Introducción a las funciones multiplicativas

PRIMERA PARTE:

Funciones aritméticas

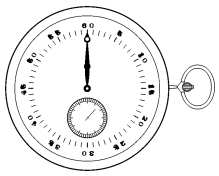
Jaime Rangel Mondragón

Facultad de Informática, UAQ
Centro Universitario,
Cerro de las Campanas s/n,
76010 Querétaro, Qro.
jrangel@sunserver.uaq.mx

RECIBIDO: *noviembre de 1999*
ACEPTADO: *agosto del 2000*

I. Introducción

La teoría de números es una rama de las matemáticas que estudia las propiedades de los enteros positivos $1, 2, 3, \ldots$ o números naturales (Schroeder, 1990). Dichos números constituyeron el primer descubrimiento matemático y el interés en ellos es tan antiguo como la misma civilización. Los retos intelectuales de los problemas de la teoría de números han atraído a matemáticos notables desde el tiempo de Pitágoras (*c.* 540 a.C.) y el trabajo realizado en la búsqueda de soluciones a dichos problemas ha resultado en la creación de nuevas ramas de las matemáticas. El desarrollo de las computadoras y las comunicaciones digitales ha mostrado que la teoría de números es capaz de dar respuestas inesperadas a problemas de aplicación práctica (Hardy y Wright, 1984). En esta serie de cuatro artículos presentaremos una introducción a las funciones multiplicativas, de relevancia en teoría de números y computación, haciendo énfasis en este último aspecto con el fin de presentar las bases matemáticas a estudiantes de esta última disciplina. Una de las aplicaciones de las funciones multiplicativas lo constituye el diseño de esquemas criptográficos modernos de clave pública, a los cuales



dedicaremos la última parte de este trabajo. Por otra parte, el uso de lenguajes simbólicos ha estimulado la aplicación de técnicas computacionales a problemas de teoría de números; en este trabajo ilustraremos dichas técnicas bajo el paradigma moderno de programación funcional mostrando la puesta en práctica de los diferentes algorítmos pertinentes a nuestro tema. Nuestro material presupone solamente un conocimiento básico de la notación y nociones de teoría de números, provenientes de un curso introductorio de matemáticas discretas, así como nociones elementales de programación funcional.

II. Funciones aritméticas

Funciones $f(n)$ del entero positivo n que expresan alguna propiedad aritmética de n son llamadas funciones aritméticas (McCarthy, 1986).

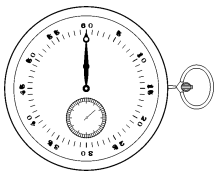
Definición 1. Cualquier función $f\colon Z^+ \to N$ del conjunto de los enteros positivos al conjunto de números naturales se denomina *función aritmética*.

Ejemplo 1. Una función aritmética de gran interés es $r(n)$, el número de formas en las que n puede ser escrito como suma de los cuadrados de dos enteros (Rademacher, 1964). Por ejemplo, existen cuatro formas de escribir el número 1 como suma de dos cuadrados:

$$1 = 1^2 + 0^2 = (-1)^2 + 0^2 = 0^2 + 1^2 = 0^2 + (-1)^2,$$

es decir, $r(1) = 4$. La secuencia de valores de r empieza como 4, 4, 0, 4, 8, 0, etc. Todos los números en esta sucesión son múltiplos de 4, pues de una expresión que utilice sólo enteros positivos siempre podemos obtener otras tres utilizando los negativos correspondientes.

Si p es un divisor primo de n con $p \equiv 3 (\mathrm{mod}\, 4)$ y si p^k es la mayor potencia de p que divide a n, Euler demostró que n es la suma de dos cuadrados si y sólo si k es par para cada divisor primo p. Existe un número infinito de tales n, siendo los primeros 3, 6, 7, 11, 12, 14, 15, 19, etc. (Hardy y Wright, 1984).



Ejemplo 2. Algunas funciones aritméticas son descritas dando dos valores $f(1)$ y $f(2)$ y expresando $f(n)$ para $n > 2$ en términos de $f(n-1)$ y $f(n-2)$. Por ejemplo, los llamados *números de Fibonacci* se definen como:

$$f(1) = f(2) = 1 \qquad \text{y} \qquad f(n) = f(n-1) + f(n-2) \qquad \text{para } n > 2.$$

En este caso particular los valores $f(n)$ se escriben simplemente como F_n.

Los primeros términos son 1, 1, 2, 3, 5, 8, 13, 21, 34, 55.

Estos números poseen muchas propiedades fascinantes. Por ejemplo,

$$F_{2n+1} = 1 + F_2 + F_4 + F_6 + \cdots + F_{2n}$$

y la n-ésima potencia de la matriz

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{es} \quad A^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \quad \text{para } n > 1.$$

La relación $(-1)^n = F_{n+1}F_{n-1} - F_n^2$ se obtiene de esta ecuación tomando determinantes en ambos miembros (Graham *et al.*, 1989; Knuth, 1981).

Los números de Fibonacci poseen también la propiedad de divisibilidad siguiente:

$$n|m \quad \Rightarrow \quad F_n|F_m.$$

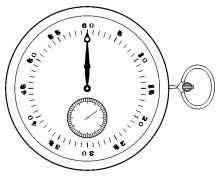
Por ejemplo, $F_8|F_{16}$ puesto que $8|16$.

Antes de mostrar ejemplos para ilustrar nuestro tema, consideremos la siguiente notación, que será utilizada extensamente:

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

Esta notación expresa la suma de la evaluación de una función aritmética f sobre todos los divisores positivos del entero n. En sí misma esta notación describe un funcional aritmético $F(n)$, aunque, a primera vista, de apariencia no muy natural. En nuestro contexto, esta sumatoria desempeñará un papel análogo al del símbolo curvilíneo empleado en el cálculo integral y cuya familiaridad ayuda a expresar de manera concisa y natural resultados importantes. En general, la condición en la sumatoria la hace totalmente diferente a una suma común sobre un rango secuencial. Notemos que, en el caso de n primo, $F(n)$ se reduce al valor $1 + n$, pero es difícil encontrar expresiones explícitas para casos más generales. A continuación mostraremos las propiedades asociadas con el uso de esta notación para definir funciones específicas. La habilidad para entender y manipular este concepto encontrará aplicaciones importantes.

La familia de aquellas funciones que puedan expresarse siguiendo esta notación, aplicada a alguna función aritmética f, formará parte importante de nuestro estudio y la denominaremos *adenda*, y sus elementos serán *adendum*.



En todo nuestro trabajo nos limitaremos al dominio de los números enteros positivos, excepto cuando indiquemos explícitamente lo contrario, y nos referiremos sólo como números a elementos de este conjunto.

Ejemplo 3. La función $d(n)$, igual al número de divisores positivos de n, y la función $\sigma(n)$, igual a la suma de éstos, son ejemplos de adenda prominentes. Esto proviene de las identidades:

$$d(n) = \sum_{d|n} 1, \qquad \sigma(n) = \sum_{d|n} d.$$

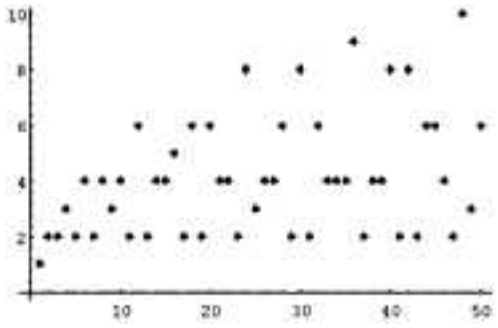


FIGURA 1. Comportamiento del adendum d.

Los primeros valores de d son 1, 2, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6, 2, 4, 4, 5, 2, 6 (figura 1) y los de σ son 1, 3, 4, 7, 6, 12, 8, 15, 13, 18, 12, 28, 14, 24, 24, 31, 18, 39 (figura 2).

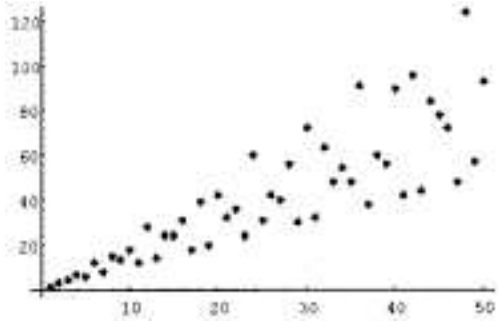
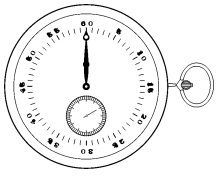


FIGURA 2. Comportamiento del adendum σ.



De las figuras 1 y 2 notamos que su comportamiento es irregular, pues los valores sucesivos difieren apreciablemente. Este comportamiento es típico de la familia de funciones aritméticas.

III. Funciones multiplicativas

Una subfamilia de las funciones aritméticas la forman las llamadas *funciones multiplicativas* (Apostol, 1971) definidas a continuación. Denotaremos al máximo común divisor de n y m como (n, m).

Definición 2. Si f es una función aritmética no nula tal que la siguiente propiedad se cumple:

$$(n, m) = 1 \quad \Rightarrow \quad f(nm) = f(n)f(m),$$

entonces se dirá que f es *multiplicativa*. La familia de tales funciones se denotará por M.

Notemos la unidireccionalidad de la definición anterior: para la función multiplicativa $f(n) = 1$, la condición $f(nm) = f(n)f(m) \Rightarrow (n, m) = 1$ es falsa. Aquellos adenda en M serán de gran interés para nosotros. Dos de sus miembros fueron mostrados en el ejemplo 3. Un ejemplo adicional importante es el siguiente:

Ejemplo 4. Consideremos la *función de Euler* $\varphi(n)$, que calcula el número de enteros positivos que son primos relativos a n, $\varphi(n) = \sum_{(d,n)=1} 1$. Sus primeros valores son: 1, 1, 2, 2, 4, 2, 6, 4, 6 (figura 3).

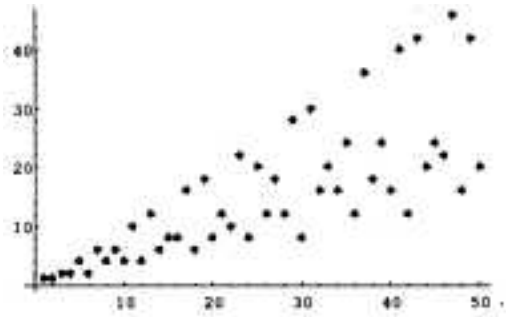
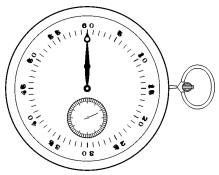


FIGURA 3. Comportamiento del adendum φ.

Ejemplo 5. Una de las más importantes funciones aritméticas es la función $p(n)$, que cuenta el número de formas en las que n puede ser escrito como la suma de números naturales que no excedan n. Por ejemplo, $p(5) = 7$, puesto que existen 7 particiones del 5 dadas por:



$$5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1.$$

En este conteo, el número de sumandos es libre, se permite la repetición y el orden de los sumandos es importante.

Euler demostró que el recíproco del producto infinito

$$\varphi(x) = \prod_{m=1}^{\infty} (1 - x^m)$$

es una función generadora para $p(n)$ (véase Graham *et al.*, 1989):

$$\frac{1}{\varphi(x)} = \sum_{n=0}^{\infty} p(n)x^n,$$

donde $p(0) = 1$. Euler demostró también que

$$\varphi(x) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \cdots,$$

donde los exponentes 1, 2, 5, 7, 12, 15 ... son los llamados *números pentagonales*, los cuales pueden derivarse de las expresiones $(3k^2 - k)/2$ y $(3k^2 + k)/2$, tomando $k = 1, 2, 3$, etc.

Multiplicando la serie de potencias de $\varphi(x)$ por aquélla de su recíproco, Euler obtuvo la siguiente fórmula recursiva para el cálculo de $p(n)$:

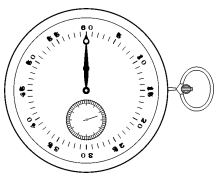
$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + \cdots,$$

donde $p(k) = 0$ si $k < 0$.

Ejemplo 6. Sea $S(n)$ la suma de todos los números menores que n y primos relativos a él. Entonces:

$$S(n) = \sum_{\substack{1 \le i \le n \\ (i,n)=1}} i = \frac{n\varphi(n)}{2} \notin M.$$

Esta función es estrictamente creciente y sus primeros valores son: 1, 1, 3, 4, 10, 6, 21, 16, 27, 20, 55 (figura 4). Éste es nuestro primer ejemplo de una función aritmética que no es multiplicativa, pues $S(6) \neq S(2)S(3)$. Su tendencia cuadrática proviene del hecho de que $S(n) = n(n-1)/2$ para valores primos de n.



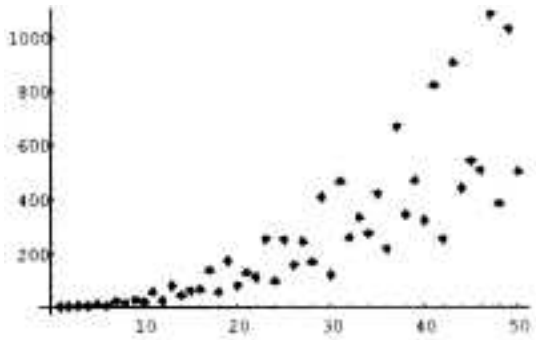


FIGURA 4. Comportamiento del adendum no multiplicativo $S(n)$.

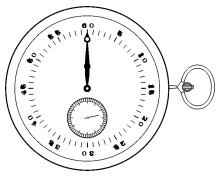
IV. PROPIEDADES BÁSICAS

Justifiquemos la importancia de φ demostrando su clasificación (Hardy y Wright, 1984).

Teorema 1. $\varphi \in M$.

Demostración: Sea $P(n) = \{i \in Z^+ | (i,n) = 1\}$, sea $n = ab$, con $(a,b) = 1$ y supongamos que $x \in U_n$. Entonces $(x,a) = (x,b) = 1$ y $(x \bmod a, a) = (x \bmod b, b) = 1$ (debido al resultado: $u \equiv v \bmod w \;\Rightarrow\; (u,w) = (v,w)$). Entonces la función $f: U_n \to U_a \times U_b$ dada por $f(x) = (x \bmod a, x \bmod b)$ está bien definida. Afirmamos que es biyectiva. Por el principio del palomar, es suficiente probar que es suprayectiva. Supongamos que tenemos un par $(i,j) \in U_a \times U_b$. Por el *Teorema chino del residuo* (Hardy y Wright, 1984) podemos encontrar una única x, tal que $x \equiv i \bmod a$ y $x \equiv j \bmod b$, puesto que $(a,b) = 1$. Como $(a,b) = 1$, podemos utilizar el algoritmo de Euclides y podemos encontrar dos números α y β, tales que $a\alpha + b\beta = 1$. Entonces $x = a\alpha j + b\beta i \bmod n$. Esta correspondencia nos permite concluir que $|U_n| = |U_a||U_b|$, es decir, $\varphi(a,b) = \varphi(a)\varphi(b)$. ■

Para ilustrar el teorema anterior supongamos que $a = 14$ y $b = 15$, es decir, $n = 210$. Consideremos $x = 173$. De acuerdo a la construcción anterior, $f(173) = (173 \bmod 14, 173 \bmod 15) = (5,8)$. Inversamente, consideremos el par $(i,j) = (11,13)$. Por el algoritmo de Euclides $14(-1) + 15(1) = 1$, es decir, $x = 14(-1)13 + 15(1)11 \bmod 210 = 193$. La tabla 1 muestra la distribución de los 48 primos relativos a 210 de acuerdo a sus parejas (i,j).



Es sencillo demostrar que si $f \in M$, entonces necesariamente $f(1) = 1$. Más generalmente, utilizando inducción matemática es posible demostrar que, para cualquier conjunto de números $n_1, n_2, \ldots, n_r$ primos relativos por

Tabla 1.

	1	3	5	9	11	13
1	1	31	61	121	151	209
2	197	17	47	107	137	13
4	169	199	19	79	109	41
7	127	157	187	37	67	83
8	113	143	173	23	53	97
11	71	101	131	191	11	139
13	43	73	103	163	193	167
14	29	59	89	149	179	181

pares, la siguiente propiedad se cumple:

$$f(n_1 n_2 \cdots n_r) = f(n_1) f(n_2) \cdots f(n_r).$$

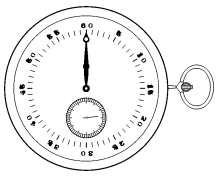
En particular, eligiendo $n_1, n_2, \ldots, n_r$ potencias de primos distintos, concluímos que, descomponiendo a n en su factorización canónica, el valor de cualquier función multiplicativa en n está determinado únicamente por su valor en todas las potencias de primos, como lo muestra el siguiente ejemplo.

Ejemplo 7. Supongamos que se desea construir una función multiplicativa f tal que para cada primo p y potencia m se cumpla $f(p^m) = p^{3m}$. Entonces, si la factorización canónica de n hace corresponder la potencia a_i al primo p_i, tendremos las siguientes ecuaciones:

$$f(n) = f\left(\prod_i p_i^{a_i}\right) = \prod_i f\left(p_i^{a_i}\right) = \prod_i p_i^{3a_i} = \left[\prod_i p_i^{a_i}\right]^3 = n^3.$$

Es decir que estamos forzados a concluir que $f(n) = n^3$ para todo número n. Podemos observar también que todas aquellas funciones de la forma $g(n) = n^m$ para alguna potencia $m \geq 0$ son multiplicativas.

La situación anterior plantea la existencia de limitaciones en la libertad de definición de una función multiplicativa para potencias de primos. Los límites de esta libertad pueden ser explorados aplicando la función a productos de enteros que no sean primos relativos. La figura 5 despliega aquellos pares (n, m) para los que una función multiplicativa f podría no cumplir $f(nm) = f(n)f(m)$. Notemos que este incumplimiento no altera en absoluto el carácter multiplicativo de f. Para todos los 345 pares mostrados en la figura 5, d, σ y φ no cumplen la propiedad multiplicativa sin restricciones. En contraste, la función $f(n) = 1$ es multiplicativa, pero extiende



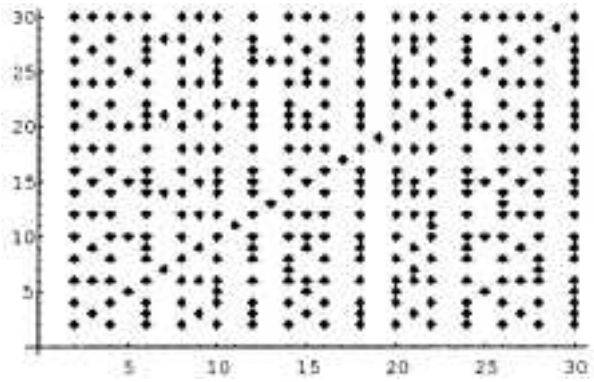


FIGURA 5. Parejas de números que no son primos relativos.

la propiedad de multiplicidad a todos estos puntos. Estos ejemplos sugieren que la categoría de las funciones multiplicativas puede subdividirse en categorías importantes y en el transcurso de este trabajo lo confirmaremos.

Ejemplo 8. El comportamiento para potencias de primos de las funciones vistas anteriormente se muestra a continuación:

$d(p^\alpha) = \alpha+1$, puesto que el conjunto de divisores de p^α es $\{1, p, p^2, \ldots, p^\alpha\}$.

$\sigma(p^\alpha) = \dfrac{p^{\alpha+1}-1}{p-1}$, ya que $\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha$.

$\varphi(p^\alpha) = p^\alpha\left(1-\dfrac{1}{p}\right)$, debido a que todos los números menores que p^α, excluyendo potencias de p, son primos relativos a p^α.

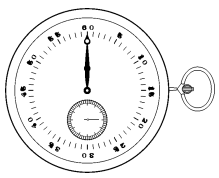
A partir de la última identidad podemos concluir que:

$$\varphi(n) \quad \text{siempre es par, excepto para} \quad n = 2.$$

Un resultado similar para $d(n)$ es el siguiente:

$$d(n) \quad \text{impar} \quad \Rightarrow \quad n \quad \text{debe ser un cuadrado.}$$

Más aún, $\prod_{d|n} d = n^{d(n)/2}$, como podemos deducir a partir de las siguientes igualdades:



$$\prod_{d|n} d = \prod_{d|n} \frac{n}{d} = n^{d(n)} \prod_{d|n} \frac{1}{d} \quad \Rightarrow \quad \left[\prod_{d|n} d\right]^2 = n^{d(n)}.$$

Veamos ahora cómo promover una función aritmética f a una multiplicativa a partir de su comportamiento para potencias de primos. Desde el punto de vista teórico, es suficiente con imponer la propiedad multiplicativa; por ejemplo, $f(1234567890) = f(2)f(5)f(9)f(3607)f(3803)$. En general, la sucesión de valores de f es:

$$1, f[2], f[3], f[4], f[5], f[2]f[3], f[7], f[8], f[9], f[2]f[5], f[11], f[3]f[4], f[13], \ldots$$

En el caso de la función $d(n)$ dichos valores serán:

$$d[1], 2, 2, 3, 2, d[6], 2, 4, 3, d[10], 2, d[12], 2, \ldots$$

y esta función se extendería a:

$$1, 2, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6, 2, \ldots$$

De manera similar, para $\sigma(n)$ ésta correspondería a la sucesión:

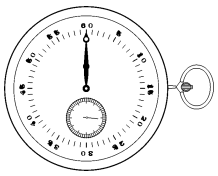
$$1, 3, 4, 7, 6, 12, 8, 15, 13, 18, 12, 28, 14, 24, 24, 31, 18, 39, 20, \ldots$$

Finalmente, para la función de Euler:

$$1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4, 12, 6, 8, 8, 16, 6, 18, 8, 12, 10, 22, \ldots$$

V. ¿Es φ un adendum?

Revisando la definición de $\varphi(n)$, es natural preguntarse si es en realidad un adendum, puesto que en su definición la suma evita correr sobre los divisores de n. Nuestra intuición nos dice que debemos considerar a los adenda como un subconjunto propio de las funciones aritméticas que a su vez contienen propiamente a las multiplicativas. Hasta ahora hemos demostrado que φ es multiplicativa; si resultara no ser un adendum, nuestras expectativas estarían fuera de lugar. Por fortuna, la respuesta que da título a esta sección es afirmativa. Supongamos que encontramos una función $f \in M$ con el siguiente comportamiento en primos:



$$f(p) = p - 2$$

$$f(p^\alpha) = p^\alpha \left[1 - \frac{1}{p}\right]^2, \qquad \alpha > 1.$$

Es sencillo demostrar que esta función es la que necesitamos para obtener $\varphi(n)$ como una sumatoria de divisores de n, pero ¿cómo podríamos encontrarla? Comencemos por notar que, dada una función $F(n) = \sum_{d|n} f(d)$, la función f está determinada unívocamente. Por ejemplo, necesariamente $f(1) = F(1)$ y $f(1) + f(2) = F(2)$, es decir, $f(2) = F(2) - F(1)$. Así, como $f(n) = F(n) - \sum_{\substack{d|n \\ d<n}} f(d)$, este hecho puede demostrarse fácilmente utilizando inducción matemática. Esta observación sugiere una serie de teoremas de inversión que veremos en secciones posteriores.

Programemos una función computacional `getf` tal que, dada la secuencia $\{F(1), F(2) \ldots, F(n)\}$, calcule la secuencia correspondiente $\{f(1), f(2) \ldots, f(n)\}$ y, en este proceso, ilustre la siguiente afirmación:

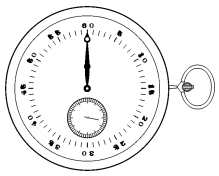
Todas las funciones aritméticas son adenda, es decir, $F \in A \;\Rightarrow\; \exists f \ni F(n) = \sum_{d|n} f(d)$.

La función `getf` pone en práctica la inversa de la transformación que nos permite construir F a partir de f y su programación nos permitirá la verificación y la manipulación de nuestros resultados. El siguiente segmento está programado en el lenguaje funcional *Mathematica* (Wolfram, 1991; Maeder, 1991), lo que permite establecer esta implementación de manera concisa. Dada la lista F, ésta genera el vector f de manera análoga a como se obtuvo $f(2)$ anteriormente:

```
getf[F_List]:=Module[{f={F[[1]]}, n, s},
    Do[s=Apply[Plus,
      f[[Select[Range[1,n-1],Mod[n,#]==0^]]]];
      AppendTo[f, F[[n]]-s], {n,2,Length[F]}];
    f]
```

A continuación haremos uso de esta función en identidades conocidas. `DivisorSigma` es una macrofunción (función del sistema) tal que `DivisorsSigma [k, n]` calcula la suma de las k-ésimas potencias de los divisores de n.

```
getf[DivisorSigma[0,Range[15]]]
{1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1}
getf[{1,1,1,1,1,1,1,1,1}]
{1, 0, 0, 0, 0, 0, 0, 0, 0}
getf[DivisorSigma[1,Range[15]]]
{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15}
getf[{1,0,0,0,0,0,0,0,0,0,0,0,0,0,0}]
{1, -1, -1, 0, -1, 1, -1, 0, 0, 1, -1, 0, -1, 1, 1, 0}
```



esta última secuencia es misteriosa y en secciones posteriores la examinaremos con detalle. El argumento de `getf` se denomina una función *Delta de*

Dirac o función *Impulso unitario*. Sólo mencionaremos aquí que su función $f(n)$ resultará corresponder a la función más importante de todo nuestro trabajo: la *función de Möbius* (Apostol, 1965; Bender y Goldman, 1975). Consideremos ahora la respuesta a la pregunta que da título a esta sección (figura 6):

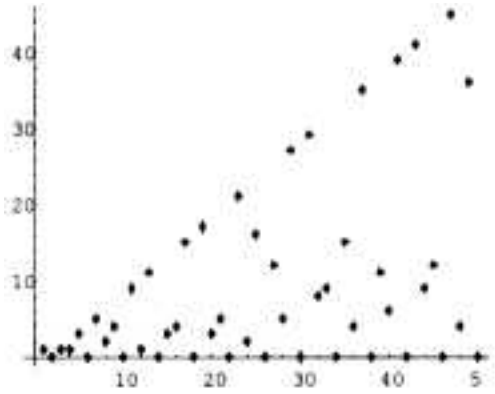


FIGURA 6. Gráfica de n *vs.* $f(n)$, donde $\varphi(n) = \sum_{d|n} f(d)$.

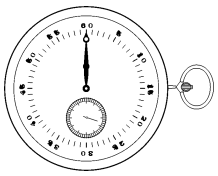
```
getf[EulerPhi[Range[15]]]
{1, 0, 1, 1, 3, 0, 5, 2, 4, 0, 9, 1, 11, 0, 3}
```

donde la macrofunción `EulerPhi [n]` corresponde a $\varphi(n)$ y, en general:

```
getf[Map[F,Range[10]]]
{F[1], -F[1] +F[2], -F[1] +F[3], -F[2] +F[4], -F[1] +F[5],
 F[1] -F[2] -F[3] +F[6], -F[1] +F[7], -F[4] +F[8],
 -F[3] +F[9], F[1] -F[2] -F[5] + F[10]}
```

donde la metafunción (constructor de funciones) `Map` aplica F sobre la secuencia de números menores de 11.

Revisemos ahora las capacidades de la función `getf` examinando sus iteraciones (composiciones) sobre la función d. Las primeras dos iteraciones son fácilmente predecibles y se ilustran en las figuras 7 y 8.



Las cuatro iteraciones siguientes son más interesantes y se muestran en la figura 9. Los dos puntos en la parte inferior de las últimas gráficas son misteriosos y su presencia aún no se ha caracterizado completamente (nótese la variación en la escala vertical).

Por último, la figura 10 ilustra la gráfica correspondiente a una función $f(n)$ tal que sumada a través de todos los divisores de n calcula el n-ésimo primo.

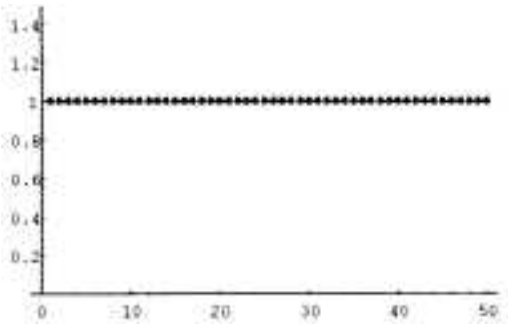


FIGURA 7. Si $F(n) = d(n)$, entonces $f(n)$ es esta función.

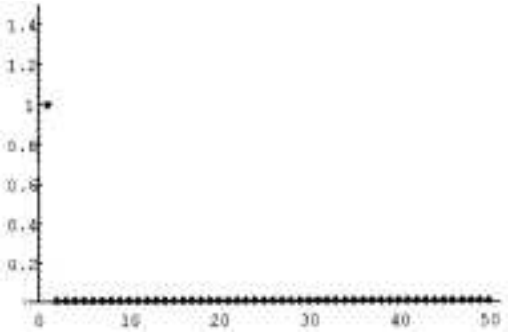
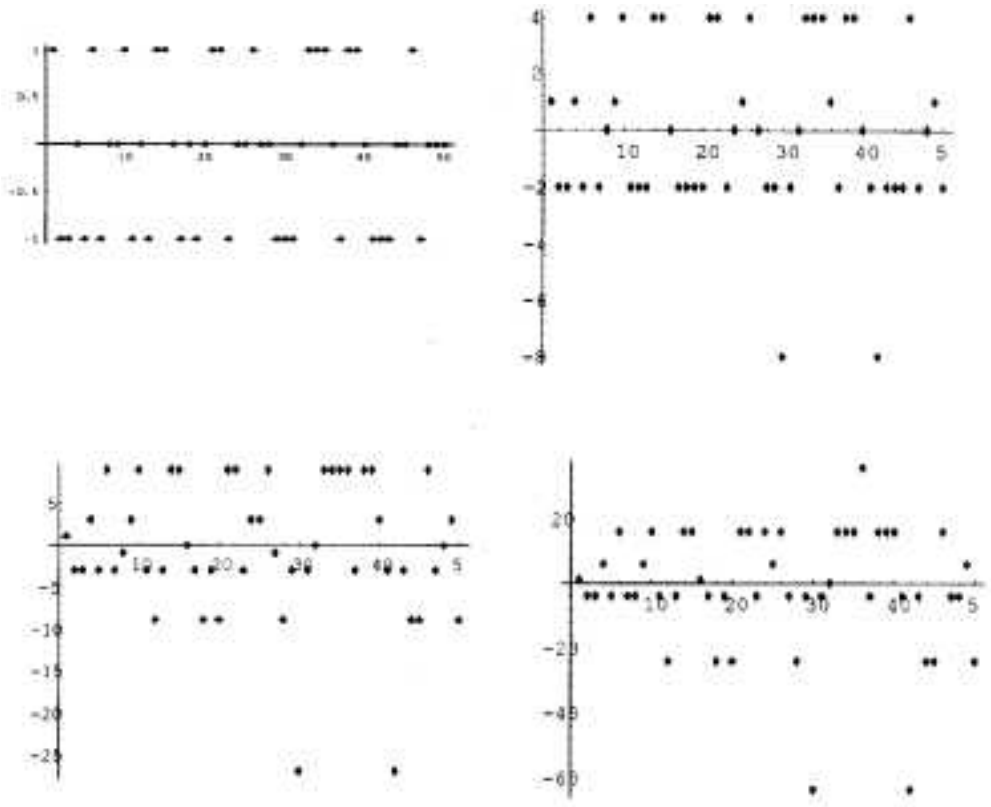


FIGURA 8. Si $d(n) = \sum_{d|n} \sum_{e|d} f(e)$, entonces $f(n)$ es esta función.



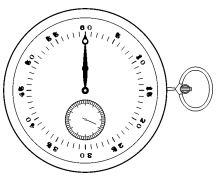


FIGURA 9. De izquierda a derecha y de arriba abajo: iteraciones 3, 4, 5 y 6 de la función $d(n)$.

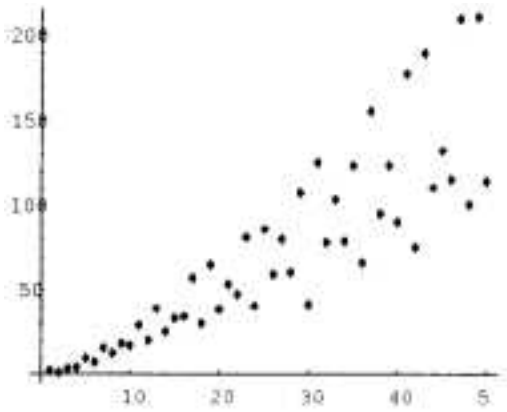


FIGURA 10. Si $F(n) = n$-ésimo número primo, entonces $f(n)$ es esta función.

VI. EJERCICIOS

1. Demostrar que el producto de dos funciones multiplicativas es multiplicativa, es decir, que el conjunto M es cerrado bajo la multiplicación.

2. Demostrar que la función

$$f(n) = \begin{cases} 1, & \text{si } n \text{ no es divisible por un cuadrado mayor que 1,} \\ 0, & \text{de otra manera,} \end{cases}$$

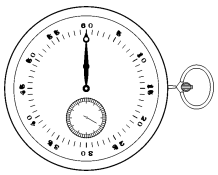
es multiplicativa. Por ejemplo, $f(1) = f(2) = f(3) = 1$, $f(4) = 0$.

3. Demostrar que la función σ es multiplicativa.

4. Demostar que la función $f(n) = c^k$, con c una constante y k un número de primos distintos que dividen a n, es multiplicativa.

5. Demostrar que

$$\varphi(n) = n \prod_{\substack{p|n \\ p\text{primo}}} \left(1 - \frac{1}{p}\right).$$



Por ejemplo, $\varphi(123456) = 123456(1-1/2)(1-1/3)(1-1/643) = 41088$.

6. Demostrar la identidad: $\displaystyle\sum_{d|n}\sum_{c|d} f(c,d) = \sum_{c|n}\sum_{d|\frac{n}{c}} f(c,cd)$

VII. Bibliografía general

[1] Rota, Gian-Carlo, "On the Foundations of Combinatorial Theory. I. Theory of Moebius Functions," *Zeit. für Wahrsh. und Verwandte Gebiete* **2** (1963–1964), pp. 340–368.

[2] Graham, Ronald L., Donald E. Knuth y Oren Patashnik, *Concrete Mathematics*, Addison-Wesley, 1989.

[3] Polya, G., y G. Szegö, *Problems and Theorems in Analysis II*, Springer-Verlag, 1998.

[4] McCarthy, Paul J., *Introduction to Arithmetical Functions*, Springer-Verlag, 1986.

[5] Rademacher, Hans, *Lectures on Elementary Number Theory*, Blaisdell, 1964.

[6] SivaramaKrishnan, R., *Classical Theory of Arithmetic Functions*, Marcel Dekker, Inc., 1989.

[7] Schroeder, M. R., *Number Theory in Science and Communication*, Springer-Verlag, 1990.

[8] Hardy, G. H., y E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon, Oxford, 1984.

[9] Fraleigh, John B., *A First Course in Abstract Algebra*, Addison-Wesley, 1982.

[10] Wolfram, Stephen, *Mathematica*, Addison-Wesley, 1991.

[11] Maeder, Roman, *Programming in Mathematica*, Addison-Wesley, 1991.

[12] Knuth, Donald E., *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, Addison-Wesley, 1981.

[13] Aho, Afred V., John E. Hopcroft y Jeffrey D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, 1974.

[14] Apostol, T. M., "Some Properties of Completely Multiplicative Arithmetical Functions," *American Mathematical Monthly* (March, 1971), pp. 266–271.

[15] Apostol, T. M., "A Characteristic Property of the Moebius Function," *American Mathematical Monthly* **72** (1965), pp. 279–282.

[16] Bender, E. A., y J. R. Goldman, "On the Applications of Möbius Inversion in Combinatorial Analysis," *American Mathematical Monthly* (October, 1975), pp. 789–803.

[17] Keng, Hua Loo, *Introduction to Number Theory*, Springer-Verlag, 1982.