ADVANCES IN APPLIED MATHEMATICS 5, 56–86 (1984)

The Construction of Orthonormal Bases Diagonalizing the Discrete Fourier Transform

R. TOLIMIERI

Department of Mathematics, The University of Connecticut, Storrs, Connecticut 06268

I. INTRODUCTION

The discrete Fourier transform is an important tool both in number theory and discrete signal processing. Although it can be introduced in several equivalent ways, depending upon the tradition of the field of study, we find it most convenient to regard it as an object of finite abelian group harmonic analysis. The discrete Fourier transform $F(m)$ on m points will be given as a unitary operator on $L^2(Z/m)$. Let Z/m denote the integers mod m, and let $L^2(Z/m)$ be the space of complex-valued functions on the abelian group, Z/m. In Section II, exact definitions can be found.

A classical number theory problem, related to quadratic reciprocity and first considered by Gauss, is the evaluation of the trace of $F(m)$ and more generally, the description of the eigen-values and eigen-vectors of $F(m)$. For a partial history of this problem see [1].

A primary concern of digital signal processing centers around computation issues, the fast Fourier transform algorithms, beginning with [6] and the more recent Winograd–Fourier transform algorithms [9]. However, as was seen in [1] and [3], certain applied results can be developed from an abstract harmonic analysis point of view. Recent work by L. Auslander, E. Feig, and S. Winograd has extended the applicability of abstract techniques to both the understanding of old and the development of new tools for computing with the discrete Fourier transform.

This work addresses itself to the problem of constructing an orthonormal basis of eigen-vectors for $F(m)$. This problem has previously been considered in [10] and in the recent work of Dickinson and Steiglitz [7]. In the latter, applications of such a basis to signal processing are discussed.

The method of attack proposed in this work is theoretical and has a number-theoretic flavor. Indeed, we will use the multiplicative characters mod m to generate eigen-vectors. (For the long history of this theory, which

0196-8858/84 $7.50

touches upon Dirichlet L-series and cyclotomic field theory, the reader should consult [5]). To complete the picture, Fortran programs for implementing the results of this paper have been written and can be found in [2].

II. Character Theory

Denote by $\mathbb{C}^x$ the multiplicative group of nonzero complex numbers, and by U_m the subgroup of $\mathbb{C}^x$ consisting of all mth roots of unity. A *character* of a finite abelian group A is a mapping χ of A into $\mathbb{C}^x$ satisfying

$$\chi(a+b) = \chi(a)\chi(b), \qquad a, b \in A.$$

If $m = 0(A)$, the order of A, then $\chi(A) \subset U_m$ for every character χ of A.

For characters χ, χ' of A, the mapping $\chi\chi'$ of A given by

$$\chi\chi''(a) = \chi(a)\chi'(a), \qquad a \in A,$$

and the mapping χ^{-1} of A given by

$$\chi^{-1}(a) = \chi(a)^{-1} = \overline{\chi(a)}, \qquad a \in A$$

are again characters of A. The set of all characters of A, under these operations, forms a group, denoted by $\mathrm{ch}(A)$. The identity element of this group is the trivial character χ_0 defined by $\chi_0(a) = 1$, for all $a \in A$. We call $\mathrm{ch}(A)$ the *dual* of A.

There are several elementary results from general character theory which will be required. Suppose $A = A_1 \oplus A_2$, the direct sum of abelian groups A_1, A_2. Then,

$$\mathrm{ch}(A) \cong \mathrm{ch}(A_1) \cdot \mathrm{ch}(A_2), \tag{2.1}$$

where the isomorphism is constructed as follows. Every $a \in A$ can be written uniquely $a = (a_1, a_2)$, where $a_1 \in A_1$, $a_2 \in A_2$. Taking characters $\chi_1 \in \mathrm{ch}(A_1)$, $\chi_2 \in \mathrm{ch}(A_2)$ the mapping

$$\chi(a) = \chi_1(a_1)\chi_2(a_2), \qquad a = (a_1, a_2) \in A,$$

is a character of A, and we can write $\chi = (\chi_1, \chi_2)$, which defines the isomorphism (2.1).

This result can be extended to any number of factors. Since any finite abelian group A can be written as the direct sum of finite cyclic groups, $A = \oplus_{j=1}^{l} C_j$, it follows that $\mathrm{ch}(A) = \prod_{j=1}^{l} \mathrm{ch}(C_j)$.

The character group of a finite cyclic group C is simple to determine. Suppose $m = 0(C)$ and g generates C. Every character χ of C is completely

determined by its value $\chi(g)$ at g. Since $\chi(g) \in U_m$, we can describe the m distinct characters of C as follows:

$$\chi_j(g) = e^{2\pi ij/m}, \qquad 0 \le j < m.$$

The mapping $jg \to \chi_j$ establishes an isomorphism between C and $\mathrm{ch}(C)$.

In general, for any finite abelian group A,

$$A \cong \mathrm{ch}(A). \tag{2.2}$$

The following two formulas will be needed and will be asserted without proof.

Consider a finite abelian group A of order h. Denote the identity element of A by 0 and the identity element of $\mathrm{ch}(A)$ by χ_0.

For any character χ of A,

$$\sum_{a \in A} \chi(a) = \begin{cases} h, & \chi = \chi_0 \\ 0, & \text{otherwise.} \end{cases} \tag{2.3}$$

For any $a \in A$,

$$\sum_{x \in \mathrm{ch}(A)} \chi(a) = \begin{cases} h, & a = 0 \\ 0, & \text{otherwise.} \end{cases} \tag{2.4}$$

For any positive integer m, denote the ring of integers mod m by $Z(m)$ and its multiplicative group of units by $U(m)$. Suppose

$$m = \prod_{j=0}^{l} p_j^{a_j}$$

is the prime decomposition of m into distinct primes p_j, $0 \le j \le l$, where we reserve p_0 for the even prime 2, whenever it occurs.

By the Chinese remainder theorem, we have the short exact sequence of rings

$$0 \to mZ \to Z \to \bigoplus_{j=0}^{l} Z\left(p_j^{a_j}\right) \to 0,$$

which leads to the isomorphism theorems

$$Z(m) \cong \bigoplus_{j=0}^{l} Z\left(p_j^{a_j}\right) \cong \prod_{j=0}^{l} \mathrm{ch}\left(Z\left(p_j^{a_j}\right)\right) \cong \mathrm{ch}(Z(m)) \tag{2.5}$$

$$U(m) \cong \prod_{j=0}^{l} U\left(p_j^{a_j}\right) \cong \prod_{j=0}^{l} \mathrm{ch}\left(U\left(p_j^{a_j}\right)\right) \cong \mathrm{ch}(U(m)). \tag{2.6}$$

The characters on $Z(m)$ will be called additive characters mod m. Since $Z(m)$ is a cyclic group of order m generated by 1, $\mathrm{ch}(Z(m))$ is the cyclic group generated, for instance, by the additive character Ψ defined by

$$\Psi(1) = e^{2\pi i(1/m)}.$$

In general, $U(m)$ is not a cyclic group. However, if p is an odd prime, $U(p^a)$ is a cyclic group of order $\phi(p^a) = p^{a-1}(p-1)$. $U(2)$ and $U(4)$ are also cyclic groups, but $U(2^a)$, $a \geq 3$, is not cyclic, being the direct product of a group of order 2 and a cyclic group of order 2^{a-2}. The characters on $U(m)$ will be called multiplicative characters mod m.

For an odd prime p, the discussion preceding (1.2) implies that $\mathrm{ch}(U(p^a))$ is the cyclic group of order $\phi(p^a)$ generated by the multiplicative character mod p^a, χ, given by

$$\chi(\alpha) = e^{2\pi i(1/\phi(p^a))},$$

where α is a generator of $U(p^a)$.

Denote the set of all complex functions on a set S by $L(S)$. A function $f \in L(Z)$ is said to have an integer m as a period if

$$f(x+m) = f(x)$$

for all $x \in Z$. Let $L(m)$ denote the space of all functions on Z having m as a period. The set of all periods of a function f will be denoted by $\mathrm{per}(f)$. It is clearly a subgroup of Z, and hence we can write

$$\mathrm{per}(f) = m(f) \cdot Z,$$

where $m(f)$ is the smallest positive period of f, when $\mathrm{per}(f)$ is not the empty set.

Let $K(m)$ be the multiplicative subset of Z consisting of all $u \in Z$ such that (u, m), the greatest common divisor of u and m, equals one. Observe that

$$K(m) + m = K(m),$$

and we can generalize the notion of periodicity to functions on $K(m)$, as follows. Take $f \in L(K(m))$. Then, f has m as a period if

$$f(u+m) = f(u), \qquad u \in K(m)$$

We will denote the space of all functions $f \in L(K(m))$ having m as a period by $L(K(m), m)$.

Denote by p_m the natural mapping of Z onto $Z(m)$ and write $p_m(u) = u \bmod m$. Take $f \in L(Z(m))$. The function $f \cdot p_m \in L(Z)$ has m as a

period and thus lies in $L(m)$. Indeed, the mapping

$$f \to f \cdot p_m$$

induces an isomorphism from $L(Z(m))$ onto $L(m)$. In all that follows we will identify $L(Z(m))$ and $L(m)$, in this way, and write $f \cdot p_m$ simply as f. In particular,

$$\mathrm{ch}(Z(m)) \subset L(m).$$

The restriction of p_m to $K(m)$ maps $K(m)$ onto $U(m)$ and p_m is multiplicative. Thus, arguing as above, we can identify $L(U(m))$ and $L(K(m), m)$. In particular

$$\mathrm{ch}(U(m)) \subset L(K(m), m).$$

Moreover, if $\chi \in \mathrm{ch}(U(m))$ is viewed as a function in $L(K(m), m)$, it satisfies the multiplicative condition

$$\chi(uv) = \chi(u)\chi(v), \qquad u, v \in K(m).$$

Indeed, $\mathrm{ch}(U(m))$ can be identified as the set of all functions on $L(K(m), m)$ satisfying this multiplicative property.

Finally, each $f \in L(K(m), m)$ can be extended to a function on Z, again denoted by f, by setting f equal to 0 outside of $K(m)$. Thus,

$$\mathrm{ch}(U(m)) \subset L(m),$$

and $\mathrm{ch}(U(m))$ can be identified as the subset of all $\chi \in L(m)$ vanishing off of $K(m)$ and satisfying the multiplicative condition on $K(m)$. For the remainder of this section, we take m to be a power of a prime p. In Appendix A, the extension to arbitrary m will be considered.

Let p be prime and consider

$$L(p^c) \subset L(p^a), \qquad c \leq a.$$

Clearly,

$$\mathrm{ch}(Z(p^c)) \subset \mathrm{ch}(Z(p^a)), \qquad c \leq a.$$

The characterization of $\mathrm{ch}(U(m))$ as a subset of $L(m)$, along with the observation that $K(p) = K(p^a)$, $a \geq 1$, implies

$$\mathrm{ch}(U(p^c)) \subset \mathrm{ch}(U(p^a)), \qquad c \leq a.$$

The inclusion can also be defined as follows. The natural mapping of $Z(p^a)$ onto $Z(p^c)$, $c \leq a$, induces a short exact sequence

$$1 \to K_0 \to U(p^a) \to U(p^c) \to 1,$$

where

$$K_0 = \{u \bmod p^a : u = 1 \bmod p^c\}.$$

For each $\chi \in \mathrm{ch}(U(p^c))$, $\chi \cdot \eta$, where η is the restriction of the natural mapping to $U(p^a)$, is a multiplicative character mod p^a. The mapping $\chi \to \chi \cdot \eta$, determines the inclusion above.

A p-primary character is a function $\chi \in L(Z)$ which, under the above identifications, is a multiplicative character mod p^a, for some $a \geq 1$. A p-primary character χ is said to be definable mod p^c if $\chi \in \mathrm{ch}(U(p^c))$, and is said to be primitive mod p^b if $m(\chi)$, the minimal period of χ, is p^b. If χ is primitive mod p^b, then χ is definable mod p^c for all $c \geq b$.

Let U_m be the mth roots of unity. Then, if χ is primitive mod p^b, χ defines, considered as an element in $U(p^c)$, $c \geq b$, a homomorphism of $U(p^c)$ onto U_m, $m = \phi(p^b)$. It is easy to see that a $\chi \in \mathrm{ch}(U(p^a))$ is definable mod p^c if and only if it factors through $U(p^c))$, in the sense of the commutative diagram

$$\begin{array}{ccc} U(p^a) & \xrightarrow[\eta]{} & U(p^c) \\ & \searrow^{\chi} & \downarrow \\ & & U_m \end{array} \quad , \qquad m = \phi(p^a).$$

Equivalently, χ is definable mod p^c if and only if

$$\chi(u) = 1, \qquad \text{for all} \quad u \equiv 1 \bmod p^c.$$

Suppose p is an odd prime and α generates $U(p^b)$. Then, we can write the multiplicative characters mod p^b as follows. For $0 \leq j < \phi(p^b)$, define

$$\chi_j(\alpha) = \exp\left(2\pi i \frac{j}{m}\right), \qquad m = \phi(p^b),$$

and extend x_j to a multiplicative character mod p^b. If χ_j is definable mod p^c, $c \leq b$, then χ_j maps $U(p^b)$ into U_m, $m = \phi(p^c)$ and it follows that p^{b-c} divides j. Thus, χ_j is primitive mod p^b if $(j, p) = 1$. There are $p^{b-2}(p-1)^2$ primitive characters mod p^b, since

$$p^{b-2}(p-1)^2 = 0(U(p^b)) - 0(U(p^{b-1})),$$

where $0(\ )$ denotes the number of elements of the set inside the brackets. The number of j's satisfying $0 \leq j < \phi(p^b)$ and $(j, p) = 1$ is also $p^{b-2}(p-1)^2$. It follows that

$$x_j \text{ is a primitive character mod } p^b \text{ if and only if } (p, j) = 1. \qquad (2.7)$$

From (2.7), we have that χ is primitive mod p^b if and only if χ maps $U(p^b)$ isomorphically onto $U_{\phi(p^b)}$. Other consequences are that

$$\chi_j \text{ is definable mod } p^c \text{ if and only if } p^{b-c} \text{ divides } j, \text{ and } \chi_j \text{ is primitive mod } p^c \text{ if and only if } (p^b, j) = p^{b-c}. \tag{2.8}$$

A multiplicative character mod p^b, χ, will be called real if it takes on only real values. This is the case when $\chi(\alpha) = \pm 1$. It follows that, except for the trivial character χ_0, there is a unique real multiplicative character mod p; namely $\chi_{(p-1)/2}$. The character $\chi_{(p-1)/2}$ is called the Legendre symbol mod p. For $b > 1$, the primitive characters mod p^b can never be real.

Suppose now $p = 2$. For $b \geq 3$, $U(2^b)$ is not cyclic. The elements of $U(2^b)$ can be written uniquely as

$$(-1)^r 5^s \bmod 2^b,$$

where $r = 0, 1$ and $0 \leq s < 2^{b-2}$. Hence $U(2^b)$ is the direct product of a cyclic group of order 2 and a cyclic group of order 2^{b-2}.

Let χ_+, χ_- be the characters on the subgroup $\{\pm 1\}$ of $U(2^b)$ defined by $\chi_+(-1) = 1, \chi_-(-1) = -1$. On the subgroup $\{5^s: 0 \leq s < 2^{b-2}\}$ of $U(2^b)$, the characters can be given according to the following scheme. For $0 \leq j < 2^{b-2}$, set

$$\chi_j(5) = \exp\left(2\pi i \frac{j}{2^{b-2}}\right).$$

The multiplicative characters mod 2^b can now be given by the functions $\chi_+\chi_j$, $\chi_-\chi_j$, $0 \leq j < 2^{b-2}$, where

$$\chi_+\chi_j((-1)^r 5^s) = \chi_j(5^s)$$
$$\chi_-\chi_j((-1)^r 5^s) = \chi_-(-1)^r \chi_j(5)^s.$$

Arguing as above, the primitive characters mod p^b are given by $\chi_+\chi_j$, $\chi_-\chi_j$, where $0 \leq j \leq 2^{b-2}$ and j is odd.

Every multiplicative character mod $U(2^b)$ is real for $b = 0, 1, 2, 3$. For $b \geq 4$, there are no real primitive characters mod 2^b.

Let p be any prime and $\Psi(p^b)$ the set of primitive characters mod p^b. The following result, while obvious, will have important consequences in the next section.

LEMMA 2.1. *For $a \geq 2$,*

$$\mathrm{ch}(U(p^a)) = \mathrm{ch}(U(p)) \cup \Psi(p^2) \cup \cdots \cup \Psi(p^a),$$

where the factors of the union are pairwise disjoint.

If χ is a multiplicative character mod p^a, then $\bar{\chi}$ is again a multiplicative character mod p^a. In particular, the set $\Psi(p^b)$ of primitive characters mod p^b is mapped bijectively onto itself by the taking of conjugates. Thus, if p is an odd prime then we can write

$$\Psi(p^b) = \Psi_0(p^b) \cup \overline{\Psi_0(p^b)},$$

where $\Psi_0(p^b) \cap \overline{\Psi_0(p^b)}$ is empty if $b \geq 2$ and

$$\Psi_0(p) \cap \overline{\Psi_0(p)} = \{\text{real primitive character mod } p\}.$$

For $p = 2$, and $b \geq 4$, we have the decomposition

$$\Psi(2^b) = \Psi_0(2^b) \cup \overline{\Psi_0(2^b)},$$

where the factors of the union are disjoint. The sets $\Psi_0(p^b)$, $\Psi_0(2^b)$ are not uniquely determined, but, in all that follows, we will assume that some fixed choice has been made. In Appendix A, we will consider in detail the analysis of the case $b = 3$.

III. The Discrete Fourier Transform

Denote by $L^2(m)$ the space $L(m)$ along with the inner product defined by

$$\langle f, g \rangle = \sum_{u=0}^{m-1} f(u)\bar{g}(u), \qquad f, g \in L(m).$$

Consider the basis e_j, $0 \leq j < m$, of $L^2(m)$ given by

$$e_j(u) = \begin{cases} 1, & u \equiv j \bmod m \\ 0, & \text{otherwise} \end{cases}, \qquad u \in Z,$$

and the basis Ψ_j, $0 \leq j < m$, of $L^2(m)$ given by

$$\Psi_j(u) = e^{2\pi i(uj/m)}, \qquad u \in Z.$$

It is easy to see that e_j, $0 \leq j < m$ is an orthonormal basis and Ψ_j, $0 \leq j < m$ is an orthogonal basis, where

$$\langle \Psi_j, \Psi_k \rangle = \begin{cases} m, & j = k \\ 0, & \text{otherwise} \end{cases}, \qquad 0 \leq j, \quad k < m. \tag{3.1}$$

Moreover,

$$\langle e_j, \Psi_k \rangle = \exp\left(-2\pi i\left(\frac{kj}{m}\right)\right), \qquad 0 \leq j, \quad k < m. \tag{3.2}$$

The discrete Fourier transform of $L^2(m)$ is the linear mapping $\mathrm{F}(m)$ of $L^2(m)$ satisfying

$$\mathrm{F}(m)e_j = m^{-1/2}\Psi_j, \qquad 0 \le j < m. \tag{3.3}$$

Because of (3.1), $\mathrm{F}(m)$ is a unitary operator and by (3.3), we have

$$\mathrm{F}(m)f = m^{-1/2} \sum_{0 \le v < m} f(v)\Psi_v \tag{3.4}$$

for any function $f \in L^2(m)$. It follows from (3.2) that the matrix of $\mathrm{F}(m)$ relative to the basis e_j, $0 \le j < m$, is given by

$$m^{-1/2}[w^{jk}]_{0 \le j,k < m}, \tag{3.5}$$

where $w = \exp(2\pi i(jk/m))$.

There are several important, although easy to prove, properties of $\mathrm{F}(m)$ which we will list below for future reference.

$$\mathrm{F}(m)\Psi_j = m^{1/2}e_{m-j} \tag{3.6}$$

$$\mathrm{F}(m)^2 e_j = e_{m-j} \tag{3.7}$$

$$\mathrm{F}(m)^4 = I, \qquad \text{the identity mapping on } L^2(m) \tag{3.8}$$

$$\mathrm{F}(m)^{-1}e_j = m^{-1/2}\Psi_{m-j} \tag{3.9}$$

$$\mathrm{F}(m)^{-1}f = m^{-1/2} \sum_{0 \le v < m} f(v)\Psi_{m-v}. \tag{3.10}$$

The analysis of $\mathrm{F}(m)$ lies at the heart of several important problems in both number theory and digital signal processing. Following Gauss, for $x \in \mathrm{ch}(U(m))$, set

$$G_m(\chi, u) = \sum_{0 \le v < m} \chi(v)\Psi_v(u) = m^{1/2}(\mathrm{F}(m)\chi)(u).$$

We call $G_m(\chi, u)$ the Gauss sum of χ at u, and

$$G_m(\chi) = G_m(\chi, 1)$$

the Gauss sum of χ. Classically, such sums were introduced by Gauss to study reciprocity laws, and were further studied by Kronecker and Dirichlet, especially in connection with Dirichlet L-series and cyclotomic fields. For an account of recent activity in this direction see [5].

We will see how the theory of multiplicative characters mod m provides an orthonormal basis of $L^2(m)$ relative to which $\mathrm{F}(m)$ is diagonal.

Let p be a prime.

LEMMA 3.1. *For* $\chi \in \mathrm{ch}(U(p^a))$,

$$\mathrm{F}^2(p^a)\chi = \chi(-1)\chi.$$

Proof. By (3.7), $(\mathrm{F}^2(p^a)\chi)(u) = \chi(-u) = \chi(-1)\chi(u)$ from the multiplicativity of χ, and the lemma follows.

This simple observation lies at the heart of our analysis of $\mathrm{F}(p^a)$. Suppose $\chi \in U(p^a)$, and $V(\chi)$ is the subspace of $L^2(p^a)$ spanned by χ and $\mathrm{F}(p^a)\chi$. By Lemma 3.1, $V(\chi)$ is invariant under the action of $\mathrm{F}(p^a)$. If $\dim V(\chi) = 1$, then χ is an eigen-vector for $\mathrm{F}(p^a)$. Otherwise, $\dim V(\chi) = 2$, and relative to the basis $\chi, \mathrm{F}(p^a)\chi$, the matrix of the restriction $\mathrm{F}(p^a)$ to $V(\chi)$ has the form

$$\begin{bmatrix} 0 & \chi(-1) \\ 1 & 0 \end{bmatrix}. \tag{3.11}$$

When $\chi(-1) = 1$, then

$$\chi + \mathrm{F}(p^a)\chi, \qquad \chi - \mathrm{F}(p^a)\chi \tag{3.12}$$

is a diagonalizing basis for the restriction of $\mathrm{F}(p^a)$ to $V(\chi)$, the eigenvalues being $+1, -1$, respectively. If $\chi(-1) = -1$, then

$$\chi + i\mathrm{F}(p^a)\chi, \qquad \chi - i\mathrm{F}(p)\chi, \tag{3.13}$$

is a diagonalizing basis, the eigenvalues being $+i, -i$, respectively.

Supposing, further, that χ and $\mathrm{F}(p^a)\chi$ are orthogonal, then the vectors (3.12) and the vectors (3.13) are orthogonal. Also, their norms are all $\sqrt{2}\sqrt{\phi(p^a)}$.

The prime p will be taken *odd* in the following discussion. The even prime 2 case will be considered in Appendix A. As a subset of $L^2(p)$, (2.3) implies that $\mathrm{ch}(U(p))$ is orthogonal. Each function in $\mathrm{ch}(U(p))$ vanishes at $u = 0 \bmod p$. It follows that the set

$$\{e_0\} \cup \mathrm{ch}(U(p)) \tag{3.14}$$

is an orthogonal basis of $L^2(p)$. If $\chi \in \mathrm{ch}(U(p))$ $\chi \neq \chi_0$, χ_0 the trivial character, then

$$(\mathrm{F}(p)\chi)(0) = p^{-1/2} \sum_{0 \le v < p} \chi(v) = 0.$$

For $u \not\equiv 0 \bmod p$, choose u^{-1} such that $uu^{-1} \equiv 1 \bmod p$.

Consider

$$(\mathrm{F}(p)\chi)(u) = p^{-1/2} \sum_{0 \le v < p} \chi(v)\psi_v(u).$$

We can replace v by $u^{-1}v$ and write

$$\begin{aligned}(\mathrm{F}(p)\chi)(u) &= p^{-1/2} \sum_{0 \le v < p} \chi(u^{-1}v)\psi_u - 1_v(u) \\ &= p^{-1/2} \sum_{0 \le v < p} \chi(u^{-1})\chi(v)\psi_v(1) \\ &= p^{-1}G_p(\chi)\bar{\chi}(u).\end{aligned}$$

The following lemma has been proved.

LEMMA 3.2. *For* $\chi \in \mathrm{ch}(U(p))$, $\chi \neq \chi_0$

$$\mathrm{F}(p)\chi = p^{-1/2}G_p(\chi)\bar{\chi}.$$

The primitive characters mod p *are simply the nontrivial multiplicative characters* mod p. *Recall* $\Psi_0(p)$ *denotes a set of primitive characters* mod p *such that*

$$\Psi(p) = \Psi_0(p) \cup \bar{\Psi}_0(p),$$

where the Legendre symbol mod p, *denoted by* χ_r, *is the common character to both terms of the union.*

To each $\chi \in \Psi_0(p)$, let $V(\chi)$ denote the subspace spanned by $\chi, \mathrm{F}(p)\chi$. The following is now obvious.

LEMMA 3.3. *For* $\chi \in \Psi_0(p)$,

(i) *If* $\chi = \chi_r$, *then* $V(\chi)$ *is* 1*-dimensional, invariant under the action of* $\mathrm{F}(p)$, *and the matrix of* $\mathrm{F}(p)$, *restricted to* $V(\chi)$, *is given by*

$$p^{-1/2}\left[G_p(\chi_r)\right].$$

(ii) *If* $\chi \neq \chi_r$, *then* $V(\chi)$ *is* 2*-dimensional, invariant under the action of* $\mathrm{F}(p)$, $\chi, \mathrm{F}(p)\chi$ *is an orthogonal basis of* $V(\chi)$, *and the matrix of* $\mathrm{F}(p)|V(\chi)$ *relative to the basis* $\chi, \mathrm{F}(p)\chi$ *is given by*

$$M(\chi) = \begin{bmatrix} 0 & \chi(-1) \\ 1 & 0 \end{bmatrix}.$$

Moreover,

$$V = \oplus \sum V(\chi), \qquad \chi \text{ running over } \Psi_0(p)$$

is an orthogonal direct sum.

It follows that the functions

$$(p-1)^{-1/2}\chi_r; (p-1)^{-1/2}\chi, (p-1)^{-1/2}F(p)\chi, \qquad \chi_r \neq \chi \in \Psi_0(p), \tag{3.15}$$

determine an orthonormal basis for V, and that the matrix of $F(p)|V$ relative to this basis (3.15) is given by

$$M(p) = p^{-1/2}\left[G_p(\chi_r)\right] \oplus \sum M(\chi), \qquad \chi \text{ running over } \Psi_0(p), \chi \neq \chi_0. \tag{3.16}$$

The functions $e_0, (p-1)^{-1/2}\chi_0$ complete (3.15) to an orthonormal basis, denoted by β. Direct evaluation gives the next lemma.

LEMMA 3.4. $F(p)e_0 = p^{-1/2}e_0 + p^{-1/2}(p-1)^{1/2}(p-1)^{-1/2}\chi_0$

$$F(p)\left((p-1)^{-1/2}\chi_0\right) = p^{-1/2}(p-1)^{1/2}e_0 - p^{-1/2}(p-1)^{-1/2}\chi_0.$$

Lemmas 3.4 and 3.5 imply our first main result.

THEOREM 3.5. *The matrix of $F(p)$ relative to the orthonormal basis β is given by*

$$p^{-1/2}\begin{bmatrix} 1 & (p-1)^{1/2} \\ (p-1)^{1/2} & -1 \end{bmatrix} \oplus M(p). \tag{3.17}$$

The problem of finding an orthonormal basis diagonalizing $F(p)$ is equivalent to the finding of unitary matrices X, $X(\chi)$ such that

$$X\begin{bmatrix} 1 & (p-1)^{1/2} \\ (p-1)^{1/2} & -1 \end{bmatrix}X^{-1},$$

and

$$X(\chi)M(\chi)X(\chi)^{-1}, \qquad \chi_r \neq \chi \in \Psi_0(p),$$

are diagonal.

By (3.12) and (3.13) we already have that

$$X(\chi) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \qquad \chi(-1) = 1,$$

$$X(\chi) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}, \qquad \chi(-1) = -1.$$

A straightforward verification shows we can take

$$X = \frac{1}{\sqrt{2}} p^{-1/4} \begin{bmatrix} (p^{1/2}+1)^{1/2} & (p^{1/2}-1)^{1/2} \\ -(p^{1/2}-1)^{1/2} & (p^{1/2}+1)^{1/2} \end{bmatrix}.$$

The case $m = 2$ is described in Appendix A. We will now consider the prime power case. In the following discussion, we take $m = p^a$, p an odd prime and $a \geq 2$. However, everything that is said holds, without change, for the case $m = 2^b$, $b \geq 4$. The cases $m = 2^2$ and $m = 2^3$, described in Appendix A, are special in that all multiplicative characters mod 2^2 and mod 2^3 are real and in particular, this is true for primitive characters mod 2^2 and mod 2^3.

The case $m = p^a$, $a \geq 2$, will now be considered. By Lemma 2.1, we can write

$$\mathrm{ch}(U(p^a)) = \mathrm{ch}(U(p)) \cup \Psi(p^2) \cup \cdots \cup \Psi(p^a). \tag{3.18}$$

We will study the action of $\mathrm{F}(p^a)$ on each of the terms of the union in (3.18). It is convenient to begin with the following definition:

For $c \leq a$ and $f \in L^2(p^c)$, let $\pi_c(f)$ be the function in $L^2(p^a)$ defined by

$$\pi_c(f)(u) = \begin{cases} f(v), & u = vp^{a-c}, 0 \leq v < p^c \\ 0, & \text{otherwise} \end{cases}, \qquad 0 \leq u < p^a. \tag{3.19}$$

The mapping

$$\pi_c : L^2(p^c) \to L^2(p^a), \qquad a > c,$$

is clearly an isometry, and $\pi_a \equiv I$, the identity mapping. Take

$$\chi \in \mathrm{ch}(U(p^c))$$

and consider

$$\pi_c(\chi).$$

By definition $\pi_c(\chi)$ vanishes off of the set $u \equiv vp^{a-c} \bmod p^a$ and $(v, p) = 1$. Thus, if $b < c \leq a$, then

$$\pi_b(\chi_1) \cdot \pi_c(\chi_2) \equiv 0$$

whenever $\chi_1 \in \mathrm{ch}(U(p^b))$ and $\chi_2 \in \mathrm{ch}(U(p^c))$. It follows from this discussion, along with (2.3), that the subset of $L^2(p^a)$,

$$\{e_0, \chi_0, \pi_1(\chi_0)\} \bigcup_{1 \leq c < a} (\Psi(p^c) \cup \pi_c(\Psi(p^c))) \cup \Psi(p^a), \tag{3.20}$$

is orthogonal. The reason for writing (3.20) in this way will soon become apparent.

THEOREM 3.6. *For* $\chi \in \mathrm{ch}(U(p^a))$, *if* χ *is primitive* mod p^c, *then*

$$\mathrm{F}(p^a)\chi = p^{(a-2c)/2} G_m(\chi)\bar{\pi}_c(\chi), \qquad m = p^c, \tag{3.21}$$

where on the right-hand side, we are considering $\chi \in L(p^c)$.

Proof. Consider

$$(\mathrm{F}(p^a)\chi)(u) = p^{-a/2} \sum_{0 \le w < p^a} \chi(w) e^{2\pi i(uw/p^a)}, \qquad 0 \le u < p^a,$$

and write $w = r + sp^c, 0 \le r < p^c, 0 \le s < p^{a-c}$. Since χ is periodic mod p^c, we have

$$\mathrm{F}(p^a)\chi(u) = p^{-a/2} \sum_{0 \le r < p^c} \chi(r) e^{2\pi i(ur/p^a)} \sum_{0 \le s < p^{a-c}} e^{2\pi i(us/p^{a-c})}.$$

For the sum on the right vanishes unless $u = vp^{a-c}$, $0 \le v < p^c$, in which case it equals p^{a-c}.

Suppose $u = vp^{a-c}$, $\quad 0 \le v < p^c$. Then,

$$(\mathrm{F}(p^a)\chi)(vp^{a-c}) = p^{(a-2c)/2} \sum_{0 \le r < p^c} \chi(r) e^{2\pi i(vr/p^c)},$$

and we are left with the need to compute

$$\sum_{0 \le r < p^c} \chi(r) e^{2\pi i(vr/p^c)}, \qquad 0 \le v < p^c,$$

where χ is a primitive character mod p^c. It is well known, and for completeness we will prove below, that this sum equals $G_m(\chi)\bar{\chi}(v)$ from which the theorem follows.

If $(v, p) = 1$, we can argue as in Lemma 3.2 to prove the result for such v's. Assume, now, that $v = v'p$, $0 \le v' < p^{c-1}$. We show that

$$\delta = \sum_{0 \le r < p^c} \chi(r) e^{2\pi i(v'r/p^{c-1})} = 0.$$

Suppose $\delta \ne 0$. We will show that if $\delta \ne 0$ and $w \equiv 1 \bmod p^{c-1}$, then $\chi(w) = 1$. This would imply χ is definable mod p^{c-1}, a contradiction.

Choose w^{-1} so that $w^{-1}w \equiv 1 \bmod p^c$. Then, since χ is multiplicative,

$$\delta = \sum_{0 \le r < p^c} \chi(r) e^{2\pi i (wv'r/p^{c-1})} = \sum_{0 \le r < p^c} \chi(w^{-1}r) e^{2\pi i (v'r/p^{c-1})} = \bar{\chi}(w)\delta.$$

Thus $\chi(w) = 1$, if $\delta \neq 0$. The theorem is proved.

Theorem 3.6 implies that the set of functions

$$\chi, \mathrm{F}(p^a)\chi \tag{3.22}$$

as χ runs, in some order, over the set $\cup_{1<c<a} \Psi_0(p^c) \cup \Psi_0(p^a)$ is an orthogonal basis of a $(p^a - p^{a-2} - 2)$-dimensional subspace in $L(p^a)$. Let $V(\chi)$ be the subspace spanned by $\chi, \mathrm{F}(p^a)\chi$. Summarizing, we have the following.

THEOREM 3.7. *The matrix of* $\mathrm{F}(p^a)|V(\chi)$ *relative to the orthogonal basis* $\chi, \mathrm{F}(p^a)\chi$ *is given by*

$$M(\chi) = \begin{bmatrix} 0 & \chi(-1) \\ 1 & 0 \end{bmatrix}.$$

Moreover,

$$V = \sum \oplus V(\chi), \qquad \chi \text{ as in (3.22)},$$

is an orthogonal direct sum and $\dim V = p^a - p^{a-2} - 2$.

The matrix of $\mathrm{F}(p^a)|V$ relative to the orthonormal basis

$$\phi(p^a)^{-1/2}\chi, \qquad \phi(p^a)^{-1/2}\mathrm{F}(p^a)\chi, \tag{3.23}$$

χ as in (3.22) is given by

$$\oplus \sum_{\chi} M(\chi).$$

The construction of an orthonormal basis of V diagonalizing $\mathrm{F}(p^a)|V$ proceeds exactly as before in the discussion of statements (3.12) and (3.31).

Consider the trivial character χ_0 and $\mathrm{F}(p^a)\chi_0$, and let W be their linear span. The next lemma immediately follows from a direct calculation.

LEMMA 3.8. $\mathrm{F}(p^a)\chi_0 = p^{(a-2)/2}((p-1)e_0 - \pi_1(\chi_0))$.

It follows that the set of functions

$$\phi(p^a)^{-1/2}\chi, \qquad \phi(p^a)^{-1/2}\mathrm{F}(p^a)\chi \tag{3.24}$$

as χ runs, in some order, over the set $\mathrm{ch}(U(p^{a-1})) \cup \Psi_0(p^a)$ is an orthonor-

mal basis of $W \oplus V$ and that relative to the basis, the matrix of $F(p^a)|W \oplus V$ is given by

$$\oplus \sum_{\chi} \begin{bmatrix} 0 & \chi(-1) \\ 1 & 0 \end{bmatrix}, \tag{3.25}$$

χ as in (3.24).

THEOREM 3.9. *Let*

$$v(\chi) = \begin{cases} \frac{1}{\sqrt{2}}\phi(p^a)^{-1/2}(\chi + F(p^a)\chi), & \chi(-1) = 1 \\ \frac{1}{\sqrt{2}}\phi(p^a)^{-1/2}(\chi + iF(p^a)\chi), & \chi(-1) = -1 \end{cases}$$

$$w(\chi) = \begin{cases} \frac{1}{\sqrt{2}}\phi(p^a)^{-1/2}(\chi - F(p^a)\chi), & \chi(-1) = 1 \\ \frac{1}{\sqrt{2}}\phi(p^a)^{-1/2}(\chi - iF(p^a)\chi), & \chi(-1) = -1. \end{cases}$$

Then, the set of functions

$$v(\chi), w(\chi), \tag{3.26}$$

where χ runs as in (3.24), *is an orthonormal basis of $W \oplus V$ diagonalizing the restriction of $F(p^a)$ to $W \oplus V$.*

Observe that $\dim(W \oplus V) = p^a - p^{a-2}$. We still need to complete the basis given either by (3.24) or (3.26) to an orthonormal basis of $L^2(p^a)$. Specifically, we will establish a procedure for doing so. Consider the subsets $E(u)$, $0 \le u < p^{a-2}$ defined by

$$E(u) = \{up + vp^{a-1} : 0 \le v < p\}.$$

Let $f_u \in L(p^a)$ be defined by

$$f_u(w) = \begin{cases} 1, & w \in E(u) \\ 0, & w \notin E(u) \end{cases}, \qquad 0 < w < p^a.$$

The following result is an immediate consequence of this definition.

LEMMA 3.10. *The set of functions*

$$f_u, \qquad 0 \le u < p^{a-2}, \tag{3.27}$$

is an orthogonal subset of $L(p^a)$, and span a p^{a-2} dimensional subspace Y.

Moreover, we have the orthogonal direct sum

$$L^2(p^a) = Y \oplus (W \oplus V).$$

THEOREM 3.11. *Y is invariant under the action of $\mathrm{F}(p^a)$ and relative to the basis* (3.27) *of Y, the matrix of $\mathrm{F}(p^a)|Y$ is given by*

$$p^{-(a-2)/2}\left[e^{2\pi i(uv/p^{a-2})}\right]_{0\le u,v<p^{a-2}}.$$

In other words, $\mathrm{F}(p^a)|Y = \mathrm{F}(p^{a-2})$.

Proof. Take $0 \le u < p^{a-2}$ and $0 \le w < p^a$. Then, by definition,

$$\begin{aligned}\left(\mathrm{F}(p^a)(f_u)(w) &= p^{-a/2} \sum_{0\le w<p} e^{2\pi i((up+vp^{a-1})/p^a)w} \\ &= p^{-a/2} e^{2\pi i(uw/p^{a-1})} \sum_{0\le v<p} e^{2\pi i(vw/p)}.\end{aligned}$$

If $(w, p) = 1$, then the sum on the right vanishes. Suppose $w \in E(r)$ and we write $w = rp + 2p^{a-1}$, $0 \le r < p^{a-2}$, $0 \le s < p$. Then,

$$\left(\mathrm{F}(p^a)f_u\right)(rp + sp^{a-1}) = p^{1-a/2} e^{2\pi i(ur/p^{a-2})},$$

which implies the theorem.

As an example, consider the case $a = 2$. Adjoining p^{-1} times the function $e_0 + \pi_1(\chi_0)$ to be orthonormal set (3.24) gives an orthonormal basis of $L^2(p^2)$ relative to which the matrix of $\mathrm{F}(p^2)$ has the form

$$[1] \oplus \sum_{\chi} M(\chi).$$

Theorem 3.11 sets up a procedure for the complete analysis of $\mathrm{F}(p^a)$. We will describe the underlying algebra in more detail.

If $T \subset S$, then $L(T)$ can be considered as a subspace of $L(S)$ by extending each function on T to all of S, the extension taking the value 0 off of T. In particular,

$$L^2(pZ/p^aZ) \subset L^2(p^a).$$

The natural mapping

$$pZ/p^aZ \to pZ/p^{a-1}Z \cong Z(p^{a-2})$$

induces, by composition, a mapping

$$L^2(p^{a-2}) \to L^2(pZ/p^aZ),$$

and hence, a monomorphism

$$L^2(p^{a-2}) \to L^2(p^a).$$

The image of this last isomorphism, $L^2(p^a)$, is the space Y of Theorem 3.11, which can now be interpreted as the commutativity of the diagram

$$\begin{array}{ccc} L^2(p^{a-2}) & \to & L^2(p^a) \\ \downarrow & & \downarrow \\ L^2(p^{a-2}) & \to & L^2(p^a) \end{array} \qquad \begin{array}{c} \\ \mathrm{F}(p^{a-2}) \\ \\ \end{array} \qquad \begin{array}{c} \\ \mathrm{F}(p^a). \\ \\ \end{array}$$

For odd a, the complete procedure for analysing $\mathrm{F}(p^a)$ can be described by the commuting diagram

$$\begin{array}{ccccccc} L^2(p) & \to & L^2(p^3) & \to & \cdots & \to & L^2(p^a) \\ \downarrow & \mathrm{F}(p) & \downarrow & \mathrm{F}(p^3) & & & \downarrow \quad \mathrm{F}(p^a). \\ L^2(p) & \to & L^2(p^3) & \to & \cdots & \to & L^2(p^a) \end{array}$$

In Appendix C we will explicitly write down the orthonormal matrix diagonalizing $\mathrm{F}(p)$.

Appendix A

In this appendix, we will consider the analysis of $\mathrm{F}(m)$ for those m not covered in Section III.

First let $m = 2^b$. If $b \geq 4$ then, as we have said, the results of Section III hold exactly as given for $m = 2^b$. It remains to consider the cases $m = 2^b$ where $b = 1, 2, 3$.

For $m = 2$, we can take $e_0, e_1 = \chi_0$ as an orthogonal basis of $L^2(2)$, and relative to this basis the matrix of $\mathrm{F}(2)$ is given by

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

This matrix is orthogonal and it is easy to find an orthonormal basis diagonalizing $\mathrm{F}(2)$.

For $m = 4$, $\mathrm{O}(U(4)) = 2$, and the multiplicative characters mod 4 are given by

$$\chi_0(3) = 1,$$
$$\chi_1(3) = -1,$$

where 3 generates $U(4)$. It is easy to see that

$$\mathrm{F}(4)\chi_0 = e_0 - e_2,$$
$$\mathrm{F}(4)\chi_1 = i\chi_1,$$

and that

$$\chi_0, \mathrm{F}(\chi_0), \chi_1, f$$

define an orthogonal basis of $L^2(4)$, where

$$f(u) = \begin{cases} 1, & u \text{ even} \\ 0, & u \text{ odd} \end{cases}$$

and relative to this basis the matrix of F(4) is given by

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \oplus [i] \oplus [1].$$

Again, an orthonormal diagonalizing basis can be easily found.

Suppose, now, $m = 2^3 = 8$. Then, $U(8) = 4$ and the multiplicative character mods are given by

$$\begin{aligned} \chi_0(-1) &= \chi_0(5) = 1 \\ \chi_1(-1) &= 1 = -\chi_1(5) \\ \chi_2(-1) &= -1 = \chi_2(5) \\ \chi_3(-1) &= -1 = -\chi_3(5), \end{aligned}$$

where $-1, 5$ generate $U(8)$. It is easy to see that

$$\begin{aligned} \mathrm{F}(\chi_0) &= \frac{2}{\sqrt{2}}(e_0 - e_4) \\ \mathrm{F}(\chi_1) &= \chi_1 \\ \mathrm{F}(\chi_2) &= i\chi_2 \\ \mathrm{F}(\chi_3) &= \frac{2}{\sqrt{2}}(e_2 - e_6), \end{aligned}$$

and hence the set of vectors

$$\chi_0, \mathrm{F}(\chi_0), \chi_1, \chi_2, \chi_3, \mathrm{F}(\chi_3)$$

are orthogonal. Let $f, g \in L^2(8)$ be defined by

$$f(u) = \begin{cases} 1, & u \text{ even} \\ 0, & \text{odd} \end{cases}$$

$$g(u) = \begin{cases} 1, & u \equiv 0 \bmod 4 \\ 0, & u \text{ odd} \\ -1, & u \equiv 2 \bmod 4 \end{cases}.$$

Then, $\mathrm{F}(8)f = (\sqrt{2}/2)(f + g)$ and $\mathrm{F}(8)g = (\sqrt{2}/2)(f - g)$. The functions

$$\chi_0, \mathrm{F}(\chi_0), \chi_1, \chi_2, \chi_3, \mathrm{F}(\chi_3), f, g$$

determine an orthogonal basis for $L^2(8)$ relative to which the matrix of F(8) is given by

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \oplus [1] \oplus [i] + \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \oplus \frac{\sqrt{2}}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Observe that χ_1, χ_2 are primitive characters mod 8, but since they take on only real values they are eigenvectors and do not determine 2×2 blocks as is the case when $m = p^a$, p odd prime, or $m = 2^b$, $b \geq 4$. Otherwise, this case is similar to the discussion of Section III.

Suppose, now, that

$$m = \prod_{1 \leq j < r} m_j,$$

where $m_j = p_j^{a_j}$, p_j, $1 \leq j < r$, and distinct primes and $a_j > 1$. To analyze F(m) we will use the tensor product. By (2.5),

$$Z(m) \cong \prod_{1 \leq j < r} Z(m_j).$$

Let $f_j \in L^2(m_j)$, $1 \leq j < r$, and define $f \in L^2(m)$ by setting

$$f(u) = \prod_{1 \leq j < r} f_j(u), \qquad u \in Z.$$

The mapping

$$(f_1, \ldots, f_r) \to f$$

is bilinear in each variable, and hence χ extends to a linear homeomorphism

$$f_1 \otimes \otimes f_r \to f$$

of $\otimes_{1 \leq u < r} L^2(m_j)$ into $L^2(m)$. It is easy to show that this mapping is a linear isomorphism, and we have

$$L^2(m) \cong \bigotimes_{1 \leq j < r} L^2(m_j).$$

Set $M_j = m/m_j$, $1 \leq j < r$. Then since the M_j's are pairwise relatively prime there exists integers c_j, $1 \leq j \leq r$ such that

$$\sum_{1 \leq j \leq r} c_j N_j = 1.$$

THEOREM A.1. *For* $f \cong \otimes_j f_j$, $f_j \in L^2(m_j)$, $1 \leq j \leq r$,

$$(f(m)f)(u) = \prod_j \big(F(m_j) f_j\big)(c_j u), \qquad u \in Z.$$

Proof. Observe that as v runs over $Z(m)$, the r-tuple $(v,\dots,v)$ runs over $\prod_j Z(m_j)$, and

$$v = \sum_j v M_j c_j.$$

Thus,

$$\begin{aligned}(\mathrm{F}(m)f)(u) &= m^{-1/2} \sum_{0 \le v < m_j} f_j(v) e^{2\pi i (uv/m)} \\ &= m^{-1/2} \prod_j \sum_{0 \le v < m_j} f_j(v) e^{2\pi i (uvc_j/m_j)} \\ &= \prod_j \big(\mathrm{F}(m_j) f_j\big)(uc_j),\end{aligned}$$

which proves the theorem.

For each j, $1 \le j \le m$, let

$$f_{j,k_j}, \qquad 0 \le k_j < m_j \tag{A.1}$$

denote an orthonormal basis of $L^2(m_j)$ diagonalizing $\mathrm{F}(m_j)$. Set

$$f_{\mathbf{k}} = \bigotimes_j f_{j,k_j}, \qquad \mathbf{k} = (k_1,\dots,k_r).$$

THEOREM A.2. *The set of functions*

$$\left\{ f_{\mathbf{k}}, \mathbf{k} \in \prod_j Z(m_j) \right\}$$

defines an orthonormal basis of $L^2(m)$ diagonalizing $F(m)$.

Proof. It is a standard result that this set of functions forms a basis of $L^2(m)$. Consider $\langle f_{\mathbf{k}}, f_{\mathbf{k}'} \rangle$, which by definition is given by

$$\begin{aligned}\sum_{0 \le u < m} f_{\mathbf{k}}(u) \bar{f}_{\mathbf{k}'}(u) &= \sum_{0 < u < m} \prod_j f_{j,k_j}(u) \bar{f}_{j,k_j'}(u) \\ &= \prod_j \sum_{0 \le u < m_j} f_{j,k_j}(u) \bar{f}_{j,k_j'}(u) \\ &= \prod_j \langle f_{j,k_j}, f_{j,k_j'} \rangle.\end{aligned}$$

This result easily implies that the set of functions $f_{\mathbf{k}}$ is an orthonormal basis. Applying Theorem A.1 gives

$$\mathrm{F}(m) f_{\mathbf{k}} = a f_{\mathbf{k}},$$

where $a = \prod_j a_{j,k_j}$ and $F(m_j)f_{j,k_j} = a_{j,k_j}f_{j,k_j}$. Thus, the $f_{\mathbf{k}}$ are eigenvectors of $F(m)$, and the theorem is proved.

Summarizing, we apply the results of Section III to find orthonormal basis diagonalizing $F(p^a)$, p a prime, and apply Theorem A.2 to extend this result to arbitrary F(m).

We have defined the notion of primitive for p-primary characters only. However (see [4]), this notion can be defined for arbitrary m. We will use the tensor product to do so and indicate how the theory of multiplicative characters mod m could be directly applied to the analysis of $F(m)$.

As asserted in (2.1)

$$\mathrm{ch}(U(m)) \cong \prod_j \mathrm{ch}\big(U(m_j)\big).$$

We will consider this isomorphism in greater detail. Suppose χ is a multiplicative character mod m. Then, we will find $\chi_j \cong \mathrm{ch}(U(m_j))$ such that

$$\chi = \bigotimes_j \chi_j.$$

Take $u \in K(m_j) = \{v \in Z\colon (v, m_j) = 1\}$. The Chinese remainder theorem implies that there exists $u_j \in Z$ such that

$$u_j = \begin{cases} u & \bmod m_j \\ 1 & \bmod m_k, \qquad k \neq j, 1 \leq k \leq r. \end{cases}$$

Then

$$u \equiv \prod_j u_j \bmod m.$$

Define $\chi_j \in \mathrm{ch}(U(m_j))$ by

$$\chi_j(u) = \chi_j(u_j) = \chi(u_j), \qquad 1 \leq j \leq r.$$

It easily follows that

$$\chi(u) = \prod_j \chi_j(u), \qquad u \in K(m),$$

and hence

$$\chi \cong \bigotimes_j \chi_j.$$

A multiplicative character χ mod m will be called primitive if writing $\chi \cong \otimes_j \chi_j$ we have that each χ_j is primitive mod m_j. Applying Theorem A.2 we have the next result.

THEOREM A.3. *Let* $\chi \cong \otimes_j \chi_j \in \mathrm{ch}(U(m))$. *Then,*

$$\mathrm{F}(m)\chi = \left(\prod_j \chi_j(M_j)\right) \bigotimes_j \mathrm{F}(m_j)\chi_j.$$

Thus, the results of Section III concerning the action of $\mathrm{F}(m_j)$, $m_j = p_j^{a_j}$ on multiplicative characters mod m_j can be directly extended to results about $\mathrm{F}(m)$ acting on multiplicative characters mod m.

APPENDIX B

In this appendix, we will collect some elementary number theoretic results which are almost immediate consequences of the theory developed in the main body of this work.

The first such results come about by applying Theorem 3.6, along with the fact that $\mathrm{F}(p^a)$ is a unitary operator.

LEMMA B.1. *Let* χ *be a primitive character* mod m, $m = p^a$.

1. $|G_m(\chi)| = m^{1/2}$
2. $G_m(\bar{\chi}) = \chi(-1)\overline{G_m(\chi)}$.

Proof. By Theorem 3.6,

$$\mathrm{F}(m)\chi = m^{-1/2} G_m(\chi)\bar{\chi}.$$

Since $\mathrm{F}(m)$ is

$$\langle \chi, \chi \rangle = \langle \mathrm{F}(m)\chi, \mathrm{F}(m)\chi \rangle = m^{-1}|G_m(\chi)|^2 \langle \bar{\chi}, \bar{\chi} \rangle,$$

which proves 1.

To prove 2, we apply Lemma 3.1. Thus,

$$\mathrm{F}(m)^2\chi = \chi(-1)\chi = m^{-1/2} G_m(\chi)\mathrm{F}(m)\bar{\chi} = m^{-1} G_m(\chi) G_m(\bar{\chi})\chi,$$

for which it follows that

$$\chi(-1) = m^{-1} G_m(\chi) G_m(\bar{\chi}).$$

Multiplying both sides by $\overline{G_m(\chi)}$ and using 1, gives result 2.

The next result depends upon Theorem 3.11 and (3.25).

LEMMA B.2.

$$\mathrm{tr}(\mathrm{F}(p^a)) = \begin{cases} 1, & a \text{ even} \\ \mathrm{tr}(\mathrm{F}(p)), & a \text{ odd.} \end{cases}$$

Proof. For $a \geq 2$, we can write

$$\mathrm{F}(p^a) \cong F(p^{a-2}) \oplus \sum_{\chi} M(\chi),$$

and since $\mathrm{tr}(M(\chi)) = 0$, the lemma follows.

We can, also, write

$$\mathrm{tr}(\mathrm{F}(p^a)) = \mathrm{tr}(\mathrm{F}(p^{a-2})), \qquad a \geq 2.$$

The same argument, using (3.24) and

$$\det M(\chi) = -\chi(-1),$$

will give results on $\det \mathrm{F}(P^a)$. First, a few simple calculations will be listed. Let $m = p^a$.

$$\text{(i)} \quad \prod_{\chi \in \mathrm{ch}(U(m))} \chi(-1) = \left(\frac{-1}{p}\right)$$

$$\text{(ii)} \quad \prod_{\chi \in \Psi_0} \chi(-1) = \begin{cases} (-1)^{p-1/4}, & p \equiv 1 \bmod 4 \\ (-1)^{p-3/4}, & p \equiv 3 \bmod 4 \end{cases}$$

$$\text{(iii)} \quad \prod_{\chi \in \Psi_0(m)} \chi(-1) = \left(\frac{-1}{p}\right), \qquad a > 1.$$

Observe that $\mathrm{ch}(U(m))U\Psi_0(p^a)$ has $p^{a-2}((p-1) + (p-1)^2/2$ elements, which is even when $a > 1$.

LEMMA B.3.

$$\det \mathrm{F}(p) = \begin{cases} (-1)^{(p+1)/4}\mathrm{tr}(\mathrm{F}(p)) & p \equiv 3 \bmod 4 \\ (-1)^{(p-1)/4}\mathrm{tr}(\mathrm{F}(p)) & p \equiv 1 \bmod 4. \end{cases}$$

LEMMA B.4.

$$\det \mathrm{F}(p^a) = \det \mathrm{F}(p^{a-2}), \qquad a > 1.$$

Proof. By $\mathrm{F}(p^a) \cong \mathrm{F}(p^{a-2}) \oplus \Sigma M(\chi)$, it follows that $\det \mathrm{F}(p^a) = \det \mathrm{F}(p^{a-2}) \cdot \prod \det M(\chi)$, and from $\prod \det M(\chi) = 1$ by (1) and (III) the lemma follows.

Lemma B.3 is an important step in Schur's evaluation of $\mathrm{tr}\,\mathrm{F}(p)$, for once we know (nontrivially) that

$$\det \mathrm{F}(p) = i^{p(p-1)/2},$$

we have

$$\operatorname{tr} \mathrm{F}(p) = \begin{cases} 1, & p \equiv 1 \bmod 4 \\ i, & p \equiv 3 \bmod 4 \end{cases}.$$

Using the tensor product observations of Appendix A, we could extend these results to the arbitrary m case.

Appendix C

The matrix of the discrete Fourier transform $\mathrm{F}(m)$, relative to the basis e_j, $0 \le j < m$, is given by

$$\mathrm{F}(m) = m^{-1/2}\left[w^{jk}\right]_{0 \le j,k < m},$$

where $w = \exp(2\pi i(1/m))$. In the appendix, we will explicitly write down an orthonormal matrix $X(m)$ diagonalizing $\mathrm{F}(m)$, i.e., $Z(m)\mathrm{F}(m)Z(m)^{-1}$ is a diagonal matrix, in case $m = p$, an odd prime or $m = 2^b$.

When $m = p$, an odd prime, we begin by choosing a generator α of $U(p)$, the multiplicative group of units of $\mathbb{Z}/p$. Any function on $\mathbb{Z}/p$ can be viewed as a p-tuple of complex numbers, taken as a column,

$$\mathrm{F} = (\mathrm{F}(0), \mathrm{F}(1), \ldots, \mathrm{F}(p-1))^t,$$

and we will do so in what follows. Thus, the matrix p describing the change of basis from the basis e_j, $0 \le j < p$ to the basis f_j, $0 \le j < p$, where

$$f_0 = e_0, \qquad f_j = e_{\alpha^{j-1}}, \qquad 1 \le j < p,$$

is given by

$$p = \left[f_0 f_1 \cdots f_{p-1}\right].$$

Recall that the matrix of $\mathrm{F}(p)$ relative to the basis f_j, $0 \le j < p$ is given by $P\mathrm{F}(p)P^{-1}$.

The multiplicative characters mod p have a simple description in terms of the basis f_j, $0 \le j < p$. Let x_j, $0 \le j < p-1$, be the multiplicative character mod p defined by setting

$$x_j(\alpha) = \exp\left(2\pi i \frac{j}{p-1}\right) = w^j,$$

where $w = \exp(2\pi i(1/(p-1)))$. A straightforward calculation shows

$$x_j = \sum_{k=0}^{p-2} w^{kj} f_{k+1}, \qquad 0 \le j < p-1.$$

Thus, the matrix describing the change of basis from f_j, $0 \le j < p$ to the basis

$$e_0, (p-1)^{-1/2} x_0, (p-1)^{-1/2} x_1, \ldots, (p-1)^{-1/2} x_{p-2} \tag{C.1}$$

is given by

$$\mathrm{F}^{\#}(p-1) = \begin{bmatrix} 1 & \\ & \mathrm{F}(p-1) \end{bmatrix}.$$

Consider, the rearrangement of the basis (C.1),

$$e_0, (p-1)^{-1/2} x_0, (p-1)^{-1/2} x_r, (p-1)^{-1/2} x_j, (p-1)^{-1/2} x_{p-1-j}, \tag{C.2}$$

where $1 \le j < r$, $r = (p-1)/2$. Let Q be the matrix describing the change of basis from (C.1) to (C.2). Then,

$$Q = \left[e_0 e_1 e_{r+1} e_2 e_{p-1} \ldots e_{r-1} e_{p-(r-2)} \right].$$

Recall that $\mathrm{F}(p)x_j = p^{-1/2} G(x_j) x_{p-j-1}$, and consider the basis

$$e_0, (p-1)^{-1/2} x_0, (p-1)^{-1/2} x_r, (p-1)^{-1/2} x_j, (p-1)^{-1/2} \mathrm{F}(p) x_j, \tag{C.3}$$

where $1 \le j < r$. The matrix

$$R = \begin{bmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & p^{-1/2} G(x_1) & & & \\ & & & & & 1 & & \\ & & & & & & p^{-1/2} G(x_{r-1}) \end{bmatrix}$$

describes the change of basis in going from (C.2) to (C.3).

Let

$$Y(p) = P \mathrm{F}^{\#}(p-1) Q R.$$

Clearly, $Y(p)$ describes the change of basis from the basis e_j, $0 \le j < p$, to the basis (C.3). By Theorem 3.5, the matrix

$$Y(p)\mathrm{F}(p)Y(p)^{-1}$$

is given by

$$p^{-1/2}\begin{bmatrix} 1 & \dfrac{(p-1)^{1/2}}{2} \\ \dfrac{(p-1)^{1/2}}{2} & -1 \end{bmatrix} \oplus p^{-1/2}G(x_r) \oplus \sum_{j=1}^{r-1} M\big((-1)^j\big),$$

where $M((-1)^j) = \begin{bmatrix} 0 & (-1)^j \\ 1 & 0 \end{bmatrix}$ since $x_j(-1) = (-1)^j$.

Let

$$X(p) = 2^{-1/2}p^{-1/4}\begin{bmatrix} (p^{1/2}+1)^{1/2} & (p^{1/2}-1)^{1/2} \\ (p^{1/2}-1)^{1/2} & -(p^{1/2}+1)^{1/2} \end{bmatrix},$$

$$X(1) = 2^{-1/2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$X(1) = 2^{-1/2}\begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix},$$

and

$$U(p) = X(p) \oplus [1] \oplus \sum_{j=1}^{r-1} X\big((-1)^j\big).$$

Then, by the comments following Theorem 3.5, the matrix

$$Z(p) = U(p) \cdot Y(p)$$

is orthonormal and diagonalizes $\mathrm{F}(p)$.

We will now study the case when $m = 2^b$. The cases $b = 1, 2, 3$, which we studied in Appendix A, can be done directly and we will simply write down the orthonormal matrix diagonalizing $J(2)^b$). They are as follows

$$Z(2) = s\begin{bmatrix} 1 & \sqrt{2}-1-1 \\ -\sqrt{2}+1 & 1 \end{bmatrix}, \qquad s = 2^{-1/2}(2-2^{-1/2})^{-1/2}$$

$$Z(4) = (x(1) \oplus [1] \oplus [1]) \cdot \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 1 & 0 & -1 & 0 \end{bmatrix}$$

$$Z(8) = (x(1) \oplus [1] \oplus [1] \oplus X(-1) \oplus Z(2)) \cdot Y(8),$$

where

$$Y(8) = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & i & 1 & -1 \\ 1 & 0 & -1 & 1 & -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & -1 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -i & 1 & -1 \\ 1 & 0 & 1 & -1 & -1 & 0 & 0 & 0 \end{bmatrix}.$$

Consider, now, $m = 2^b$, $b > 3$. Let

$$f_j = e_{2j}, \qquad 0 \le j < \frac{m}{2} = n_1,$$

$$g_{2j} = e_5 j, \qquad 0 \le j < \frac{m}{4} = n_2,$$

$$g_{2j} = e_{-5} j, \qquad 0 \le j < \frac{m}{4}.$$

Then, the functions

$$f_0, f_1, \ldots, f_{n_1-1}, g_0, g_1, \ldots, g_{n_1-1} \tag{C.4}$$

define a basis of $L^2(m)$, which we will also denote by h_j, $0 \le j < m$. The matrix P describing the change of basis from e_j, $0 \le j < m$ to the basis (C.4) is given by

$$P = [h_0 h_1 \ldots h_{n-1}].$$

We will write the multiplicative characters mod m in the following way. Let v_j, $0 \le j < n_1 = m/2$ be the multiplicative character mod m determined by the conditions

$$v_{2j}(5) = v_{2j+1}(5) = w^j$$

$$v_{2j}(-1) = 1 \qquad \text{and} \qquad v_{2j+1}(-1) = -1,$$

where $0 \le j < n_2 = m/4$. Then,

$$v_{2j} = \sum_{j=r_1}^{n_1+n_2-2} w^j (h_j + h_{j+1})$$

$$v_{2j+1} = \sum_{j=r_1}^{n_1+n_2-2} w^j (h_j + h_{j+1}).$$

Let

$$C_j = \mathrm{F}(2) \otimes \begin{bmatrix} 1 \\ w^{-1} \\ \vdots \\ w^{(n_2-1)j} \end{bmatrix}$$

$$D_j = \begin{bmatrix} O_{n_1} & O_{n_1} \\ C_j & j \end{bmatrix},$$

where O_{n_1} is the r_1-tuple of zeroes.

Order the subset of multiplicative characters mod m according to the following scheme

$$v_{2j}, v_{2j+1}, \tag{C.5}$$

where j runs first over the odd integers from 1 to $m/8 - 1$ and then over the even integers from 0 to $m/4 - 2$, inclusively. The matrix describing the ordered set of functions in terms of the basic (C.4) is given by

$$\left[D_1 D_3 \ldots D_{m/8-1} D_0 D_2 \ldots D_{m/4-2} \right].$$

The matrix of $\mathrm{F}(m)$ relative to basis (3.4) is given by $P\mathrm{F}(m)P^{-1}$. Thus, the matrix describing the ordered set of functions beginning with (C.5) and followed by the ordered set

$$(m)v_{2j}, \mathrm{F}(m)v_{2j+1}, \tag{C.6}$$

the j's ordered as before, is given by

$$\mathscr{D} = \left[DPJ(m)P^{-1}D \right].$$

Let $fu \in L^2(m)$ be defined by

$$f_u = e_{2u} + e_{2u+n_1}, \qquad 0 \le u < n_2,$$

and consider the set of functions

$$\begin{gathered} n_1^{-1/2} v_{2j}, n_1^{-1/2} v_{2j+1} \\ N_1^{-1/2} \mathrm{F}(m) v_{2j}, n_1^{-1/2} \mathrm{F}(m) v_{2j}. \\ f_0, f_1, \ldots, f_{n_2-1}. \end{gathered} \tag{C.7}$$

By (3.24) and Lemma 3.10, (C.7) is an orthonormal basis of $L^2(m)$. The matrix describing the basis in terms of the basis e_j, $0 \le j < m$, is given by

$$\left[P\mathscr{D} f_0 f_1 \ldots f_{n_2-1} \right].$$

Writing (C.7), in the order given below,

$$n_1^{-1/2}v_{2j},\ n_1^{-1/2}\mathrm{F}(m)v_{2j},\ n_1^{-1/2}v_{2j+1},\ n_1^{-1/2}\mathrm{F}(m)v_{2j+1}f_0,\ f_1,\ldots,f_{n_2-1}, \tag{C.8}$$

we have an orthonormal basis, relative to which the matrix of $\mathrm{F}(m)$ has the form

$$\sum_{j=0}^{3n_2-1} \oplus\, M\big((-1)^j\big) \oplus J(n_2). \tag{C.9}$$

The matrix describing (C.8) in terms of (C.7) is given by

$$\begin{bmatrix} Q & O \\ 0 & I_{n_2} \end{bmatrix} = Q^{\#},$$

where

$$Q = \left[e_0 e_{n_3} e_1 e_{n_3+1} \cdots e_{n_3-1} e_{2n_3-1}\right], \qquad n_3 = (3/8)m$$

and I_{n_2} is the $n_2 \times n_2$ identity matrix.

Let

$$Y(m) = \left[P\mathscr{D}Qf_0 f_1 \cdots f_{n_2-1}\right].$$

Then

$$Y(m)J(m)Y(m)^{-1}$$

is given by (C.9). Thus,

$$Z(m) = \left(\sum_{j=0}^{3n_2-1} \oplus\, X\big((-1)^j\big) \oplus Z(n_2)\right) Y(m)$$

is an orthonormal matrix diagonalizing $J(m)$.

Note added in proof. A related paper, "On the Eigen-vectors of Schur's Matrix" by P. Morton, *J. of Number Theory*, **12** (1980), 122–127, has recently come to the author's attention.

REFERENCES

1. L. AUSLANDER AND R. TOLIMIERI, Is computing with the finite Fourier transform pure or applied mathematics? *Bull. Amer. Math. Soc.* **1** (1979), 847–897.
2. L. AUSLANDER AND R. TOLIMIERI, Program for diagonalizing the discrete Fourier transform by an orthonormal matrix,
3. L. AUSLANDER, R. TOLIMIERI, AND S. WINOGRAD, Heckes' theorem on quadratic reciprocity, finite nilpotent groups and the Cooley–Tukey algorithms, *Adv. in Math.* **43**, No. 2 (1982), 122–172.

4. R. AYOUB, An introduction to the analytic theory of numbers, *Amer. Math. Soc.* No. 10 (1963).
5. B. BERNDT AND R. EVANS, The determination of Gauss sums, *Bull. Amer. Math. Soc.* (1982),
6. J. W. COOLEY AND J. W. TUKEY, An algorithm for the machine calculation of complex Fourier series, *Math. Comp.* **19** (1965), 297–301.
7. B. DICKINSON AND K. STEIGLITZ, Eigenvectors and functions of the discrete Fourier transform, *IEEE Trans. Acoust. Speech Signal Process.* **30**, No. 1 (1982), 25–30.
8. C. RADER, Discrete Fourier transforms when the number of data samples is prime, *Proc. IEEE* **56** (1968), 1107–1108.
9. S. WINOGRAD, On the multiplicative complexity of the discrete Fourier transform, *Advances of Math.*, in press.
10. R. YARLAGADDA, A note on the eigenvectors of DFT matrices, *IEEE Trans. Acoust. Speech Signal Process.*