissa of convergence* of $D(s)$. Similarly, let σ_a be the infimum of all σ for which $D(s)$ converges absolutely. We call σ_a the *abscissa of absolute convergence* of $D(s)$. As the summands of $D(s)$ are holomorphic, the convergence is locally absolutely uniform for $\sigma > \sigma_a$ (actually uniform in sectors) and so $D(s)$ is holomorphic in this half-plane.

The abscissas σ_c and σ_a act as the boundaries of convergence and absolute convergence respectively. Anything can happen on the lines $\sigma = \sigma_c$ and $\sigma = \sigma_a$, but to the right of them we have convergence and absolute convergence of $D(s)$ respectively. It turns out that σ_a is never far from σ_c provided σ_c is finite.

Theorem 7.1.2. *If $D(s)$ is a Dirichlet series with finite abscissa of convergence σ_c then*

$$\sigma_c \leq \sigma_a \leq \sigma_c + 1.$$

Proof. The first inequality is clear since absolute convergence implies convergence. For the second inequality, the terms $a(n)n^{-(\sigma_c+\varepsilon)}$ tend to zero as $n \to \infty$ because $D(s)$ converges at $s = \sigma_c + \varepsilon$. Therefore $a(n) \ll_\varepsilon n^{\sigma_c+\varepsilon}$ and so $D(s)$ is absolutely convergent at $s = \sigma_c + 1 + 2\varepsilon$. This means $\sigma_a \leq \sigma_c + 1 + 2\varepsilon$. Taking the limit as $\varepsilon \to 0$ gives the second inequality. $\square$

We now turn to the question of uniqueness of Dirichlet series. In particular, we would like to show that Dirichlet series are uniquely determined by their coefficient as this would allow us compare coefficient analogous to that of Taylor series. This is indeed possible.

Proposition 7.1.3. *Suppose $D(s)$ is a Dirichlet series with finite abscissa of convergence σ_c such that*

$$D(s) = \sum_{n\geq1} \frac{a(n)}{n^s} \quad \text{and} \quad D(s) = \sum_{n\geq1} \frac{b(n)}{n^s}.$$

Then $a(n) = b(n)$ for all n.

Proof. Set $c(n) = a(n) - b(n)$. Then it suffices to prove $c(n) = 0$ for all n and we will do so by induction. Take $\sigma \geq \sigma_a$ so that $D(s)$ converges absolutely. Letting $\sigma \to \infty$, the dominated convergence theorem implies

$$\lim_{\sigma\to\infty} D(\sigma) = a(1) \quad \text{and} \quad \lim_{\sigma\to\infty} D(\sigma) = b(1).$$

Whence $c(1) = 0$. Assume by induction that $c(n) = 0$ for $n \leq N$ and consider the Dirichlet series

$$\sum_{n\geq1} \frac{c(n)}{n^s}.$$

Its abscissa of absolute convergence is σ_a. As

$$\sum_{n>N} \frac{c(n)}{n^s} = 0,$$

by assumption, it follows that

$$c(N+1) = -\sum_{n>N} c(n) \left(\frac{N}{n}\right)^{\sigma}.$$

Letting $\sigma \to \infty$, the dominated convergence theorem implies

$$\lim_{\sigma\to\infty} \left(-\sum_{n>N} c(n) \left(\frac{N}{n}\right)^{\sigma}\right) = 0.$$

Hence $c(N+1) = 0$ which completes the proof. $\square$

We will now introduce several resulting concerning the growth and average growth of the coefficients of a Dirichlet series. For legibility, it will be useful to introduce some notation. If $D(s)$ is a Dirichlet series with coefficients $a(n)$ then for $X > 0$, we set

$$A(X) = \sum_{n\leq X} a(n) \quad \text{and} \quad |A|(X) = \sum_{n\leq X} |a(n)|.$$

These are the partial sums of the coefficients $a(n)$ and their absolute values up to X respectively. Many of our results will be in terms of these sums. Our first result shows that the coefficients of a Dirichlet series grown at most polynomially provided the Dirichlet series converges absolutely at some point.

Proposition 7.1.4. *Suppose $D(s)$ is a Dirichlet series with coefficients $a(n)$ that converges absolutely at $s = \alpha$ for some real α. Then*

$$a(n) \ll_\varepsilon n^{\alpha+\varepsilon}.$$

In particular, if $D(s)$ has finite abscissa of absolute convergence σ_a then

$$a(n) \ll_\varepsilon n^{\sigma_a+\varepsilon}.$$

Proof. Necessarily $\sigma_a \leq \alpha$ and so $D(s)$ converges absolutely in the half-plane $\sigma > \alpha$. Write

$$|a(n)| \leq n^{\alpha+\varepsilon} \sum_{n\geq 1} \frac{|a(n)|}{n^{\alpha+\varepsilon}}.$$

The sum is $O_\varepsilon(1)$ because $D(s)$ is absolutely convergent for $\sigma > \alpha$. The first estimate follows at once. The second is immediate from the first and the definition of the abscissa of absolute convergence. □

It is natural to be curious about the converse, namely, is it possible to determine an upper bound on the abscissa of absolute convergence if we know a polynomial bound for the coefficients. This is indeed possible.

Proposition 7.1.5. *Suppose $D(s)$ is a Dirichlet series whose coefficients satisfy the estimate $a(n) \ll_\alpha n^\alpha$ for some real α. Then the abscissa of absolute convergence satisfies $\sigma_a \leq \alpha + 1$.*

Proof. Let $\sigma > \alpha + 1$. It suffices to show convergence of the series

$$\sum_{n\geq 1} \frac{|a(n)|}{n^\sigma}.$$

As

$$\sum_{n\geq 1} \frac{|a(n)|}{n^\sigma} \ll_\alpha \sum_{n\geq 1} \frac{1}{n^{\sigma-\alpha}},$$

and the latter series converges, the proof is complete. □

Let us now turn to the same questions but using averages of the coefficients. Our first result is analogous to Proposition 7.1.4.

Proposition 7.1.6. *Suppose $D(s)$ is a Dirichlet series with coefficients $a(n)$ that converges absolutely at $s = \alpha$ for some real α. Then*

$$A(X) \ll X^{\alpha+\varepsilon} \quad \textit{and} \quad |A|(X) \ll X^{\alpha+\varepsilon}.$$

In particular,

$$A(X) \ll_\varepsilon X^{\sigma_a+\varepsilon} \quad \textit{and} \quad |A|(X) \ll_\varepsilon X^{\sigma_a+\varepsilon}.$$

Proof. Necessarily $\sigma_a \leq \alpha$ and so $D(s)$ converges absolutely in the half-plane $\sigma > \alpha$. Write

$$\sum_{n \leq X} |a(n)| \leq X^{\alpha+\varepsilon} \sum_{n \geq 1} \frac{|a(n)|}{n^{\alpha+\varepsilon}}.$$

The sum is $O_\varepsilon(1)$ because $D(s)$ is absolutely convergent for $\sigma > \alpha$. As $A(x) \ll |A|(x)$, the first statement follows at once. The second is immediate from the first and the definition of the abscissa of absolute convergence. $\square$

It turns out that if $A(X)$ is bounded then σ_c is negative.

Proposition 7.1.7. *Suppose $D(s)$ is a Dirichlet series and that $A(X) \ll 1$. Then $\sigma_c \leq 0$.*

Proof. Let $\sigma > 0$. Abel summation gives

$$\sum_{n \leq X} \frac{a(n)}{n^s} = \frac{A(X)}{X^s} + \int_1^X A(u)u^{-(s-1)}\, du.$$

As $A(X) \ll 1$, take the limit as $X \to \infty$ to obtain

$$D(s) = s\int_1^\infty A(u)u^{-(s+1)}\, du.$$

This expresses $D(s)$ as an integral. Direct evaluation shows that the integral is finite. Therefore $D(s)$ converges for $\sigma > 0$ which means $\sigma_c \leq 0$. $\square$

Unfortunately, it is not often the case that $A(X)$ is bounded as this is quite a strong condition for most Dirichlet series. Fortunately, we can still obtain nice result analogous to that of Proposition 7.1.5 if we assume $|A|(X)$ grows at most polynomially.

Proposition 7.1.8. *Suppose $D(s)$ is a Dirichlet series such that $|A|(X) \ll_\alpha X^\alpha$ for some $\alpha \geq 0$. Then the abscissa of absolute convergence satisfies $\sigma_a \leq \alpha$.*

Proof. Let $\sigma > \alpha$. It suffices to show convergence of the series

$$\sum_{n \geq 1} \frac{|a(n)|}{n^\sigma}.$$

Abel summation gives

$$\sum_{n \leq X} \frac{|a(n)|}{n^\sigma} = \frac{|A|(X)}{X^\sigma} + \sigma\int_1^X |A|(u)u^{-(\sigma+1)}\, du.$$

In view of the bound $|A|(X) \ll_\alpha X^\alpha$, take the limit as $X \to \infty$ to obtain

$$\sum_{n \geq 1} \frac{|a(n)|}{n^\sigma} = \sigma\int_1^\infty |A|(u)u^{-(\sigma+1)}\, du.$$

Direct evaluation shows that the integral is bounded. Therefore our series is bounded and hence must converge. $\square$

Unfortunately, Proposition 7.1.8 does not immediately imply a sharper upper bound for the abscissa of absolute convergence than that of Proposition 7.1.5. This is because if $a(n) \ll_\alpha n^\alpha$ then the trivial bounds for $A(X)$ and $|A(X)|$ are

$$A(X) \ll_\alpha X^{\alpha+1} \quad \text{and} \quad |A|(X) \ll_\alpha X^{\alpha+1}.$$

In particular, using the second bound in Proposition 7.1.8 will give $\sigma_a \leq \alpha + 1$. So if we want to obtain sharper upper bounds for the abscissa of absolute convergence then we must improve the polynomial bound for the coefficients directly. Unfortunately, this is often a daunting task in practice especially if the Dirichlet series is connected to a deep algebraic or arithmetic object. However, if we assume that the coefficients are nonnegative then *Landau's theorem* provides a way of locating the abscissa of absolute convergence exactly:

Theorem (Landau's theorem). *Suppose $D(s)$ is a Dirichlet series with nonnegative coefficients $a(n)$ and finite abscissa of absolute convergence σ_a. Then σ_a is a singularity of $D(s)$.*

Proof. Replacing $a(n)$ by $a(n)n^{-\sigma_a}$, if necessary, we may assume $\sigma_a = 0$. Now suppose to the contrary that $D(s)$ was holomorphic at $s = 0$. Then $D(s)$ is holomorphic in the domain

$$\mathcal{D} = \{s \in \mathbb{C} : \sigma_a > 0\} \cup \{s \in \mathbb{C} : |s| < \delta\},$$

for some $\delta > 0$. Let $P(s)$ be the power series expansion of $D(s)$ at $s = 1$. Then

$$P(s) = \sum_{k \geq 0} \frac{c_k}{k!}(s-1)^k,$$

where

$$c_k = \sum_{n \geq 1} \frac{a(n)(-\log(n))^k}{n},$$

upon differentiating $D(s)$ termwise. The radius of convergence of $P(s)$ is the distance from $s = 1$ to the nearest singularity of $P(s)$. Since $P(s)$ is holomorphic on $\mathcal{D}$, the closest possible singularities are at $s = \pm i\delta$. Therefore, the radius of convergence is at least $\sqrt{1+\delta^2}$. Write $\sqrt{1+\delta^2} = 1 + \delta'$ for some $\delta' > 0$. Then for $|s-1| < 1 + \delta'$, $P(s)$ is holomorphic and can be expressed as

$$P(s) = \sum_{k \geq 0} \frac{(s-1)^k}{k!} \sum_{n \geq 1} \frac{a(n)(-\log(n))^k}{n}.$$

Now choose s in this region to be real with with $-\delta' < s < 1$. Then this double sum is a sum of positive terms by assumption of the $a(n)$ being nonnegative. As $P(s)$ is necessarily absolutely convergent, interchanging the sums and a short computation shows

$$P(s) = D(s).$$

As $-\delta' < s < 1$ and $D(s)$ has nonnegative coefficients, it converges absolutely for some $s < 0$. This contradicts $\sigma_a = 0$. $\square$

There is a very important distinction in Landau's theorem that abscissa of absolute convergence is a singularity and not just a point where the Dirichlet series does not converge. Indeed, this means that if $D(s)$ could be analytically continued to a region containing $\sigma = \sigma_a$ then the continuation must have a pole at $s = \sigma_a$. In particular, the abscissa of absolute convergence would then be a pole with the largest possible real part. This signals that the singularity is an inherent property of the analytic continuation and not one of the representation of the function as a Dirichlet series.

7.2 Euler Products

Generally speaking, if the coefficients $a(n)$ are chosen at random, $D(s)$ is not guaranteed to good properties outside of absolute convergence in some half-plane (provided it converges at a point). However, many Dirichlet series of interest will have coefficients that are multiplicative. These Dirichlet series admits product expressions.

Proposition 7.2.1. *Suppose $D(s)$ is a Dirichlet series with finite abscissa of absolute convergence σ_a and whose coefficients $a(n)$ are multiplicative. Then*

$$D(s) = \prod_p \left(\sum_{k \geq 0} \frac{a(p^k)}{p^{ks}} \right),$$

for $\sigma > \sigma_a$. If the prime power coefficients satisfy

$$a(p^k) = \sum_{1 \leq j_1 \leq \cdots \leq j_k \leq d} \alpha_{j_1}(p) \cdots \alpha_{j_k}(p),$$

for some $\alpha_1(p), \ldots, \alpha_d(p) \in \mathbb{C}$ and positive integer d, then the product takes the form

$$D(s) = \prod_p (1 - \alpha_1(p)p^{-s})^{-1} \cdots (1 - \alpha_d(p)p^{-s})^{-1}.$$

Proof. Let $\sigma > \sigma_a$ and consider the series

$$\sum_{k \geq 0} \frac{a(p^k)}{p^{ks}}.$$

This series converges absolutely because $D(s)$ does. Now let N be a positive integer. By absolute convergence and the fundamental theorem of arithmetic,

$$\prod_{p \leq N} \left(\sum_{k \geq 0} \frac{a(p^k)}{p^{ks}} \right) = \sum_{n \leq N} \frac{a(n)}{n^s} + \sum_{n > N}^{*} \frac{a(n)}{n^s},$$

where the $*$ indicates that we are summing over only those additional terms $\frac{a(n)}{n^s}$ that appear in the expanded product. As $N \to \infty$, the first sum on the right-hand side tends to $D(s)$ and the second sum tends to zero because it is part of the tail of $D(s)$.

This proves that the product converges and is equal to $D(s)$. If the prime power coefficients are of the form

$$a(p^k) = \sum_{1 \le j_1 \le \cdots \le j_k \le d} \alpha_{j_1}(p) \cdots \alpha_{j_k}(p),$$

then

$$\sum_{k \ge 0} \frac{a(p^k)}{p^{ks}} = (1 - \alpha_1(p)p^{-s})^{-1} \cdots (1 - \alpha_d(p)p^{-s})^{-1},$$

from which the product formula follows. $\square$

The representation

$$D(s) = \prod_p \left(\sum_{k \ge 0} \frac{a(p^k)}{p^{ks}} \right),$$

the called the *Euler product* of $D(s)$. By Proposition 7.2.1, multiplicativity of the coefficients is enough to ensure that the Euler product exists and is equal to the Dirichlet series in the half-plane of absolute convergence. If the Euler product takes the form

$$D(s) = \prod_p (1 - \alpha_1(p)p^{-s})^{-1} \cdots (1 - \alpha_d(p)p^{-s})^{-1},$$

then it is said to be of *degree* d. The special case of complete multiplicative coefficients corresponds to degree 1 Euler products as

$$D(s) = \prod_p (1 - a(p)p^{-s})^{-1}.$$

The condition

$$a(p^k) = \sum_{1 \le j_1 \le \cdots \le j_k \le d} \alpha_{j_1}(p) \cdots \alpha_{j_k}(p),$$

guarantees that the Dirichlet series has an Euler product of degree d.

Remark 7.2.2. Replacing $D(s)$ with its absolute series in Proposition 7.2.1 shows that

$$\sum_{n \ge 1} \frac{|a(n)|}{n^\sigma} = \prod_p \left(\sum_{k \ge 0} \frac{|a(p^k)|}{p^{k\sigma}} \right)$$

for $\sigma > \sigma_a$. Under the stronger assumption of an Euler product of degree d this identity becomes

$$\sum_{n \ge 1} \frac{|a(n)|}{n^\sigma} = \prod_p (1 - |\alpha_1(p)|p^{-\sigma})^{-1} \cdots (1 - |\alpha_d(p)|p^{-\sigma})^{-1}.$$

Either of these equalities is stronger than mere absolute convergence of the infinite product since each factor is replaced with its absolute series not just the absolute value of the series. In particular, this implies that the Euler product converges locally absolutely uniformly in the same region that the Dirichlet series does.

If $D(s)$ admits a Euler product, we write $D^{(N)}(s)$ to denote the Dirichlet series with the factors $p \mid N$ in the Euler product removed. This means

$$D^{(N)}(s) = D(s) \prod_{p \mid N} \left(\sum_{k \geq 0} \frac{a(p^k)}{p^{ks}} \right).$$

Dually, we let $D_{(N)}(s)$ denote the Dirichlet series consisting only of the factors $p \mid N$ in the Euler product. This means

$$D_{(N)}(s) = \prod_{p \mid N} \left(\sum_{k \geq 0} \frac{a(p^k)}{p^{ks}} \right).$$

With this notation, we have the relationship

$$D(s) = D^{(N)}(s) D_{(N)}(s).$$

7.3 Dirichlet Convolution

We now turn to discussing how Dirichlet series behave with respect to products. Let $D_f(s)$ and $D_g(s)$ be the Dirichlet series defined by

$$D_f(s) = \sum_{n \geq 1} \frac{f(n)}{n^s} \quad \text{and} \quad D_g(s) = \sum_{n \geq 1} \frac{g(n)}{n^s},$$

for some arithmetic functions f and g. Let $f * g$ be the Dirichlet convolution of f and g. A short computation shows

$$D_f(s) D_g(s) = D_{f*g}(s).$$

In other words, $D_f(s)D_g(s)$ is again a Dirichlet series whose coefficients are given by the Dirichlet convolution of f and g. This relation also shows that $D_{f*g}(s)$ converges absolutely wherever both $D_f(s)$ and $D_g(s)$ do. Since Dirichlet convolution preserves multiplicativity, $D_{f*g}(s)$ will have multiplicative coefficients if both $D_f(s)$ and $D_g(s)$ do. Moreover, from the Möbius inversion formula we immediately find that

$$D_g(s) = D_{f*\mathbf{1}}(s),$$

if and only if

$$D_f(s) = D_{g*\mu}(s).$$

These identities can be used to compute the Dirichlet series for many types of arithmetic functions.

7.4 Perron Formulas

With Mellin inversion, it is possible to relate the sums of coefficients of a Dirichlet series to an integral of its associated Dirichlet series. Such formulas are desirable because they allow for the examination of these sums by methods in complex analysis. First, we setup some general notation. Let $D(s)$ be a Dirichlet series with coefficients $a(n)$. For $X > 0$, we set

$$A^*(X) = \sum_{n \le X}^{*} a(n),$$

where the $*$ indicates that the last term is multiplied by $\frac{1}{2}$ if X is an integer. This slight modification of $A(X)$ accounts for the fact that Mellin inversion returns the average at a jump discontinuity. We would like to relate $A^*(X)$ to the inverse Mellin transform of $D(s)$. We will prove several variants of this basic idea. The first being *(classical) Perron's formula* which is a consequence of Abel summation and Mellin inversion applied to Dirichlet series.

Theorem (Perron's formula, classical). *Let $D(s)$ be a Dirichlet series with coefficient $a(n)$ and finite and nonnegative abscissa of absolute convergence σ_a. Then for any $c > \sigma_a$, we have*

$$A^*(X) = \frac{1}{2\pi i} \int_{(c)} D(s) X^s \, \frac{ds}{s}.$$

Proof. Let $\sigma > \sigma_a$. By Proposition 7.1.6, $A(X) \ll_\varepsilon X^{\sigma_a + \varepsilon}$. Taking ε sufficiently small, we find that $A(X)X^{-s} \to 0$ as $X \to \infty$. Abel summation then gives

$$D(s) = s \int_1^\infty A(u) u^{-(s+1)} \, du. \tag{7.1}$$

As $A(u) = 0$ in the interval $[0, 1)$, we can write the previous identity in the form

$$\frac{D(s)}{s} = \int_0^\infty A(u) u^{-(s+1)} \, du.$$

Mellin inversion immediately gives the result. □

In the proof of classical Perron's formula, we obtained a useful integral representation for a Dirichlet series. We collect this in the following corollary:

Corollary 7.4.1. *Let $D(s)$ be a Dirichlet series with finite and nonnegative abscissa of absolute convergence σ_a. Then for $\sigma > \sigma_a$, we have*

$$D(s) = s \int_1^\infty A(u) u^{-(s+1)} \, du.$$

Proof. The identity is Equation (7.1). □

Classical Perron's formula is not always useful in applications because often it is necessary to estimate the integral of the Dirichlet series. As the integral need not be absolutely bounded, this would require nontrivial estimates for the Dirichlet series in vertical strips. Fortunately, there are two ways to correct for this defect each of which leads to a different variant of Perron's formula. The first is to truncate the integral while the latter is to introduce a smoothing function. In the former case, a careful estimation of the error term is often necessary while the latter case requires estimates for the smoothing function. Both variants can be equally useful and the choice of which to use is often dependent upon what methods are available in the current setting.

Let us first focus on the truncated variant. To state it, we will need to setup some notation and prove a lemma. For $c > 0$ and $T > 0$, consider the integrals

$$\delta(y) = \frac{1}{2\pi i}\int_{(c)} y^s \frac{ds}{s} \quad \text{and} \quad I(y,T) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT} y^s \frac{ds}{s},$$

defined for $y > 0$. Note that $I(y,T)$ is just $d(y)$ truncated outside height T. The lemma we require gives an explicit evaluation of $\delta(y)$ and gives an approximation for the error between $\delta(y)$ and its truncation $I(y,T)$. The proof is quite laborious but standard.

Lemma 7.4.2. *We have*

$$\delta(y) = \begin{cases} 0 & \text{if } y < 1, \\ \frac{1}{2} & \text{if } y = 1, \\ 1 & \text{if } y > 1. \end{cases}$$

Moreover,

$$I(y,T) - \delta(y) = \begin{cases} O\left(y^c \min\left(1, \frac{1}{T\log(y)}\right)\right) & \text{if } y \neq 1, \\ O\left(\frac{c}{T}\right) & \text{if } y = 1. \end{cases}$$

Proof. Since $I(y,T) \to \delta(y)$ as $T \to \infty$, it suffices to estimate $I(y,T)$ and then take the limit as $T \to \infty$. First consider the case $y = 1$. A short computation shows

$$I(1,T) = \frac{1}{\pi}\tan^{-1}\left(\frac{T}{c}\right).$$

Truncate the Laurent series of the inverse tangent after the first term to write $\tan^{-1}(t) = \frac{\pi}{2} + O\left(\frac{1}{t}\right)$. Then

$$I(1,T) = \frac{1}{2} + O\left(\frac{c}{T}\right),$$

and we see that $\delta(y) = \frac{1}{2}$. This proves everything when $y = 1$. Now suppose $y < 1$ and let $d > c$. Let $\eta = \sum_{1\le i\le 4}\eta_i$ be the rectangular contour in Figure 7.1 where the horizontal lines are along $t = \pm T$ and the vertical lines are along $\sigma = c$ and $\sigma = d$. Consider

$$\frac{1}{2\pi i}\int_{\eta} y^s \frac{ds}{s}.$$

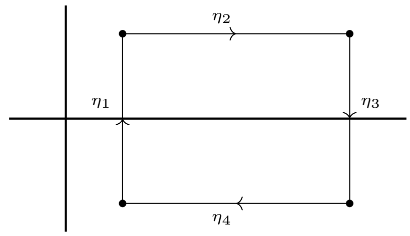

Figure 7.1: A rectangular contour.

We will evaluate this integral in the limit as $d \to \infty$. The contour does not enclose the only pole of the integrand which is at $s = 0$. So on the one hand, the residue theorem gives

$$\frac{1}{2\pi i}\int_{\eta} y^s \frac{ds}{s} = 0.$$

On the other hand, the integral is a sum along all four contours. Observe that

$$\frac{1}{2\pi i}\int_{\eta_1} y^s \frac{ds}{s} = I(y, T).$$

For the integrals over η_2 and η_4, the parameterizations $s \mapsto \sigma \pm iT$ show

$$\frac{1}{2\pi i}\int_{\eta_2} y^s \frac{ds}{s} + \frac{1}{2\pi i}\int_{\eta_4} y^s \frac{ds}{s} = O\left(\frac{y^c}{\log(y)T}\right),$$

as $y < 1$. For the integral over η_3, the parameterization $s \mapsto d + it$ shows

$$\frac{1}{2\pi i}\int_{\eta_3} y^s \frac{ds}{s} = O\left(y^d \log(T)\right).$$

Whence

$$I(y, T) = O\left(\frac{y^c}{\log(y)T}\right),$$

upon taking the limit as $d \to \infty$ since $y < 1$. It follows that $\delta(y) = 0$. We now obtain another estimate for $I(y, T)$ this time using a modified contour. Let $\eta = \eta_1 + \eta_2$ be the semicircular contour in Figure 7.2 where the vertical line is along $\sigma = c$ with endpoints at $s = c \pm iT$.

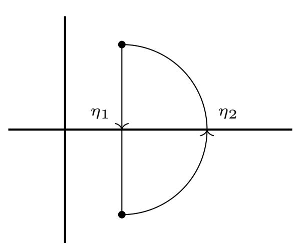

Figure 7.2: A semicircular contour.

As before, the residue theorem gives

$$\frac{1}{2\pi i}\int_{\eta} y^s \frac{ds}{s} = 0.$$

However, now

$$\frac{1}{2\pi i}\int_{\eta_1} y^s \frac{ds}{s} = -I(y,T).$$

The parameterization $s \mapsto \sqrt{(c^2+T^2)}e^{i\theta}$ shows that

$$\frac{1}{2\pi i}\int_{\eta_2} y^s \frac{ds}{s} = O(y^c).$$

Whence

$$I(y,T) = O(y^c).$$

Combining these two estimates for $I(y,T)$ proves everything when $y < 1$. Now suppose $y > 1$ and let $d < 0$. We argue as in the case $y < 1$ except we use the the rectangular contour in Figure 7.3.

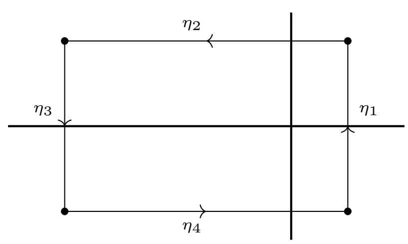

Figure 7.3: A rectangular contour.

This time the the contour encloses the simple pole of the integrand at $s = 0$ whose residue is 1. Arguing analogously, we find

$$I(y,T) = 1 + O\left(\frac{y^c}{\log(y)T}\right),$$

and so $\delta(y) = 1$.

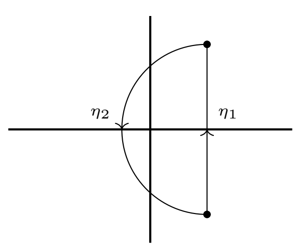

Figure 7.4: A semicircular contour.

We now modify the contour by using the semicircular one in Figure 7.4. Again, the contour encloses the simple pole of the integrand at $s = 0$ whose residue is 1. Arguing analogously, we obtain

$$I(y, T) = 1 + O(y^c).$$

Combining these two estimates for $I(y, T)$ proves everything when $y < 1$ and completes the proof. $\square$

This result will provide the estimate we need to prove (truncated) *Perron's formula*:

Theorem (Perron's formula, truncated). *Let $D(s)$ be a Dirichlet series with coefficient $a(n)$ and finite and nonnegative abscissa of absolute convergence σ_a. Then for any $c > \sigma_a$ and $T > 0$, we have*

$$\begin{aligned} A^*(X) &= \frac{1}{2\pi i}\int_{c-iT}^{c+iT} D(s)X^s \frac{ds}{s} \\ &\quad + O\left(X^c \sum_{\substack{n\geq 1 \\ n\neq X}} \frac{|a(n)|}{n^c} \min\left(1, \frac{1}{T\left|\log\left(\frac{X}{n}\right)\right|}\right) + \delta_X |a(X)| \frac{c}{T} \right), \end{aligned}$$

where $\delta_X = 1, 0$ according to if X is an integer or not.

Proof. By Lemma 7.4.2, we may write

$$A^*(X) = \sum_{n\geq 1} a(n)\delta\left(\frac{X}{n}\right),$$

and

$$\delta(y) = I(y, T) - \begin{cases} O\left(y^c \min\left(1, \frac{1}{T\log(y)}\right)\right) & \text{if } y \neq 1, \\ O\left(\frac{c}{T}\right) & \text{if } y = 1. \end{cases}$$

Substituting the second identity into the first and combining the O-estimates gives

$$\begin{aligned} A^*(X) &= \sum_{n\geq 1} a(n)\frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{X^s}{n^s}\frac{ds}{s} \\ &\quad + O\left(X^c \sum_{\substack{n\geq 1 \\ n\neq X}} \frac{|a(n)|}{n^c} \min\left(1, \frac{1}{T\left|\log\left(\frac{X}{n}\right)\right|}\right) + \delta_X |a(X)| \frac{c}{T} \right). \end{aligned}$$

As $D(s)$ converges absolutely, we may interchange the sum and the integral. The statement follows. $\square$

Since the integral in truncated Perron's formula is over a finite vertical line, the integral is automatically absolutely bounded. There is also a mor crude variant of truncated Perron's formula that follows as a corollary:

Corollary 7.4.3. *Let $D(s)$ be a Dirichlet series with coefficient $a(n)$ and finite and nonnegative abscissa of absolute convergence σ_a. Then for any $c > \sigma_a$ and $0 < T < X^c$, we have*
$$A^*(X) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT} D(s)X^s\,\frac{ds}{s} + O_c\left(\frac{X^c}{T}\right),$$

Proof. For $0 < T < X^c$, we have
$$\min\left(1, \frac{1}{T\log\left(\frac{X}{n}\right)}\right) \ll \frac{X^c}{T}.$$
Also, Proposition 7.1.4 guarantees $a(X) \ll X^c$. These estimates and that $D(s)$ is absolutely convergent at $s = c$ together imply that error term in truncated Perron's formula is $O_c\left(\frac{X^c}{T}\right)$. The claim follows. □

Having discussed truncated Perron's formula, we turn to the variant where we instead introduce a smoothing function. We call $\psi(y)$ a *smooth weight* if it is a positive bump function whose support is bounded away from zero. For any $X > 0$, we set
$$A_\psi(X) = \sum_{n\geq 1} a(n)\psi\left(\frac{n}{X}\right),$$
We distinguish between two cases. The first is when we choose $\psi(y)$ to assign weight 1 or 0 to the coefficients and we obtain sums such as
$$\sum_{\frac{X}{2}\leq n<X} a(n) \quad \text{or} \quad \sum_{X\leq n<X+Y} a(n).$$
Sums of this type are called *unweighted*. As an example of an unweighted sum, let $\psi(y)$ be a smooth weight that is identically 1 on $\left[\frac{1}{2}, 1\right]$ and supported in $\left[\frac{1}{2} - \frac{1}{X}, 1 + \frac{1}{X}\right]$. Then
$$A_\psi(X) = \sum_{\frac{X}{2}\leq n\leq X} a(n).$$
In the second case, we want $\psi(y)$ to dampen the coefficients with a weight other than 1 or 0. Sums of this type are called *weighted*. In either case, the Mellin transform $\Psi(s)$ of $\psi(y)$ is given by
$$\Psi(s) = \int_0^\infty \psi(y)y^s\,\frac{dy}{y}.$$
As $\psi(y)$ has compact support, the integral defining $\Psi(s)$ is a locally absolutely uniformly bounded on $\mathbb{C}$. In particular, $\Psi(s)$ is holomorphic and Mellin inversion implies that $\psi(y)$ is the Mellin inverse of $\Psi(s)$. As for nice properties, $\Psi(s)$ exhibit rapid decay.

Proposition 7.4.4. *Suppose $\psi(y)$ is smooth weight and let $\Psi(s)$ be its Mellin transform. Then for bounded σ, we have*
$$\Psi(s) \ll (|s| + 1)^{-N},$$
for any positive integer N.

Proof. Consider
$$\Psi(s) = \int_0^\infty \psi(y) y^s \, \frac{dy}{y}.$$
Since $\psi(y)$ is compactly supported, integration by parts yields
$$\Psi(s) = \frac{1}{s} \int_0^\infty \psi'(y) y^{s+1} \, \frac{dy}{y}.$$
Repeated integration by parts gives
$$\Psi(s) = \frac{1}{s(s+1)\cdots(s+N-1)} \int_0^\infty \psi^{(N)}(y) y^{s+N} \, \frac{dy}{y}.$$
Therefore
$$\Psi(s) \ll (|s|+1)^{-N} \int_0^\infty \psi^{(N)}(y) y^{\sigma+N} \, \frac{dy}{y}.$$
Now $\psi^{(N)}(y)$ is compactly supported in the same region as $\psi(y)$. In particular, $\psi^{(N)}(y)$ has compact support away from zero. Therefore
$$\int_0^\infty \psi^{(N)}(y) y^{\sigma+N} \, \frac{dy}{y} \ll 1,$$
and the estimate follows. □

The following result is (smoothed) *Perron's formula*:

Theorem (Perron's formula, smoothed). *Let $D(s)$ be a Dirichlet series with coefficient $a(n)$ and finite and nonnegative abscissa of absolute convergence σ_a. Let $\psi(y)$ be a smooth weight and let $\Psi(s)$ be its Mellin transform. Then for any $c > \sigma_a$, we have*
$$A_\psi(X) = \frac{1}{2\pi i} \int_{(c)} D(s)\Psi(s) X^s \, ds.$$
In particular,
$$\sum_{n \geq 1} a(n)\psi(n) = \frac{1}{2\pi i} \int_{(c)} D(s)\Psi(s) \, ds.$$

Proof. By Mellin inversion, we may write
$$A_\psi(X) = \sum_{n \geq 1} \frac{a(n)}{2\pi i} \int_{(c)} \Psi(s) \left(\frac{n}{X}\right)^{-s} ds.$$
We may interchange the sum and integral by the absolute convergence of $D(s)$ and Proposition 7.4.4. This gives
$$A_\psi(X) = \frac{1}{2\pi i} \int_{(c)} D(s)\Psi(s) X^s \, ds,$$
which is the first statement. For the second, take $X = 1$. □

The integral in smoothed Perron's formula is absolutely bounded (this permitted the interchange of the sum and integral). In practice, this means that the integral can be estimated directly and we do not need to truncate. The compensation for this is that we have introduced a weighting factor to the sum of coefficients.

Chapter 8

Analytic L-functions

Throughout, $s = \sigma + it$ and $u = \tau + ir$ will stand for complex variables with σ, τ, t, and r real. We also write

$$(u)_k = u(u+1)\cdots(u+(k-1)),$$

for the Pochhammer symbol.

8.1 Analytic Data

An *analytic L-function* $L(s)$ is a Dirichlet series

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

with coefficients $a_L(n) \in \mathbb{C}$ such that $a_L(1) = 1$ and satisfying the following properties:

Analyticity: There exists a nonnegative integer m_L such that the Dirichlet series of $L(s)$ is absolutely convergent for $\sigma > 1$ and admits meromorphic continuation to $\mathbb{C}$ with at most a pole at $s = 1$ of order m_L. Moreover, $(s-1)^{m_L}L(s)$ is order 1.

Functional Equation: There is a positive integer q_L, called the *conductor* of $L(s)$, a positive integer d_L called the *degree* of $L(s)$, complex numbers $(\mu_j)_{1\leq j\leq d_L}$ called the *gamma parameters* of $L(s)$ that are either real or occur in conjugate pairs and satisfy $\mathrm{Re}(\mu_j) \geq 0$, and a complex number ε_L called the *root number* of $L(s)$ with $|\varepsilon_L| = 1$, all of which determine functions

$$\Lambda(s, L) = q_L^{\frac{s}{2}}\gamma_L(s)L(s) \quad \text{and} \quad \gamma_L(s) = \pi^{-\frac{d_L s}{2}} \prod_j \Gamma\left(\frac{s+\mu_j}{2}\right),$$

called the *completion* of $L(s)$ and the *gamma factor* of $L(s)$ respectively, satisfying

$$\Lambda(s, L) = \varepsilon_L \overline{\Lambda(1-\overline{s}, L)}.$$

This is called the *functional equation* of $L(s)$. The tuple $(\varepsilon_L, q_L, \mu_1, \ldots, \mu_{d_L})$ is called the *functional equation data* of $L(s)$.

Euler product: For every prime p, there exist complex numbers $(\alpha_j(p))_{1\le j\le d_L}$ called the *Euler parameters* of $L(s)$ at p satisfying $|\alpha_j(p)| \le p^\theta$ for some $0 \le \theta < 1$ and are such that $L(s)$ admits the Euler product

$$L(s) = \prod_p (1-\alpha_1(p)p^{-s})^{-1} \cdots (1-\alpha_{d_L}(p)p^{-s})^{-1},$$

for $\sigma > 1$. The polynomial L_p defined by

$$L_p(T) = (1-\alpha_1(p)T)\cdots(1-\alpha_{d_L}(p)T),$$

is called the *Euler factor* of $L(s)$ at p. If $p \nmid q_L$ then L_p is of degree d_L while if $p \mid q_L$ then L_p is of degree less than d_L.

An analytic L-function is said to be *Selberg class* if it satisfies the following additional property:

Ramanujan bound: We may take $\theta = 0$ so that $|\alpha_j(p)| \le 1$.

Some comments on the definition of analytic L-functions are in order.

(i) As the Dirichlet series of $L(s)$ converges absolutely for $\sigma > 1$ its converges locally absolutely uniformly in this half-plane and therefore defines a holomorphic function there. Moreover, the Euler product necessarily converges locally absolutely uniformly in the same half-plane and hence defines a holomorphic function there as well which agrees with the Dirichlet series.

(ii) The bound $\mathrm{Re}(\mu_j) \ge 0$ ensures that the gamma factor is holomorphic in the half-plane $\sigma > 0$. As this factor is then guaranteed to be finite and nonzero at $s = 1$, the completion possesses a pole at $s = 1$ of order r. By the functional equation, the completion also has a pole at $s = 0$ of the same order.

(iii) If we merely assume $(s-1)^{m_L}L(s)$ is finite order then the functional equation forces the order to be 1. This can be deduced by considering the entire function

$$s^{m_L}(s-1)^{m_L}\Lambda(s, L),$$

and applying the Phragmén-Lindelöf convexity principle in vertical strips.

(iv) The condition that the root number satisfies $|\varepsilon_L| = 1$ isn't strictly necessary. For applying the functional equation twice shows $|\varepsilon_L|^2 = 1$.

(v) As the gamma function is conjugation-equivariant and the gamma parameters are real or occur in conjugate pairs, the gamma factor is also conjugation-equivariant. This means that we can write the functional equation in the form

$$q_L^{\frac{s}{2}}\gamma_L(s)L(s) = \varepsilon_L q_L^{\frac{1-s}{2}}\gamma_L(1-s)\overline{L(1-\overline{s})}.$$

(vi) The Euler product implies that the coefficients $a_L(n)$ are multiplicative and are determined on prime powers by

$$a_L(p^k) = \sum_{1 \le j_1 \le \cdots \le j_k \le d_L} \alpha_{j_1}(p) \cdots \alpha_{j_k}(p).$$

In other words, $a_L(p^k)$ is the complete symmetric polynomial of degree k in the Euler parameters at p. If the Ramanujan bound holds, then it follows that $a_L(n) \ll \sigma_{d_L}(n)$. This implies the slightly weaker, but more practical, estimate $a_L(n) \ll_\varepsilon n^\varepsilon$.

It it clear from the definition that analytic L-functions are closed under multiplication and that the degree is additive. Moreover, this closure respects Selberg class L-functions. This makes the set of analytic L-functions into a graded commutative semigroup where the grading is induced by degree. It follows that there exist irreducible elements with respect to the grading and we say that an analytic L-function is *primitive* if it such an irreducible. Clearly any analytic L-function of degree 1 is primitive. Moreover, every analytic L-function factors into a product of primitive L-functions. Such a factorization is only conjectured to be unique for Selberg class L-functions. A sufficient condition would be *Selberg's orthogonality conjecture.*

Conjecture (Selberg's orthogonality conjecture). *For any two primitive Selberg class L-functions $L_1(s)$ and $L_2(s)$, we have*

$$\sum_{p \le x} \frac{a_{L_1}(p)\overline{a_{L_2}(p)}}{p} = \delta_{L_1,L_2} \log\log(x) + O(1).$$

Indeed, we have the following result:

Proposition 8.1.1. *Assume Selberg's orthogonality conjecture. Then every Selberg class L-function factors uniquely into a product of primitive Selberg class L-functions.*

Proof. If the factorization into primitive unity L-functions were not unique, then we would have distinct factorizations satisfying

$$L_1(s) \cdots L_n(s) = M_1(s) \cdots M_m(s),$$

for some primitive Selberg class L-functions L_i and M_j. By uniqueness of coefficients of Dirichlet series, compare the p-th coefficient to see that

$$\sum_i a_{L_i}(p) = \sum_j a_{M_j}(p).$$

Now consider

$$\sum_{p<x} \frac{1}{p} \left(\sum_i a_{L_i}(p) \right) \left(\sum_j \overline{a_{M_j}(p)} \right) = \sum_{i,j} \sum_{p<x} \frac{a_{L_i}(p)\overline{a_{M_j}(p)}}{p}.$$

Selberg's orthogonality conjecture implies

$$O(1) = c \log\log(x) + O(1),$$

for some positive integer c since the factorizations are distinct. This is impossible. □

To an analytic L-function $L(s)$, we associate its *analytic conductor* $\mathfrak{q}(s, L)$ defined by

$$\mathfrak{q}(s, L) = q_L \mathfrak{q}_\infty(s, L),$$

where

$$\mathfrak{q}_\infty(s, L) = \prod_j (|s + \mu_j| + 3).$$

The choice of 3 in $|s + \mu_j| + 3$ is a matter of convenience as could use any positive constant. In particular, it is useful when taking logarithms as $\log(|s + \mu_j| + 3) \geq 1$. For legibility, we will also write

$$\mathfrak{q}(t, L) = \mathfrak{q}\left(\frac{1}{2} + it, L\right) \quad \text{and} \quad \mathfrak{q}_\infty(t, L) = \mathfrak{q}_\infty\left(\frac{1}{2} + it, L\right).$$

as well as

$$\mathfrak{q}(L) = \mathfrak{q}\left(\frac{1}{2}, L\right) \quad \text{and} \quad \mathfrak{q}_\infty(L) = \mathfrak{q}_\infty\left(\frac{1}{2}, L\right),$$

Estimates for the analytic conductor follow from those of the gamma function. Recall from Stirling's formula that

$$\Gamma(s) \ll_\varepsilon (|t| + 3)^{\sigma - \frac{1}{2}} e^{-\frac{\pi}{2}|t|} \quad \text{and} \quad \frac{1}{\Gamma(s)} \ll (|t| + 3)^{\frac{1}{2} - \sigma} e^{\frac{\pi}{2}|t|}, \tag{8.1}$$

for bounded σ provided that in the former estimate s is at least distance ε away from the poles of the gamma function. Hence

$$\frac{\Gamma(1 - s)}{\Gamma(s)} \ll_\varepsilon (|t| + 3)^{1 - 2\sigma},$$

for bounded σ provided s is at least distance ε away from the poles of $\Gamma(1 - s)$. Then the estimates

$$\frac{\gamma_L(1 - s)}{\gamma_L(s)} \ll_\varepsilon \mathfrak{q}_\infty(s, L)^{\frac{1}{2} - \sigma} \quad \text{and} \quad q_L^{\frac{1}{2} - s} \frac{\gamma_L(1 - s)}{\gamma_L(s)} \ll_\varepsilon \mathfrak{q}(s, L)^{\frac{1}{2} - \sigma}, \tag{8.2}$$

hold for bounded σ provided s is at least distance ε away from the poles of $\gamma_L(1 - s)$. An associated estimate can be obtain for the logarithmic derivative of the analytic conductor. Recall from the logarithm of Stirling's formula that

$$\frac{\Gamma'}{\Gamma}(s) \ll \log(|s| + 3),$$

provided σ is bounded and s is at least distance ε away from the poles of the gamma function. Then the estimates

$$\frac{\gamma_L'}{\gamma_L}(s) \ll_\varepsilon \log \mathfrak{q}_\infty(s, L) \quad \text{and} \quad \log q_L + \frac{\gamma_L'}{\gamma_L}(s) \ll_\varepsilon \log \mathfrak{q}(s, L), \tag{8.3}$$

hold for bounded σ provided s is at least distance ε away from the poles of the gamma factor.

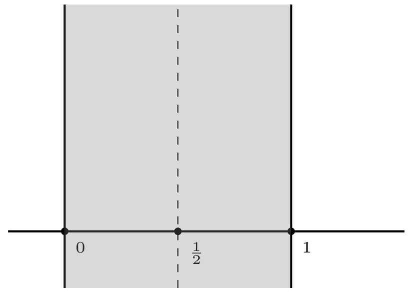

Figure 8.1: The critical strip.

The *critical strip* of an analytic L-function is the vertical strip left invariant by the transformation $s \mapsto 1-s$. This region can also be described as

$$\left\{s \in \mathbb{C} : \left|\sigma - \frac{1}{2}\right| \leq \frac{1}{2}\right\}.$$

The *critical line* is the vertical line left invariant by the transformation $s \mapsto 1-s$ which is also given by $\sigma = \frac{1}{2}$. The critical line bisects the critical strip vertically. The *central point* is the fixed point of the transformation $s \mapsto 1-s$, in other words, the point $s = \frac{1}{2}$. Clearly the central point is also the center of the critical line. The critical strip, critical line, and central point are all displayed in Figure 8.1.

In the half-plane $\sigma > 1$ we may study the analytic properties of $L(s)$ via its Dirichlet series. Using the functional equation, we may write

$$L(s) = \varepsilon_L q_L^{\frac{1}{2}-s} \frac{\gamma_L(1-s)}{\gamma_L(s)} \overline{L(1-\overline{s})}.$$

This permits the study of $L(s)$ in the half-plane $\sigma < 0$ by using the Dirichlet series of $\overline{L(1-\overline{s})}$ and the the functional equation data. The interior of the critical strip is exactly the region where we cannot use either of these methods to study the analytic properties of $L(s)$. Of course, anything may be possible on the boundary lines $\sigma = 0$ and $\sigma = 1$ (for example Landau's theorem).

8.2 The Approximate Functional Equation

Despite not being able to study an analytic L-function $L(s)$ in the critical strip by means of Dirichlet series, there is formula which acts as a compromise between the functional equation and the Dirichlet series. This formula is known as the approximate functional equation. The usefulness comes from the fact that the approximate functional equation is valid inside of the critical strip and therefore can be used to obtain analytic properties about $L(s)$ in that region. We will first derive a preliminary result showing $L(s)$ has at most polynomial growth.

Proposition 8.2.1. *Let $L(s)$ be an analytic L-function with σ bounded and σ at least distance ε away from the possible pole at $s = 1$. Then there is a positive constant A such that*

$$L(s) \ll_\varepsilon (|t| + 3)^A.$$

Proof. Observe that $(s-1)^{m_L}L(s) \ll_\varepsilon (|t|+3)^{m_L}$ on the vertical line $\sigma = \max(1+\varepsilon, \sigma_2)$. Now suppose $\sigma = \min(-\varepsilon, \sigma_1)$. On this vertical line, the functional equation and Equation (8.2) together show

$$L(s) \ll_\varepsilon \mathfrak{q}(s,L)^{\frac{1}{2}-\sigma}\overline{L(1-\overline{s})}.$$

Hence there exists a positive constant A'' with

$$(s-1)^{m_L}L(s) \ll_\varepsilon (|t|+3)^{A''},$$

on the vertical line $\sigma = \min(-\varepsilon, \sigma_1)$. As $(s-1)^{m_L}L(s)$ is entire and of order 1, we can apply the Phragmén-Lindelöf convexity principle to $(s-1)^{m_L}L(s)$ the vertical strip $\min(-\varepsilon, \sigma_1) \le \sigma \le \max(1+\varepsilon, \sigma_2)$. Whence there is a positive constant A' such that

$$(s-1)^{m_L}L(s) \ll_\varepsilon (|t|+3)^{A'},$$

provided σ is bounded. Assuming s is at least distance ε away from the possible pole at $s=1$, diving by $(s-1)^{m_L}$ completes the proof. $\square$

We are almost ready to prove the approximate function equation for an analytic L-function $L(s)$. The formula itself consists of two sums representing the Dirichlet series at s and a dualized Dirichlet series at $1-s$ as well as a potential residue term. The dual sum comes equip with a term containing the data of the functional equation. Both sums will also be dampened by a smooth cutoff function. In the statement of the approximate function equation, we will make use of a test function $\Phi(u)$. We require $\Phi(u)$ be an even holomorphic function bounded in the vertical strip $|\tau| < a+1$ for some $a > 1$ and such that $\Phi(0) = 1$. For s in the critical strip, we let $V_s(y)$ be the inverse Mellin transform

$$V_s(y) = \frac{1}{2\pi i}\int_{(a)} \frac{\gamma_L(s+u)}{\gamma_L(s)}\Phi(u)y^{-u}\frac{du}{u},$$

defined for $y > 0$. For legibility, we will write

$$V_t(y) = V_{\frac{1}{2}+it}(y).$$

Stirling's formula implies

$$\frac{\Gamma(s+u)}{\Gamma(s)} \ll_\varepsilon \frac{(|t+r|+3)^{\sigma+\tau-\frac{1}{2}}}{(|t|+3)^{\sigma-\frac{1}{2}}}e^{-\frac{\pi}{2}(|t+r|-|t|)},$$

for s in the critical strip and bounded τ provided $s+u$ is at least distance ε away from the poles of the gamma function. Whence

$$\frac{\gamma_L(s+u)}{\gamma_L(s)} \ll_\varepsilon \frac{\mathfrak{q}_\infty(s+u)^{\frac{\sigma+\tau}{2}-\frac{1}{4}}}{\mathfrak{q}_\infty(s)^{\frac{\sigma}{2}-\frac{1}{4}}}e^{-d_L\frac{\pi}{2}(|t+r|-|t|)}, \tag{8.4}$$

for s in the critical strip and bounded τ provided $s+u$ is at least distance ε away from the poles of the gamma factor. Since $\Phi(u)$ is bounded in the vertical strip $|\tau| < a+1$, the integrand exhibits exponential decay. Therefore the integral is locally absolutely uniformly bounded and hence $V_s(y)$ is smooth. The function $V_s(y)$ is the smooth cutoff function mentioned previously. We will also let $\varepsilon_L(s)$ be given by

$$\varepsilon_L(s) = \varepsilon_L q_L^{\frac{1}{2}-s} \frac{\gamma_L(1-s)}{\gamma_L(s)}.$$

For legibility, we let

$$\varepsilon_L(t) = \varepsilon_L\left(\frac{1}{2}+it\right).$$

This term appears as a factor in the dual sum accounting for the functional equation data. We now prove the *approximate function equation*:

Theorem (Approximate functional equation). *Suppose $L(s)$ is an analytic L-function, $\Phi(u)$ is an even holomorphic function bounded in the vertical strip $|\tau| < a+1$ for some $a > 1$ and such that $\Phi(0) = 1$, and let $X > 0$. Then for s in the critical strip, we have*

$$L(s) = \sum_{n\geq 1} \frac{a_L(n)}{n^s} V_s\left(\frac{n}{\sqrt{q_L}X}\right) + \varepsilon_L(s) \sum_{n\geq 1} \frac{\overline{a_L(n)}}{n^{1-s}} V_{1-s}\left(\frac{nX}{\sqrt{q_L}}\right) + \frac{R(s,X,L)}{q_L^{\frac{s}{2}}\gamma_L(s)},$$

where $R(s,X,L)$ is given by

$$R(s,X,L) = \operatorname*{Res}_{u=1-s} \frac{\Lambda(s+u,L)\Phi(u)X^u}{u} + \operatorname*{Res}_{u=-s} \frac{\Lambda(s+u,L)\Phi(u)X^u}{u}.$$

Proof. Consider the integral

$$\frac{1}{2\pi i}\int_{(a)} \Lambda(s+u,L)\Phi(u)X^u \,\frac{du}{u}.$$

Stirling's formula shows that $\gamma_L(s+u)$ exhibits exponential decay while $L(s+u)$ has at most polynomial growth by Proposition 8.2.1. Since $\Phi(u)$ is bounded in the vertical strip $|\tau| < a+1$, it follows that the integrand exhibits exponential decay. Therefore the integral is locally absolutely uniformly bounded. We will evaluate the integral in two ways. On the one hand, we can expand $L(s+u)$ inside the integrand as a Dirichlet series and by absolute boundedness of the integral we may interchange the sum and integral. A short computation shows that this is

$$q_L^{\frac{s}{2}}\gamma_L(s) \sum_{n\geq 1} \frac{a_L(n)}{n^s} V_s\left(\frac{n}{\sqrt{q_L}X}\right).$$

On the other hand, we can shift the line of integration to $(-a)$. In doing so we pass by a simple pole at $u = 0$ and possible poles at $u = 1-s$ and $u = -s$ giving

$$\frac{1}{2\pi i}\int_{(-a)} \Lambda(s+u,L)\Phi(u)X^u \,\frac{du}{u} + \Lambda(s,L) + R(s,X,L).$$

Apply the functional equation and perform the change of variables $u \mapsto -u$ to rewrite this as

$$-\varepsilon_L \frac{1}{2\pi i} \int_{(a)} \overline{\Lambda(1-\overline{s+u}, L)} \Phi(u) X^{-u} \frac{du}{u} + \Lambda(s, L) + R(s, X, L).$$

Analogous to the above, we can now expand $\overline{L(1-\overline{s+u})}$ inside the integrand as a Dirichlet series and by absolute boundedness of the integral we may interchange the sum and integral. A short computation shows that our previous expression becomes

$$-\varepsilon_L q_L^{\frac{1-s}{2}} \gamma_L(1-s) \sum_{n \geq 1} \frac{\overline{a_L(n)}}{n^{1-s}} V_s\left(\frac{nX}{\sqrt{q_L}}\right) + \Lambda(s, L) + R(s, X, L).$$

Equating these two evaluations and isolating the completion gives

$$\begin{aligned} \Lambda(s, L) = {} & q_L^{\frac{s}{2}} \gamma_L(s) \sum_{n \geq 1} \frac{a_L(n)}{n^s} V_s\left(\frac{n}{\sqrt{q_L} X}\right) \\ & + \varepsilon_L q_L^{\frac{1-s}{2}} \gamma_L(1-s) \sum_{n \geq 1} \frac{\overline{a_L(n)}}{n^{1-s}} V_{1-s}\left(\frac{nX}{\sqrt{q_L}}\right) + R(s, X, L). \end{aligned}$$

Diving by $q_L^{\frac{s}{2}} \gamma_L(s)$ completes the proof. $\square$

Let us now show how $V_s(y)$ has the effect of dampening the two dual sums appearing on the right-hand side of the approximate functional equation. In practice, it is common to choose $\Phi(u)$ such that it has exponential decay and we can make the vertical strip on which it is bounded arbitrarily wide. For example, let

$$\Phi(u) = \cos^{-4d_L M}\left(\frac{\pi u}{4M}\right),$$

for some positive integer M. Clearly $\Phi(u)$ is an even holomorphic function in the vertical strip $|\tau| < (2M-1)+1$ and satisfies $\Phi(0) = 1$. In view of the identity $\cos(u) = \frac{e^{iu}+e^{-iu}}{2}$, we find that

$$\cos^{-4d_L M}\left(\frac{\pi u}{4M}\right) \ll_\varepsilon e^{-d_L \pi |r|}, \tag{8.5}$$

for $|\tau| < (2M-1)+1$ provided u is at least distance ε away from the poles of $\Phi(u)$. Therefore $\Phi(u)$ admits exponential decay. For this choice of $\Phi(u)$, $V_s(y)$ and its derivatives will possess rapid decay.

Proposition 8.2.2. *Let $L(s)$ be an analytic L-function, set $\Phi(u) = \cos^{-4d_L M}\left(\frac{\pi u}{4M}\right)$ for some positive integer M, and let $V_s(y)$ be the inverse Mellin transform defined by*

$$V_s(y) = \frac{1}{2\pi i} \int_{(2M-1)} \frac{\gamma_L(s+u)}{\gamma_L(s)} \Phi(u) y^{-u} \frac{du}{u}.$$

Then for s in the critical strip, any nonnegative integer k, and positive integer N with $N < 2M$, $V_s(y)$ satisfies the estimates

$$(-y)^k V_s^{(k)}(y) = \begin{cases} \delta_{k,0} + O_\varepsilon\left(\left(\frac{y}{\sqrt{\mathfrak{q}_\infty(s,L)}}\right)^N\right) & \text{if } y \ll \sqrt{\mathfrak{q}_\infty(s,L)}, \\ O_\varepsilon\left(\left(\frac{y}{\sqrt{\mathfrak{q}_\infty(s,L)}}\right)^{-N}\right) & \text{if } y \gg \sqrt{\mathfrak{q}_\infty(s,L)}. \end{cases}$$

In particular,

$$(-y)^k V_s^{(k)}(y) \ll_\varepsilon \left(1 + \frac{y}{\sqrt{\mathfrak{q}_\infty(s,L)}}\right)^{-N}.$$

Proof. As we have already seen, the integrand defining $V_s(y)$ admits exponential decay. This permits us to differentiate under the integral sign and shift the line of integration. The former shows

$$(-y)^k V_s^{(k)}(y) = \frac{1}{2\pi i}\int_{(2M-1)} \frac{\gamma_L(s+u)}{\gamma_L(s)}\Phi(u)(u)_k y^{-u}\frac{du}{u}.$$

Shifting to $(-N)$, we pass by a simple pole at $u = 0$ of residue 1 if and only if $k = 0$. This gives

$$(-y)^k V_s^{(k)}(y) = \delta_{k,0} + \frac{1}{2\pi i}\int_{(-N)} \frac{\gamma_L(s+u)}{\gamma_L(s)}\Phi(u)(u)_k y^{-u}\frac{du}{u}.$$

This integrand also exhibits exponential decay since the Pochhammer symbol grows polynomially. Therefore the integral is dominated by the contribution when $u \ll 1$ and the Equations (8.4) and (8.5) together show

$$(-y)^k V_s^{(k)}(y) = \delta_{k,0} + O_\varepsilon\left(\left(\frac{y}{\sqrt{\mathfrak{q}_\infty(s,L)}}\right)^N\right).$$

If we instead shift to (N), we do not pass by any poles and obtain

$$(-y)^k V_s^{(k)}(y) = \frac{1}{2\pi i}\int_{(N)} \frac{\gamma_L(s+u)}{\gamma_L(s)}\Phi(u)(u)_k y^{-u}\frac{du}{u}.$$

An analogous argument to estimate the remaining integral shows

$$(-y)^k V_s^{(k)}(y) = O_\varepsilon\left(\left(\frac{y}{\sqrt{\mathfrak{q}_\infty(s,L)}}\right)^{-N}\right).$$

From these O-estimates we obtain nontrivial bounds in the ranges $y \ll \sqrt{\mathfrak{q}_\infty(s,L)}$ and $y \gg \sqrt{\mathfrak{q}_\infty(s,L)}$ respectively. Combining both of these estimates produces the bound

$$(-y)^k V_s^{(k)}(y) \ll_\varepsilon \left(1 + \frac{y}{\sqrt{\mathfrak{q}_\infty(s,L)}}\right)^{-N}.$$

□

With our choice of $\Phi(u)$, this result shows that $V_s(y)$ is essentially 1 up to some admissible error for $y \ll \sqrt{\mathfrak{q}_\infty(s,L)}$ and exhibits rapid decay thereafter as we can take M (and hence N) to be arbitrarily large.

In a similar spirit to the approximate functional equation, a useful summation formula can be derived from the functional equation. Let $\psi(y)$ be a smooth weight where $\Psi(s)$ is its Mellin transform. Then we will let $\psi(y,L)$ be the inverse Mellin transform

$$\psi(y,L) = \frac{1}{2\pi i}\int_{(a)} q_L^s \frac{\gamma_L(s)}{\gamma_L(1-s)} y^{-s}\Psi(1-s)\,ds,$$

defined for $y > 0$ where $a > 1$. By our choice of $\psi(y)$, its inverse Mellin transform $\Psi(s)$ has rapid decay. Since $L(s)$ has at most polynomial growth by Proposition 8.2.1, the integrand has rapid decay as well. Therefore the integral is locally absolutely uniformly bounded and hence $\psi(y,L)$ is smooth for $y > 0$. Our result is the following:

Theorem 8.2.3. *Let $L(s)$ be an analytic L-function and let $\psi(y)$ be a smooth weight where $\Psi(s)$ is its Mellin transform. Then*

$$\sum_{n\ge 1} a_L(n)\psi(n) = \frac{\varepsilon_L}{\sqrt{q_L}}\sum_{n\ge 1}\overline{a_L(n)}\psi(n,L) + R(L)\Psi(1),$$

where $R(L)$ is given by

$$R(L) = \operatorname*{Res}_{s=1} L(s).$$

Proof. Smoothed Perron's formula implies

$$\sum_{n\ge 1} a_L(n)\psi(n) = \frac{1}{2\pi i}\int_{(a)} L(s)\Psi(s)\,ds.$$

By our choice of $\psi(y)$, its inverse Mellin transform $\Psi(s)$ has rapid decay. Since $L(s)$ has at most polynomial growth by Proposition 8.2.1, the integrand has rapid decay as well. Therefore the integral is locally absolutely uniformly bounded which permits us to shift the line of integration. Shifting to $(1-a)$, we pass by a potential pole at $s = 1$ and obtain

$$\sum_{n\ge 1} a_L(n)\psi(n) = \frac{1}{2\pi i}\int_{(1-a)} L(s)\Psi(s)\,ds + R(L)\Psi(1).$$

Apply the functional equation to rewrite this equality in the form

$$\sum_{n\ge 1} a_L(n)\psi(n) = \frac{1}{2\pi i}\int_{(1-a)} \varepsilon_L q_L^{\frac{1}{2}-s}\frac{\gamma_L(1-s)}{\gamma_L(s)}\overline{L(1-\overline{s})}\Psi(s)\,ds + R(L)\Psi(1).$$

Performing the change of variables $s \mapsto 1-s$ in this latter integral gives

$$\sum_{n\ge 1} a_L(n)\psi(n) = \frac{1}{2\pi i}\int_{(a)} \varepsilon_L q_L^{s-\frac{1}{2}}\frac{\gamma_L(s)}{\gamma_L(1-s)}\overline{L(\overline{s})}\Psi(1-s)\,ds + R(L)\Psi(1).$$

The proof is complete upon expanding $\overline{L(\overline{s})}$ as a Dirichlet series, interchanging the sum and integral by absolute boundedness of the integral, and factoring out $\frac{\varepsilon_L}{\sqrt{q_L}}$. $\square$

8.3 The Riemann Hypothesis and Nontrivial Zeros

The zeros of an L-functions $L(s)$ has interesting behavior. From the Euler product we immediately see that $L(s)$ has no zeros in the half-plane $\sigma > 1$. We can use the functional equation to determine the zeros for $\sigma < 0$. Indeed, write the functional equation in the form

$$L(s) = \varepsilon_L q_L^{\frac{1}{2}-s} \frac{\gamma_L(1-s)}{\gamma_L(s)} \overline{L(1-\overline{s})}.$$

So for $\sigma < 0$, we see that $\overline{L(1-\overline{s})}$ is nonzero. Moreover, $\gamma_L(1-s)$ is as well. Together this means that for $\sigma < 0$ the poles of $\gamma_L(s)$ are zeros of $L(s)$. Such a zero is called a *trivial zero* of $L(s)$. From the definition of the gamma factor, they are all simple and of the form $s = -(\mu_j + 2n)$ for some gamma parameter μ_j and some nonnegative integer n.

Any other zero of $L(s)$ is called a *nontrivial zero* and it necessarily lies inside of the critical strip. Let ρ be a nontrivial zero of $L(s)$. Then the functional equation implies that $1-\overline{\rho}$ is also a nontrivial zero of $L(s)$. This means that nontrivial zeros occur in pairs

$$\rho \quad \text{and} \quad 1-\overline{\rho}.$$

It is possible to say more when $L(s)$ takes real values for $s > 1$. For in this case, the Schwarz reflection principle implies $L(\overline{s}) = \overline{L(s)}$ and that $L(s)$ takes real values on the entire real axis save for the possible pole at $s = 1$. It follows from the functional equation that $\overline{\rho}$ and $1-\rho$ are also nontrivial zeros. Therefore the nontrivial zeros of $L(s)$ come in sets of four

$$\rho, \quad \overline{\rho}, \quad 1-\rho, \quad \text{and} \quad 1-\overline{\rho}.$$

See Figure 8.2 for an example of this symmetry.

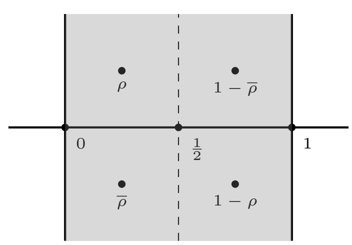

Figure 8.2: Symmetric nontrivial zeros.

The *Riemann hypothesis* for $L(s)$ says that this symmetry should be as simple as possible.

Conjecture (Riemann hypothesis, $L(s)$). *The nontrivial zeros of the analytic L-function $L(s)$ all lie on the vertical line $\sigma = \frac{1}{2}$.*

While stated as a conjecture, we not expect the Riemann hypothesis to hold for just any analytic L-function. We do however expect it to hold for Selberg class L-functions. In particular, the *Selberg class Riemann hypothesis* says that this symmetry should hold for any Selberg class L-function:

Conjecture (Selberg class Riemann hypothesis). *The nontrivial zeros of any Selberg class L-function $L(s)$ lie on the vertical line $\sigma = \frac{1}{2}$.*

So far, the Riemann hypothesis remains completely out of reach for any analytic L-function and thus the Selberg class Riemann hypothesis does as well.

8.4 The Lindelöf Hypothesis and Estimates on the Critical Line

Instead of asking about the zeros of an analytic L-function $L(s)$ on the critical line we can ask about its growth there. Let us begin this investigation by deriving an upper bound for $L(s)$ on the critical line using the Phragmén-Lindelöf convexity principle. This amounts to a more refined version of the argument used in Proposition 8.2.1 for the critical strip.

Theorem 8.4.1. *Let $L(s)$ be an analytic L-function. Then for $-\varepsilon \leq \sigma \leq 1+\varepsilon$, we have*

$$L(s) \ll_{\varepsilon} \mathfrak{q}(s, L)^{\frac{1-\sigma}{2}+\varepsilon},$$

provided s is at least distance ε away from the possible pole at $s = 1$.

Proof. Since $(s-1)^{r_L} L(s)$ is entire and of order 1, we will apply the Phragmén-Lindelöf convexity principle just outside the edges of the critical strip. Just past the right edge along the vertical line $\sigma = 1+\varepsilon$, we have

$$(s-1)^{r_L} L(s) \ll_{\varepsilon} (s-1)^{r_L}.$$

Just past the left edge along the vertical line $\sigma = -\varepsilon$, the functional equation and Equation (8.2) together imply the bound

$$(s-1)^{r_L} L(s) \ll_{\varepsilon} (s-1)^{r_L} \mathfrak{q}(s, L)^{\frac{1}{2}+\varepsilon}.$$

By the Phragmén-Lindelöf convexity principle, we obtain

$$(s-1)^{r_L} L(s) \ll_{\varepsilon} (s-1)^{r_L} \mathfrak{q}(s, L)^{\frac{1-\sigma}{2}+\varepsilon},$$

provided $-\varepsilon \leq \sigma \leq 1+\varepsilon$. Assuming s is at least distance ε away from the possible pole at $s = 1$, dividing by $(s-1)^{r_L}$ completes the proof. $\square$

At the critical line this theorem produces the bound

$$L\left(\frac{1}{2}+it\right) \ll_{\varepsilon} \mathfrak{q}\left(t, L\right)^{\frac{1}{4}+\varepsilon}.$$

This is known as the *convexity bound* for $L(s)$. The *Lindelöf hypothesis* for $L(s)$ says that the exponent can be reduced to ε:

Conjecture (Lindelöf hypothesis, $L(s)$). *The analytic L-function $L(s)$ satisfies*

$$L\left(\frac{1}{2}+it\right) \ll_{\varepsilon} \mathfrak{q}\,(t,L)^{\varepsilon}.$$

Unlike the Riemann hypothesis, the Lindelöf hypothesis is expected to hold for any analytic L-function. In any case, the *Selberg class Lindelöf hypothesis* says that the exponent can be reduced to ε for any Selberg class L-function:

Conjecture (Selberg class Lindelöf hypothesis). *Any Selberg class L-function $L(s)$ satisfies*

$$L\left(\frac{1}{2}+it\right) \ll_{\varepsilon} \mathfrak{q}\,(t,L)^{\varepsilon}.$$

Like the Riemann hypothesis, we have been unable to prove the Lindelöf hypothesis for any analytic L-function. However, in practice the Lindelöf hypothesis is more tractable. Generally speaking, any improvement upon the exponent in the convexity bound in any aspect of the analytic conductor is called a *subconvexity estimate* (or a *convexity breaking bound*). In the uniform case, we would like to prove bounds of the form

$$L\left(\frac{1}{2}+it\right) \ll_{\varepsilon} \mathfrak{q}\,(t,L)^{\delta+\varepsilon},$$

for some $0 \le \delta \le \frac{1}{4}$. The convexity bound says that we may take $\delta = \frac{1}{4}$ while the Lindelöf hypothesis for $L(s)$ implies that we may take $\delta = 0$. Any uniform subconvexity estimate would give a δ strictly less than $\frac{1}{4}$. Subconvexity estimates are viewed with great interest. This is primarily because of their connection to the Lindelöf hypothesis, but also because any improvement upon the convexity bound in any aspect of the analytic conductor often has drastic consequences in applications.

Remark 8.4.2. Some subconvexity bounds are deserving of names. The cases $\delta = \frac{3}{16}$ and $\delta = \frac{1}{6}$ are referred to as the *Burgess bound* and *Weyl bound* respectively.

With a little more work, we can obtain a a similar bound for the derivatives of analytic L-functions. First observe that Theorem 8.4.1 gives the estimate

$$L(s) \ll_{\varepsilon} \mathfrak{q}\,(t,L)^{\frac{1}{4}+\varepsilon},$$

in the vertical strip $\left|\sigma - \frac{1}{2}\right| \le \frac{\varepsilon}{2}$. This is just slightly stronger than the convexity bound. By Cauchy's integral formula, we may write

$$L^{(k)}\left(\frac{1}{2}+it\right) = \frac{k!}{2\pi i}\int_{\eta} \frac{L(s)}{(s-\frac{1}{2}-it)^{k+1}}\,ds,$$

where η is the circle about $\frac{1}{2}+it$ of radius $\frac{\varepsilon}{2}$. The parameterization $u \mapsto \frac{1}{2}+it+\frac{\varepsilon}{2}e^{i\theta}$ for η shows that

$$L^{(k)}\left(\frac{1}{2}+it\right) \ll_{\varepsilon} \mathfrak{q}\,(t,L)^{\frac{1}{4}+\varepsilon}.$$

This is known as the *convexity bound* for $L^{(k)}(s)$.

We now turn to the question of how to obtain estimates on the critical line. There are many methods one can apply often depending upon the particular analytic L-function of interest. Here we will provide a method that works in vast generality and reduces the estimation of $L\left(\frac{1}{2}+it\right)$ to that of estimating smoothed finite sums of coefficients. To achieve this we need to establish the existence of certain bump functions. We say that a function $\omega(y)$ is a *smooth dyadic weight* if it is a positive bump function supported in $[1-\delta, 2+\delta]$ and such that

$$\sum_{k\in\mathbb{Z}} \omega\left(\frac{y}{2^k}\right) = 1,$$

for all positive y. This last condition means $\left(\omega\left(\frac{y}{2^k}\right)\right)_{k\in\mathbb{Z}}$ is a partition of unity on $(0,\infty)$. To see that dyadic weights exist, let $\psi(y)$ be a smooth weight that is identically 1 on $[1,2]$ and supported in $[1-\delta, 2+\delta]$. Write

$$\sigma(y) = \sum_{k\in\mathbb{Z}} \psi\left(\frac{y}{2^k}\right).$$

Then $\sigma(y)$ is finite as finitely many of its summands are nonzero since any positive y satisfies $2^k \le y < 2^{k+1}$ for some unique integer k. This forces $\sigma(y)$ to be smooth and bounded. It is also bounded away from zero as $\sigma(y) \ge 1$ because $\psi(y)$ is identically 1 on $[1,2]$. Then we may take

$$\omega(y) = \frac{\psi(y)}{\sigma(y)}.$$

This shows that smooth dyadic weights exist. For any $t \in \mathbb{R}$ and $X > 0$, set

$$A_\omega(t, X, L) = \sum_{n\ge1} a_L(n) n^{-it} \omega\left(\frac{n}{X}\right).$$

and write

$$A_\omega(X, L) = A_\omega(0, X, L).$$

Our result estimates $L(s)$ at $s = \frac{1}{2}+it$ in terms of $A_\omega(t, X, L)$.

Theorem 8.4.3. *Let $L(s)$ be an analytic L-function and let $\omega(y)$ be a smooth dyadic weight. Then*

$$L\left(\frac{1}{2}+it\right) \ll_\varepsilon \mathfrak{q}\,(t,L)^\varepsilon \sup_{X \ll \sqrt{\mathfrak{q}(t,L)}} \left(\frac{|A_\omega(t,X,L)|}{\sqrt{X}}\right).$$

Proof. Take $s = \frac{1}{2}+it$, $X = 1$, and $\Phi(u) = \cos^{-4d_L M}\left(\frac{\pi u}{4M}\right)$ for some large positive integer M in the approximate functional equation. This permits us to write

$$\begin{aligned} L\left(\frac{1}{2}+it\right) = &\sum_{n\ge1} \frac{a_L(n)n^{-it}}{\sqrt{n}} V_t\left(\frac{n}{\sqrt{q_L}}\right) \\ &+ \varepsilon_L(t) \sum_{n\ge1} \frac{\overline{a_L(n)} n^{it}}{\sqrt{n}} V_t\left(\frac{n}{\sqrt{q_L}}\right) + \frac{R\left(\frac{1}{2}+it, 1, L\right)}{q_L^{\frac{1}{4}+i\frac{t}{2}} \gamma_L\left(\frac{1}{2}+it\right)}. \end{aligned}$$

Equation (8.2) implies $\varepsilon_L(t) \ll 1$ while Equations (8.1) and (8.5) together imply that the residue term exhibits exponential decay. This implies that right-hand side of the approximate functional equation is

$$O\left(\sum_{n\geq 1}\frac{a_L(n)n^{-it}}{\sqrt{n}}V_t\left(\frac{n}{\sqrt{q_L}}\right)\right)+O\left(\sum_{n\geq 1}\frac{\overline{a_L(n)}n^{it}}{\sqrt{n}}V_{-t}\left(\frac{n}{\sqrt{q_L}}\right)\right)+O(e^{-|t|}).$$

We now turn to estimating the remaining sums which will be accomplished by applying the smooth dyadic weight. Consider the first sum. By our choice of $\Phi(u)$, the estimates in Proposition 8.2.2 are valid which implies that the summands exhibit rapid decay for $n \gg \sqrt{\mathfrak{q}\,(t, L)}$. Whence the sum is say

$$\sum_{n\ll\sqrt{\mathfrak{q}(t,L)}}\frac{a_L(n)n^{-it}}{\sqrt{n}}V_t\left(\frac{n}{\sqrt{q_L}}\right)+O_{\varepsilon}\left(\mathfrak{q}\,(t,L)^{\varepsilon}\right)$$

Now write

$$V_s(y)=\sum_{k\in\mathbb{Z}}\omega\left(\frac{y}{2^k}\right)V_s(y).$$

Apply this identity to the sum and interchange the resulting two sums by local finiteness to obtain

$$\sum_{k\in\mathbb{Z}}\sum_{n\ll\sqrt{\mathfrak{q}(t,L)}}\frac{a_L(n)n^{-it}}{\sqrt{n}}\omega\left(\frac{n}{2^k\sqrt{q_L}}\right)V_t\left(\frac{n}{\sqrt{q_L}}\right).$$

By compact support of the smooth dyadic weight, for each k the inner sum over n is supported on the dyadic block $n \asymp X_k$ where $X_k = 2^k\sqrt{q_L}$. As $n \ll \sqrt{\mathfrak{q}\,(t, L)}$, the summands which contribute must satisfy $k \ll \log \mathfrak{q}_\infty\,(t, L)$. Therefore our double sum can be expressed as

$$\sum_{k\ll\log\mathfrak{q}_\infty(t,L)}\sum_{n\asymp X_k}\frac{a_L(n)n^{-it}}{\sqrt{n}}\omega\left(\frac{n}{X_k}\right)V_t\left(\frac{n}{\sqrt{q_L}}\right).$$

Let $V_k(y) = \frac{1}{\sqrt{y}}V_t\left(\frac{y}{\sqrt{q_L}}\right)$. By Abel summation, the inner sum is O of

$$\sup_{n\asymp X_k}|A_\omega(X_k,t,L)|\,|V_k(n)|+\int_{u\asymp X_k}|A_\omega(u,t,L)||V_k'(u)|\,du.$$

In view of Proposition 8.2.2, we have the estimates

$$V_k(y)=O\left(\frac{1}{\sqrt{y}}\right)\quad\text{and}\quad V_k'(y)=O\left(\frac{1}{y^{\frac{3}{2}}}\right),$$

for $y \ll \sqrt{\mathfrak{q}\,(t, L)}$. Whence our previous expression is O of

$$\sup_{X\asymp X_k}\left(\frac{|A_\omega(t,X,L)|}{\sqrt{X}}\right).$$

As there are $O_\varepsilon\left(\mathfrak{q}\left(t,L\right)^\varepsilon\right)$ many such k, the bound above implies that our sum is O_ε of

$$\mathfrak{q}\left(t,L\right)^\varepsilon \sup_{X \ll \sqrt{\mathfrak{q}(t,L)}} \left(\frac{|A_\omega(t,X,L)|}{\sqrt{X}}\right).$$

The estimate for the second sum is treated analogously. Thus

$$L\left(\frac{1}{2}+it\right) \ll_\varepsilon \mathfrak{q}\left(t,L\right)^\varepsilon \sup_{X \ll \sqrt{\mathfrak{q}(t,L)}} \left(\frac{|A_\omega(t,X,L)|}{\sqrt{X}}\right),$$

upon absorbing smaller order error terms. □

As any useful estimate for the sum $A_\omega(t,X,L)$ will be in terms of powers of X, the supremum in Theorem 8.4.4 will automatically pick out the largest possible bound when X is the square root of the analytic conductor. This means that the savings of $\sqrt{X}$ in the denominator is essentially as large as possible. For example, we obtain the convexity bound as an application. Since the Dirichlet series of $L(s)$ is absolutely convergent for $\sigma < 1$, we have a bound of shape

$$\sum_{n \le X} |a_L(n)| \ll_\varepsilon X^{1+\varepsilon}.$$

Then $A_\omega(t,X,L) \ll_\varepsilon X^{1+\varepsilon}$ as well and we obtain

$$\sup_{X \ll \sqrt{\mathfrak{q}(t,L)}} \frac{|A_\omega(t,X,L)|}{\sqrt{X}} \ll_\varepsilon \mathfrak{q}\left(t,L\right)^{\frac{1}{4}+\varepsilon}, \tag{8.6}$$

which gives the convexity bound. As we believe $L(s)$ satisfies the Lindelöf hypothesis, we should expect lots of cancellation in the sum $A_\omega(t,X,L)$. In fact, the expected cancellation should be $O\left(\mathfrak{q}\left(t,L\right)^{\frac{1}{4}}\right)$ in light of the aforementioned bound. This means we expect $A_\omega(t,X,L)$ to exhibit square-root cancellation in the sense

$$A_\omega(t,X,L) \ll_\varepsilon X^{\frac{1}{2}+\varepsilon}.$$

As the coefficients $a_L(n)$ may very well be real, the expected cancellation must come from the terms $n^{-it} = e^{-it\log(n)}$ which acts on the coefficients $a_L(n)$ by rotation. In effect, we should think of the terms $a_L(n)n^{-it}$ as modeling identically distributed random variables.

The case when $t = 0$ is deserving of unique importance. In this case, we are estimating the value of $L(s)$ at the central point. The value of $L(s)$ at the central point is called the *central value* of $L(s)$. Many important properties about $L(s)$ can be connected to its central value. Any argument used to estimate the central value of an L-function is called a *central value estimate*. Taking $t = 0$ in Theorem 8.4.3 gives a way to obtain central value estimates.

Theorem 8.4.4. *Let $L(s)$ be an analytic L-function and let $\omega(y)$ be a smooth dyadic weight. Then*

$$L\left(\frac{1}{2}\right) \ll_\varepsilon \mathfrak{q}\left(L\right)^\varepsilon \max_{X \ll \sqrt{\mathfrak{q}(L)}} \left(\frac{|A_\omega(X,L)|}{\sqrt{X}}\right).$$

Proof. Take $t = 0$ in Theorem 8.4.3. □

8.5 Logarithmic Derivatives

Recall that $L(s)$ nonzero in the half-plane $\sigma > 1$. As this region is simply connected, there exists a unique holomorphic logarithm $\log L(s)$ there. By absolute convergence of the Euler product, we may write

$$\log L(s) = -\sum_{p}\sum_{j}\log(1-\alpha_j(p)p^{-s}).$$

Moreover, the bound $|\alpha_j(p)| \leq p^{\theta}$ ensures that $|\alpha_j(p)p^{-s}| < 1$ in this half-plane. Therefore the Taylor series of the logarithm is valid in this region and we may further write

$$\log L(s) = \sum_{p}\sum_{j}\sum_{k\geq 1}\frac{\alpha_j(p)^k}{kp^{ks}}.$$

While this triple sum converges for $\sigma > 1$, the bound $|\alpha_j(p)p^{-s}| < p^{\theta-\sigma}$ only guarantees absolutely convergence for $\sigma > 1+\theta$. It is in this half-plane that we may differentiate termwise. A short computation shows

$$\frac{L'}{L}(s) = -\sum_{n\geq 1}\frac{\Lambda_L(n)}{n^s},$$

where

$$\Lambda_L(n) = \begin{cases} \sum_j \alpha_j(p)^k\log(p) & \text{if } n = p^k, \\ 0 & \text{otherwise.} \end{cases}$$

We call $\Lambda_L(n)$ the *Von Mangoldt coefficients* of $L(s)$.

There is an incredibly useful formula for the logarithmic derivative of $L(s)$ which is often the starting point for deeper analytic investigations. To deduce it, we require a more complete understanding of the completion $\Lambda(s,L)$. First observe that the zeros ρ of $\Lambda(s,L)$ are contained within the critical strip. Indeed, by our earlier discussion of zeros, $\Lambda(s,L)$ is nonzero for $\sigma > 1$ and the functional equation implies that $\Lambda(s,L)$ is nonzero for $\sigma < 0$ too. This means that the zeros of $\Lambda(s,L)$ are exactly nontrivial zeros of $L(s)$. Now let us setup some notation. We define $\xi(s,L)$ by

$$\xi(s,L) = (s(1-s))^{r_L}\Lambda(s,L).$$

Then $\xi(s,L)$ is just $\Lambda(s,L)$ with the potential poles at $s=0$ and $s=1$ removed. This means $\xi(s,L)$ is entire. The functional equation also implies

$$\xi(s,L) = \varepsilon_L\overline{\xi(1-\overline{s},L)}.$$

Our result will compute the Hadamard factorization of $\xi(s,L)$ and taking its logarithmic derivative will give a formula relating the logarithmic derivative of $L(s)$ to the zeros of $L(s)$.

Proposition 8.5.1. *For any analytic L-function $L(s)$, there exist constants A_L and B_L such that*

$$\xi(s, L) = e^{A_L + B_L s} \prod_{\rho \neq 0,1} \left(1 - \frac{s}{\rho}\right) e^{\frac{s}{\rho}},$$

and hence the sum

$$\sum_{\rho \neq 0,1} \frac{1}{|\rho|^{1+\varepsilon}},$$

is convergent provided the product and sum are both counted with multiplicity and ordered with respect to the size of the ordinate. Moreover,

$$-\frac{L'}{L}(s) = \frac{r_L}{s} + \frac{r_L}{s-1} + \frac{1}{2}\log q_L + \frac{\gamma_L'}{\gamma_L}(s) - B_L - \sum_{\rho \neq 0,1} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right).$$

Proof. Recall that $\xi(s, L)$ is entire and its zeros are exactly the nontrivial zeros of $L(s)$. We claim $\xi(s, L)$ is of order 1. This follows from Stirling's formula and that $(s-1)^{r_L} L(s)$ is of order 1. Then the Hadamard factorization theorem implies

$$\xi(s, L) = e^{A_L + B_L s} \prod_{\rho \neq 0,1} \left(1 - \frac{s}{\rho}\right) e^{\frac{s}{\rho}},$$

for some constants A_L and B_L and that the desired sum converges. This proves the first statement. We will compute the logarithmic derivative of $\xi(s, L)$ in two ways to prove the second statement. On the one hand, taking the logarithmic derivative of the definition of $\xi(s, L)$ yields

$$\frac{\xi'}{\xi}(s, L) = \frac{r_L}{s} + \frac{r_L}{s-1} + \frac{1}{2}\log q_L + \frac{\gamma_L'}{\gamma_L}(s) + \frac{L'}{L}(s).$$

On the other hand, taking the logarithmic derivative of the Hadamard factorization gives

$$\frac{\xi'}{\xi}(s, L) = B_L + \sum_{\rho \neq 0,1} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right).$$

Equating these expressions to obtain

$$B_L + \sum_{\rho \neq 0,1} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) = \frac{r_L}{s} + \frac{r_L}{s-1} + \frac{1}{2}\log q_L + \frac{\gamma_L'}{\gamma_L}(s) + \frac{L'}{L}(s).$$

This is equivalent to the second statement. □

Explicit evaluation of the constants A_L and B_L can be challenging and heavily depend upon the particular L-function under investigation. However, useful estimates are not too difficult to obtain and this is often sufficient for applications.

Chapter 9

Todo: [Moments]

Chapter 10

Todo: [Analytic Theory of the Riemann Zeta Function]

Chapter 11

Todo: [Analytic Theory of Dirichlet L-functions]

Chapter 12

Todo: [Analytic Theory of Dedekind Zeta Functions]

Part IV

Appendices