# 1. 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. Estos resultados se puede encontrar en [5].

*Observación 1.1.* Durante todo el capítulo se supondrá que $r$ es un entero positivo arbitrario pero fijo.

**Definición 1.1.** (Función par)**.** Una función aritmética se dice **par** $\text{mód } r$ 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 1.2.** (Función periódica)**.** Una función aritmética se dice **periódica** con periodo $r$ (o periódica $\text{mód } r$) 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 1.1.** *Toda función par* $\text{mód } r$ *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 $(m,r) \mid m$ 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 $f(n) = f((n,r)) = f((m,r)) = f(m)$. ■

## 1.1. Sumas de Ramanujan

**Definición 1.3.** (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 1.2.** *Algunas propiedades de la sumas de Ramanujan son las siguientes:*

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

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

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

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

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

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

*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

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

(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

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

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

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

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

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

- 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

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

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 1.1.** *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 1.1.** *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

$$\begin{aligned}
\sum_{d|k} c_r(k/d)c_d(k/s) &= \sum_{d|k} c_d(k/s) \sum_{d'|(k/d,r)} \mu(r/d')d' \\
&= \sum_{d|k} c_d(k/s) \sum_{\substack{d'|r \\ d'|k/d}} \mu(r/d')d' \\
&= \sum_{\substack{d|k \\ d'|r \\ d'|k/d}} c_d(k/s)\mu(r/d')d' \\
&= \sum_{\substack{d|k/d' \\ d'|r \\ d'|r}} c_d(k/s)\mu(r/d')d' \\
&= \sum_{\substack{d'|r \\ d'|k}} \mu(r/d')d' \sum_{d|k/d'} c_d(k/s) \\
&= \sum_{d'|(k,r)} \mu(r/d)d'\eta_{k/d'}(k/s), \text{por el corolario anterior} \\
&= \sum_{d'|r} \mu(r/d)d'\eta_{k/d'}(k/s), \qquad (1.1)
\end{aligned}$$

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 (1.1) 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 (1.1) es igual a

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

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

**Lema 1.2.** *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

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

■

**Corolario 1.2.** *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. Para probarlo serán necesarios algunos resultados preliminares.

**Definición 1.4**. (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 1.5.** Una función aritmética $f$ se dirá *separable* si $f(n) = f(n_*)$, para cada $n \in \mathbb{N}$.

**Lema 1.3.** *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,

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

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

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

es decir, $f$ es separable.

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

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

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 1.4.** *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 $i = \text{mín}\{m, n\}$. 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,

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

(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

$$\left(\frac{a_*}{(a,b)_*}, b\right) = 1. \tag{1.2}$$

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 (1.2), se tiene que

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

Finalmente,

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

■

*Ejemplo 1.1.* 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 1.5** (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

$$c_r(n) = \sum_{d|(n,r)} \mu\left(\frac{r}{d}\right) d = \sum_{\substack{d|(n,r)\\ \left(\frac{r}{(n,r)},\frac{(n,r)}{d}\right)>1}} \mu\left(\frac{r}{d}\right) d + \sum_{\substack{d|(n,r)\\ \left(\frac{r}{(n,r)},\frac{(n,r)}{d}\right)=1}} \mu\left(\frac{r}{d}\right) d, \tag{1.3}$$

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 $r = p^2dq_1q_2$ y por tanto $p^2 \mid r/d$, así que $\mu(r/d) = 0$. Luego la ecuación (1.3) es igual a

$$\begin{aligned}
\sum_{\substack{d|(n,r)\\ \left(\frac{r}{(n,r)},\frac{(n,r)}{d}\right)=1}} \mu\left(\frac{r}{d}\right) d &= \sum_{\substack{d|(n,r)\\ \left(\frac{r}{(n,r)},\frac{(n,r)}{d}\right)=1}} \mu\left(\frac{r}{(n,r)}\right)\mu\left(\frac{(n,r)}{d}\right) d \\
&= \mu\left(\frac{r}{(n,r)}\right) \sum_{\substack{d|(n,r)\\ \left(\frac{r}{(n,r)},\frac{(n,r)}{d}\right)=1}} \mu\left(\frac{(n,r)}{d}\right) d \\
&= \mu\left(\frac{r}{(n,r)}\right) \sum_{\substack{d|(n,r)\\ \left(\frac{r}{(n,r)},d\right)=1}} \mu(d)\frac{(n,r)}{d} \\
&= (n,r)\mu\left(\frac{r}{(n,r)}\right) \sum_{\substack{d|(n,r)\\ \left(\frac{r}{(n,r),d}=1\right)}} \frac{\mu(d)}{d}
\end{aligned} \tag{1.4}$$

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

$$\begin{aligned}
\Phi(s) = \sum_{d|s} \mu(d)\overline{\varphi}\left(\frac{s}{d}\right) &= \sum_{d|s} \mu(d)\varphi\left(\frac{s}{d}\right)\frac{1}{s/d} = \sum_{d|s}\mu(d)\sum_{e|s/d}\mu(e)\frac{s/d}{e}\frac{1}{s/d} \\
&= \sum_{d|s}\mu(d)\sum_{e|s/d}\frac{\mu(e)}{e} = \sum_{e|s}\frac{\mu(e)}{e}\sum_{d|s/e}\mu(d) = \frac{\mu(s)}{s}
\end{aligned} \tag{1.5}$$

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 (1.4) es igual a

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

donde la primera igualdad se cumple por definición de $\Phi$ y la ecuación (1.5), la segunda por ser $\overline{\varphi}$ multiplicativa, separable y por el Lema 1.4 (II), la tercera por el Lema 1.4 (I) y la quinta por definición de $\overline{\varphi}$. ■

**Teorema 1.1.** *Toda función $f$ par* mód $r$ *tiene una expansión de la forma*

$$f(n) = \sum_{d|r}\alpha(d)c_n(n), \tag{1.6}$$

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

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

*o por la fórmula equivalente,*

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

*donde $\phi$ es la función phi de Euler.*

*Demostración.* Es claro que toda función de la forma (1.6) 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 Lema 1.1, 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 **??** se puede rescatar el hecho de que el conjunto $\{1, 2, \dots, r\}$ 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

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

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 **??** y la fórmula de Hölder (Lema 1.5). ■

# Bibliografía


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

[2] 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.

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

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

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

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

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

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

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

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

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