FOURIER ANALYSIS IN NUMBER THEORY

SHANSHAN DING

04/01/2008

Contents

Mathematics compares the most diverse phenomena and discovers the secret analogies that unite them.

–J. Fourier, 1822

1. Introduction

One of the most surprising and stunning interplays in mathematics has been that between Fourier analysis and number theory, which also brings together strands of harmonic analysis, complex analysis, mathematical physics, ergodic theory, and class field theory. In this paper we present several results from this seemingly unlikely but incredibly revealing intersection of ideas. In Section 3, we give a proof of the quadratic reciprocity law that fully incorporates the discrete Fourier transform. In Section 4, we prove Dirichlet's theorem on primes in arithmetic progression in all its glory, where we use the theory of Fourier analysis on finite abelian groups in the first and indispensable step of the proof. In Section 5, we visit the border between number theory and dynamical systems with Weyl's criterion, where we use a key result from Fourier analysis on the circle to carry out a pivotal step in its proof. Finally in Section 6, we give a brief overview of some more advanced topics, including areas of active current research.

Our presentation of the material is almost entirely self-contained up until Section 6. Dirichlet's theorem in particular is painstakingly proved in full and from scratch; our proof makes only sparing use of available properties of the zeta function[1]. We begin with an introduction to Fourier analysis in Section 2.

2. Preliminaries

In this section we develop the elements of Fourier analysis that we will use in later sections to prove our number-theoretic results.

2.1. **Discrete Fourier transform.** We begin with Fourier analysis on the group of integers modulo n. Suppose $a, x \in \mathbb{Z}/n\mathbb{Z}$. Define

$$e_a(x) = \exp\left(\frac{2\pi i a x}{n}\right). \tag{2.1}$$

Definition 2.1. *Suppose f is a complex-valued function on $\mathbb{Z}/n\mathbb{Z}$. The* discrete Fourier transform *of f on $\mathbb{Z}/n\mathbb{Z}$ is*

$$\hat{f}(x) = (f, e_x) = \sum_{k=0}^{n-1} f(k) e_x(-k).$$

The result most helpful to us will be the following:

Theorem 2.2 (Inversion formula)**.** *Let $\hat{f}$ be defined as above. Then*

$$f(k) = \frac{1}{n} \sum_{x=0}^{n-1} \hat{f}(x) e_k(x).$$

The key to proving the inversion formula is thinking of the set of complex-valued functions on $\mathbb{Z}/n\mathbb{Z}$ as an n-dimensional vector space V, endowed with the Hermitian

[1]The purpose of this is to help the author gain a better grasp of real analytic techniques.

inner product

$$(f,g) = \sum_{k=0}^{n-1} f(k)\overline{g(k)} \tag{2.2}$$

and the associated norm

$$\|f\|^2 = \sum_{k=0}^{n-1} |f(k)|^2. \tag{2.3}$$

Lemma 2.3. *The family* $\{e_0, e_1, \ldots, e_{n-1}\}$ *is orthogonal. In fact,*

$$(e_m, e_l) = \begin{cases} n & \text{if } m = l, \\ 0 & \text{if } m \neq l. \end{cases}$$

Proof. We have

$$(e_m, e_l) = \sum_{k=0}^{n-1} e_m(k)\overline{e_l(k)} = \sum_{k=0}^{n-1} \exp\left(\frac{2\pi i(m-l)k}{n}\right). \tag{2.4}$$

If $m = l$, then each term in the sum is equal to 1, thus the sum is equal to n. If $m \neq l$, then let $r = \exp\left(\frac{2\pi i(m-l)}{n}\right)$ and observe that

$$(e_m, e_l) = 1 + r + \cdots + r^{n-1} = \frac{1-r^n}{1-r}. \tag{2.5}$$

Since $r \neq 1$ and $r^n = 1$, $(e_m, e_l) = 0$. □

Proof of Theorem 2.2. Since the n functions $e_0, e_1, \ldots, e_{n-1}$ are orthogonal, they must be linearly independent, and since the vector space V is n-dimensional, $\{e_0, e_1, \ldots, e_{n-1}\}$ is an orthogonal basis for V. Now define $\tilde{e}_l = \frac{e_l}{\sqrt{n}}$. By Lemma 2.3, each vector e_l has norm $\sqrt{n}$, so $\{\tilde{e}_0, \tilde{e}_1, \ldots, \tilde{e}_{n-1}\}$ is an orthonormal basis for V. Hence for any complex-valued function f on $\mathbb{Z}/n\mathbb{Z}$, we have

$$f = \sum_{x=0}^{n-1} (f, \tilde{e}_x)\tilde{e}_x = \frac{1}{n}\sum_{x=0}^{n-1} (f, e_x)e_x = \frac{1}{n}\sum_{x=0}^{n-1} \hat{f}(x)e_x. \tag{2.6}$$

Observing that $e_x(k) = e_k(x)$, the proof of the inversion formula is complete. □

2.2. **Fourier analysis on finite abelian groups.** Having introduced Fourier analysis on $\mathbb{Z}/n\mathbb{Z}$, we want to generalize to finite abelian groups.

Definition 2.4. *Let* G *be a finite abelian group and let* S^1 *denote the unit circle in* $\mathbb{C}$. *A* character *on* G *is a complex-valued function* $e : G \to S^1$ *such that for all* $a, b \in G$, $e(ab) = e(a)e(b)$. *The* trivial character *satisfies* $e(a) = 1$ *for all* $a \in G$.

We denote by $\hat{G}$ the set of all characters of G. Observe that $\hat{G}$ is an abelian group under the group law defined by $(ee')(a) = e(a)e'(a)$ for all $a \in G$, with the trivial character as the identity. We call $\hat{G}$ the *dual group* of G.

Example. If $G = \mathbb{Z}/n\mathbb{Z}$, then

$$\hat{G} = \{e_0, e_1, \ldots, e_{n-1}\} \cong G, \tag{2.7}$$

where e_m is defined as in (2.1).

Theorem 2.5. *Let V be the vector space of complex-valued functions on G. Then $\hat{G}$ is an orthonormal basis for V.*

To prove this theorem, first we prove that the characters of G are orthonormal. The following proposition will be helpful:

Proposition 2.6. *If e is a non-trivial character of G, then $\sum_{a\in G} e(a) = 0$.*

Proof. Since e is non-trivial, we can choose $b \in G$ such that $e(b) \neq 1$. Then we have

$$e(b)\sum_{a\in G} e(a) = \sum_{a\in G} e(b)e(a) = \sum_{a\in G} e(ba) = \sum_{a\in G} e(a), \tag{2.8}$$

where the last equality follows because both a and ba range over G. Since $e(b) \neq 1$, it must be that $\sum_{a\in G} e(a) = 0$. □

Lemma 2.7. *The characters of G form an orthonormal family with respect to the Hermitian inner product on V defined by*

$$(f, g) = \frac{1}{|G|}\sum_{a\in G} f(a)\overline{g(a)}.$$

Proof. Let $e \in \hat{G}$. Since e takes its values on S^1, $|e(a)| = 1$, and thus

$$(e, e) = \frac{1}{|G|}\sum_{a\in G} e(a)\overline{e(a)} = \frac{1}{|G|}\sum_{a\in G}|e(a)|^2 = 1. \tag{2.9}$$

Now suppose $e, e' \in \hat{G}$ and $e \neq e'$. Then $e(e')^{-1}$ is non-trivial, and by Proposition 2.6,

$$\sum_{a\in G} e(a)(e'(a))^{-1} = \sum_{a\in G}(e(e')^{-1})(a) = 0. \tag{2.10}$$

Since $(e'(a))^{-1} = \overline{e'(a)}$, $(e, e') = 0$. □

The orthonormality of $\hat{G}$ shows that $|\hat{G}| \leq |G|$. The key to proving Theorem 2.5 is showing that $|\hat{G}| = |G|$. We start with a sufficient condition for a function to be a character.

Proposition 2.8. *If $e : G \to \mathbb{C}\backslash\{0\}$ is a multiplicative function, namely $e(ab) = e(a)e(b)$ for all $a, b \in G$, then $e \in \hat{G}$.*

Proof. We want to show that e takes all of its values on S^1. Assume $|e(a)| \neq 1$ for some $a \in G$. Then $|e(a)|^n$ is different for every n. But $|e(a)|^n = |e(a^n)|$, and since G is a finite group, $\{|e(a^n)| : n = 1, 2, \ldots\}$ is a finite set. Thus $e(a) \in S^1$ for all $a \in G$. □

Proposition 2.9. *Suppose $G = G_1 \oplus G_2$. If $e_i : G_i \to S^1$ is a character of G_i $(i = 1, 2)$, then $e = e_1 \oplus e_2$, defined by $e(a_1, a_2) = e_1(a_1)e_2(a_2)$, is a character of G. In fact, all characters of G is of this form, thus*

$$\hat{G} \cong \hat{G}_1 \oplus \hat{G}_2.$$

Proof. Observe that e is a non-vanishing multiplicative function on $G_1 \oplus G_2$, and that as such, it is a character of G by Proposition 2.8. Conversely, if $e \in G$, then $e_i = e|_{G_i}$ is clearly a character of G_i, and it is not difficult to see that $e = e_1 \oplus e_2$. □

Proof of Theorem 2.5. By the fundamental theorem of finite abelian groups,

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}, \tag{2.11}$$

for integers $n_1, \ldots, n_k$. Denote $\mathbb{Z}/n_i\mathbb{Z}$ as G_i. By Proposition 2.9 and (2.7),

$$\hat{G} \cong \hat{G}_1 \oplus \cdots \oplus \hat{G}_k \cong G_1 \oplus \cdots \oplus G_k \cong G. \tag{2.12}$$

In particular, this shows that $|\hat{G}| = |G| = \dim V$. Since we have already shown that the characters of G are orthonormal, they must be linearly independent, and as such, $\hat{G}$ is an orthonormal basis for V. □

Theorem 2.5 allows us to generalize the inversion formula for finite abelian groups.

Theorem 2.10. *Let G be a finite abelian group, and let f be a function on G. Define*

$$\hat{f}(e) = (f, e) = \frac{1}{|G|} \sum_{a \in G} f(a)\overline{e(a)},$$

then $f = \sum_{e \in \hat{G}} \hat{f}(e)e$.

Proof. Since the characters of G form a basis for the vector space of functions on G, we know that $f = \sum_{e \in \hat{G}} c_e e$ for some set of constants c_e. By the orthonormality relations satisfied by the characters, we see that $c_e = (f, e)$. □

The sum $\sum_{e \in \hat{G}} \hat{f}(e)e$ is known as the *Fourier series* of f. The preceding theorem says that a function on a finite abelian group is equal to its Fourier series.

2.3. **Fourier analysis on the circle.** We now shift our focus to the continuous Fourier transform. Here we will use the terms "2π-periodic function on $\mathbb{R}$" and "function on the circle" interchangeably.

Definition 2.11. *If f is a Riemann integrable function on an interval $[a, b] \subset \mathbb{R}$ of length L, then the n^{th}* Fourier coefficient *of f is defined by*

$$\hat{f}(n) = \frac{1}{L} \int_a^b f(x) \exp\left(\frac{-2\pi i n x}{L}\right) dx, \quad n \in \mathbb{Z}.$$

Analogously to the finite case, the *Fourier series* of f is given formally by

$$\sum_{n=-\infty}^{\infty} \hat{f}(n) \exp\left(\frac{2\pi i n x}{L}\right). \tag{2.13}$$

In the case where f is defined on an interval in $\mathbb{R}$, the Fourier series of f exhibits mean-square convergence to f. As we will not need this result in later sections, we do not prove it here.

Fourier series are a subset of a larger family called the *trigonometric series*, which are expressions of the form

$$\sum_{n=-\infty}^{\infty} c_n \exp\left(\frac{2\pi i n x}{L}\right). \tag{2.14}$$

If $c_n = 0$ for all but finitely many terms, then trigonometric series is called a *trigonometric polynomial*. For N a positive integer, the N^{th} *partial sum* of the Fourier series of f

$$S_N(f)(x) = \sum_{n=-N}^{N} \hat{f}(n) \exp\left(\frac{2\pi i n x}{L}\right) \tag{2.15}$$

is a trigonometric polynomial.

The primary result of importance to us is the following:

Theorem 2.12 (Periodic analogue of Weierstrass approximation theorem)**.** *If f is a continuous function on the circle, then f can be uniformly approximated by trigonometric polynomials.*

Remark. By simple scaling, this result would actually tell us that any continuous periodic function can be uniformly approximated by trigonometric polynomials.

In working toward a proof of Theorem 2.12, we introduce one of the most fundamental concepts in Fourier analysis.

Definition 2.13. *Let f and g be two Riemann integrable functions on the circle. We define their* convolution *$f * g$ on $[-\pi, \pi]$ by*

$$(f * g)(x) = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(y) g(x - y) dy.$$

Observe that by the linearity of the integral, for any Riemann integrable functions f, g, and h on the circle,

$$f * (g + h) = (f * g) + (f * h), \tag{2.16}$$

and for any complex number c,

$$(cf) * g = c(f * g) = f * (cg). \tag{2.17}$$

For our purposes, the importance of convolutions lies in their relationship with the partial sums of Fourier series. Let f be a Riemann integrable function on the circle, and observe

that

$$S_N(f)(x) = \sum_{n=-N}^{N} \hat{f}(n)e^{inx} = \sum_{n=N}^{N} \left(\frac{1}{2\pi} \int_{-\pi}^{\pi} f(y)e^{-iny}dy \right) e^{inx} \\ = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(y) \left(\sum_{n=-N}^{N} e^{in(x-y)} \right) dy, \tag{2.18}$$

so that

$$S_N(f)(x) = (f * D_N)(x), \quad \text{where} \quad D_N(x) = \sum_{n=-N}^{N} e^{inx}. \tag{2.19}$$

Definition 2.14. *As defined above, D_N $(N \geq 0)$ is known as the N^{th}* Dirichlet kernel. *The N^{th}* Fejèr kernel *F_N $(N \geq 1)$ is given by*

$$F_N(x) = \frac{D_0(x) + \cdots + D_{N-1}(x)}{N}. \tag{2.20}$$

Proposition 2.15. *We have*

$$D_N(x) = \frac{\sin(N + 1/2)x}{\sin(x/2)} \quad \textit{and} \quad F_N(x) = \frac{1}{N} \frac{\sin^2(Nx/2)}{\sin^2(x/2)}.$$

Proof. For the Dirichlet kernel,

$$D_N(x) = \sum_{n=-N}^{N} e^{inx} = e^{-iNx} \frac{1 - e^{i(2N+1)x}}{1 - e^{ix}} = \frac{e^{-i(N+1/2)x}}{e^{-ix/2}} \frac{(1 - e^{i(2N+1)x})}{(1 - e^{ix})} \\ = \frac{e^{-i(N+1/2)x} - e^{i(N+1/2)x}}{e^{-ix/2} - e^{ix/2}} = \frac{\sin((N + 1/2)x)}{\sin(x/2)}. \tag{2.21}$$

For the Fejèr kernel, by the identity we just derived,

$$\sin(x/2)D_N(x) = \sin((N + 1/2)x), \tag{2.22}$$

thus

$$N \sin^2(x/2)F_N(x) = \sin^2(x/2) \sum_{n=0}^{N-1} D_n(x) = \sum_{n=0}^{N-1} \sin((n + 1/2)x) \sin(x/2) \\ = \frac{1}{2} \sum_{n=0}^{N-1} (\cos nx - \cos((n + 1)x)) = \frac{1 - \cos Nx}{2} = \sin^2(Nx/2), \tag{2.23}$$

and the desired identity follows at once. □

Lemma 2.16. *The Fejèr kernels $\{F_N(x)\}$ satisfy the following properties:*

(1) For all $N \geq 1$

$$\frac{1}{2\pi} \int_{-\pi}^{\pi} F_N(x)dx = 1.$$

(2) There exists $M > 0$ such that for all $N \geq 1$,

$$\int_{-\pi}^{\pi} |F_N(x)|dx \leq M.$$

(3) For every $\delta > 0$,

$$\int_{\delta \leq |x| \leq \pi} |F_N(x)|dx \to 0 \quad as\ N \to \infty.$$

Proof. To see the first property, note that for an integer n,

$$\int_{-\pi}^{\pi} e^{inx}dx = \begin{cases} 2\pi & \text{if } n = 0 \\ 0 & \text{if } n \neq 0, \end{cases} \tag{2.24}$$

so that

$$\int_{-\pi}^{\pi} D_N(x)dx = 2\pi \ \text{ for all } \ N \geq 0. \tag{2.25}$$

The second property follows at once from the first property and the observation that F_N is positive. Finally, for every $\delta > 0$, there exists constant $c_\delta > 0$ such that $\sin^2(x/2) \geq c_\delta$ whenever $\delta \leq |x| \leq \pi$, hence

$$\int_{\delta \leq |x| \leq \pi} |F_N(x)|dx \leq \int_{\delta \leq |x| \leq \pi} \frac{dx}{Nc_\delta} \leq \frac{2(\pi - \delta)}{Nc_\delta}, \tag{2.26}$$

from which the third property follows. □

It is interesting to note that while the Dirichlet kernels fail to satisfy all of the properties in Lemma 2.16, their averages, namely the Fejèr kernels, are very well behaved functions, as the next theorem illustrates.

Theorem 2.17. *Let f be a Riemann integrable function on the circle. If f is continuous at x, then*

$$\lim_{N \to \infty} (f * F_N)(x) = f(x).$$

If f is continuous everywhere, then this limit is uniform.

Proof. By (1) of Lemma 2.16,

$$\begin{aligned} (f * F_N)(x) - f(x) &= \frac{1}{2\pi} \int_{-\pi}^{\pi} F_N(y) f(x - y)dy - \frac{f(x)}{2\pi} \int_{-\pi}^{\pi} F_N(y)dy \\ &= \frac{1}{2\pi} \int_{-\pi}^{\pi} F_N(y)[f(x - y) - f(x)]dy. \end{aligned} \tag{2.27}$$

Let f be bounded by B, and suppose f is continuous at x. For $\varepsilon > 0$, let us choose δ such that $|f(x - y) - f(x)| < \varepsilon$ whenever $|y| < \delta$. Then

$$\begin{aligned} |(f * F_N)(x) - f(x)| &= \left| \frac{1}{2\pi} \int_{-\pi}^{\pi} F_N(y)[f(x - y) - f(x)]dy \right| \\ &\leq \frac{\varepsilon}{2\pi} \int_{|y| < \delta} |F_N(y)|dy + \frac{B}{\pi} \int_{\delta \leq |y| \leq \pi} |F_N(y)|dy. \end{aligned} \tag{2.28}$$

By (2) of Lemma 2.16, the first term above is bounded by $\frac{\varepsilon M}{2\pi}$ for some constant M, and by (3) of the same Lemma, the second term is less than ε for all large N. This proves the first claim. To see the second claim, recall that continuous functions on compact sets are uniformly continuous, so δ could be chosen independent of x. □

Proof of Theorem 2.12. By the linearity of convolutions,

$$f * F_n = \frac{(f * D_0) + \cdots + (f * D_{N-1})}{N} = \frac{S_0(f) + \cdots + S_{N-1}(f)}{N}. \tag{2.29}$$

Since the partial sums of Fourier series are trigonometric polynomials, Theorem 2.12 follows immediately from Theorem 2.17. □

3. Quadratic Reciprocity Law

The quadratic reciprocity law is a classic result from elementary number theory. It was conjectured by Euler and Legendre and first proven by Gauss in 1796. There are now over 200 published proofs of the theorem, some even draw techniques from class field theory and K-theory (see [5]). In this section we give a proof using the discrete Fourier transform, which is a variant of Gauss's sixth proof (with Gauss sums).

Definition 3.1. *Let a be an integer and p be an odd prime. The* Legendre symbol *for this pair is defined by*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution,} \\ -1 & \text{otherwise.} \end{cases}$$

Theorem 3.2 (Quadratic reciprocity law)**.** *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

We begin with some elementary observations regarding the Legendre symbol.

Proposition 3.3. *Let a and p be as above. Then*

(1) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$,

(2) $\left(\frac{1}{p}\right) = 1$ *while* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,

(3) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$, *and*

(4) $a \equiv b \pmod{p}$ *implies that* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proof. The first part is known as Euler's criterion, of which all subsequent parts are simple corollaries. To see Euler's criterion, note that the case where p divides a is trivial, so it suffices to show that $x^2 \equiv a \pmod{p}$ has a solution if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. If $x^2 \equiv a \pmod{p}$ for some x, then $x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}$, and thus by Fermat's little theorem, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Conversely, if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, then let b be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, and we have that $b^{\frac{n(p-1)}{2}} \equiv 1 \pmod{p}$ for some n such that $a = b^n$. Since b

is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, $(p-1)$ must divide $\frac{n(p-1)}{2}$, and thus n must be even. It follows that $b^{\frac{n}{2}}$ is a solution to $x^2 \equiv a \pmod{p}$. □

Next we derive four lemmas involving the discrete Fourier transform of the Legendre symbol as a function of its top entry. For p an odd prime, let $h_p(x) = \left(\frac{x}{p}\right)$. Note that by (4) of Proposition 3.3, $h_p(x)$ is well-defined on $\mathbb{Z}/p\mathbb{Z}$.

Lemma 3.4. *Let $\hat{h}_p$ be the discrete Fourier transform of h_p on $\mathbb{Z}/p\mathbb{Z}$. Then*

$$\hat{h}_p(-x) = h_p(x)\hat{h}_p(-1).$$

Proof. By definition of the discrete Fourier transform,

$$\hat{h}_p(-x) = \sum_{a=0}^{p-1} h_p(a) \exp\left(\frac{2\pi i a x}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \exp\left(\frac{2\pi i a x}{p}\right). \tag{3.1}$$

First suppose $x \neq 0$. Let $ax = b$. Since a and b both range over $(\mathbb{Z}/p\mathbb{Z})^*$,

$$\hat{h}_p(-x) = \sum_{b=1}^{p-1} \left(\frac{x^{-1}b}{p}\right) \exp\left(\frac{2\pi i b}{p}\right) = \left(\frac{x^{-1}}{p}\right) \sum_{b=1}^{p-1} \left(\frac{b}{p}\right) \exp\left(\frac{2\pi i b}{p}\right), \tag{3.2}$$

where x^{-1} is the multiplicative inverse of x in $(\mathbb{Z}/p\mathbb{Z})^*$. It follows from (2) through (4) of Proposition 3.3 that $\left(\frac{x}{p}\right) = \left(\frac{x^{-1}}{p}\right)$, hence

$$\hat{h}_p(-x) = \left(\frac{x}{p}\right) \hat{h}_p(-1) = h_p(x)\hat{h}_p(-1). \tag{3.3}$$

If $x = 0$, then since there are as many squares as non-squares in $(\mathbb{Z}/p\mathbb{Z})^*$,

$$\hat{h}_p(-x) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0, \tag{3.4}$$

and since $h_p(0) = 0$, this concludes the proof of the lemma. □

Lemma 3.5. *Let $g = \hat{h}_p(-1)$. Then $g^2 = (-1)^{\frac{p-1}{2}} p$.*

Remark. This g is a Gauss sum.

Proof. By the inversion formula for the discrete Fourier transform,

$$p h_p(x) = \sum_{a=0}^{p-1} \hat{h}_p(a) \exp\left(\frac{2\pi i a x}{p}\right) = \hat{\hat{h}}_p(-x). \tag{3.5}$$

Taking the discrete Fourier transform of both sides of the equation in Lemma 3.4 and noting that $\hat{h}_p(-1)$ is a constant, we see that

$$p h_p(x) = \hat{\hat{h}}_p(-x) = \hat{h}_p(x)\hat{h}_p(-1). \tag{3.6}$$

Setting $x = -1$, we obtain that

$$g^2 = p h_p(-1) = p\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} p, \tag{3.7}$$

as was to be shown. □

Lemma 3.6. *Let g be defined as above. If p and q are distinct odd primes, then*

$$g^{q-1} \equiv \left(\frac{g^2}{q}\right) \pmod{q}.$$

Proof. This lemma follows at once from Euler's criterion. □

Lemma 3.7. *If p and q are distinct odd primes, then*

$$(\hat{h}_p(x))^q \equiv \hat{h}_p(qx) \pmod{q},$$

where the congruence takes place in the ring $\mathbb{Z}[e^{2\pi i/p}]$.

Proof. Recall that for all integers u and v, $(u+v)^q \equiv u^q + v^q \pmod{q}$. Thus

$$\begin{aligned}(\hat{h}_p(x))^q &= \left(\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\exp\left(\frac{-2\pi iax}{p}\right)\right)^q \\ &\equiv \sum_{a=1}^{p-1}\left(\left(\frac{a}{p}\right)\exp\left(\frac{-2\pi iax}{p}\right)\right)^q \pmod{q}.\end{aligned} \tag{3.8}$$

Because q is odd, $\left(\frac{a}{p}\right)^q = \left(\frac{a}{p}\right)$, hence

$$(\hat{h}_p(x))^q \equiv \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\exp\left(\frac{-2\pi iaqx}{p}\right) \pmod{q}, \tag{3.9}$$

as desired. □

We are now ready to prove the quadratic reciprocity law.

Proof of Theorem 3.2. Let $x = -1$ in Lemma 3.7, we have

$$g^q = (\hat{h}_p(-1))^q \equiv \hat{h}_p(-q) \pmod{q}, \tag{3.10}$$

hence by Lemma 3.4,

$$g^q \equiv \left(\frac{q}{p}\right) g \pmod{q}. \tag{3.11}$$

Since g is not an integer, at this point we are still working in the ring $\mathbb{Z}[e^{2\pi i/p}]$, which in general is not a unique factorization domain, so we cannot cancel g from both sides of the congruence just yet.

Multiply both sides of (3.11) by g and apply Lemma 3.6, we see that

$$\left(\frac{g^2}{q}\right) g^2 \equiv \left(\frac{q}{p}\right) g^2 \pmod{q}. \tag{3.12}$$

By Lemma 3.5, g^2 is an integer, so the above congruence takes place in the unique factorization domain $\mathbb{Z}$. Now we divide g^2 from both sides and obtain

$$\left(\frac{g^2}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod{q}. \tag{3.13}$$

Recall that $\left(\frac{g^2}{q}\right)$ and $\left(\frac{q}{p}\right)$ can only take the values of ± 1. Since q is odd, (3.13) is actually an equality, and since $g^2 = (-1)^{\frac{p-1}{2}}p$, by (4) of Proposition 3.3,

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{3.14}$$

To finish, simply multiply both sides of (3.14) by $\left(\frac{p}{q}\right)$. □

4. Dirichlet's Theorem on Primes in Arithmetic Progression

A number theorist by trade, Dirichlet learned analysis from Fourier and other like-minded mathematicians while studying in Paris. Later, Dirichlet's theorem on primes in arithmetic progression represented the beginning of rigorous analytic number theory. It was conjectured by Gauss and proved by Dirichlet in 1837, and the theory of Fourier series on finite abelian groups played a key role in its proof.

Theorem 4.1 (Dirichlet's theorem)**.** *If q and l are relatively prime positive integers, then there are infinitely many primes of the form $l + kq$ with $k \in \mathbb{Z}$.*

As Euler had proven the infinitude of primes by illustrating the divergence of $\sum_{p \text{ prime}} 1/p$, Dirichlet proved his theorem on primes in arithmetic progression by showing the divergence of $\sum_{p \equiv l \pmod q} 1/p$, where the sum is over all primes congruent to l modulo q. For convenience, in what follows p will be understood to be prime, and since q will be fixed, we shall omit "(mod q)" in our notation.

4.1. Dirichlet characters, L-functions, and outline of the proof.

In the notation of Section 2.2, let $G = (\mathbb{Z}/q\mathbb{Z})^*$. Note that $|G| = \varphi(q)$, where φ is the Euler phi-function. Consider the function δ_l on G defined by

$$\delta_l(n) = \begin{cases} 1 & \text{if } n \equiv l \pmod q, \\ 0 & \text{otherwise.} \end{cases} \tag{4.1}$$

We can expand this function in a Fourier series as

$$\delta_l(n) = \sum_{e \in \hat{G}} \hat{\delta}_l(e) e(n), \tag{4.2}$$

where

$$\hat{\delta}_l(e) = \frac{1}{|G|} \sum_{m \in G} \delta_l(m)\overline{e(m)} = \frac{1}{|G|}\overline{e(l)}, \tag{4.3}$$

and hence

$$\delta_l(n) = \frac{1}{|G|} \sum_{e \in \hat{G}} \overline{e(l)} e(n). \tag{4.4}$$

We can extend δ_l to all of $\mathbb{Z}$ by setting $\delta_l(m) = 0$ whenever m and q are not relatively prime. The characters of G can be extended similarly.

Definition 4.2. *The extensions of the characters $e \in \hat{G}$ to all of $\mathbb{Z}$ given by*

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

are called the Dirichlet characters *modulo q.*

Remark. The Legendre symbol from Section 3 is a Dirichlet character.

In the the above definition, the m in $e(m)$ should be understood to mean the reduction of m modulo q. We shall denote the trivial character's extension to $\mathbb{Z}$ by χ_0, and once again we will omit reference to q for convenience. Observe that the Dirichlet characters are multiplicative on all of $\mathbb{Z}$. Moreover,

$$\delta_l(m) = \frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi(l)}\chi(m), \tag{4.5}$$

where the sum is over all Dirichlet characters. With this Fourier-analytic result, we are ready to take the first step toward proving Dirichlet's theorem.

Proposition 4.3. *Let χ be a non-trivial Dirichlet character. If we can show that $\sum_p \frac{\chi(p)}{p^s}$ remains bounded as $s \to 1^+$, then we will have proven Dirichlet's theorem.*

Proof. By (4.5),

$$\begin{aligned} \sum_{p \equiv l} \frac{1}{p^s} = \sum_p \frac{\delta_l(p)}{p^s} &= \frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi(l)} \sum_p \frac{\chi(p)}{p^s} \\ &= \frac{1}{\varphi(q)} \sum_p \frac{\chi_0(p)}{p^s} + \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_0} \overline{\chi(l)} \sum_p \frac{\chi(p)}{p^s} \\ &= \frac{1}{\varphi(q)} \sum_{p \nmid q} \frac{1}{p^s} + \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_0} \overline{\chi(l)} \sum_p \frac{\chi(p)}{p^s}. \end{aligned} \tag{4.6}$$

Since there are only finitely many primes dividing q, the divergence of $\sum_p \frac{1}{p}$ implies that the first term on the final line above diverges as $s \to 1^+$. Thus if we can show that the second term on the final line above remains finite as $s \to 1^+$, then we would have proved the divergence of $\sum_{p \equiv l} \frac{1}{p^s}$. □

Our goal therefore is to prove that $\sum_p \frac{\chi(p)}{p^s}$ remains bounded as $s \to 1^+$. This requires the introduction of the Dirichlet L-functions. But first, a brief interlude.

Proposition 4.4. *If $|x| < 1/2$, then $\log(1+x) = x + O(x^2)$.*

Proof. By the power series expansion of $\log(1+x)$ for $|x| < 1$,

$$\log(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n, \tag{4.7}$$

and thus

$$\log(1+x) - x = -\frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots . \tag{4.8}$$

By the triangle inequality,

$$|\log(1+x) - x| \leq \frac{x^2}{x}(1 + |x| + |x|^2 + \cdots). \tag{4.9}$$

If $|x| \leq 1/2$, we can sum the geometric series and obtain that

$$|\log(1+x) - x| \leq \frac{x^2}{2}\left(\frac{1}{2} + \frac{1}{2^2} + \cdots\right) \leq \frac{x^2}{2}\left(\frac{1}{1-1/2}\right) = x^2, \tag{4.10}$$

as desired. □

Definition 4.5. *A* Dirichlet L-function *is a function of the form* $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$, *where* $s > 1$ *and* χ *is a Dirichlet character.*

Theorem 4.6. *If* $s > 1$, *then*

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

Remark. This result, known as the Dirichlet product formula, is the analogue of expressing the zeta function as an infinite product, namely the Euler product formula

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}. \tag{4.11}$$

Assuming this theorem, we take the logarithm of both sides (more on the legitimacy of this later) of the above equality and get

$$\begin{aligned} \log L(s,\chi) &= -\sum_p \log(1 - \chi(p)p^{-s}) \\ &= -\sum_p \left[-\frac{\chi(p)}{p^s} + O\left(\frac{1}{p^{2s}}\right)\right] = \sum_p \frac{\chi(p)}{p^s} + O(1), \end{aligned} \tag{4.12}$$

where we have used Proposition 4.4 and the observation that $\sum_p \frac{1}{p^{2s}} \leq \sum_{n=1}^{\infty} \frac{1}{n^2}$. From this point on, if we can show that $\log L(s,\chi)$ is bounded as $s \to 1^+ (\chi \neq \chi_0)$, then we will have proven that $\sum_p \frac{\chi(p)}{p^s}$ is bounded as $s \to 1^+$.

Summarizing the tasks at hand, first we need to prove Theorem 4.6. Second, we must justify taking the logarithm of both sides of the equality in Theorem 4.6. The difficulty lies in that $\chi(p)$ may be a complex number, and the complex logarithm is not single-valued. Third, we need to prove that if $\chi \neq \chi_0$, then $\log L(s,\chi)$ is bounded as $s \to 1^+$.

As we will see, if $L(s,\chi)$ is continuous[2] at $s=1$, then it suffices to show the non-vanishing of $L(1,\chi)$.

4.2. **Proof of the Dirichlet product formula.** For $|z|<1$, define

$$\log_1\left(\frac{1}{1-z}\right)=\sum_{k=1}^{\infty}\frac{z^k}{k}. \tag{4.13}$$

Note that $\log_1 w$ is well-defined if $\Re(w)>1/2$, and by (4.7), $\log_1 w$ gives an extension of the usual $\log x$ when x is a real number great than $1/2$.

Proposition 4.7. *The logarithm function* $\log_1$ *satisfies the following properties:*

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

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

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

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

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

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

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

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

$$(1-re^{i\theta})\exp\left(\sum_{k=1}^{\infty}\frac{(re^{i\theta})^k}{k}\right)=1. \tag{4.14}$$

Differentiating the left-hand side of (4.7) with respect to r gives

$$\left[-e^{i\theta}+(1-re^{i\theta})\left(\sum_{k=1}^{\infty}\frac{(re^{i\theta})^k}{k}\right)'\right]\exp\left(\sum_{k=1}^{\infty}\frac{(re^{i\theta})^k}{k}\right), \tag{4.15}$$

and since

$$\begin{aligned}(1-re^{i\theta})\left(\sum_{k=1}^{\infty}\frac{(re^{i\theta})^k}{k}\right)' &= (1-re^{i\theta})e^{i\theta}\left(\sum_{k=1}^{\infty}(re^{i\theta})^{k-1}\right)\\ &= (1-re^{i\theta})e^{i\theta}\frac{1}{1-re^{i\theta}}=e^{i\theta},\end{aligned} \tag{4.16}$$

we see that the left-hand side of (4.14) is a constant function of r. Setting $r=0$ then allows us to obtain the desired result.

The proof of the second property is completely analogous to that of Proposition 4.4. The third property follows immediately from the second. □

[2]Here we choose to think of $L(s,\chi)$ as a function of the real variable s. Alternatively, we could let s be complex-valued, in which case $L(s,\chi)$ is defined on $\Re(s)>1$ and, by analytic continuation, can be extended to a meromorphic function on all of $\mathbb{C}$.

Proposition 4.8. *Suppose $\{a_n\}$ is a sequence of complex numbers such that $a_n \neq 1$ for all n. If $\sum_{n=1}^{\infty}|a_n|$ converges, then $\prod_{n=1}^{\infty}\left(\frac{1}{1-a_n}\right)$ converges to a non-zero value.*

Proof. Since $\sum|a_n|$ converges, $|n| < 1/2$ for all but finitely many n, so we may assume without loss of generality that $|n| < 1/2$ for all n. Then by (1) of Proposition 4.7,

$$\prod_{n=1}^{\infty}\left(\frac{1}{1-a_n}\right) = \prod_{n=1}^{N} e^{\log_1\left(\frac{1}{1-a_n}\right)} = \exp\left(\sum_{n=1}^{N}\log_1\left(\frac{1}{1-a_n}\right)\right). \tag{4.17}$$

By (2) of Proposition 4.7,

$$\left|\log_1\left(\frac{1}{1-a_n}\right)\right| \leq 2|a_n|, \tag{4.18}$$

so the convergence of $\sum|a_n|$ implies the convergence of $\sum_{n=1}^{\infty}\log_1\left(\frac{1}{1-a_n}\right)$. That the infinite product is non-zero is clear from (4.17). □

We are now ready to prove the Dirichlet product formula that

$$\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s} = \prod_{p}\frac{1}{1-\chi(p)p^{-s}} \tag{4.19}$$

for $s > 1$.

Proof of Theorem 4.6. Let L denote the left-hand side of (4.19), and define the partial sums $L_N = \sum_{n\leq N}\chi(n)n^{-s}$ and the partial products $R_N = \prod_{p\leq N}\left(\frac{1}{1-\chi(p)p^{-s}}\right)$. Note that if $s > 1$, then $\sum_{p}\chi(p_n)p_n^{-s} < \infty$, so by Proposition 4.8, $R = \lim_{N\to\infty} R_N$ is finite. Also, define

$$R_{N,M} = \prod_{p\leq N}\left(1 + \frac{\chi(p)}{p^s} + \cdots + \frac{\chi(p^M)}{p^{Ms}}\right). \tag{4.20}$$

Fix $\varepsilon > 0$ and choose N sufficiently large such that $|L - L_N| < \varepsilon$ and $|R - R_N| < \varepsilon$. By the fundamental theorem of arithmetic and the fact that the Dirichlet characters are multiplicative, we can choose M_1 large enough so that $|L_N - R_{N,M_1}| < \varepsilon$. Observe that $\sum_{n=1}^{\infty}\frac{\chi(p^n)}{p^{ns}}$ converges for all primes p, so we can also choose M_2 large enough such that $|R_{N,M_2} - R_N| < \varepsilon$. Let $M = \max\{M_1, M_2\}$, then we have that

$$|L - R| \leq |L - L_N| + |L_N - R_{N,M}| + |R_{N,M} - R_N| + |R_N - R| < 4\varepsilon, \tag{4.21}$$

and the proof of the Dirichlet product formula is complete. □

4.3. **Closer look at logarithms.** Next we need to justify taking logarithms of both sides of the Dirichlet product formula when $\chi \neq \chi_0$. We begin by obtaining a better understanding of the L-functions.

Proposition 4.9. *If χ is a non-trivial Dirichlet character modulo q, then $\sum_{n=1}^{k} \chi(n)$ is bounded by q for any k.*

Proof. By Proposition 2.6, $\sum_{n \in (\mathbb{Z}/q\mathbb{Z})^*} \chi(n) = 0$. Writing $k = sq + t$ with $0 \leq t < q$ and noting that $\chi(n) = 0$ whenever $n \notin (\mathbb{Z}/q\mathbb{Z})^*$, we see that

$$\sum_{n=1}^{k} \chi(n) = \sum_{n=1}^{sq} \chi(n) + \sum_{sq < n \leq sq+t} \chi(n) = \sum_{sq < n \leq sq+t} \chi(n). \tag{4.22}$$

Since $|\chi(n)| \leq 1$, the result is now immediate. □

This proposition helps us extend the definition of $L(s, \chi)$ to all $s > 0$.

Lemma 4.10. *If $\chi \neq \chi_0$, then $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges for $s > 0$. In fact, $L(s, \chi)$ is continuously differentiable on $s > 0$.*

Proof. We know $L(s, \chi)$ is defined for $s > 1$ by the series $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$, which is continuously differentiable on $s > 1$. To extend this result to $s > 0$, let $a_k = \sum_{n=1}^{k} \chi(n)$ and $a_0 = 0$, and observe that

$$\sum_{k=1}^{N} \frac{\chi(k)}{k^s} = \sum_{k=1}^{N} \frac{a_k - a_{k-1}}{k^s} = \sum_{k=1}^{N-1} a_k \left[\frac{1}{k^s} - \frac{1}{(k+1)^s} \right] + \frac{a_N}{N^s}. \tag{4.23}$$

By Proposition 4.9, $|a_k| \leq q$ for all k, thus an application of the mean-value theorem shows that

$$a_k \left[\frac{1}{k^s} - \frac{1}{(k+1)^s} \right] \leq \frac{qs}{k^{1+s}}. \tag{4.24}$$

As such, the series $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges for $s > 0$. To see that it is also continuously differentiable on $s > 0$, we differentiate it term by term and once again use summation by parts to obtain

$$\sum (\log n) \frac{\chi(n)}{n^s} = \sum a_k \left[-\frac{\log(k)}{k^s} + \frac{\log(k+1)}{(k+1)^s} \right]. \tag{4.25}$$

An application of the mean-value theorem to the function $\frac{\log x}{x^s}$ shows that the terms are $O(k^{-1-s/2})$, thereby proving the absolute and uniform convergence of the differentiated series on $s > 0$. □

Proposition 4.11. *There exists constants c_1 and c_2 such that*

$$L(s,\chi) = 1 + O(e^{-c_1 s}) \text{ as } s \to \infty \text{ and}$$
$$L'(s,\chi) = O(e^{-c_2 s}) \text{ as } s \to \infty.$$

Proof. Observe that for all large s,

$$|L(s,\chi) - 1| \leq 2q \sum_{n=2}^{\infty} n^{-s} \leq 2^{-s} O(1), \tag{4.26}$$

so we can take c_1 to be $\log 2$. A similar argument illustrates the second half of the assertion, with in fact $c_2 = c_1$. □

At this point we are ready to define the logarithm of the L-function by integrating its logarithmic derivative. Explicitly, if $\chi \neq \chi_0$ and $s > 1$, we define

$$\log_2 L(s,\chi) = -\int_s^{\infty} \frac{L'(t,\chi)}{L(t,\chi)} dt. \tag{4.27}$$

By Proposition 4.8 and the Dirichlet product formula, $L(t,\chi) \neq 0$ for all $t > 1$. Furthermore, by Proposition 4.11,

$$\frac{L'(t,\chi)}{L(t,\chi)} = O(e^{-ct}) \tag{4.28}$$

for some constant c, hence the integral in (4.27) is convergent. We want to link $\log_2$ with the $\log_1$ that we defined in (4.13).

Proposition 4.12. *If $s > 1$, then*

(1) $e^{\log_2 L(s,\chi)} = L(s,\chi)$, *and*

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

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

$$-\frac{L'(s,\chi)}{L(s,\chi)} \frac{L(s,\chi)}{e^{\log_2 L(s,\chi)}} + \frac{L'(s,\chi)}{e^{\log_2 L(s,\chi)}} = 0, \tag{4.29}$$

so $e^{-\log_2 L(s,\chi)} L(s,\chi)$ is constant. As $s \to \infty$, $\log_2 L(s,\chi) \to 0$, and by Proposition 4.11, $L(s,\chi) \to 1$. Thus as $s \to \infty$, $e^{-\log_2 L(s,\chi)} L(s,\chi) \to 1$, so in fact $e^{-\log_2 L(s,\chi)} L(s,\chi) = 1$. This proves the first claim.

Now fix s and observe that

$$\begin{aligned} \exp\left(\sum_p \log_1 \left(\frac{1}{1-\chi(p)p^{-s}} \right) \right) &= \prod_p e^{\log_1 \left(\frac{1}{1-\chi(p)p^{-s}} \right)} \\ &= \prod_p \left(\frac{1}{1-\chi(p)p^{-s}} \right) = L(s,\chi), \end{aligned} \tag{4.30}$$

where we have used (1) of Propostion 4.7 and the Dirichlet product formula. Comparing with the first claim, we see that for each s there exists an integer $M(s)$ such that

$$\log_2 L(s,\chi) - \sum_p \log_1\left(\frac{1}{1-\chi(p)p^{-s}}\right) = 2\pi i M(s). \tag{4.31}$$

Since the left-hand side of (4.31) is continuous in s, $M(s)$ must also be continuous in s. But $M(s)$ is integer-valued, hence it must be constant. Letting s go to infinity, we see that $M(s) = 0$. This proves the second claim. □

Propositions 4.7 and 4.12 show that

$$\begin{aligned} -\int_s^\infty \frac{L'(t,\chi)}{L(t,\chi)}dt &= \sum_p \log_1\left(\frac{1}{1-\chi(p)p^{-s}}\right) \\ \sum_p \left[\frac{\chi(p)}{p^s} + O\left(\frac{1}{p^{2s}}\right)\right] &= \sum_p \frac{\chi(p)}{p^s} + O(1). \end{aligned} \tag{4.32}$$

Thus to finish the proof of Dirichlet's theorem, we need to prove that $\int_s^\infty \frac{L'(t,\chi)}{L(t,\chi)}dt$ remains bounded as $s \to 1^+$. Since $L(s,\chi)$ is continuously differentiable at $s = 1$, it remains to show the following:

Theorem 4.13. *If $\chi \neq \chi_0$, then $L(1,\chi) \neq 0$.*

Several proofs exist of this highly non-trivial theorem. Some extract advanced machineries from algebraic number theory, while some others utilize results from complex analysis, including deep properties of the zeta function (see [6]). In the spirit of keeping our presentation self-contained, we opt for a more elementary approach. Our proof splits into two cases, depending on whether χ is complex or real.

4.4. **Non-vanishing of the L-function: complex Dirichlet characters.** A Dirichlet character is said to be real if it takes on only real values (namely ± 1 and 0) and complex otherwise. The case where χ is complex is the (much) simpler of the two cases.

Lemma 4.14. *If $s > 1$, then*

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

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

Proof. By (4.30), for $s > 1$,

$$\begin{aligned} \prod_\chi L(s,\chi) &= \exp\left(\sum_\chi \sum_p \log_1\left(\frac{1}{1-\chi(p)p^{-s}}\right)\right) \\ &= \exp\left(\sum_\chi \sum_p \sum_{k=1}^\infty \frac{1}{k}\frac{\chi(p^k)}{p^{ks}}\right) = \exp\left(\sum_p \sum_{k=1}^\infty \sum_\chi \frac{1}{k}\frac{\chi(p^k)}{p^{ks}}\right). \end{aligned} \tag{4.33}$$

By (4.5) (with $l = 0$), we have that $\sum_{\chi} \chi(p^k) = \varphi(q)\delta_0(p^k)$, hence

$$\prod_{\chi} L(s,\chi) = \exp\left(\varphi(q) \sum_{q} \sum_{k=1}^{\infty} \frac{1}{k} \frac{\delta_0(p^k)}{p^{ks}}\right). \tag{4.34}$$

The lemma now follows directly from the observation that the exponential term is real and non-negative. □

Proof of Theorem 4.13 for complex χ. We do this by contradiction. Suppose $L(1,\chi) = 0$ for some non-trivial complex Dirichlet character χ. Since $L(1,\overline{\chi}) = \overline{L(1,\chi)}$, we have $L(1,\overline{\chi}) = 0$ as well. Recall that if $\chi \neq \chi_0$, then $L(s,\chi)$ is continuously differentiable on $s > 0$, so an application of the mean-value theorem shows that if $L(1,\chi) = 0$, then $|L(s,\chi)| \leq C|s-1|$ when $1 \leq s \leq 2$. As χ is complex, $\chi \neq \overline{\chi}$, so there are at least two terms in the product $\prod_{\chi} L(s,\chi)$ that vanish like $|s-1|$ as $s \to 1^+$. Moreover, since $L(1,\chi)$ is finite for all $\chi \neq \chi_0$, no non-trivial character contributes growth terms to the product as $s \to 1^+$.

To investigate what, if any, growth term the trivial Dirichlet character contributes, recall that

$$\chi_0(n) = \begin{cases} 1 & \text{if } n \text{ and } q \text{ are relatively prime,} \\ 0 & \text{otherwise.} \end{cases} \tag{4.35}$$

So if $q = p_1^{a_1} \cdots p_k^{a_k}$ is the prime factorization of q, then upon comparing the Dirichlet and Euler product formulas, we see that

$$L(s,\chi_0) = (1 - p_1^{-s}) \cdots (1 - p_k^{-s})\zeta(s). \tag{4.36}$$

Observe that since $1/x^s$ is decreasing in x, if $s > 1$, then

$$\zeta(s) = 1 + \sum_{n=2}^{\infty} \frac{1}{n^s} \leq 1 + \int_1^{\infty} \frac{dx}{x^s} = 1 + \frac{1}{s-1}. \tag{4.37}$$

Together with (4.36), (4.37) shows that $L(s,\chi)$ is $O(|s-1|^{-1})$ as $s \to 1^+$. But since at least two terms in the product $\prod_{\chi} L(s,\chi)$ vanish like $|s-1|$ as $s \to 1^+$, we should find that $\prod_{\chi} L(s,\chi) \to 0$ as $s \to 1^+$, contradicting the result from Lemma 4.14. □

4.5. **Non-vanishing of the L-function: real Dirichlet characters.** When χ is a real Dirichlet character, it is no longer true that $\chi \neq \overline{\chi}$, so our proof in the complex case does not readily transfer over. Instead, let us define

$$F(m,n) = \frac{\chi(n)}{(nm)^{1/2}} \quad \text{and} \quad S_N = \sum \sum F(m,n), \tag{4.38}$$

where the double sum is taken over all pairs of positive integers (m,n) such that $mn \leq N$. The vanishing of $L(1,\chi)$ would contradict the following proposition, which consequently is the final step of our proof:

Proposition 4.15. *If χ is a non-trivial real Dirichlet character, then*

(1) $S_N \geq c \log N$ *for some constant* $c > 0$*, and*
(2) $S_N = 2N^{1/2}L(1,\chi) + O(1)$.

Some preparations are necessary before we can prove these claims.

Proposition 4.16. *If* N *is a positive integer, then*

(1) $\sum_{n=1}^{N} \frac{1}{n} = \log N + O(1)$*, and*
(2) $\sum_{n=1}^{N} \frac{1}{n^{1/2}} = 2N^{1/2} + c + O(N^{-1/2})$

for some constant c.

Proof. Let $\gamma_n = \frac{1}{n} - \int_n^{n+1} \frac{dx}{x}$, and observe that since $1/x$ is decreasing,

$$0 \leq \gamma_n \leq \frac{1}{n} - \frac{1}{n+1} \leq \frac{1}{n^2}, \tag{4.39}$$

so that $\sum_{n=1}^{\infty} \gamma_n$ converges to a limit which we denote by γ. Moreover,

$$\sum_{n=1}^{N} \frac{1}{n} - \int_1^{N+1} \frac{dx}{x} = \gamma - \sum_{n=N+1}^{\infty} \gamma_n, \tag{4.40}$$

where

$$\int_1^{N+1} \frac{dx}{x} = \log N + \int_N^{N+1} \frac{dx}{x}, \tag{4.41}$$

and

$$\sum_{n=N+1}^{\infty} \gamma_n \leq \sum_{n=N+1}^{\infty} \frac{1}{n^2} \leq \int_N^{\infty} \frac{dx}{x^2} = O(N^{-1}). \tag{4.42}$$

Since $\int_N^{N+1} \frac{dx}{x}$ is $O(N^{-1})$ as $N \to \infty$, this proves the first assertion. Repeating the above with the function $1/x^{1/2}$ and the fact that

$$\left| \frac{1}{n^{1/2}} - \frac{1}{(n+1)^{1/2}} \right| \leq \frac{a}{n^{3/2}} \tag{4.43}$$

for some constant a, we find that

$$\sum_{n=1}^{N} \frac{1}{n^{1/2}} = \int_1^N \frac{dx}{x^{1/2}} + b + O(N^{-1/2}) \tag{4.44}$$

for some constant b. The second assertion now follows via an application of the mean-value theorem. □

Remark. The γ alluded to in the proof above is known as *Euler's constant* and defined, naturally, as

$$\gamma = \lim_{N \to \infty} \sum_{n=1}^{N} \frac{1}{n} - \log N. \tag{4.45}$$

Proposition 4.17. *For all integers $0 < a < b$,*

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

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

Proof. As in the proof of Lemma 4.10, we use summation by parts. Let $s_n = \sum_{k=1}^{n} \chi(k)$, and recall from Proposition 4.9 that $|s_n| \leq q$ for all n. Then

$$\begin{aligned} \sum_{n=a}^{b} \frac{\chi(n)}{n^{1/2}} &= \sum_{n=a}^{b-1} s_n \left[n^{-1/2} - (n+1)^{-1/2}\right] + O(a^{-1/2}) \\ &= O\left(\sum_{n=1}^{\infty} n^{-3/2}\right) + O(a^{-1/2}). \end{aligned} \tag{4.46}$$

By comparing the sum $\sum_{n=a}^{\infty} n^{-3/2}$ with the integral $\int_a^{\infty} x^{-3/2}$, we see that the first term is also $O(a^{-1/2})$. A similar argument establishes (2). □

Lemma 4.18. *Let χ be a non-trivial real Dirichlet character. For all positive integers k, $\sum_{n|k} \chi(n) \geq 0$, and if k is a perfect square, then $\sum_{n|k} \chi(n) \geq 1$.*

Proof. First suppose k is the power of a prime, say $k = p^a$. Then the divisors of k are $1, p, p^2, \cdots, p^a$, so that

$$\sum_{n|k} \chi(n) = \chi(1) + \chi(p) + \cdots + \chi(p^a) = 1 + \chi(p) + \cdots + (\chi(p))^a, \tag{4.47}$$

hence

$$\sum_{n|k} \chi(n) = \begin{cases} a+1 & \text{if } \chi(p) = 1, \\ 1 & \text{if } \chi(p) = -1 \text{ and } a \text{ is even}, \\ 0 & \text{if } \chi(p) = -1 \text{ and } a \text{ is odd}, \\ 1 & \text{if } \chi(p) = 0, \text{ that is, if } p \mid q. \end{cases} \tag{4.48}$$

In the general case where $k = p_1^{a_1} \cdots p_N^{a_N}$, a divisor of k is of the form $p_1^{b_1} \cdots p_N^{b_N}$, where $0 \leq b_j \leq a_j$ for all j. Thus by the multiplicative property of χ,

$$\sum_{x|k} \chi(n) = \prod_{j=1}^{N} \left(\chi(1) + \chi(p_j) + \cdots + \chi(p_j^{a_j})\right). \tag{4.49}$$

If k is a perfect square, then each a_j is even. The lemma is now obvious. □

The key to proving Proposition 4.15 is to visualize the pairs (m, n) as points with integer coordinates enclosed by the x-, y- axes and the curve $xy = N$. Note that we

can carry out the summation $\sum\sum F(m,n)$ vertically, horizontally, or along hyperbolas. More precisely,

$$\begin{aligned} S_N = \sum_{1\le m\le N}\left(\sum_{1\le n\le N/m} F(m,n)\right) &= \sum_{1\le n\le N}\left(\sum_{1\le m\le N/n} F(m,n)\right) \\ &= \sum_{1\le k\le N}\left(\sum_{nm=k} F(m,n)\right). \end{aligned} \tag{4.50}$$

Proof of Proposition 4.15.(1). Observe that

$$\sum_{nm=k}\frac{\chi(n)}{(nm)^{1/2}} = \frac{1}{k^{1/2}}\sum_{n|k}\chi(n), \tag{4.51}$$

so summing along hyperbolas and applying Lemma 4.18, we find that

$$\begin{aligned} S_N = \sum_{1\le k\le N}\left(\sum_{nm=k} F(m,n)\right) &= \sum_{1\le k\le N}\left(\frac{1}{k^{1/2}}\sum_{n|k}\chi(n)\right) \\ &\ge \sum_{\substack{k^{1/2}\in\mathbb{Z}\\ 1\le k\le N}}\frac{1}{k^{1/2}} = \sum_{1\le t\le N^{1/2}}\frac{1}{t} \ge c\log N, \end{aligned} \tag{4.52}$$

where the last inequality follows from (1) of Proposition 4.16. □

To prove the second half of Proposition 4.15, we break S_N into the two sums

$$\begin{aligned} S_I &= \sum_{1\le m<N^{1/2}}\left(\sum_{N^{1/2}<n\le N/m} F(m,n)\right) \quad \text{and} \\ S_{II} &= \sum_{1\le n\le N^{1/2}}\left(\sum_{1\le m\le N/n} F(m,n)\right). \end{aligned} \tag{4.53}$$

To see that $S_N = S_I + S_{II}$, note that

$$S_{II} = \sum_{1\le m\le N^{1/2}}\left(\sum_{1\le n\le N^{1/2}} F(m,n)\right) + \sum_{N^{1/2}<m\le N/n}\left(\sum_{1\le n<N^{1/2}} F(m,n)\right). \tag{4.54}$$

Essentially, we are summing vertically in S_I and horizontally in S_{II}.

Proof of Proposition 4.15.(2). Since

$$S_I = \sum_{1\le m<N^{1/2}}\frac{1}{m^{1/2}}\left(\sum_{N^{1/2}<n\le N/m}\frac{\chi(n)}{x^{1/2}}\right), \tag{4.55}$$

Propositions 4.16.(2) and 4.17.(1) show that S_I is $O(1)$.

Applying Proposition 4.16.(2) once more, we get

$$\begin{aligned} S_{II} &= \sum_{1\le n\le N^{1/2}} \frac{\chi(n)}{n^{1/2}} \left(\sum_{m\le N/n} \frac{1}{m^{1/2}} \right) \\ &= \sum_{1\le n\le N^{1/2}} \frac{\chi(n)}{n^{1/2}} \left[2\left(\frac{N}{n}\right)^{1/2} + c + O\left(\left(\frac{n}{N}\right)^{1/2}\right)\right] \qquad (4.56) \\ &= 2N^{1/2} \sum_{1\le n\le N^{1/2}} \frac{\chi(n)}{n} + c \sum_{1\le n\le N^{1/2}} \frac{\chi(n)}{n^{1/2}} + O\left(\frac{1}{N^{1/2}} \sum_{1\le n\le N^{1/2}} 1 \right). \end{aligned}$$

Clearly, the last term is $O(1)$, and Proposition 4.17 implies

$$\begin{aligned} 2N^{1/2} \sum_{1\le n\le N^{1/2}} \frac{\chi(n)}{n} &= 2N^{1/2} \left(\sum_{1\le n\le N^{1/2}} \frac{\chi(n)}{n} + \sum_{n>N^{1/2}} \frac{\chi(n)}{n} - \sum_{n>N^{1/2}} \frac{\chi(n)}{n} \right) \qquad (4.57) \\ &= 2N^{1/2}[L(1,\chi) + O(N^{-1/2})] = 2N^{1/2}L(1,\chi) + O(1) \end{aligned}$$

and

$$c \sum_{1\le n\le N^{1/2}} \frac{\chi(n)}{n^{1/2}} = O(1), \qquad (4.58)$$

so that

$$S_N = 2N^{1/2}L(1,\chi) + O(1). \qquad (4.59)$$

This completes the proof that $L(1,\chi) \neq 0$ when χ is a non-trivial real Dirichlet character, and also the proof of Dirichlet's theorem on primes in arithmetic progression. □

5. Weyl's Criterion

In 1916, Weyl gave the necessary and sufficient condition for a sequence of real numbers to be equidistributed modulo 1. Not only was this result one of the first theorems in ergodic theory, it became instrumental for much subsequent work on Diophantine approximations. In this section we give a proof of this powerful result that incorporates the periodic analogue of Weierstrass approximation theorem.

If γ is a real number, we let $\lfloor\gamma\rfloor$ denote the greatest integer less than or equal to γ and call $\lfloor\gamma\rfloor$ the integer part of γ. The fractional part of γ is then defined by $\langle\gamma\rangle = \gamma - \lfloor\gamma\rfloor$.

Definition 5.1. *A sequence of numbers $\{\alpha_n\}$ in $[0,1)$ is said to be* equidistributed *if for every interval $[a,b) \subseteq [0,1)$,*

$$\lim_{N\to\infty} \frac{\#\{1\le n\le N : \alpha_n \in [a,b)\}}{N} = b - a.$$

A sequence of real numbers $\{\beta_n\}$ is said to be equidistributed modulo 1 *if $\{\langle\beta_n\rangle\}$ is equidistributed.*

Theorem 5.2 (Weyl's criterion)**.** *A sequence of real numbers $\{\beta_n\}$ is equidistributed modulo 1 if and only if*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}e^{2\pi ik\beta_n}=0$$

for all integers $k\neq 0$.

First we prove an intermediate result.

Lemma 5.3. *A sequence of numbers $\{\alpha_n\}$ in $[0,1)$ is equidistributed if and only if*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}f(\alpha_n)=\int_0^1 f(x)dx$$

for every function f that is Riemann integrable on $[0,1]$.

Proof. We may assume f to be real-valued, for otherwise we could consider its real and imaginary parts separately. To see the sufficiency half of the claim, given an interval $[a,b)\subseteq[0,1)$, simply let f be the characteristic function of $[a,b)$ on $[0,1]$, that is, for $x\in[0,1]$, define

$$f(x)=\begin{cases}1 & \text{if } x\in[a,b),\\ 0 & \text{otherwise.}\end{cases}\tag{5.1}$$

Then

$$\sum_{n=1}^{N}f(\alpha_n)=\#\{1\leq n\leq N:\alpha_n\in[a,b)\}\ \text{ while }\ \int_0^1 f(x)dx=b-a.\tag{5.2}$$

By the condition in the lemma, we see that

$$\lim_{N\to\infty}\frac{\#\{1\leq n\leq N:\alpha_n\in[a,b)\}}{N}=\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}f(\alpha_n)=\int_0^1 f(x)dx=b-a,\tag{5.3}$$

so $\{\alpha_n\}$ is equidistributed.

Conversely, suppose $\{\alpha_n\}$ is equidistributed, then

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}f(\alpha_n)=\int_0^1 f(x)dx\tag{5.4}$$

holds for the characteristic function of any interval $[a,b)$ on $[0,1]$. By linearity, (5.4) also holds for any step function on $[0,1]$. If f is Riemann integrable on $[0,1]$, then given $\varepsilon>0$, there exist step functions f_1,f_2 such that $f_1\leq f\leq f_2$ and $\int_0^1[f_2(x)-f_1(x)]dx<\varepsilon$. Thus

$$\lim_{N\to\infty}\sum_{n=1}^{N}f_1(\alpha_n)=\int_0^1 f_1(x)dx\geq\int_0^1 f(x)dx-\varepsilon,\tag{5.5}$$

so that for all large N,

$$\sum_{n=1}^{N} f(\alpha_n) \geq \sum_{n=1}^{N} f_1(\alpha_n) > \int_0^1 f(x)dx - 2\varepsilon. \tag{5.6}$$

Similarly, by comparing f with f_2 we see that

$$\sum_{n=1}^{N} f(\alpha_n) < \int_0^1 f(x)dx + 2\varepsilon \tag{5.7}$$

for all large N. Hence

$$\left| \frac{1}{N} \sum_{n=1}^{N} f(\alpha_n) - \int_0^1 f(x)dx \right| < 2\varepsilon \tag{5.8}$$

for all large N, as desired. □

Proof of Theorem 5.2. Let $\alpha_n = \langle \beta_n \rangle$. First suppose $\{\beta_n\}$ is equidistributed modulo 1. Then $\{\alpha_n\}$ is equidistributed, so by Lemma 5.3,

$$\lim_{n\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i k \beta_n} = \lim_{n\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i k \alpha_n} = \int_0^1 e^{2\pi i k x} dx = 0 \tag{5.9}$$

for all integers $k \neq 0$.

Conversely, suppose that for every non-zero integer k,

$$\lim_{n\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i k \beta_n} = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i k \alpha_n} = 0. \tag{5.10}$$

By Lemma 5.3, it suffices to show that (5.4) is satisfied for every Riemann integrable function on $[0, 1]$. Note that (5.4) clearly holds for $f(x) = 1$ and, by hypothesis, for any $f(x) = e^{2\pi i k x}$ where k is a non-zero integer. This implies that (5.4) is satisfied for all trigonometric polynomials. Recall from Section 2.3 that any continuous periodic function can be uniformly approximated by trigonometric polynomials, so if f is a continuous 1-periodic function, then for any $\varepsilon > 0$ we can find trigonometric polynomial P such that $|f(x) - P(x)| < \varepsilon$ for all $x \in [0, 1]$. Thus for all large N, we see that

$$\begin{aligned} \left| \frac{1}{N} \sum_{n=1}^{N} f(\alpha_n) - \int_0^1 f(x)dx \right| \leq & \frac{1}{N} \sum_{n=1}^{N} |f(\alpha_n) - P(\alpha_n)| \\ & + \left| \frac{1}{N} \sum_{n=1}^{N} P(\alpha_n) - \int_0^1 P(x)dx \right| \\ & + \int_0^1 |P(x) - f(x)|dx \quad < 3\varepsilon. \end{aligned} \tag{5.11}$$

As such, (5.4) holds for any continous 1-periodic function. Now let f be a step function on $[0, 1]$. For any $\varepsilon > 0$, we can find continuous 1-periodic functions f_1, f_2 such that $f_1 \leq f \leq f_2$ and $\int_0^1 [f_2(x) - f_1(x)]dx < \varepsilon$, so as in the proof of Lemma 5.3, (5.4) holds

for f. That (5.4) holds for any step function on $[0,1]$ implies, as before, that it holds for any Riemann integrable function on $[0,1]$. □

An application of Weyl's criterion gives the following, which Weyl had actually proved in 1909:

Theorem 5.4 (Weyl's equidistribution theorem)**.** *If γ is irrational, then $\{n\gamma\}_{n\in\mathbb{Z}^+}$ is equidistributed modulo 1.*

Remark. It should be clear that the $\langle n\gamma\rangle$ are all distinct.

Proof. Let $\xi = k\gamma$, where k is a non-zero integer. By Weyl's criterion, it suffices to show that $\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} e^{2\pi i n\xi} = 0$. Since γ is irrational, $e^{2\pi i\xi} \neq 1$, so that

$$\begin{aligned}\left|\sum_{n=1}^{N} e^{2\pi i n\xi}\right| &= \left|(e^{2\pi i\xi})\frac{1-e^{2\pi iN\xi}}{1-e^{2\pi i\xi}}\right| \\ &= \left|\frac{e^{2\pi i(N+1)\xi}-e^{2\pi i\xi}}{e^{2\pi i\xi}-1}\right| \leq \frac{2}{|e^{2\pi i\xi}-1|} = \frac{1}{|\sin\pi\xi|}.\end{aligned} \tag{5.12}$$

The result follows at once from the boundedness of $\sum_{n=1}^{N} e^{2\pi i n\xi}$. □

Theorem 5.4 immediately yields a corollary that is interesting in its own right.

Corollary 5.5 (Kronecker's approximation theorem)**.** *If γ is irrational, then the sequence $\{\langle n\gamma\rangle\}_{n\in\mathbb{Z}^+}$ is dense in $[0,1)$.*

6. Survey of Advanced Topics

The theorems in the previous sections represent only the beginning of the rich and fruitful interplay between Fourier analysis and number theory. In the theory of modular forms, for instance, the Eisenstein series and the Weierstrass $\wp$ function have Fourier series expansions that are worthwhile to study (see [1]).

In Section 2 we developed elements of Fourier analysis on finite abelian groups and on finite real intervals. We could have, in fact, continued to the Fourier transform on $\mathbb{R}$ (or even $\mathbb{R}^n$). If f is a function of moderate decrease, then we define its Fourier transform for $\xi \in \mathbb{R}$ by

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x)e^{-2\pi ix\xi}dx, \tag{6.1}$$

and if f is in the Schwartz space on $\mathbb{R}$, we have the Fourier inversion formula

$$f(x) = \int_{-\infty}^{\infty} \hat{f}(\xi)e^{2\pi ix\xi}d\xi. \tag{6.2}$$

Let $\delta > 0$, and let h be an even function that is holomorphic on the strip $|\Im(s)| \leq 1/2+\delta$. Furthermore, suppose that

(1) $h(s) = O(|s|^{-1-\delta})$ as $|s| \to \infty$,

(2) $h_0(t) = h(2\pi it)$ is real-valued for all $t \in \mathbb{R}$, and
(3) the Fourier transform of h_0 satisfies the bound $\hat{h}_0(y) = O(e^{-(1/2+\delta)y})$ as $y \to \infty$.

There exists a Fourier type duality between prime numbers and zeros of the Riemann-zeta function that is expressed in Weil's explicit formula (1952)

$$\sum_{\gamma} h(i\gamma) = h\left(\frac{1}{2}\right) - \frac{1}{2}(\log \pi)\hat{h}_0(0) + \int_{-\infty}^{\infty} \frac{\Gamma'(1/4 + i\pi t)}{\Gamma(1/4 + i\pi t)} h_0(t)dt - \sum_{n=1}^{\infty} \frac{\Lambda(n)}{\sqrt{n}} \hat{h}_0(\log n), \tag{6.3}$$

where Γ is the Gamma function

$$\Gamma(z) = \int_0^{\infty} t^{z-1} e^{-t} dt, \tag{6.4}$$

Λ is the van Mangoldt function

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^a \text{ for some prime } p \text{ and } a \geq 1, \\ 0 & \text{otherwise,} \end{cases} \tag{6.5}$$

and $1/2 + i\gamma$ is a non-trivial zero of $\zeta(s)$. Note that the Riemann hypothesis is the assertion that every γ is real.

This Fourier type duality has been a significant area of research in number theory and harmonic analysis over the past half century. Selberg, perhaps looking for a spectral interpretation of the zeros of $\zeta(s)$, proved a trace formula for the Laplace operator acting on the space of real-analytic functions defined on the upper-half plane $\mathbb{H}$ and invariant under the group $SL(2, \mathbb{Z})$ of linear fractional transformations with integer entries and determinant one. The Laplace operator in this case is

$$\Delta = -y^2 \left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial x^2} \right). \tag{6.6}$$

The spectrum of Δ splits into a continuous part and a discrete part. The eigenvalues λ are all positive and usually expressed as $\lambda = s(1-s)$. The continuous part consists of all $s = 1/2 + it, t \geq 0$, and we write the discrete part as $s_j = 1/2 + ir_j$. Then the Selberg trace formula (1956) gives

$$\begin{aligned} \sum_{j=1}^{\infty} h(r_j) = -h(0) - \hat{h}_0(0) \log\left(\frac{\pi}{2}\right) - \frac{1}{2\pi} \int_{-\infty}^{\infty} h(r) G(r) dr \\ + 2 \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n} \hat{h}_0(2 \log n) + \sum_{P} \sum_{l=1}^{\infty} \frac{\hat{h}_0(l \log P) \log P}{P^{l/2} - P^{-l/2}}, \end{aligned} \tag{6.7}$$

where the last sum is over the norms P of prime geodesics of $SL(2, \mathbb{Z}) \backslash \mathbb{H}$, and

$$G(r) = \frac{\Gamma'}{\Gamma}\left(\frac{1}{2} + ir\right) + \frac{\Gamma'}{\Gamma}(1 + ir) - \frac{\pi}{6} r \tanh \pi r + \frac{\pi}{\cosh \pi r} \left(\frac{1}{8} + \frac{\sqrt{3}}{9} \cosh \frac{\pi r}{3} \right). \tag{6.8}$$

The resemblance between Weil's explicit formula and Selberg's trace formula is striking and not yet well understood.

Selberg's trace formula may be interpreted as the non-commutative generalization of the Poisson summation formula, which states that if f is a Schwartz function, then

$$\sum_{n=-\infty}^{\infty} f(x+n) = \sum_{n=-\infty}^{\infty} \hat{f}(n)e^{2\pi inx}. \tag{6.9}$$

This formula itself played an important role in the derivation of a functional equation of ζ. Define the theta function for $s > 0$ by

$$\vartheta(s) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 s}, \tag{6.10}$$

then a simple application of the Poisson summation formula to the pair $f(x) = e^{-\pi s x^2}$ and $\hat{f}(y) = s^{-1/2}e^{-\pi y^2/s}$ gives the functional equation of ϑ, namely

$$s^{-1/2}\vartheta(1/s) = \vartheta(s). \tag{6.11}$$

It turns out that ζ, ϑ, and Γ are related by the identity

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \frac{1}{2}\int_0^{\infty} t^{s/2-1}(\vartheta(s) - 1)dt, \tag{6.12}$$

so if we define on $\Re(s) > 1$ the xi function

$$\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s), \tag{6.13}$$

then after some work, the functional equation of ϑ helps us derive that

$$\xi(s) = \xi(1-s), \tag{6.14}$$

from which we can obtain a version of the functional equation of ζ, that is,

$$\zeta(s) = \zeta(1-s)\pi^{s-1/2}\frac{\Gamma((1+s)/2)}{\Gamma(s/2)}. \tag{6.15}$$

While we are on the subject, in what was then titled "Fourier analysis in number fields and Hecke's zeta-functions" (1950), Tate proved the functional equations for a very general class of zeta and L-functions by using a version of the Poisson summation formula for idèle groups of algebraic number fields (see [10]). This visionary paper was Tate's Ph.D. disseration, and as such, it is now generally known as Tate's thesis.

We conclude by briefly outlining a proof for the function field counterpart of Fermat's last theorem, a result that seemingly belongs to algebraic geometry.

Theorem 6.1. *If k is an integer, q is a prime power, and $q \geq k^4 + 4$, then the Fermat equation $x^k + y^k = z^k$ has a non-trivial solution in the finite field $\mathbb{F}_q$.*

We could in fact prove a more general result.

Theorem 6.2. *Let A_1 and A_2 be subsets of $\mathbb{F}_q$, and let $l_i = \frac{q-1}{|A_i|}$. Suppose $q \geq k^2 l_1 l_2 + 4$ for some integer k, then the equation $x + y = z^k$ ($x \in A_1$, $y \in A_2$, $z \in \mathbb{F}_q^*$) has at least one solution.*

Note that Theorem 6.1 follows from Theorem 6.2 if we set $A_1 = A_2 = \{a^k : a \in \mathbb{F}_q^*\}$. Clearly, $|A_i| = \frac{q-1}{\gcd(q-1,k)} \geq \frac{q-1}{k}$, and thus $l_i \leq k$.

For G a finite abelian group, A a subset of G, and f_A the characteristic function of A on G, define

$$\Phi(A) = \max\{|\hat{f}_A(e)| : e \in \hat{G}, e \neq e_0\}, \tag{6.16}$$

where $\hat{G}$ is the dual group of G, e_0 is the trivial character of G, and $\hat{f}_A(e)$ is the Fourier coefficient of f_A with respect to the character e. This Φ gives an index on the "randomness" of A. The smaller the $\Phi(A)$, the "smoother" and more "random looking" A is. Some Fourier analysis on finite abelian groups and an application of the Cauchy-Schwarz inequality give the following:

Proposition 6.3. *Let A_1, A_2, and A_3 be subsets of G, and let N denote the number of solutions to the equation $a_1 + a_2 + a_3 = a$ ($a_i \in A_i$, $a \in G$), then*

$$\left| N - \frac{|A_1||A_2||A_3|}{n} \right| \leq \Phi(A_3)\sqrt{|A_1||A_2|}. \tag{6.17}$$

Furthermore, linking the Fourier coefficients of cyclotomic classes in $\mathbb{F}_q$ to Gauss sums over $\mathbb{F}_q$ via a simple sieve leads to the following:

Proposition 6.4. *If A is a cyclotomic class in $\mathbb{F}_q$, then $\Phi(A) < \sqrt{q}$.*

Synthesizing Propositions 6.3 and 6.4 reveals the following:

Lemma 6.5. *Let k be an integer that divides $q-1$, let A_1 and A_2 be subsets of $\mathbb{F}_q$, and let N be the number of solutions to $x + y = z^k$ ($x \in A_1$, $y \in A_2$, $z \in \mathbb{F}_q^*$), then*

$$\left| N - \frac{|A_1||A_2|(q-1)}{q} \right| < k\sqrt{|A_1||A_2|q}. \tag{6.18}$$

From this point on, it is straightforward to verify Theorem 6.2 for the case where k divides $q-1$. The general case reduces to this case via

$$\{a^k : a \in \mathbb{F}_q^*\} = \{a^d : a \in \mathbb{F}_q^*\}, \tag{6.19}$$

where $d = \gcd(q-1, k)$.

For full proofs of the above series of results, see [2].

References

[1] T. M. Apostol, *Modular Functions and Dirichlet Series in Number Theory*, 2nd ed., Springer-Verlag, New York, 1990.

[2] L. Babai, "The Fourier transform and equations over finite abelian groups: an introduction to the method of trigonometric sums", lectures notes, version 1.3, 2002, http://people.cs.uchicago.edu/∼laci/reu02/fourier.pdf.

[3] K. Chandrasekharan, *Introduction to Analytic Number Theory*, Springer-Verlag, Berlin, 1968.

[4] J. B. Conrey, "The Riemann Hypothesis", Not. Amer. Math. Soc. 50, 341-353, 2003.

[5] F. J. Lemmermeyer, "Proofs of the Quadratic Reciprocity Law", ongoing webliography, http://www.danielbruederle.de/∼hb3/rchrono.html.

[6] C. J. Moreno, *Advanced Analytic Number Theory: L-Functions*, American Mathematical Society, Providence, 2005.

[7] M. R. Murty, *Problems in Analytic Number Theory*, Springer-Verlag, New York, 2000.
[8] I. M. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5^{th} ed., John Wiley & Sons, New York, 1991.
[9] E. M. Stein and R. Shakarchi, *Fourier Analysis: An Introduction*, Princeton University Press, Princeton, 2003.
[10] J. T. Tate, "Fourier analysis in number fields and Hecke's zeta functions", in *Algebraic Number Theory*, edited by J. W. S. Cassels and A. Fröhlich, Academic Press, London, 1967.
[11] A. A. Terras, *Fourier Analysis on Finite Groups and Applications*, Cambridge University Press, Cambridge, 1999.
[12] E. C. Titchmarsh and D. R. Heath-Brown, *The Theory of the Riemann Zeta-Function*, 2^{nd} ed., Oxford University Press, Oxford, 1986.
[13] A. Vretblad, *Fourier Analysis and Its Applications*, Springer-Verlag, New York, 2003.
[14] M. R. Watkins, "Fourier analysis and number theory", part of the ongoing *Number Theory and Physics* web archive, http://www.secamlocal.ex.ac.uk/people/staff/mrwatkin/zeta/NTfourier.htm.

E-mail address: sd2204@columbia.edu