Borrador de tesis

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

Índice general

Introducción

Euclides (circa 325 a. C.) probó que $2^{p-1}(2^p - 1)$ es un número perfecto si y sólo si $2^p - 1$ es un número primo [4]. En 1638, Descartes afirmó que todo número perfecto par es de la forma descrita por Euclides y que todo número perfecto impar debe ser de la forma ps^2, con p un número primo. Dickson [4] dió una prueba para lo primero, aunque Euler ya había probado ambos casos mucho antes y sus demostraciónes no salieron a la luz hasta después de su muerte.

Mersenne publicó en 1644 los primeros once números perfectos pares, dados por la fórmula de Euclides para los primos $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ y 257, pero se equivocó al agregar al 67 y al no incluir a los primos $61, 89$ y 107. Más tarde en 1640 y probablemente influenciado por éstas observaciones sobre números perfectos, Fermat consideró a los números de la forma $a^{p-1} - 1$, donde p es cualquier primo y a cualquier entero. Observó que si a no es divisible por p entonces $a^{p-1} - 1$ es divisible por p, hecho que se conocería más tarde como el Teorema de Fermat. El caso $a = 2$ era conocido en China al menos desde el año 500 a. C. La primera demostración publicada fue dada por Euler en 1736 y más tarde generalizada a cualquier entero: si $\varphi(n)$ denota el número de enteros positivos menores que n que son primos relativos a n, entonces $a^{\varphi(n)} - 1$ es divisible por n, para cualquier entero a primo relativo a n.

Aunque la función φ de Euler se definió inicialmente para enunciar la generalización anterior, ésta posee remarcables propiedades que hacen valer la pena estudiarla por sí misma. Por ejemplo, en 1801, Gauss probó que si $n \in \mathbb{N}$ y $d_1, d_2, \cdots, d_k$ son todos los divisores positivos de n, entonces $\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_k) = n$.

1. El teorema fundamental de la aritmética

1.1. Algoritmo de la división

Definición 1.1. *Sean $a, b \in \mathbb{Z}$. Decimos que a divide a b, o que a es factor de b, o que b es múltiplo de a, si existe $q \in \mathbb{Z}$ tal que $b = aq$.*

Notación. Utilizaremos la expresión $a \mid b$ para indicar que a divide a b. La notación $a \nmid b$ significa que a no divide a b.

Proposición 1.1. *Las siguientes propiedades de divisibilidad serán ocasionalmente útiles:*

(i) $a \mid a, \forall\ a \in \mathbb{Z}$

(ii) $a \mid 0, \forall\ a \in \mathbb{Z}$

(iii) $0 \mid a \iff a = 0$

(iv) $1 \mid a, \forall\ a \in \mathbb{Z}$

(v) $b \mid 1 \iff |a| = 1$

(vi) $a \mid b$ *y* $b \mid a \implies |a| = |b|$

(vii) $a \mid b$ *y* $b \mid c$ *implica* $a \mid c$

(viii) $a \mid b \implies a \mid bc, \forall\ c \in \mathbb{Z}$

(ix) $a \mid b$ *y* $a \mid c$ *implica* $a \mid a + c$

(x) $a \mid b$ *y* $a \mid c$ *implica* $a \mid bs + ct, \forall\ s, t \in \mathbb{Z}$

(xi) $|a| \mid |b| \iff a \mid b \iff -a \mid b \iff a \mid -b \iff -a \mid -b$

(xii) $a \mid b \implies ca \mid cb, \forall\ c \in \mathbb{Z}$

(xiii) $ca \mid cb$ *y* $c \neq 0$ *implica que* $a \mid b$.

Proposición 1.2. *Si $a \mid b$ y $b \neq 0$, entonces $|a| \leq |b|$.*

Demostración. Como $a \mid b$, existe $q \in \mathbb{Z}$ tal que $b = aq$ y dado que $b \neq 0$ entonces $q \neq 0$, de manera que $1 \leq |q|$, luego $|a| \leq |a||q| = |b|$. ∎

Teorema 1.1 (Algoritmo de la división). *Si $a, b \in \mathbb{Z}$ y $b \neq 0$, entonces existen únicos $q, r \in \mathbb{Z}$ tales que*

$$a = bq + r \quad \text{con} \quad 0 \leq r < |b|$$

Demostración. Supongamos primero que $b > 0$. Sea

$$S = \{a - bx \ : \ x \in \mathbb{Z} \text{ y } 0 \leq a - bx\}.$$

Como $0 < b$, entonces $1 \leq b$, luego $-b \leq -1$, por tanto $-b|a| \leq -|a|$, pero $-|a| \leq a$, así que $-b|a| \leq a$, osea $0 \leq a + b|a| = a - b(-|a|)$. Luego el conjunto S es no vacío, de manera que debe tener un elemento mínimo r, escribamos $r = a - bq$. Entonces $a = bq + r$ y $0 \leq r$ por elección de r. Si $b \leq r$, entonces $0 \leq r - b < r$, donde $r - b = a - bq - b = a - b(q + 1) \in S$, lo que contradice la elección de r, así que necesariamente $r < b$. Luego q, r son los enteros buscados. Supongamos ahora que $b < 0$. Entonces $|b| = -b > 0$ y por lo anterior existen $q', r' \in \mathbb{Z}$ tales que $a = -bq' + r'$ con $0 \leq r' < |b|$, es decir, $a = b(-q') + r'$ y por tanto los enteros buscados son ahora $-q'$ y r'.

Finalmente, veamos que estos tales enteros son únicos. Supongamos que $q, r, q', r' \in \mathbb{Z}$ son enteros tales que

$$a = bq + r, \quad 0 \leq r < |b|$$
$$a = bq' + r', \quad 0 \leq r' < |b|.$$

Entonces $bq + r = bq' + r'$, es decir, $b(q - q') = r' - r$, osea $b \mid r' - r$. Si $r' - r \neq 0$, por la proposición (1.2) se debe cumplir que $|b| \leq |r' - r|$. Por otro lado, se tiene que $-|b| < -r$ y $0 \leq r'$, por tanto $-|b| < r' - r$. Análogamente, $-r \leq 0$ y $r' < |b|$ implican que $r' - r < |b|$. Juntando estas dos desigualdades obtenemos que $|r' - r| < |b|$, osea $|b| < |b|$, lo cual es imposible. En consecuencia, $r' - r = 0$ y cómo $b \neq 0$ necesariamente $q - q' = 0$, es decir, $r = r'$ y $q = q'$. ∎

1.2. Máximo común divisor

Proposición 1.3 (y definición). *Si $a, b \in \mathbb{Z}$ con $a \neq 0$, entonces el conjunto*

$$D = \{c \in \mathbb{N} \ : \ c \mid a \text{ y } c \mid b\}$$

es no vacío y finito. Al elemento máximo de D se le llama máximo común divisor de a y b.

Demostración. Como 1 divide a cualquier entero, entonces $1 \in D$. Si $c \in D$ se tiene, en particular, que $c \mid a$ y como $a \neq 0$, por la proposición (1.2) se tiene que $|c| = c \leq |a|$. Luego $D \subset \{1, \ldots, |a|\}$ y por tanto D es finito por ser subconjunto de un conjunto finito. ■

Notación. Para decir que un número $d \in \mathbb{Z}$ es máximo común divisor de a y b, escribiremos $d = (a, b)$ ó $d = \text{mcd}\,\{a, b\}$.

Observación 1.1. El máximo común divisor de dos números a, b no ambos cero es único por ser el elemento máximo de un conjunto. También se sigue sin más que $(a, b) = (b, a)$.

Teorema 1.2. *Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ y sea $d = (a, b)$. Entonces el conjunto*

$$L = \{as + bt > 0 \ : \ s, t \in \mathbb{Z}\} \subset \mathbb{N}$$

es no vacío y su elemento mínimo es igual a d.

Demostración. Si $a > 0$, entonces $0 < a(1) + b(0) \in L$ y si $a < 0$ entonces $-a > 0$, de manera que $0 < a(-1) + b(0) \in L$. En cualquier caso L es no vacío. Dado que $\mathbb{N}$ está bien ordenado, L admite un elemento mínimo, sea d' este elemento y escribamos $d' = as + bt$, para algunos $s, t \in \mathbb{Z}$. Afirmamos que $d' \mid a$ y $d' \mid b$. En efecto, supongamos por ejemplo que $d' \nmid a$. Por el algoritmo de la división, existen $q, r \in \mathbb{Z}$ tales que

$$a = d'q + r \quad \text{con} \quad 0 \leq r < d'.$$

Más aún, $0 \neq r$ pues por hipótesis $d' \nmid a$, así que $0 < r$. Entonces

$$\begin{aligned} 0 < r &= a - d'q \\ &= a - (as + bt)q \\ &= a - asq - btq \\ &= a(1 - sq) + b(-tq) \in L \end{aligned}$$

lo que contradice la elección de d', así que necesariamente $d' \mid a$. Similarmente se demuestra que $d' \mid b$. Luego $d' \in D$, con D definido como en la proposición (1.3) y por tanto $d' \leq d$, pues d es el elemento máximo de D.

Por otro lado, como $d \mid a$ y $d \mid b$ por ser d un elemento de D, entonces $d \mid as + bt = d'$ en virtud del inciso (x) de la proposición (1.1), luego $d \leq d'$, pues $d' \neq 0$ y ambos d', d son mayores que cero. Se sigue finalmente que $d = d'$. ■

Observación 1.2. Si $d = (a, b)$, el teorema anterior nos permite escribir $d = as + bt$, para algunos $s, t \in \mathbb{Z}$. A los coeficientes s, t se les llama *coeficientes de Bezout* y se pueden calcular explicitamente usando, por ejemplo, el algoritmo de Euclides. Véase [9].

Proposición 1.4. *Sean $a, b \in \mathbb{Z}$ con $a \neq 0$. Si un número $d' \in \mathbb{N}$ es tal que*

(I) $d' \mid a$ *y* $d' \mid b$

(II) $c \mid a$ *y* $c \mid b \implies c \mid d'$, $\forall\ c \in \mathbb{Z}$

entonces d' es el máximo común divisor de a y b. Y recíprocamente, el máximo común divisor de a y b satisface las condiciones (i) y (ii).

Demostración. En efecto, tenemos que $d = (a, b)$ es el elemento máximo del conjunto $D = \{c \in \mathbb{N} : c \mid a \text{ y } c \mid b\}$. Por (i) se tiene que $d' \in D$, de tal manera que $d' \leq d$. Por otro lado, como $d \in D$, entonces $d \mid a$ y $d \mid b$, por tanto el inciso (ii) asegura que $d \mid d'$, luego $d \leq d'$. En consecuencia, $d = d'$.

Veamos ahora que d también satisface ambas condiciones. Como $d \in D$, entonces d satisface (i). Ahora, por el teorema (1.2), existen $s, t \in \mathbb{Z}$ tales que $d = as + bt$. Si $c \in \mathbb{Z}$ es tal que $c \mid a$ y $c \mid b$, entonces $c \mid as + bt = d$ y como $c \in \mathbb{Z}$ fue arbitrario, entonces d también cumple la condición (ii). ■

Proposición 1.5. *Si $a, b \in \mathbb{Z}$ son no ambos cero y $c \in \mathbb{Z} \setminus \{0\}$, entonces*

(I) $(a, b) = (|a|, |b|)$

(II) $(ca, cb) = |c|(a, b)$

(III) $(c, 1) = 1$.

Proposición 1.6. *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 1.1. *Si $r \in \mathbb{N}$, $e \mid r$ y $d \mid r$ con $e, r \in \mathbb{N}$, entonces*

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

1.3. Mínimo común múltiplo

Proposición 1.7 (y definición)**.** *Si $a, b \in \mathbb{Z} \setminus \{0\}$, entonces el conjunto*

$$M = \{m \in \mathbb{N} \,:\, a \mid m \text{ y } b \mid m\} \subset \mathbb{N}$$

es no vacío. Al elemento mínimo de M se le llama mínimo común múltiplo de a y b.

Demostración. Notemos que como $a, b \in \mathbb{Z} \setminus \{0\}$, entonces $1 \leq |ab|$, $a \mid |ab|$ y $b \mid |ab|$. Luego $|ab| \in M$. ■

Notación. Para indicar que $m \in \mathbb{N}$ es mínimo común múltiplo de a y b, escribiremos $m = [a, b]$ ó $m = \text{mcm}\,\{a, b\}$.

Observación 1.3. El mínimo común múltiplo de dos números a, b distintos de cero es único. Además, $[a, b] = [b, a]$.

Proposición 1.8. *Sean $a, b \in \mathbb{Z} \setminus \{0\}$. Si un número $m' \in \mathbb{N}$ es tal que*

(i) $a \mid m'$ *y* $b \mid m'$

(ii) $a \mid c$ *y* $b \mid c \implies m' \mid c, \ \forall\ c \in \mathbb{Z}$

entonces m' es el mínimo común múltiplo de a y b. Y recíprocamente, el mínimo común múltiplo satisface las condiciones (i) y (ii).

Demostración. Sea $d = [a, b]$. Por (i) se tiene que a $\mid m'$ y $b \mid m'$, entonces $m' \in M$, con M definido como en la proposición (1.7). Luego $m \leq m'$ por ser m el elemento mínimo de este conjunto. Por otro lado, como $a \mid m$ y $b \mid m$, el inciso (ii) asegura que $m' \mid m$, luego $m' \leq m$ y por tanto $m' = m$.

Además, m también satisface estas condiciones. La condición (i) se cumple por ser m un elemento de M, es decir, $a \mid m$ y $b \mid m$. Si $c \in \mathbb{Z}$ es tal que $a \mid c$ y $b \mid c$, por el algortimo de la división, existen $q, r \in \mathbb{Z}$ tales que $c = mq + r$ con $0 \leq r < m$. Como $a \mid c$ y $a \mid m$, entonces $a \mid c - mq = r$ y analogamente $b \mid r$. Si $0 < r$ esto nos llevaría a una contradicción en la elección de m, así que necesariamente $r = 0$ y por tanto $c = mq$, o lo que es lo mismo, $m \mid c$. Como $c \in \mathbb{Z}$ fue arbitrario, entonces m satisface la condición (ii). ■

Teorema 1.3. *Si $a, b \in \mathbb{Z} \setminus \{0\}$, entonces $|ab| = (a, b)[a, b]$.*

Demostración. Como $a \neq 0$, existe $d = (a, b)$. Se tiene que $d \mid a$ y $d \mid b$, por tanto, $d \mid |ab|$ y en consecuencia existe $m \in \mathbb{Z}$ tal que $|ab| = dm$. Más aún, $m \in \mathbb{N}$, pues $|ab|$ y d son enteros positivos. Afirmamos que $m = [a, b]$.

(i) Notemos que $d \mid a$ y $d \mid b$ y por tanto $d \mid |a|$ y $d \mid |b|$, por lo que existen $q_1, q_2 \in \mathbb{Z}$ tales que $|a| = dq_1$ y $|b| = dq_2$, por lo tanto, $|ab| = d^2 q_1 q_2 = dm$, lo cual implica que $dq_1 q_2 = m$ de tal manera que $|a|q_2 = m$ y $|b|q_1 = m$, es decir, $|a| \mid m$ y $|b| \mid m$, luego $a \mid m$ y $b \mid m$.

(ii) Si $c \in \mathbb{Z}$ es tal que $a \mid c$ y $b \mid c$ entonces $|a| \mid c$ y $|b| \mid c$, por tanto existen $q_1, q_2 \in \mathbb{Z}$ tales que $c = |a|q_1$ y $c = |b|q_2$. Notemos que también por el inciso anterior, $a \mid m$ y $b \mid m$, por lo que $|a| \mid m$ y $|b| \mid m$, por tanto, existen $r_1, r_2 \in \mathbb{Z}$ tales que $m = |a|r_1$ y $m = |b|r_2$. Además, como $d = (a, b) = (|a|, |b|)$, existen $s, t \in \mathbb{Z}$ tales que $d = |a|s + |b|t$, así que $dm = |a|sm + |b|tm$. Más aún $|ab| \neq 0$, pues a y b son distintos de cero, así

$$\begin{aligned}
dm = |a|sm + |b|tm &\implies |ab| = dm = |a|s|b|r_2 + |b|t|a|r_1 \\
&\implies |ab| = |ab|(sr_2 + tr_1) \\
&\implies 1 = sr_2 + tr_1 \\
&\implies c = csr_2 + ctr_1 \\
&\implies c = |b|q_2 sr_2 + |a|q_1 tr_1 \\
&\implies c = mq_2 s + mq_1 t = m(q_2 s + q_1 t) \\
&\implies m \mid c.
\end{aligned}$$

De (i) y (ii) se sigue que $m = [a, b]$ y por tanto $|ab| = (a, b)[a, b]$. ∎

1.4. Primos y factorización única

Definición 1.2. *Se dice que dos enteros a y b son **coprimos** o **primos relativos** si $(a, b) = 1$.*

Teorema 1.4 (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 $a \mid c$. ∎

Definición 1.3. *Dado $p \in \mathbb{Z}$, con $p > 1$, decimos que p es un **número primo** si tiene exactamente dos divisores positivos, 1 y p mismo.*

Corolario 1.2. *Si p es un número primo y $a \in \mathbb{Z}$ entonces*

$$(p, a) = \begin{cases} 1 & si\ p \nmid a \\ p & si\ p \mid a. \end{cases}$$

Lema 1.1. *Si $a > 1$ y $a \in \mathbb{Z}$, entonces el menor divisor positivo de a mayor que uno es un número primo.*

Demostración. Sea $A = \{m \in \mathbb{N} \,:\, m \mid a\}$. Como $a \in A$, entonces $A \neq$ vec y por tanto A tiene elemento mínimo, digamos p. Si p no fuera primo, entonces $p = qr$ para algunos $q, r \in \mathbb{Z}$ con $1 < q < p$ y $1 < r < p$. Entonces $q \mid p$, y además $p \mid a$, por tanto $q \mid a$, lo que contradice la elección de p, luego p debe de ser primo. ■

Teorema 1.5 (de factorización única)**.** *Si $a \in \mathbb{Z}$ y $a > 1$, entonces a se puede expresar como*

$$a = p_1 p_1 \cdots p_r$$

donde los p_i son números primos y $r \in \mathbb{N}$. Además, si $a = q_1 q_2 \ldots q_s$ es otra factorización de esta forma, entonces $r = s$ y existe una permutación $\sigma : \{1, 2, \ldots, r\} \longrightarrow \{1, 2, \ldots, r\}$ tal que $p_i = q_{\sigma(i)}$, $\forall\ i \in \{1, 2, \ldots, r\}$.

Demostración. [9, §I.2, pp. 23–24]. Una demostración no constructiva se puede encontrar en [6, §2.11, p. 26]. ■

Definición 1.4. *Si $n > 1$ es un entero con factorización $a = p_1 \cdots p_m$, podemos asociar primos iguales y escribirlos en orden creciente, es decir escribir a n de la forma $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, donde $0 < p_i$, $\forall\ i = 1, \ldots, s$ y $p_1 < p_2 < \cdots < p_s$. Decimos entonces que esta es la **forma estándar** o **descomposición canónica** de n como producto de primos. También decimos que un número primo tiene multiplicidad α en n si aparece α veces como factor de n.*

Teorema 1.6 (Eratóstenes)**.** *Sea $n \in \mathbb{N}$, $a > 1$. Si para cada primo tal que $p^2 \leq a$ se tiene que $p \nmid a$, entonces a es primo.*

Demostración. Sea m el menor entero mayor que 1 que divide a a. Por el lema (1.1), m debe ser un número primo. Como $m \mid a$, entonces $m \leq a$.

Supongamos que $m < a$. Como $m \mid a$, existe $q \in \mathbb{N}$ tal que $a = mq$, luego $q \mid a$. Más aún, $1 < q$, pues $m < a$ y en consecuencia $m \leq q$ por elección de m. Luego

$$m^2 \leq mq = a.$$

Luego m es un primo tal que $m^2 \leq a$ y $m \mid a$, lo que contradice la hipótesis. Por tanto debe ser que $m = a$ y como m es primo, a también lo es. ■

Corolario 1.3. *Si $a \in \mathbb{N}$ no es primo entonces existe un primo p tal que $p \leq \sqrt{a}$ y $p \mid a$.*

Teorema 1.7 (Euclides)**.** *El conjunto de números primos es infinito.*

Demostración. Supongamos lo contrario y listemos todos los primos como $p_1, \ldots, p_m$. Consideremos el entero $n = p_1 \cdots p_m + 1$. Tenemos que $n > 1$ y por tanto debe ser primo o producto de primos. Si n es primo, entonces $n = p_i$ para algún $i = 1, \ldots, m$, pero esto es imposible pues $n > p_i, \forall\, i = 1, \ldots, m$. Si n es producto de primos, entonces algún p_i lo divide, pero esto tampoco puede ser pues todos los p_i dejan residuo 1 al dividir a n, es decir, ningún primo lo divide. En consecuencia el conjunto de números primos no es finito. ■

2. Estructura del anillo de funciones aritméticas

Definición 2.1. *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 2.2. (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 2.3. (Función de Möbius)**.** *La función* μ *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*

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

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

Definición 2.4. *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) $fg = gf$.

2.1. Convolución de Dirichlet

Definición 2.5. (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 2.1. *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 2.2. *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 2.1. *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 (2.2). ■

Definición 2.6. (Función identidad)**.** *Definimos a la función identidad I como*

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

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 2.2. *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

$$((f * g) * h)(n) = \sum_{i=1}^{k} \sum_{j=1}^{m_i} f(c_{i,j})g(c_{i,m_i+1-j})h(d_{k+1-i}) \tag{2.1}$$

y

$$(f * (g * h))(n) = \sum_{i=1}^{k} \sum_{j=1}^{m_{k+1-i}} f(d_i)g(c_{m_{k+1-i},j})h(c_{m_{k+1-i},m_{k+1-i}+1-j}). \tag{2.2}$$

Definamos los conjuntos

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

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

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 $c_{i,j}c_{i,m_i+1-j}d_{k+1-i} = d_i d_{k+1-i} = n$, aplicando dos veces el lema (2.2). 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 (2.2), 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 (2.1) y (2.2) 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 (2.1) 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

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

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

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

■

2.2. Una norma para funciones aritméticas

Definición 2.7. *Sea $\mathcal{A}$ el conjunto de todas las funciones aritméticas. Definimos la función*

$$\begin{aligned} \mathcal{N} : \mathcal{A} &\longrightarrow \mathbb{N} \cup \{0\} \\ f &\longmapsto \mathcal{N}(f) = \begin{cases} 0 & \text{si } f = \mathbf{0} \\ \min\{n : f(n) \neq 0\} & \text{si } f \neq \mathbf{0}. \end{cases} \end{aligned}$$

Proposición 2.3. *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) $\min\{\mathcal{N}(f), \mathcal{N}(g)\} \leq \mathcal{N}(f + g), \forall\, f, g \in \mathcal{A}$.

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

Demostración. (i) Si $f = 0$ por definición se tiene que $\mathcal{N}(f) = 0$. Si $f \neq 0$, entonces $\min\{n : f(n) \neq 0\} \neq 0$, 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 $ab = \min\{n : (f * g)(n) \neq 0\} = m$.

En efecto, se tiene

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

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

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 mín$\{a, b\} = a$. Si $n < a$ entonces $(f + g)(n) = f(n) + g(n) = 0$, por lo que

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

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

■

Teorema 2.1. *$\mathcal{A}$ 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 2.1. 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 2.4. *$f \in \mathcal{A}^*$ si y sólo si $\mathcal{N}(f) = 1$.*

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

$$f^{-1}(1) = \frac{1}{f(1)}$$
$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d\neq n}} f\left(\frac{n}{d}\right) f^{-1}(d), \quad n > 1. \tag{2.3}$$

Es fácil verificar que la ecuación (2.3) define a f^{-1} de tal forma que $f * f^{-1} = I$, pues $f(1)f^{-1}(1) = 1$ y si $n > 1$ entonces

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

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 2.5. *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 2.2 (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 2.6. *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 $1 = g_2$, 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 2.2. 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 $1 = p_2$, 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 2.2. 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 2.3. *$\mathcal{A}$ 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 [3, 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 [8]. 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 2.1. *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 2.7. *$\mathcal{A}$ 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 [7, §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 2.4. *$\mathcal{A}$ es un anillo local.*

Demostración. Por [7, §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 2.8. *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, entonces se tendría que $g(1) = 0$ y $f(1) = 0$, por tanto, $f(1) = (g * h)(1) = g(1)h(p) + g(p)h(1) = 0$, 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 2.1 es el siguiente.

Corolario 2.2. *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 2.9. *$\mathcal{A}$ 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. ■

2.3. Funciones multiplicativas

Definición 2.8. (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 2.2. 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 2.3. *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 2.4. *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 2.5. *$(\mathcal{M}, *)$ 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

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

por el Lema 2.4.

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 2.3. *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. ■

2.4. 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 2.5. $(\mathcal{A}_{\mathbb{R}}, +) \cong (P, *)$.

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 2.10. *$f \in \mathcal{M}$ 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

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

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

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

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

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

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

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 ϕ 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 ϕ 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 ϕ 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 2.8. $(\mathcal{A}_{\mathbb{R}}, +) \cong (\mathcal{A}_1, +)$, *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 ψ 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 ψ 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, ψ 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 2.9. $(\mathcal{A}_{\mathbb{R}}, +) \cong (\mathcal{A}, +)$.

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 γ 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 γ 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 γ 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 2.5, 2.6, 2.7, 2.8 y 2.9.

Teorema 2.6. *Los grupos* $(\mathcal{A}_{\mathbb{R}}, +)$, $(P, *)$, $(\mathcal{M}, *)$, $(\mathcal{A}', +)$, $(\mathcal{A}_1, +)$ *y* $(\mathcal{A}, +)$ *son todos isomorfos.*

2.5. Algunas funciones aritméticas conocidas

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

Definición 2.9. (Función idéntica)**.** *La función idéntica N es tal que $N(n) = n$, para cada $n \in \mathbb{N}$.*

Definición 2.10. (Función φ de Euler)**.** *Para cada $n \geq 1$, se define la función φ de Euler $\varphi(n)$ como el número de enteros positivos no mayores a que n que son primos relativos a n.*

Definición 2.11. (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 2.12. (Función de Liouville)**.** *Se define a la función λ 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 2.13. (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 σ en vez de σ_1. La función divisor de orden 0 se denomina función número de divisores.

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:

Definición 2.14. *Sean f una función aritmética, $n \in \mathbb{N}$ y $d_1, d_2, \cdots, d_k$ todos los divisores positivos de n. Definimos*

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

Se tienen las siguientes propiedades básicas de algunas funciones aritméticas.

Proposición 2.11. *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 [2]. 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 2.4 (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 2.12 (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 [5]. 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 μ es primo relativo a M y ν 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 μ y φ al sumar sobre los divisores de un entero positivo. El siguiente lema será útil para probar dicha relación.

Lema 2.10. *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 2.13. *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 (2.10) 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

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

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

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

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

■

3. 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 considerarán dos clases de funciones aritméticas que capturan esta noción y se probará que son equivalentes. También se expondran resultados análogos a los de análisis respecto a funciones periódicas.

Observación 3.1. Durante todo el capítulo se supondrá que r es un entero positivo arbitrario pero fijo.

Definición 3.1. (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 3.2. (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 3.1. *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 $(m,r) \mid r$, entonces $(m,r) \mid n + qr = m$, luego $(n,r) \mid (m,r)$. Análogamente, se tiene que $(m,r) \mid m$ y $(m,r) \mid r$, por lo que $(m,r) \mid m - qr = n$, luego $(m,r) \mid (n,r)$. Se sigue que $(n,r) = (m,r)$ y por tanto $f(n) = f((n,r)) = f((m,r)) = f(m)$. ∎

3.1. Sumas de Ramanujan

Definición 3.3. (Sumas de Ramanujan)**.** *Se define la función aritmética* c_r *como*

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

Esta función será referida como la suma de Ramanujan módulo r *o simplemente suma de Ramanujan cuando no haya riesgo de confusión.*

Proposición 3.2. *Algunas propiedades de la sumas de Ramanujan son las siguientes:*

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

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

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

(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 $\mu(p^i) = 0$.

■

Del la demostración del punto 4 se puede rescatar el siguiente corolario, usando la inversión de Möbius (corolario 2.4).

Corolario 3.1. *Para cada $n \in \mathbb{N}$ fijo se tiene*

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

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

Lema 3.1. *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

$$\begin{aligned}
\sum_{d|k} c_r(k/d)c_d(k/s) &= \sum_{d|k} c_d(k/s) \sum_{d'|(k/d,r)} \mu(r/d')d' \\
&= \sum_{d|k} c_d(k/s) \sum_{\substack{d'|r \\ d'|k/d}} \mu(r/d')d' \\
&= \sum_{\substack{d|k \\ d'|r \\ d'|k/d}} c_d(k/s)\mu(r/d')d' \\
&= \sum_{\substack{d|k/d' \\ d'|r \\ d'|r}} c_d(k/s)\mu(r/d')d' \\
&= \sum_{\substack{d'|r \\ d'|k}} \mu(r/d')d' \sum_{d|k/d'} c_d(k/s) \\
&= \sum_{d'|(k,r)} \mu(r/d)d'\eta_{k/d'}(k/s), \text{ por el corolario anterior} \\
&= \sum_{d'|r} \mu(r/d)d'\eta_{k/d'}(k/s), \qquad (3.1)
\end{aligned}$$

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 (3.1) 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 (3.1) 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 $s \mid d'$. ∎

Lema 3.2. *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 3.2. *La suma de Ramanujan módulo r es par* mód r.

El lema anterior permite probar uno de los resultados importantes de este capítulo, el cuál establece la existencia de una expansión finita de cualquier función par mód r, con sumas de Ramanujan como coeficientes.

Teorema 3.1. *Toda función f par* mód r *tiene una expansión de la forma*

$$f(n) = \sum_{d|r} \alpha(d) c_n(n), \tag{3.2}$$

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

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

o por la fórmula equivalente,

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

donde ϕ es la función phi de Euler.

Demostración. Es claro que toda función de la forma (3.2) 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 Lema 3.1, 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 2.12 se puede rescatar el hecho de que el conjunto $\{1, 2, \ldots, r\}$ es igual a $\bigcup_{e|r} \{rx/e \,:\, (x,e) = 1, 1 \leq x \leq e\}$ y todos

los conjuntos son disjuntos a pares, por tanto

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

por ser f par mód r. Además $(rx/e, r) = r/e$, pues $(x, e) = 1$ implica que $(r/e)(x, e) = r/e$, y como r/e es un entero positivo, entonces $(rx/e, r) = r/e$. Y la penúltima igualdad se cumple por el `cor:mcd1` y la fórmula de Hölder. ■

Bibliografía

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

[2] Brualdi, R. A. *Introductory Combinatorics*, 3 ed. Prentice-Hall, 1999.

[3] Cashwell, E. D., and Everett, C. J. The ring of number-theoretic functions. *Pacific Journal of Mathematics 9*, 4 (1959).

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

[5] Gauss, C. F. *Disquisitiones Arithmeticae*, english ed. Springer-Verlag, 1966.

[6] Hardy, G. H., and Wright, E. M. *An Introduction to the Theory of Numbers*, 5 ed. Oxford University Press, 1979.

[7] Hungerford, T. W. *Algebra*. Springer, 1974.

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

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