

La propiedad multiplicativa de la función de Euler $\phi(n)$

Hemos definido en clase la *función de Euler*, $\phi(n)$, para todo entero $n > 1$, como el número de elementos del conjunto $\{0, 1, 2, \dots, n-1\}$ que son primos relativos a n . Definición equivalente: el número de elementos de \mathbb{Z}_n que tienen un recíproco.

Teorema: si a, b son primos relativos, $(a, b) = 1$, entonces $\phi(ab) = \phi(a)\phi(b)$.

Demostración: para cada $n > 1$ denotamos por $\mathbb{Z}_n^* \subset \mathbb{Z}_n$ al subconjunto de las clases de residuos (mod n) que tienen recíproco. Con esta notación, $\phi(n) = \#(\mathbb{Z}_n^*)$. Como $\#(\mathbb{Z}_a^* \times \mathbb{Z}_b^*) = \#(\mathbb{Z}_a^*) \cdot \#(\mathbb{Z}_b^*) = \phi(a)\phi(b)$, basta entonces demostrar que $\#(\mathbb{Z}_{ab}^*) = \#(\mathbb{Z}_a^* \times \mathbb{Z}_b^*)$. Para demostrar esto, construimos una biyección $f : \mathbb{Z}_{ab}^* \rightarrow \mathbb{Z}_a^* \times \mathbb{Z}_b^*$. Para este fin, construimos primero una función $\tilde{f} : \mathbb{Z}_{ab} \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b$ con las siguientes 4 propiedades:

1. \tilde{f} es inyectiva.
2. \tilde{f} es suprayectiva.
3. $\tilde{f}(\mathbb{Z}_{ab}^*) \subset \mathbb{Z}_a^* \times \mathbb{Z}_b^*$. (Es decir, $[z] \in \mathbb{Z}_{ab}^* \implies \tilde{f}([z]) \in \mathbb{Z}_a^* \times \mathbb{Z}_b^*$.)
4. $\mathbb{Z}_a^* \times \mathbb{Z}_b^* \subset \tilde{f}(\mathbb{Z}_{ab}^*)$. (Es decir, $([\alpha], [\beta]) \in \mathbb{Z}_a^* \times \mathbb{Z}_b^* \implies$ existe un $[z] \in \mathbb{Z}_{ab}^*$ tal que $\tilde{f}([z]) = ([\alpha], [\beta])$.)

Una vez definida tal \tilde{f} , con estas propiedades, podemos definir la $f : \mathbb{Z}_{ab}^* \rightarrow \mathbb{Z}_a^* \times \mathbb{Z}_b^*$ por $f([z]) = \tilde{f}([z])$ para todo $[z] \in \mathbb{Z}_{ab}^*$ (“restricción” de \tilde{f} a \mathbb{Z}_{ab}^*). La propiedad (3) de \tilde{f} implica que f está bien definida, la propiedad (1) que es inyectiva, y la propiedad (4) que es suprayectiva, así que es biyectiva. (La propiedad (2) usaremos para demostrar la (4)).

La definición de \tilde{f} . Primero una notación: si z es un entero, denotamos por $[z]_n \in \mathbb{Z}_n$ su clase de congruencia módulo n . Ahora definimos $\tilde{f} : \mathbb{Z}_{ab} = \mathbb{Z}_a \times \mathbb{Z}_b$ por $\tilde{f}([z]_{ab}) := ([z]_a, [z]_b)$.

Ejercicio 1. Demuestra que f está bien definida; es decir, que la definición de $\tilde{f}([z]_{ab})$ solo depende de la clase de congruencia de z módulo ab , y no del entero z mismo.

(Sugerencia: basta demostrar que $z \equiv z' \pmod{ab} \implies z \equiv z' \pmod{a}$ y $z \equiv z' \pmod{b}$.)

Ahora demostraremos que \tilde{f} cumple con las 4 propiedades prometidas.

Demostración de la propiedad (1): sean z, z' tal que $\tilde{f}([z]) = \tilde{f}([z'])$. Esto implica que $z \equiv z' \pmod{a}$ y $z \equiv z' \pmod{b}$. Es decir, ambos a y b dividen a $z - z'$.

Ejercicio 2. Si $a, b|n$, $(a, b) = 1 \implies ab|n$.

Aplicando este ejercicio a $n = z - z'$ obtenemos que $z \equiv z' \pmod{ab}$, así que $[z]_{ab} = [z']_{ab}$. Esto termina la demostración de la inyectividad de \tilde{f} .

Demostración de la propiedad (2): el dominio y codominio de la función \tilde{f} tienen el mismo número de elementos ab y ya demostramos que es inyectiva. Por “principio de casillas”, concluimos que es suprayectiva.

Demostración de la propiedad (3): sea $[z]_{ab} \in \mathbb{Z}_{ab}^*$. Es decir, $(z, ab) = 1$. Si $d|z, a$ (d es un divisor común de z y a) $\implies d|a \implies d|ab \implies d|z, ab \implies d \leq 1 \implies (z, a) = 1$. De manera similar se demuestra que $(z, b) = 1$. Así que, $\tilde{f}([z]_{ab}) = ([z]_a, [z]_b) \in \mathbb{Z}_a^* \times \mathbb{Z}_b^*$.

Demostración de la propiedad (4): sean $([\alpha]_a, [\beta]_b) \in \mathbb{Z}_a^* \times \mathbb{Z}_b^*$. Según la propiedad (2), existe un entero z tal que $\tilde{f}([z]_{ab}) = ([\alpha]_a, [\beta]_b)$. Es decir, $z \equiv \alpha \pmod{a}$ y $z \equiv \beta \pmod{b}$. Tenemos entonces que demostrar que $(z, ab) = 1$.

Ejercicio 3. $z \equiv z' \pmod{n}, (z, n) = 1 \implies (z', n) = 1$.

Aplicando este ejercicio a $z \equiv \alpha \pmod{a}$ y $z \equiv \beta \pmod{b}$ concluimos que $(z, a) = (z, b) = 1$.

Ejercicio 4. $(z, a) = (z, b) = 1 \implies (z, ab) = 1$. □

Ejercicio 5. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ la descomposición de un entero $n > 1$ en producto de primos, donde p_1, \dots, p_m son primos distintos. Demuestra que

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$