Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA
Unidad Iztapalapa

División de Ciencias Básicas e Ingeniería

Maestría en Ciencias Matemáticas

Tesis

# SOBRE EL ESPECTRO Y LA TRAZA DE LA TRANSFORMADA DE FOURIER DISCRETA

que presenta

**Irasema Castro Hernández**

matrícula
**2212801540**

para obtener el grado de

**Maestra en Ciencias Matemáticas**

Esta tesis fue dirigida por

**Dr. Roberto Quezada Batalla**

Y defendida ante jurado, conformado por

**Presidente:** Dr. Jorge Ricardo Bolaños Servín

**Secretario:** Dr. Josué Daniel Vázquez Becerra

**Vocal:** Dr. Crispín Herrera Yáñez

Iztapalapa, Ciudad de México a 31 de octubre de 2023.

# Sobre el espectro y la traza de la transformada de Fourier discreta

Alumna: Irasema Castro Hernández

Tesis de Maestría

Departamento de Matemáticas
Universidad Autónoma Metropolitana
Iztapalapa
Ciudad de México

---

Dr. Roberto Quezada Batalla (asesor)

31 de octubre del 2023

# Índice general

# Agradecimientos

Agradezco a la Universidad Autónoma Metropolitana por los años que me ha permitido formar parte de su gran comunidad, en particular al Posgrado en Matemáticas por darme la oportunidad de seguir creciendo profesionalmente.

Gracias a los miembros de la comunidad de la UAM, profesores y compañeros que me han apoyado, orientado e inspirado en este camino, especialmente a mi asesor de tesis, Dr. Roberto Quezada Batalla, a quien admiro por su trayectoria académica y aprecio por su paciencia, tiempo y sobre todo le agradezco mucho por guiarme durante este proyecto de investigación.

Gracias a mis sinodales quienes con sus conocimientos me ayudaron a mejorar mi trabajo y me ofrecieron su apoyo en todo momento.

Agradezco a Dios, a mis padres y hermano por su eterno apoyo, su aliento y por creer en mi para lograr mis objetivos, por ser mi motivación para dar lo mejor de mi cada día. Gracias a mis amigos y familiares que estuvieron a mi lado y me demostraron su apoyo incondicional de muchas maneras.

Por último quiero agradecer al Consejo Nacional de Ciencia y Tecnología (CONACYT) por el apoyo económico brindado en esta etapa de mi formación.

Irasema Castro Hernández

# Resumen

En este trabajo presentamos una exposición auto-contenida del cálculo de la traza y el espectro de la transformada de Fourier discreta (DFT), siguiendo la referencia [1]. En particular, hemos completado la demostración de la equivalencia de los problemas del cálculo el espectro de la DFT y el cálculo de su traza, que aparece sólo esbozada en la referencia anterior. Con este propósito hemos tenido que introducir las nociones de representaciones unitarias, caracteres, el símbolo de Legendre, la fórmula de Euler, la ley de reciprocidad cuadrática y el cálculo de algunas sumas de Gauss.

"El estudio profundo de la naturaleza es la fuente
más fértil de descubrimientos matemáticos".
Joseph Fourier

# Introducción

La transformada de Fourier discreta (DFT) es una versión discreta de la transformada de Fourier usual, que actúa como una aplicación lineal unitaria del espacio de Hilbert $\mathbb{C}^{\mathbb{N}}$ en sí mismo. Se conoce ampliamente por sus aplicaciones en ingeniería y física pero tiene una profunda relación con matemáticas puras que intentaremos describir en este trabajo.

Desde el punto de vista teórico y también por sus aplicaciones, el conocimiento del espectro de la DFT es relevante y se sabe que el cálculo la traza es equivalente al problema de la multiplicidad de sus eigenvalores. La traza de la DFT es una suma de Gauss calculada por primera vez por K. F. Gauss cuando investigaba sobre la construcción de polígonos regulares, véase el teorema 99 en [10]. El cálculo que describimos en este trabajo aprovecha casos particulares de estas sumas combinadas con ciertas relaciones entre la traza de la DFT y la traza del producto de la DFT con elementos de la representación regular unitaria del grupo de unidades de $\mathbb{Z}_n$. Gauss realmente resolvió el problema de la traza y los valores propios de la transformada de Fourier discreta. Todas estas ideas se presentan en el Capítulo I de [1] y parte de este trabajo.

Como hemos citado antes, de acuerdo con J. Fourier, *el estudio profundo de la naturaleza es la fuente más fértil de descubrimientos matemáticos*. En efecto, J. Fourier inventó su transformada motivado por su interés en describir fenómenos naturales y este concepto es tan profundo que el estudio de sus propiedades constituye un área del análisis matemático llamada análisis de Fourier, cuya versión discreta tiene una importante componente algebraica y sus aplicaciones en ciencias e ingeniería son muy relevantes. Esto ilustra claramente que la matemática tiene muchas ramificaciones, más o menos alejadas de las aplicaciones en ciencias naturales, pero unidas en un sólo cuerpo que las armoniza. La separación entre matemáticas puras y aplicadas es artificial, se debe más bien a razones sociológicas que a una división real de esta bella disciplina.

En el primer capítulo de este trabajo, revisamos algunos conceptos del Álgebra Lineal y Teoría de Números, presentamos el grupo de unidades de $\mathbb{Z}_n$, denotado por $\mathbb{Z}_n^\times$ y demostramos algunas propiedades importantes de ellos. Aquí también se describe la representación regular unitaria $\rho$ de $\mathbb{Z}_n^\times$, el conjunto de todos los caracteres de esta representación denotado por $\widehat{\mathbb{Z}}_n$ y se muestra que el álgebra de las matrices $\mathbb{Z}_n^\times$-circulantes es una $*$-álgebra.

Posteriormente en el capítulo 2 definimos el símbolo de Legendre y el subgrupo de residuos

cuadráticos de $\mathbb{Z}_n$. Aquí también introducimos el Criterio de Euler y describimos algunos resultados con respecto a la DFT del símbolo de Legendre como función de su numerador y mostramos algunos teoremas sobre residuos cuadráticos, lo cual nos conduce al teorema de Wilson. Además demostramos la ley de reciprocidad cuadrática.

También presentamos una función propia de la transformada de Fourier discreta y calculamos explícitamente la traza de la DFT en el capítulo 3.

En el capítulo 4 mostramos que una suma de Gauss se puede expresar en términos del símbolo de Legendre. Así mismo demostramos que la traza de la DFT es una suma de Gauss y representamos otra suma de Gauss como la traza del producto de la representación regular unitaria del grupo $\mathbb{Z}_n^\times$ con la DFT y finalmente demostramos una relación entre estas trazas y el símbolo de Legendre, que es útil para calcular explícitamente la traza de la DFT.
Finalmente describimos el polinomio característico de la matriz $F^2(n)$ y los valores propios de la transformada de Fourier $F(n)$ así como sus multiplicidades.

"Los encantos de esta ciencia sublime, las matemáticas,
sólo se revelan a aquellos que tienen el valor de profundizar en ella".
Carl F. Gauss

# Capítulo 1

# Preliminares

En este capítulo expondremos algunas nociones y proposiciones necesarias para capítulos subsecuentes. En primer lugar veremos condiciones suficientes para obtener un sistema completo de residuos así como también demostraremos el Teorema Chino del Residuo, todo lo anterior en el contexto de congruencias de la Teoría de Números. En segundo lugar introducimos la noción de producto tensorial de espacios vectoriales y demostramos su existencia así como algunas de sus propiedades. Finalmente, en tercer lugar, introducimos al grupo de caracteres sobre $\mathbb{Z}_n$ e introduciremos la representación unitaria del grupo multiplicativo $\mathbb{Z}_n^\times = \mathbb{Z}_n \backslash \{0\}$ determinada por la acción multiplicativa de $\mathbb{Z}_n^\times$ sobre $\mathbb{Z}_n$.

## 1.1. Teoría de Números

Recordemos que el anillo $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ es el anillo cociente $\mathbb{Z}/m\mathbb{Z}$ en el cual cualesquiera dos enteros $a, b \in \mathbb{Z}$ representan al mismo elemento de $\mathbb{Z}/m\mathbb{Z}$ si y sólo si $a - b$ pertenece a $m\mathbb{Z} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}$, es decir, $m$ es un divisor de la diferencia $a - b$. Esto último suele expresarse como *a es congruente con b módulo m* y escribirse por medio de símbolos como $a \equiv b \mod m$, o bien, $m|a - b$. Puesto que $\{0, 1, \ldots, m-1\}$ es el conjunto de todos los posibles residuos que se obtienen al dividir por $m$, un conjunto de enteros $m$ enteros, digamos $A \subset \mathbb{Z}$, recibe el nombre de *sistema completo de residuos módulo m* si para cada $k \in \{0, 1, ..., m-1\}$ existe $a \in A$ tal que $a \equiv k \mod m$.

**Proposición 1.1.1** *Supongamos que $m, n$ son enteros positivos. Si $m, n$ son primos relativos entre sí, entonces el conjunto $\{\gamma_{\alpha\beta} = \alpha m + \beta n : 0 \leq \alpha < n,\ 0 \leq \beta < m\}$ es un sistema completo de residuos módulo $nm$.*

**Demostración.** Supóngase que $m, n$ son primos relativos entre sí, es decir, $(n, m) = 1$. Vemos que si $\beta$ corre sobre un sistema completo de residuos módulo $m$ y $\alpha$ corre sobre un sistema completo de residuos módulo $n$, entonces $\alpha m + \beta n$ corre sobre un sistema de residuos módulo $mn$. En efecto, supongamos que $\alpha m + \beta n \equiv \alpha' m + \beta' n \mod mn$. Entonces $(\alpha - \alpha')m + (\beta - \beta')n \equiv 0 \mod mn$, pero puesto que $m, n$ son primos relativos se obtiene que

$$\alpha \equiv \alpha' \mod n, \quad \text{y} \quad \beta \equiv \beta' \mod m$$

entonces cada clase es distinta. El resultado se sigue dado que hay $mn$ clases $\mod mn$. ■

Para cada entero postivo $m$, denotamos por $\phi(m)$ al número de enteros positivos no mayores que $m$ que además son primos relativos con $m$, es decir, el número de enteros $n$ tales que

$$0 < n \leq m, \quad (n, m) = 1.$$

Notemos que si $a$ es primo relativo con $m$, entonces también lo es cualquier número $x$ congruente con $a$ móulo $m$. De esta manera, el conjunto de enteros $\mathbb{Z}$ se puede partir en $\phi(m)$ clases de residuos primos relativos con $m$, y cualquier conjunto de $\phi(m)$ residuos primos relativos con $m$, uno de cada clase, se denomina *conjunto completo de residuos primos relativos con m*. Es evidente que uno de esos conjuntos completos de residuos de primos relativos con $m$ es el conjunto de enteros positivos menores $m$ y que además son primos relativos con $m$. Veamos ahora cómo obtener conjuntos completos de residuos primos relativos con $m$ a partir de un conjunto de tal tipo dado.

**Teorema 1.1.2** *Sean $m, k$ primos relativos entre sí. Si $a_1, a_2, \ldots, a_{\phi(m)}$ es un conjunto completo de residuos primos relativos de $m$, entonces $ka_1, ka_2, \ldots, ka_{\phi(m)}$ es también un conjunto de este tipo.*

**Demostración.** Cada uno de los elementos del segundo conjunto son primos relativos con $m$ y cualquier par de ellos son distintos. Entonces es un conjunto completo de residuos primos relativos con $m$. ■

Un resultado que necesitaremos más adelante es el Teorema Chino del Residuo el cual establece las condiciones bajo las cuales un sistema de congruencias posee una solución que además es única. Antes de demostrar tal resultado necesitamos del siguiente lema.

**Lema 1.1.3** *Sean $n_1, n_2 \in \mathbb{Z}$ con $(n_1, n_2) = 1$. Si $a \in \mathbb{Z}$ es tal que $n_1|a$ y $n_2|a$, entonces $n_1 \cdot n_2|a$.*

**Demostración.** De la hipótesis se tiene que existen $p, q \in \mathbb{Z}$ tales que $a = pn_1$ y $a = qn_2$ y además existen $s, t \in \mathbb{Z}$ que satisfacen $sn_1 + tn_2 = 1$. Entonces, $n_1 \cdot n_2|a$ puesto que

$$a = a \cdot 1 = a(sn_1 + tn_2) = asn_1 + atn_2 = qn_2 \cdot sn_1 + pn_1 \cdot tn_2 = n_1 n_2(sq + tp)$$

■

**Teorema 1.1.4** *(Teorema Chino del residuo). Supongamos $n_1, n_2, \ldots, n_k \in \mathbb{N}$ son números naturales tales que $(n_i, n_j) = 1$ para $i \neq j$. Entonces para cualesquiera $k$ enteros $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ el sistema de congruencias*

$$x \equiv a_1 \mod n_1, \; x \equiv a_2 \mod n_2, \; \ldots, \; x \equiv a_k \mod n_k \tag{1.1}$$

*tiene solución única módulo $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k$ la cual está determinada por la congruencia*

$$x \equiv a_1 \cdot c_1 \cdot d_1 + a_2 \cdot c_2 \cdot d_2 + \ldots + a_k \cdot c_k \cdot d_k \mod N,$$

*donde $c_i = \frac{N}{n_i}$ y $d_i$ es tal que $c_i \cdot d_i \equiv 1 \mod n_i$, para $i = 1, 2, \ldots, k$.*

**Demostración.** Tomemos $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k$ y además $c_i = \frac{N}{n_i}$ para $i = 1, \ldots, k$. Veamos por contradicción que $n_i$ y $c_i = \prod_{j \neq i} n_j$ son primos relativos entre sí. Supongamos que existe un primo $p$ tal que $p|n_i$ y $p|c_i$. Como $p| \prod_{j \neq i} n_j$ con $p$ primo, existe un entero $l \in \{1, \ldots, k\}$ distinto de $i$ tal que $p|n_l$. Pero entonces se tendría que $p|n_i$ y $p|n_l$ con $i \neq l$, lo que contradice la hipótesis de que $(n_i, n_l) = 1$. Por consiguiente, $(n_i, c_i) = 1$. Por la afirmación anterior sabemos que $c_i$ tiene recíproco módulo $n_i$, es decir, existe $d_i \in \mathbb{Z}$, tal que $c_i \cdot d_i \equiv 1 \mod n_i$. Vemos ahora que

$$x := \sum_{i=1}^{k} a_i \cdot c_i \cdot d_i,$$

es solución del sistema de congruencias considerado. Sea $l \in \{1, \ldots, k\}$. Si $j \neq l$, se tiene que $n_l|c_j$ pues $c_j = \prod_{i \neq j} n_i$, entonces $n_l|a_j \cdot c_j \cdot d_j$, es decir, $a_j \cdot c_j \cdot d_j \equiv 0 \mod n_l$. Por otro lado, $c_l \cdot d_l \equiv 1 \mod n_l$ implica que $a_l \cdot c_l \cdot d_l \equiv a_l \mod n_l$. Sumando las congruencias anteriores sobre $j$ se obtiene

$$x = \sum_{j=1}^{k} a_j \cdot c_j \cdot d_j \equiv a_l \mod n_l.$$

Ahora veamos que $x$ es la solución única módulo $N$. Para esto, supongamos que $y \in \mathbb{Z}$ es tal que

$$y \equiv a_1 \mod n_1, \quad y \equiv a_2 \mod n_2, \ \ldots, \quad y \equiv a_k \mod n_k.$$

Esto implica que $x \equiv y \mod n_i$, es decir, $n_i|(x-y)$ para $i = 1, 2, \ldots, k$. Como $(n_i, n_j) = 1$ si $i \neq j$, aplicando el lema anterior de manera iterada se obtiene $n_1 \cdot n_2 \cdots n_k|(x-y)$, es decir, $x \equiv y \mod N$. Por lo tanto, $x = \sum_{i=1}^{k} a_i \cdot c_i \cdot d_i$ es solución única módulo $N$. ■

## 1.2. Producto Tensorial

En esta sección desarrollamos algunas propiedades del producto tensorial de dos espacios vectoriales complejos.

**Definición 1.2.1** *Sean $V$, $W$ y $U$ espacios vectoriales sobre el campo $\mathbb{C}$. La función $G : V \times W \longrightarrow U$ es una función sesquilineal si son lineales las aplicaciones*

$$\forall v \in V \quad w \mapsto G(v, w) \quad y \quad \forall w \in V \quad v \mapsto G(v, w)$$

**Teorema 1.2.2** *Existencia del producto tensorial y propiedades básicas.*
*Si $V$ y $W$ son espacios vectoriales de dimensión $n$ y $m$ respectivamente sobre $\mathbb{C}$, entonces existe un espacio vectorial $V \otimes W$ de dimensión $nm$ y una función bilineal $\tau : V \times W \longrightarrow V \otimes W$, tal que $(v, w) \mapsto^{\tau} v \otimes w$ satisface las siguientes propiedades:*

1. *El producto de $v \in V$ y $w \in W$ se denota por $v \otimes w$ y satisface las siguientes relaciones:*

   *Si $v_1, v_2 \in V$ y $w \in W$,*

   $$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$$

*Si* $w_1, w_2 \in W$ *y* $v \in V$,

$$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$$

*Si* $c$ *es un escalar arbitrario y* $w_2 \in W$, $v \in V$,

$$c(v \otimes w) = (cv) \otimes w = v \otimes (cw)$$

2. *Todo elemento del producto tensorial se puede escribir en la forma* $\sum_i c_i v_i \otimes u_i$ *para algunos escalares* $c_i$, *y algunos* $v_i \in V, u_i \in W$.

3. *Si* $\{v_1, \dots v_n\}$ *y* $\{w_1, \dots w_m\}$ *son bases de* $V$ *y* $W$ *respectivamente, entonces los elementos* $v_i \otimes w_j$, $i = 1, \dots, n$ *y* $j = 1, \dots m$ *constituyen una base de* $V \otimes W$.

4. *Propiedad Universal. Si* $U$ *es un espacio vectorial sobre* $\mathbb{C}$ *y* $\mathcal{L} : V \times W \longrightarrow U$ *es una función bilineal, entonces existe una* **única aplicación lineal** $L : V \times W \longrightarrow U$ *tal que* $\mathcal{L} = L \circ \tau$ *es decir*

$$\mathcal{L}(v, w) = L(u \otimes v) \ \forall v \in V, \forall w \in V.$$

**Demostración.**

1. Sean $\{v_1, \dots v_n\}$ y $\{w_1, \dots w_m\}$ bases de $V$ y $W$ y sea $\mathcal{S} = \{s_{ij}\}_{ij}$ un conjunto con $nm$ elementos. Definimos $V \otimes W$ como el espacio vectorial libre sobre $\mathbb{C}$ con base $\mathcal{S}$. Es decir $V \otimes W$ es un espacio vectorial de dimensión $nm$ y consta de todas la combinaciones lineales formales de elementos $s_{ij}$ con coeficientes en $\mathbb{C}$, o sea expresiones de la forma $\sum_{i=1}^n \sum_{j=1}^m c_{ij} s_{ij}$ con $c_{ij} \in \mathbb{K}$. Si $v = \sum_{i=1}^n x_i v_i$ y $w = \sum_{j=1}^m y_j w_j$ son las expresiones de $v$ y $w$ en términos de los básicos se define el producto tensorial como el elemento

$$v \otimes w = \sum_{i=1}^{n} \sum_{j=1}^{m} x_i y_j s_{ij}$$

en particular $v_i \otimes w_j = s_{ij}$. Probemos que $(v, w) \mapsto^\tau v \otimes w$ es bilineal. Sea $v' = \sum_{i=1}^n x_i' v_i$ y sean $v$ y $w$ como antes, entonces $cv + v' = \sum_{i=1}^n (cx_i + x_i') v_i$, luego por definición $(cv + v') \otimes w = \sum_i \sum_j (cx_i + x_i') y_j s_{ij} = \sum_i \sum_j c x_i y_j s_{ij} + \sum_i \sum_j x_i' y_j s_{ij} = cv \otimes w + v' \otimes w$. La prueba de la linealidad en el otro lado es semejante.

2. Con la notación anterior, sabemos que un elemento arbitrario del producto tensorial es de la forma $\xi = \sum_i \sum_j c_{ij} v_i \otimes w_j$, reescribiendolo tenemos que $\xi = \sum_i v_i \otimes \left( \sum_j c_{ij} w_j \right)$ lo que muestra el resultado.

3. Sean $\{v_1', \dots, v_n'\}$ y $\{w_1', \dots, w_m'\}$ bases de $V$ y $W$ respectivamente, si $v = \sum_i x_i v_i'$ y $w = \sum_j y_j w_j'$ son las expresiones en términos de los básicos de $v$ y $w$, entonces $v \otimes w = \sum_i \sum_j x_i y_i (v_i' \otimes w_j')$ es decir los $nm$ elementos $v_i' \otimes w_j'$ generan al espacio vectorial $V \otimes W$ de dimensión $nm$ y por tanto, necesariamente son linealmente independientes lo que prueba que formen una base.

4. Sea $\mathcal{L} : V \times W \longrightarrow U$ es una función sesquilineal. Existe una única transformación lineal $L : V \times W \longrightarrow U$ tal que $L(v_i \otimes w_j) = \mathcal{L}(v_i, w_j)$, entonces para cualesquiera $v$ y $w$ expresados (como antes) en términos de los básicos tenemos

$$\mathcal{L}(v, w) = \mathcal{L}\big(\sum_i x_i v_i, \sum_j y_j w_j\big) = \sum_i \sum_j x_i y_j \mathcal{L}(v_i, w_j) = L(v \otimes w).$$

Es decir $L$ existe y está determinada en forma única.

■

## 1.3. Representaciones Unitarias y Caracteres

La teoría de representaciones es un término que comprende algunos temas de álgebra y de análisis matemático, los cuáles comparten la descripción de simetría en espacios vectoriales. El trabajo de ésta teoría es deducir propiedades esenciales de la estructura original a partir de las matrices que la representan.

A continuación presentamos algunas definiciones importantes como la definición de la representación unitaria $\rho$ de $\mathbb{Z}_n^\times$ en $L_2(\mathbb{Z}_n)$ y damos respuesta a cómo actúa $\rho$ en la base ortonormal de $L_2(\mathbb{Z}_n)$.

**Definición 1.3.1** *Sea $f$ una función sobre un sistema completo de residuos* mód $n$ *tal que si $\xi \in R_n$ y $\xi' \in R_n$ con $\xi \equiv \xi'$* mód $n$ *se tiene que $f(\xi) = f(\xi')$. Diremos que $f$ es una función en $\mathbb{Z}_n$ y usaremos la notación $f(\xi), \xi \in \mathbb{Z}_n$.*

Veamos otra forma del lema (4.3.2). Sea $L_2(\mathbb{Z}_n)$ el conjunto de funciones complejas sobre $\mathbb{Z}_n$. Recordemos que $L_2(\mathbb{Z}_n)$ es un espacio vectorial de dimensión $n$.

$\mathbb{Z}_n^\times$ actúa sobre $\mathbb{Z}_n$ multiplicativamente, es decir, para cada elemento $a \in \mathbb{Z}_n^\times$ se tiene un homomorfismo $\widehat{a} : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$, definido por $\widehat{a}(z) = az = za$.

**Definición 1.3.2** *Definimos la representación regular unitaria $\rho$ de $\mathbb{Z}_n^\times$ en $L_2(\mathbb{Z}_n)$ como el homomorfismo*

$$\rho : \mathbb{Z}_n^\times \longrightarrow B(L_2(\mathbb{Z}_n)) \tag{1.2}$$

*tal que para cada $a \in \mathbb{Z}_n^\times$, $\rho(a)$ es la transformación lineal $\rho(a) : L_2(\mathbb{Z}_n) \longrightarrow L_2(\mathbb{Z}_n)$, definida mediante $(\rho(a)f)(z) = f(az) = f(za)$, $z \in \mathbb{Z}_n, f \in L_2(\mathbb{Z}_n)$.*

Observación:

1. $L_2(\mathbb{Z}_n) = \{f : \mathbb{Z}_n \longrightarrow \mathbb{C}\}$ se puede identificar con $\mathbb{C}^n$, pues una función se puede identificar con sus valores $f \sim (f_0, f_1, \ldots, f_{n-1})$.

2. Bajo la identificación de $L_2(\mathbb{Z}_n) \sim \mathbb{C}^n$, con cada $a \in \mathbb{Z}_n^\times$ corresponde una transformación lineal (matriz) $\rho(a) : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ definida mediante $\rho(a)f(z) = f(az) = (f_0, f_a, f_{2a}, \ldots, f_{(n-1)a})$.

Sean $e_b$ funciones de $L_2(\mathbb{Z}_n) = \mathbb{C}^n$ tales que para todo $z \in \mathbb{Z}_n$, se tiene:

$$e_b(z) = \delta_{bz} = \begin{cases} 1 & \text{si } b = z, \\ 0 & \text{si } b \neq z. \end{cases} \tag{1.3}$$

Por ejemplo, si $b = 0$,

$$e_0(z) = \delta_{0z} = \begin{cases} 1 & \text{si } z = 0, \\ 0 & \text{si } z \neq 0. \end{cases} \tag{1.4}$$

entonces las coordenadas de $e_0$ estan dadas por $e_0 = (1, 0, 0, \ldots, 0)$, de manera similar se construye $e_1 = (0, 1, 0, \ldots, 0)$ y así sucesivamente. De esta forma $(e_b)_{b\in\mathbb{Z}_n}$ es la base ortonormal de $L_2(\mathbb{Z}_n) \sim \mathbb{C}^n$.

¿Cómo actúa $\rho(a)$ en la base?
Nótese que $(\rho(a)e_b)(z) = e_b(az)$, $a \in \mathbb{Z}_n^\times$, pero para cada $z \in \mathbb{Z}_n$,.

$$e_b(az) = \delta_{b,az} = \begin{cases} 1 & \text{si } az = b \quad \Leftrightarrow \quad z = ba^{-1} \\ 0 & \text{si } az \neq b \quad \Leftrightarrow \quad z = ba^{-1} \end{cases} \tag{1.5}$$

Es decir, $\rho(a)e_b = e_{ba^{-1}}$. Así, por ejemplo, si $a = 1$, tenemos $\rho(1)e_b = e_b$, para cada $b \in \mathbb{Z}_n$. Usando la linealidad concluimos que $\rho(1)$ es la identidad.

El grupo de unidades $\mathbb{Z}_n^\times$ es isomorfo al subgrupo de matrices generado por el conjunto $\mathrm{Im}(\rho) = \{\rho(a) : a \in \mathbb{Z}_n^\times\}$, por lo que todas las $\rho(a)$ son invertibles. Asociada con este grupo existe un álgebra llamada el grupo álgebra de $\mathbb{Z}_n^\times$, a la que también se le llama álgebra de matrices $\mathbb{Z}_n^\times$-circulantes, que consiste del álgebra generada por $\{\rho(a) : a \in \mathbb{Z}_n^\times\}$. Obsérvese que $\rho(a)\rho(a') = \rho(aa')$ y $\rho(a^{-1}) = \rho(a)^{-1}$. El adjunto del elemento $\rho(a)$ es el único elemento $\rho(a)^*$ que satisface la relación

$$\langle u, \rho(a)v\rangle = \langle \rho(a)^* u, v\rangle$$

Pero, si ponemos $\rho(a)^* = \rho(d)$, entonces

$$\begin{aligned} \langle u, \rho(a)v\rangle =& \langle \sum_b u_b e_b, \rho(a) \sum_c v_c e_c\rangle = \sum_{b,c} u_b \overline{v}_c \langle e_b, \rho(a)e_c\rangle = \sum_{b,c} u_b \overline{v}_c \langle e_b, e_{ca^{-1}}\rangle \\ =& \langle \rho(d)u, v\rangle = \sum_{b,c} u_b \overline{v}_c \langle \rho(d)e_b, e_c\rangle = \sum_{b,c} u_b \overline{v}_c \langle e_{bd^{-1}}, e_c\rangle \end{aligned} \tag{1.6}$$

pero esta identidad se cumple si y sólo si $c = ba = bd^{-1}$, lo cual implica que $d = a^{-1}$. Es decir, el adjunto de $\rho(a)$ es $\rho(a)^* = \rho(a^{-1})$, consecuentemente, para cada $a \in \mathbb{Z}_n^\times$ tenemos

$$\rho(a)\rho(a)^* = \rho(a)\rho(a^{-1}) = \rho(aa^{-1}) = \rho(1) = 1 = \rho(a)^*\rho(a)$$

lo cual implica que $\rho(a)$ es una matriz unitaria, i.e., $\rho(a) \in U(n)$, donde $U(n)$ es el grupo de matrices unitarias, u operadores unitarios sobre $L_2(\mathbb{Z}_n)$. Por lo tanto el álgebra de las matrices $\mathbb{Z}_n^\times$-circulantes es una $*$-álgebra. Cada elemento de esta $*$-álgebra se puede escribir en la forma $A = \sum_a \alpha_a \rho(a)$, con $\alpha$ una función de $\mathbb{Z}_n^\times$ en $\mathbb{C}$.

Sea $\mathbb{C}$ el campo de los números complejos y $\mathbb{C}_1^\times$ los complejos de módulo 1. Un caracter es un homomorfismo $\lambda$ de $\mathbb{Z}_n$ en $\mathbb{C}_1^\times$. El conjunto de todos los caracteres se denota por $\widehat{\mathbb{Z}}_n$. Para $\lambda_1, \lambda_2 \in \widehat{\mathbb{Z}}_n$ definimos

$$(\lambda_1 + \lambda_2)(a) = \lambda_1(a)\lambda_2(a), \;\; a \in \mathbb{Z}_n$$

Así, $\widehat{\mathbb{Z}}_n$ es un grupo isomorfo a $\mathbb{Z}_n$. Para $0 \leq \alpha < n, \;\; \alpha \in \mathbb{N}$, sea $\lambda_\alpha : \mathbb{Z}_n \longrightarrow \mathbb{C}_1^\times$ definida por

$$\lambda_\alpha(a) = e^{-2\pi i a\alpha/n}, \;\; a \in \mathbb{Z}_n.$$

Claramente $\lambda_\alpha$ es un caracter bien definido en $\mathbb{Z}_n$ y se comprueba fácilmente que $\widehat{\mathbb{Z}}_n$ consiste de los $n$ caracteres $\lambda_\alpha$, $0 \leq \alpha < n$. Notemos que $\lambda_\alpha \in L^2(\mathbb{Z}_n)$ y

$$\langle \lambda_\alpha, \lambda_\beta \rangle = \sum_{a \in \mathbb{Z}_n} e^{-2\pi i a\alpha/n} e^{2\pi i a\beta/n} = \sum_{a \in \mathbb{Z}_n} e^{2\pi i a(\beta-\alpha)/n},$$

entonces

$$\langle \lambda_\alpha, \lambda_\beta \rangle = \begin{cases} n, & \alpha = \beta, \\ 0, & \alpha \neq \beta, \end{cases} \tag{1.7}$$

$\alpha, \beta \in \mathbb{Z}_n$. Por esa razón los $\lambda_\alpha$, $0 \leq \alpha < n$, son una base ortogonal de $L_2(\mathbb{Z}_n)$.

# Capítulo 2

# Símbolo de Legendre

En la teoría de números, el símbolo de Legendre es una función multiplicativa utilizada para determinar el carácter cuadrático de un número (módulo $p$). Éste símbolo fué introducido por Adrien-Marie Legendre en 1798 e intentó demostrar la ley de recíprocidad cuadrática. Algunas generalizaciones del símbolo de Legendre incluyen el símbolo de Jacobi y los caracteres de Dirichlet de orden superior.

En éste capítulo, definimos el símbolo Legendre que es una notación asociada a residuos cuadráticos y probamos algunos teoremas relacionados como el teorema de Wilson, el criterio de Euler, entre otros resultados e identidades del símbolo de Legendre, así como se demuestra la ley de reciprocidad cuadrática en términos del símbolo de Legendre.

## 2.1. Residuos Cuadráticos

Comenzaremos ésta sección recordando el concepto de residuo cuadrático para así conocer la ley de reciprocidad cuadrática. Dentro de la teoría de números se denomina residuo cuadrático módulo $n$ a cualquier entero $a$ coprimo con $n$ para el cual tiene solución la congruencia $x^2 \equiv a \mod n$ o lo que es lo mismo cuando $a$ es un cuadrado no nulo módulo $n$ y que por lo tanto tiene una raíz cuadrada en la aritmética de módulo $n$. A los enteros que no son congruentes con cuadrados perfectos módulo $n$ se les denomina no-residuos cuadráticos. A continuación veremos ésta definición con más detalle, así como algunos resultados importantes y damos a conocer la definición de el símbolo de Legendre.

Sea $n$ un primo impar, tal que $n \nmid a$, y $x$ uno de los números

$$1, 2, 3, \ldots, n-1.$$

Entonces, por el teorema 1.1.2, solo uno de los números

$$1 \cdot x, 2 \cdot x, \ldots, (n-1)x$$

es congruente con $a \mod n$. Existe por tanto un único $x'$ tal que

$$xx' \equiv a \mod n, \quad 0 < x' < n.$$

Llamaremos a $x^{'}$ el asociado de $x$. Hay entonces dos posibilidades: al menos una $x$ es asociada de sí misma, de modo que $x^{'} = x$, o no existe tal $x$.

1. Supongamos que la primera alternativa es verdadera, es decir, $x$ esta asociada con sigo misma. En este caso la congruencia

$$x^2 \equiv a \quad \text{mód } n$$

tiene la solución $x = x_1$, y decimos que $a$ es un residuo cuadrático de $n$ o, cuando no exista confusión, lo llamaremos simplemente un residuo de $n$, y escribimos $a\mathrm{R}n$. Claramente

$$x = n - x_1 \equiv -x_1 \quad \text{mód } n$$

es otra solución de la congruencia. Además si $x^{'} = x$ para cualquier otro valor $x_2$ de $x$, tenemos que

$$x_1^2 \equiv a,\ x_2^2 \equiv a,\ (x_1 - x_2)(x_1 + x_2) = x_1^2 - x_2^2 \equiv 0 \quad \text{mód } n.$$

Por lo tanto $x_2 \equiv x_1$ o

$$x_2 \equiv -x_1 \equiv n - x_1;$$

y solo hay dos soluciones de la congruencia, a saber, $x_1$ y $n - x_1$. En este caso los números.

$$1, 2, ..., n - 1$$

pueden agruparse como $x_1, n - x_1$, y $\frac{1}{2}(n - 3)$ pares de números asociados distintos. Ahora

$$x_1(n - x_1) \equiv -x_1^2 \equiv -a \quad \text{mód } n,$$

mientras $xx^{'} \equiv a \ \ \text{mód } n$, para cualquier par asociado $x, x^{'}$. Por eso

$$(n-1)! = \prod x \equiv -a \cdot a^{\frac{1}{2}(n-3)} \equiv -a^{\frac{1}{2}(n-1)} \quad \text{mód } n.$$

2. Si la segunda alternativa es verdadera y ningún $x$ está asociado consigo mismo, decimos que $a$ es un no-residuo cuadrático de $n$, o simplemente no es un residuo cuadrático de $n$, y escribimos $aNn$. En este caso la congruencia

$$x^2 \equiv a \quad \text{mód } n$$

no tiene solución, y los números

$$1, 2, ..., n - 1$$

pueden estar ordenados en $\frac{1}{2}(n - 1)$ pares desiguales asociados. Por lo tanto

$$(n-1)! = \prod x \equiv a^{\frac{1}{2}(n-1)} \quad \text{mód } n.$$

Definimos el símbolo $\left[\frac{a}{n}\right]$, donde $n$ es un primo impar y $a$ es cualquier número no divisible por $n$, como

$$\begin{aligned}\left[\frac{a}{n}\right] &= +1, \ si \ aRn, \\ \left[\frac{a}{n}\right] &= -1, \ si \ aNn.\end{aligned} \tag{2.1}$$

Es claro que

$$\left[\frac{a}{n}\right] = \left[\frac{b}{n}\right]$$

si $a \equiv b \mod n$.

Hemos demostrado el siguiente teorema.

**Teorema 2.1.1** *Si $n$ es un primo impar y $a$ no es múltiplo de $n$, entonces*

$$(n-1)! \equiv -\left[\frac{a}{n}\right] a^{\frac{1}{2}(n-1)} \mod n.$$

Suponiendo que $n$ es impar. Es claro que, $0 = 0^2$, $1 = 1^2$, y por lo tanto todos los números son residuos cuadráticos de 2. No definiremos los símbolos $[\frac{0}{2}]$ y $[\frac{1}{2}]$ y en lo que sigue ignoraremos este caso.

Los dos casos mas simples del teorema anterior (2.1.1), son aquellos en los que $a = 1$ y $a = -1$.

Sea $a = 1$. Entonces

$$x^2 \equiv 1 \mod n$$

tiene soluciones $x = \pm 1$, por lo tanto 1 es un residuo cuadrático de $n$ y

$$\left[\frac{1}{n}\right] = 1.$$

Por lo tanto, si ponemos $a = 1$ en el teorema anterior (2.1.1), este se convierte en el siguiente.

**Teorema 2.1.2** *Teorema de Wilson*

$$(n-1)! \equiv -1 \mod n.$$

La congruencia

$$(n-1)! + 1 \equiv 0 \mod n^2$$

es cierta para

$$n = 5, n = 13, n = 563,$$

pero para ningún otro valor de $n$ menor que 200000. Aparentemente no se conoce un teorema general concerniente a esta congruencia. Si $m$ es compuesto, entonces

$$m|(m-1)! + 1$$

es falso, porque hay un número $d$ tal que,

$$d|m, \ 1 < d < m,$$

y $d$ no divide $(m-1)! + 1$.

**Teorema 2.1.3** *Si $n$ es un primo impar y $a$ no es múltiplo de $n$, entonces*

$$\left[\frac{a}{n}\right] \equiv a^{\frac{1}{2}(n-1)} \quad \text{mód } n.$$

**Demostración.** Es una combinación de los teoremas (2.1.1) y (2.1.2). ■

**Definición 2.1.4** *Sea $n$ un primo impar, $(n > 2)$, consecuentemente $\mathbb{Z}_n$ es campo. Sea $\mathbb{Z}_n^\times$ el grupo de unidades de $\mathbb{Z}_n$, es decir, aquellos elementos $x \in \mathbb{Z}_n$, tales que $x^{-1} \in \mathbb{Z}_n$.*

**Proposición 2.1.5** *$\mathbb{Z}_n^\times$ es un grupo cíclico de orden $n-1$.*

**Demostración.** Como $\mathbb{Z}_n^\times = \mathbb{Z}_n \backslash \{0\}$, entonces $\mathbb{Z}_n^\times$ tiene exactamente $n-1$ elementos, es decir, el orden de $\mathbb{Z}_n^\times$ es $n-1$. Sea $m$ el máximo orden de los elementos de $\mathbb{Z}_n^\times$, consideremos el polinomio $\lambda^m - 1$ en el grupo $\mathbb{Z}_n^\times$. Como sabemos, el orden de un elemento $a$ es el entero positivo $p$ más pequeño tal que $a^p = 1$, $a \in \mathbb{Z}_n^\times$, así que para cada elemento $x \in \mathbb{Z}_n^\times$, el orden de $x$ divide a $m$. Por lo tanto, cada uno de estos elemento es un cero en el polinomio $\lambda^m - 1$, lo cual implica que $m \geq n-1$. Pero el orden de un elemento de un grupo no puede ser más grande que el orden del grupo. Así tenemos que $m = n-1$ y cualquier elemento de orden $m$ es generador de $\mathbb{Z}_n^\times$. ■

**Proposición 2.1.6** *Sea $S = \{\xi^2 \mid \xi \in \mathbb{Z}_n^\times\}$, $S$ es un subgrupo de $\mathbb{Z}_n^\times$.*

**Demostración.** Sean $\xi^2, \eta^2$ dos elementos de $S$, entonces $\xi^2\eta^2 = (\xi\eta)^2$, así $\xi^2\eta^2 \in \mathbb{Z}_n^\times$. Sea $\xi^2 \in S$, entonces $(\xi^{-1})^2\xi^2 = (\xi^{-1}\xi)^2 = 1$, entonces $(\xi^2)^{-1} = (\xi^{-1})^2 \in S$. Por lo que $S$ es subgrupo de $\mathbb{Z}_n^\times$. ■

$S$ es el subgrupo de residuos cuadráticos módulo $n$.

**Proposición 2.1.7** *El subgrupo de residuos cuadráticos $S$ satisface:*

*(i) $S$ es subgrupo normal de $\mathbb{Z}_n^\times$.*

*(ii) El grupo cociente $\mathbb{Z}_n^\times / S$ tiene orden 2.*

**Demostración.** El inciso $(i)$ es inmediato por la conmutatividad. Si $a \in \mathbb{Z}_n^\times$ y $a \notin S$, entonces $S$ y $aS$ son dos clases laterales diferentes, de hecho:

- $S \cap aS = \varnothing$, pues la condición $x = ay$, $x, y \in S$ implica que $a = xy^{-1} \in S$; y
- $\mathbb{Z}_n^\times = S \cup aS$, pues si $g$ es el generador de $\mathbb{Z}_n^\times$ y $a = g^{2p+1}$ entonces cada $x \notin S$, equivalentemente, $x = g^{2k+1}$, se puede escribir en la forma $x = g^{2k+1} = g^{2p+1}g^{2(k-p)} = ag^{2(k-p)} \in aS$.

Por lo tanto sólo hay dos clases laterales $S$ y $aS$ con $a \notin S$. ■

**Definición 2.1.8** *Sean* $\mathbb{Z}_3^\times = \{1, -1\} \subset \mathbb{Z}_3$ *el grupo multiplicativo de orden* 2 *y el grupo* $\mathbb{Z}_n^\times$. *Definimos el homomorfismo* $h : \mathbb{Z}_n^\times \longrightarrow \mathbb{Z}_3^\times$, *tal que* $\ker h = S$. *Es decir* $h(a) = 1$ *si* $a \in S$ *y* $h(a) = -1$ *si* $a \notin S$.

**Definición 2.1.9** *Para los enteros* $\mathbb{Z}$, *consideremos el homomorfismo* $\tilde{n} : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ *con* $\ker \tilde{n} = n\mathbb{Z}$. *Para* $m \in \mathbb{Z}$ *definimos* $(\frac{m}{n})$ *como el símbolo de Legendre*

$$\left(\frac{m}{n}\right) = \begin{cases} 0 & si\ m \equiv 0 \mod n, \\ h(\tilde{n}(m)) & si\ m \not\equiv 0 \mod n. \end{cases} \tag{2.2}$$

**Proposición 2.1.10** *Sean* $n_1, n_2 \in \mathbb{Z}$ *y* $n$ *un primo impar, si* $n_1 \equiv n_2 \mod n$, *entonces* $(n_1/n) = (n_2/n)$.

**Demostración.** Si $n_1$ es residuo cuadrático módulo $n$ tenemos que $(n_1/n) = 1$. Entonces existe un entero $a$ tal que $n_1 \equiv a^2 \mod n$. Como $n_1 \equiv n_2 \mod n$, resulta que $a^2 \equiv n_2 \mod n$ y así $(n_2/n) = 1 = (n_1/n)$.
Ahora, si $n_1$ no es residuo cuadrático módulo $n$, entonces para cualquier entero $a$, $a^2 \not\equiv n_1 \mod n$, y como $n_1 \equiv n_2 \mod n$, se sigue que $a^2 \not\equiv n_2 \mod n$. En consecuencia, $n_2$ no es residuo cuadrático módulo $n$ y $(n_2/n) = -1 = (n_1/n)$. ■
Consideraremos $\left(\frac{m}{n}\right)$ como una función de $m$ para $m \in \mathbb{Z}_n^\times$.

## 2.2. Ley de Recíprocidad Cuadrática

La ley de reciprocidad cuadrática o mejor conocida como el teorema áureo por Friedrich Gauss (1777-1855) que relaciona la solución de dos congruencias de la forma $x^2 \equiv a \mod n$ y $y^2 \equiv n \mod a$, donde $a$ y $n$ son números primos impares, es muy reconocida en teoría de números por lo que en ésta sección probamos el criterio de Euler, hacemos uso del símbolo de Legendre y de algunas identidades para probar resultados relevantes que nos sirven de guía para demostrar la ley de reciprocidad cuadrática.

**Proposición 2.2.1** *(Criterio de Euler, ver [4]) Sean* $m \in \mathbb{Z}_n$ *y* $n$ *un primo impar que no es divisor de* $m$, *entonces*

$$\left(\frac{m}{n}\right) = m^{\frac{n-1}{2}} \tag{2.3}$$

**Demostración.** Como $m$ no es congruente con $0 \mod n$, entonces $\left(\frac{m}{n}\right) = \pm 1$. Ahora $\mathbb{Z}_n$ es un campo, entonces cada polinomio de grado $k$ tiene a lo más $k$ raíces. En particular la ecuación $x^2 \equiv m \mod n$ tiene a lo más dos soluciones para cada $m$. Entonces además de 0, hay a lo más $\frac{n-1}{2}$ residuos cuadráticos módulo $n$. Pues cada uno de los $n-1$ posibles valores de $x$ puede ir acompañado sólo de un valor más, distinto de $x$, con el mismo residuo módulo $n$.

Nótese que $(n-x)^2 \equiv x^2 \mod n$, pues $(n-x)^2 - x^2 = n(n-2x)$. Entonces los $\frac{n-1}{2}$ residuos cuadráticos son: $1^2, 2^2, \cdots, \left(\frac{n-1}{2}\right)^2, \mod n$.

Por el pequeño teorema de Fermat, como $n$ es primo, $m^{n-1} \equiv 1 \mod n$, es decir,

$$(m^{\frac{n-1}{2}} - 1)(m^{\frac{n-1}{2}} + 1) \equiv 0 \mod n \tag{2.4}$$

Si $m$ es residuo cuadrático, digamos $m \equiv k^2 \mod n$, entonces $m^{\frac{n-1}{2}} \equiv k^{n-1} \equiv 1 \mod n$, nuevamente por el pequeño teorema de Fermat. Es decir cada residuo cuadrático anula al primer factor en (2.4). El resto de los residuos deben anular al segundo factor, pues en otro caso no se cumpliría el pequeño teorema de Fermat, entonces $m^{\frac{n-1}{2}} = -1$ si $m$ no es residuo cuadrático. Podemos concluir que

$$m^{\frac{n-1}{2}} = \left(\frac{m}{n}\right) \tag{2.5}$$

■

Demostraremos ahora algunos resultados concernientes a la transformada de Fourier discreta del símbolo de Legendre como función de su numerador que llamaremos función gaussianal discreta. Iniciamos con una definición.

**Definición 2.2.2** *Sea $n$ un primo impar, defínase para cada $k$ entero,*

$$h_n(k) = \left(\frac{k}{n}\right) \tag{2.6}$$

*y el correspondiente vector $h_n$ con coordenadas $h_n(k)$, mediante $h_n = \sum_{k=0}^{n-1} h_n(k)e_k$, con $(e_k)_{1\leq k\leq n}$ la base canónica de $\mathbb{C}^n$.*

**Lema 2.2.3** *Para cualquier $m, k \in \mathbb{Z}$, si $n$ no es divisor de $m$ ni de $k$, entonces se cumple que*

$$\left(\frac{mk}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{k}{n}\right) \tag{2.7}$$

**Demostración.** Por el criterio de Euler tenemos que

$$\left(\frac{mk}{n}\right) = (mk)^{\frac{n-1}{2}} = (m)^{\frac{n-1}{2}}(k)^{\frac{n-1}{2}} = \left(\frac{m}{n}\right)\left(\frac{k}{n}\right) \tag{2.8}$$

■

**Lema 2.2.4** *Para $n$ primo impar y $n, k$ primos relativos se cumple que*

$$\left(\frac{k}{n}\right) = \left(\frac{k^{-1}}{n}\right) \tag{2.9}$$

*módulo $n$.*

**Demostración.** Como k no es divisible por $n$, entonces $k$ tiene inverso en $\mathbb{Z}_n$, i.e., existe $k^{-1} \in \mathbb{Z}_n$ y $k\,k^{-1} = 1$. Ahora si $b^2 = k \mod n$ tenemos que

$$1 = \Big(\frac{kk^{-1}}{n}\Big) = \Big(\frac{k}{n}\Big)\Big(\frac{k^{-1}}{n}\Big) = 1\Big(\frac{k^{-1}}{n}\Big) = \Big(\frac{k^{-1}}{n}\Big) \tag{2.10}$$

Si $k$ no es residuo cuadrático y no es divisible por $n$, tenemos que $\left(\frac{k}{n}\right) = -1$ y consecuentemente

$$1 = \Big(\frac{kk^{-1}}{n}\Big) = \Big(\frac{k}{n}\Big)\Big(\frac{k^{-1}}{n}\Big) = -1\Big(\frac{k^{-1}}{n}\Big) \tag{2.11}$$

Por lo tanto,

$$\Big(\frac{k^{-1}}{n}\Big) = -1$$

Esto demuestra el lema. ■

Sea $p$ un entero, si $n$ es un primo impar solo hay un residuo de $p \mod n$ entre $-\frac{1}{2}n$ y $\frac{1}{2}n$. A éste residuo lo llamamos residuo mínimo de $p \mod n$, es positivo o negativo, dependiendo de que menor residuo no negativo de $p$ se encuentre entre 0 y $\frac{1}{2}n$ ó entre $\frac{1}{2}n$ y $n$. Recordemos que definimos $(m/n)$ como el símbolo de Legendre.

**Teorema 2.2.5** *Sea $\mu$ el número de miembros del conjunto*

$$\{m, 2m, 3m, \ldots, \frac{1}{2}(n-1)m\}$$

*cuyos residuos mínimos positivos* mód $n$ *sean mayores que $\frac{1}{2}n$ se tiene,*

$$\Big(\frac{m}{n}\Big) = (-1)^{\mu} \tag{2.12}$$

**Demostración.** Supongamos que $m$ es un número entero, positivo o negativo, no divisible por $n$, y considere los residuos mínimos de los $\frac{1}{2}(n-1)$ números

$$m, 2m, 3m, \ldots, \frac{1}{2}(n-1)m \tag{2.13}$$

podemos escribir estos residuos en la forma

$$r_1, r_2, \ldots, r_\lambda, -r_1^{'}, -r_2^{'}, \ldots, -r_\mu^{'}$$

donde

$$\lambda + \mu = \frac{n-1}{2}, \quad 0 < r_i \leq \frac{n}{2}, \quad 0 < r_i^{'} < \frac{n}{2}$$

Dado que los números (2.13) no son congruentes mód $n$, ningún par de $r$'s pueden ser iguales y lo mismo ocurre con los $r^{'}$. Si un $r$ y un $r^{'}$ son iguales, digamos $r_i = r_j^{'}$, sean $am$ y $bm$ los dos números de (2.13) tales que,

$$am \equiv r_i,\ bm \equiv -r_j^{'} \quad \text{mód } n$$

después

$$\begin{aligned} am + bm &\equiv 0 \quad \text{mód } n \\ a + b &\equiv 0 \quad \text{mód } n \end{aligned} \tag{2.14}$$

lo cual no es posible porque $0 < a < \frac{1}{2}n$, $0 < b < \frac{1}{2}n$. De esto se deduce que los números $r_i, r_j^{'}$ son un reordenamiento de los números

$$1, 2, \ldots, \frac{1}{2}(n-1);$$

y por lo tanto tenemos que

$$\begin{aligned} m \cdot 2m \cdots \frac{1}{2}(n-1)m &\equiv (-1)^{\mu} 1 \cdot 2 \cdots \frac{1}{2}(n-1) \quad \text{mód } n \\ \text{así que } m^{\frac{1}{2}(n-1)} &\equiv (-1)^{\mu} \quad \text{mód } n \end{aligned} \tag{2.15}$$

Pero

$$\left(\frac{m}{n}\right) \equiv m^{\frac{1}{2}(n-1)} \quad \text{mód } n \tag{2.16}$$

por el Criterio de Euler. ■

**Corolario 2.2.6** *Si $n$ es primo impar, entonces*

$$\left[\frac{m}{n}\right] = \left(\frac{m}{n}\right)$$

**Demostración.** Es una consecuencia de los teoremas (2.1.3) y (2.2.5). ■

Escribimos $[x]$ para referirnos a la parte entera de $x$, el entero más grande que no excede a $x$. De este modo tenemos el siguiente teorema

**Teorema 2.2.7** *Se cumplen las identidades,*

*(i)* $\left(\frac{2}{n}\right) = (-1)^{[\frac{1}{4}(n+1)]}$

*(ii)* $\left(\frac{2}{n}\right) = (-1)^{[\frac{1}{8}(n^2-1)]}$

*Por lo tanto, 2 es residuo cuadrático de los primos de la forma $8l \pm 1$ no es un residuo cuadrático de los primos de la forma $8l \pm 3$..*

**Demostración.** Tomemos $m = 2$, de modo que los números en (2.13) son $2, 4, \ldots, n-1$. En este caso $\lambda$ es el número de enteros pares positivos menores que $\frac{1}{2}n$. Con esta notación $\lambda = [\frac{1}{4}n]$, pero

$$\begin{aligned} \lambda + \mu =& \frac{1}{2}(n-1) \\ \mu =& \frac{1}{2}(n-1) - [\frac{1}{4}n] \end{aligned} \tag{2.17}$$

Si $n \equiv 1 \mod 4$, es de la forma $n = 4k+1$, $k \in \mathbb{Z}$ entonces

$$\mu = \frac{1}{2}(n-1) - \frac{1}{4}(n-1) = \frac{1}{4}(n-1) = \frac{1}{4}((4k+1)-1) = \frac{1}{4}(4k) = k = [\frac{1}{4}(n+1)]$$

pues

$$[\frac{1}{4}(n+1)] = [\frac{1}{4}(4k+2)] = [k + \frac{1}{2}] = k$$

Y si $n \equiv 3 \mod 4$, es de la forma $n = 4k+3$, $k \in \mathbb{Z}$ entonces

$$\mu = \frac{1}{2}(n-1) - \frac{1}{4}(n-3) = \frac{1}{4}(n+1) = \frac{1}{4}((4k+3)+1) = \frac{1}{4}(4k+4) = k+1 = [\frac{1}{4}(n+1)]$$

pues

$$[\frac{1}{4}(n+1)] = [\frac{1}{4}(4k+4)] = [k+1] = k+1$$

Por eso

$$\left(\frac{2}{n}\right) \equiv (-1)^{[\frac{1}{4}(n+1)]} \mod n$$

es decir

$$\left(\frac{2}{n}\right) = 1 \text{ si } n = 8l+1 \text{ ó } 8l-1$$

,

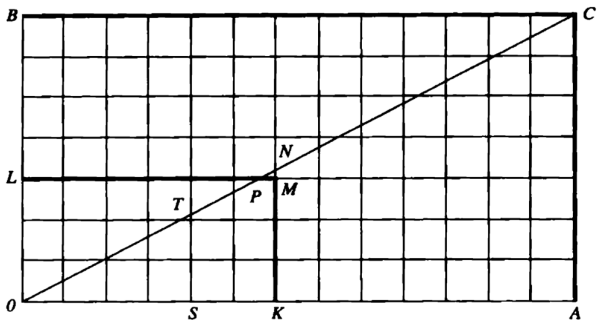
$$\left(\frac{2}{n}\right) = -1 \text{ si } n = 8l+3 \text{ ó } 8l-3$$

Si $n = 8l \pm 1$ entonces $\frac{1}{8}(n^2-1)$ es par, mientras que si $n = 8l \pm 3$, es impar. Por eso

$$(-1)^{[\frac{1}{4}(n+1)]} = (-1)^{[\frac{1}{8}(n^2-1)]}$$

■

**Teorema 2.2.8** *Sean $n' = \frac{n-1}{2}$, $m' = \frac{m-1}{2}$ con $m, n$ primos impares. Si $S(m,n) = \sum_{s=1}^{n'}[\frac{sm}{n}]$ entonces $S(m,n) + S(n,m) = n'm'$.*




**Demostración.** La demostración puede expresarse en forma geométrica. En la siguiente figura AC y BC son $x = n, y = m$, y KM y LM son $x = n^{'}, y = m^{'}$.

Si $n > m$, entonces $m^{'}/n^{'} < m/n < 1$, por lo tanto M está por debajo de la diagonal OC. Como

$$m^{'} < \frac{mn^{'}}{n} < m^{'} + 1,$$

no hay ningún número entero entre KM $= m^{'}$ y KN $= mn^{'}/n$. Contamos de dos maneras diferentes el número de puntos de la red en el rectángulo OKML, contando los puntos en KM y LM pero no los que están sobre los ejes. En primer lugar, este número es claramente $n^{'}m^{'}$. Pero no hay puntos de la reticula sobre OC, pues en caso contrario si $p$ y $q$ son tales que $\frac{q}{p} = \frac{m}{n}$, equivalentemente $qn = pm$, pero $n$ y $m$ son primos, entonces $m$ es factor primo de $q$ y $n$ factor primo de $p$ lo cual implica $n > p$ y $m > q$ lo cual es imposible dentro de la retícula. Además, no hay ningún punto de la retícula en el triángulo PMN excepto quizás sobre PM. Por lo tanto el número de puntos de red en OKML es la suma de los triángulos OKN y OLP, contando aquellos sobre KN y LP pero no sobre los ejes. El número de puntos sobre ST, la línea $x = s$ es $[sm/n]$, ya que $sm/n$ es la ordenada de T. Por lo tanto el número total de puntos sobre OKN es

$$\sum_{s=1}^{n^{'}} [\frac{sm}{n}] = S(m, n).$$

De la misma manera, el número en OLP es $S(n, m)$, y se sigue la conclusión. ■

**Corolario 2.2.9** ***(Ley de reciprocidad cuadrática)*** *Para $m$ y $n$ primos impares se cumple la fórmula de Gauss para la reciprocidad cuadrática*

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{(\frac{n-1}{2})(\frac{m-1}{2})} \tag{2.18}$$

**Demostración.** Sean $n^{'} = \frac{n-1}{2}$ y $m^{'} = \frac{m-1}{2}$. Podemos escribir

$$km = n\left[\frac{kn}{n}\right] + u_k \tag{2.19}$$

donde $1 \leq k \leq n^{'}$, $1 \leq u_k \leq n-1$. Aquí $u_k$ es el menor residuo positivo de $km \mod n$. Si $u_k = v_k \leq n^{'}$, entonces $u_k$ es uno de los residuos minimos $r_i$ como se definen en la prueba del teorema 2.2.5, mientras que si $u_k = w_k > n^{'}$, entonces $u_k - n$ es uno de los residuos minimos $-r_j^{'}$, de modo que $r_j = v_k$, $r_j^{'} = n - w_k$ para cada $i, j$ y algún $k$. Los $r_j$ y $r_j^{'}$ son (como vimos en el teorema 2.2.5) los números $1, 2, \ldots, n^{'}$, en algún orden. Por lo tanto, si

$$R = \sum r_i = \sum v_k, \quad R^{'} = \sum r_j^{'} = \sum (n - w_k) = \mu n - \sum w_k$$

(donde $\mu$ es como 6.11, el número de los $r_j^{'}$)., tenemos que

$$R + R^{'} = \sum_{v=1}^{n^{'}} v = \frac{1}{2}\frac{n-1}{2}\frac{n+1}{2} = \frac{n^2-1}{8}$$

y entonces

$$\mu n + \sum v_k - \sum w_k = \frac{n^2-1}{8} \tag{2.20}$$

Por otro lado, sumando (2.19) de $k = 1$ hasta $k = n^{'}$, tenemos

$$\frac{m(n^2-1)}{8} = nS(m,n) + \sum u_k = nS(m,n) + \sum v_k + \sum w_k \tag{2.21}$$

De (2.20) y (2.21) deducimos

$$\frac{(n^2-1)(m-1)}{8} = nS(m,n) + 2\sum w_k - \mu n \tag{2.22}$$

Ahora $m-1$ es par, y $n^2 - 1 \equiv 0 \mod 8$., de modo que el lado izquierdo de (2.22) es par, y también el segundo término de la derecha. Por lo tanto (ya que $n$ es impar)

$$S(m,n) \equiv \mu \mod 2,$$

y por el teorema 2.2.5,

$$\left(\frac{m}{n}\right) = (-1)^{\mu} = (-1)^{S(m,n)}$$

Finalmente

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{S(m,n)+S(n,m)} = (-1)^{n^{'}m^{'}}$$

por el teorema 2.2.8. ■

# Capítulo 3

# Transformada de Fourier discreta I

A continuación presentamos la definición de la transformada de Fourier en términos de la base ortonormal canónica que explícitamente podemos ver en su representación matricial como se define en la siguiente sección. Además de demostrar que la transformada de Fourier es unitaria y algunas propiedades de la misma que involucran su traza y la relación que ésta tiene con el símbolo de Legendre, así como la función $h_n$ que es una función propia de la transformada de Fourier que a su vez la transformada de $h_n$ resulta ser una suma de Gauss bajo ciertas condiciones.

## 3.1. Definición de la Transformada de Fourier Discreta

Sea $n \geq 1$ y $\{e_1, e_2, ..., e_n\}$ la base ortonormal canónica de $\mathbb{C}^n$, el cual es un espacio de Hilbert con producto interno $\langle \cdot, \cdot \rangle$ lineal en la primera coordenada y lineal conjugado en la segunda.

**Definición 3.1.1** *Para cada $1 \leq j, k \leq n$ definimos la transformación lineal (proyector básico) $|e_j\rangle\langle e_k| : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ mediante la correspondencia*

$$|e_j\rangle\langle e_k|u = \langle e_k, u\rangle e_j, \quad \forall u \in \mathbb{C}^n. \tag{3.1}$$

La matriz de $|e_j\rangle\langle e_k|$ respecto de la base canónica, consiste de la unidad en la entrada $j, k$ y ceros en las entradas restantes.

En general para cada par $u, v \in \mathbb{C}^n$ se define el proyector $|u\rangle\langle v|$ mediante, $|u\rangle\langle v|w = \langle v, w\rangle u, \quad \forall w \in \mathbb{C}^n$.

Usaremos esta notación para escribir la transformada de Fourier.

En muchas aplicaciones, la transformada de Fourier discreta de dimensión $n$, $F(n)$ con $n$ un entero positivo, es la matriz $n \times n$ cuya entrada en la fila $j$ y la columna $k$, $1 \leq j, k \leq n$, es el número

$$F(n)_{jk} = \frac{1}{\sqrt{n}}\, e^{2\pi ijk/n}$$

donde $i$ es la unidad imaginaria. Nosotros preferimos definir la transformada de Fourier discreta como una combinación lineal de los proyectores $|e_j\rangle\langle e_k|, \ \ 1 \leq j, k \leq n$.

**Definición 3.1.2** *Sea $n$ un entero positivo, se define $F(n) : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ como la aplicación dada por*

$$F(n) := \frac{1}{\sqrt{n}} \sum_{j,k=1}^{n} e^{2\pi ijk/n} |e_j\rangle\langle e_k|$$

Obsérvese que

$$\begin{aligned} F(n)_{jk} =& \langle e_j, F(n)e_k\rangle = \Big\langle e_j, \frac{1}{\sqrt{n}} \sum_{j',k'=1}^{n} e^{2\pi ij'k'/n} |e_{j'}\rangle\langle e_{k'}|e_k\Big\rangle \\ =& \frac{1}{\sqrt{n}} \sum_{j',k'=1}^{n} e^{2\pi ij'k'/n} \langle e_j, |e_{j'}\rangle\langle e_{k'}, e_k\rangle = \frac{1}{\sqrt{n}} e^{2\pi ijk/n}, \end{aligned} \tag{3.2}$$

lo cual explica nuestra definición.

**Ejemplo 3.1.3** *Si $n = 3$ usando (3.2) se obtiene $F(3)_{jk} = \frac{1}{\sqrt{3}} e^{2\pi ijk/3}$. Entonces $F(3)_{jk} = \frac{1}{\sqrt{3}}$ si $j = 3,\ k = 1, 2$; $j = 1, 2,\ k = 3$ y $j = 3,\ k = 3$, $F(3)_{jk} = \frac{1}{\sqrt{3}} e^{4\pi i/3}$ si $j = 1;\ k = 2$; o $j = 2,\ k = 1$ y $F(3)_{11} = \frac{1}{\sqrt{3}} e^{2\pi i/3}$, $F(3)_{22} = \frac{1}{\sqrt{3}} e^{8\pi i/3}$, i.e.,*

$$F(3) = \frac{1}{\sqrt{3}} \begin{pmatrix} e^{2\pi i/3} & e^{4\pi i/3} & 1 \\ e^{4\pi i/3} & e^{8\pi i/3} & 1 \\ 1 & 1 & 1 \end{pmatrix} \tag{3.3}$$

En Análisis Armónico, la transformada de Fourier discreta se define de una manera, aparentemente diferente, en términos de caracteres.

Denótese mediante $\mathbb{C}^\times(n)$ al grupo multiplicativo de números complejos $e^{2\pi ik/n}$, $0 \leq k < n - 1$, llamado también grupo de raíces $n$-ésimas de la unidad.

**Definición 3.1.4** *Sea $\hat{\mathbb{Z}}_n$ el conjunto de homomorfismos $h : \mathbb{Z}_n \longrightarrow \mathbb{C}^\times(n)$, con la estructura de grupo definida mediante*

$$(h_1 + h_2)(j) = h_1(j)h_2(j)$$

*con $h_1, h_2 \in \hat{\mathbb{Z}}_n$, $j \in \mathbb{Z}_n$*

Al grupo $\hat{\mathbb{Z}}_n$ se le denomina grupo de caracteres de $\mathbb{Z}_n$ y es isomorfo a $\mathbb{Z}_n$.

**Ejemplo 3.1.5** *Sea $h(j) = e^{\frac{2\pi ij}{n}}$, $j \in \mathbb{Z}_n$. Veamos que $h$ es un homomorfismo,*

$$h(j + j') = e^{\frac{2\pi i(j+j')}{n}} = e^{\frac{2\pi ij}{n}} \cdot e^{\frac{2\pi ij'}{n}} = h(j) \cdot h(j')$$

*entonces $h$ es un homomorfismo.*

Usaremos la notación $(j,h) = h(j)$, $j \in \mathbb{Z}_n$, $h \in \hat{\mathbb{Z}}_n$

El espacio $L_2(\mathbb{Z}_n)$, consiste de todas las funciones complejas $f : \mathbb{Z}_n \longrightarrow \mathbb{C}$.

**Definición 3.1.6** *Sean $f, g \in L_2(\mathbb{Z}_n)$. Definimos su producto interno como se sigue:*

$$\langle f, g\rangle = \sum_{j=1}^{n} f(j)\overline{g(j)}.$$

Si $f = g$ se tiene

$$\|f\|^2 := \langle f, f\rangle = \sum_{j=1}^{n} f(j)\overline{f(j)} = \sum_{j=1}^{n} |f(j)|^2$$

De manera análoga se define el espacio $L_2(\hat{\mathbb{Z}}_n)$.

Podemos identificar a la función $f \in L_2(\mathbb{Z}_n)$ con el conjunto o vector de sus valores, así

$$f = (f_0, f_1, \cdots, f_{n-1})$$

Mediante esta identificación resulta que $L_2(\mathbb{Z}_n)$ coincide con $\mathbb{C}^n$. En efecto, la aplicación $f \mapsto (f_0, f_1, \cdots, f_{n-1})$ define un isomorfismo isométrico de $L_2(\mathbb{Z}_n)$ sobre $\mathbb{C}^n$ con la norma euclideana, pues

$$\|f\|^2 = \sum_{j=0}^{n-1} |f_j|^2 = \|(f_0, f_1, \cdots, f_{n-1})\|^2_{\mathbb{C}^n}$$

En términos de los caracteres de $\hat{\mathbb{Z}}_n$, la transformada de Fourier $F(n)$ se define como la transformación $F(n) : L_2(\mathbb{Z}_n) \longrightarrow L_2(\hat{\mathbb{Z}}_n)$ dada por

$$(F(n)f)(h) := \frac{1}{\sqrt{n}} \sum_{j\in\mathbb{Z}_n} f(j)(j,h) = \frac{1}{\sqrt{n}} \sum_{j\in\mathbb{Z}_n} f(j)h(j) \tag{3.4}$$

¿Cómo se relacionan las dos definiciones de $F(n)$?

**Proposición 3.1.7** *Sea $r : \mathbb{Z}_n \longrightarrow \mathbb{C}^\times(n)$ la función definida mediante $r(j) = e^{2\pi ij/n}$. entonces $r$ es un isomorfismo.*

**Demostración.** Para cada $j, k \in \mathbb{Z}_n$ tenemos que

$$r(j+k) = e^{2\pi i(j+k)/n} = r(j)r(k)$$

lo cual demuestra que $r$ es un homomorfismo. Como $r(j) = 1$, $j \in \mathbb{Z}_n$ si y sólo si $j = 0$. Entonces $r$ es inyectivo. Ahora, si $z$ es una raíz $n$-ésima de la unidad, i.e., $z^n = 1$, entonces si $z = |z|e^{i\theta}$, $z^n = |z|^n e^{in\theta} = 1$, lo cual implica que $|z| = 1$ y $n\theta = 2\pi j$ para algún $j \in \mathbb{Z}_n$, consecuentemente $\theta = 2\pi j/n$. Esto demuestra que $z = e^{2\pi ij/n}$, es decir, $r$ es suprayectivo. ■

Consideremos ahora la aplicación $s : \mathbb{Z}_n \longrightarrow \hat{\mathbb{Z}}_n$ definida para cada $j \in \mathbb{Z}_n$ mediante

$$s(j) : \mathbb{Z}_n \longrightarrow \mathbb{C}^\times_n, \quad s(j)(k) = \big(k, s(j)\big) = e^{2\pi ijk/n}$$

**Proposición 3.1.8** *La aplicación $s : \mathbb{Z}_n \longrightarrow \hat{\mathbb{Z}}_n$ es un isomorfismo.*

**Demostración.** Para cada $j, k \in \mathbb{Z}_n$,

$$s(j+k)(l) = e^{2\pi i(j+k)l/n} = s(j)(l)s(k)(l) = \big(s(j)s(k)\big)(l),\ \forall\, l \in \mathbb{Z}_n$$

Por lo tanto $s(j+k) = s(j)s(k),\ \forall\, j, k \in \mathbb{Z}_n$, i.e., $s$ es un homomorfismo.

Ahora, si $s(j) = 1 \in \mathbb{C}_n^{\times}$, i.e., $s(j)(k) = 1(k) = 1,\ \forall\, k \in \mathbb{Z}_n$, entonces $e^{2\pi ijk/n} = 1$ para todo $k \in \mathbb{Z}_n$, lo cual implica que $j = 0$. Entonces $s$ es inyectiva.

Finalmente, si $h \in \hat{\mathbb{Z}}_n$, i.e., $h$ es un homomorfismo $h : \mathbb{Z}_n \longrightarrow \mathbb{C}^{\times}(n)$, entonces $h(1)^n = h(1+1+\cdots+1) = h(n) = h(0) = 1$, i.e., $h(1) \in \mathbb{C}$ es una raíz $n$-ésima de 1. Esto implica que $h(1) = e^{2\pi ij/n} = s(j)$ para alguna $j \in \mathbb{Z}_n$. Por lo tanto $s(j)(k) = e^{2\pi ijk/n} = (e^{2\pi ij/n})^k = h(1)^k = h(k),\ \forall\, k \in \mathbb{Z}_n$, i.e., $s(j) = h$. Esto completa la demostración. ■

Identificando $k$ con $s(k)$ a partir de (3.4) se obtiene

$$(F(n)f)(k) := \frac{1}{\sqrt{n}} \sum_{j \in \mathbb{Z}_n} f(j) e^{2\pi ijk/n} \tag{3.5}$$

La transformada de Fourier discreta $F(n)$ de $\mathbb{Z}_n$ como el mapeo lineal de $L_2(\mathbb{Z}_n)$ en sí mismo está definida para $f \in L_2(\mathbb{Z}_n)$ por

$$(F(n)f)(\alpha) = \frac{1}{\sqrt{n}} \langle f, \lambda_\alpha \rangle = \frac{1}{\sqrt{n}} \sum_{a \in \mathbb{Z}_n} f(a) e^{2\pi i \alpha a/n}$$

donde $\alpha \in \mathbb{Z}_n$.

Demostremos la propiedad de unitariedad $F(n)F(n)^* = I = F(n)^* F(n)$, i.e.,

$$\begin{aligned} \big(F(n)e_b\big)(\alpha) =& \frac{1}{\sqrt{n}} \langle e_b, \lambda_\alpha \rangle = \frac{1}{\sqrt{n}} \sum_{a \in \mathbb{Z}_n} e_b(a) \overline{\lambda_\alpha}(a) = \frac{1}{\sqrt{n}} \sum_{a \in \mathbb{Z}_n} \delta_{ba} \overline{\lambda_\alpha}(a) \\ =& \frac{1}{\sqrt{n}} \overline{\lambda_\alpha}(b) = \frac{1}{\sqrt{n}} e^{2\pi ib\alpha/n} = \frac{1}{\sqrt{n}} \lambda_{-b}(\alpha),\ \ \forall\ \alpha \in \mathbb{Z}_n \end{aligned} \tag{3.6}$$

entonces $F(n)e_b = \frac{1}{\sqrt{n}} \lambda_{-b}$. Así mismo

$$\big(F(n)\lambda_\alpha\big)(\beta) = \frac{1}{\sqrt{n}} \langle \lambda_\alpha, \lambda_\beta \rangle = \frac{n}{\sqrt{n}} \delta_{\alpha\beta} = \sqrt{n} e_\alpha(\beta),\ \ \forall\ \beta \in \mathbb{Z}_n,$$

i.e., $F(n)\lambda_\alpha = \sqrt{n} e_\alpha$. Así que

$$\begin{aligned} F(n)^2 e_a =& e_{-a} \\ \text{y}\quad F(n)^4 =& I \end{aligned} \tag{3.7}$$

donde $I$ es el mapeo identidad. Además,

$$\langle F(n)e_a, F(n)e_b \rangle = \frac{1}{n} \langle \lambda_{-a}, \lambda_{-b} \rangle = \left\{ \begin{array}{llll} 1 & si & a = b, \\ 0 & si & a \neq b \end{array} \right\} = \langle e_a, e_b \rangle$$

Por eso $\langle F(n)e_a, F(n)e_b\rangle = \langle e_a, e_b\rangle$, i.e., $F(n)$ es un operador unitario, $F(n)F(n)^* = F(n)^*F(n) = I$, en $L_2(\mathbb{Z}_n)$ e idempotente de orden 4.

Tenemos que

$$\begin{aligned}\langle f, F(n)g\rangle =& \sum_{b\in\mathbb{Z}_n} f(b)\overline{\big(F(n)g(b)\big)} = \frac{1}{\sqrt{n}}\sum_{b\in\mathbb{Z}_n} f(b)\sum_{a\in\mathbb{Z}_n}\overline{f(a)}e^{-2\pi iba/n}\\ =&\frac{1}{\sqrt{n}}\sum_{a\in\mathbb{Z}_n}\sum_{b\in\mathbb{Z}_n} f(b)e^{-2\pi iba/n}\overline{f(a)} = \langle F(n)^*f, g\rangle\end{aligned} \tag{3.8}$$

entonces $\big(F(n)^*f\big)(a) = \frac{1}{\sqrt{n}}\sum_{b\in\mathbb{Z}_n} f(b)e^{-2\pi iba/n} = \frac{1}{\sqrt{n}}\langle f, \lambda_{-a}\rangle$.

$$(F(n)^{-1}f)(\alpha) = \big(F(n)^*f\big)(\alpha) = \frac{1}{\sqrt{n}}\langle f, \lambda_{-a}\rangle = \frac{1}{n}\sum_{\beta\in\mathbb{Z}_n} f(\beta)e^{-2\pi i\alpha\beta/n}.$$

Como

$$F(n)e_\beta(\alpha) = \frac{1}{\sqrt{n}}\langle e_\beta, \lambda_\alpha\rangle = \frac{1}{\sqrt{n}}\sum_{\gamma\in\mathbb{Z}_n} e^{2\pi i\gamma\beta/n}e_\gamma(\alpha)$$

se sigue que la matriz de $F(n)$ con respecto a la base $e_\beta$, $\beta\in\mathbb{Z}_n$, esta dada por

$$F(n) = \Big(\frac{1}{\sqrt{n}}(e^{2\pi i\beta\gamma/n})\Big)_{0\le\beta,\gamma<n} \tag{3.9}$$

Aunque la transformación lineal $F(n)$ está representada por diferentes matrices con respecto a diferentes bases, también denotaremos la matriz anterior por $F(n)$. Como $\rho(a)\in U(n)$, $a\in\mathbb{Z}_n^\times$ y $F(n)\in U(n)$ podemos formar $F(n)\rho(a)F(n)^{-1}$. Como $\big(\rho(a)\lambda_\alpha\big)(z) = \lambda_\alpha(az) = e^{-2\pi i\alpha az} = \lambda_{a\alpha}(z)$ y así se tiene que

$$\begin{aligned}\Big(F(n)\rho(a)F(n)^{-1}f\Big)(\alpha) =&F(n)\rho(a)\big(\frac{1}{\sqrt{n}}\sum_{\beta\in\mathbb{Z}_n} f(\beta)e^{-2\pi i\alpha\beta/n}\big)\\ =&F(n)\frac{1}{\sqrt{n}}\sum_{\beta\in\mathbb{Z}_n} f(\beta)\big(\rho(a)\lambda_\alpha\big)(\beta)\\ =&\frac{1}{\sqrt{n}}\sum_{\beta\in\mathbb{Z}_n} f(\beta)\big(F(n)\lambda_{\alpha a}\big)(\beta) = \sqrt{n}\frac{1}{\sqrt{n}}\sum_{\beta\in\mathbb{Z}_n} f(\beta)e_{\alpha a}(\beta)\\ =&\sum_{\beta\in\mathbb{Z}_n} f(\beta)\big(\rho(a^{-1})e_\alpha\big)(\beta) = \rho(a^{-1})\sum_{\beta\in\mathbb{Z}_n} f(\beta)e_\alpha(\beta)\\ =&\rho(a^{-1})f(\alpha)\end{aligned} \tag{3.10}$$

Entonces, $F(n)\rho(a)F(n)^{-1} = \rho(a^{-1}) = \rho(a)^{-1}$.

## 3.2. Algunas propiedades de la Transformada de Fourier Discreta

Ahora podemos relacionar los resultados anteriores con el lema 4.3.2 y el valor de las sumas cuadráticas de Gauss. Si $\mathrm{Tr}(\cdot)$ denota la traza de la transformación lineal dentro del paréntesis, inmediatamente obtenemos de (3.9) que

$$\begin{aligned}\mathrm{Tr}(F(n)) =& \frac{1}{\sqrt{n}} \sum_{\alpha\in\mathbb{Z}_n} e^{2\pi i\alpha^2/n},\\ \mathrm{Tr}(\rho(a)F(n)) =& \frac{1}{\sqrt{n}} \sum_{\alpha\in\mathbb{Z}_n} e^{2\pi ia\alpha^2/n}\end{aligned} \tag{3.11}$$

Pues

$$\begin{aligned}\rho(a)F(n)e_\beta(\alpha) =& \rho(a)\frac{1}{\sqrt{n}}\langle e_\beta, \lambda_\alpha\rangle = \frac{1}{\sqrt{n}} \sum_{\gamma\in\mathbb{Z}_n} e^{2\pi i\gamma\beta/n}\rho(a)e_\gamma(\alpha)\\ =& \frac{1}{\sqrt{n}} \sum_{\gamma\in\mathbb{Z}_n} e^{2\pi i\gamma\beta/n}e_{\gamma a^{-1}}(\alpha) = \frac{1}{\sqrt{n}} \sum_{\gamma\in\mathbb{Z}_n} e^{2\pi i\gamma a\beta/n}e_\gamma(\alpha)\end{aligned} \tag{3.12}$$

entonces la matriz de $\rho(a)F(n)$ es $\frac{1}{\sqrt{n}}\left(e^{2\pi i\gamma a\beta/n}\right)_{0\le\gamma,\beta<n}$

Sean $e_\alpha \in L_2(\mathbb{Z}_n)$, $0 \le \alpha < n$, $e_\beta \in L_2(\mathbb{Z}_m)$, $0 \le \beta < m$, bases ortonormales de $L_2(\mathbb{Z}_n)$ y $L_2(\mathbb{Z}_m)$, respectivamente y sea $e_\gamma$, $0 \le \gamma < nm$ una base ortonormal de $L_2(\mathbb{Z}_{nm})$. Definimos $\chi(e_\alpha, e_\beta) = e_{\alpha m+\beta n}$ y extendemos por linealidad $\chi$ a una aplicación bilineal de $L_2(\mathbb{Z}_n) \times L_2(\mathbb{Z}_m) \to L_2(\mathbb{Z}_{nm})$. Por la propiedad universal del producto tensorial, $\chi$ induce una aplicación lineal $\chi^* : L_2(\mathbb{Z}_n) \otimes L_2(\mathbb{Z}_m) \to L_2(\mathbb{Z}_{nm})$ tal que $\chi^*(e_\alpha \otimes e_\beta) = \chi(e_\alpha, e_\beta)$, entonces para cualesquiera $v$ y $w$ expresados en términos de los básicos, tenemos

$$\chi(v, w) = \chi(\sum_\alpha x_\alpha e_\alpha, \sum_\beta y_\beta e_\beta) = \sum_\alpha \sum_\beta x_\alpha y_\beta \chi(e_\alpha, e_\beta) = \chi^*(v \otimes w)$$

es decir $\chi^*$ existe y esta determinada en forma única. Veamos que $\chi^*$ es un isomorfismo. Si $\chi^*(u) = 0$, para algún $u = \sum_{\alpha,\beta} u_{\alpha\beta} e_\alpha \otimes e_\beta$, entonces

$$\sum_{\alpha,\beta} u_{\alpha\beta} e_{\alpha m+\beta n} = 0$$

y por la independencia lineal se obtiene $u_{\alpha\beta} = 0$ para todo par $(\alpha, \beta)$, i.e., $u = 0$. Y cada $v = \sum v_{\alpha\beta} e_{\alpha m+\beta n}$ es la imagen bajo $\chi^*$ del vector $u = \sum v_{\alpha\beta} e_\alpha \otimes e_\beta$. Esto demuestra que $\chi^*$ es un isomorfismo.

Tenemos el siguiente diagrama

$$\begin{array}{ccc} L_2(\mathbb{Z}_n) \otimes L_2(\mathbb{Z}_m) & \xrightarrow{\rho(m)F(n)\otimes\rho(n)F(m)} & L_2(\mathbb{Z}_n) \otimes L_2(\mathbb{Z}_m) \\ \downarrow \chi^* & & \downarrow \chi^* \\ L_2(\mathbb{Z}_{nm}) & \xrightarrow[\chi^*\rho(m)F(n)\otimes\rho(n)F(m)\chi^{*-1}]{} & L_2(\mathbb{Z}_{nm}) \end{array}$$

**Proposición 3.2.1** *El producto tensorial de los operadores lineales $\rho(m)F(n)$ y $\rho(n)F(m)$ satisfacen*

$$\chi^*\rho(m)F(n)\otimes\rho(n)F(m)\chi^{*-1}=F(nm) \tag{3.13}$$

**Demostración.** Como $\chi(e_\alpha,e_\beta)=e_{\alpha m+\beta n}\ \in L_2(\mathbb{Z}_{nm})$, al aplicar el operador inverso $\chi^{*-1}$ se tiene $\chi^{*-1}e_{\alpha m+\beta n}=e_\alpha\otimes e_\beta$. Ahora

$$\rho(m)F(n)\otimes\rho(n)F(m)\ e_\alpha\otimes e_\beta=\rho(m)F(n)e_\alpha\otimes\rho(n)F(m)e_\beta$$

y aplicando el resultado de la ecuación (3.12), resulta

$$\begin{aligned}\rho(m)F(n)e_\alpha\otimes\rho(n)F(m)e_\beta=&\frac{1}{\sqrt{n}}\sum_{\alpha'\in\mathbb{Z}_n}e^{2\pi i\alpha' m\alpha/n}e_{\alpha'}\otimes\frac{1}{\sqrt{m}}\sum_{\beta'\in\mathbb{Z}_m}e^{2\pi i\beta' n\beta/m}e_{\beta'}\\ =&\frac{1}{\sqrt{nm}}\sum_{\substack{\alpha'\in\mathbb{Z}_n\\ \beta'\in\mathbb{Z}_m}}e^{2\pi i(\alpha'\alpha m/n\ +\ \beta'\beta n/m)}e_{\alpha'}\otimes e_{\beta'}\end{aligned} \tag{3.14}$$

Por lo tanto

$$\begin{aligned}\chi^*\rho(m)F(n)\otimes\rho(n)F(m)\chi^{*-1}e_{\alpha m+\beta n}=&\chi^*\Big(\frac{1}{\sqrt{nm}}\sum_{\substack{\alpha'\in\mathbb{Z}_n\\ \beta'\in\mathbb{Z}_m}}e^{2\pi i(\alpha'\alpha m/n\ +\ \beta'\beta n/m)}e_{\alpha'}\otimes e_{\beta'}\Big)\\ =&\frac{1}{\sqrt{nm}}\sum_{\substack{\alpha'\in\mathbb{Z}_n\\ \beta'\in\mathbb{Z}_m}}e^{2\pi i(\alpha'\alpha m/n\ +\ \beta'\beta n/m)}e_{\alpha' m+\beta' n}\\ =&\frac{1}{\sqrt{nm}}\sum_{\gamma'\in\mathbb{Z}_{nm}}e^{2\pi i\gamma'\gamma/nm}e_{\gamma'}\\ =&F(nm)e_\gamma\end{aligned} \tag{3.15}$$

donde hemos hecho el cambio de variable $\gamma'=\alpha' m+\beta' n$ y usado que

$$\begin{aligned}\frac{\gamma'\gamma}{nm}=&\frac{(\alpha' m+\beta' n)(\alpha m+\beta n)}{nm}\\ =&\frac{\alpha'\alpha m}{n}+\frac{\beta'\beta n}{m}+\frac{\alpha' m\beta n}{mn}+\frac{\beta' n\alpha m}{nm}\\ =&\frac{\alpha'\alpha m}{n}+\frac{\beta'\beta n}{m}+\alpha'\beta+\beta'\alpha\end{aligned} \tag{3.16}$$

lo cual lleva a

$$e^{2\pi i\gamma'\gamma/nm}=e^{2\pi i(\alpha'\alpha m/n\ +\ \beta'\beta n/m)}$$

La última identidad se obtiene al usar la identidad que precede a (3.9). ■

Más adelante podemos ver que de (3.11) el lema 4.3.2 se escribe en la forma

$$\mathrm{Tr}\big(\rho(m)F(n)\big)=\Big(\frac{m}{n}\Big)\,\mathrm{Tr}F(n),\ \ m\not\equiv 0\mod n \tag{3.17}$$

con $n$ un primo impar.

**Corolario 3.2.2** *Para $m$ y $n$ primos impares se cumple que*

$$\Big(\frac{n}{m}\Big)\Big(\frac{m}{n}\Big) = \frac{\mathrm{Tr}F(nm)}{\mathrm{Tr}F(n)\mathrm{Tr}F(m)} \tag{3.18}$$

**Demostración.** De la ecuación (3.13) se obtiene

$$\mathrm{Tr}F(nm) = \mathrm{Tr}\big(\chi^*\rho(m)F(n)\otimes\rho(n)F(m)\chi^{*-1}\big)$$

Pero $\chi^*$ es un operador unitario y por la propiedad de ciclicidad de la traza se obtiene aplicando (3.17)

$$\begin{aligned}\mathrm{Tr}F(nm) =& \mathrm{Tr}\big(\rho(m)F(n)\otimes\rho(n)F(m)\big) = \mathrm{Tr}\big(\rho(m)F(n)\big)\mathrm{Tr}\big(\rho(n)F(m)\big)\\ =& \Big(\frac{m}{n}\Big)\mathrm{Tr}F(n)\Big(\frac{n}{m}\Big)\mathrm{Tr}F(m)\end{aligned} \tag{3.19}$$

■

**Corolario 3.2.3** *Si $m$ y $n$ son primos impares se cumple que*

$$\frac{\mathrm{Tr}F(nm)}{\mathrm{Tr}F(n)\mathrm{Tr}F(m)} = (-1)^{(\frac{n-1}{2})(\frac{m-1}{2})} \tag{3.20}$$

**Demostración.** Es una consecuencia inmediata de (2.18) y (3.18). ■

Usando $h_n$ como se define en 2.2.2, se tiene el siguiente lema.

**Lema 3.2.4** *Sea $n$ un primo impar, para cada $k$ entero se satisface que*

$$F(h_n)(-k) = h_n(k)F(h_n)(-1) \tag{3.21}$$

**Demostración.** Sea $\zeta_n = e^{2\pi i/n}$, tenemos que

$$\begin{aligned}F(h_n) &= \frac{1}{\sqrt{n}}\sum_{m,m'=0}^{n-1}\zeta_n^{mm'}|e_m\rangle\langle e_{m'}|\sum_{l=0}^{n-1}h_n(l)e_l\\ &= \frac{1}{\sqrt{n}}\sum_{m,m',l=0}^{n-1}\zeta_n^{mm'}h_n(l)\langle e_{m'},e_l\rangle e_m = \frac{1}{\sqrt{n}}\sum_{m,m'=0}^{n-1}\zeta_n^{mm'}h_n(m')e_m\end{aligned} \tag{3.22}$$

lo cual implica que $F(h_n)(m) = \frac{1}{\sqrt{n}}\sum_{m'=0}^{n-1}\zeta_n^{mm'}h_n(m')$ para cada $m\in\mathbb{Z}$. Entonces si $n$ no divide a $k$, por el lema 2.2.4

$$\begin{aligned}F(h_n)(-k) &= \frac{1}{\sqrt{n}}\sum_{m'=0}^{n-1}\zeta_n^{-km'}h_n(m') = \frac{1}{\sqrt{n}}\sum_{m'=0}^{n-1}\zeta_n^{-km'}\Big(\frac{m'}{n}\Big),\ \textit{con } b = km',\\ &= \frac{1}{\sqrt{n}}\sum_{b=0}^{n-1}\zeta_n^{-b}\Big(\frac{bk^{-1}}{n}\Big) = \Big(\frac{k^{-1}}{n}\Big)\frac{1}{\sqrt{n}}\sum_{b=0}^{n-1}\zeta_n^{-b}\Big(\frac{b}{n}\Big)\\ &= h_n(k)F(h_n)(-1)\end{aligned} \tag{3.23}$$

pues $n$ no divide a $m'$ ni a $km'$ si $0 \leq m' \leq n-1$. Ahora, si $n$ divide a $k$

$$\begin{aligned} F(h_n)(-k) &= \frac{1}{\sqrt{n}} \sum_{m'=0}^{n-1} \zeta_n^{-km'} h_n(m') \\ &= \frac{1}{\sqrt{n}} \sum_{b=0}^{n-1} \zeta_n^{-b} h_n(k^{-1}b) = 0 \end{aligned} \tag{3.24}$$

pues $n$ divide a cada $b = km'$. Esto completa la demostración. ■

**Teorema 3.2.5** *La función $h_n$ es una función propia de la transformada de Fourier discreta, de hecho,*

$$F(h_n) = g^{-1} h_n \tag{3.25}$$

*donde $g$ es la suma de Gauss $g = F(h_n)(-1) = \sum_{m=1}^{n-1} \left(\frac{m}{n}\right)\zeta_n^m$, que satisface $g^2 = (-1)^{\frac{n-1}{2}}$, i.e.,*

$$g = \begin{cases} \pm 1 & si \quad \frac{n-1}{2} \text{ es par} \\ \pm i & si \quad \frac{n-1}{2} \text{ es impar} \end{cases} \tag{3.26}$$

**Demostración.** Tomando transformada de Fourier discreta en (3.21) y usando la fórmula de inversión en la ecuación (3.7) se obtiene que como $h_n = \sum_{k=0}^{n-1} h_n(k) e_k$, entonces

$$F\big(F(\sum_{k=0}^{n-1} h_n(k) e_k)\big) = \sum_{k=0}^{n-1} h_n(k) F\big(F(e_k)\big) = \sum_{k=0}^{n-1} h_n(k) e_{-k} = \sum_{k=0}^{n-1} h_n(-k) e_k$$

entonces

$$F\big(F(h_n)\big)(k) = h_n(-k)$$

Por lo tanto,

$$h_n(k) = F\big(F(h_n)\big)(-k) = F\big(F(h_n)(-k)\big) = F(h_n)(-1)F(h_n)(k) = gF(h_n)(k), \ \ \forall \ \ k \tag{3.27}$$

Ahora, evaluando (3.27) en $k = -1$ se obtiene que $h_n(-1) = g^2$. Recordando que

$$h_n(-1) = \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

la última identidad es por el Criterio de Euler, se concluye que $g^2 = (-1)^{\frac{n-1}{2}}$ y termina la demostración. ■

**Lema 3.2.6** *Sean $m, n$ primos impares distintos, entonces poniendo $n^* = (-1)^{\frac{n-1}{2}}$ si $g$ es la anterior suma de Gauss, entonces*

$$g^{m-1} = (\frac{n^*}{m})$$

**Demostración.** Tenemos que $m-1$ es par y por el teorema anterior (3.2.5),

$$g^{m-1} = g^{2\frac{(m-1)}{2}} = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}$$

Ahora por el criterio de Euler,

$$(\frac{n^*}{m}) = (n^*)^{\frac{m-1}{2}} = (-1)^{(\frac{n-1}{2})(\frac{m-1}{2})}$$

■

# Capítulo 4

# Transformada de Fourier Discreta II

En éste capítulo abordamos el cálculo de la traza y el espectro de la transformada de Fourier discreta, es decir, analizamos las razones por las cuales el cálculo de la traza de la transformada de Fourier es equivalente a calcular el espectro. Además veremos que la transformada de Fourier discreta es practicamente una suma de Gauss y se divide en tres casos, el primer caso $n \equiv 2 \mod 4$ que es resuelto mediante un argumento de simetría, el segundo $n \equiv 1 \mod 4$ y $n \equiv 3 \mod 4$ que se resuelve por medio de identidades trigonométricas y el caso $n \equiv 0 \mod 4$ que se resuelve usando el símbolo de Legendre y algunas identidades utilizando representaciones unitarias para finalmente exponer la multiplicidad de los valores propios a partir de la traza de la transformada de Fourier discreta.

## 4.1. Equivalencia entre la traza y el espectro

Esta sección relacionan el cálculo de $\mathrm{Tr}(F(n))$, $n > 0$, y el problema de multiplicidad de los eigenvalores de $F(n)$. Dado que la traza de una transformación lineal es la suma de sus valores propios, está claro que una solución del problema de multiplicidad para $F(n)$ implica la identidad (4.36) o el resultado de Gauss en sumas cuadráticas de Gauss. Lo que es muy sorprendente es que conocer la $\mathrm{Tr}(F(n))$ para todo $n$ nos permite resolver el problema de multiplicidad de los eigenvalores de $F(n)$. La demostración de este hecho se basa en el teorema 7 de [3] pag. 349, en cuya demostración se encuentra que

$$F^2(n) = \begin{pmatrix} 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 & 1 \\ 0 & 0 & \cdot & \cdot & 1 & 0 \\ \vdots & \vdots & \cdot & \cdot & \cdot & \vdots \\ 0 & 1 & 0 & \cdot & \cdot & 0 \end{pmatrix} \tag{4.1}$$

y que su polinomio característico está dado por

$$(t-1)^{\frac{(n+1)}{2}}(t+1)^{\frac{(n-1)}{2}}, \quad \text{n impar}, \tag{4.2}$$

$$(t-1)^{\frac{(n+2)}{2}}(t+1)^{\frac{(n-2)}{2}}, \quad \text{n par}. \tag{4.3}$$

Como los eigenvalores de $F^2(n)$ son los cuadrados de los valores propios de $F(n)$, se sigue que los valores propios de $F(n)$ son $\pm 1, \pm i$ y la ecuación (4.2) implica que si las correspondientes multiplicidades son $m_1, m_2, m_3, m_4$, entonces

$$\begin{aligned} m_1 + m_2 =& \frac{n+1}{2}, \quad m_3 + m_4 = \frac{n-1}{2}, \text{ n impar} \\ m_1 + m_2 =& \frac{n+2}{2}, \quad m_3 + m_4 = \frac{n-2}{2}, \text{ n par} \end{aligned} \tag{4.4}$$

y

$$\operatorname{Tr}\big(F(n)\big) = m_1 - m_2 + i(m_3 - m_4)$$

Ahora, si $\operatorname{Tr}\big(F(n)\big) = \alpha + i\beta$, entonces para $n$ impar

$$\begin{aligned} m_1 - m_2 =& \alpha, \quad m_3 - m_4 = \beta, \\ m_1 + m_2 =& \frac{n+1}{2}, \quad m_3 + m_4 = \frac{n-1}{2} \end{aligned} \tag{4.5}$$

y algo similar para $n$ par. Resolviendo para $m_j$, $j = 1, 2, 3, 4$ en términos de $\alpha$ y $\beta$, se tiene una solución completa del problema de eigenvalores. Esto demuestra que el problema de eigenvalores es equivalente al problema del cálculo de la traza.

## 4.2. Identidades Trigonométricas

Acontinuación presentamos los cálculos correspondientes de las identidades trigonométricas que utilizaremos más adelante.

**Lema 4.2.1** *Para cada entero impar $n \geq 1$, se tiene*

$$\prod_{k=1}^{\frac{1}{2}(n-1)} 2 \operatorname{sen} \frac{k\pi}{n} = \sqrt{n}. \tag{4.6}$$

**Demostración.** Como los números complejos $e^{\frac{2k\pi i}{n}}$, $1 \leq k \leq n-1$ son raíces $n$-ésimas de la unidad para $n > 1$, tenemos que

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{1 - x^n}{1 - x} = \prod_{k=1}^{n-1} (x - e^{\frac{2k\pi i}{n}}) \tag{4.7}$$

y de aquí se sigue que

$$\begin{aligned} n =& \prod_{k=1}^{n-1} (-2i \operatorname{sen} \frac{k\pi}{n}) \big( \cos \frac{k\pi}{n} + i \operatorname{sen} \frac{k\pi}{n} \big) \\ =& (-i)^{n-1} (e^{\frac{\pi i}{n} \sum_{k=1}^{n-1} k}) \prod_{k=1}^{n-1} 2 \operatorname{sen} \frac{k\pi}{n} \\ =& (-i)^{n-1} e^{\frac{(n-1)\pi i}{2}} \prod_{k=1}^{n-1} 2 \operatorname{sen} \frac{k\pi}{n} = \prod_{k=1}^{n-1} 2 \operatorname{sen} \frac{k\pi}{n} \end{aligned} \tag{4.8}$$

Como $\operatorname{sen}\frac{(n-k)\pi}{n} = \operatorname{sen}\frac{k\pi}{n}$ obtenemos que para cada $n$ impar

$$\prod_{k=1}^{\frac{1}{2}(n-1)} 2\operatorname{sen}\frac{k\pi}{n} = \sqrt{n}. \tag{4.9}$$

Esto demuestra el lema. ■

**Lema 4.2.2** *Sean $n > 1$ un entero impar y $\varphi(m,n) = \sum_{s=0}^{n-1} e^{\frac{2\pi i m s^2}{n}}$, entonces*

$$\varphi(1,n) = \prod_{k=i}^{\frac{1}{2}(n-1)} 2i\operatorname{sen}\frac{(4k-2)\pi}{n} = (-1)^{[\frac{n}{4}]} i^{\frac{1}{2}(n-1)}\sqrt{n} \tag{4.10}$$

**Demostración.** Usaremos la identidad algebraica, válida para $h$ par:

$$\begin{aligned} &1 - \frac{1-x^h}{1-x} + \frac{(1-x^h)(1-x^{h-1})}{(1-x)(1-x^2)} - \frac{(1-x^h)(1-x^{h-1})(1-x^{h-2})}{(1-x)(1-x^2)(1-x^3)} + \cdots \\ =&(1-x)(1-x^3)\cdots(1-x^{h-1}) \end{aligned} \tag{4.11}$$

Para una demostración veáse la sección 52 de [10].

Ahora supóngase $n > 1$ impar y póngase $\nu = \frac{1}{2}(n-1)$. Sea $m$ un entero primo relativo con $n$ y pongamos $\eta = e^{\frac{2\pi i m}{n}}$. Con $h = n-1$, $x = \eta^{-2} = e^{\frac{4\pi i m}{n}}$ a partir de la identidad (4.11), tomando en cuenta que para cada entero $t$,

$$\frac{1 - e^{\frac{2\pi i(tn-2k)}{n}}}{1 - e^{\frac{-4\pi i k}{n}}} = -e^{\frac{4\pi i k}{n}} \tag{4.12}$$

tenemos

$$1 + \eta^2 + \eta^6 + \eta^{12} + \cdots + \eta^{n(n-1)} = (1-\eta^{-2})(1-\eta^{-6})\cdots(1-\eta^{-2n+4}) \tag{4.13}$$

pues

$$\begin{aligned} 1 - \frac{1-x^h}{1-x} =& 1 + \eta^2 \\ \frac{1-x^{h-1}}{1-x^2} =& -\eta^4 \end{aligned} \tag{4.14}$$

por lo tanto,

$$\frac{1-x^h}{1-x}\frac{1-x^{h-1}}{1-x^2} = (-\eta^2)(-\eta^4) = \eta^6$$

etcétera. Equivalentemente,

$$\begin{aligned} \sum_{k=0}^{n-1} \eta^{k(k+1)} =& \eta^{-1}(\eta - \eta^{-1})\eta^{-3}(\eta^3 - \eta^{-3})\cdots\eta^{-(n-2)}(\eta^{n-2} - \eta^{-(n-2)}) \\ =& \eta^{-1-3-5-\cdots-(n-2)} \prod_{k=0}^{\nu-1}(\eta^{2k+1} - \eta^{-(n-2)}) \end{aligned} \tag{4.15}$$

Ahora tenemos,

$$\eta^{(\nu-k)^2} = e^{\frac{2\pi im}{n}\left(\frac{1}{2}(n-1)-k\right)^2} = e^{\frac{2\pi im}{n}\left(\frac{1}{4}(n-1)^2-nk+k+k^2\right)} = e^{\frac{2\pi im}{n}\left(\nu^2+k(k+1)\right)} = \eta^{\nu^2+k(k+1)} \tag{4.16}$$

Consecuentemente,

$$\eta^{\nu^2}\sum_{k=0}^{\nu}\eta^{k(k+1)} = \sum_{k=0}^{\nu}\eta^{(\nu-k)^2} = \eta^{\nu^2}+\eta^{(\nu-1)^2}+\cdots+\eta+1 \tag{4.17}$$

Además,

$$\begin{aligned}\eta^{(n-k)(n-k+1)+\nu^2} =& e^{\frac{2\pi im}{n}(n^2-2nk+k^2+n-k+\nu^2)} = e^{\frac{2\pi im}{n}(\nu^2+k(k-1))}\\ =& e^{\frac{2\pi im}{n}(k^2+\nu^2+(n-1)k)} = e^{\frac{2\pi im}{n}(k+\nu)^2} = \eta^{(\nu+k)^2}\end{aligned} \tag{4.18}$$

Por lo tanto,

$$\eta^{\nu^2}\sum_{k=1}^{\nu}\eta^{(n-k)(n-k+1)} = \quad \eta^{\nu^2}\textstyle\sum_{k=1}^{\nu}\eta^{k(k-1)} = \sum_{k=1}^{\nu}\eta^{(\nu+k)^2} \tag{4.19}$$

$$= \quad \eta^{(\nu+1)^2}+\eta(\nu+2)^2+\cdots+\eta^{(n-1)^2} \tag{4.20}$$

Pero como $1+3+5+\cdots+(n-2)=\nu^2$ obtenemos de (4.15) y (4.17) que

$$\eta^{\nu^2}\sum_{k=0}^{n-1}\eta^{k(k+1)} = \prod_{k=0}^{\nu-1}\left(\eta^{2k+1}-\eta^{-2k-1}\right)$$

Es decir,

$$\begin{aligned}\varphi(m,n) =& 1+\eta+\eta^4+\eta^9+\cdots+\eta^{(n-1)^2} = (\eta-\eta^{-1})(\eta^3-\eta^{-3})\cdots(\eta^{n-2}-\eta^{-n+2})\\ =& (e^{\frac{2\pi im}{n}}-e^{-\frac{2\pi im}{n}})(e^{\frac{6\pi im}{n}}-e^{-\frac{6\pi im}{n}})\cdots(e^{\frac{2(n-2)\pi im}{n}}-e^{-\frac{2(n-2)\pi im}{n}})\\ =& \prod_{k=1}^{\frac{1}{2}(n-1)} 2i\,\mathrm{sen}\left(\frac{(4k-2)m\pi}{n}\right)\end{aligned} \tag{4.21}$$

El conjunto $\{4k-2\}_{k=1}^{\frac{1}{2}(n-1)}$es un sistema completo de residuos módulo n, entonces por el lema 4.2.1 se obtiene,

$$\left|\prod_{k=1}^{\frac{1}{2}(n-1)} 2i\,\mathrm{sen}\left(\frac{(4k-2)m\pi}{n}\right)\right| = \sqrt{n}$$

Además, como $\mathrm{sen}\left(\frac{(4k-2)m\pi}{n}\right)$ es negativo para $\frac{n}{4}+\frac{1}{2} < k < \frac{1}{2}n$. Entonces el número de factores negativos en el producto es

$$r = \frac{1}{2}(n-1) - [\frac{n}{4}+\frac{1}{2}]$$

Si $n \in \mathbb{Z}_4$, se tiene $r = [\frac{n}{4}]$ así que para cada $n$ impar,

$$\varphi(1,n) = \prod_{k=1}^{\frac{1}{2}(n-1)} 2i \operatorname{sen}\Big(\frac{(4k-2)m\pi}{n}\Big) = i^{\frac{1}{2}}(-1)^{[\frac{n}{4}]}\sqrt{n}$$

■

## 4.3. Suma de Gauss

En ésta sección se demuestran los casos mencionados al inicio de este capítulo en donde analizamos que la traza de la transformada de Fourier es en realidad una suma de Gauss y hacemos uso de recursos vistos anteriormente como es el símbolo de Legendre, residuos cuadráticos y representaciones unitarias.

**Definición 4.3.1** *Sea un sistema completo de residuos módulo $n$, cualquier subconjunto $R_n \subset \mathbb{Z}$ para el cual el homomorfismo $\tilde{n}$ restringido a $R_n$ define una biyección de $R_n$ sobre $\mathbb{Z}_n$. Equivalentemente,*

$$R_n = \{r_0, r_1, \cdots, r_{n-1} : r_j \equiv j \mod n,\ 0 \leq j \leq n-1\} \tag{4.22}$$

**Lema 4.3.2** *Si $m \not\equiv 0 \mod n$, entonces*

$$\sum_{0\leq\xi\leq n-1} e^{2\pi i m\xi^2/n} = \Big(\frac{m}{n}\Big) \sum_{0\leq\xi\leq n-1} e^{2\pi i\xi^2/n} \tag{4.23}$$

**Demostración.** Para cualquier sistema completo de residuos módulo $n$, tenemos

$$\begin{aligned}\sum_{\xi\in R_n} e^{2\pi i m\xi^2/n} &= \sum_{0\leq j\leq n-1} e^{2\pi i m r_j^2/n} = \sum_{0\leq j\leq n-1} e^{2\pi i m(k_j n+j)^2/n} \\ &= \sum_{0\leq j\leq n-1} e^{2\pi i m(k_j^2 n+2k_j j)} e^{2\pi i m j^2/n} = \sum_{0\leq\xi\leq n-1} e^{2\pi i m\xi^2/k}\end{aligned} \tag{4.24}$$

donde los $k_j$'s son enteros. Sea $l \not\equiv 0 \mod n$ y sea $R_n$ un sistema completo de residuos módulo $n$, entonces

$$lR_n = \{l\xi : \xi \in R_n\}$$

también es un sistema completo de residuos módulo $n$. En efecto, si $R_n = \{r_j : 0 \leq j \leq n-1\}$, entonces $lr_j \not\equiv lr_{j'} \mod n$ si $r_j \not\equiv r_{j'} \mod n$, pues en caso contrario la condición

$$l\big(r_j - r_{j'}\big) \equiv 0, \quad \mod n$$

implica que $l \equiv 0, \mod n$. Ahora, sea $\big(\frac{m}{n}\big) = 1$, i.e., $m \equiv t^2 \mod n$; $t \in \mathbb{Z}_n^\times$, entonces

$$\sum_{\xi\in R_n} e^{2\pi i m\xi^2/n} = \sum_{\xi\in R_n} e^{2\pi i(t\xi)^2/n} = \sum_{\eta\in tR_n} e^{2\pi i\eta^2/n} = \Big(\frac{m}{n}\Big) \sum_{\xi\in R_n} e^{2\pi i\xi^2/n} \tag{4.25}$$

Si $\left(\frac{m}{n}\right) = -1$, i.e., $\tilde{n}(m) \in \mathbb{Z}_n^\times$ pero $\tilde{n}(n) \notin S$, i.e., $m \notin S$. Poniendo $R_n = \{r_j : 0 \leq j \leq n-1\}$, obtenemos que $r_j^2 \equiv r_{j'}^2 \mod n$ con $r_j \not\equiv r_{j'} \mod n$, si sólo si $r_j^2 - r_{j'}^2 = (r_j - r_{j'})(r_j + r_{j'}) \equiv 0 \mod n$. Esto implica que $r_j + r_{j'} \equiv 0 \mod n$. Por lo tanto $r_j^2 \equiv (-r_j)^2 \mod n$. Esto implica que cuando $\xi$ recorre $R_n$, $\tilde{n}(\xi^2) \equiv \xi^2$ recorre dos veces $S$ y una vez el $0 \in \mathbb{Z}_n$. Similarmente, $a\xi^2$ recorre dos veces $aS$ y una vez $0 \in \mathbb{Z}_n$. Consecuentemente,

$$\begin{aligned}\sum_{\xi\in R_n} e^{2\pi i n\xi^2/n} + \sum_{\xi\in R_n} e^{2\pi i\xi^2/n} &= \sum_{m\xi^2\in mS} e^{2\pi i m\xi^2/n} + \sum_{\xi^2\in S} e^{2\pi i\xi^2/n} + 2 \\ &= 2\sum_{\xi\in S\cup mS\cup\{0\}} e^{2\pi i\xi/n} = 2\sum_{0\leq\xi\leq n-1} e^{2\pi i\xi/n} = 0\end{aligned} \tag{4.26}$$

Por lo tanto,

$$\sum_{\xi\in R_n} e^{2\pi i m\xi^2/n} = (-1)\sum_{\xi\in R_n} e^{2\pi i\xi^2/n} = \left(\frac{m}{n}\right)\sum_{\xi\in R_n} e^{2\pi i\xi^2/n} \tag{4.27}$$

■

**Teorema 4.3.3** ***(K.F. Gauss)*** *Sea $F(n)$ la transformada de Fourier discreta en $L_2(\mathbb{Z}_n)$ y sea $\mathrm{Tr}\big(F(n)\big)$ la traza de $F(n)$. Entonces,*

$$\mathrm{Tr}\big(F(n)\big) = \begin{cases} 1 & \text{si } n \equiv 1 \mod 4, \\ 0 & \text{si } n \equiv 2 \mod 4, \\ i & \text{si } n \equiv 3 \mod 4. \end{cases} \tag{4.28}$$

**Demostración.** Comenzaremos demostrando que para $r$ impar, i.e., $n = 2r \equiv 2 \mod 4$, $\mathrm{Tr}(F(2r)) = 0$. A partir de la primera ecuación en (3.11), se obtiene que

$$\begin{aligned}\mathrm{Tr}(F(2r)) &= \frac{1}{\sqrt{2r}}\sum_{0\leq\xi<r} e^{2\pi i\xi^2/2r} + \frac{1}{\sqrt{2r}}\sum_{0\leq\xi<r} e^{2\pi i(\xi+r)^2/2r} \\ \mathrm{Tr}(F(2r)) &= \frac{1}{\sqrt{2r}}\sum_{0\leq\xi<r} e^{2\pi i\xi^2/2r} + \frac{1}{\sqrt{2r}}\sum_{0\leq\xi<r} e^{2\pi i(\xi^2+2\xi r+r^2)/2r} \\ \mathrm{Tr}(F(2r)) &= \frac{1}{\sqrt{2r}}\sum_{0\leq\xi<r} e^{2\pi i\xi^2/2r} + \frac{1}{\sqrt{2r}}\sum_{0\leq\xi<r} e^{2\pi i\xi^2/2r} e^{2\pi i 2\xi r/2r} e^{2\pi i r^2/2r} \\ \mathrm{Tr}(F(2r)) &= \frac{1}{\sqrt{2r}}\sum_{0\leq\xi<r} e^{2\pi i\xi^2/2r} + \frac{1}{\sqrt{2r}}\sum_{0\leq\xi<r} e^{2\pi i\xi^2/2r} e^{2\pi i\xi} e^{2\pi i r/2}\end{aligned} \tag{4.29}$$

Pues como $r$ es impar, $e^{2\pi i r/2} = -1$ y $e^{2\pi i(\xi+r)^2/2r} = -e^{2\pi i\xi^2/2r} e^{2\pi i\xi} = -e^{2\pi i\xi^2/2r}$, entonces

$$\mathrm{Tr}(F(2r)) = \frac{1}{\sqrt{2r}}\sum_{0\leq\xi<r} \left(e^{2\pi i\xi^2/2r} - e^{2\pi i\xi^2/2r}\right) = 0 \tag{4.30}$$

Hemos establecido que $\mathrm{Tr}(F(2r)) = 0$, $r$ impar.

Ahora, por el lemma 4.2.2, se ve que $\varphi(1,n)$ toma el valor $\sqrt{n}$ si $n \equiv 1 \mod 4$ y el valor $i\sqrt{n}$ si $n \equiv 3 \mod 4$. ■

Resta demostrar que $\mathrm{Tr}(F(n)) = 1+i$ si $n \equiv 0 \mod 4$.

Sea $p$ un primo impar, el lema 4.3.2 en la forma de la ecuación (3.17) nos da

$$\mathrm{Tr}(\rho(4)F(p)) = \Big(\frac{4}{p}\Big)\mathrm{Tr}(F(p)) = \mathrm{Tr}(F(p))$$

ya que es fácil verificar que $\left(\frac{4}{p}\right) = 1$, porque $p$ es un primo impar y 4 es un cuadrado mód $p$, es decir, $p \nmid 4$. De la identidad (3.19), resulta

$$\mathrm{Tr}\big(F(4p)\big) = \mathrm{Tr}\big(\rho(4)F(p)\big)\mathrm{Tr}\big(\rho(p)F(4)\big) = \mathrm{Tr}\big(F(p)\big)\mathrm{Tr}\big(\rho(p)F(4)\big)$$

donde $\rho$ es el homomorfismo en la definición 1.3.2. Pero podemos escribir fácilmente los cuatro términos de la suma $\mathrm{Tr}(\rho(p)F(4))$ para probar que usando la segunda identidad de (3.11) se obtiene

$$\mathrm{Tr}\big(\rho(p)F(4)\big) = \frac{1}{2}\big(2 + 2e^{i\pi\frac{p}{2}}\big) = 1+i$$

si $p \equiv 1 \mod 4$, y

$$\mathrm{Tr}\big(\rho(p)F(4)\big) = \frac{1}{2}\big(2 - 2e^{i\pi\frac{p}{2}}\big) = 1-i$$

si $p \equiv 3 \mod 4$. Así que

$$\mathrm{Tr}\big(F(4p)\big) = \mathrm{Tr}\big(F(p)\big)\mathrm{Tr}\big(\rho(p)F(4)\big) = (1+i)$$

si $p \equiv 1 \mod 4$. Y de manera similar,

$$\mathrm{Tr}\big(F(4p)\big) = \mathrm{Tr}\big(F(p)\big)\mathrm{Tr}\big(\rho(p)F(4)\big) = i(1-i) = (1+i)$$

si $p \equiv 3 \mod 4$.

Para $n$ general congruente con 0 módulo 4 tenemos lo siguiente, donde usaremos la identidad (3.18). Nosotros hemos demostrado esta identidad sólo para $m$ y $n$ primos impares, pero es válida para $m$ y $n$ coprimos. Ver el Lema 1.2.5 en [2].

**Teorema 4.3.4** ***(K.F. Gauss)*** *Si $n$ es congruente con 0 módulo 4, entonces*

$$\mathrm{Tr}\big(F(n)\big) = (1+i)$$

**Demostración.** Supóngase que $n = k2^s$ con $s \geq 2$ y $k$ un entero impar. Las identidades (3.18) y (3.17) implican que

$$\mathrm{Tr}\big(F(k2^s)\big) = \Big(\frac{2^s}{k}\Big)\mathrm{Tr}(F(k))\mathrm{Tr}(\rho(k)F(2^s))$$

donde $\left(\frac{2^s}{k}\right)$ es el símbolo de Legendre. Pero para cada $k$ impar tenemos por el teorema anterior que

$$\mathrm{Tr}\big(F(k)\big) = \begin{cases} 1 & \text{si } n \equiv 1 \mod 4, \\ i & \text{si } n \equiv 3 \mod 4. \end{cases} \tag{4.31}$$

es decir, $\mathrm{Tr}(F(k)) = i^{\frac{(k-1)^2}{4}}$ si $k$ es impar. Además por el teorema 2.2.7 tenemos que

$$\left(\frac{2}{k}\right) = (-1)^{\frac{k^2-1}{8}}$$

para cada $k$ impar, pues si $k$ es impar $\frac{k^2-1}{8}$ es un entero. Así que por la propiedad multiplicative del símbolo de Legendre, obtenemos

$$\left(\frac{2^s}{k}\right) = \left(\frac{2}{k}\right)^s = \big(-1\big)^{s(\frac{k^2-1}{8})}$$

Esto implica que

$$\left(\frac{2^s}{k}\right)\mathrm{Tr}(F(k)) = \big(-1\big)^{s(\frac{k^2-1}{8})} i^{\frac{(k-1)^2}{4}} \tag{4.32}$$

Por otra parte, por la identidad (3.11) sabemos que

$$\mathrm{Tr}(\rho(k)F(2^s)) = \frac{1}{\sqrt{2^s}} \sum_{\alpha \in \mathbb{Z}_{2^s}} e^{\frac{2\pi i k \alpha^2}{2^s}}$$

Calculando directamente se obtiene que para $s = 2$, $\mathrm{Tr}(\rho(k)F(4)) = 2^{-\frac{s}{2}} 2(1 + i^k)$ y para $s = 3$

$$\mathrm{Tr}(\rho(k)F(8)) = 4e^{\frac{i\pi k}{4}} = \left(\frac{2}{k}\right) 2^{\frac{2}{3}-\frac{s}{2}}(1 + i^k)$$

para cada $k$ impar. Ahora, para $k$ impar y $s \geq 4$, tenemos

$$\sum_{\alpha \in \mathbb{Z}_{2^s}} e^{\frac{2\pi i k \alpha^2}{2^s}} = \sum_{\alpha=0,\ \alpha\ impar}^{2^s-1} e^{\frac{2\pi i k \alpha^2}{2^s}} + 2\mathrm{Tr}(\rho(k)F(2^{s-2})) = 2\mathrm{Tr}(\rho(k)F(2^{s-2}))$$

Entonces,

$$\mathrm{Tr}(\rho(k)F(2^s)) = 2\mathrm{Tr}(\rho(k)F(2^{s-2})), \ \ s \geq 4$$

De esta manera obtenemos

$$\mathrm{Tr}\big(\rho(k)F(2^s)\big) = \begin{cases} 2^{\frac{s-2}{2}}\mathrm{Tr}(\rho(k), F(4)) & \text{si } s \text{ es par}, \\ 2^{\frac{s-3}{2}}\mathrm{Tr}(\rho(k), F(8)) & \text{si } s \text{ es impar}. \end{cases} \tag{4.33}$$

Después de sustituir nos queda

$$\mathrm{Tr}\big(\rho(k)F(2^s)\big) = \left(\frac{2^s}{k}\right)(1 + i^k) \tag{4.34}$$

Finalmente de (4.32) y (4.34) concluimos que

$$\mathrm{Tr}\big(F(k2^s)\big) = \Big(\frac{2^s}{k}\Big) i^{\frac{(k-1)^2}{4}} \Big(\frac{2^s}{k}\Big)(1+i^k) = \big(-1\big)^{2s(\frac{k^2-1}{8})} i^{\frac{(k-1)^2}{4}}(1+i^k) = 1+i, \qquad (4.35)$$

pues $k \equiv 1$ o $k \equiv 3$ módulo 4. ■

Resumiendo, tenemos que

$$\mathrm{Tr}\big(F(n)\big) = \begin{cases} (i+1) & \text{si } n \equiv 0 \mod 4, \\ 1 & \text{si } n \equiv 1 \mod 4, \\ 0 & \text{si } n \equiv 2 \mod 4, \\ i & \text{si } n \equiv 3 \mod 4. \end{cases} \qquad (4.36)$$

Es decir,

$$\mathrm{Tr}\big(F(n)\big) = \frac{1}{2}(1+i)(1+(-i)^n)$$

## 4.4. Traza y espectro de la Transformada de Fourier Discreta

Finalmente exponemos la multiplicidad de los valores propios de la transformada de Fourier, así el teorema 4.36 tiene la siguiente forma equivalente.

**Teorema 4.4.1** *Sea $F(n)$ la transformada de Fourier en $\mathbb{Z}_n$ y sean $m_j$, $j = 1, 2, 3, 4$ las multiplicidades de los eigenvalores $1, -1, i, -i$ de $F(n)$, respectivamente. Los valores de $m_j$, $j = 1, 2, 3, 4$, como funciones de $n$ están dados en la siguiente tabla.*

| $n$ | $m_1 = 1$ | $m_2 = -1$ | $m_3 = i$ | $m_4 = -i$ |
|---|---|---|---|---|
| 4m | m + 1 | m | m | m - 1 |
| 4m + 1 | m + 1 | m | m | m |
| 4m + 2 | m + 1 | m + 1 | m | m |
| 4m + 3 | m + 1 | m + 1 | m + 1 | m |

# Conclusiones y perspectivas

Hemos presentado una exposición auto-contenida del cálculo de la traza y el espectro de la transformada de Fourier discreta (DFT), siguiendo la referencia [1]. Completamos la demostración de la equivalencia de los problemas del cálculo el espectro de la DFT y el cálculo de su traza que en [1] sólo se esboza. Con este propósito,

- Definimos el símbolo de Legendre y mostramos que una suma de Gauss se puede expresar en términos del este símbolo.
- Describimos la representación regular unitaria $\rho$ del grupo de unidades $\mathbb{Z}_n^\times$ de $\mathbb{Z}_n$.
- Demostramos que la traza de la DFT es una suma de Gauss.
- Demostramos una relación entre estas trazas y el símbolo de Legendre, que es útil para calcular explícitamente la traza de la DFT.
- Demostramos la ley de reciprocidad cuadrática y calculamos explícitamente la traza de la DFT.
- Calculamos los valores propios de la transformada de Fourier $F(n)$ así como sus multiplicidades.

Concluimos que el cálculo del espectro y la traza de la DFT involucra una cantidad considerable de conceptos matemáticos profundos.
Este trabajo se podría continuar examinando otras demostraciones de los teoremas 4.3.3 y 4.4.1, como se hace en [1]. También se puede continuar buscando otras funciones propias de la DFT, tomando en cuenta que es un operador normal, i.e., conmuta con su adjunto, al respecto véanse las referencias [5], [7] y [8]. Así mismo, se podrían considerar los problema de la traza y el espectro de la transformada de Fourier discreta en grupos no necesariamente conmutativos.

# Apéndice

## La traza de una matriz

Denotaremos mediante el símbolo $\mathbb{M}_{n\times n}(\mathbb{C})$ al espacio de las matrices complejas $n \times n$. Recuérdese que la traza de una matriz $A = (a_{i,j})_{1\leq i,j\leq n}$ es el número complejo

$$tr(A) = \sum_{i=1}^{n} a_{i,i}$$

La traza tiene las siguientes propiedades.

**Teorema 4.4.2** *1. La traza es una función lineal*

$$tr : \mathbb{M}_{n\times n}(\mathbb{C}) \longrightarrow \mathbb{C} \tag{4.37}$$

*2. Si* $A \in \mathbb{M}_{n\times m}(\mathbb{C}), B \in \mathbb{M}_{m\times n}(\mathbb{C})$, *entonces* $\mathrm{tr}(AB) = tr(BA)$.

*3. Si* $A \in \mathbb{M}_{n\times n}(\mathbb{C}), entonces\ tr(A) = tr(A^*)$, *donde* $A^*$ *es la transpuesta conjugada de* $A$.

*4.* $A \in \mathbb{M}_{n\times n}(\mathbb{C}), entonces\ tr(\overline{A}) = \overline{tr(A)}$

**Demostración.**

1. Se sigue del hecho de que $Hom_{\mathbb{C}}(\mathbb{M}_{n\times n}(\mathbb{C}), \mathbb{C}) = (\mathbb{M}_{n\times n}(\mathbb{C}))^*$, es un espacio vectorial.
2. $tr(AB) = \sum_i \left( \sum_k a_{i,k}b_{k,i} \right) = \sum_{i,k} a_{i,k}b_{k,i} = tr(BA)$
3. Esto resulta porque $A$ es una matriz cuadrada y tiene la misma diagonal principal que su transpuesta, y la traza es la suma de los elementos de la diagonal.
4. $tr(\overline{A}) = \sum \overline{a}_{i,i} = \overline{\sum a_{i,i}} = \overline{tr(A)}$.

■

# Bibliografía


[1] Auslander L. and Tolimieri R., Is computing with the finite Fourier transform pure or applied mathematics?. Bulletin (New series), Of the American Mathematical Society, Volume 1, Number 6, 1979.

[2] Berndt B.C., Evans R.J. and Williams K.S., Gauss and Jacobi Sums, Wiley & Sons, 1998.

[3] Borevich Z.I. and Shafarevich I.R., Number Theory, Academic Press, 1966.

[4] Dense Joseph B. and Dence Thomas P., Elements of the Theory of Numbers. Harcourt Academic Press. p. 197, 1999, ISBN 9780122091308.

[5] Dickinson B.W. and Steinglitz K., Eigenvectors and Functions of the Discrete Fourier Transform, IEEE Transactions on acoustics, speech and signal processing, Vol. SSP-30, Number 1, 1982.

[6] Euler Leonhard, Theorematum quorundam ad numeros primos spectantium demonstratio. Commentarii academiae scientiarum Petropolitanae 8, 1741, pp. 141-146, Reprinted in Opera Omnia: Series 1, Volume 2, pp. 33 - 37.

[7] Grünbaum A., The Eigenvectors of the Discrete Fourier Transform: a Version of the Hermite Functions, Journal of Mathematical Analysis and Applications 88, 355-363, 1982.

[8] Gurevich S. and Heading R., On the Diagonalization of the Discrete Fourier Transform, Appl. and Comput. Harmon. Anal., 27 ,87-99, 2009.

[9] Hardy G.H., Wright E.M., Heath-Brown D.R. and Silverman J.H., An Introduction to theory of numbers. Oxford University Press. 2008, ISBN 9787115214270.

[10] Nagell Trygve, Introduction to number theory, John Wiley & Sons Inc, New York and Almqvist & Wiksell, Stockholm, 1951.

[11] Terras A., Fourier Analysis on Finite Groups and Applications, Cambridge University Press, 1999.

[12] Pantaleón-Martínez L. y Quezada-Batalla R., Una Introducción la Teoría Cuántica de la Información. 1er Coloquio del Departamento de Matemáticas, UAM.

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

# ACTA DE EXAMEN DE GRADO

No. 00233
Matrícula: 2212801540

Sobre el espectro y la traza de la transformada de Fourier discreta.

IRASEMA CASTRO HERNANDEZ
ALUMNO

En la Ciudad de México, se presentaron a las 12:00 horas del día 31 del mes de octubre del año 2023 en la Unidad Iztapalapa de la Universidad Autónoma Metropolitana, los suscritos miembros del jurado:

DR. JORGE RICARDO BOLAÑOS SERVIN
DR. CRISPIN HERRERA YAÑEZ
DR. JOSUE DANIEL VAZQUEZ BECERRA

Bajo la Presidencia del primero y con carácter de Secretario el último, se reunieron para proceder al Examen de Grado cuya denominación aparece al margen, para la obtención del grado de:

MAESTRO EN CIENCIAS (MATEMÁTICAS)

DE: IRASEMA CASTRO HERNANDEZ

y de acuerdo con el artículo 78 fracción III del Reglamento de Estudios Superiores de la Universidad Autónoma Metropolitana, los miembros del jurado resolvieron:

Aprobar

Acto continuo, el presidente del jurado comunicó al interesado el resultado de la evaluación y, en caso aprobatorio, le fue tomada la protesta.

REVISÓ

MTRA. ROSALVA SERRANO DE LA PAZ
DIRECTORA DE SISTEMAS ESCOLARES

DIRECTOR DE LA DIVISIÓN DE CBI

Román Linares Romero
DR. ROMAN LINARES ROMERO

PRESIDENTE

DR. JORGE RICARDO BOLAÑOS SERVIN

VOCAL

DR. CRISPIN HERRERA YAÑEZ

SECRETARIO

DR. JOSUE DANIEL VAZQUEZ BECERRA