Universidad Nacional Autónoma de México
Facultad de Ciencias
Teoría de los números II

Tarea 2

Ángel Iván Gladín García
No. cuenta: 313112470
angelgladin@ciencias.unam.mx

13 de Abril 2019

1. Sean f y g dos funciones aritméticas y multiplicativas, demuestra que $f * g$ es multiplicativa.

   Demostración. Sean $n, m \in \mathbb{Z}^+$ y $(n, m) = 1$.

$$\begin{aligned}
(f * g)(nm) &= f(nm) * g(nm) \\
&= f(n) * f(m) * g(n) * g(m) && \text{Def. de func. aritmética multiplicativa} \\
&= f(n) * g(n) * f(m) * g(m) && \text{Conmutatividad en } \mathbb{C} \\
&= (f * g)(n) * (f \ * g)(m)
\end{aligned}$$

   Ergo $f * g$ es multiplicativa. □

2. Sea $f \neq 0$ una función aritmética multiplicativa, demuestra que existe su inversa respecto a la convolución de Dirichlet y es multiplicativa.

   Recordemos que si f y g son son funciones aritméticas su producto de Dirichlet (o convolución de Dirichlet) es la función aritmética h definida por la ecuación como

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

   Demostración. **Existencia de inversa respecto a la convolución de Dirichlet,** tal que

$$f * f^{-1} = f^{-1} * f = I$$

   Más aún, f^{-1} está dada por las fórmulas recursivas

$$f^{-1}(1) = \frac{1}{f(1)}, \qquad f^{-1}(n) = \frac{-1}{f(1)} \sum_{d|n,\ d<n} f\left(\frac{n}{d}\right) f^{-1}(d) \quad \text{para } n > 1.$$

   - Para $n = 1$ se debe cumplir que $(f * f^{-1})(1) = I(1)$.
     Lo cual se reduce a $f(1)f^{-1}(1) = 1$. Como $f(1) \neq 0$, solo hay una solución, es decir $f^{-1}(1) = 1/f(1)$.

- Consideremos $n > 1$,

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

Como $f(1) \neq 0$, entonces se tiene demostrado su existencia y unicidad de f^{-1}.

Donde la función aritmética I está dada por por,

$$I(n) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1, \end{cases}$$

que es llamada la función identidad.
Además se tiene que para toda f función aritmética $f * I = I * f = f$

Demostración.

$$(f * I)(n) = \sum_{d|n} f(d) I\left(\frac{n}{d}\right) = \sum_{d|n} f(d)\left[\frac{d}{n}\right] = f(n)$$

dado que $[d/n] = 0$ si $d < n$. □

□

Demostración. **Es multiplicativa.**
La fórmula para la inversa ahora es,

$$f^{-1}(n) = -\sum_{d|n,\ d<n} f^{-1}(d) f\left(\frac{nm}{d}\right)$$

Así si $(n, m) = 1$ entonces[1],

$$f^{-1}(nm) = -\sum_{d|n,\ d<n} f^{-1}(d) f\left(\frac{nm}{d}\right) = -\sum_{d_1|n,\ d_2\ |m,\ d_1 d_2<n} f^{-1}(d_1 d_2) f\left(\frac{nm}{d_1 d_2}\right)$$

Supongamos por inducción que f^{-1} es multiplicativa con argumentos $< nm$.

□

3. Decimos que una función aritmética es completamente multiplicativa si para cuales quiera $m, n \in \mathbb{Z}^+$, se tiene que $f(mn) = f(m)f(n)$.

   Demuestra que si f es una función aritmética multiplicativa, entonces es completamente multiplicativa si y solo si $f^{-1} = f\mu$. (Donde f^{-1} es la inversa respecto a la convolución de Dirichlet).

[1] Factorizamos la expresión de abajo, i.e., el -1 porque si f es multiplicativa entonces $f(1) = 1$.

Demostración. Sea[2] $g(n) = \mu(n)f(n)$. Si f es completamente multiplicativa tenemos que

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

como $f(1) = 1$ y $I(n) = 0$ para $n > 1$. Por tanto $g = f^{-1}$.

De manera análoga, asumimos $f^{-1}(n) = \mu(n)f(n)$. Para probar que f es completamente multiplicativa es suficiente con probar que que $f(p^\alpha) = f(p)^\alpha$ para potencias primas. La ecuación $f^{-1}(n) = \mu(n)f(n)$ implica que

$$\sum_{d|n} \mu(d)f(d)\left(\frac{n}{d}\right) \quad \forall n > 1$$

De ahí, tomando $n = p^\alpha$ se tiene

$$\mu(1)f(1)f(p)^\alpha + \mu(p)f(p)f(a^{\alpha-1}) = 0$$

del cual encontramos $f(p^\alpha) = f(p)f(p^{\alpha-1})$. Que implica que $f(p^\alpha) = f(p)^\alpha$, así f es completamente multiplicativa. □

4. Sea $m \in \mathbb{Z}^+$, demuestra que la función $f(n) = (n, m)$ es multiplicativa.

Demostración. Denotemos a $\gcd(a, b)$ como el *máximo común divisor* y a $\operatorname{lcm}(a, b)$ el *mínimo común múltiplo* de dos enteros a y b. Por demostrar que el máximo común divisor con un argumento fijo (el cual es m) es una función multiplicativa.

Sea $n = ab$ con $a, b \in \mathbb{Z}$ tal que $\gcd(a, b) = 1$ entonces,

$$\begin{aligned}
\gcd(m, ab) &= \gcd(m, \operatorname{lcm}(a, b)) && \text{Como } \gcd(a,b) = 1, \text{ entonces } \operatorname{lcm}(a,b) = ab \\
&= \operatorname{lcm}(\gcd(m, a), \gcd(m, b)) && \text{El gcd y lcm se distribuyen sobre cada uno} \\
&= \frac{\gcd(m, a)\gcd(m, b)}{\gcd(\gcd(m, a)\gcd(m, b))} && \text{Producto del gcd con el lcm} \\
&= \frac{\gcd(m, a)\gcd(m, b)}{\gcd(m, \gcd(a, \gcd(m, b)))} && \text{Máximo común divisor es asociativo} \\
&= \frac{\gcd(m, a)\gcd(m, b)}{\gcd(m, \gcd(\gcd(a, b), m))} && \text{Máximo común divisor es asociativo} \\
&= \frac{\gcd(m, a)\gcd(m, b)}{\gcd(n, \gcd(1, n))} && \text{Por ser primos relativos} \\
&= \frac{\gcd(m, a)(m, b)}{\gcd(m, 1)} \\
&= \frac{\gcd(m, a)\gcd(m, b)}{1} \\
&= \gcd(m, a)\gcd(m, b)
\end{aligned}$$

Ergo, el máximo común divisor con un argumento fijo es una función multiplicativa, i.e.

$$f(ab) = \gcd(ab, m) = \gcd(a, m) \cdot \gcd(b, m) = f(a) \cdot f(b).$$

□

[2]Donde μ es la función de Möbius definida como $\mu(1) = 1$.
Si $n > 1$ escribimos a $n = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$. Entonces

$$\mu(n) = \begin{cases} (-1)^k & \text{si } a_1 = a_2 = \ldots = a_k = 1 \\ 0 & \text{e.o.c} \end{cases}$$

Hay que notar que $\mu(n) = 0$ si y sólo si n es tiene un factor cuadrado > 1.

5. Sea $m \in \mathbb{Z}^+$, demuestra que la función

$$f(n) = \frac{\varphi(mn)}{\varphi(m)} \quad \text{es multiplicativa}$$

Demostración. ☹ □

6. Denotamos [.] como la parte entera de cualquier número real. Sea $f(n) = \left[\sqrt{n}\right] - \left[\sqrt{n-1}\right]$, demuestra que f es multiplicativa.

Demostración. La función f es la indicadora de cuadrados, i.e. $f(n) = 1$ si n es un cuadraro y $f(n) = 0$ en otro caso. Sea $n = ab$ donde $(a, b) = 1$. De este modo la factorización de a y b consiste de conjuntos disjuntos de primos. Entonces si a y b don ambos cuadrados, el producto también es un cuadrado. Y si uno de a o b no es un cuadrado entonces si producto no es un cuadrado. Por tanto la función f es multiplicativa. □

7. Demuestra que

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

Demostración. Sea $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ donde $\alpha_i \geq 1$. Usando el hecho de que el cociente de dos funciones aritméticas multiplicativas es multiplicativa y al serlo se cumple que la función $f(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k})$. Además tenemos que para cada numerador evaluado en la función de Möbius no cero se tiene que $|\mu(d)| = 1$.

Entonces con las observaciones previas, se tiene que

$$\sum_{d|n} \frac{|\mu(d)|}{\varphi(d)} = \prod_{i=1}^{k} \sum_{j=0}^{a_i} \frac{|\mu(p_i^j)|}{\varphi(p_i^j)} \qquad \text{Evaluando cada una de las combs. de sus factores}$$

$$= \prod_{i=1}^{k} \left(1 + \frac{1}{p_i - 1}\right) \qquad \text{Como } |\mu(d)| = 1 \text{ y observando que,}$$

$$\frac{1}{p_1 \cdots p_j} = \frac{1}{p_1 \cdots p_j \prod_{i=1}^{j} \frac{p_i - 1}{p_i}} = \frac{1}{(p_1 - 1) \cdots (p_j - 1)}$$

$$= \prod_{i=1}^{k} \frac{p_i}{p_i - 1} = \prod_{i=1}^{k} \frac{1}{\frac{1}{p_i}(p_i - 1)} = \prod_{i=1}^{k} \frac{1}{1 - \frac{1}{p_i}} \qquad \text{Reacomodo}$$

$$= \frac{n}{\varphi(n)} \qquad \text{Porque } \varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \text{ y agrupando}$$

□

8. Demuestra que

$$\sum_{d|n} \tau(d)^3 = \left(\sum_{d|n} \tau(d)\right)^2$$

Demostración. Recordando que la función aritmética multiplicativa τ es el número enteros positivos divosores de n, la cual por sé multiplicativa cumple que, sea $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ entonces $\tau(n) = \prod_{i=1}^{k} (a_i + 1)$.

Sea $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$,

$$
\begin{aligned}
\tau(n)^3 &= \prod_{i=1}^{k} \tau(p_i^{\alpha_i})^3 = \prod_{i=1}^{k} \sum_{j=1}^{a_i} (j_i + 1)^3 && \text{Por ser multiplicativa y haciendo aritmética} \\
&= \prod_{i=1}^{k} \left(\sum_{j=1}^{a_i} (j_i + 1) \right)^2 && \text{Por } (*) \\
&= \prod_{i=1}^{k} \tau(p_i^{\alpha_i})^2 \\
&= (\tau(n))^2
\end{aligned}
$$

□

Ahora solo hace falta probar $(*)$, ósea

$$\sum_{i=1}^{n} i^3 = \left(\sum_{i=1}^{n} i \right)^2$$

Demostración. **Por inducción**
Tenemos que $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, entonces $\left(\sum_{i=1}^{n} i\right)^2 = \frac{n^2(n+1)^2}{4}$. Mostrar por inducción que

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$$

Paso inductivo con $n = k + 1$*,*

$$
\begin{aligned}
\sum_{i=1}^{k+1} i^3 &= \sum_{i=1}^{k} i^3 + (k+1)^3 \\
&= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\
&= \frac{k^4 + 2k^3 + k^2}{4} + \frac{4k^3 + 12k^2 + 12k + 4}{4} \\
&= \frac{k^4 + 6k^3 + 13k^2 + 12k + 4}{4} \\
&= \frac{(k+1)^2(k+2)^2}{4}
\end{aligned}
$$

□

Por tanto $\sum_{d|n} \tau(d)^3 = \left(\sum_{d|n} \tau(d)\right)^2$.

9. Sea f una función aritmética, demuestra que existe g una función aritmética y multiplicativa tal que:

$$\sum_{k=1}^{n} f((k,n)) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

Demostración. Recordando la función aritmética N la cual $N(n)$ para toda n y teniendo la siguiente identidad,

$$\sum_{k=1}^{n} (k,n)\mu((k,n)) = \mu(n) \tag{1}$$

Tomando convenientemente $g = \varphi$, partiendo a k por su máximo común múltiplo con n da

$$
\begin{aligned}
\sum_{k=1}^{n} f((k,n)) &= \sum_{d|n} \sum_{1\le k\le n,\ (k,n)=d} f((k,n)) \\
&= \sum_{d|n} f(d) \sum_{1\le k\le n,\ (k,n)=d} 1 \\
&= \sum_{d|n} f(d)\varphi\left(\frac{n}{d}\right)
\end{aligned}
$$

Ahora como $\varphi = N * \mu$ y aplicando la identidad (1), se tiene

$$f * \varphi = (N * \mu) * (N * \mu) = (N^{-1} * N) * \mu = I * \mu = \mu.$$

□

10. Sea $n \in \mathbb{Z}^+$, definimos $\mathrm{rad}(n)$ el radical de n como la función multiplicativa que satisface que $\mathrm{rad}(p^\alpha) = p$ para todo p número primo y $\alpha \ge 1$. Demuestra que

$$\mathrm{rad}(n) = \sum_{d|n} \varphi(d)|\mu(d)|$$

Demostración. Sea $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ con $\alpha_i \ge 1$.
Desarrollando en lado izquierdo de la ecuación,

$$
\begin{aligned}
\mathrm{rad}(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= \mathrm{rad}(p_1^{\alpha_1}) \cdots \mathrm{rad}(p_k^{\alpha_k}) && \text{Por ser multiplicativa} \\
&= \prod_{i=1}^{k} p_i
\end{aligned}
$$

Desarrollando en lado derecho de la ecuación,

$$
\begin{aligned}
\sum_{d|n} \varphi(d)|\mu(d)| &= \prod_{i=1}^{k} \sum_{d|p_i^{\alpha_i}} \varphi(d)|\mu(d)| && \text{Por ser multiplicativa} \\
&= \prod_{i=1}^{k} \sum_{d|p_i} \varphi(d)|\mu(d)| && \text{Por def. de func. de Möbius}
\end{aligned}
$$

Además si se tenia $\alpha_i > 1$ su valor es cero y se cancela, y en otro caso 1.

$$
\begin{aligned}
&= \prod_{i=1}^{k} (\varphi(1)|\mu(1)|) + (\varphi(p_i)|\mu(p_i)|) = \prod_{i=1}^{k} 1 + (p_i - 1) && \text{Evaluando} \\
&= \prod_{i=1}^{k} p_i
\end{aligned}
$$

Teniendo ambos lados de la ecuación iguales. □