International Journal of Number Theory
Vol. 11, No. 6 (2015) 1913–1939
© World Scientific Publishing Company
DOI: 10.1142/S1793042115500839

On primitivity of Dirichlet characters

R. Daileda

Department of Mathematics
Trinity University
One Trinity Place, San Antonio
TX 78212-7200, USA
rdaileda@trinity.edu

N. Jones

Department of Mathematics
Statistics, and Computer Science
University of Illinois at Chicago
322 Science and Engineering Offices (M/C 249)
851 S. Morgan Street
Chicago, IL 60607-7045, USA
ncjones@uic.edu

Received 8 April 2014
Accepted 29 October 2014
Published 16 July 2015

Recall that a Dirichlet character is called imprimitive if it is induced from a character of smaller level, and otherwise it is called primitive. In this paper, we introduce a modification of "inducing to higher level" which causes imprimitive characters to behave primitively, in the sense that the properties of the associated Gauss sum and the functional equation of the attached L-function take on a form usually associated to a primitive character.

Keywords: Dirichlet character; Gauss sum; L-function; orthogonality.

Mathematics Subject Classification 2010: 11M06, 11L05

1. Introduction

Let q be any positive integer and χ a multiplicative group homomorphism

$$\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times.$$

It is traditional to extend χ to all of $\mathbb{Z}/q\mathbb{Z}$ by declaring that

$$\chi(n) = 0 \quad \text{if } n \in \mathbb{Z}/q\mathbb{Z} - (\mathbb{Z}/q\mathbb{Z})^\times. \tag{1}$$

In this way, χ defines a multiplicative function (known as a *Dirichlet character*)

$$\chi : \mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}.$$

Dirichlet characters were used by Dirichlet [3] to prove his celebrated theorem on the infinitude of primes in arithmetic progressions.

The following properties are valid for all Dirichlet characters:

(1) Complete multiplicativity:

$$\forall\, n, m \in \mathbb{Z}, \quad \chi(nm) = \chi(n)\chi(m). \tag{2}$$

(2) Orthogonality:

$$\begin{aligned}\forall\, \chi_1, \chi_2 \mod q, \quad \langle \chi_1, \chi_2\rangle_q &:= \sum_{n\in\mathbb{Z}/q\mathbb{Z}} \chi_1(n)\overline{\chi}_2(n) \\ &= \begin{cases} \varphi(q) & \text{if } \chi_1 = \chi_2, \\ 0 & \text{otherwise.}\end{cases}\end{aligned} \tag{3}$$

Because $(\mathbb{Z}/q\mathbb{Z})^\times$ is self-dual, there are exactly $\varphi(q)$ Dirichlet characters, and (3) then implies that the square matrix of character values divided by $\sqrt{\varphi(q)}$ is orthogonal. It follows that its transpose is also orthogonal, yielding the dual relationship

$$\forall\, n_1, n_2 \in (\mathbb{Z}/q\mathbb{Z})^\times, \qquad \sum_{\chi\in((\mathbb{Z}/q\mathbb{Z})^\times)^*} \chi(n_1)\overline{\chi}(n_2) = \begin{cases} \varphi(q) & \text{if } n_1 = n_2, \\ 0 & \text{otherwise.}\end{cases} \tag{4}$$

The *conductor* of χ is the smallest (positive) divisor q_1 of q for which there is a homomorphism

$$\chi_1 : (\mathbb{Z}/q_1\mathbb{Z})^\times \to \mathbb{C}^\times$$

such that $\chi = \chi_1 \circ \text{red}$ is the composition of χ_1 with the reduction modulo q_1 map. We say that $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ is *primitive* if its conductor is equal to q, and *imprimitive* otherwise.

Primitivity can alternatively be characterized in terms of the *Gauss sum* $\mathcal{G}_q(\chi, n)$ attached to a character χ, which is defined for $n \in \mathbb{Z}/q\mathbb{Z}$ by

$$\mathcal{G}_q(\chi, n) := \sum_{m\in\mathbb{Z}/q\mathbb{Z}} \chi(m) \exp\left(\frac{2\pi i n m}{q}\right).$$

One can show that χ is primitive if and only if the associated Gauss sum has the following property:

(3) Separability of the Gauss sum:

$$\forall\, n \in \mathbb{Z}/q\mathbb{Z}, \quad \mathcal{G}_q(\overline{\chi}, n) = \chi(n)\mathcal{G}_q(\overline{\chi}, 1). \tag{5}$$

The purpose of this paper is to observe that, if one makes the mild sacrifice[a] of replacing (2) by

$$\forall\, n, m \in \mathbb{Z}, \quad \chi(nm) = \chi(n)\chi(m), \quad \text{provided } \gcd(n, m, q) = 1, \tag{6}$$

[a] Note that any $\chi : \mathbb{Z} \to \mathbb{C}$ satisfying (6) is multiplicative, although perhaps not completely multiplicative.

then, by altering the convention (1), one may arrange that (5) holds for imprimitive characters as well as primitive ones. Furthermore, an appropriate extension of (3) (and hence (4)) continues to hold. For any function $\chi : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$, denote by $\chi^\times$ its restriction to $(\mathbb{Z}/q\mathbb{Z})^\times$. Note that if χ satisfies (6), then its restriction

$$\chi^\times : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$$

is a group homomorphism, and in this case we define the *conductor of* χ to be the conductor of $\chi^\times$. Our main result is the following theorem. In its statement, $\tau(n)$ denotes the number of positive divisors of n.

Theorem 1.1. *Let q be a positive integer. There exists a set $\mathfrak{C}$ of functions $\chi : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ with the following properties.*

(1) *The set $\mathfrak{C}$ contains exactly q functions, and each $\chi \in \mathfrak{C}$ satisfies* (6).
(2) *If $\psi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ is a character of conductor d, then there are exactly $\tau(q/d)$ functions $\chi \in \mathfrak{C}$ that extend ψ. Furthermore, if ψ is primitive* (*i.e. if $d = q$*), *then its unique extension χ still satisfies* (1) *and* (2).
(3) *The identity* (5) *holds for all $\chi \in \mathfrak{C}$.*
(4) *For $\chi_1, \chi_2 \in \mathfrak{C}$, we have*

$$\langle \chi_1, \chi_2 \rangle_q = \begin{cases} \tau(q/d)\varphi(q) & \textit{if } \chi_1 = \chi_2 \textit{ has conductor } d, \\ 0 & \textit{otherwise.} \end{cases} \tag{7}$$

We remark that other papers have deviated from convention (1). See for instance [7], which does so while improving bounds for the error term in the prime geodesic theorem, and also [2], which does so in constructing a double Dirichlet series in connection with $\mathrm{GL}_3(\mathbb{Z})$ Eisenstein series.

It is natural to ask to what extent the set $\mathfrak{C}$ in Theorem 1.1 is unique. As we will see, it is not unique in general, and our proof gives an explicit parametrization of a collection of such sets $\mathfrak{C}$, as follows. Let

$$\mathfrak{F}_q := \{\text{Subsets } \mathfrak{C} \subseteq \mathbb{C}^{\mathbb{Z}/q\mathbb{Z}} \text{ which satisfy the conclusions of Theorem 1.1}\}. \tag{8}$$

For any positive integer $N \geq 1$, let us make the definition

$$\mathbb{T}_N := \left\{ (\theta_j) \in (\mathbb{R}/\pi\mathbb{Z})^N \,\middle|\, \sum_{j=0}^{N-1} e^{2\theta_j i} = 0 \right\}.$$

Note that the symmetric group S_N acts on $\mathbb{T}_N$ by permuting the coordinates θ_j, and let

$$\mathbb{T}_N/S_N$$

denote the quotient by this action. The orthogonal group is defined as usual by

$$O_N(\mathbb{R}) := \{X \in \mathrm{GL}_N(\mathbb{R}) : X^t X = I\}.$$

Given a character $\psi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ of conductor d_ψ, define the non-negative integers $\alpha_p = \alpha_p(q)$, γ_p^ψ and N_p^ψ by

$$q =: \prod_p p^{\alpha_p}, \quad d_\psi =: \prod_p p^{\gamma_p^\psi}, \quad N_p^\psi := \alpha_p - \gamma_p^\psi, \tag{9}$$

where here and throughout the paper, p denotes a prime number.

Theorem 1.2. *Let*

$$\mathfrak{F}_q := \{\textit{Subsets } \mathfrak{C} \subseteq \mathbb{C}^{\mathbb{Z}/q\mathbb{Z}} \textit{ which satisfy the conclusions of Theorem } 1.1\}.$$

Then there is an injective map

$$\prod_{\psi\in((\mathbb{Z}/q\mathbb{Z})^\times)^*}\left(\prod_{\substack{p|q\\ N_p^\psi\geq 2}}\Big((\mathbb{T}_{N_p^\psi+1}/S_{N_p^\psi+1})\times O_{N_p^\psi-1}(\mathbb{R})\Big)\times\prod_{\substack{p|q\\ \gamma_p^\psi\geq 1\\ N_p^\psi=1}}(\mathbb{T}_{N_p^\psi+1}/S_{N_p^\psi+1})\right)\hookrightarrow \mathfrak{F}_q, \tag{10}$$

where any empty product on the left-hand side is interpreted as a set with one element. Furthermore, there exists a set $\mathfrak{C} \in \mathfrak{F}_q$ for which $\overline{\mathfrak{C}} = \mathfrak{C}$.

Remark 1.3. If $q = p^\alpha$ is a prime power, then the injection (10) is a bijection.

One may interpret the Gauss sum $\mathcal{G}_q(\cdot, n)$ as a linear operator on the q-dimensional vector space of functions $\mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$. In fact, in terms of the discrete Fourier transform

$$\hat{f}(n) := \sum_{m\in\mathbb{Z}/q\mathbb{Z}} f(m)\exp\left(-\frac{2\pi i n m}{q}\right),$$

one finds that for characters χ,

$$\mathcal{G}_q(\overline{\chi}, n) = \overline{\widehat{\chi}}(n).$$

In this context, the identity (5) says that a primitive character χ is a coneigenvector of the conjugate-linear operator $f \mapsto \overline{\widehat{f}}$, with coneigenvalue $\mathcal{G}_q(\overline{\chi}, 1)$. Theorem 1.1 uses the imprimitive characters to extend the set of primitive characters to a coneigenbasis for this operator, consisting of functions which additionally respect the multiplicative action of $(\mathbb{Z}/q\mathbb{Z})^\times$ on $\mathbb{Z}/q\mathbb{Z}$.

We emphasize that, when one restricts each of the modified characters from Theorem 1.1 to $(\mathbb{Z}/q\mathbb{Z})^\times$, one recovers all multiplicative characters mod q, except that the imprimitive characters χ induced from level d occur with multiplicity $m_\chi = \tau(q/d)$. Moreover, the orthogonality relation (7) immediately implies the dual relation

$$\forall\, n_1, n_2 \in \mathbb{Z}/q\mathbb{Z}, \quad \sum_{\chi\in\mathfrak{C}} \frac{1}{m_\chi}\chi(n_1)\overline{\chi}(n_2) = \begin{cases} \varphi(q) & \text{if } n_1 \equiv n_2 \mod q, \\ 0 & \text{otherwise}, \end{cases}$$

which is the analogue of (4) from the classical situation.

That Theorem 1.1 extends each imprimitive character mod q to $\mathbb{Z}/q\mathbb{Z}$ in multiple ways is unavoidable: the total number of characters, namely $\varphi(q)$, is strictly less than the dimension of the space we are attempting to span. However, while the "weight equidistribution" assumption $m_\chi = \tau(q/d)$ is a convenient and somewhat natural choice, it may be possible to prove the analogue of Theorem 1.1 using a different set of multiplicities for the imprimitive characters.

One advantage to our viewpoint is that we may now treat primitive and imprimitive characters equally when regarding their L-functions. For any character χ as in Theorem 1.1, we regard its conductor as q, forming the usual L-function

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \text{ prime}} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \cdots\right)$$

and its completion

$$\Lambda(s,\chi) := \left(\frac{q}{\pi}\right)^{\frac{s}{2}} \Gamma\left(\frac{s+\mathfrak{a}}{2}\right) L(s,\chi) \quad \left(\mathfrak{a} := \begin{cases} 0 & \text{if } \chi(-1) = 1, \\ 1 & \text{if } \chi(-1) = -1 \end{cases}\right).$$

Then, the functional equation of any of the characters in Theorem 1.1 assumes the same form as the functional equation of an L-function attached to a primitive character.

Theorem 1.4. *Let* $\mathfrak{C}$ *be as in Theorem* 1.1. *Then, with the notation as above, one has*

$$\Lambda(1-s,\overline{\chi}) = \frac{i^{\mathfrak{a}} q^{1/2}}{\tau(\chi,1)} \Lambda(s,\chi),$$

for any *character* $\chi \in \mathfrak{C}$.

We will provide some details of the proof of Theorem 1.4 in Sec. 4, but one can simply note that the Gauss sum identity (5) also implies that

$$|\mathcal{G}_q(\chi,1)|^2 = q, \tag{11}$$

for any $\chi \in \mathfrak{C}$. The classical proof of the functional equation via Mellin transforms and theta series is then generally valid.

Remark 1.5. More generally, suppose that

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

is any L-function with known analytic continuation and functional equation, and consider the twist

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

by a primitive Dirichlet character. Provided $L(s, \chi)$ also satisfies an analytic continuation and functional equation, and that this may be proved only using property (5) of the primitive character χ, then the same proof will demonstrate the analytic continuation and functional equation of the twist $L(s, \chi)$ for *any* $\chi \in \mathfrak{C}$, independent of the primitivity of $\chi^\times$.

For some examples of higher rank L-functions as in Remark 1.5, see for instance [1].

Let us illustrate Theorem 1.1 when $q = p$, a prime. In this case, the only classical Dirichlet character which is imprimitive is the trivial character χ_0. Let $\{\chi_1, \chi_2, \ldots, \chi_{p-2}\}$ denote the set of primitive characters modulo p, viewed simply as functions

$$\chi_i : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times.$$

We extend the definition of each primitive χ_i to all of $\mathbb{Z}/p\mathbb{Z}$ by setting $\chi_i(0) := 0$. If we further extend the definition of the trivial character modulo p by setting

$$\chi_0^\pm(0) := \pm i\sqrt{p-1}, \tag{12}$$

then $\{\chi_1, \chi_2, \ldots, \chi_{p-2}, \chi_0^+, \chi_0^-\}$ is the unique set of p characters mod p which satisfy the conclusion of Theorem 1.1, as will be shown below. In this case,

$$m_\chi = \begin{cases} 2 & \text{if } \chi = \chi_0^\pm, \\ 1 & \text{otherwise.} \end{cases}$$

For similar examples of explicit constructions at levels p^2 and p^3, see Example 3.14.

2. Notation and Terminology

Any function

$$\chi : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$$

which is not identically zero and satisfies (6) will be called *q-multiplicative*. The restriction of χ to $(\mathbb{Z}/q\mathbb{Z})^\times$ will be denoted by $\chi^\times$. Note that if χ is q-multiplicative then $\chi^\times$ is a group homomorphism,

$$\chi^\times : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times.$$

In particular, $|\chi(n)| = 1$ if $(n, q) = 1$. Furthermore, we will denote by $\mathcal{G}_q^\times(\chi, n)$ the classical Gauss sum

$$\mathcal{G}_q^\times(\chi, n) := \sum_{m \in (\mathbb{Z}/q\mathbb{Z})^\times} \chi(m) \exp\left(\frac{2\pi i n m}{q}\right).$$

If d is a divisor of q and $\psi : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$, we will say that ψ *induces* χ if $\chi^\times = \psi^\times \circ \mathrm{red}$, where $\mathrm{red}(\cdot)$ is the reduction modulo d map. This is equivalent to requiring that $\chi(n) = \psi(n)$ for all $n \in \mathbb{Z}/q\mathbb{Z}$ for which $(n, q) = 1$. If χ is q-multiplicative, we define the *conductor* of χ to be the conductor of $\chi^\times$. Equivalently, the conductor d is the smallest modulus for which χ can be induced by a d-multiplicative function.

For $m \in \mathbb{Z}/p^\alpha\mathbb{Z}$, we will use the notation $m = p^\nu n$ $(0 \le \nu \le \alpha)$ to mean that ν is the p-adic valuation of m and $p \nmid n$. Finally, we define

$$\delta_S := \begin{cases} 1 & \text{if } S \text{ is true,} \\ 0 & \text{if } S \text{ is false.} \end{cases}$$

3. Defining the Characters

We will prove Theorem 1.1 by producing a set $\mathfrak{C} = \{\chi_1, \chi_2, \ldots, \chi_q\}$ of functions on $\mathbb{Z}/q\mathbb{Z}$ that satisfy (5)–(7), and that when restricted to $(\mathbb{Z}/q\mathbb{Z})^\times$ reproduces every character of conductor d precisely $\tau(q/d)$ times. Along the way we will also prove Theorem 1.2, characterizing a family of such sets $\mathfrak{C}$. We begin by reducing our consideration to the subset of those functions in $\mathfrak{C}$ which restrict to a given fixed character $\psi \in ((\mathbb{Z}/q\mathbb{Z})^\times)^*$.

3.1. *Reduction to fibers over a fixed character*

Given a set $\mathfrak{C} \in \mathfrak{F}_q$ and a character $\psi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$, define

$$\mathfrak{C}^\psi := \{\chi \in \mathfrak{C} : \chi^\times = \psi\}. \tag{13}$$

By property (2) of Theorem 1.1, each $\mathfrak{C}^\psi$ contains exactly $\tau(q/d)$ functions, where d is the conductor of ψ.

Proposition 3.1. *Let q be a positive integer, d a divisor of q and $\psi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ a character of conductor d. There exists a set $\mathfrak{C}^\psi$ of functions $\chi : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ with the following properties.*

(1) *The set $\mathfrak{C}^\psi$ contains exactly $\tau(q/d)$ functions, and each $\chi \in \mathfrak{C}^\psi$ satisfies* (6).
(2) *For each $\chi \in \mathfrak{C}^\psi$, one has $\chi^\times = \psi$.*
(3) *The identity* (5) *holds for all $\chi \in \mathfrak{C}^\psi$.*
(4) *For $\chi_1, \chi_2 \in \mathfrak{C}^\psi$, we have*

$$\langle \chi_1, \chi_2 \rangle_q = \begin{cases} \tau(q/d)\varphi(q) & \text{if } \chi_1 = \chi_2, \\ 0 & \text{otherwise.} \end{cases} \tag{14}$$

If $\mathfrak{C}$ satisfies the conclusions of Theorem 1.1, then the set $\mathfrak{C}^\psi$ defined by (13) is immediately seen to satisfy the conclusions of Proposition 3.1; thus Theorem 1.1 implies Proposition 3.1. Conversely, Proposition 3.1 implies Theorem 1.1. Indeed, define

$$\mathfrak{F}_q^\psi := \{\text{Subsets } \mathfrak{C}^\psi \subseteq \mathbb{C}^{\mathbb{Z}/q\mathbb{Z}} \text{ which satisfy the conclusions of Proposition 3.1}\}. \tag{15}$$

Proposition 3.1 asserts that every $\mathfrak{F}_q^{\psi}$ is non-empty, while Theorem 1.1 asserts that $\mathfrak{F}_q$ is non-empty. Thus, the following lemma shows that Theorem 1.1 is equivalent to Proposition 3.1.

Lemma 3.2. *Let $\mathfrak{F}_q$ be defined by* (8) *and $\mathfrak{F}_q^{\psi}$ by* (15). *There is a bijection*

$$\mathfrak{F}_q \leftrightarrow \prod_{\psi\in((\mathbb{Z}/q\mathbb{Z})^{\times})^*} \mathfrak{F}_q^{\psi}.$$

Proof. The bijection is given by

$$\mathfrak{F}_q \ni \mathfrak{C} \mapsto (\mathfrak{C}^{\psi})_{\psi\in((\mathbb{Z}/q\mathbb{Z})^{\times})^*}$$

(where $\mathfrak{C}^{\psi}$ is as in (13)) and

$$\prod_{\psi\in((\mathbb{Z}/q\mathbb{Z})^{\times})^*} \mathfrak{F}_q^{\psi} \ni (\mathfrak{C}^{\psi})_{\psi\in((\mathbb{Z}/q\mathbb{Z})^{\times})^*} \mapsto \bigsqcup_{\psi\in((\mathbb{Z}/q\mathbb{Z})^{\times})^*} \mathfrak{C}^{\psi}.$$

To see that $\sqcup_{\psi\in((\mathbb{Z}/q\mathbb{Z})^{\times})^*} \mathfrak{C}^{\psi} \in \mathfrak{F}_q$, write $\mathbb{Z}/q\mathbb{Z} = \sqcup_{d|q} d(\mathbb{Z}/q\mathbb{Z})^{\times}$ and note that, for $\psi_1 \neq \psi_2$ and $\chi_1 \in \mathfrak{C}^{\psi_1}$, $\chi_2 \in \mathfrak{C}^{\psi_2}$, one has

$$\langle \chi_1, \chi_2\rangle_q = \sum_{d|q} \chi_1(d)\overline{\chi_2(d)}\frac{\varphi(q/d)}{\varphi(q)} \sum_{m\in(\mathbb{Z}/q\mathbb{Z})^{\times}} \psi_1(m)\overline{\psi_2(m)} = 0.$$

All other details are readily verified. □

We have thus reduced Theorem 1.1 to Proposition 3.1. Furthermore, Lemma 3.2 reduces Theorem 1.2 to the following proposition.

Proposition 3.3. *Let*

$$\mathfrak{F}_q^{\psi} := \{\textit{Subsets } \mathfrak{C}^{\psi} \subseteq \mathbb{C}^{\mathbb{Z}/q\mathbb{Z}} \textit{ which satisfy the conclusions of Proposition } 3.1\}.$$

Then there is an injective map

$$\prod_{\substack{p|q\\ N_p^{\psi}\geq 2}} ((\mathbb{T}_{N_p^{\psi}+1}/S_{N_p^{\psi}+1}) \times O_{N_p^{\psi}-1}(\mathbb{R})) \times \prod_{\substack{p|q\\ \gamma_p^{\psi}\geq 1\\ N_p^{\psi}=1}} (\mathbb{T}_{N_p^{\psi}+1}/S_{N_p^{\psi}+1}) \hookrightarrow \mathfrak{F}_q^{\psi}, \tag{16}$$

where any empty product on the left-hand side is interpreted as a set with one element. Furthermore, there exists a set $\mathfrak{C}^{\psi} \in \mathfrak{F}_q^{\psi}$ for which $\overline{\mathfrak{C}^{\psi}} \in \mathfrak{F}_q^{\overline{\psi}}$.

Remark 3.4. Since $\mathbb{T}_{N+1} \neq \emptyset$ (for instance $(\frac{\pi j}{N+1}) \in \mathbb{T}_{N+1}$), the right-hand side of (16) is non-empty, and so Proposition 3.1 follows from Proposition 3.3.

In the next section, we will reduce Proposition 3.3 to the case where q is a prime power.

3.2. *Reduction to the case of prime power modulus*

We now use the Chinese remainder theorem to reduce the proof of Proposition 3.3 to the case where q is a prime power. Fix once and for all a group homomorphism

$$\psi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$$

of conductor d, which is understood to be the character occurring in the statement of Proposition 3.3. For each prime power p^α exactly dividing q, let

$$\iota_{p^\alpha} : \mathbb{Z}/p^\alpha\mathbb{Z} \to \prod_{\ell^\alpha \| q} \mathbb{Z}/\ell^\alpha\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z}$$

be the injective function defined by $x \mapsto (1, \ldots, 1, x, 1, \ldots 1)$, followed by the isomorphism of the Chinese remainder theorem. Thus, $\iota_{p^\alpha}(x) = m$ if and only if $m \equiv x \bmod p^\alpha$ and $m \equiv 1 \bmod q/p^\alpha$. Notice that, for any $n \in \mathbb{Z}/q\mathbb{Z}$,

$$n = \prod_{p^\alpha \| q} \iota_{p^\alpha}(n \bmod p^\alpha). \tag{17}$$

For any function $\chi : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$, put $\chi_{p^\alpha} := \chi \circ \iota_{p^\alpha}$. It follows from (17) that, provided χ satisfies (6), one has

$$\forall\, n \in \mathbb{Z}/q\mathbb{Z}, \quad \chi(n) = \prod_{p^\alpha \| q} \chi_{p^\alpha}(n \bmod p^\alpha), \tag{18}$$

or in other words, $\chi = \bigotimes_{p^\alpha \| q} \chi_{p^\alpha}$. Conversely, if each local character χ_{p^α} satisfies

$$\chi_{p^\alpha}(nm) = \chi_{p^\alpha}(n)\chi_{p^\alpha}(m), \quad \text{provided either } n \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \text{ or } m \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times, \tag{19}$$

then the function χ defined by (18) satisfies (6). Furthermore, the local version of (5) is

$$\forall\, n \in \mathbb{Z}/p^\alpha\mathbb{Z}, \quad \mathcal{G}_q(\overline{\chi_{p^\alpha}}, n) = \chi_{p^\alpha}(n)\mathcal{G}_q(\overline{\chi_{p^\alpha}}, 1). \tag{20}$$

For any set $\mathfrak{C}$ of functions $\chi : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$, define

$$\mathfrak{C}_{p^\alpha} := \{\chi_{p^\alpha} : \chi \in \mathfrak{C}\}.$$

If p^γ is the exact power of p dividing d, then ψ_{p^α} is the local character of conductor p^γ associated to ψ. Note that

$$\chi^\times = \psi \Rightarrow \chi_{p^\alpha}^\times = \psi_{p^\alpha}.$$

If $\mathfrak{C}^\psi$ is a set of functions $\chi : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$, each of which satisfies $\chi^\times = \psi$, then we introduce the notation

$$\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}} = (\mathfrak{C}^\psi)_{p^\alpha} := \{\chi_{p^\alpha} : \ \chi \in \mathfrak{C}^\psi\}. \tag{21}$$

It is reasonable to expect the set $\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}$ to satisfy the following local version of Proposition 3.1.

Proposition 3.5. *Let α and γ be non-negative integers with $0 \leq \gamma \leq \alpha$, and let $\psi_{p^\alpha} : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to \mathbb{C}^\times$ be a character of conductor p^γ. There exists a set $\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}$ of functions $\chi_{p^\alpha} : \mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{C}$ with the following properties.*

(1) *The set $\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}$ contains exactly $\tau(p^{\alpha-\gamma}) = \alpha - \gamma + 1$ functions, and each $\chi_{p^\alpha} \in \mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}$ satisfies* (19).

(2) *For each $\chi_{p^\alpha} \in \mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}$, one has $\chi_{p^\alpha}^\times = \psi_{p^\alpha}$.*

(3) *The identity* (20) *holds for all $\chi_{p^\alpha} \in \mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}$.*

(4) *For $\chi_1, \chi_2 \in \mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}$, we have*

$$\langle \chi_1, \chi_2 \rangle_{p^\alpha} = \begin{cases} \tau(p^{\alpha-\gamma})\varphi(p^\alpha) & \text{if } \chi_1 = \chi_2, \\ 0 & \text{otherwise.} \end{cases} \tag{22}$$

Furthermore, we extend (15) by defining

$$\mathfrak{F}_{p^\alpha}^{\psi_{p^\alpha}} := \{\text{Subsets } \mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}} \subseteq \mathbb{C}^{\mathbb{Z}/p^\alpha\mathbb{Z}} \text{ which satisfy the conclusions of Proposition 3.5}\}. \tag{23}$$

The following is the local version of Proposition 3.3.

Proposition 3.6. *Let $0 \leq \gamma \leq \alpha$ be non-negative integers and $\psi_{p^\alpha} : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to \mathbb{C}^\times$ a character of conductor p^γ. Let $\mathfrak{F}_{p^\alpha}^{\psi_{p^\alpha}}$ be defined by* (23). *Then there is a one-to-one correspondence*

$$\mathfrak{F}_{p^\alpha}^{\psi_{p^\alpha}} \leftrightarrow \begin{cases} (\mathbb{T}_{\alpha-\gamma+1}/S_{\alpha-\gamma+1}) \times O_{\alpha-\gamma-1}(\mathbb{R}) & \text{if } \alpha - \gamma \geq 2, \\ \mathbb{T}_{\alpha-\gamma+1}/S_{\alpha-\gamma+1} & \text{if } \gamma \geq 1 \text{ and } \alpha - \gamma = 1, \\ \{1\} & \text{otherwise.} \end{cases} \tag{24}$$

Furthermore, there exists a set $\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}} \in \mathfrak{F}_{p^\alpha}^{\psi_{p^\alpha}}$ for which $\overline{\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}} \in \mathfrak{F}_{p^\alpha}^{\overline{\psi_{p^\alpha}}}$.

We will show (see Lemma 3.8) that $\mathfrak{C}^\psi$ satisfies the conclusions of Proposition 3.1, provided each $\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}$ satisfies the conclusions of Proposition 3.5. However, our current proof does not show that the converse holds. We emphasize this with the following question.

Question 3.7. *Defining $\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}$ is as in* (21), *is the implication*

$$\mathfrak{C}^\psi \in \mathfrak{F}_q^\psi \Rightarrow \forall\, p^\alpha \parallel q, \mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}} \in \mathfrak{F}_{p^\alpha}^{\psi_{p^\alpha}} \tag{25}$$

necessarily true? (*A proof of* (25) *would imply that the injection* (10) *of Theorem* 1.2 *is in fact a bijection.*)

As before, Proposition 3.5 follows from Proposition 3.6, since the right-hand side of (24) is non-empty. The following lemma shows that Proposition 3.3 follows from Proposition 3.6.

Lemma 3.8. *There is an injection of sets*

$$\prod_{p^\alpha \parallel q} \mathfrak{F}_{p^\alpha}^{\psi_{p^\alpha}} \hookrightarrow \mathfrak{F}_q^\psi.$$

Proof. The injection is given by

$$\prod_{p^\alpha \,\|\, q} \mathfrak{F}_{p^\alpha}^{\psi_{p^\alpha}} \ni (\mathfrak{C}_{p^\alpha})_{p^\alpha \,\|\, q} \mapsto \left\{ \bigotimes_{p^\alpha \,\|\, q} \chi_{p^\alpha} : (\chi_{p^\alpha}) \in \prod_{p^\alpha \,\|\, q} \mathfrak{C}_{p^\alpha} \right\}.$$

Equation (18) shows that if χ_{p^α} is p^α-multiplicative, then $\chi := \bigotimes_{p^\alpha \,\|\, q} \chi_{p^\alpha}$ is q-multiplicative. Also, since

$$\langle \chi_1, \chi_2 \rangle_q = \prod_{p^\alpha \,\|\, q} \langle (\chi_1)_{p^\alpha}, (\chi_2)_{p^\alpha} \rangle_{p^\alpha}$$

holds for any q-multiplicative χ_1 and χ_2, one deduces (14) from (22). Finally, using the identity

$$\mathcal{G}_q(\chi, n) = \prod_{p^\alpha \,\|\, q} \chi_{p^\alpha}(q/p^\alpha) \mathcal{G}_{p^\alpha}(\chi_{p^\alpha}, n),$$

which holds for any q-multiplicative χ, one deduces (5) from (20). This completes the proof of Lemma 3.8. □

The remainder of the paper is devoted to proving Proposition 3.6, from which Theorem 1.2, and hence Theorem 1.1, will follow.

3.3. *The construction for a prime power modulus*

For brevity, the character $\psi_{p^\alpha} : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to \mathbb{C}^\times$ of conductor p^γ will henceforth be denoted simply by ψ, and the corresponding set $\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}$ will likewise be abbreviated by $\mathfrak{C}_\psi$. Furthermore, consistently with (9), we define

$$N_\psi := \alpha - \gamma.$$

We will produce a set $\mathfrak{C}_\psi$ of $\tau(p^\alpha/p^\gamma) = N_\psi + 1$ functions $\chi : \mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{C}$ so that

$$\forall\, \chi \in \mathfrak{C}_\psi, \quad \chi \text{ is } p^\alpha\text{-multiplicative} \quad \text{and} \quad \chi^\times = \psi, \tag{26}$$

and so that every $\chi \in \mathfrak{C}_\psi$ satisfies (20) and any pair $\chi_1, \chi_2 \in \mathfrak{C}_\psi$ satisfies (22). Furthermore, we will parametrize all such sets $\mathfrak{C}_\psi$.

Note that, if $n \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, then $\chi(p^\nu n) = \chi(p^\nu)\chi(n)$, and so extending ψ to a function $\chi : \mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{C}$ satisfying (19) amounts to specifying the complex numbers $\chi(p^\beta)$ for $0 \le \beta \le \alpha$. The following lemma shows that we only need to concern ourselves with β in the range $0 \le \beta \le \alpha - \gamma$.

Lemma 3.9. *Suppose that* $\chi : \mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{C}$ *is any* p^α*-multiplicative function of conductor* p^γ. *Then* $\chi(p^\beta) = 0$ *for each* $\beta > \alpha - \gamma$.

Proof. Suppose that $\beta > \alpha - \gamma$. Since $\gamma > \alpha - \beta$, there is an element

$$n \in 1 + p^{\alpha-\beta} \frac{\mathbb{Z}/p^\alpha\mathbb{Z}}{p^\beta\mathbb{Z}/p^\alpha\mathbb{Z}}$$

for which $\chi^{\times}(n) \neq 1$. Then,

$$\chi(p^{\beta}) = \chi(p^{\beta}n) = \chi(p^{\beta})\chi(n),$$

which proves that $\chi(p^{\beta}) = 0$. □

The next lemma computes the inner product $\langle \chi_1, \chi_2 \rangle_{p^{\alpha}}$ in terms of the complex numbers $\chi(p^{\nu})$.

Lemma 3.10. *Let* $\chi_1, \chi_2 : \mathbb{Z}/p^{\alpha}\mathbb{Z} \to \mathbb{C}$ *be two functions satisfying* (19). *Then one has*

$$\langle \chi_1, \chi_2 \rangle_{p^{\alpha}} = \begin{cases} \displaystyle\sum_{\nu=0}^{\alpha} \varphi(p^{\alpha-\nu})\chi_1(p^{\nu})\overline{\chi}_2(p^{\nu}) & \textit{if } \chi_1^{\times} = \chi_2^{\times}, \\ 0 & \textit{if } \chi_1^{\times} \neq \chi_2^{\times}. \end{cases}$$

Proof. Let p^{γ_i} be the conductor of $\chi_i^{\times}$ and put $\gamma := \max\{\gamma_1, \gamma_2\}$. By Lemma 3.9, we have

$$\sum_{m \in \mathbb{Z}/p^{\alpha}\mathbb{Z}} \chi_1(m)\overline{\chi}_2(m) = \sum_{\nu=0}^{\alpha-\gamma} \chi_1(p^{\nu})\overline{\chi}_2(p^{\nu}) \sum_{n \in (\mathbb{Z}/p^{\alpha-\nu}\mathbb{Z})^{\times}} \chi_1^{\times}(n)\overline{\chi}_2^{\times}(n),$$

which proves the lemma. □

The following proposition transforms the conditions (20) and (22) into properties of the various complex numbers $\chi(p^{\nu})$. It will be convenient to renormalize as follows. Let $\mathfrak{S}$ denote the one-to-one correspondence

$$\mathfrak{S} : \{\chi : \mathbb{Z}/p^{\alpha}\mathbb{Z} \to \mathbb{C} \text{ satisfying (19) and } \chi^{\times} = \psi\} \to \left\{\frac{1}{\sqrt{N_{\psi}+1}}\right\} \times \mathbb{C}^{N_{\psi}}$$

defined by

$$\mathfrak{S}(\chi) := \begin{cases} \dfrac{1}{\sqrt{N_{\psi}+1}}\left(\dfrac{\chi(p^0)}{p^{0/2}}, \dfrac{\chi(p^1)}{p^{1/2}}, \ldots, \dfrac{\chi(p^{N_{\psi}})}{p^{N_{\psi}/2}}\right) & \text{if } \psi \text{ is non-trivial} \\ \dfrac{1}{\sqrt{N_{\psi}+1}}\left(\dfrac{\chi(p^0)}{p^{0/2}}, \dfrac{\chi(p^1)-\chi(p^0)}{p^{1/2}}, \ldots, \dfrac{\chi(p^{N_{\psi}})-\chi(p^{N_{\psi}-1})}{p^{N_{\psi}/2}}\right) & \text{if } \psi \text{ is trivial.} \end{cases} \tag{27}$$

Furthermore, for each $\chi \in \mathfrak{C}_{\psi}$, define x_{ν}^{χ} to be the νth coordinate of $\mathfrak{S}(\chi)$, i.e. put

$$\mathfrak{S}(\chi) =: (x_0^{\chi}, x_1^{\chi}, x_2^{\chi} \ldots x_{N_{\psi}}^{\chi}) \in \left\{\frac{1}{\sqrt{N_{\psi}+1}}\right\} \times \mathbb{C}^{N_{\psi}}.$$

Finally, define the matrix $T_\psi \in M_{(N_\psi+1)\times(N_\psi+1)}(\mathbb{R})$ by specifying its (j,k)th coordinate $T_\psi(j,k)$ as follows[b]:

$$T_\psi(j,k) := \begin{cases} \delta_{j=k} & \text{if } \psi \text{ is non-trivial,} \\ p^{\frac{-|j-k|}{2}}\left(1-\dfrac{1}{p}\right)^{-1} & \text{if } \psi \text{ is trivial.} \end{cases}$$

The matrix T_ψ is checked in either case to be positive-definite (see the proof of Proposition 3.11 below for the case in which ψ is trivial), and so it determines an inner product

$$\langle x, y\rangle_\psi := x^t T_\psi \overline{y} \quad (x, y \in \mathbb{C}^{N_\psi+1}).$$

Proposition 3.11. *Let $\psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to \mathbb{C}^\times$ be a multiplicative character and let $\mathfrak{C}_\psi$ be any set of $N_\psi + 1$ functions satisfying* (26). *Then,*

$$\mathfrak{C}_\psi \textit{ satisfies } (22) \Leftrightarrow \forall\, v_1, v_2 \in \mathfrak{S}(\mathfrak{C}_\psi), \langle v_1, v_2\rangle_\psi = \delta_{v_1=v_2}.$$

Furthermore, for each $\chi \in \mathfrak{C}_\psi$,

$$\chi \textit{satisfies } (20) \Leftrightarrow \forall\, \nu \textit{ with } 0 \le \nu \le N_\psi, x_\nu^\chi \overline{x}_{N_\psi}^\chi = \overline{x}_{N_\psi-\nu}^\chi x_0^\chi.$$

Proof. The first statement follows by using (27) and some linear algebra to translate Lemma 3.10 into a statement about the vectors $\mathfrak{S}(\chi_1)$ and $\mathfrak{S}(\chi_2)$, although the case where ψ is trivial is somewhat involved. It makes use of the fact that T_ψ is a Gram matrix, i.e. one can write $T_\psi = Q_\psi^t Q_\psi$, where $Q_\psi^{-1} \in M_{(N_\psi+1)\times(N_\psi+1)}(\mathbb{R})$ is defined to have (j,k)th coordinate given by

$$Q_\psi^{-1}(j,k) := \begin{cases} 1 & \text{if } j = k < N_\psi, \\ \left(1-\dfrac{1}{p}\right)^{1/2} & \text{if } j = k = N_\psi, \\ -p^{-1/2} & \text{if } j = k+1, \\ 0 & \text{otherwise.} \end{cases} \tag{28}$$

The second statement is deduced from the following lemma, whose proof is a calculation, using repeatedly that the sum of the values of a non-trivial character on a finite group is zero.

Lemma 3.12. *Let $\psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to \mathbb{C}^\times$ be a multiplicative character of conductor p^γ and let $\mathfrak{C}_\psi$ be any set of functions $\chi : \mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{C}$ for which* (26) *holds. Then, for any $m = p^\nu n \in \mathbb{Z}/p^\alpha\mathbb{Z}$ (where $p \nmid n$), one has*

$$\mathcal{G}_{p^\alpha}(\chi, p^\nu n) = \begin{cases} p^\nu \chi(p^{N_\psi-\nu}) \cdot \delta_{\nu \le N_\psi} \cdot \mathcal{G}_{p^\gamma}^\times(\chi, n) & \textit{if } \gamma > 0, \\ -p^\nu \chi(p^{\alpha-1-\nu}) \cdot \delta_{\nu \le \alpha-1} + \displaystyle\sum_{\mu=\alpha-\nu}^{\alpha} \varphi(p^{\alpha-\mu})\chi(p^\mu) & \textit{if } \gamma = 0. \end{cases}$$

The rest of the details of the proof of Proposition 3.11 are left to the reader. □

[b] We will assume that all matrix index ranges begin with 0.

Corollary 3.13. *Let ψ and $\mathfrak{C}_\psi$ be as in the hypotheses of Proposition* 3.11. *Let X_ψ denote the $(N_\psi + 1) \times (N_\psi + 1)$ matrix whose columns are the vectors in $\mathfrak{S}(\mathfrak{C}_\psi)$, and let V_ψ denote the matrix of the same dimensions given by*

$$V_\psi(j,k) := \delta_{j+k=N_\psi}.$$

Then $\mathfrak{C}_\psi$ satisfies (22) *if and only if*

$$X_\psi^t T_\psi \overline{X_\psi} = I. \tag{29}$$

Moreover, (20) *is satisfied for all $\chi \in \mathfrak{C}_\psi$ if and only if there is a diagonal matrix D_ψ so that*

$$V_\psi \overline{X_\psi} = X_\psi D_\psi. \tag{30}$$

From this result it follows that in order to construct the desired set $\mathfrak{C}_\psi$ it suffices to find a solution X_ψ to the matrix equations (29) and (30) which has the additional property that

$$X_\psi(0,k) = \frac{1}{\sqrt{N_\psi + 1}} \tag{31}$$

for $k = 0, 1, \ldots, N_\psi$. When ψ is non-trivial this is straightforward. Since T_ψ is simply the identity in this case, an appropriately scaled version of the character table for $\mathbb{Z}/(N_\psi + 1)\mathbb{Z}$ provides a solution. Specifically, the matrix defined by

$$X_\psi(j,k) = \frac{1}{\sqrt{N_\psi + 1}} \exp\left(\frac{2\pi i jk}{N_\psi + 1}\right) \tag{32}$$

is readily seen to satisfy (29)–(31). We will see that this is not the only solution, however.

When ψ is trivial matters are decidedly more complicated, as the following examples illustrate.

Example 3.14. We now exhibit three extensions to all of $\mathbb{Z}/p^2\mathbb{Z}$ of the trivial character on $(\mathbb{Z}/p^2\mathbb{Z})^\times$. In this case, $N_\psi + 1 = 3$ and we consider the 3×3 matrix X_3 defined by

$$X_3 := \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ -2p^{-1/2} + r & (p^{-1/2} + r)\zeta_3 & (p^{-1/2} + r)\zeta_3^2 \\ 1 & \zeta_3^2 & \zeta_3 \end{pmatrix},$$

where $r := \sqrt{1 - \frac{1}{p}}$ and $\zeta_3 \in \mathbb{C}$ denotes a primitive third root of unity. The matrix X_3 seen to satisfy $X_3^t T_3 \overline{X_3} = I$, where

$$T_3 = \left(1 - \frac{1}{p}\right)^{-1} \begin{pmatrix} 1 & p^{-1/2} & p^{-1} \\ p^{-1/2} & 1 & p^{-1/2} \\ p^{-1} & p^{-1/2} & 1 \end{pmatrix}.$$

Furthermore, one verifies that (30) holds, i.e. we have that $V_3\overline{X_3} = X_3 D_3$, where

$$V_3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{and} \quad D_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta_3 & 0 \\ 0 & 0 & \zeta_3^2 \end{pmatrix}.$$

Thus, the three characters χ defined via (27) using the columns of X_3 fit into a family $\mathfrak{C}$ of extensions which satisfy the conclusions of Theorem 1.1 with $q = p^2$.

Turning to level $q = p^3$, we now construct four extensions χ to all of $\mathbb{Z}/p^3\mathbb{Z}$ of the trivial character on $(\mathbb{Z}/p^3\mathbb{Z})^\times$, again via (27) by the columns of the matrix

$$X_4 := \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ -2p^{-\frac{1}{2}} + r_1 & \dfrac{(-1+i)(r_1 - ir_2)}{2} & 2p^{-\frac{1}{2}} - r_2 & \dfrac{(-1-i)(r_1 + ir_2)}{2} \\ -2p^{-\frac{1}{2}} + r_1 & \dfrac{(-1+i)(r_1 + ir_2)}{2} & -2p^{-\frac{1}{2}} + r_2 & \dfrac{(-1-i)(r_1 - ir_2)}{2} \\ 1 & -i & -1 & i \end{pmatrix}$$

where $r_j = p^{-1/2} + \sqrt{1 + \frac{(-1)^j}{\sqrt{p}}}$ for $j = 1, 2$. One verifies that $X_4^t T_4 \overline{X_4} = I$, where

$$T_4 = \left(1 - \frac{1}{p}\right)^{-1} \begin{pmatrix} 1 & p^{-1/2} & p^{-1} & p^{-3/2} \\ p^{-1/2} & 1 & p^{-1/2} & p^{-1} \\ p^{-1} & p^{-1/2} & 1 & p^{-1/2} \\ p^{-3/2} & p^{-1} & p^{-1/2} & 1 \end{pmatrix}.$$

Furthermore, one has $V_4\overline{X_4} = X_4 D_4$, where

$$V_4 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad D_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix}.$$

Note that, as $p \to \infty$, the matrix $\sqrt{3}X_3$ (respectively $\sqrt{4}X_4$) limits to the character table for the group $\mathbb{Z}/3\mathbb{Z}$ (respectively for the group $\mathbb{Z}/4\mathbb{Z}$), while T limits to the identity matrix.

We now return to the proof of Proposition 3.6. As we will now be focusing on the trivial character exclusively, it will cause no confusion to drop the subscript ψ from our notation. If $Q = Q_\psi$ is defined by (28) and if we let $Y = QX$ and $W = QVQ^{-1}$, then X satisfies (29)–(31) if and only if Y satisfies

$$Y^t\overline{Y} = I, \tag{33}$$

$$Y^{-1}W\overline{Y} = D \text{ is diagonal}, \tag{34}$$

$$Y(0,k) = \frac{1}{\sqrt{N+1}}, \quad \forall\, k. \tag{35}$$

Observe that if we multiply both sides of $W\overline{Y} = YD$ by W on the left and use the fact that $W^2 = I$, we are led to

$$\overline{Y} = WYD = \overline{YD}D,$$

from which it follows that (34) can only occur if the diagonal entries of D have complex modulus 1. If we let $D^{1/2}$ denote any diagonal square root of D and set $Z = YD^{1/2}$, then Y satisfies (33)–(35) if and only if Z satisfies

$$Z^t\overline{Z} = I, \tag{36}$$

$$Z^{-1}W\overline{Z} = I, \tag{37}$$

$$|Z(0,k)| = \frac{1}{\sqrt{N+1}}, \quad \forall\, k. \tag{38}$$

In this case, the jth diagonal entry of $D^{1/2}$ is given by $Z(0,j)\sqrt{N+1}$. Note that Z and X are related directly by $X = Q^{-1}Z(D^{1/2})^{-1}$.

We will now completely determine all the matrices $Z \in M_{(N+1)\times(N+1)}(\mathbb{C})$ that simultaneously satisfy Eqs. (36)–(38). Set

$$M_1 = \left\lceil \frac{N+1}{2} \right\rceil,$$

$$M_2 = \left\lfloor \frac{N+1}{2} \right\rfloor.$$

Note that, for $l \in \{1,2\}$,

$$M_l \text{ is the dimension of the } (-1)^{l-1}\text{-eigenspace of } V, \tag{39}$$

and in particular, $M_1 + M_2 = N+1$. Let I_n denote the $n \times n$ identity matrix and define $U_1 \in M_{M_1\times M_1}(\mathbb{R})$ and $U_2 \in M_{M_2\times M_2}(\mathbb{R})$ to be the block-diagonal matrices

$$U_1 = \begin{cases} \begin{pmatrix} I_{M_1-1} & \\ & (1-p^{-1/2})^{1/2} \end{pmatrix} & \text{if } N \text{ is odd,} \\ \begin{pmatrix} I_{M_1-2} & & \\ & 1 & -p^{-1/2} \\ & 0 & \sqrt{2}(1-p^{-1})^{1/2} \end{pmatrix} & \text{if } N \text{ is even} \end{cases}$$

and

$$U_2 = \begin{cases} \begin{pmatrix} I_{M_2-1} & \\ & (1+p^{-1/2})^{1/2} \end{pmatrix} & \text{if } N \text{ is odd,} \\ I_{M_2} & \text{if } N \text{ is even.} \end{cases}$$

We will use U_1 and U_2 to characterize matrices $Z \in M_{(N+1)\times(N+1)}(\mathbb{C})$ which satisfy (36) and (37) (see Proposition 3.17), but first we establish two preparatory lemmas.

Lemma 3.15. *For $l \in \{1,2\}$,*

$$I + (-1)^{l-1}W = \begin{pmatrix} U_l^tU_l & * \\ * & * \end{pmatrix}.$$

Proof. From the definition of Q^{-1} we can write

$$Q^{-1} = (I - p^{-1/2}L)\Delta,$$

where L is the nilpotent matrix whose only non-zero entries are ones along the lower main subdiagonal, and Δ is diagonal. Therefore

$$Q = \Delta^{-1}\sum_{\lambda=0}^{\infty} p^{-\lambda/2}L^{\lambda}$$

and since $W = QVQ^{-1}$, we find that

$$W = \Delta^{-1}\left(V + \left(\sum_{\lambda=0}^{\infty} p^{-(\lambda+1)/2}L^{\lambda}\right)(LV - VL)\right)\Delta.$$

As only the $\lambda = 0, 1$ terms contribute to the upper-left $M_1 \times M_1$ block of W, the result follows by explicit computation. □

Lemma 3.16. *For $l \in \{1, 2\}$ let E_l denote the $(-1)^{l-1}$-eigenspace of W. Then*

$$E_l = \mathrm{Col}(I + (-1)^{l-1}W).$$

In particular, the first M_l columns of $I + (-1)^{l-1}W$ form a basis of E_l.

Proof. Since $W^2 = I$, multiplication by $I + (-1)^{l-1}W$ provides a linear transformation from $\mathbb{C}^{N+1}$ onto E_l, which proves the first equality. Since V and W are similar, and the $(-1)^{l-1}$-eigenspace of V has dimension M_l, $\dim E_l = M_l$. The second statement now follows from Lemma 3.15 and the fact that $\det U_l^t U_l \neq 0$. □

Proposition 3.17. *A matrix $Z \in M_{(N+1)\times(N+1)}(\mathbb{C})$ satisfies (36) and (37) if and only if*

$$Z = (I + W)\begin{pmatrix} U_1^{-1}A \\ 0 \end{pmatrix} + i(I - W)\begin{pmatrix} U_2^{-1}B \\ 0 \end{pmatrix}, \tag{40}$$

where $A \in M_{M_1\times(N+1)}(\mathbb{R}), B \in M_{M_2\times(N+1)}(\mathbb{R})$, 0 represents a zero matrix of sufficient size to make the indicated matrix square, and

$$\sqrt{2}\begin{pmatrix} A \\ B \end{pmatrix} \in O_{N+1}(\mathbb{R}). \tag{41}$$

The matrices A and B are unique. Furthermore, if $N \geq 2$ then

$$Z(0, k) = A(0, k) + iB(0, k) \tag{42}$$

for $k = 0, 1, \ldots, N$.

Proof. Write $Z = \hat{A} + i\hat{B}$, with $\hat{A}, \hat{B} \in M_{(N+1)\times(N+1)}(\mathbb{R})$. Then Z satisfies (37) if and only if $W\hat{A} - iW\hat{B} = \hat{A} + i\hat{B}$. Since W is real, this shows that the columns of $\hat{A}$ belong to the 1-eigenspace of W and that the columns of $\hat{B}$ belong to W's -1-eigenspace. By Lemma 3.16,

$$\hat{A} = (I + W)\begin{pmatrix} \tilde{A} \\ 0 \end{pmatrix}$$

and

$$\hat{B} = (I - W)\begin{pmatrix} \tilde{B} \\ 0 \end{pmatrix}$$

for a unique pair of matrices $\tilde{A} \in M_{M_1 \times (N+1)}(\mathbb{R})$ and $\tilde{B} \in M_{M_2 \times (N+1)}(\mathbb{R})$. Since W is symmetric (this is a consequence of the fact that T and V commute) and $W^2 = 1$, Lemma 3.15 implies that

$$\hat{A}^t \hat{A} = 2\tilde{A}^t U_1^t U_1 \tilde{A}$$

and

$$\hat{B}^t \hat{B} = 2\tilde{B}^t U_2^t U_2 \tilde{B},$$

and that $\hat{A}^t \hat{B} = \hat{B}^t \hat{A} = 0$. Thus, $\bar{Z}^t Z = 2(\tilde{A}^t U_1^t U_1 \tilde{A} + \tilde{B}^t U_2^t U_2 \tilde{B})$. Upon setting $A := U_1 \tilde{A}$ and $B := U_2 \tilde{B}$, this simply becomes $\bar{Z}^t Z = 2(A^t A + B^t B)$. The equivalence of (36) and (37) with (40) and (41) now follows. Since $\hat{A}$ and $\hat{B}$ are uniquely defined by Z, and these in turn uniquely define $\tilde{A}$ and $\tilde{B}$, A and B must be unique as well.

If Z has the form given by (40), then Lemma 3.15 implies that

$$Z = \begin{pmatrix} U_1^t A \\ * \end{pmatrix} + i \begin{pmatrix} U_2^t B \\ * \end{pmatrix}.$$

Since the first column of U_j is $(1, 0, \ldots, 0)^t$ when $N \geq 2$, (42) holds. This completes the proof. □

As an application of Proposition 3.17, consider the case $N = \alpha = 1$. Write $A = \begin{pmatrix} a_0 & a_1 \end{pmatrix}$ and $B = \begin{pmatrix} b_0 & b_1 \end{pmatrix}$. Then (41) becomes the three equations

$$a_j a_k + b_j b_k = \frac{\delta_{j=k}}{2}, \quad 0 \leq j \leq k \leq 1. \tag{43}$$

Instead of (42), (40) now yields

$$Z(0, j) = (1 - p^{-1/2})^{1/2} a_j + i(1 + p^{-1/2})^{1/2} b_j$$

so that (38) holds if and only if

$$(1 - p^{-1/2}) a_j^2 + (1 + p^{-1/2}) b_j^2 = \frac{1}{2} \tag{44}$$

for $j = 0, 1$. When $j = k$, (43) and (44) imply that

$$a_j^2 = b_j^2 = \frac{1}{4}$$

so that $a_j, b_j \in \{\pm 1/2\}$. There are exactly eight ways to choose the signs so that the final equation $a_1a_2 + b_1b_2 = 0$ is also satisfied. After some straightforward, but tedious, computations we arrive at the conclusion that, up to the order of its columns, the only matrix that satisfies (29)–(31) in the case that ψ is trivial and $N = 1$ is

$$X = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -p^{-1/2} + i(1-p^{-1})^{1/2} & -p^{-1/2} - i(1-p^{-1})^{1/2} \end{pmatrix}. \tag{45}$$

Inverting (27), we recover the two extensions (12) of the trivial character given in Sec. 1.

Returning now to the general case, let us make the definition

$$\tilde{\mathbb{T}}_N := \left\{ (\theta_j) \in (\mathbb{R}/2\pi\mathbb{Z})^N \,\middle|\, \sum_{j=0}^{N-1} e^{2\theta_j i} = 0 \right\}.$$

Suppose $N \geq 2$. Given $\theta = (\theta_j) \in \tilde{\mathbb{T}}_{N+1}$, define $a(\theta), b(\theta) \in \mathbb{R}^{N+1}$ by

$$a(\theta) + ib(\theta) := \frac{1}{\sqrt{N+1}}(e^{\theta_0 i}, e^{\theta_1 i}, \ldots, e^{\theta_N i})$$

and let $\mathcal{C}(\theta) = \{c_1(\theta), c_2(\theta), \ldots, c_{N-1}(\theta)\}$ be any (fixed) real orthonormal basis for $\mathrm{Span}_{\mathbb{R}}\{a(\theta), b(\theta)\}^{\perp}$ (note that for any $\theta \in \tilde{\mathbb{T}}_{N+1}$, $a(\theta)$ and $b(\theta)$ must be $\mathbb{R}$-linearly independent). For $R \in O_{N-1}(\mathbb{R})$ define $d_j(\theta, R)$ through the equation

$$\begin{pmatrix} d_1(\theta,R) \\ d_2(\theta,R) \\ \vdots \\ d_{N-1}(\theta,R) \end{pmatrix} := R \begin{pmatrix} c_1(\theta) \\ c_2(\theta) \\ \vdots \\ c_{N-1}(\theta) \end{pmatrix}.$$

Finally, define $A(\theta, R) \in M_{M_1 \times (N+1)}(\mathbb{R})$ and $B(\theta, R) \in M_{M_2 \times (N+1)}(\mathbb{R})$ by

$$A(\theta,R) := \frac{1}{\sqrt{2}}\begin{pmatrix} \sqrt{2}a(\theta) \\ d_1(\theta,R) \\ \vdots \\ d_{M_1-1}(\theta,R) \end{pmatrix}, \quad B(\theta,R) := \frac{1}{\sqrt{2}}\begin{pmatrix} \sqrt{2}b(\theta) \\ d_{M_1}(\theta,R) \\ \vdots \\ d_{N-1}(\theta,R) \end{pmatrix}.$$

Proposition 3.18. *Let $N \geq 2$. Given $(\theta, R) \in \tilde{\mathbb{T}}_{N+1} \times O_{N-1}(\mathbb{R})$, let*

$$\mathfrak{Z}(\theta,R) := (I+W)\begin{pmatrix} U_1^{-1}A(\theta,R) \\ 0 \end{pmatrix} + i(I-W)\begin{pmatrix} U_2^{-1}B(\theta,R) \\ 0 \end{pmatrix},$$

where 0 represents a zero matrix of sufficient size to make the indicated matrix square. Then $Z = \mathfrak{Z}(\theta, R)$ satisfies (36)–(38). Furthermore, $\mathfrak{Z}$ provides a bijection between $\tilde{\mathbb{T}}_{N+1} \times O_{N-1}(\mathbb{R})$ and the set of matrices which satisfy (36)–(38).

Proof. Let Z satisfy (36)–(38). Write Z as in (40). According to (41), the rows of A and B are orthogonal and each has norm $1/\sqrt{2}$. Let the first row of A be

$a = (a_0, a_1, \ldots, a_N)$ and let the first row of B be $b = (b_0, b_1, \ldots, b_N)$. The equalities (38) and (42) occur if and only if

$$a_j + ib_j = \frac{e^{i\theta_j}}{\sqrt{N+1}} \tag{46}$$

for some unique tuple $(\theta_0, \theta_1, \ldots, \theta_N) \in (\mathbb{R}/2\pi\mathbb{Z})^{N+1}$. We then have

$$\frac{1}{N+1}\sum_{j=0}^{N} e^{2i\theta_j} = \sum_{j=0}^{N}(a_j + ib_j)^2 = |a|^2 - |b|^2 + 2i\langle a, b\rangle = 0. \tag{47}$$

This shows that $\theta = (\theta_0, \theta_1, \ldots, \theta_N) \in \tilde{\mathbb{T}}_{N+1}$ and that $a = a(\theta)$, $b = b(\theta)$. Since the remaining rows of $\sqrt{2}A$ and $\sqrt{2}B$ give an orthonormal basis for $\mathrm{Span}_{\mathbb{R}}\{a, b\}^{\perp}$, and any two such bases are related by a unique element of $O_{N-1}(\mathbb{R})$, we find that we can write $Z = \mathfrak{Z}(\theta, R)$ for a unique pair $(\theta, R) \in \tilde{\mathbb{T}}_{N+1} \times O_{N-1}(\mathbb{R})$. A reversal of this reasoning ensures that any matrix of the form $\mathfrak{Z}(\theta, R)$ does indeed satisfy (36)–(38), completing the proof. □

Proposition 3.18 proves the bijection (24) in the case where $\psi = \psi_{p^\alpha}$ is the trivial character and $\alpha - \gamma \geq 2$. (The passage from $\tilde{\mathbb{T}}_{N+1}$ to $\mathbb{T}_{N+1}$ is accounted for by the ambiguity in the choice of the square roots in $D^{1/2}$, and a matrix X_ψ corresponds via its columns to an *ordered* set of characters, so we must quotient by the action of S_{N+1}.) A moment's thought shows that if we let $p \to \infty$ in Proposition 3.18 (recall that the matrices W, U_1 and U_2 are functions of p), it actually does the same for non-trivial characters ψ as well, if $\alpha - \gamma \geq 2$. This follows from the fact that the matrix T_ψ in the non-trivial case is the limiting value of the trivial case. The case $\alpha - \gamma = \alpha = 1$ has already been dealt with; see (43) and (44). If $\alpha - \gamma = 1$ and $\alpha > 1$, then we take the limit as $p \to \infty$ in (44), and find that it becomes unnecessary, since it repeats particular cases of (43). As before, by (40), we find that (46) holds, which by (47) implies that $(\theta_0, \theta_1) \in \tilde{\mathbb{T}}_2$. Finally, in the remaining case $\alpha = \gamma$, Lemma 3.9 implies that we must have

$$\gcd(n, p^\alpha) > 1 \Rightarrow \chi(n) = 0,$$

and so the extension χ is unique. We have verified (24).

To finish the proof of Proposition 3.6, it only remains to show that there exists a set $\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}} \in \mathfrak{F}_{p^\alpha}^{\psi_{p^\alpha}}$ for which $\overline{\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}} \in \mathfrak{F}_{p^\alpha}^{\overline{\psi_{p^\alpha}}}$, which we now do, by using Proposition 3.18 to impose additional restrictions on our character extensions. Given the limiting behavior of the matrix T_ψ just mentioned, it is natural to look for matrices X_ψ which enjoy a similar relationship. Equation (32) gives one choice for the extension matrix of a non-trivial character, and it seems natural to ask whether one can arrange to have the matrices X_ψ (for ψ trivial) converge to it as $p \to \infty$. The next result shows that this is indeed case.

Proposition 3.19. *Fix $N \geq 2$ and let $C_N \in M_{(N+1)\times(N+1)}(\mathbb{C})$ be given by*

$$C_N(j,k) = \frac{1}{\sqrt{N+1}} \exp\left(\frac{2\pi ijk}{N+1}\right).$$

For every character ψ with $N_\psi = N$, it is possible to choose X_ψ satisfying (29)–(31) *so that*

$$\lim_{p\to\infty} X_\psi = C_N.$$

Proof. According to (32) it suffices to assume that ψ is trivial. Moreover, (45) shows that we may assume $N \geq 2$. Define $A \in M_{M_1\times(N+1)}(\mathbb{R})$ and $B \in M_{M_2\times(N+1)}(\mathbb{R})$ through the equations

$$A(j,k) + iB(j,k) := \frac{1}{\sqrt{N+1}} \exp\left(\frac{i\pi(2j+1)k}{N+1}\right) \tag{48}$$

for $0 \leq j \leq M_2 - 1$ and, when $M_1 > M_2$,

$$A(M_1 - 1, k) := \frac{(-1)^k}{\sqrt{2(N+1)}}. \tag{49}$$

We claim first that

$$\sqrt{2}\begin{pmatrix} A \\ B \end{pmatrix} \in O_{N+1}(\mathbb{R}).$$

To see this, let the jth rows of A and B be denoted by a_j and b_j, respectively. By expanding the inner products $\langle a_{j_1} + ib_{j_1}, a_{j_2} \pm ib_{j_2}\rangle$ first using linearity, and then explicitly using (48) and (49), one finds that the first $M_2 - 1$ rows of A and B are mutually orthogonal with norms equal to $1/\sqrt{2}$. When $M_1 = M_2$ this establishes our claim. When $M_1 > M_2$ similar computations can be carried out for the final row a_{M_1-1} of A, making use of the fact that N is even in this case.

Now construct Z using A and B according to (40) and let $D^{1/2}$ be the diagonal matrix whose diagonal entries are $\exp(i\pi k/(N+1))$. Proposition 3.17 then guarantees that Z satisfies (36)–(38), and hence that $X = Q^{-1}Z(D^{1/2})^{-1}$ satisfies (29)–(31). With these choices we have

$$\begin{aligned}
\lim_{p\to\infty} X &= \lim_{p\to\infty} Q^{-1}Z(D^{1/2})^{-1} \\
&= \left(\lim_{p\to\infty} Z\right)(D^{1/2})^{-1} \\
&= \left((I+V)\begin{pmatrix} \left(\lim\limits_{p\to\infty} U_1\right)^{-1} A \\ 0 \end{pmatrix}\right. \\
&\qquad \left. + i(I-V)\begin{pmatrix} \left(\lim\limits_{p\to\infty} U_2\right)^{-1} B \\ 0 \end{pmatrix}\right)(D^{1/2})^{-1}.
\end{aligned}$$

The reader can verify that this last expression is exactly C_N. □

We now deduce the following lemma, which will complete the proof of Proposition 3.6.

Lemma 3.20. *It is possible to choose $\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}} \in \mathfrak{F}_{p^\alpha}^{\psi_{p^\alpha}}$ so that $\overline{\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}} \in \mathfrak{F}_{p^\alpha}^{\overline{\psi_{p^\alpha}}}$.*

Proof. We begin by observing that since the matrices X_ψ provided by the proof of Proposition 3.19 depend only on the conductor of ψ, one has $X_\psi = X_{\overline{\psi}}$. We claim furthermore that the columns of X_ψ occur in complex conjugate pairs.

When ψ is non-trivial this is an immediate consequence of (32). If ψ is trivial, construct Z as in the proof of Proposition 3.19. Since Q has only real entries, left multiplication by Q preserves pairs of complex conjugate columns. Therefore X will have conjugate-paired columns if and only if $Z(D^{1/2})^{-1}$ does. But the definition of A and B implies that column 0 of $Z(D^{1/2})^{-1}$ has only real entries, and that for $k \geq 1$ the complex conjugate of column k is column $N - k + 1$.

It now follows that $\overline{\mathfrak{C}_{p^\alpha}^{\psi_{p^\alpha}}} \in \overline{\mathfrak{F}_{p^\alpha}^{\psi_{p^\alpha}}}$, which completes the proof. □

4. The Functional Equation of the Attached L-Function

In this section we provide a proof of Theorem 1.4. For the convenience of the reader, we will state explicitly various facts, some of which have already appeared earlier (see Lemma 4.1).

Let q be a positive integer, let $\mathfrak{C}$ be a set of functions satisfying the conclusion of Theorem 1, and let $\chi \in \mathfrak{C}$. If d is the conductor of $\chi^\times$ then there is a unique primitive character $\psi \in ((\mathbb{Z}/d\mathbb{Z})^\times)^*$ so that $\chi \in \mathfrak{C}^\psi$. Given a prime p and an arithmetic function f, we define the associated *Euler factor* to be the sum

$$E_p(s, f) = \sum_{\nu=0}^{\infty} \frac{f(p^\nu)}{p^s}.$$

If f is multiplicative then (formally at least)

$$L(s, f) := \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p E_p(s, f).$$

Since it is primitive, the extension of ψ to all of $\mathbb{Z}/d\mathbb{Z}$ is zero outside of $(\mathbb{Z}/d\mathbb{Z})^\times$ and $L(s, \psi)$ is the classically defined Dirichlet L-function associated to ψ. Since ψ induces χ,

$$L(s, \chi) = \left(\prod_{p \mid q} \frac{E_p(s, \chi)}{E_p(s, \psi)} \right) L(s, \psi).$$

Since $L(s, \psi)$ is known to possess a meromorphic continuation (analytic when ψ is non-trivial) to all of $\mathbb{C}$, this equation furnishes a continuation of $L(s, \chi)$.

We will prove the functional equation of $L(s, \chi)$ by first proving local functional equations for the factors $E_p(s, \chi)/E_p(s, \psi)$ for $p \mid q$ and then utilizing the well-known functional equation for $L(s, \psi)$. This is primarily for the interested reader and can be avoided altogether. Indeed (as mentioned in Sec. 1), because the Gauss sum identities (5) and (11) hold independent of primitivity, the classical proof of the functional equation via the Mellin transform and theta series is now generally valid.

Beginning with a factorization $q = q_1q_2$ with $(q_1, q_2) = 1$, let

$$\iota_{q_1} : \mathbb{Z}/q_1\mathbb{Z} \to \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z}$$

be the injective function defined by $x \mapsto (x, 1)$, followed by the isomorphism of the Chinese remainder theorem. Explicitly, $\iota_{q_1}(x) = y$ where $y \equiv x \pmod{q_1}$ and $y \equiv 1 \pmod{q_2}$. Notice that, for any $n \in \mathbb{Z}/q\mathbb{Z}$,

$$n = \iota_{q_1}(n \bmod q_1)\iota_{q_2}(n \bmod q_2). \tag{50}$$

For any function $\chi : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$, put $\chi_{q_1} := \chi \circ \iota_{q_1}$. The following lemma gives some of the salient properties of χ_{q_1}. Its proof is straightforward and is left to the reader.

Lemma 4.1. *Let q be a positive integer, $\chi : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ a function, and suppose $q = q_1q_2$ with $(q_1, q_2) = 1$.*

(i) *χ is q-multiplicative (respectively, completely multiplicative) if and only if $\chi(n) = \chi_{q_1}(n)\chi_{q_2}(n)$ for all $n \in \mathbb{Z}$ and χ_{q_i} is q_i-multiplicative (respectively, completely multiplicative) for $i = 1, 2$.*

(ii) *If $q_1 = q_3q_4$ with $(q_3, q_4) = 1$ then $(\chi_{q_1})_{q_3} = \chi_{q_3}$.*

(iii) *Suppose χ is q-multiplicative, $d \,|\, q$ and $\psi : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$ is d-multiplicative. Then ψ induces χ if and only if $\psi_{(d,q_i)}$ induces χ_{q_i} for $i = 1, 2$.*

(iv) *If χ is q-multiplicative then d is the conductor of χ if and only if (q_i, d) is the conductor of χ_{q_i} for $i = 1, 2$.*

(v) *If χ is q-multiplicative then*

$$G_{q_1}(\chi_{q_1}, n)G_{q_2}(\chi_{q_2}, n) = \frac{G_q(\chi, n)}{\chi_{q_1}(q_2)\chi_{q_2}(q_1)}.$$

In particular, if χ_{q_i} satisfies (5) (respectively, (11)) with $q = q_i$ and $\chi = \chi_{q_1}$ for $i = 1, 2$ then χ satisfies (5) (respectively, (11)).

(vi) *If $\psi : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ is a function and both χ and ψ are q-multiplicative then*

$$\langle \chi_{q_1}, \psi_{q_1}\rangle\langle \chi_{q_2}, \psi_{q_2}\rangle = \langle \chi, \psi\rangle.$$

We will now use Lemma 4.1 to prove the following lemma, which gives explicitly the L-function of $\chi \in \mathfrak{C}_\psi$.

Lemma 4.2. *Let $p \,|\, q$. If $p^\alpha \,\|\, q$ and $p^\gamma \,\|\, d$ then for* $\mathrm{Re}(s) > 0$

$$\frac{E_p(s, \chi)}{E_p(s, \psi)} = \sqrt{\alpha - \gamma + 1}\sum_{\nu=0}^{\alpha-\gamma} \frac{\chi_{q/p^\alpha}(p)^\nu x_\nu^{\chi_{p^\alpha}} p^{\nu/2}}{p^{\nu s}}.$$

Proof. If $\gamma > 0$ then $E_p(s, \psi) = 1$ and the conclusion follows immediately from part (i) of Lemma 4.1, Lemma 3.9, definition (27) and the fact that $\chi_{q/p^\alpha}(p^\nu) = \chi_{q/p^\alpha}(p)^\nu$. When $\gamma = 0$ we have $\chi_{p^\alpha}(p^\alpha) = \chi_{p^\alpha}(p^{\alpha+k})$ for any natural k so that

$$E_p(s, \chi) = \sum_{\nu=0}^{\alpha-1} \frac{\chi_{q/p^\alpha}(p)^\nu\chi_{p^\alpha}(p^\nu)}{p^{\nu s}} + \chi_{p^\alpha}(p^\alpha)\sum_{\nu=\alpha}^{\infty} \frac{\chi_{q/p^\alpha}(p)^\nu}{p^{\nu s}}.$$

Since $|\chi_{q/p^\alpha}(p)| = 1$, the series on the right is geometric and so

$$\begin{aligned} E_p(s,\chi) &= \sum_{\nu=0}^{\alpha-1} \frac{\chi_{q/p^\alpha}(p)^\nu \chi_{p^\alpha}(p^\nu)}{p^{\nu s}} + \frac{\chi_{q/p^\alpha}(p)^\alpha \chi_{p^\alpha}(p^\alpha)}{p^{\alpha s}} \left(1 - \frac{\chi_{q/p^\alpha}(p)}{p^s}\right)^{-1} \\ &= \left(1 - \frac{\chi_{q/p^\alpha}(p)}{p^s}\right)^{-1} \left(1 + \sum_{\nu=1}^{\alpha} \frac{\chi_{q/p^\alpha}(p)^\nu \left(\chi_{p^\alpha}(p^\nu) - \chi_{p^\alpha}(p^{\nu-1})\right)}{p^{\nu s}}\right). \end{aligned}$$

Since $\chi_{q/p^\alpha}(p) = \psi(p)$, definition (27) shows that the conclusion holds in this case as well. □

Lemma 4.3. *Let $p \mid q$. If $p^\alpha \parallel q$ and $p^\gamma \parallel d$ then for $0 < \mathrm{Re}(s) < 1$*

$$\frac{E_p(1-s,\overline{\chi})}{E_p(1-s,\overline{\psi})} = \overline{\chi}_{q/p^\alpha}(p)^{\alpha-\gamma} p^{(\alpha-\gamma)\left(s-\frac{1}{2}\right)} \left(\frac{\overline{x_{\alpha-\gamma}^{\chi_{p^\alpha}}}}{x_0^{\chi_{p^\alpha}}}\right) \frac{E_p(s,\chi)}{E_p(s,\psi)}.$$

Proof. This is a consequence of Lemma 4.2, the second part of Proposition 3.11 and the fact that $x_\nu^{\overline{\chi_{p^\alpha}}} = \overline{x_\nu^{\chi_{p^\alpha}}}$. □

We remark that although Corollary 3.20 shows that we may construct $\mathfrak{C}$ so that it is closed under complex conjugation, this hypothesis is not necessary in Lemma 4.3. That is, whether or not $\overline{\chi} \in \mathfrak{C}_{\overline{\psi}}$, $\overline{\chi}$ provides an extension of $\overline{\psi}$ and the lemma holds.

Proof of Theorem 1.4. The completed L-functions of χ and ψ related through the equation

$$\Lambda(s,\chi) = \left(\frac{q}{d}\right)^{\frac{s}{2}} \left(\prod_{p|q} \frac{E_p(s,\chi)}{E_p(s,\psi)}\right) \Lambda(s,\psi).$$

Applying the functional equation for $\Lambda(s,\psi)$ and Lemma 4.3 this yields

$$\Lambda(1-s,\overline{\chi}) = \frac{i^a d^{1/2}}{\mathcal{G}_d(\psi,1)} \left(\prod_{p|q} \overline{\chi_{q/p^\alpha}}(p)^{\alpha-\gamma} \left(\frac{\overline{x_{\alpha-\gamma}^{\chi_{p^\alpha}}}}{x_0^{\chi_{p^\alpha}}}\right)\right) \Lambda(s,\chi),$$

where for each $p \mid q$ we assume that $p^\alpha \parallel q$ and $p^\gamma \parallel d$. Equation (11) and Lemma 4.1 give

$$\begin{aligned} \frac{d^{1/2}}{\mathcal{G}_d(\psi,1)} &= \frac{q}{d^{1/2}\mathcal{G}_q(\chi,1)} \overline{\left(\frac{\mathcal{G}_d(\psi,1)}{\mathcal{G}_q(\chi,1)}\right)} \\ &= \frac{q}{d^{1/2}\mathcal{G}_q(\chi,1)} \overline{\prod_{p|q} \frac{\psi_{p^\gamma}(d/p^\gamma)\mathcal{G}_{p^\gamma}(\psi_{p^\gamma},1)}{\chi_{p^\alpha}(q/p^\alpha)\mathcal{G}_{p^\alpha}(\chi_{p^\alpha},1)}}. \end{aligned}$$

Definition (27) and Lemma 3.12 imply that the product on the right is equal to

$$\left(\frac{d}{q}\right)^{\frac{1}{2}} \prod_{p|q} \frac{\psi_{p^\gamma}(d/p^\gamma)\chi_{q/p^\alpha}(p)^{\alpha-\gamma}}{\chi_{p^\alpha}(q/p^\alpha)}$$

which proves the functional equation up to the factor

$$\prod_{p|q} \frac{\psi_{p^\gamma}(d/p^\gamma)\chi_{q/p^\alpha}(p)^{\alpha-\gamma}}{\chi_{p^\alpha}(q/p^\alpha)} = \prod_{p|q} \frac{\psi_{p^\gamma}(d/p^\gamma)\chi_{q/p^\alpha}(p^\alpha)}{\psi_{d/p^\gamma}(p^\gamma)\chi_{p^\alpha}(q/p^\alpha)}.$$

Lemma 4.1 can be used to show that this product is exactly 1, finishing the proof. □

5. Concluding Remarks

There are many natural questions about this work which remain to be addressed. We will end by mentioning some of them.

5.1. *Characters on more general rings*

One may replace $\mathbb{Z}$ with any ring R with the property that, for each ideal $I \subseteq R$, the quotient ring R/I is finite. The notion of primitivity of multiplicative characters is also present in this context, and it would be natural to extend our ideas to this more general setting.

5.2. *Higher rank groups*

The present paper was initially motivated by the following question: When should an irreducible representation

$$\pi : \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{C})$$

be regarded as "primitive"? A study of Gauss sums attached to such π (with $\mathbb{Z}/q\mathbb{Z}$ replaced by a finite field) has been carried out in [5] (see also [6]), but its connection with primitivity does not seem to have been addressed in the literature.

More generally, one may replace GL_2 with any group scheme $\mathcal{G}$, and ask for the appropriate definition of primitivity of π. In these contexts, analogues of Theorems 1.1 and 1.2 should also hold, and we plan to explore this in future work.

5.3. *L-functions attached to extensions χ*

The L-functions $L(s, \chi)$ attached to our extensions χ do not in general belong to the Selberg class, but it appears that, for some choices of parameters, they *do* continue to satisfy the Generalized Riemann Hypothesis. In addition to (5)–(7), one might impose additional hypotheses on the extensions χ (for instance that $L(s, \chi)$ satisfy GRH, have only simple zeroes, and/or possess appropriate p-adic interpolation properties), in hopes of arriving at a *unique* set $\mathfrak{C}$ of extensions.

5.4. *Averages over $\chi \in \mathfrak{C}$*

It appears that the families $\mathfrak{F}_q$ of sets $\mathfrak{C}$ of extensions may shed some light on certain Euler factors appearing in previous work. For example, fix a quadratic number field

K and an order $\mathcal{O} \subseteq \mathcal{O}_K$ of conductor f. The zeta function $\zeta_{\mathcal{O}}(s)$ attached to the order $\mathcal{O}$ is defined by

$$\zeta_{\mathcal{O}}(s) := \sum_{\mathfrak{A} \subseteq \mathcal{O}} \frac{1}{N(\mathfrak{A})^s},$$

where the sum is over all *proper* ideals of $\mathcal{O}$. As shown in [8], there is a factorization

$$\zeta_{\mathcal{O}}(s) = \zeta_K(s) \cdot \prod_{p|f} \varepsilon_{f,p}(s), \tag{51}$$

where $\zeta_K(s)$ is the Dedekind zeta function attached to K and $\varepsilon_{f,p}$ is a polynomial in p^{-s} and $\chi_K(p)$. The local factors $\varepsilon_{f,p}(s)$ are shown in [4] to satisfy a Riemann Hypothesis, and they seem to be connected to our family $\mathfrak{F}_q$. Indeed, consider the factorization

$$\zeta_K(s) = \zeta(s) \cdot L(s, \chi_K) = L(s, \chi_0) \cdot L(s, \chi_K)$$

of $\zeta_K(s)$ (where χ_K is the Kronecker symbol attached to K), and view the Riemann zeta function $\zeta(s)$ as the L-function attached to the trivial character χ_0. For simplicity, assume that f is coprime with the conductor n_K of K. If one extends the characters χ_0 and χ_K to level $f \cdot n_K$, using characters from sets $\mathfrak{C}$ from Theorem 1.1, and averages appropriately over $\mathfrak{F}_q$, then in certain cases one recovers the factorization on the right-hand side of (51). We will continue to explore this connection in future work.

Acknowledgments

This work was partially supported by a Ralphe E. Powe Junior Faculty Enhancement award and also by NSA grant H98230-12-1-0210. The second author gratefully acknowledges Oak Ridge Associated Universities and the National Security Agency for their support.

References

[1] D. Bump, *Automorphic Forms and Representations* (Cambridge University Press, 1998).

[2] G. Chinta and O. Offen, Orthogonal period of a $\mathrm{GL}_3(\mathbb{Z})$ Eisenstein series, in *Representation Theory, Complex Analysis and Integral Geometry*, eds. Krötz, O. Offen and E. Sayag, Progress in Mathematics, Vol. 601 (Birkhäuser, 2012), pp. 41–59.

[3] J. P. G. L. Dirichlet, Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält, *Abhand. Ak. Wiss. Berlin* **48** (1837) 45–81.

[4] M. Kaneko, On the local factor of the zeta function of quadratic orders, in *Zeta Functions, Topology and Quantum Physics*, Development in Mathematics, Vol. 14 (Springer, 2005), pp. 75–79.

[5] T. Kondo, On Gaussian sums attached to the general linear groups over finite fields, *J. Math. Soc. Japan* **15**(3) (1963) 244–255.

[6] E. Lamprecht, Struktur und Relationen allgemeiner Gausscher Summen in endlichen Ringen I, II, *J. Reine Angew. Math.* **197** (1957) 1–48.

[7] K. Soundararajan and M. Young, The prime geodesic theorem, *J. Reine Angew. Math.* **676** (2013) 105–120.

[8] D. Zagier, Modular forms whose Fourier coefficients involve zeta functions of quadratic fields, in *Modular Functions of One Variable VI*, Lecture Notes in Mathematics, No. 627 (Springer-Verlag, 1977), pp. 105–169.