# Estructura del anillo de funciones aritméticas y una aplicación al procesamiento de señales

Asesor Dr. Pablo Lam Estrada *ESFM-IPN*
Borrador hecho por José Luis Juanico López

# Índice general

# Introducción

En 1640 Fermat afirmó que poseía una demostración del hecho de que si $p$ es un número primo y $x$ es cualquier entero no divisible por $p$, entonces $x^{p-1}-1$ es divisible por $p$. Ahora llamado Teorema de Fermat, es uno de los teoremas fundamentales de la teoría de números. Este resultado fue generalizado más tarde por Euler en 1760: si $\varphi(n)$ denota el número de enteros positivos no mayores a $n$ que son primos relativos a $n$, entonces $x^{\varphi(n)-1}-1$ es divisible por $p$. Aunque la función $\varphi$ de Euler se definió para enunciar la generalización anterior, ésta posee remarcables propiedades que hacen valer la pena estudiarla por sí misma. Gauss (1801) probó que si $n \in \mathbb{N}$ y $d_1, d_2, \cdots, d_k$ son todos los divisores positivos de $n$, entonces $\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_k) = n$.

Por otro lado, en 1832 A. F. Möbius definió la función $\mu(n)$ como cero si $n$ es divisible por un cuadrado distinto de 1, y como $(-1)^k$ si $n$ es producto de $k$ primos distintos, mientras que $\mu(1) = 1$ y empleó dicha función en la inversión de series:

$$F(x) = \sum_{s=1}^{\infty} \frac{f(sx)}{s^n} \text{ implica } f(x) = \sum_{s=1}^{\infty} \mu(s) \frac{F(sx)}{s^n}.$$

Dedekind (1857) probó que si $F(m) = \sum f(d)$, donde $d$ recorre todos los divisores positivos de $m$, entonces

$$f(n) = F(n) - \sum F\left(\frac{n}{a}\right) + \sum F\left(\frac{n}{ab}\right) - \sum F\left(\frac{n}{abc}\right) + \cdots,$$

donde las sumas se extienden sobre todas las combinaciónes de los distintos factores primos $a, b, \ldots$ de $n$. Laguerre (1863) expresó la ecuación anterior como

$$f(n) = \sum \mu\left(\frac{n}{d}\right) F(d).$$

En particular, como $\sum \varphi(d) = n$, se tiene

$$\varphi(n) = n - \sum \frac{n}{a} + \sum \frac{n}{ab} - \cdots = n\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\cdots$$

En 1874, F. Mertens notó que $\sum \mu(d) = 0$ si $n > 1$, donde $d$ recorre todos los divisores positivos de $n$. N. V. Bugaiev (1888) consideró la función $\nu(x)$ con valor $\log p$ si $x$ es potencia de un primo $p$ y con valor 0 en otro caso. Si $d$ recorre todos los divisores positivos de $n$, $\sum \nu(d) = \log n$ implica que $\sum \mu(d) \log d = -\nu(n)$. Bugaiev llamó a $F(n) = \sum f(d)$, la integral numérica de $f(n)$, donde la suma es sobre todos los divisores positivos $d$ de $n$, y llamó a $f(n)$ la derivada numérica de la función $F(n)$ [7].

En 1857 Liouville estableció sin prueba un gran número de identidades interesantes similares a las anteriores, en sus cuatro artículos *Sur quelques functions numeriques*, sobre funciones ariméticas específicas, como la suma y número de divisores de un entero, la función $\varphi$ de Euler, la función de Möbius $\mu$, su propia función $\lambda$, etc. Afirmó que estaba en posesión de un método general de extrema simplicidad, con el que tales identidades se podrían escribir a voluntad. Tales identidades provaron ser un valioso punto de partida para la evaluación asintótica de funciones aritméticas, pero su interés peculiar era más bien de naturaleza algebráica [3].

En 1911, al buscar pruebas para las fórmulas de Liouville, E. T. Bell construyó un método general con las características deseadas y lo extendió a otros campos además de los números racionales. Aunque Bell tenía intenciones de publicar su teoría completa en 1915, no fue sino hasta 1927 que una introducción desde un punto de vista lógico fue publicada en [2]. En lo concerniente a los *enteros racionales*, terminología de la época para referirse a los números enteros, en 1912 y 1915 [3], probó el teorema de inversión de Möbius, el cuál es un análogo a la inversión de series de Möbius en un contexto puramente aritmético y lo aplicó a numerosos ejemplos.

Bell (1928), llamó a una función $f(x)$ *función numérica* si $f(1) \neq 0$ y $f(x)$ está definida para todo entero mayor que cero. El lector que recorra este trabajo podrá darse cuenta de que esta definición coincide con la de una función aritmética *invertible* (citar definición). También llamó a una función *factorizable* a una función numérica $g(x)$ tal que $g(1) = 1$ y $g(mn) = g(m)g(n)$ para todos los pares $(m, n)$ de primos relativos positivos, que en este trabajo serán referidas como *funciones multiplicativas*.

Asimismo, Bell consideró la función *unidad* (aquí llamada *identidad*) $\varepsilon(x)$ definida como $\varepsilon(1) = 1$ y $\varepsilon(n) = 0$ para cada $n > 1$ y probó que para cualquier función numérica existe otra función numérica tal que

$$\sum f(d)f'(d) = \varepsilon(n), \qquad (n = 1, 2, 3, \ldots)$$

donde la suma se extiende sobre todos los pares de enteros $(d, \delta)$ tales que $d, \delta > 0$ y $n = d\delta$, y llama a $f'(x)$ la *recíproca* de $f(x)$, que aquí se le dará el nombre de *inversa* de $f$.

El lector con conocimiento básico de álgebra abstracta puede comenzar a identificar lo que está sucediendo aquí. Hasta ahora, resulta que la función $\varepsilon$ está actuando como la identidad respecto a la operación de anterior, es decir, hasta ahora el conjunto de funciones aritméticas contituye un *monoide*. ¿Será esta operación también asociativa o conmutativa? La repuesta a estas preguntas es afirmativa y más aún, con la operación de suma de funciones punto a punto, este conjunto forma un anillo conmutativo

con identidad y resulta ser también un dominio entero y de factorización única. En el primer capítulo, el objetivo de este trabajo es presentar algunos resultados sobre la esctructura del anillo de funciones aritméticas en un contexto puramente algebraico, condensando y resumiendo los resultados probados en [5], [14] y [3], en notación algebraica moderna. Después, se exponen varias isomorfismos entre los subgrupos del anillo de funciones aritméticas, aditivos y multiplicativos. Al final de este capítulo se presentan algunas funciones aritméticas conocidas y algunas relaciones entre ellas, derivadas fácilmente con los resultados probados en las secciones anteriores. (agregar varias relaciones entre funciones, algebráicas, tal vez una tabla).

El segundo capítulo se ocupa de presentar dos clases de funciones, llamadas funciones *pares* y funciones *periódicas*, y se probará que son equivalentes. Se presenta una teoría análoga a la teoría de Fourier del análisis real, usando únicamente propiedades de divisibilidad de los enteros. Además, se introducen las sumas de Ramanujan y algunas propiedades topológicas del espacio vectorial formado por las combinaciones lineales finitas de estas. Al final del capítulo se presenta un resultado relativo a la expasión finita de cualquier función aritmética con sumas de Ramanujan como coeficientes (y la unicidad de esta representación) (y también a la densidad de estas funciones en el conjunto de todas las funciones aritméticas). Los resultados presentados en este capítulo se pueden encontrar en [6].

En el último capítulo se presenta una aplicación de los resultados expuestos en el segundo capítulo, usándolos para el procesamiento discreto de señales, haciendo énfasis en la simplicidad de los cálculos realizados.

# 1. Estructura del anillo de funciones aritméticas

**Definición 1.1.** A partir de ahora, nos referiremos como **función aritmética** a cualquier función $f : \mathbb{N} \longrightarrow \mathbb{C}$. Se denota al conjunto de todas las funciones aritméticas como $\mathcal{A}$.

**Definición 1.2**. (Función constante)**.** La función constante de valor $c \in \mathbb{C}$ es claramente una función aritmética en $\mathbb{N}$, a la cuál denotaremos en negritas como **c**. Por ejemplo, $\mathbf{1}(n) = 1, \forall\, n \in \mathbb{N}$.

La siguiente función aritmética, conocida como función de Möbius, es de importancia central en la teoría de números. Aunque a primera vista su definición parece más bien artificial, se verá que aparece naturalmente al derivar propiedades del producto de Dirichlet.

**Definición 1.3**. (Función de Möbius)**.** La función $\mu$ de Möbius está definida por $\mu(1) = 1$ y dada $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ la factorización de $n$ en primos, entonces

$$\mu(n) = \begin{cases} (-1)^k & \text{si } \alpha_1 = \alpha_2 = \cdots = \alpha_k = 1 \\ 0 & \text{en otro caso} \end{cases}$$

Una primera forma natural de operar funciones aritméticas es haciéndo su suma o multiplicación puntual, obteniéndo otra función aritmética.

**Definición 1.4.** Si $f, g \in \mathcal{A}$, definimos la **suma** de $f$ y $g$ como la función

$$\begin{aligned} f + g : \mathbb{N} &\longrightarrow \mathbb{C} \\ n &\longmapsto f(n) + g(n) \end{aligned}$$

y el **producto** de $f$ y $g$ como la función

$$\begin{aligned} fg : \mathbb{N} &\longrightarrow \mathbb{C} \\ n &\longmapsto f(n)g(n). \end{aligned}$$

Es fácil verificar que para cualesquiera funciones aritméticas $f$ y $g$,

(i) $f + \mathbf{0} = \mathbf{0} + f = f$

(ii) $f\mathbf{1} = \mathbf{1}f = f$

(iii) $f + g = g + f$

(iv) $fg = gf$.

## 1.1. Convolución de Dirichlet

**Definición 1.5.** Sean $f$ una función aritmética, $n \in \mathbb{N}$ y $d_1, d_2, \cdots, d_k$ todos los divisores positivos de $n$. Definimos

$$\sum_{d|n} f(d) = f(d_1) + f(d_2) + \cdots + f(d_k).$$

**Definición 1.6**. (Convolución de Dirichlet)**.** Si $f$ y $g$ son funciones aritméticas, definimos la **convolución de Dirichlet** o **producto de Dirichlet** de $f$ y $g$, como la función aritmética $f * g$ definida como:

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right), \ \forall \ n \in \mathbb{N}.$$

Para ver que la operación $*$ es asociativa, conmutativa y distributiva respecto a la suma, necesitaremos algunos lemas.

**Lema 1.1.** *Si $k \in \mathbb{N}$, $D \subset \mathbb{N}$ y $f, g : \{1, \ldots, k\} \longrightarrow D$ son dos funciones biyectivas y estrictamente crecientes, entonces $f = g$.*

*Demostración.* Como $D \subset \mathbb{N}$ podemos ordenar los elementos de $D$, digamos $D = \{d_1, \ldots, d_k\}$, donde $d_1 < d_2 < \cdots < d_k$. Tenemos que $d_1$ es entonces el elemento mínimo de $D$. Sin embargo, tenemos que $f(1) \leq f(i)$ y $g(1) \leq g(i)$, $\forall \ i = 1, \ldots, k$ y como $f$ y $g$ son suprayectivas, entonces $f(1) \leq d_1$ y $g(1) \leq d_1$, además $d_1 \leq f(1)$ y $d_1 \leq g(1)$ por ser $d_1$ el elemento mínimo de $D$. Luego $f(1) = d_1 = g(1)$.

Supongamos que $f(i) = d_i = g(i), \forall\, i = 1, \ldots, n$ y $n+1 \leq k$. Si $n+1 = k$, como $f$ y $g$ son biyectivas, necesariamente $f(n+1) = d_{n+1} = g(n+1)$. Supongamos pues que $n+1 < k$. Tenemos que $d_{n+1}$ es el elemento mínimo del conjunto $D \setminus \{1, \ldots, d_n\}$. Notemos que $f(n+1), g(n+1) \in D \setminus \{1, \ldots, d_n\}$. En efecto, pues si $f(n+1) = d_{i_1}$ o $g(n+1) = d_{i_2}$, para algunos $i_1, i_2 \in \{1, \ldots, n\}$, entonces $f(n+1) = f(i_1)$ y $g(n+1) = g(i_2)$ por hipótesis de inducción y por inyectividad se tendría que $n+1 = i_1 \leq n$ o $n+1 = i_2 \leq n$, lo cual es absurdo. En consecuencia $f(n+1), g(n+1) \in D \setminus \{1, \ldots, d_n\}$ y por tanto $d_{n+1} \leq f(n+1)$ y $d_{n+1} \leq g(n+1)$.

Por otra parte, se tiene por suprayectividad que existen $j_1, j_2 \in \{1, \ldots, k\}$ tales que $f(j_1) = d_{n+1}$ y $g(j_2) = d_{n+1}$, más aún, $n+1 \leq j_1$ y $n+1 \leq j_2$, pues en caso contrario se tendría que $j_1 < n$ o $j_2 < n$, es decir, $f(j_1) < f(n)$ o $g(j_2) < g(n)$, es decir, $d_{n+1} < d_n$, lo que contradice la hipótesis. Luego $f(n+1) \leq f(j_1) = d_{n+1}$ y $g(n+1) \leq g(j_2) = d_{n+1}$. Se sigue finalmente que $f(n+1) = d_{n+1} = g(n+1)$. ∎

**Lema 1.2.** *Si $n \in \mathbb{N}$ y $d_1 = 1 < d_2 < \cdots < d_{k-1} < d_k = n$ son todos los divisores positivos de $n$, entonces $d_i d_{k+1-i} = n$, $\forall\ i = 1, \ldots, k$.*

*Demostración.* Sea $D = \{d_1, \ldots, d_k\}$ y consideremos las funciones $f : \{1, \ldots, k\} \longrightarrow D$ definida como $f(i) = d_i$, $\forall\ i = 1, \ldots, k$ y $g : \{1, \ldots, k\} \longrightarrow D$ definida como $g(i) = n/d_{k+1-i}$, $\forall\ i = 1, \ldots, k$. Es fácil ver que $f$ y $g$ cumplen las condiciones del lema anterior y por tanto $f(i) = g(i)$, $\forall\ i = 1, \ldots, k$, es decir, $d_i d_{k+1-i} = n$, $\forall\ i = 1, \ldots, k$. ■

**Proposición 1.1.** *Si $f$ y $g$ son funciones aritméticas, $n \in \mathbb{N}$ y $d_1 < \cdots < d_k$ son todos los divisores positivos de $n$, entonces*

$$(f * g)(n) = \sum_{i=1}^{k} f(d_i) g(d_{k+1-i}) = f(d_1)g(d_k) + \cdots + f(d_k)g(d_1).$$

*Demostración.* Se sigue de la definición de $(f * g)(n)$ y del Lema 1.2. ■

**Definición 1.7**. (Función identidad)**.** Definimos a la función identidad $I$ como

$$I(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1, \end{cases}$$

para cada $n \in \mathbb{N}$.

La siguiente proposición muestra que la función $I$ actúa como la identidad bajo la convolución de Dirichlet, entre otras propiedades algebraicas.

**Proposición 1.2.** *Si $f, g$ y $h$ son funciones aritméticas entonces se verifica lo siguiente:*

(i) $(f * g) * h = f * (g * h)$

(ii) $f * I = I * f = f$

(iii) $f * (g + h) = (f * g) + (f * h)$

(iv) $f * g = g * f$

*Demostración.* Sea $n \in \mathbb{N}$, sean $d_1 = 1 < d_2 < \cdots < d_k = n$ todos los divisores positivos de $n$ y para cada $i = 1, \ldots, k$ sean $c_{i,1} < c_{i,2} < \cdots < c_{i,m_i}$ los divisores positivos de $d_i$.

(i) Tenemos que

$$((f * g) * h)(n) = \sum_{i=1}^{k} \sum_{j=1}^{m_i} f(c_{i,j}) g(c_{i,m_i+1-j}) h(d_{k+1-i}) \tag{1.1}$$

y

$$(f*(g*h))(n)=\sum_{i=1}^{k}\sum_{j=1}^{m_{k+1-i}} f(d_i)g(c_{m_{k+1-i},j})h(c_{m_{k+1-i},m_{k+1-i}+1-j}). \tag{1.2}$$

Definamos los conjuntos

$$A=\left\{f(c_{i,j})g(c_{i,m_i+1-j})h(d_{k+1-i}) \mid i=1,\dots,k, j=1,\dots,m_i\right\}$$

$$B=\left\{f(d_i)g(c_{m_{k+1-i},j})h(c_{m_{k+1-i},m_{k+1-i}+1-j}) \mid i=1,\dots,k, j=1,\dots,m_i\right\},$$

y $C=\{f(a)f(b)f(c) \mid a,b,c\in\mathbb{N} \text{ y } abc=n\}$. Afirmamos que $A=C$ y $B=C$. En efecto, si $f(c_{i,j})g(c_{i,m_i+1-j})h(d_{k+1-i})$, entonces $c_{i,j}c_{i,m_i+1-j}d_{k+1-i}=d_id_{k+1-i}=n$, aplicando dos veces el Lema 1.2. Recíprocamente, si $a,b,c\in\mathbb{N}$ son tales que $abc=n$, entonces $c\mid n$, por tanto $c=d_j$, para algún $j=1,\dots,k$, es decir, $c=d_{k+1-i}$ para $i=k+1-j$ con $i=1,\dots,k$. Notemos entonces que por el lema 1.2, necesariamente se debe tener $ab=d_i$, por lo que $a=c_{i,j}$, para algún $j=1,\dots,m_i$ y aplicando el lema de nuevo se debe tener que $b=c_{i,m_i+1-j}$. En consecuencia $f(a)g(b)h(c)=f(c_{i,j})g(c_{i,m_i+1-j})h(d_{k+1-i})\in A$. Se sigue pues que $A=C$. Similarmente se demuestra que $B=C$.

Se tiene pues que $A=B$ y como las sumas (1.1) y (1.2) se extienden sobre los conjuntos $A$ y $B$, entonces deben coincidir, es decir, $((f*g)*h)(n)=(f*(g*h))(n)$.

(ii) Como $1<d_i,\ \forall\ i=2,\dots,k$ entonces $I(d_i)=0,\ \forall\ i=2,\dots,k$, luego por la proposición (1.1) se tiene que

$$\begin{aligned}(f*I)(n)&=\sum_{i=1}^{k}f(d_i)I(d_{k+1-i})=f(d_1)I(d_k)+\cdots+f(d_k)I(d_1)\\&=f(d_k)I(d_1)=f(n)I(1)=f(n)\cdot 1=f(n)\end{aligned}$$

Y

$$\begin{aligned}(I*f)(n)&=\sum_{i=1}^{k}I(d_i)f(d_{k+1-i})=I(d_1)f(d_k)+\cdots+I(d_k)f(d_1)\\&=I(d_1)f(d_k)=I(n)f(1)=1\cdot f(n)=f(n)\end{aligned}$$

(iii) Tenemos que

$$(f*(g+h))(n)=\sum_{i=1}^{k}f(d_i)(g+h)(d_{k+1-i})=\sum_{i=1}^{k}f(d_i)[g(d_{k+1-i})+h(d_{k+1-i})]$$

$$= \sum_{i=1}^{k} f(d_i)g(d_{k+1-i}) + \sum_{i=1}^{k} f(d_i)h(d_{k+1-i}) = (f * g)(n) + (f * h)(n).$$

(iv) La conmutatividad de la convolución de Dirichlet es clara, pues

$$(f * g)(n) = \sum_{i=1}^{k} f(d_i)g(d_{k+1-i}) = \sum_{i=1}^{k} g(d_i)f(d_{k+1-i}) = (g * f)(n).$$

■

Se puede definir también una multiplicación por escalares en el conjunto de funciones aritméticas.

**Definición 1.8.** Dados $c \in \mathbb{C}$ y $f \in \mathcal{A}$, se define $cf \in \mathcal{A}$ como la función

$$\begin{aligned} cf : \mathbb{N} &\longrightarrow \mathbb{C} \\ n &\longmapsto cf(n). \end{aligned}$$

Es una demostración rutinaria verificar la siguiente proposición.

**Proposición 1.3.** *El grupo abeliano $(\mathcal{A}, +)$ junto con la multiplicación por escalares definida anteriormente constituyen un espacio vectorial sobre el campo $\mathbb{C}$, donde el elemento neutro aditivo es la función $\mathbf{0}$. De ahora en adelante, este espacio vectorial será llamado simplemente el espacio de las funciones aritméticas.*

**Proposición 1.4.** *Si $c \in \mathbb{C}$ y $f, g \in \mathcal{A}$ entonces $c(f * g) = (cf) * g = f * (cg)$.*

*Demostración.* Se tiene que para cualquier $n \in \mathbb{N}$,

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

Luego $c(f * g) = (cf) * g$. Las demás igualdades se prueban similarmente. ■

**Corolario 1.1.** *El anillo $(\mathcal{A}, +, *)$ es un álgebra conmutativa con identidad sobre el campo $\mathbb{C}$.*

## 1.2. Una norma para funciones aritméticas

**Definición 1.9.** Sea $\mathcal{A}$ el conjunto de todas las funciones aritméticas. Definimos la función

$$\mathcal{N} : \mathcal{A} \longrightarrow \mathbb{N} \cup \{0\}$$

$$f \longmapsto \mathcal{N}(f) = \begin{cases} 0 & \text{si } f = \mathbf{0} \\ \text{mín}\,\{n : f(n) \neq 0\} & \text{si } f \neq \mathbf{0}. \end{cases}$$

**Proposición 1.5.** *La función $\mathcal{N}$ definida anteriormente tiene las siguientes propiedades:*

(i) $\mathcal{N}(f) = 0 \iff f = 0, \forall\, f \in \mathcal{A}$.

(ii) $\mathcal{N}(f * g) = \mathcal{N}(f)\mathcal{N}(g), \forall\, f, g \in \mathcal{A}$.

(iii) $\text{mín}\{\mathcal{N}(f), \mathcal{N}(g)\} \leq \mathcal{N}(f + g), \forall\, f, g \in \mathcal{A}$.

(iv) *Si* $\mathcal{N}(f) \neq \mathcal{N}(g)$ *entonces* $\mathcal{N}(f + g) = \text{mín}\{\mathcal{N}(f), \mathcal{N}(g)\}$.

*Demostración.* (i) Si $f = 0$ por definición se tiene que $\mathcal{N}(f) = 0$. Si $f \neq 0$, entonces mín $\{n : f(n) \neq 0\} \neq 0$, i.e. $\mathcal{N}(f) \geq 1 \neq 0$. Por tanto $\mathcal{N}(f) = 0$ implica que $f = 0$.

(ii) Si $f = 0$ o $g = 0$ entonces $\mathcal{N}(f) = 0$ o $\mathcal{N}(g) = 0$. Además $(f * g)(n) = \sum_{d|n} f(n)g(n/d) = 0$, $\forall\ n \in \mathbb{N}$, es decir, $\mathcal{N}(f * g) = 0 = \mathcal{N}(f)\mathcal{N}(g)$. Supongamos pues que $f \neq 0$ y $g \neq 0$. Sean $a = \mathcal{N}(f)$ y $b = \mathcal{N}(g)$. Afirmamos que $ab = \text{mín}\,\{n : (f * g)(n) \neq 0\} = m$.

En efecto, se tiene

$$\begin{aligned} (f * g)(ab) &= \sum_{d|ab} f(d)g(ab/d) \\ &= \sum_{\substack{d|ab \\ a\leq d}} f(d)g(ab/d), \text{ pues } f(d) = 0,\ \forall\ d < a \\ &= \sum_{\substack{d|ab \\ a\leq d \\ ab/d\leq b}} , \text{ pues } a \leq d \implies ab/d \leq b \\ &= \sum_{a=d} f(d)g(ab/d), \text{ pues } g(d) = 0,\ \forall\ d < b \\ &= f(a)g(b) \neq 0. \end{aligned}$$

Luego $m \leq ab$ por elección de $m$. Si $m < ab$ entonces

$$(f * g)(m) = \sum_{d|m} f(d)g(m/d) = \sum_{\substack{d|m \\ b\leq m/d}} f(d)g(m/d) = \sum_{\substack{d|m \\ d<a}} f(d)g(m/d) = 0,$$

pues $b \leq m/d$ implica que $d < a$ y $f(d) = 0$. Pero esto contradice la elección de $m$. Por tanto, $m = ab$.

(iii) Sin pérdida de generalidad se puede suponer que $a \leq b$, de tal manera que $\min\{a, b\} = a$. Si $n < a$ entonces $(f + g)(n) = f(n) + g(n) = 0$, por lo que

$$\min\{\mathcal{N}(f), \mathcal{N}(g)\} = a \leq \min\{n : (f + g)(n) \neq 0\} = \mathcal{N}(f + g).$$

(iv) Supóngase de nuevo sin pérdida de generaliad que $a < b$. Entonces

$$(f + g)(a) = f(a) + f(a) = f(a) + 0 = f(a) \neq 0,$$

por tanto, $N(f+g) \leq a = \min\{a, b\} = \min\{\mathcal{N}(f), \mathcal{N}(g)\}$. El resultado se sigue ahora del inciso (iii).

■

**Teorema 1.1.** *$\mathcal{A}$ es un dominio entero.*

*Demostración.* Si $f, g \in \mathcal{A}$ y $f * g = 0$ entonces $\mathcal{N}(f * g) = 0 \implies \mathcal{N}(f)\mathcal{N}(g) = 0 \implies \mathcal{N}(f) = 0$ o $\mathcal{N}(g) = 0 \implies f = 0$ o $g = 0$. ■

*Observación 1.1.* Como ocurre en cualquier anillo con identidad, el conjunto de elementos invertibles forma un grupo respecto a la operación de multiplicación, en este caso, respecto a la convolución de Dirichlet. Este grupo se denotará $(\mathcal{A}^*, *)$ o simplemente como $\mathcal{A}^*$ cuando no haya riesgo de confusión.

**Proposición 1.6.** *$f \in \mathcal{A}^*$ si y sólo si $\mathcal{N}(f) = 1$.*

*Demostración.* Si $f(1) \neq 0$, defínase

$$\begin{aligned} f^{-1}(1) &= \frac{1}{f(1)} \\ f^{-1}(n) &= -\frac{1}{f(1)} \sum_{\substack{d|n \\ d\neq n}} f\left(\frac{n}{d}\right) f^{-1}(d), \quad n > 1. \end{aligned} \tag{1.3}$$

Es fácil verificar que la ecuación (1.3) define a $f^{-1}$ de tal forma que $f * f^{-1} = I$, pues $f(1)f^{-1}(1) = 1$ y si $n > 1$ entonces

$$\begin{aligned} (f * f^{-1})(n) = \sum_{d|n} f(d) f^{-1}\left(\frac{n}{d}\right) &= f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d\neq n}} f(d) f^{-1}\left(\frac{n}{d}\right) \\ &= f(1)f^{-1}(n) - f(1)f^{-1}(n) = 0 \end{aligned}$$

es decir, $f * f^{-1} = I$.

Si se supone ahora que $f$ es invertible, entonces, en particular, se tiene que $(f * f^{-1})(1) = 1$, y por tanto $f(1) \neq 0$, es decir, $\mathcal{N}(f) = 1$. ■

**Proposición 1.7.** *Si $\mathcal{N}(f) = p$ para algún número primo $p$, entonces $f$ es irreducible en $\mathcal{A}$.*

*Demostración.* Como $p \neq 0$ y $p \neq 1$, entonces $f$ no es cero ni es una unidad. Además, si $f = g * h$ para algunas funciones $g, h \in \mathcal{A}$, entonces $g, h \neq 0$, pues en caso contrario $f = 0$ y en consecuencia $\mathcal{N}(f) = 0 \neq p$, así que $\mathcal{N}(f)$ y $\mathcal{N}(h)$ son enteros positivos. Luego $\mathcal{N}(f) = \mathcal{N}(g * h) = \mathcal{N}(g)\mathcal{N}(h) = p$ y como $p$ es primo, entonces $\mathcal{N}(g) = 1$ o bien $\mathcal{N}(h) = 1$, es decir, $g$ o $h$ es unidad. Como $g$ y $h$ fueron arbitrarios, entonces $f$ debe ser irreducible en $\mathcal{A}$. ■

**Teorema 1.2** (Condición de la cadena ascendente)**.** *Si $\{f_i\}_{i\in\mathbb{N}}$ es un un conjunto de funciones aritméticas con la propiedad de que $f_1 \neq 0$ y $f_i = f_{i+1} * g_i$ y $g_i$ no es unidad, para cada $i \in \mathbb{N}$, entonces $\{f_i\}_{i\in\mathbb{N}}$ es un conjunto finito.*

*Demostración.* Supóngase que $\{f_i\}_{i\in\mathbb{N}}$ es un conjunto infinito. Se tiene que $\mathcal{N}(i) = \mathcal{N}(f_{i+1})\mathcal{N}(g_{i+1}) > \mathcal{N}(f_{i+1})$, para cada $i \in \mathbb{N}$, pues $g_{i+1}$ no es unidad, en particular $\mathcal{N}(f_1) > \mathcal{N}(f_i), \forall\, i \in \mathbb{N}$. Luego $\{\mathcal{N}(f_i)\}_{i\in\mathbb{N}}$ es una sucesión en $\mathbb{N}$, por ser $\{f_i\}_{i\in\mathbb{N}}$ infinito, y además estrictamente creciente, por tanto $\lim_{i\to\infty} \mathcal{N}(f_i) = \infty$, pero esto implica que $\mathcal{N}(f_1) > n, \forall\, n \in \mathbb{N}$, en particular $\mathcal{N}(f_1) > \mathcal{N}(f_1)$, lo cual es absurdo. ■

El teorema anterior permite probar inmediatamente que cualquier elemento no cero y no unidad de $\mathcal{A}$ se puede expresar como producto finito de elementos irreducibles de $A$.

**Proposición 1.8.** *Si $f \in \mathcal{A} \setminus (\mathcal{A}^* \cup \{\mathbf{0}\})$, entonces $f$ es producto finito de elementos irreducibles en $\mathcal{A}$.*

*Demostración.* Como $f \neq \mathbf{0}$, en lo que sigue de esta demostración se debe tener que todas las funciones involucradas son distintas de cero. Se probará primero que $f$ tiene un factor irreducible. En efecto, si $f$ es irreducible, entonces no hay nada que probar. Supóngase que este no es el caso y por tanto $f = f_1 * g_1$, donde $f_1$ y $g_1$ no son unidades. Si $f_1$ es irreducible hemos concluido. En caso contrario se tiene $f_1 = f_2 * g_2$, donde $f_2$ y $g_2$ no son unidades y además $f_1 \neq f_2$, pues de otra forma se tendría, por la ley de cancelación, que $I = g_2$, contradiciendo la elección de $g_2$. De manera inductiva se tiene una sucesión de funciones $\{f_i\}_{i\in\mathbb{N}}$ tal que $f_i = f_{i+1} * g_{i+1}$, donde $g_{i+1}$ no es unidad y $f_i \neq f_{i+1}, \forall\, i \in \mathbb{N}$, luego dicho conjunto es infinito, lo que contradice el Teorema 1.2. En consecuencia, el proceso anterior debe terminar y debe existir $M \in \mathbb{N}$ tal que $f_{M-1} = f_M * g_M$, donde $f_M$ es irreducible y $f_M \mid f$.

Se probará ahora el resultado principal. Escribiendo $f_M = p_1$, se tiene que $f = p_1 * q_1$, con $p_1$ irreducible. Si $q_1$ es una unidad, entonces $f$ es irreducible y ya terminamos. Si $q_1$ no es unidad, por el párrafo anterior, $q_1$ debe tener un factor irreducible, es decir,

$q_1 = p_2 * q_2$, donde $p_2$ es irreducible, y por tanto no es unidad, además, $q_1 \neq q_2$ pues de otra forma se tendría, por la ley de cancelación, que $I = p_2$, lo que contradice la elección de $p_2$. Si $q_2$ es unidad, entonces $q_1$ es irreducible y $f = p_1 * q_1$ es la factorización buscada. Si este proceso nunca terminara, de forma inductiva se tendría una sucesión $\{q_i\}_{i\in\mathbb{N}}$ tal que $q_i = p_{i+1} * q_{i+1}$, con $p_i$ no unidad y además $q_i \neq q_{i+1}, \forall\, i \in \mathbb{N}$, de tal manera que dicho conjunto es infinito, lo que contradice de nuevo el Teorema 1.2. En consecuencia, el proceso eventualmente termina y por tanto existe $N \in \mathbb{N}$ tal que $q_N = p_{N+1} * q_{N+1}$, donde $q_{N+1}$ es unidad y $p_{N+1}$ es irreducible. Luego

$$f = p_1 * p_2 * \cdots * p_N * q_N,$$

donde $p_1, \ldots, p_N$ y $q_N$ son irreducibles. ■

Habiendo llegado hasta aquí, uno puede sospechar que el dominio $\mathcal{A}$ es un dominio de factorización única. Esta sospecha es, de manera sorprendente, acertada. Sin embargo, la demostración de este hecho no es tan sencilla como la de la proposición anterior.

**Teorema 1.3.** *$\mathcal{A}$ es un dominio de factorización única.*

*Demostración.* El hecho de que toda función aritmética se puede escribir como producto de funciones aritméticas irreducibles ha quedado en evidencia en la proposición anterior. Una demostración de la unicidad de dicha factorización se puede encontrar en [5, 18, p. 985]. Ahí se prueba que el anillo de series de potencias formales en un conjunto numerable de variables $\{x_1, x_2, \ldots\}$ es un dominio de factorización única. El resultado se sigue entonces del hecho de que este anillo es isomorfo al anillo de funciones aritméticas mediante el isomorfismo

$$\begin{aligned} P : \mathcal{A} &\longrightarrow \mathbb{C}[[x_1, x_2, \ldots]] \\ P(f) &\longmapsto \sum_{n\in\mathbb{N}} f(n) x_1^{\alpha_1} \cdots x_\nu^{\alpha_\nu}, \end{aligned}$$

donde $n = p_1^{\alpha_1} \cdots p_\nu^{\alpha_\nu}$ es la factorización en primos de $n$. Se tiene que $P(f+g) = P(f) + P(g)$ y $P(f*g) = P(f)P(g)$, donde la multiplicación de dos series de este tipo se realiza agrupando términos "semejantes", es decir, monomios iguales. Otra demostración de este hecho se puede encontrar en [14]. Ambas demostraciones utilizan el hecho de que los anillos de series de potencias formales en un número finito de variables $\mathbb{C}[[x_1, \ldots, x_n]]$ son dominios de factorización única, para cada $n \in \mathbb{N}$. ■

**Corolario 1.2.** *Todo elemento irreducible en $\mathcal{A}$ es primo en $\mathcal{A}$.*

Siendo $\mathcal{A}$ un dominio de factorización única, cabe preguntarse si también es un dominio de ideales principales. La siguiente proposición muestra que este no es el caso.

**Proposición 1.9.** *$\mathcal{A}$ no es un dominio de ideales principales.*

*Demostración.* Considere $f = (0, 1, 0, \ldots)$ y $g = (0, 0, 1, 0, \ldots)$. Se tiene que $\mathcal{N}(f) = 2$ y $\mathcal{N}(g) = 3$, ambos números primos. Afirmamos que $I$ es un máximo común divisor de $f$ y $g$. Claro que $I \mid f$ y $I \mid g$. Si $h \in \mathcal{A}$ es tal que $h \mid f$ y $h \mid g$, entonces $f = hk_1$ y $g = hk_2$, con $h, k_1, k_1 \in \mathcal{A} \setminus \{\mathbf{0}\}$. Luego $2 = \mathcal{N}(h)\mathcal{N}(k_1) < 3 = \mathcal{N}(h)\mathcal{N}(k_2)$, en consecuencia, $1 \leq \mathcal{N}(k_1) < \mathcal{N}(k_2)$, así que necesariamente $\mathcal{N}(k_2) = 3$ y $\mathcal{N}(h) = 1$. Luego $h$ es unidad, es decir $h \mid I$. Esto prueba que $I$ es máximo común divisor de $f$ y $g$.

Si $\mathcal{A}$ fuera un dominio de ideales principales por [10, §III.3, Thm. 3.11.(ii), p. 140], existirían $s, t \in \mathcal{A}$ tales que $I = f * s + g * t$, en particular, $1 = I(1) = f(1)s(1) + g(1)t(1) = 0$, lo cual es imposible. ■

**Teorema 1.4.** *$\mathcal{A}$ es un anillo local.*

*Demostración.* Por [10, §III.4, Thm. 4.13.(iii), p. 147], basta probar que los elementos no invertibles de $\mathcal{A}$ forman un ideal de $\mathcal{A}$. En efecto, se tiene que $\mathbf{0} \in \mathcal{A} \setminus \mathcal{A}^*$. Si $f \in \mathcal{A} \setminus \mathcal{A}^*$ y $g \in \mathcal{A}$, entonces $f(1) = 0$, en consecuencia $(f * g)(1) = f(1)g(1) = 0$, es decir, $f * g \in \mathcal{A} \setminus \mathcal{A}^*$. Además, si $h \in \mathcal{A} \setminus \mathcal{A}^*$, entonces $h(1) = 0$ y por tanto $f(1) - h(1) = 0$, es decir $f - h \in \mathcal{A} \setminus \mathcal{A}^*$. Esto prueba que $\mathcal{A} \setminus \mathcal{A}^*$ es un ideal de $\mathcal{A}$. ■

**Proposición 1.10.** *Si $f \in \mathcal{A}$ es tal que $f(1) = 0$ y $f(p) \neq 0$ para algún primo $p$, entonces $f$ es irreducible en $\mathcal{A}$.*

*Demostración.* Por hipótesis $f$ no es cero y no es unidad. Supongamos que $f = g * h$. Si $g$ y $h$ no fueran unidades se tendría que $g(1) = 0$ y $h(1) = 0$, por tanto, $f(p) = (g * h)(p) = g(1)h(p) + g(p)h(1) = 0$, lo que contradice la hipótesis. En consecuencia alguna de las funciones $g$ o $h$ es unidad. ■

Un colorario de la proposición anterior y el Corolario 1.2 es el siguiente.

**Corolario 1.3.** *Si $f \in \mathcal{A}$ es tal que $f(1) = 0$ y $f(p) \neq 0$ para algún primo $p$, entonces $f$ es un elemento primo de $\mathcal{A}$.*

Hasta aquí se tiene que el anillo $\mathcal{A}$ satisface cierto tipo de condición de la cadena ascendente. Sin embargo, la siguiente proposición muestra que en general no se cumple la condición de la cadena descendente, es decir, $\mathcal{A}$ no es artiniano.

**Proposición 1.11.** *$\mathcal{A}$ no es un anillo artiniano.*

*Demostración.* Para cada $n \in \mathbb{N}$ defínase $I_n = \{f \in \mathcal{A} : \mathcal{N}(f) \geq n\} \cup \{\mathbf{0}\}$. Se tiene lo siguiente:

(1) $I_n$ es un ideal de $\mathcal{A}$, para cada $n$. En efecto, por definición se tiene $I_n \neq \emptyset$. Si $f, g \in I_n$ entonces $\mathcal{N}(f) \geq n$ y $\mathcal{N}(g) \geq n$, luego $\mathcal{N}(f-g) \geq \min\{\mathcal{N}(f), \mathcal{N}(-g)\} = \min\{\mathcal{N}(f), \mathcal{N}(g)\} \geq n$, luego $f - g \in I_n$.

Además, si $h \in \mathcal{A}$, se tienen dos casos. Si $h = \mathbf{0}$, entonces $f * h = 0 \in I_n$. Si $h \neq \mathbf{0}$, entonces $\mathcal{N}(f) \geq 1$, de tal manera que $\mathcal{N}(f * g) = \mathcal{N}(f)\mathcal{N}(h) \geq \mathcal{N}(f) \geq n$, es decir, $f * h \in I_n$. Esto prueba que $I_n$ es un ideal de $\mathcal{A}$.

(2) $I_{n+1} \subset I_n$, para cada $n \in \mathbb{N}$, pues $\mathcal{N}(f) \geq n+1$ implica que $\mathcal{N}(f) \geq n$.

(3) $I_n \not\subset I_{n+1}$, para cada $n \in \mathbb{N}$, pues considere $f \in \mathcal{A}$ definida como

$$f(k) = \begin{cases} 1 & \text{si } k = n \\ 0 & \text{en otro caso.} \end{cases}$$

Entonces $\mathcal{N}(f) = n < n+1$, es decir, $f \in I_n$, pero $f \notin I_{n+1}$.

Se tiene pues una cadena descendente infinita de ideales de $\mathcal{A}$, luego $\mathcal{A}$ no es artiniano. ■

## 1.3. Funciones multiplicativas

**Definición 1.10**. (Función multiplicativa)**.** Se dice que una función aritmética $f$ es **multiplicativa** si no es idénticamente cero y para todo $m, n \in \mathbb{N}$, $(m,n) = 1$ implica que $f(mn) = f(m)f(n)$.

*Observación 1.2.* Se denota al conjunto de funciones multiplicativas como $\mathcal{M}$. En general si $f$ y $g$ son funciones multiplicativas entonces $f - g$ no es necesariamente una función multiplicativa, sin embargo, $f * g$ sí lo es.

**Lema 1.3.** *Si $(a,b) = 1$ y $d \in \mathbb{N}$, entonces $(ab,d) = (a,d)(b,d)$.*

*Demostración.* Escríbanse $(a,d) = ax+dy$ y $(b,d) = bs+dt$, para algunos $x, y, s, t \in \mathbb{Z}$. Entonces

$$(a,d)(b,d) = abxs + axdt + dybs + dydt = ab(xs) + d(axt + ybs + ydt),$$

por tanto, $(ab,d) \mid (a,d)(b,d)$.

Por otro lado, escríbase $1 = az + bw$, para algunos $z, w \in \mathbb{Z}$. Entonces $d = daz + dbw$. Además, como $a = (a,d)m$, $b = (b,d)n$, $d = (b,d)p$ y $d = (a,d)q$ para algunos $m, n, p, q \in \mathbb{Z}$, entonces

$$d = (a,d)(b,d)(pmz + qnw),$$

es decir, $(a,d)(b,d) \mid d$. Dado que $ab = (a,d)(b,d)mn$, entonces $(a,d)(b,d) \mid ab$ y en consecuencia $(a,d)(b,d) \mid (ab,d)$. Se sigue que $(ab,d) = (a,d)(b,d)$. ■

**Lema 1.4.** *Si $(a,b) = 1$, $a_1, \ldots, a_l$ son todos los divisores positivos de $a$ y $b_1, \ldots, b_m$ son todos los divisores positivos de $b$, entonces $\{d > 0 : d \mid ab\} = \{a_i b_j : i = 1, \ldots, l, \ \ j = 1, \ldots, m\}$.*

*Demostración.* Si $a_i, b_j$ son divisores de $a$ y $b$, respectivamente, entonces existen $s, t \in \mathbb{Z}$ tales que $a = a_i s$ y $b = b_j t$, luego $ab = a_i b_j st$, es decir, $a_i b_j \mid ab$. Recíprocamente, si $d$ es un divisor de $ab$, entonces $(ab,d) = d$, pero por el lema anterior $(ab,d) = (a,d)(b,d)$, luego $d = (a,d)(b,d)$, donde $(a,d)$ es un divisor positivo de $a$ y $(b,d)$ es un divisor positivo de $b$. ■

**Teorema 1.5.** *$(\mathcal{M}, *)$ es un subgrupo de $(\mathcal{A}^*, *)$.*

*Demostración.* Si $f \in \mathcal{M}$, entonces $f \neq \mathbf{0}$ y existe $N \in \mathbb{N}$ tal que $f(N) \neq 0$, luego $f(N) = f(1 \cdot N) = f(1)f(N)$ y en consecuencia $1 = f(1)$, es decir, $f \in \mathcal{A}^*$. Esto prueba que $\mathcal{M} \subset \mathcal{A}^*$.

Claro que el conjunto $\mathcal{M}$ es no vacío, pues $I \in \mathcal{M}$. Veamos que la operación $*$ es cerrada en $\mathcal{M}$. Sean $f, g$ funciones multiplicativas, sean $a, b \in \mathbb{N}$ tales que $(a,b) = 1$ y sean $a_1, \ldots, a_l$ y $b_1, \ldots, b_m$ todos los divisores positivos de $a$ y $b$, respectivamente. Entonces $(a_i, b_j) = 1$, para cada $i = 1, \ldots, l$ y para cada $j = 1, \ldots, m$, luego

$$\begin{aligned}
(f*g)(a)(f*g)(b) &= \left[\sum_{i=1}^{l} f(a_i) g\left(\frac{a}{a_i}\right)\right]\left[\sum_{j=1}^{m} f(b_j) g\left(\frac{b}{b_i}\right)\right] \\
&= \sum_{i=1}^{l}\sum_{j=1}^{m} f(a_i) g\left(\frac{a}{a_i}\right) f(b_i) g\left(\frac{b}{b_i}\right) \\
&= \sum_{i=1}^{l}\sum_{j=1}^{m} f(a_i b_j) g\left(\frac{ab}{a_i b_j}\right) \\
&= \sum_{d \mid ab} f(d) g\left(\frac{ab}{d}\right) = (f*g)(ab)
\end{aligned}$$

por el Lema 1.4.

Como ya se probó al inicio de esta demostración, si $f$ es multiplicativa entonces $f(1) = 1$, por lo que existe $f^{-1}$. Veamos que $f^{-1} \in \mathcal{M}$. Para esto construiremos, a partir de $f$, una función multiplicativa $g$ con la propiedad de que $f * g = I$, con lo que quedará demostrado que $f^{-1}$ es multiplicativa por la unicidad de la inversa. Se procede definiendo a $g$ de forma gradual:

(1) $g(1) = 1$.

(2) Para cada primo $p$ se define $g(p) = -f(p)$. De tal manera que

$$(f * g)(p) = \sum_{d|p} f(p)g\left(\frac{p}{d}\right) = f(1)g(p) + f(p)g(1) = -f(p) + f(p) = 0.$$

(3) Para cada $a \in \mathbb{N}$ y para cada primo $p$ se define, recursivamente,

$$g(p^a) = -f(p)g(p^{a-1}) - \cdots - f(p^a)g(1)$$

de tal manera que

$$\begin{aligned}(f * g)(p^a) &= \sum_{d|p^a} f(d)g\left(\frac{p^a}{d}\right) = f(1)g(p^a) + f(p)g(p^{a-1}) + \cdots + f(p^a)g(1) \\ &= -f(p)g(p^{a-1}) - \cdots - f(p^a)g(1) + f(p)g(p^{a-1}) + \cdots + f(p^a)g(1) = 0.\end{aligned}$$

(4) Se define

$$g\left(\prod p_i^{a_i}\right) = \prod g(p_i^{a_i}).$$

para cualquier producto finito de potencias de primos, con $p_i \neq p_j$ si $i \neq j$. La función $g$ ha quedado entonces definida para cualquier entero positivo.

(5) $g$ es multiplicativa, pues si $a = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ y $b = q_1^{\beta_1} \cdots q_l^{\beta_l}$ son tales que $(a, b) = 1$, entonces $p_i \neq q_j$, luego

$$\begin{aligned}g(ab) = g(p_1^{\alpha_1} \cdots p_m^{\alpha_m} q_1^{\beta_1} \cdots q_l^{\beta_l}) &= g(p_1^{\alpha_1}) \cdots g(p_m^{\alpha_m}) g(q_1^{\beta_1}) \cdots g(q_l^{\beta_l}) \\ &= g(p_1^{\alpha_1} \cdots p_m^{\alpha_m}) g(q_1^{\beta_1} \cdots q_l^{\beta_l}) = g(a)g(b)\end{aligned}$$

(6) Como la operación $*$ es cerrada en $\mathcal{M}$, entonces $f * g$ es multiplicativa.

(7) Si $n > 1$ y $n = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$ es su factorización en primos, entonces

$$(f * g)(n) = (f * g)(p_1^{\alpha_1}) \cdots (f * g)(p_l^{\alpha_l}) = 0$$

donde la primera igualdad se cumple por ser $f * g$ multiplicativa y la segunda por el inciso (3). Además, $(f * g)(1) = f(1)g(1) = 1$. En consecuencia $f * g = I$.

(8) Se sigue que $g = f^{-1}$ y como $g$ es multiplicativa, entonces $f^{-1}$ también lo es.

■

**Corolario 1.4.** *Si $f * g$ es multiplicativa y $g$ es multiplicativa, entonces $f$ también lo es.*

*Demostración.* Como $g$ es multiplicativa, entonces existe $g^{-1}$ y también es multiplicativa, luego $f = (f * g) * g^{-1}$ es multiplicativa por ser producto de funciones multiplicativas. ■

## 1.4. Isomorfismos entre grupos de funciones aritméticas

Se denotará como $\mathcal{A}_{\mathbb{R}}$ al conjunto de funciones aritméticas real valuadas, es decir, $\mathcal{A}_{\mathbb{R}} = \{f \in \mathcal{A} : f(n) \in \mathbb{R}, \forall\, n \in \mathbb{N}\}$. Asimismo, se define $P = \{f \in \mathcal{A} : f(1) > 0\}$. Es fácil verificar que $(\mathcal{A}_{\mathbb{R}}, +)$ y $(P, *)$ son subgrupos de $(\mathcal{A}, +)$ y de $(\mathcal{A}^*, *)$, respectivamente. Más aún, estos grupos son isomorfos.

**Lema 1.5.** $(\mathcal{A}_{\mathbb{R}}, +) \cong (P, *)$.

*Demostración.* El isomorfismo buscado es

$$\begin{aligned} L : (P, *) &\longrightarrow (\mathcal{A}_{\mathbb{R}}, +) \\ f &\longmapsto Lf \end{aligned}$$

donde $Lf(1) = \log(1)$ y $Lf(n) = \sum_{d|n} \log(d) f(d) f^{-1}(n/d)$ para $n > 1$. Se tiene que $L$ es en efecto un homomorfismo, pues para $n = 1$ se tiene

$$L(f * g)(1) = \log(f * g)(1) = \log(f(1)g(1)) = \log f(1) + \log g(1) = Lf(1) + Lg(1).$$

Para el caso $n > 1$, nótese primero que para cualquier $n \in \mathbb{N}$,

$$\begin{aligned} \log(n)(f * g)(n) &= \log(n) \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \\ &= \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \left[\log \frac{n}{d} + \log d\right] \\ &= \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \log\left(\frac{n}{d}\right) + \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \log(d) \\ &= (f * (\log \cdot g))(n) + ((\log \cdot f) * g)(n), \end{aligned}$$

es decir, $\log \cdot (f * g) = f * (\log \cdot g) + (\log \cdot f) * g$. Multiplicando por $(f * g)^{-1} = f^{-1} * g^{-1}$ a ambos lados de la ecuación, se tiene que

$$(\log \cdot (f * g)) * (f * g)^{-1} = (\log \cdot g) * g^{-1} + (\log \cdot f) * f^{-1},$$

es decir, $L(f * g) = Lf + Lg$ y en particular para $n > 1$. Esto prueba que $L$ es un homomorfismo.

$L$ también es suprayectivo, pues si $f \in \mathcal{A}_{\mathbb{R}}$, defínase $g(1) = \exp(f(1))$. Entonces $Lg(1) = \log g(1) = \log \exp(f(1)) = f(1)$, pues $f(1) \in \mathbb{R}$. Además, como $g(1) > 0$ existe $g^{-1}$ y se define recursivamente, para $n > 1$,

$$g(n) = \frac{1}{\log(n) g^{-1}(1)} \left[ f(n) - \sum_{\substack{d|n \\ d \neq 1, n}} \log(d) g(d) g^{-1}\left(\frac{n}{d}\right) \right].$$

Esta ecuación implica que

$$f(n) = g(n)\log(n)g^{-1}(1) + g(1)\log(1)g^{-1}(n) + \sum_{\substack{d|n \\ d\neq 1,n}} \log(d)g(d)g^{-1}\left(\frac{n}{d}\right)$$
$$= \sum_{d|n} \log(d)g(d)g^{-1}\left(\frac{n}{d}\right) = Lg(n).$$

En consecuencia, $Lg(n) = f(n), \forall\, n \in \mathbb{N}$, es decir, $Lg = f$.

Finalmente, se tiene que $L$ es inyectivo. En efecto, si $L(f) = L(g)$, entonces $L(f) - L(g) = 0$, pero $-Lg = Lg^{-1}$ por ser $L$ un homomorfismo, luego $Lf + Lg^{-1} = L(f * g^{-1}) = 0$. Para $n = 1$ esto implica que $\log(f * g^{-1}(1)) = 0$ y por tanto $(f * g^{-1})(1) = 1$. Si $n = 2$, entonces

$$L(f * g^{-1})(2) = \log(1)(f * g^{-1})(1)(f * g^{-1})^{-1}(2) + \log(2)(f * g^{-1})(2)(f * g^{-1})(1) = 0,$$

pero $\log(1) = 0$, por tanto $\log(2)(f * g^{-1})(2)(f * g^{-1})(1) = 0$ y dado que $(f * g^{-1})(1) \neq 0$, entonces $(f * g^{-1})(2) = 0$. Supóngase que $(f * g^{-1})(d) = 0$, para cada $1 < d < n$. Entonces $L(f * g) = 0$ implica que

$$\log(n)(f * g^{-1})(n)(f * g^{-1})(1) + \sum_{\substack{d|n \\ d\neq 1,n}} \log(d)\underbrace{(f * g^{-1})(d)}_{0}(f * g^{-1})^{-1}\left(\frac{n}{d}\right) = 0,$$

pues $\log(1) = 0$, por tanto, $\log(n)(f * g^{-1})(n)(f * g^{-1})(1) = 0$ y por tanto $(f * g^{-1})(n) = 0$. Esto prueba que para cada $n > 1$, $(f * g^{-1}) = 0$. Así pues, se tiene que $f * g^{-1} = I$, por tanto, $f = g$. ∎

Se denota $\mathcal{A}' = \{f \in \mathcal{A}_{\mathbb{R}} : f(n) = 0, \forall\, n \neq p^{\alpha}, p \text{ primo y } \alpha \in \mathbb{N}\}$. La siguiente proposición es una caracterización de las funciones multiplicativas respecto al conjunto $\mathcal{A}'$ y al isomorfismo $L$.

**Proposición 1.12.** *$f \in \mathcal{M}$ si y sólo si $Lf \in \mathcal{A}'$.*

*Demostración.* Supóngase primero que $f$ es multiplicativa. Entonces $f(1) = 1$, por tanto, $Lf(1) = \log f(1) = \log 1 = 0$. Si $N > 1$ no es potencia de ningún primo, entonces $N = mn$, con $(m, n) = 1$ y $n, m > 1$. Luego

$$Lf(N) = Lf(mn) = \sum_{d|mn} \log(d)f(d)f^{-1}\left(\frac{mn}{d}\right)$$
$$= \sum_{d|m}\sum_{e|n} f(d)f(e)f^{-1}\left(\frac{m}{d}\right)f^{-1}\left(\frac{n}{e}\right)(\log(d) + \log(e))$$

$$
\begin{aligned}
&= \sum_{d|m} \log(d) f(d) f^{-1}\left(\frac{m}{d}\right) \sum_{e|n} f(e) f^{-1}\left(\frac{n}{e}\right) \\
&+ \sum_{e|n} \log(e) f(e) f^{-1}\left(\frac{n}{e}\right) \sum_{d|m} f(d) f^{-1}\left(\frac{m}{e}\right) \\
&= Lf(m) \sum_{e|n} f(e) f^{-1}\left(\frac{n}{e}\right) + Lf(n) \sum_{d|m} f(d) f^{-1}\left(\frac{m}{d}\right) \\
&= Lf(m) I(n) + Lf(n) I(m) = 0,
\end{aligned}
$$

pues $m, n > 1$. Luego $f \in \mathcal{A}'$.

Recíprocamente, supóngase que $Lf \in \mathcal{A}'$. En particular se tilene que $Lf(1) = 0$ y por tanto $f(1) = 1$. Se definirá una función multiplicativa $g$ y se probará que coincide con $f$.

(1) Se define $g(1) = 1 = f(1)$.

(2) Para cada primo, se define

$$g(n) = \prod_{p|n} f(p^{\nu}),$$

donde $\nu := \max\{\alpha : p^{\alpha} \mid n\}$.

(3) $g$ es multiplicativa, pues $(m, n) = 1$ implica que

$$g(mn) = \prod_{p|mn} f(p^{\nu}) = \prod_{p|n} f(p^{\nu}) \prod_{p|n} f(p^{\nu}) = g(m)g(n).$$

(4) $g$ coincide con $f$ en todas las potencias de primos, pues si $q$ es un primo y $\alpha \in \mathbb{N}$,

$$g(q^{\alpha}) = \prod_{p|q^{\alpha}} f(p^{\nu}) = f(q^{\alpha}).$$

(5) $g^{-1}$ coincide con $f^{-1}$ en todas las potencias de primos, pues si $q$ es primo,

$$g^{-1}(q) = -\sum_{\substack{d|q \\ d \neq q}} g\left(\frac{q}{d}\right) g^{-1}(d) = -g(q)g^{-1}(1) = -g(q) = -f(q) = f^{-1}(q),$$

por el punto 4. Además, de forma recursiva se tiene que

$$
\begin{aligned}
g^{-1}(q^{\alpha}) &= -[g(q^{\alpha-1})g^{-1}(1) + \cdots + g(q)g^{-1}(q^{\alpha-1})] \\
&= -[f(q^{\alpha-1})f^{-1}(1) + \cdots + f(q)f^{-1}(q^{\alpha-1})] = f^{-1}(q^{\alpha}),
\end{aligned}
$$

donde $g^{-1}$ coincide con $f^{-1}$ en $1, q, q^2, \ldots, q^{\alpha-1}$.

(6) El punto anterior implica que $Lf(q^\alpha) = Lg(q^\alpha)$ para todo primo $q$ y para todo $\alpha \in \mathbb{N}$, pues

$$Lf(q^\alpha) = \sum_{d|p^\alpha} \log(d) f(d) f^{-1}\left(\frac{n}{d}\right) = \sum_{d|p^\alpha} \log(d) g(d) g^{-1}\left(\frac{n}{d}\right) = Lg(q^\alpha).$$

Además, como $g$ es multiplicativa, entonces $Lg(n) = 0$ para todo $n$ no potencia de algún primo, por la primera parte de esta demostración. Luego, por hipótesis se tiene que $Lf(n) = 0 = Lg(n)$ para todo $n$ no potencia de algún primo, así que de hecho $Lf(n) = Lg(n)$ para todo $n$, es decir, $Lf = Lg$ y como la aplicación $L$ es inyectiva, entonces $f = g$. Luego $f$ es multiplicativa, pues $g$ lo es.

■

**Lema 1.6.** $(\mathcal{M}, *) \cong (\mathcal{A}', +)$.

*Demostración.* Es fácil ver que $(\mathcal{A}', +)$ es un subgrupo de $(\mathcal{A}_{\mathbb{R}}, +)$ y que $(\mathcal{M}, *)$ es un subgrupo de $(P, *)$. Luego la restricción del homomorfismo a $L$ a $(\mathcal{M}, *)$ sigue siendo un isomorfismo y su imagen es $(\mathcal{A}', +)$ por la proposición anterior. ■

**Lema 1.7.** $(\mathcal{A}_{\mathbb{R}}, +) \cong (\mathcal{A}', +)$.

*Demostración.* Sea

$$\begin{aligned} \phi : (\mathcal{A}_{\mathbb{R}}, +) &\longrightarrow (\mathcal{A}', +) \\ f &\longmapsto F, \end{aligned}$$

donde $F$ es la función definida como $F(n) = f(p_n), \forall\, n \in \mathbb{N}$ y $p_n$ es el $n-$ésimo término en la sucesión de potencias de primos en orden ascendente.

Se tiene que $\phi$ es un homomorfismo, pues $\phi(f+g)(n) = (f+g)(p_n) = f(p_n)+g(p_n) = \phi(f)(n)+\phi(g)(n), \forall\, n \in \mathbb{N}$, luego $\phi(f+g) = F+G$. Se también tiene que $\phi$ es inyectivo, pues si $f, g \in (\mathcal{A}', +)$ son tales que $\phi(f) = \phi(g)$, entonces $f(p_n) = g(p_n), \forall\, n \in \mathbb{N}$, además $f(n) = g(n) = 0$ si $n$ no es potencia de algún primo, de manera que $f(n) = g(n), \forall\, n \in \mathbb{N}$, es decir, $f = g$.

Finalmente se tiene que $\phi$ es suprayectivo, pues si $F \in (\mathcal{A}', +)$, defínase $f(p_n) = F(n), \forall\, n \in \mathbb{N}$ y $f(n) = 0$ para toda $n$ no potencia de algún primo. Entonces $f \in (\mathcal{A}_{\mathbb{R}}, +)$ y $\phi(f)(n) = f(p_n) = F(n), \forall\, n \in \mathbb{N}$, es decir, $\phi(f) = F$. ■

**Lema 1.8.** $(\mathcal{A}_{\mathbb{R}}, +) \cong (\mathcal{A}_1, +)$, *donde* $\mathcal{A}_1 = \{f \in \mathcal{A} : f(1) \in \mathbb{R}\}$.

*Demostración.* Es claro que $(\mathcal{A}_1, +)$ es un grupo aditivo. Defínase

$$\begin{aligned} \psi : (\mathcal{A}_{\mathbb{R}}, +) &\longrightarrow (\mathcal{A}_1, +) \\ f &\longmapsto F \end{aligned}$$

donde $F$ es la función definida como $F(n) = f(2n-2) + if(2n-1), \forall\, n > 1$ y $F(1) = f(1)$. Se tiene que $\psi$ es un homomorfismo, pues $\psi(f+g)(1) = (f+g)(1) = f(1) + g(1) = \psi(f)(1) + \psi(g)(1)$, además,

$$\begin{aligned} \psi(f+g)(n) &= (f+g)(2n-2) + i(f+g)(2n-1) \\ &= f(2n-2) + g(2n-2) + if(2n-1) + ig(2n-1) \\ &= [f(2n-2) + if(2n-1)] + [g(2n-2) + ig(2n-1)] \\ &= \psi(f)(n) + \psi(g)(n), \end{aligned}$$

luego $\psi(f+g) = \psi(f) + \psi(g)$.

El homomorfismo $\psi$ es también inyectivo, pues si $f, g \in (\mathcal{A}_{\mathbb{R}}, +)$ son tales que $\psi(f) = \psi(g)$, entonces $f(n), g(n) \in \mathbb{R}, \forall\, n \in \mathbb{N}$ y además $f(2n-2) + if(2n-1) = g(2n-2) + ig(2n-1)$, por tanto $f(2n-2) = g(2n-2)$ y $f(2n-1) = g(2n-1)$ y $f(1) = g(1)$, así que $f(n) = g(n), \forall\, n \in \mathbb{N}$, es decir $f = g$.

Finalmente, $\psi$ también es suprayectivo, pues dada $F \in (\mathcal{A}_1, +)$, se puede escribir $F = F_1 + iF_2$, donde $F_1, F_2 \in \mathcal{A}_{\mathbb{R}}$. Defínase $g(1) = F(1)$ y

$$g(n) = \begin{cases} F_1\left(\dfrac{n}{2} + 1\right) & \text{si } n \text{ es par} \\ F_2\left(\dfrac{n+1}{2}\right) & \text{si } n \text{ es impar y } n > 1. \end{cases}$$

Entonces $g \in \mathcal{A}_{\mathbb{R}}$, $\psi(g)(1) = g(1) = F(1)$ y $\psi(g)(n) = g(2n-2) + ig(2n-1) = F_1(n) + iF_2(n) = F(n)$ para cada $n > 1$, es decir, $\psi(g) = F$. ∎

**Lema 1.9.** $(\mathcal{A}_{\mathbb{R}}, +) \cong (\mathcal{A}, +)$.

*Demostración.* Defínase

$$\begin{aligned} \gamma : (\mathcal{A}_{\mathbb{R}}, +) &\longrightarrow (\mathcal{A}, +) \\ f &\longmapsto F, \end{aligned}$$

donde $F$ es la función definida como $F(n) = f(2n-1) + if(2n), \forall\, n \in \mathbb{N}$. Se tiene que $\gamma$ es un homomorfismo, pues

$$\gamma(f+g)(n) = (f+g)(2n-1) + i(f+g)(2n)$$

$$\begin{aligned}
&= f(2n-1) + g(2n-1) + if(2n) + ig(2n) \\
&= [f(2n-1) + if(2n)] + [g(2n-1) + ig(2n)] \\
&= \gamma(f)(n) + \gamma(g)(n),
\end{aligned}$$

por tanto, $\gamma(f+g) = \gamma(f) + \gamma(g)$.

El homomorfismo $\gamma$ es también inyectivo, pues si $f, g \in \mathcal{A}_{\mathbb{R}}$ son tales que $\gamma(f) = \gamma(g)$, entonces $\gamma(f)(n) = \gamma(g)(n)$ para cada $n$, luego $f(2n-1)+if(2n) = g(2n-1)+ig(2n)$, por tanto $f(2n-1) = g(2n-1)$ y $f(2n) = g(2n)$ para cada $n$, en consecuencia $f(n) = g(n), \forall\, n \in \mathbb{N}$, es decir, $f = g$.

Finalmente, se tiene que $\gamma$ es suprayectivo, pues si $F \in \mathcal{A}$, se puede escribir $F = F_1 + iF_2$, con $F_1, F_2 \in \mathcal{A}_{\mathbb{R}}$. Defínase

$$f(n) = \begin{cases} F_1\left(\dfrac{n+1}{2}\right) & \text{si } n \text{ es impar} \\ F_2\left(\dfrac{n}{2}\right) & \text{si } n \text{ es par.} \end{cases}$$

Entonces, $\gamma(f)(n) = f(2n-1) + if(2n) = F_1(n) + iF_2(n) = F(n)$, para cada $n$, es decir, $f \in \mathcal{A}_{\mathbb{R}}$ es tal que $\gamma(f) = F$. ■

El resultado principal de esta sección es el siguiente, corolario de los lemas 1.5, 1.6, 1.7, 1.8 y 1.9.

**Teorema 1.6.** *Los grupos* $(\mathcal{A}_{\mathbb{R}}, +)$, $(P, *)$, $(\mathcal{M}, *)$, $(\mathcal{A}', +)$, $(\mathcal{A}_1, +)$ *y* $(\mathcal{A}, +)$ *son todos isomorfos.*

## 1.5. Algunas funciones aritméticas conocidas

A continuación se presentan algunas funciones aritméticas que aparecen frecuentemente en teoría de números.

**Definición 1.11**. (Función idéntica)**.** La función idéntica $N$ es tal que $N(n) = n$, para cada $n \in \mathbb{N}$.

**Definición 1.12**. (Función $\varphi$ de Euler)**.** Para cada $n \geq 1$, se define la función $\varphi$ de Euler $\varphi(n)$ como el número de enteros positivos no mayores a que $n$ que son primos relativos a $n$.

**Definición 1.13**. (Función de Mangoldt)**.** Para todo $n \in \mathbb{N}$, definimos la función de Mangoldt como

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^m \text{ para algún primo } p \text{ y } m \geq 1 \\ 0 & \text{en otro caso.} \end{cases}$$

**Definición 1.14**. (Función de Liouville)**.** Se define a la función $\lambda$ de Liouville como $\lambda(1) = 1$ y dada $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ la factorización de $n$ en primos, entonces $\lambda(n) = (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_k}$.

**Definición 1.15**. (Función divisor)**.** Para cada $k \in \mathbb{C}$ se define la función divisor de orden $k$ como

$$\sigma_k(n) = \sum_{d|n} d^k.$$

A la función divisor de orden 1 la llamaremos simplemente función divisor y se denotará como $\sigma$ en vez de $\sigma_1$. La función divisor de orden 0 se denomina función número de divisores y se denota $d$.

Las funciones aritméticas por sí mismas pueden tener comportamientos aleatorios y difíciles de predecir, pero se pueden observar algunas regularidades cuando sumamos todos los valores que toma la función en los divisores positivos de un número natural dado. Para esto definimos la siguiente notación:
Se tienen las siguientes propiedades básicas de algunas funciones aritméticas.

**Proposición 1.13.** *Para todo $n \in \mathbb{N}$, se tiene que*

$$\sum_{d|n} \mu(d) = I(n) = \begin{cases} 1 & si\ n = 1 \\ 0 & si\ n > 1 \end{cases}$$

*Demostración.* Si $n = 1$, por definición $\mu(n) = 1$. Supongamos que $n > 2$ y sea $n = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ la factorización de $n$ en primos. Todos los divisores de $n$ son de la forma $n = q_1^{\beta_1} \cdots q_k^{\beta_k}$, con $0 \leq \beta_i \leq \alpha_i$, $\forall\ i = 1, \ldots, k$. Sin embargo, hace falta considerar sólo los factores donde $0 \leq \beta_i \leq 1$, pues la función de Möbius se anula para cualesquiera otros. Para un $1 \leq i \leq k$ dado, existen $\binom{k}{i}$ $i$-combinaciones (sin repetición y desordenadas) de elementos del conjunto $P = \{q_1, \cdots, q_k\}$, véase [4]. Luego la suma buscada es igual a

$$\mu(1) + \sum_{p_1 \in \{q_1,\ldots,q_k\}} \mu(p_1) + \sum_{\substack{p_1,p_2 \in \{q_1,\ldots,q_k\} \\ p_1 \neq p_2}} \mu(p_1 p_2) + \cdots + \sum_{\substack{p_1,\ldots,p_k \in \{q_1,\ldots,q_k\} \\ p_1 \neq p_2 \neq \cdots \neq p_k}} \mu(p_1 \cdots p_k)$$

$$= \binom{k}{0}(-1)^0 + \binom{k}{1}(-1)^1 + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k = (1-1)^k = 0$$

Es decir, $\sum_{d|n} \mu(d) = 0$. ∎

**Corolario 1.5** (Inversión de Möbius)**.** *Si $f, g \in \mathcal{A}$, entonces para cada $n \in \mathbb{N}$,*

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

*Demostración.* De acuerdo con la proposición anterior, se tiene $\mu * \mathbf{1} = \mathbf{1} * \mu = I$, de tal manera que

$$f * \mathbf{1} = g \iff f * \mathbf{1} * \mu = g * \mu \iff f * I = g * \mu \iff f = g * \mu,$$

lo cual es equivalente al enunciado. ∎

**Proposición 1.14** (Gauss)**.** *Para todo $n \in \mathbb{N}$ se verifica que*

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

*Demostración.* La siguiente demostración es debida a Gauss en [8]. Sea $n \in \mathbb{N}$ y sean $d_1, \cdots, d_k$ los distintos divisores positivos de $n$. Para cada $d_i$, sean $c_{i,1}, \cdots, c_{i,m_i}$ todos los enteros positivos primos relativos y no mayores a $d_i$. Notemos que $\varphi(d_i) = m_i$. Afirmamos que el conjunto formado por los números

$$\begin{array}{cccc}
(n/d_1)c_{1,1} & (n/d_1)c_{1,2} & \cdots & (n/d_1)c_{1,m_1} \\
(n/d_2)c_{2,1} & (n/d_2)c_{2,2} & \cdots & (n/d_2)c_{2,m_2} \\
\vdots & \vdots & \ddots & \vdots \\
(n/d_k)c_{k,1} & (n/d_k)c_{k,2} & \cdots & (n/d_k)c_{k,m_k}
\end{array}$$

es igual a $\{1, 2, \ldots, n\}$. En efecto, sea $r$ un entero positivo tal que $1 \leq r \leq n$ y sea $d = (n, r)$. Notemos que $n/d$ es un divisor de $n$, $r/d \leq n/d$ y $(n/d, r/d) = 1$. Además $(n/(n/d))(r/d) = r$, luego $r$ está entre los elementos de la tabla anterior. Recíprocamente, se tiene que $1 \leq (n/d_i)c_{i,j} \leq (n/d_i)d_i = n$, $\forall\ i = 1, \ldots, k$, $\forall\ j = 1, \ldots, m_i$.

Finalmente veamos que todos los elementos de la tabla son distintos. Es claro que todos los elementos de cada fila son distintos, pues los divisores de cada $d_i$ son distintos por hipótesis. Si dos números fueran iguales, para algunos divisores $M$ y $N$ de $n$ distintos, podemos suponer que $M > N$. Se tendría pues que $(n/M)\mu = (n/N)\nu$, donde $\mu$ es primo relativo a $M$ y $\nu$ es primo relativo a $N$, luego $\mu N = \nu M$, de manera que $M \mid \mu N$, por tanto $M \mid N$, lo cual no puede ser pues $M > N$. Finalmente:

$$\sum_{d|n} \varphi(d) = \varphi(d_1) + \cdots + \varphi(d_k) = m_1 + \cdots + m_k = |\{1, \ldots, n\}| = n$$

■

Existe una relación entre las funciones $\mu$ y $\varphi$ al sumar sobre los divisores de un entero positivo. El siguiente lema será útil para probar dicha relación.

**Lema 1.10.** *Si $n \in \mathbb{N}$, $d$ es un divisor positivo de $n$, $S = \{x \in \mathbb{N} : 1 \leq x \leq n\}$ y $A = \{x \in S : d \mid x\}$ entonces $|A| = n/d$.*

*Demostración.* En efecto, tenemos que la función

$$\begin{aligned} F : \{1, \ldots, n/d\} &\longrightarrow A \\ x &\longmapsto dx \end{aligned}$$

es biyectiva, pues si $x, y \in \{1, \ldots, n/d\}$ son tales que $F(x) = F(y)$, entonces $dx = dy$ y por tanto $x = y$, pues $d \neq 0$. Además, si $r \in A$ entonces $d \mid r$ y $1 \leq r \leq n$, por lo que existe $q \in \mathbb{N}$ tal que $r = dq$, luego $q$ es tal que $1 \leq q \leq n/d$ y $F(q) = dq = r$. En consecuencia $|A| = |\{1, \ldots, n/d\}| = n/d$ ■

**Proposición 1.15.** *Para todo $n \in \mathbb{N}$ se verifica que*

$$\sum_{d|n} \mu(d)\frac{n}{d} = \varphi(n).$$

*Demostración.* Si $n = 1$ claro que se tiene $\mu(1) = \varphi(1) = 1$. Supongamos que $n > 1$ y sea $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ su factorización en primos. Sea $S = \{1, \ldots, n\}$ y para cada $i = 1, \ldots, r$ definamos $A_i = \{x \in S : p_i \mid x\}$.

Si $1 \leq m \leq r$, como todos los $p_i$ son primos distintos, se debe tener que

$$\bigcap_{s=1}^{m} A_i = \{x \in S \ : \ p_1 \mid x, p_2 \mid x, \ldots, p_m \mid x\} = \{x \in S \ : \ p_1 p_2 \ldots p_m \mid x\}\,.$$

Por otro lado, notemos que si $P = \{x \in S \ : \ (n, x) = 1\}$ entonces

$$\bigcap_{i=1}^{r} S \setminus A_i = P.$$

En efecto, si $x \in \bigcup_{i=1}^{r} A_i$ entonces $x \in S$ y $p_i \mid x$, para algún $p_i$, de manera que $p_i \mid n$ y $p_i \mid x$, y por tanto $(n, x) \geq p_i > 1$, luego $x \notin P$. Recíprocamente, si $x \in S$ y $x \notin P$, entonces $(n, x) > 1$ y por tanto debe existir un primo $q$ que divide a $(n, x)$, pero $(n, x) \mid n$ y $(n, x) \mid x$, por lo que $q \mid n$ y $q \mid x$, luego $q = p_i$, para algún $i = 1, \ldots, m$. En consecuencia, $p_i \mid x$ y por tanto $x \in \bigcup_{i=1}^{r} A_i$. Se sigue que $\bigcup_{i=1}^{r} A_i = S \setminus P$, o bien $\bigcap_{i=1}^{r} S/A_i = P$.

Como $p_1 \cdots p_m \mid n$, $\forall\ m = 1, \ldots, r$, por el lema (1.10) se debe tener que $|\bigcap_{s=1}^{m} A_i| = n/p_1 \cdots p_m$, $\forall\ m = 1, \ldots, r$. Finalmente, por el principio de inclusión-exclusión, se tiene que

$$\varphi(n) = |P| = \left|\bigcap_{i=1}^{r} S \setminus A_i\right| = |S| + \sum_{i_1 \in \{1,\ldots,r\}} (-1)|A_{i_1}| + \sum_{\substack{i_1, i_2 \in \{1,\ldots,r\} \\ i_1 \neq j_2}} |A_{i_1} \cap A_{i_2}| + \cdots$$

$$+ \sum_{\substack{i_1, \ldots, i_r \in \{1,\ldots,r\} \\ i_1 \neq \cdots \neq i_r}} (-1)^r |A_{i_1} \cap \cdots \cap A_{i_r}| = n + \sum_{i_1 \in \{1,\ldots,r\}} (-1)\frac{n}{p_{i_1}} + \sum_{\substack{i_1, i_2 \in \{1,\ldots,r\} \\ i_1 \neq j_2}} \frac{n}{p_{i_1} p_{i_2}} + \cdots$$

$$+ \sum_{\substack{i_1, \ldots, i_r \in \{1,\ldots,m\} \\ i_1 \neq \cdots \neq i_r}} (-1)^r \frac{n}{p_{i_1} \cdots p_{i_r}} = n + \sum_{i_1 \in \{1,\ldots,r\}} \mu(p_{i_1})\frac{n}{p_{i_1}} + \sum_{\substack{i_1, i_2 \in \{1,\ldots,r\} \\ i_1 \neq j_2}} \mu(p_{i_1} p_{i_2})\frac{n}{p_{i_1} p_{i_2}} +$$

$$\cdots + \sum_{\substack{i_1, \ldots, i_r \in \{1,\ldots,m\} \\ i_1 \neq \cdots \neq i_r}} \mu(p_{i_1} \cdots p_{i_r})\frac{n}{p_{i_1} \cdots p_{i_r}} = \sum_{d \mid n} \mu(d)\frac{n}{d}.$$

■

**Corolario 1.6.** *La función $\varphi$ es multiplicativa, pues $\varphi = \mu * N$, donde $\mu$ y $N$ son funciones multiplicativas.*

# 2. Funciones pares

Al estudiar el espacio de funciones aritméticas se puede hacer una analogía con la teoría de Fourier del análisis para funciones definidas en todo el plano real o complejo, para la cuál se necesitará la noción de periodicidad. En este capítulo se considerará una clase de funciones aritméticas que captura esta noción. También se expondran resultados análogos a los de análisis respecto a funciones periódicas. Estos resultados se puede encontrar en [6].

*Observación 2.1.* Durante todo el capítulo se supondrá que $r$ es un entero positivo arbitrario pero fijo.

**Definición 2.1**. (Función par)**.** Una función aritmética se dice **par** mód $r$ si $f(n) = f((n,r))$, donde $(m,r)$ es el máximo común divisor de $n$ y $r$, para cada $n \in \mathbb{N}$.

**Definición 2.2**. (Función periódica)**.** Una función aritmética se dice **periódica** con periodo $r$ (o periódica mód $r$) si $m, n \in \mathbb{N}$ y $m \equiv n \pmod{r}$ implica que $f(m) = f(n)$.

La siguiente proposición es una consecuencia inmediata de las definiciones anteriores.

**Proposición 2.1.** *Toda función par* mód $r$ *es periódica con periodo* $r$.

*Demostración.* Si $m \equiv n \pmod{r}$ entonces $r \mid m - n$, por tanto existe $q \in \mathbb{Z}$ tal que $m - n = qr$. Por demostrar que $(n,r) = (m,r)$. En efecto, como $(n,r) \mid n$ y $(n,r) \mid r$, entonces $(n,r) \mid n + qr = m$, luego $(n,r) \mid (m,r)$. Análogamente, se tiene que $(m,r) \mid (n,r)$. Se sigue que $(n,r) = (m,r)$ y por tanto $f(n) = f((n,r)) = f((m,r)) = f(m)$. ∎

## 2.1. Sumas de Ramanujan

En 1918, Ramanujan publicó el artículo [16], que contiene varias fórmulas notables expresando algunas funciones sobre $\mathbb{N}$ como el límite puntual de ciertas series trigonométricas. Por ejemplo, probó que

$$\frac{\sigma(n)}{n} = \frac{\pi^2}{6}\left(1 + \frac{(-1)^n}{2^2} + \frac{2\cos\left(\frac{2}{3}\pi n\right)}{3^2} + \frac{2\cos\left(\frac{1}{2}\pi n\right)}{4^2} + \frac{2\left[\cos\left(\frac{2}{5}\pi n\right) + \cos\left(\frac{4}{5}\pi n\right)\right]}{5^2} + \frac{2\cos\left(\frac{1}{3}\pi n\right)}{6^2} + \cdots\right),$$

o escrito de otra manera,

$$\frac{\sigma(n)}{n} = \frac{\pi^2}{6} \sum_{r=1}^{\infty} \frac{c_r(n)}{r^2},$$

donde

$$c_r(n) = \sum_{\substack{a=1 \\ (a,r)=1}}^{r} \cos\left(\frac{2\pi}{r} an\right).$$

Estas sumas son conocidas como sumas de Ramanujan. El valor $c_r(n)$ es de hecho la suma de las $n$-ésimas potencias de las raíces primitivas de la unidad.

**Proposición 2.2.** *Para toda $n \in \mathbb{N}$ se tiene que*

$$c_r(n) = \sum_{\substack{a=1 \\ (a,r)=1}}^{r} e^{i(2\pi/r)an},$$

*donde $i$ es la unidad imaginaria.*

*Demostración.* En efecto,

$$\sum_{\substack{a=1 \\ (a,r)=1}}^{r} e^{i(2\pi/r)an} = \sum_{\substack{a=1 \\ (a,r)=1}}^{r} \cos\left(\frac{2\pi}{r} an\right) + i \sum_{\substack{a=1 \\ (a,r)=1}}^{r} \sin\left(\frac{2\pi}{r} an\right).$$

Pero $(a, r) = 1$ si y sólo si $(a - r, r) = 1$. Además, si $1 \leq a \leq r - 1$ entonces $1 \leq r - a \leq r - 1$, por tanto

$$\begin{aligned}\sum_{\substack{a=1 \\ (a,r)=1}}^{r} \sin\left(\frac{2\pi}{r} an\right) = \sum_{\substack{a=1 \\ (r-a,r)=1}}^{r} \sin\left(\frac{2\pi}{r}(r-a)n\right) &= \sum_{\substack{a=1 \\ (r-a)=1}}^{r} -\sin\left(\frac{2\pi}{r} an\right) \\ &= -\sum_{\substack{a=1 \\ (a,r)=1}}^{r} \sin\left(\frac{2\pi}{r} an\right).\end{aligned}$$

Se sigue que la parte imaginaria de la primera suma se anula y se tiene la igualdad deseada. ∎

En el siguiente capítulo se verá que esta expresión aparece de forma natural al calcular los coeficientes de Fourier clásicos de cierta función aritmética.

**Proposición 2.3.** *Para toda $n \in \mathbb{N}$ se tiene que*

$$c_r(n) = \sum_{d|(n,r)} \mu\left(\frac{r}{d}\right) d.$$

*Demostración.* Por la proposición ?? se tiene que la suma $\sum_{d|k} \mu(d)$ es igual a 1 si $k = 1$ e igual a 0 en otro caso, luego por la proposición anterior,

$$c_r(n) = \sum_{\substack{a=1 \\ (a,r)=1}}^{r} e^{i(2\pi/r)an} = \sum_{a=1}^{r} e^{i(2\pi/r)an} \left( \sum_{d|(a,r)} \mu(d) \right) = \sum_{\substack{d|a \\ d|r}} \sum_{a=1}^{r} \mu(d) e^{i(2\pi/r)an}$$

$$= \sum_{d|r} \mu(d) \sum_{\substack{d|a \\ 1\leq a\leq r}} e^{i(2\pi/r)an} = \sum_{d|r} \mu(d) \sum_{b=1}^{r/d} e^{i(2\pi/(r/d))bn}$$

El valor de la suma interior depende de si $r/d$ divide a $n$ o no. Si lo hace, cada uno de sus términos es igual a 1 y por tanto la suma vale $r/d$. Si este no es el caso se puede sumar,

$$\sum_{b=1}^{r/d} e^{i(2\pi/(r/d))bn} = \frac{e^{i(2\pi/r)/(r/d)}(e^{i(2\pi n)} - 1)}{e^{i(2\pi/r)/(r/d)} - 1} = 0,$$

pues el denominador no se anula. Luego

$$c_r(n) = \sum_{\substack{a=1 \\ (a,r)=1}}^{r} e^{i(2\pi/r)an} = \sum_{d|r} \mu(d) \begin{cases} r/d & \text{si } r/d \mid n \\ 0 & \text{en otro caso} \end{cases} = \sum_{\substack{d|q \\ (r/d)|n}} \mu(d)(r/d)$$

$$= \sum_{\substack{d|r \\ d|n}} \mu\left(\frac{r}{d}\right) d = \sum_{d|(n,r)} \mu\left(\frac{r}{d}\right) d.$$

■

En lo que sigue de este capítulo se trabajará exclusivamente con ésta última representación de $c_r$ y se le referirá como *suma de Ramanujan módulo r* o simplemete *suma de Ramanujan* cuando no haya riesgo de confusión.

**Proposición 2.4.** *Algunas propiedades de la sumas de Ramanujan son las siguientes:*

(1) $c_1 = \mathbf{1}$

(2) $c_r(1) = \mu(r)$

(3) $c_r(n) \leq \max\{\sigma(r), \sigma(n)\}$

(4) $c_r(n)$ *es una función multiplicativa de* $r$

(5) *Si $p$ es primo y $m$ es un entero positivo, entonces*

$$c_{p^m}(n) = \begin{cases} p^m - p^{m-1} & si\ p^m \mid n \\ -p^{m-1} & si\ p^{m-1}\ pero\ p^m \nmid n \\ 0 & si\ p^{m-1} \nmid n. \end{cases}$$

*Demostración.* (1) Para cada $n \in \mathbb{N}$ se tiene que $(n, 1) = 1$ y por tanto

$$c_1(n) = \sum_{d|(n,1)} \mu\left(\frac{1}{d}\right) d = \mu(1)1 = 1.$$

(2) De manera similar,

$$c_r(1) = \sum_{d|(1,r)} \mu\left(\frac{r}{d}\right) d = \mu(r)1 = \mu(r).$$

(3) Por definición se tiene que $\sigma(k) = \sum_{d|k} d$. Además $\mu(k) \leq 1$ para todo $k \in \mathbb{N}$, luego

$$c_r(n) = \sum_{d|(n,r)} \mu\left(\frac{r}{d}\right) d \leq \sum_{d|(n,r)} d = \sum_{\substack{d|n \\ d|r}} d \leq \sum_{d|n} d, \sum_{d|r} d \leq \text{máx}\{\sigma(n), \sigma(r)\}.$$

(4) Defínase

$$\eta_r(n) = \begin{cases} r & \text{si } r \mid n \\ 0 & \text{en otro caso.} \end{cases}$$

Se tiene que la función $\eta_\square(n)$ es multiplicativa para $n$ fijo. En efecto, si $r, s \in \mathbb{N}$ son tales que $(r, s) = 1$, entonces

$$\eta_{rs}(n) = \begin{cases} rs & \text{si } rs \mid n \\ 0 & \text{en otro caso,} \end{cases}$$

pero $rs \mid n$ si y sólo si $r \mid n$ y $s \mid n$. En efecto, si $rs \mid n$ es claro que $r \mid n$ y $s \mid n$. Supóngase que $r \mid n$ y $s \mid n$, de tal manera que existen $q_1, q_2 \in \mathbb{Z}$ tales que $n = rq_1 = sq_2$. Como $(r, s) = 1$, también existen $x, y \in \mathbb{Z}$ tales que $1 = rx + sy$, luego $n = nrx + nsy$, por lo que $n = rs(q_2x + q_1y)$, es decir, $rs \mid n$. Luego, si $rs \mid n$, entonces

$$\eta_{rs}(n) = rs = \eta_r(n)\eta_s(n),$$

y si $rs \nmid$ entonces $r \nmid n$ y $s \nmid n$, por lo que

$$\eta_{rs}(0) = 0 = \eta_r(n)\eta_s(n).$$

Por otro lado, se tiene que

$$\sum_{d|r} \mu\left(\frac{r}{d}\right)\eta_d(n) = \sum_{\substack{d|r \\ d|n}} \mu\left(\frac{r}{d}\right) d = \sum_{d|(n,r)} \mu\left(\frac{r}{d}\right) d = c_r(n),$$

es decir, $c_\square(n) = \mu * \eta_\square(n)$. Luego $c_\square(n)$ debe ser multiplicativa para $n$ fijo, por ser producto de funciones multiplicativas.

(5) Tenemos los siguientes casos:

- Si $p^m \mid n$, entonces $(n, p^m) = p^m$, luego

$$c_{p^m}(n) = \sum_{d|p^m} \mu\left(\frac{p^m}{d}\right) d = \mu(1)p^m + \mu(p)p^{m-1} = p^m - p^{m-1},$$

pues $\mu(p^i) = 0$ para toda $i > 1$.

- Si $p^{m-1} \mid n$ pero $p^m \nmid n$, entonces $(n, p^m) = p^{m-1}$. En efecto, se tiene que $p^{m-1} \mid p^m$ y además $p^{m-1} \mid n$ por hipótesis. Si $e \in \mathbb{Z}$ es tal que $e \mid p^m$ y $e \mid n$, entonces $e = p^i$, para algún $0 \leq i \leq m-1$, pues $p^m \nmid n$, por tanto $e \mid p^{m-1}$. Esto prueba que $(p^m, n) = p^{m-1}$, así

$$c_{p^m}(n) = \sum_{d|p^{m-1}} \mu\left(\frac{p^m}{d}\right) d = \mu(p)p^{m-1} = -p^{m-1}$$

- Finalmente, si $p^{m-1} \nmid n$, entonces $p^m \nmid n$. Además, $(n, p^m) \mid p^m$, por tanto $(n, p^m) = p^i$ para algún $0 \leq i \leq m$. Más aún, por la hipótesis se debe tener que $0 \leq i \leq m-2$. Luego

$$c_{p^m}(n) = \sum_{d|p^i} \mu\left(\frac{p^m}{d}\right) d = \mu(p^m)1 + \mu(p^{m-1})p + \cdots + \mu(p^{m-i})p^i = 0,$$

pues $i \leq m-2$ implica que $2 \leq m-i$ y por tanto $\mu(p^m) = \ldots = \mu(p^{m-i}) = 0$.

■

Del la demostración del punto 4 se puede rescatar el siguiente corolario, usando la inversión de Möbius (Corolario 1.5).

**Corolario 2.1.** *Para cada $n \in \mathbb{N}$ fijo se tiene*

$$\sum_{d|r} c_d(n) = \eta_r(n) = \begin{cases} r & \text{si } r \mid n \\ 0 & \text{en otro caso.} \end{cases}$$

Otro corolario notable de la proposición anterior es el siguiente.

**Corolario 2.2.** *La suma de las raíces $r$-ésimas primitivas de la unidad es igual a $\mu(r)$.*

*Demostración.* Por el punto (2) de la proposición anterior, se tiene que

$$\sum_{\substack{a=1 \\ (a,r)=1}}^{r} e^{i(2\pi/r)a} = c_r(1) = \mu(r).$$

■

Las sumas de Ramanujan gozan de la siguiente propiedad de "ortogonalidad".

**Lema 2.1.** *Si $r$ y $s$ dividen a $k$, entonces*

$$\sum_{d|k} c_r(k/d)c_d(k/s) = \begin{cases} k & \text{si } r = s \\ 0 & \text{en otro caso.} \end{cases}$$

*Demostración.* Si $r$ y $s$ dividen a $k$, entonces

$$\begin{aligned} \sum_{d|k} c_r(k/d)c_d(k/s) &= \sum_{d|k} c_d(k/s) \sum_{d'|(k/d,r)} \mu(r/d')d' \\ &= \sum_{d|k} c_d(k/s) \sum_{\substack{d'|r \\ d'|k/d}} \mu(r/d')d' = \sum_{\substack{d|k \\ d'|r \\ d'|k/d}} c_d(k/s)\mu(r/d')d' \\ &= \sum_{\substack{d|k/d' \\ d'|r \\ d'|r}} c_d(k/s)\mu(r/d')d' = \sum_{\substack{d'|r \\ d'|k}} \mu(r/d')d' \sum_{d|k/d'} c_d(k/s) \\ &= \sum_{d'|(k,r)} \mu(r/d)d'\eta_{k/d'}(k/s) = \sum_{d'|r} \mu(r/d)d'\eta_{k/d'}(k/s), \end{aligned} \tag{2.1}$$

dado que $(k, r) = r$ por ser $r$ divisor de $k$ y dado que los conjuntos $\{d, d' \in \mathbb{N} : d \mid k, d' \mid r, d' \mid k/d\}$ y $\{d, d' \in \mathbb{N} : d \mid k/d', d' \mid r, d' \mid k\}$ son iguales. En efecto, si $d \mid k$ entonces $k/d$ es un entero, lueg $d' \mid k/d$ implica que $k/d = d'q'$, luego $k = d'q'd$, por tanto $d \mid k/d'$ y $d' \mid k$.

Recíprocamente, si $d' \mid k$ entonces $k/d'$ es un entero, luego $d \mid k/d'$ implica que $k/d' = dq$, por tanto $k = dqd'$, por tanto $d \mid k$ y $d' \mid k/d$.

Si $s \nmid r$ entonces $s \nmid d'$ y por tanto $k/d' \nmid k/s$. En efecto, pues si $s \mid d'$, como $d' \mid r$ entonces se tendría que $s \mid r$ por transitividad. Además, si $k/d' \mid k/s$ se tendría que $s \mid d'k$. Luego la suma (2.1) se anula si $s \nmid r$ y en particular si $r \neq s$, pues en este caso se tiene que $\eta_{k/d'}(k/s) = 0$ para cada $d' \mid r$.

Si $s \mid r$ entonces la suma (2.1) es igual a

$$\begin{aligned}\sum_{\substack{d'\mid r\\ k/d'\mid k/s}} \mu(r/d')d'\frac{k}{d'} &= \sum_{\substack{d'\mid r\\ k/d'\mid k/s}} \mu(r/d')k = \sum_{\substack{d'\mid r\\ s\mid d'}} \mu(r/d')k \\ &= k\sum_{\substack{d'\mid r\\ d'=se}} \mu(r/se) = k\sum_{e\mid r/s} \mu(r/se) \\ &= k\sum_{se\mid r} \mu(r/se) = \begin{cases} k & \text{si } r = s \\ 0 & \text{en otro caso,}\end{cases}\end{aligned}$$

pues $k/d' \mid k/s$ si y sólo si $s \mid d'$. ∎

**Corolario 2.3.** *Las sumas de Ramanujan son linealmente independientes respecto a la suma sobre los divisores de $r$. Más específicamente, si $\alpha, \beta$ son funciones aritméticas tales que*

$$\sum_{d\mid r} \alpha(d)c_d(n) = \sum_{d\mid r} \beta(d)c_d(n),$$

*para todo $n \in \mathbb{N}$, entonces $\alpha(d) = \beta(d)$ para todo $d \mid r$.*

*Demostración.* Basta probar que $\sum_{d\mid r} \alpha(d)c_d(n) = 0$ implica que $\alpha(d) = 0$ para todo $d \mid r$. Supóngase la hipótesis y sea $\delta \mid r$ arbitrario pero fijo. Si $e$ es un divisor de $r$, se tiene que $\sum_{d\mid r} \alpha(d)c_d(r/e) = 0$, luego

$$0 = \sum_{e\mid r}\left(\sum_{d\mid r} \alpha(d)c_d\left(\frac{r}{e}\right)\right)c_e\left(\frac{r}{\delta}\right) = \sum_{d\mid r} \alpha(d)\sum_{e\mid r} c_d\left(\frac{r}{e}\right)c_e\left(\frac{r}{\delta}\right) = \alpha(\delta)r,$$

por el la proposición anterior, y dado que $r \neq 0$ entonces $\alpha(\delta) = 0$. Como $\delta$ fue un divisor arbitrario de $r$, se tiene el resultado. ∎

**Lema 2.2.** *Si $d \mid r$ entonces $c_d(n) = c_d((n, r))$.*

*Demostración.* Si $d \mid r$ entonces $(n,d) = ((n,r),d)$. En efecto, dado que $(n,d) \mid n$ y $(n,d) \mid d$, entonces $(n,d) \mid n$, $(n,d) \mid d$ y $(n,d) \mid r$, por lo que $(n,d) \mid (n,r)$ y $(n,d) \mid d$, es decir, $(n,d) \mid ((n,r),d)$. Recíprocamente se tiene que $((n,r),d) \mid n$ y $((n,r),d) \mid d$, así que $((n,r),d) \mid (n,d)$. Se sigue que $(n,d) = ((n,r),d)$. Luego

$$c_d(n) = \sum_{e \mid (n,d)} \mu(d/e)e = \sum_{e \mid ((n,r),d)} \mu(d/e)e = c_d((n,r)).$$

■

**Corolario 2.4.** *La suma de Ramanujan módulo $r$ es par* mód $r$.

**Definición 2.3**. (Radical)**.** Sea $n \in \mathbb{N}$. Se define el *radical* de $n$, denotado por $n_*$ como

$$n_* = \begin{cases} 1 & \text{si } n = 1 \\ p_1 \cdots p_r & \text{si } n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \end{cases}$$

donde $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ es la factorización de $n > 1$ en primos.

**Definición 2.4.** Una función aritmética $f$ se dirá *separable* si $f(n) = f(n_*)$, para cada $n \in \mathbb{N}$.

**Lema 2.3.** *Una función multiplicativa es separable si y sólo si $(\mu * f)(n) = 0$ para todo $n$ no libre de cuadrado.*

*Demostración.* Sea $F = \mu * f$. Entonces $F * \mathbf{1} = f$, es decir,

$$\sum_{d \mid n} F(d) = f(n), \forall\, n \in \mathbb{N}.$$

Si $F(n) = 0$ para cada $n$ no libre de cuadrado, entonces

$$f(n) = \sum_{d \mid n} F(d) = \sum_{d \mid n_*} F(d) = f(n_*),$$

es decir, $f$ es separable.

Supóngase ahora que $f$ es separable. Se tiene que para cada primo $p$ y para cada $m > 1$,

$$\begin{aligned} F(p^m) = \sum_{d \mid p^m} \mu(d) f\left(\frac{p^m}{d}\right) &= \mu(1)f(p^m) + \mu(p)f(p^{m-1}) \\ &= f(p^m) - f(p^{m-1}) = f(p) - f(p) = 0. \end{aligned}$$

Además como $f$ es multiplicativa, entonces $F$ también lo es. Si $n$ es un entero positivo no libre de cuadrado, entonces existen un primo $p$ y enteros positivos $q$ y $m > 1$ tales que $n = p^m q$ y $(p^m, q) = 1$. Luego $F(n) = F(p^m)F(q) = 0 \cdot F(q) = 0$. ■

**Lema 2.4.** *Si $f$ es multiplicativa y separable, entonces para cualesquiera $a, b \in \mathbb{N}$ se tiene:*

(i) $f(a)f(b) = f(ab)f((a,b))$.

(ii) $f(a) = f((a,b)) \sum_{\substack{d|a \\ (d,b)=1}} (\mu * f)(d)$

*Demostración.* (i) Nótese que si $p$ es un primo y $m, n > 1$ entonces

$$f(p^m)f(p^n) = f(p)f(p) = f(p^{m+n})f((p^m, p^n)),$$

pues $(p^m, p^n) = p^i$, con $i = \min\{m, n\}$. Sean $a, b \in \mathbb{N}$ y escríbase sin pérdida de generalidad $a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ y $b = p_1^{\beta_1} \cdots p_r^{\beta_r}$, $0 \leq \alpha_i, \beta_i$. Entonces, como $f$ es multiplicativa,

$$\begin{aligned}
f(ab)f((a,b)) &= f(p_1^{\alpha_1+\beta_1} \cdots p_r^{\alpha_r+\beta_r}) f(p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_r^{\min\{\alpha_r,\beta_r\}}) \\
&= f(p_1^{\alpha_1+\beta_1}) \cdots f(p_r^{\alpha_r+\beta_r}) f(p_1^{\min\{\alpha_1,\beta_1\}}) \cdots f(p_r^{\min\{\alpha_r,\beta_r\}}) \\
&= f(p_1^{\alpha_1+\beta_1}) \cdots f(p_r^{\alpha_r+\beta_r}) f((p_1^{\alpha_1}, p_1^{\beta_1})) \cdots f((p_r^{\alpha_r}, p_r^{\beta_r})) \\
&= f(p_1^{\alpha_1}) f(p_1^{\beta_1}) \cdots f(p_r^{\alpha_r}) f(p_r^{\beta_r}) \\
&= f(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) f(p_1^{\beta_1} \cdots p_r^{\beta_r}) \\
&= f(a)f(b)
\end{aligned}$$

(ii) Al igual que en la demostración anterior, si $F = \mu * f$, entonces

$$\sum_{d|n} F(d) = f(n), \forall\, n \in \mathbb{N}.$$

Se verá primero que los conjuntos $\{d \in \mathbb{N} : d \mid a_* \text{ y } (d,b) = 1\}$ y $\{d \in \mathbb{N} : d \mid a_*/(a,b)_*\}$ son iguales.

Para empezar, se tiene que $a_*/(a,b)_*$ es un entero. Si $(a,b)_* = 1$ esto es claro. Si $(a,b)_* > 1$ se puede escribir $(a,b)_* = q_1 \cdots q_s$, donde todos los primos son distintos. Luego $q_i \mid (a,b)_*$, pero $(a,b)_* \mid (a,b)$ y $(a,b) \mid a$, por tanto $q_i \mid a$ y por tanto $q_i \mid a_*$. Como $i \in \{1, \ldots, s\}$ fue arbitrario y todos los primos $q_i$ son distintos, entonces $q_1 \cdots q_s = (a,b)_* \mid a_*$, que es lo que se quería probar.

Procedamos a probar la igualdad de los conjuntos. Supóngase primero que $d \mid a_*$ y $(d,b) = 1$. Entonces existe $c \in \mathbb{N}$ tal que $a_* = dc$. Por otro lado, se tiene que $(a,b) \mid b$ y por tanto $((a,b),d) = 1$, más aún, como $(a,b)_* \mid (a,b)$ entonces también

$((a,b)_*, d) = 1$ y como $(a,b)_* \mid a_* = dc$, por el lema de Euclides se debe tener que $(a,b)_* \mid c$ es decir, $a_* = (a,b)_* dq$, para algún $q \in \mathbb{N}$, luego $d \mid a_*/(a,b)_*$.

Recíprocamente, supóngase que $d \mid a_*/(a,b)_*$. Se debe tener que

$$\left(\frac{a_*}{(a,b)_*}, b\right) = 1. \tag{2.2}$$

Pues en caso contrario, es decir, si este máximo común divisor fuera mayor que uno, existiría un primo $p$ tal que $p \mid b$ y $p \mid a_*/(a,b)_*$, pero $a_*/(a,b)_* \mid a_*$, luego $p \mid a_*$ y por tanto $p \mid a$. En consecuencia, $p \mid (a,b)$ y por tanto $p \mid (a,b)_*$. Se puede escribir entonces $a_* = pp_1 \cdots p_r$, $(a,b)_* = pq_1 \cdots q_s$, donde todos los primos son distintos. Además, como $a_* = (a,b)_* n$ para algún $n \in \mathbb{N}$, se tiene que $pp_1 \cdots p_r = pq_1 \cdots q_s r_1 \cdots r_t$, con $n = r_1 \cdots r_t$, y $r_i$ números primos, no necesariamente distintos. Luego $p_1 \cdots p_r = q_1 \cdots q_s r_1 \cdots r_t$ y dado que ningúno de los primos $p_i$ son iguales a $p$, entonces ninguno de los primos $r_j$ puede ser igual a $p$, es decir $p$ no divide a $n = a_*/(a,b)_*$, lo cual es absurdo.

Esto prueba la igualdad de dichos conjuntos. Ahora es fácil calcular la siguiente suma,

$$\sum_{\substack{d \mid a \\ (d,b)=1}} F(d) = \sum_{\substack{d \mid a_* \\ (d,b)=1}} F(d) = \sum_{d \mid a_*/(a,b)_*} F(d) = \sum_{d \mid (a_*/(a,b)_*)} (\mu * f)(d) = f(a_*/(a,b)_*).$$

Además, por una demostración similar a la de la ecuación (2.2), se tiene que

$$\left((a,b)_*, \frac{a_*}{(a,b)_*}\right) = 1.$$

Finalmente, como $f$ es multiplicativa,

$$f(a) = f(a_*) = f((a,b)_*) f(a_*/(a,b)_*) = f((a,b)) \sum_{\substack{d \mid a \\ (d,b)=1}} (\mu * f)(d).$$

■

*Ejemplo 2.1.* La función $\overline{\varphi} = \varphi(n)/n$ es separable. Nótese que para cualquier primo $p$ y $m > 0$ se tiene $\varphi(p^m) = p^m - p^{m-1}$, luego $\varphi(p^m)/p^m = 1 - p^{-1}$ y también $\varphi(p)/p = 1 - p^{-1}$. Ahora, si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ entonces, como $\varphi$ es multiplicativa,

$$\frac{\varphi(n)}{n} = \frac{\varphi(p_1^{\alpha_1})}{p_1^{\alpha_1}} \cdots \frac{\varphi(p_r^{\alpha_r})}{p_r^{\alpha^r}} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) = \frac{\varphi(p_1)}{p_1} \cdots \frac{\varphi(p_r)}{p_r} = \frac{\varphi(n_*)}{n_*}$$

**Lema 2.5** (Fórmula de Hölder). *Para cada $n \in \mathbb{N}$ se tiene*

$$c_r(n) = \frac{\varphi(r)\mu\left(\dfrac{r}{(n,r)}\right)}{\varphi\left(\dfrac{r}{(n,r)}\right)}$$

*Demostración.* Se tiene

$$c_r(n) = \sum_{d|(n,r)} \mu\left(\frac{r}{d}\right) d = \sum_{\substack{d|(n,r) \\ \left(\frac{r}{(n,r)}, \frac{(n,r)}{d}\right)>1}} \mu\left(\frac{r}{d}\right) d + \sum_{\substack{d|(n,r) \\ \left(\frac{r}{(n,r)}, \frac{(n,r)}{d}\right)=1}} \mu\left(\frac{r}{d}\right) d, \tag{2.3}$$

pero si $(r/(n,r), (n,r)/d) > 1$ entonces $r/d$ debe tener un factor cuadrado, pues en este caso existe un primo $p$ tal que $p \mid r/(n,r)$ y $p \mid (n,r)/d$, luego $r = p(n,r)q_1$ y $(n,r) = pdq_2$ para algunos enteros $q_1$ y $q_2$, luego $r = p^2 dq_1q_2$ y por tanto $p^2 \mid r/d$, así que $\mu(r/d) = 0$. Luego la ecuación (2.3) es igual a

$$\begin{aligned}
\sum_{\substack{d|(n,r) \\ \left(\frac{r}{(n,r)}, \frac{(n,r)}{d}\right)=1}} \mu\left(\frac{r}{d}\right) d &= \sum_{\substack{d|(n,r) \\ \left(\frac{r}{(n,r)}, \frac{(n,r)}{d}\right)=1}} \mu\left(\frac{r}{(n,r)}\right)\mu\left(\frac{(n,r)}{d}\right) d \\
&= \mu\left(\frac{r}{(n,r)}\right) \sum_{\substack{d|(n,r) \\ \left(\frac{r}{(n,r)}, \frac{(n,r)}{d}\right)=1}} \mu\left(\frac{(n,r)}{d}\right) d \\
&= \mu\left(\frac{r}{(n,r)}\right) \sum_{\substack{d|(n,r) \\ \left(\frac{r}{(n,r)}, d\right)=1}} \mu(d)\frac{(n,r)}{d} \\
&= (n,r)\mu\left(\frac{r}{(n,r)}\right) \sum_{\substack{d|(n,r) \\ \left(\frac{r}{(n,r),d}\right)=1}} \frac{\mu(d)}{d}
\end{aligned} \tag{2.4}$$

pues $\mu$ es multiplicativa. Sea ahora $\Phi = \mu * \overline{\varphi}$, donde $\overline{\varphi}(s) = \varphi(s)/s$ para cada $s \in \mathbb{N}$. Se tiene entonces que

$$\begin{aligned}
\Phi(s) = \sum_{d|s} \mu(d)\overline{\varphi}\left(\frac{s}{d}\right) &= \sum_{d|s} \mu(d)\varphi\left(\frac{s}{d}\right)\frac{1}{s/d} = \sum_{d|s} \mu(d) \sum_{e|s/d} \mu(e)\frac{s/d}{e}\frac{1}{s/d} \\
&= \sum_{d|s} \mu(d) \sum_{e|s/d} \frac{\mu(e)}{e} = \sum_{e|s} \frac{\mu(e)}{e} \sum_{d|s/e} \mu(d) = \frac{\mu(s)}{s}
\end{aligned} \tag{2.5}$$

pues si $d \mid s$ y $c \mid s/d$, entonces $d/s$ es un entero y $s/d = eq$ para algún entero $q$, luego $s = deq$ y por tanto $e \mid s$ y $d \mid s/e$. El recíproco es similar. Además, todos los términos en la penúltima suma son cero excepto aquel para el cual $s/e = 1$, es decir, $s = e$. Luego la suma (2.4) es igual a

$$\begin{aligned}
(n,r)\mu\left(\frac{r}{(n,r)}\right) \sum_{\substack{d\mid(n,r)\\ \left(\frac{r}{(n,r)},d\right)=1}} \Phi(d) &= (n,r)\mu\left(\frac{r}{(n,r)}\right) \sum_{\substack{d\mid(n,r)\\ \left(\frac{r}{(n,r)},d\right)=1}} (\mu * \overline{\varphi}(d)) \\
&= (n,r)\mu\left(\frac{r}{(n,r)}\right) \frac{\overline{\varphi}((n,r))}{\overline{\varphi}\left((n,r),\frac{r}{(n,r)}\right)} \\
&= (n,r)\mu\left(\frac{r}{(n,r)}\right) \frac{\overline{\varphi}(r)\overline{\varphi}((n,r))}{\overline{\varphi}((n,r))\overline{\varphi}\left(\frac{r}{(n,r)}\right)} \\
&= (n,r)\mu\left(\frac{r}{(n,r)}\right) \frac{\overline{\varphi}(r)}{\overline{\varphi}\left(\frac{r}{(n,r)}\right)} \\
&= (n,r)\mu\left(\frac{r}{(n,r)}\right) \frac{r\varphi(r)}{(n,r)r\varphi\left(\frac{r}{(n,r)}\right)} \\
&= \frac{\mu\left(\frac{r}{(n,r)}\right)\varphi(r)}{\varphi\left(\frac{r}{(n,r)}\right)}
\end{aligned}$$

donde la primera igualdad se cumple por definición de $\Phi$ y la ecuación (2.5), la segunda por ser $\overline{\varphi}$ multiplicativa, separable y por el Lema 2.4 (II), la tercera por el Lema 2.4 (I) y la quinta por definición de $\overline{\varphi}$. ■

**Teorema 2.1.** *Toda función $f$ par* mód $r$ *tiene una expansión de la forma*

$$f(n) = \sum_{d\mid r} \alpha(d) c_d(n), \tag{2.6}$$

*y recíprocamente, toda función aritmética de esta forma es par* mód $r$*. Los coeficientes $\alpha(d)$ están dados por*

$$\alpha(d) = \frac{1}{r} \sum_{e\mid r} f\left(\frac{r}{e}\right) c_e\left(\frac{r}{d}\right), \tag{2.7}$$

*o por la fórmula equivalente,*

$$\alpha(d) = \frac{1}{r\varphi(d)} \sum_{m=1}^{r} f(m) c_d(m).$$

*A los coeficientes $\alpha$ se les llamará* ***coeficientes de Fourier*** *de la función par $f$.*

*Demostración.* Es claro que toda función de la forma (2.6) es par mód $r$, pues por el lema anterior si $d \mid r$ entonces $c_d(n) = c_d((n,r))$. Nótese que

$$\begin{aligned}\sum_{d|r} \alpha(d)c_d(n) &= \sum_{d|r}\left(\frac{1}{r}\sum_{e|r} f\left(\frac{r}{e}\right)c_e\left(\frac{r}{d}\right)\right)c_d(n)\\ &= \frac{1}{r}\sum_{e|r} f\left(\frac{r}{e}\right)\sum_{d|r} c_e\left(\frac{r}{d}\right)c_d(n)\\ &= \frac{1}{r}\sum_{e|r} f\left(\frac{r}{e}\right)\sum_{d|r} c_e\left(\frac{r}{d}\right)c_d((n,r))\\ &= \frac{1}{r}f\left(\frac{r}{q}\right)r = f((n,r)) = f(n),\end{aligned}$$

por el **??**, donde $r = (n,r)q$, para algún $q \in \mathbb{N}$ y donde la última igualdad se cumple por ser $f$ par mód $r$.

Por otro lado, de la demostración de la proposición 1.14 se puede rescatar el hecho de que el conjunto $\{1, 2, \ldots, r\}$ es igual a $\bigcup_{e|r}\{rx/e \,:\, (x,e) = 1, 1 \le x \le e\}$ y todos los conjuntos son disjuntos a pares, por tanto

$$\begin{aligned}\frac{1}{r\varphi(d)}\sum_{m=1}^{r} f(m)c_d(m) &= \frac{1}{r\varphi(d)}\sum_{e|r}\sum_{\substack{(x,e)=1\\1\le x\le e}} f\left(\frac{rx}{e}\right)c_d\left(\frac{rx}{e}\right)\\ &= \frac{1}{r\varphi(d)}\sum_{e|r}\sum_{\substack{(x,e)=1\\1\le x\le e}} f\left(\left(\frac{rx}{e}, r\right)\right)c_d\left(\left(\frac{rx}{e}, r\right)\right)\\ &= \frac{1}{r\varphi(d)}\sum_{e|r}\sum_{\substack{(x,e)=1\\1\le x\le e}} f\left(\frac{r}{e}\right)c_d\left(\frac{r}{e}\right)\\ &= \frac{1}{r\varphi(d)}\sum_{e|r} f\left(\frac{r}{e}\right)c_d\left(\frac{r}{e}\right)\varphi(e)\\ &= \frac{1}{r\varphi(d)}\sum_{e|r} f\left(\frac{r}{e}\right)c_e\left(\frac{r}{d}\right)\varphi(d)\\ &= \frac{1}{r}\sum_{e|r}\left(\frac{r}{e}\right)c_e\left(\frac{r}{d}\right),\end{aligned}$$

donde la segunda igualdad se cumple por ser $f$ par mód $r$, la tercera por ser $(rx/e, r) = r/e$, pues $(x,e) = 1$ implica que $(r/e)(x,e) = r/e$, y como $r/e$ es un entero positivo,

entonces $(rx/e, r) = r/e$. La cuarta por definición de $\varphi$, y la penúltima igualdad se cumple por la fórmula de Hölder (Lema 2.5) y el Corolario A.1, pues $e$ y $d$ dividen a $d$, así que

$$c_d\left(\frac{r}{e}\right)\varphi(e) = \frac{\varphi(d)\mu\left(\frac{d}{(r/e,d)}\right)}{\varphi\left(\frac{d}{(r/e,d)}\right)} = \frac{\varphi(d)\mu\left(\frac{e}{(r/d,e)}\right)}{\varphi\left(\frac{e}{(r/d,e)}\right)}\varphi(e) = \varphi(d)c_e\left(\frac{r}{d}\right) \tag{2.8}$$

■

**Corolario 2.5.** *Si $f$ y $f'$ son funciones pares* mód $r$*, entonces se verifican las siguientes implicaciones*

$$f(n) = \sum_{d|r} f'(d)c_d(n), \forall\, n \in \mathbb{N} \implies f'(\delta) = \frac{1}{r\varphi(\delta)} \sum_{m=1}^{r} f(m)c_d(m), \forall\, \delta \mid r,$$

$$f'(\delta) = \sum_{m=1}^{r} f(m)c_\delta(m), \forall\, d \mid r \implies f(n) = \frac{1}{r} \sum_{d|r} \frac{f'(d)}{\varphi(d)} c_d(n), \forall\, n \in \mathbb{N}.$$

*Demostración.* En efecto, como $f$ es par, entonces $f$ tiene una única representación de la forma (2.6), por tanto se verifica la primera implicación. Para la segunda implicación se tiene que, de nuevo por la ecuación (2.6),

$$f(n) = \sum_{d|r} \left( \frac{1}{r\varphi(d)} \sum_{m=1}^{r} f(m)c_d(m) \right) c_d(n) = \frac{1}{r} \sum_{d|r} \frac{f'(d)}{\varphi(d)} c_d(n).$$

■

Considerando los casos $\delta = 1$ y $n = r$ se tiene el siguiente corolario.

**Corolario 2.6.** *Si $f$ y $f'$ son funciones pares* mód $r$*, entonces*

$$f(n) = \sum_{d|r} f'(d)c_d(n), \forall\, n \in \mathbb{N} \implies f'(1) = \frac{1}{r} \sum_{m=1}^{r} f(m),$$

$$f'(\delta) = \sum_{m=1}^{r} f(m)c_\delta(m), \forall\, d \mid r \implies f(r) = \frac{1}{r} \sum_{d|r} f'(d).$$

Volviendo a la definición de la suma de Ramanujan módulo $r$, **??**, se puede considerar una clase más general de funciones, aquellas que se pueden escribir como

$$f(n) = \sum_{\delta|(n,r)} g(\delta), \forall\, n \in \mathbb{N},$$

donde $g$ es una función aritmética.

La siguiente proposición muestra que esta generalización preserva la modularidad respecto a $r$. Más aún, el Teorema 2.1 permite caracterizar a las funciones pares módulo $r$ de esta forma.

**Teorema 2.2.** *Toda función $f$ par módulo $r$ se puede expresar como*

$$f(n) = \sum_{\delta|(n,r)} g(\delta), \forall\, n \in \mathbb{N}. \tag{2.9}$$

*Y recíprocamente, toda función aritmética que tenga esta forma es par módulo $r$.*

*Demostración.* Dado que $(n, r) = ((n, r), r)$, es claro que toda función arimética que tenga dicha forma es par mód $r$. Supóngase que $f$ es par mód $r$. Por el Teorema 2.1, se puede escribir

$$\begin{aligned} f(n) &= \sum_{d|r} \alpha(d) c_d(n) = \sum_{d|r} \alpha(d) \sum_{\delta|(n,d)} \mu\left(\frac{d}{\delta}\right) \delta \\ &= \sum_{\delta|(n,d)} \sum_{d|r} \alpha(d) \mu\left(\frac{d}{\delta}\right) \delta = \sum_{\delta|(n,r)} \delta \sum_{d|r} \mu\left(\frac{d}{\delta}\right) \delta = \sum_{\delta|(n,r)} g(\delta) \end{aligned}$$

■

En vista de que toda función par tiene al menos dos representaciones, la del teorema anterior y la del Teorema 2.1, cabe preguntarse si existe alguna relación entre ellas. El siguiente teorema da respuesta a esta inquietud.

**Teorema 2.3.** *Si $f$ es par módulo $r$, entonces sus respectivas expansiones* (2.6) *y* (2.9) *están relacionadas mediante la fórmula*

$$\alpha(d) = \frac{1}{r} \sum_{e|r/d} g\left(\frac{r}{e}\right) e.$$

*Demostración.* Se tiene que

$$\alpha(d) = \frac{1}{r} \sum_{\delta|r} f\left(\frac{r}{\delta}\right) c_\delta\left(\frac{r}{d}\right) = \frac{1}{r} \sum_{\delta|r} c_\delta\left(\frac{r}{d}\right) \sum_{e|(r/\delta,\delta)} g(e) = \frac{1}{r} \sum_{\delta|r} c_\delta\left(\frac{r}{d}\right) \sum_{e|r/\delta} g(e)$$

$$= \frac{1}{r}\sum_{\delta|r} c_\delta\left(\frac{r}{d}\right)\sum_{e|r/\delta} g(e) = \frac{1}{r}\sum_{e|r} g\left(\frac{r}{e}\right)\sum_{\delta|e} c_\delta\left(\frac{r}{d}\right)$$
$$= \frac{1}{r}\sum_{e|r} g\left(\frac{r}{e}\right)\cdot\begin{cases} e & \text{si } e \mid r/d \\ 0 & \text{en otro caso} \end{cases} = \frac{1}{r}\sum_{e|r/d} g\left(\frac{r}{e}\right) e.$$

por el corolario 2.1. ■

## 2.2. El subespacio de funciones pares

Recuérdese del corolario 1.1 que el anillo $(\mathcal{A}, +, *)$ es un álgebra conmutativa con identidad. Se tiene que el conjunto de funciones pares es un subespacio de $\mathcal{A}$, pero no es un subanillo, pues en general $(f * g)(n) \neq (f * g)((n, r))$ aún cuando $f$ y $g$ sean pares mód $r$, tome por ejemplo dos funciones constantes. Se denotará como $\mathcal{A}_r$ al conjunto de funciones pares módulo $r$.

**Proposición 2.5.** *El conjunto $\mathcal{A}_r$ es una subespacio de $\mathcal{A}$.*

*Demostración.* Basta verificar las siguientes condiciones:

(i) $\mathcal{A}_r \neq \emptyset$

(ii) $f, g \in \mathcal{A}_r$ implica $f + g \in \mathcal{A}_r$

(iii) $c \in \mathbb{C}$ y $f \in \mathcal{A}_r$ implica $cf \in \mathcal{A}$.

Claro que $\mathbf{0} \in \mathcal{A}_r$. Sea $n \in \mathbb{N}$ y supóngase que $f, g \in \mathcal{A}_r$. Se tiene que $(cf)(n) = cf(n) = cf((n, r)) = (cf)((n, r))$, luego $cf \in \mathcal{A}_r$.

Además, $(f + g)(n) = f(n) + g(n) = f((n, r)) + g((n, r)) = (f + g)((n, r))$, así que $f + g \in \mathcal{A}_r$. ■

El corolario 2.3 afirma que las sumas de Ramanujan $\mathcal{B}_r = \{c_d\}_{d|r}$ son linealmente independientes respecto a la suma sobre los divisores de $r$, además el Teorema 2.1 nos permite expresar cualquier función par como una suma de este tipo. En otras palabras, el conjunto $\mathcal{B}_r$ es una base del espacio vectorial $\mathcal{A}_r$.

**Corolario 2.7.** *El espacio vectorial $\mathcal{A}_r$ tiene dimensión $d(r)$.*

En lo que sigue de esta sección se verá que los coeficientes de la expansión (2.6) pueden ser derivados de un producto interno en este espacio de funciones.

**Proposición 2.6.** *La operación* $\langle\ ,\ \rangle : \mathcal{A}_r \times \mathcal{A}_r \longrightarrow \mathbb{C}$ *definida como*

$$\langle f, g\rangle = \sum_{d|r} \varphi(d) f\left(\frac{r}{d}\right) \overline{g\left(\frac{r}{d}\right)}$$

*es un producto interno en* $\mathcal{A}_r$.

*Demostración.* Sean $c \in \mathbb{C}$ y $f, g, h \in \mathcal{A}_r$. Escríbase $f(n) = f_1(n) + if_2(n)$ para todo $n \in \mathbb{N}$, donde $f_1, f_2 \in \mathcal{A}_{\mathbb{R}}$. Entonces

(i)

$$\begin{aligned}\langle f, f\rangle &= \sum_{d|r} \varphi(d) \left[f_1\left(\frac{r}{d}\right) + if_2\left(\frac{r}{d}\right)\right] \overline{\left[f_1\left(\frac{r}{d}\right) + if_2\left(\frac{r}{d}\right)\right]} \\ &= \sum_{d|r} \varphi(d) \left[f_1^2\left(\frac{r}{d}\right) + f_2^2\left(\frac{r}{d}\right)\right] \geq 0\end{aligned}$$

Además, si $\langle f, f\rangle = 0$, como todos los términos de la suma anterior son positivos, se debe tener que $f_1(d) = f_2(d) = 0$ para todo $d$ divisor de $r$. Si $n \in \mathbb{N}$ entonces $f_1(n) = f((n, r)) = 0$, pues $f$ es par mód $r$ y $(n, r) \mid r$. Análogamente se tiene $f_2(n) = 0$. Luego $f(n) = f_1(n) + if_2(n) = 0$ para cada $n \in \mathbb{N}$, es decir $f = \mathbf{0}$.

(ii)

$$\begin{aligned}\langle f + g, h\rangle &= \sum_{d|r} \varphi(d)(f + g)\left(\frac{r}{d}\right) \overline{g\left(\frac{r}{d}\right)} = \sum_{d|r} \varphi(d) \left[f\left(\frac{r}{d}\right) \overline{h\left(\frac{r}{d}\right)} + g\left(\frac{r}{d}\right) \overline{h\left(\frac{r}{d}\right)}\right] \\ &= \sum_{d|r} \varphi(d) f\left(\frac{r}{d}\right) \overline{h\left(\frac{r}{d}\right)} + \sum_{d|r} g\left(\frac{r}{d}\right) \overline{h\left(\frac{r}{d}\right)} = \langle f, h\rangle + \langle g, h\rangle\end{aligned}$$

(iii)

$$\langle cf, g\rangle = \sum_{d|r} \varphi(d) cf\left(\frac{r}{d}\right) \overline{g\left(\frac{r}{d}\right)} = c \sum_{d|r} \varphi(d) f\left(\frac{r}{d}\right) \overline{g\left(\frac{r}{d}\right)} = c\langle f, g\rangle$$

(iv)

$$\overline{\langle g, f\rangle} = \overline{\sum_{d|r} \varphi(d) g\left(\frac{r}{d}\right) \overline{f\left(\frac{r}{d}\right)}} = \sum_{d|r} \varphi(d) f\left(\frac{r}{d}\right) \overline{g\left(\frac{r}{d}\right)} = \langle f, g\rangle$$

■

El producto interno así definido podría haberse escrito sin el factor $\varphi(d)$ dentro de la suma. Su uso se justifica al usar la ecuación (2.8) para probar que este producto interno hace de $\mathcal{B}_r$ una base ortogonal de $\mathcal{A}_r$.

**Proposición 2.7.** *Si $i, j$ son divisores positivos de $r$, entonces*

$$\langle c_i, c_j \rangle = \begin{cases} r\varphi(j) & \text{si } i = j \\ 0 & \text{en otro caso.} \end{cases}$$

*Demostración.* En efecto,

$$\langle c_i, c_j \rangle = \sum_{d|r} \varphi(d) c_i\left(\frac{r}{d}\right) c_j\left(\frac{r}{d}\right) = \sum_{d|r} c_i\left(\frac{r}{d}\right) \varphi(j) c_d\left(\frac{r}{j}\right) = \begin{cases} r\varphi(j) & \text{si } i = j \\ 0 & \text{en otro caso,} \end{cases}$$

donde la segunda igualdad se cumple por la ecuación (2.8) y la tercera por el **??**. ∎

**Corolario 2.8.** *El conjunto*

$$\mathcal{B}'_r = \left\{ c'_d = \frac{1}{\sqrt{r\varphi(d)}} c_d \right\}_{d|r}$$

*es una base ortonormal de $\mathcal{A}_r$.*

Como consecuencia del corolario anterior, toda función $f$ par mód $r$ debe tener una expansión de la forma $\sum_{e|r} \beta(e) c'_e$. Además, si $d$ es un divisor arbitrario de $r$, entonces

$$\left\langle f, c'_d \right\rangle = \left\langle \sum_{e|r} \beta(e) c'_e, c'_d \right\rangle = \sum_{e|r} \beta(e) \left\langle c'_e, c'_d \right\rangle = \beta(d),$$

pero $f$ también tiene una única representación de la forma $\sum_{e|r} \alpha(d) c_d$, en consecuencia, $\alpha(d) = \beta(d)/\sqrt{r\varphi(d)}$ para cada $d$ divisor de $r$. Por tanto,

$$\begin{aligned} \alpha(d) &= \frac{\beta(d)}{\sqrt{r\varphi(d)}} = \frac{1}{\sqrt{r\varphi(d)}} \left\langle f, c'_d \right\rangle \\ &= \frac{1}{\sqrt{r\varphi(d)}} \sum_{e|r} \varphi(e) f\left(\frac{r}{e}\right) c'_d\left(\frac{r}{e}\right) \\ &= \frac{1}{\sqrt{r\varphi(d)}} \sum_{e|r} \varphi(e) f\left(\frac{r}{e}\right) \frac{1}{\sqrt{r\varphi(d)}} c_d\left(\frac{r}{e}\right) \\ &= \frac{1}{r\varphi(d)} \sum_{e|r} f\left(\frac{r}{e}\right) \varphi(d) c_e\left(\frac{r}{d}\right) \end{aligned}$$

$$= \frac{1}{r} \sum_{e|r} f\left(\frac{r}{e}\right) c_e\left(\frac{r}{d}\right),$$

donde la cuarta igualdad se cumple nuevamente por (2.8). Esta es la ecuación (2.7). Como es usual en el análisis funcional, ahora se pueden llamar propiamente *coeficientes de Fourier* a los coeficientes $\alpha$ del Teorema 2.1.

# 3. Procesamiento de señales

Una *señal* es una descripción de un fenómeno que evoluciona en el tiempo o espacio; el *procesamiento de señales* se refiere a cualquier operación manual o mecánica que modifique, analice o manipule de otra forma la información contenida en una señal. Considérese, por ejemplo, la temperatura ambiente; se puede medir su evolución coon el tiempo de muchas formas y los datos resultantes representan una "señal" de temperatura. Algunas operaciones sobre esta señal se pueden hacer incluso a mano, por ejemplo calcular la temperatura promedio en un mes o graficar la señal en una hoja de papel.

El adjetivo "digital" proviene de *digitus*, palabra latina para dedo. En este contexto, se refiere a un paradigma en el que el mundo físico se puede describir usando únicamente números enteros. El *procesamiento digital de señales* es por tanto una rama del procesamiento de señales en la cual todo, incluido el tiempo, es descrito en términos de números enteros. En el procesamiento de digital de señales, la representación abstracta subyacente siempre es el conjunto de números naturales, independientemente de la naturaleza de la señal [15].

**Definición 3.1.** Más específicamente, una *señal* es cualquier función $x : \mathbb{Z} \longrightarrow \mathbb{C}$.

*Observación 3.1.* Es necesario establecer las dos convenciones siguientes a lo largo del capítulo, siguiendo la notación estándar en la literatura de procesamiento de señales:

- El valor de una señal $x$ en un índice entero $n$ se denotará como $x[n]$, con corchetes en vez de paréntesis.
- A partir de ahora se le denotará $j$ a la unidad imaginaria, es decir, $j = \sqrt{-1}$.
- Nuevamente, durante todo el capítulo se supondrá que $r$ es un entero positivo arbitrario pero fijo.

En este capítulo se estudiará una clase particular de señales periódicas, llamadas señales *simétricas* o *pares*, con las herramientas del capítulo anterior. Estas señales no son más que funciones aritméticas pares definidas en los enteros.

## 3.1. Transformada Discreta de Fourier

**Definición 3.2**. (Señal periódica)**.** Desde luego, una señal periódica con periodo $r \in \mathbb{N}$ es una señal para la cual $x[n] = x[n + kr]$ para cada $n, k \in \mathbb{Z}$.

Una señal periódica con periodo $r$ contiene toda su información en un periodo, en el cuál toma $r$ valores complejos. Considérese pues un arreglo con estos valores, es decir, un elemento de $\mathbb{C}^r$.

Sea $W_r = e^{-j(2\pi/r)}$ y considérese el producto interno $\langle x, y\rangle = \sum_{n=1}^{r} \overline{x[n]}y[n]$ en $\mathbb{C}^r$. Se sabe, véase por ejemplo [15], que el conjunto $\{w_k\}_{k=1}^{r}$, donde

$$w_k = (W_r^{-k}, W_r^{-2k}, \ldots, W_r^{-(r-1)k}, 1) \in \mathbb{C}^r, w = 1, \ldots, r,$$

es una base ortogonal de $\mathbb{C}^r$. En efecto,

$$\langle w_m, w_n\rangle = \sum_{i=1}^{r} \overline{W_r^{-mi}} W_r^{-ni} = \sum_{i=1}^{r} W_r^{(m-n)i} = \begin{cases} r & \text{si } m = n \\ \dfrac{1 - W_r^{(m-n)r}}{1 - W_r^{m-n}} = 0 & \text{en otro caso.} \end{cases}$$

Por otro lado, si $x \in \mathbb{C}^r$, existen por tanto $X(k) \in \mathbb{C}, k = 1, \ldots, r$, tales que $rx = \sum_{k=1}^{r} X[k]w_k$. Pero

$$\langle w_k, x\rangle = \left\langle w_k, \frac{1}{r}\sum_{n=1}^{r} X[n]w_n \right\rangle = \frac{1}{r}\sum_{n=1}^{r} \langle w_k, X[n]w_n\rangle = \frac{X[k]}{r} r = X[k].$$

En consecuencia,

$$X[k] = \sum_{n=1}^{r} \overline{W_r^{-nk}} x[n] = \sum_{n=1}^{r} x[n] W_r^{nk}, \forall\, k = 1, \ldots, r \tag{3.1}$$

y

$$x[n] = \frac{1}{r}\sum_{k=1}^{r} X[k]w_k[n] = \frac{1}{r}\sum_{k=1}^{r} X[k] W_r^{-nk}, \forall\, n = 1, \ldots, r. \tag{3.2}$$

La ecuación (3.1) se conoce como fórmula de *análisis* o *coeficientes de Fourier discretos* y la ecuación (3.2) como fórmula de *síntesis* o *reconstrucción* del elemento $x \in \mathbb{C}^r$.

Considere la fórmula de síntesis. Dado que $W_r^{(n+ir)k} = W_r^{nk}$ para cada $i \in \mathbb{Z}$, entonces $x[n + ir] = x[n]$ para todos $i \in \mathbb{Z}$, $n = 1, \ldots, r$, de manera que se puede extender $x \in \mathbb{C}^r$ a una señal periódica a todo $\mathbb{Z}$ de forma natural. Si $\tilde{x}$ es una señal periódica y se calcula la fórmula de reconstrucción con los valores de su periodo, dicha extensión coincide con $\tilde{x}$ en todo $\mathbb{Z}$, así que se puede escribir

$$\tilde{X}[k] = \sum_{n=1}^{r} \overline{W_r^{-nk}} \tilde{x}[n] = \sum_{n=1}^{r} \tilde{x}[n] W_r^{nk}, \forall\, k \in \mathbb{Z} \tag{3.3}$$

y

$$\tilde{x}[n] = \frac{1}{r}\sum_{k=1}^{r} \tilde{X}[k] w_k[n] = \frac{1}{r}\sum_{k=1}^{r} \tilde{X}[k] W_r^{-nk}, \forall\, n \in \mathbb{Z}, \tag{3.4}$$

donde la fórmula (3.1) se ha extendido implicitamente a todos los enteros. Dicha extensión, la ecuación (3.3), se llama *transformada discreta de Fourier* de la señal $\tilde{x}$. La ecuación (3.4) también será llamada fórmula de *síntesis* o *reconstrucción* de la señal $\tilde{x}$.

## 3.2. Señales simétricas

Las señales simétricas son un análogo a las funciones aritméticas pares estudiadas en el capítulo anterior.

**Definición 3.3**. (Señal simétrica)**.** Una señal $x$ se dice *simétrica módulo* $r$ si $x[n] = x[(n, r)]$ para cada $n \in \mathbb{Z}$.

Toda señal simétrica módulo $r$ es periódica módulo $r$ y la demostración es idéntica a la de la Proposición 2.1. Una de las principales diferencias entre las señales periódicas y las simétricas, es que las últimas en general tienen una imagen más pequeña, más específicamente, la cardinalidad de su imagen no puede exceder $d(r)$.

**Proposición 3.1.** *Si $x : \mathbb{Z} \longrightarrow \mathbb{C}$ es una señal simétrica módulo $r$, entonces $|x(Z)| \leq d(r)$, donde $d(r)$ es el número de divisores de $r$.*

*Demostración.* Para cada divisor positivo $d$ de $r$, sea

$$S_d = \left\{ \left(\frac{r}{d}\right) \alpha \ : \ (\alpha, d) = 1, 1 \leq \alpha \leq d \right\}.$$

Por la proposición ??, se tiene que $\bigcup_{d|r} S_d = \{1, 2, \ldots, r\}$.

Además, si $(r/d)\alpha \in S_d$ entonces

$$\left(\left(\frac{r}{d}\alpha\right), r\right) = \left(\left(\frac{r}{d}\right), r\right) = \frac{r}{d}, \tag{3.5}$$

pues $(\alpha, d) = 1$ y $d \mid r$. Más aún, si $x$ es simétrica y $n, m \in S_e$ entonces $\alpha[n] = \alpha[m]$. En efecto, se debe tener que $n = (r/d)\alpha$ y $m = (r/d)y$ con $(\alpha, d) = (\beta, d) = 1$ y $1 \leq \alpha, \beta \leq d$. Luego, como $x$ es simétrica,

$$x[n] = x\left[\frac{r}{d}\alpha\right] = x\left[\left(\frac{r}{d}\alpha, r\right)\right] = x\left[\frac{r}{d}\right]$$

y

$$x[m] = x\left[\frac{r}{d}\beta\right] = x\left[\left(\frac{r}{d}\beta, r\right)\right] = x\left[\frac{r}{d}\right],$$

por tanto $x[n] = x[m]$. Como $x$ es periódica con periodo $r$, hace falta conocer sus valores únicamente en los enteros $1, \ldots, r$. Así,

$$\{x[1], \ldots, x[r]\} = \bigcup_{d|r} \left\{x\left[\left(\frac{r}{d}\right)\alpha\right] \,:\, (\alpha, d) = 1, 1 \leq \alpha \leq d\right\} = \bigcup_{d|r} \{x[r/d]\},$$

donde el último conjunto tiene a lo sumo $d(r)$ elementos. ■

Los conjuntos $S_d$ de la proposición anterior de llaman *sistemas de residuos* de los divisores $d$ de $r$ [18]. Al igual que con las sumas de Ramanujan, cada señal par se puede expresar como combinación lineal de señales indicadoras sobre los sistemas de residuos.

**Definición 3.4.** Si $d$ es un divisor de $r$, se define $h_{r,d} : \{1, \ldots, r\} \longrightarrow \mathbb{C}$ como

$$h_{r,d}[n] = \begin{cases} 1 & \text{si } n \in S_d \\ 0 & \text{en otro caso.} \end{cases}$$

**Proposición 3.2.** *Para cada $n \in \{1, 2, \ldots, r\}$ se tiene $h_{r,d}[n] = h_{r,d}[(n, r)]$.*

*Demostración.* Sea $d$ un divisor positivo de $r$ y sea $n \in \{1, 2, \ldots, r\}$. Basta probar que $n \in S_d$ si y sólo si $(n, r) \in S_d$.

Si $n \in S_d$, entonces $n = (r/d)x$ con $(x, d) = 1$ y $1 \leq x \leq d$. Además, como $(n, r) \mid n$ y $(n, r) \mid r$, existen $a, b \in \mathbb{N}$ tales que $n = (n, r)a$ y $r = (n, r)b$. Luego $(n, r)a = (r/d)x$ y por tanto $(n, r)ad = (n, r)bx$, así que $ad = bx$. Dado que $(a, b) = (n/(n, r), r/(n, r)) = 1$ y $a \mid bx$, entonces $a \mid x$ y por tanto $x = aq$, para algún $q \in \mathbb{N}$. Se sigue que $(n, r) = (r/d)q$ y además $1 \leq q \leq aq = x \leq d$. Luego $(n, r) \in S_d$.

Recíprocamente, si $(n, r) \in S_d$, escríbase $(n, r) = (r/d)y$ con $(y, d) = 1$ y $1 \leq y \leq d$. Como $(n, r) \mid r$ entonces $(r/d)y \mid r$, luego $r = (r/d)yq$ para algún $q \in \mathbb{N}$ y por tanto $rd = ryq$, así que $d = yq$, es decir $y \mid d$. Se debe tener por tanto que $y = (y, d) = 1$, luego $(n, r) = (r/d)$ y como $n = (n, r)a$ para algún $a \in \mathbb{N}$, entonces $n = (r/d)a$. Además, como $n \leq r$, entonces $(r/d)a \leq r$, luego $ra \leq rd$, es decir, $1 \leq a \leq d$ y por tanto $n \in S_d$. ■

Las funciones $h_{r,d}$ se pueden extender de forma natural a una función simétrica a todo $\mathbb{Z}$ definiendo $h_{r,d}[n] = h_{r,d}[(n, r)]$ para cada $n \in \mathbb{Z}$ y abusando de la notación se le seguirá denotando $h_{r,d}$. Sin embargo, en lo que sigue será suficiente considerar únicamente su restricción a $\{1, 2, \ldots, r\}$.

**Proposición 3.3.** *Cualquier señal simétrica $x$ módulo $r$ se puede escribir como*

$$x[n] = \sum_{d|r} x\left[\frac{r}{d}\right] h_{r,d}[n], \tag{3.6}$$

*para todo $n \in \mathbb{Z}$.*

*Demostración.* Sin pérdida de generalidad supóngase que $n \in \{1, 2, \ldots, r\}$. Entonces existe un único $e \mid r$ tal que $n \in S_e$, es decir, tal que $n = (r/e)\alpha$, con $(e, \alpha) = 1$ y $1 \leq \alpha \leq e$. Luego

$$\begin{aligned}\sum_{d|r} x\left[\frac{r}{d}\right] h_{r,d}[n] = \sum_{\substack{d|r \\ n\in S_d}} x\left[\frac{r}{d}\right] = x\left[\frac{r}{e}\right] = x\left[\left(\frac{r}{e}, r\right)\right] \\ = x\left[\left(\frac{r}{e}\alpha, r\right)\right] = x[(n, r)] = x[n]\end{aligned}$$

por (3.5) y por ser $x$ simétrica. ∎

La siguiente proposición muestra que las sumas de Ramanujan aparecen naturalmente como los coeficientes de Fourier clásicos en la fórmula de síntesis (3.4) para las señales $h_{r,d}$.

**Proposición 3.4.** *Los coeficientes de Fourier de la señal $h_{r,d}$ están dados por*

$$H_{r,d}[k] = c_d[k].$$

*donde $c_d$ es la suma de Ramanujan módulo $d$.*

*Demostración.* Utilizando (3.1) para calcular los coeficientes de $h_{r,d}$ en (3.4), se tiene que:

$$\begin{aligned}H_{r,d}[k] = \sum_{n=1}^{r} h_{r,d}(n) W_r^{nk} = \sum_{\substack{n=1 \\ n\in S_d}}^{r} W_r^{nk} = \sum_{\substack{n=1 \\ n=(r/d)x \\ 1\leq x\leq d \\ (x,d)=1}}^{r} W_r^{nk} \\ = \sum_{\substack{x=1 \\ (x,d)=1}}^{d} W_d^{xk} = \sum_{\substack{x=1 \\ (x,d)=1}}^{d} W_d^{-xk} = c_d[k], \qquad (3.7)\end{aligned}$$

pues $e^{-i(2\pi/r)nk} = e^{-i(2\pi/d)xk}$ si $n = (r/d)x$. ∎

**Proposición 3.5.** *Si $x$ es una señal simétrica, sus coeficientes de Fourier discretos están dados por*

$$X[k] = \sum_{d|r} x\left[\frac{r}{d}\right] c_d[k].$$

*Demostración.* Utilizando las ecuaciones ecuaciones (3.1), (3.6) y (3.7) se tiene que

$$\begin{aligned} X[k] = \sum_{n=1}^{r} x[n] W_r^{nk} = \sum_{n=1}^{r} \sum_{d|r} x\left[\frac{r}{d}\right] h_{r,d}[n] W_r^{nk} = \sum_{d|r} x\left[\frac{r}{d}\right] \sum_{n=1}^{r} h_{r,d}[n] W_r^{nk} \\ = \sum_{d|r} x\left[\frac{r}{d}\right] H_{r,d}[k] = \sum_{d|r} x\left[\frac{r}{d}\right] c_d[k]. \end{aligned}$$

■

*Observación 3.2.* Dado que $c_d[k] = c_d[(k,d)]$, la proposición anterior implica que la transformada discreta de Fourier de una señal simétrica módulo $r$ también es simétrica módulo $r$. Además tal ecuación define una extensión natural de $c_d$ a todo $\mathbb{Z}$.

**Proposición 3.6.** *Si $x$ es una señal simétrica módulo $r$, entonces*

$$x[n] = \frac{1}{r} \sum_{d|r} X\left[\frac{r}{d}\right] c_d[n], \forall\, n \in \mathbb{Z}.$$

*Demostración.* Considere la transformada de Fourier discreta $X$ de $x$. Dado que $X$ también es simétrica módulo $r$, la proposición 3.3 implica que

$$X[n] = \sum_{d|r} x\left[\frac{r}{d}\right] h_{r,d}[n], \forall\, n \in \mathbb{Z},$$

luego, usando la fórmula de reconstrucción (3.4), se tiene

$$\begin{aligned} x[n] = \frac{1}{r} \sum_{k=1}^{r} X[k] W_r^{-nk} = \frac{1}{r} \sum_{k=1}^{r} \sum_{d|r} X\left[\frac{r}{d}\right] h_{r,d}[k] W_r^{-nk} \\ = \frac{1}{r} \sum_{d|r} X\left[\frac{r}{d}\right] \sum_{k=1}^{r} h_{r,d}[k] W_r^{-nk} = \frac{1}{r} \sum_{d|r} X\left[\frac{r}{d}\right] c_d[n], \end{aligned}$$

para todo $n \in \mathbb{Z}$. ■

*Ejemplo 3.1.* Como ejemplo concreto, considere una señal $x$ arbitraria y simétrica módulo $r = 10$. Por la proposición 3.1, $x$ puede tomar a lo sumo $d(10) = 4$ valores y estos estarán agrupados en los sistemas de residuos de los divisores de 10.

Específicamente, se tiene $S_1 = \{10\}, S_2 = \{5\}, S_5 = \{2,4,6,8\}, S_{10} = \{1,3,5,7\}$. Por tanto, $x[2] = x[4] = x[6] = x[8]$ y $x[1] = x[3] = x[5] = x[7]$. Luego los coeficientes $X[k]$, dados por 3.5, son

$$\begin{aligned}
X[1] = X[3] = X[5] = X[7] &= \sum_{d|10} x\left[\frac{10}{d}\right] c_d[1] = x[10] - x[5] - x[2] + x[1] \\
X[2] = X[4] = X[6] = X[8] &= \sum_{d|10} x\left[\frac{10}{d}\right] c_d[2] = x[10] + x[5] - x[2] - x[1] \\
X[5] &= \sum_{d|10} x\left[\frac{10}{d}\right] c_d[5] = x[10] - x[5] + 4x[2] - 4x[1] \\
X[10] &= \sum_{d|10} x\left[\frac{10}{d}\right] c_d[10] = x[10] + x[5] + 4x[2] + 4x[1].
\end{aligned}$$

El cálculo de estos coeficientes se reduce entonces a calcular $c_d[k]$ para cada $d \mid r$ y $k \mid r$. A diferencia de la transformada discreta de Fourier clásica, éstos cálculos no requieren la implementación de las funciones sin y cos en un microprocesador. Las sumas de Ramanujan se puede implementar o bien usando la proposición 2.3, implementando sólo la función de Möbius, una una suma condicional y el máximo común divisor, o bien utilizando la fórmula cerrada sin sumatorias 2.5 (fórmula de Hölder), pero implementando la función de Möbius, la función $\varphi$ de Euler y el máximo común divisor.

*Ejemplo 3.2.* Suponga que se quiere obtener una señal simétrica $x$ módulo 3 tal que $x[1] = x[2] = 1$ y $x[3] = 3$. Calculando sus coeficientes de Fourier, se tiene

$$\begin{aligned}
X[1] = X[2] &= \sum_{d|3} x\left[\frac{3}{d}\right] c_d[1] = x[3] - x[1] = 2 \\
X[2] &= \sum_{d|3} x\left[\frac{3}{d}\right] c_d[3] = x[3] + 2x[1] = 5.
\end{aligned}$$

Utilizando la fórmula de reconstrucción, se puede escribir

$$x[n] = \frac{1}{3} \sum_{d|3} X\left[\frac{3}{d}\right] c_d[n] = \frac{1}{3} \left(5c_1[n] + 2c_3[n]\right), \forall\, n \in \mathbb{Z}.$$

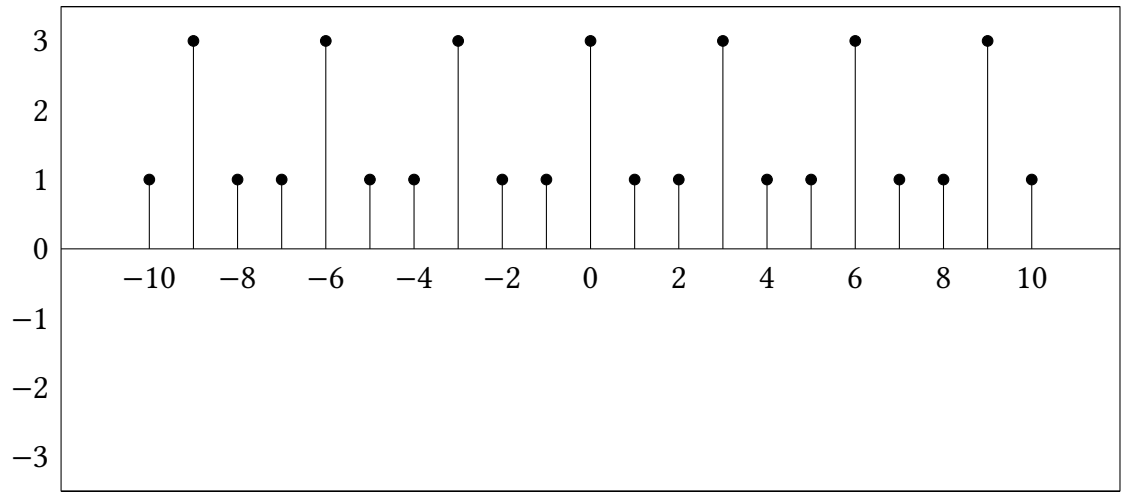


**Figura 1:** $x[n] = \frac{1}{3}(5c_1[n] + 2c_3[n])$

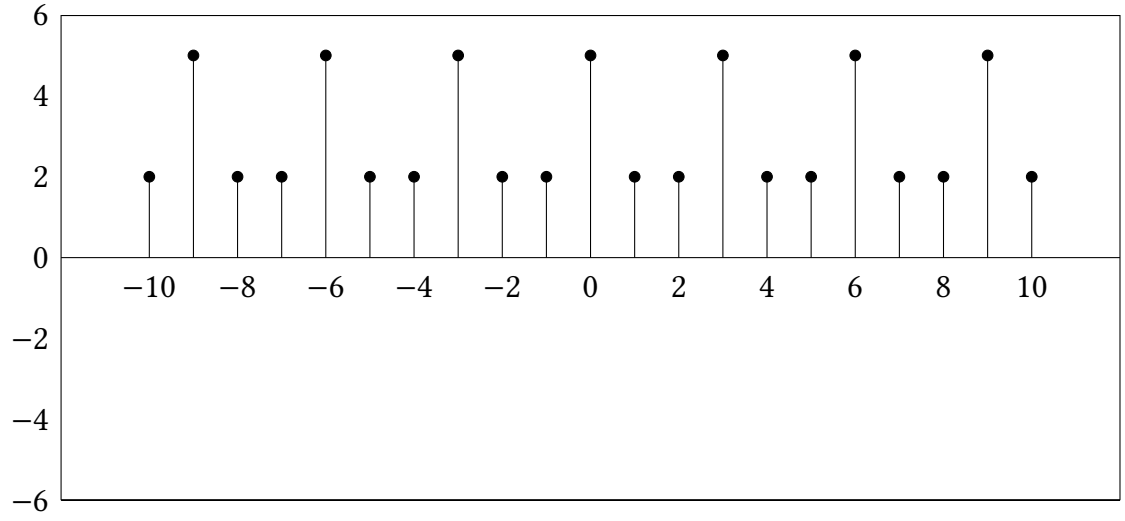


**Figura 2:** $X[n] = 3c_1[k] + c_3[k]$

Se puede calcular también su transformada discreta de Fourier usando la proposición 3.5 para todo entero $k$,

$$X[k] = \sum_{d|3} x\left[\frac{3}{d}\right] c_d[k] = 3c_1[k] + c_3[k], \forall\, k \in \mathbb{Z}.$$

La gráfica de esta señal se muestra en la Figura 2.

# A. Divisibilidad

**Proposición A.1.** *Si* $r \in \mathbb{N}$, $r = eq_1$, $r = dq_2$, $d = (q_1, d)k_1$ *y* $e = (q_2, e)k_2$ *entonces* $k_1 = k_2$.

*Demostración.* Nótese que $q_1, q_2$ enteros positivos, además $(q_1q_2, r) = (q_1q_2, r)$, luego $(q_1q_2, eq_1) = (q_1q_2, dq_2)$ y por tanto $q_1(q_2, e) = q_2(q_1, d)$ por la proposición anterior. Luego, dado que $r = (q_2, e)k_2q_1 = (q_1, d)k_1q_2$, la ley de cancelación implica que $k_1 = k_2$. ■

**Corolario A.1.** *Si* $r \in \mathbb{N}$, $e \mid r$ *y* $d \mid r$ *con* $e, r \in \mathbb{N}$, *entonces*

$$d/(r/e, d) = e/(r/d, e)\,.$$

**Teorema A.1** (Lema de Euclides)**.** *Si* $a \mid bc$ *y* $(a, b) = 1$ *entonces* $a \mid c$.

*Demostración.* Si $(a, b) = 1$, podemos escribir $1 = as + bt$, donde $s, t \in \mathbb{Z}$. Luego $c = a(sc) + bc(t)$ y como $a \mid a$ y $a \mid bc$ por hipótesis, entonces $a \mid c$. ■

# Bibliografía

[1] APOSTOL, T. M. *Introduction to Analytic Number Theory*. Springer, 1976.

[2] BELL, E. T. Arithmetic of logic. *Transactions of the American Mathematical Society 29*, 3 (1927), 597–611.

[3] BELL, E. T. Outline of a theory of arithmetical functions in their algebraic aspects. *The Journal of the Indian Mathematical Society 17* (1928), 249–260.

[4] BRUALDI, R. A. *Introductory Combinatorics*, 3 ed. Prentice-Hall, 1999.

[5] CASHWELL, E. D., AND EVERETT, C. J. The ring of number-theoretic functions. *Pacific Journal of Mathematics 9*, 4 (1959).

[6] COHEN, E. A class of arithmetical functions. *Proceedings of the National Academy of Sciences of the United States of America 41*, 11 (1955).

[7] DICKSON, L. E. *History of the Theory of Numbers*, vol. I. Chelsea Publishing Company, 1952.

[8] GAUSS, C. F. *Disquisitiones Arithmeticae*, english ed. Springer-Verlag, 1966.

[9] HARDY, G. H., AND WRIGHT, E. M. *An Introduction to the Theory of Numbers*, 5 ed. Oxford University Press, 1979.

[10] HUNGERFORD, T. W. *Algebra*. Springer, 1974.

[11] KNOPFMACHER, J. *Abstract Analytic Number Theory*, vol. 12. North-Holland Publishing Company, 1975.

[12] KNOPFMACHER, J. Fourier analysis of arithmetical functions. *Annali di Matematica Pura ed Applicata 109* (1976), 177–201.

[13] MURTY, M. R. Ramanujan series for arithmetical functions. *Hardy-Ramanujan Journal 36* (2013).

[14] NISHIMURA, H. On the unique factorization theorem for formal power series. *Journal of Mathematical Sciences, Kyoto Univ.* (1967).

[15] PRANDONI, P., AND VETTERLI, M. *Signal processing for comunnications*, 1 ed. EPFL Press, 2008.

[16] Ramanujan, S. On certain trigonometric sums and their applications in the theory of numbers. *Transactions of the Cambridge Phil. Society 22* (1918), 179–199.

[17] Rearick, D. F. Operators on algebras of arithmetic functions. *Duke Mathematical Journal 35* (1968), 761–766.

[18] Samadi, S., Ahmad, M., and Swamy, M. Ramanujan sums and discrete Fourier transforms. *IEEE Signal Processing Letters 12*, 4 (2005), 293–296.

[19] Zaldívar, F. *Introducción a la teoría de números*, 1 ed. Fondo de Cultura Económica, 2014.