

Tarea núm. 4 – soluciones

1. Demuestra el siguiente teorema:

Teorema. Para todo $a, n \in \mathbb{Z}$, donde $n > 1$, las siguientes 3 condiciones son equivalentes:

- a) $[a] \in \mathbb{Z}_n$ tiene un recíproco, i.e. existe un $[b] \in \mathbb{Z}_n$ tal que $[a][b] = [1]$.
- b) $(a, n) = 1$ (a y n son primos relativos).
- c) Existe un par de enteros x, y tal que $ax + ny = 1$.

Solución.

a) \implies b): sea $[b]$ un recíproco de $[a]$. Entonces $ab \equiv 1 \pmod{n}$, o sea $ab - 1 = kn$ para algún $k \in \mathbb{Z}$, por lo que $ab - kn = 1$. Esta última ecuación implica que todo divisor común d de a y b es también un divisor de 1, por lo que el máximo tal divisor es 1.

b) \implies c): primero demostramos el inciso para el caso de $0 < a < n$. Esto lo hacemos por inducción sobre a . Para $a = 1$ tenemos que $(1, n) = 1$ y que $1x + ny = 0$ para $x = 1$ y $y = 0$ así que el inciso es correcto. Para a general, dividimos a n entre a con residuo r , o sea $n = ak + r$ para algunos enteros k, r , con $0 \leq r < n$. Ahora notamos que $(r, a) = (a, n)$ (demostración: si $d|r, a$ entonces $d|ak + r = n$, así que $d|a, n$, y si $d|a, n$ entonces $d|ak - n = r$, así que $d|r, a$, por lo que r, a y n, a tienen el mismo conjunto de divisores comunes, así que tienen el mismo máximo común divisor). Así que $(r, a) = 1$ y $0 < r < a$, por lo que podemos aplicar la suposición de la inducción al par r, a , obteniendo que existe un par de enteros x_1, y_1 tal que $rx_1 + ay_1 = 1$. Multiplicamos ahora la ecuación $ak + r = n$ por x_1 y restamos el resultado de la ecuación $rx_1 + ay_1 = 1$; obtenemos la ecuación $a(y_1 - kx_1) - nx_1 = 1$. Esta da una solución a la ecuación $ax + ny = 1$ con $x = y_1 - kx_1$ y $y = -x_1$.

En caso que a no satisface $0 < a < n$ dividimos a a entre n con residuo a_1 , o sea $a = nk + a_1$ para algunos $k, a_1 \in \mathbb{Z}$, con $(a, n) = (a_1, n) = 1$ y $0 < a_1 < n$ (ver la demostración en paréntesis en el párrafo anterior). Así que el par a_1, n satisface las condiciones del caso del párrafo anterior \implies existen x_1, y_1 tal que $a_1x_1 + ny_1 = 1$. Multiplicamos ahora la ecuación $a = nk + a_1$ por x_1 y restamos el resultado de la ecuación $a_1x_1 + ny_1 = 1$; obtenemos la ecuación $ax_1 + n(y_1 - kx_1) = 1$. Esta da una solución a la ecuación $ax + ny = 1$ con $x = x_1$ y $y = y_1 - kx_1$.

c) \implies a): si $ax + ny = 1 \implies 1 - ax = ny \implies n|1 - ax \implies ax \equiv 1 \pmod{n}$. □

2. Calcula $\phi(p^k)$ para p primo y $k > 0$. (Por ejemplo, hemos visto en clase que $\phi(p) = p - 1$.)

Solución. Según el problema anterior, las clases de congruencia en \mathbb{Z}_{p^k} que *no* tienen recíproco son las clases $[a]$ tal que $(a, p^k) > 1$. Esto es equivalente a que $p|a$, o que a es un múltiplo de p . En el rango $0 \leq a < p^k$, los múltiplos de p son $0, p, 2p, \dots, p^k - p$, que son p^{k-1} números. Los demás números en este rango representan las clases que *sí* tienen un recíproco, por lo que su número es $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$. □

3. Si $n, m > 1$ y $(n, m) = 1$ entonces $\phi(mn) = \phi(m)\phi(n)$.

Solución. Idea de la demostración: para demostrar la igualdad de los dos números $\phi(mn)$ y $\phi(m)\phi(n)$ vamos a interpretar estos números como las cardinalidades (=número de elementos) de dos conjuntos distintos, y luego definimos una biyección entre los dos conjuntos.

Ahora $\phi(mn)$ es, por definición, la cardinalidad del conjunto \mathbb{Z}_{mn}^* y $\phi(m)\phi(n)$ la cardinalidad del conjunto $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ (la cardinalidad del producto cartesiano de dos conjuntos finitos es el producto de las cardinalidades de los conjuntos).

Definimos ahora una función $f : \mathbb{Z}_{mn}^* \rightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ de la manera siguiente: para una clase $c \in \mathbb{Z}_{mn}^*$ se escoge un $x \in c$ (o sea $c = [x]$ o x "representa" la clase c), y se define a $f(c) := (c_1, c_2)$, donde c_1 es la clase de congruencia de $x \pmod{m}$ y c_2 es la clase de congruencia de $x \pmod{n}$.

Antes de seguir, es cómodo de introducir la notación $[x]_N \in \mathbb{Z}_N$ para la clase de congruencia de un entero x modulo un entero $N > 1$. Así que, en esta notación, f se define por $f([x]_{mn}) := ([x]_m, [x]_n)$.

Ahora es importante darse cuenta que esta definición de f requiere una demostración que f está “bien definida”. Primero, tenemos que demostrar que $([x]_m, [x]_n) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$, o sea $[x]_m \in \mathbb{Z}_m^*$ y $[x]_n \in \mathbb{Z}_n^*$. Esto es (según el problema anterior), que $(x, m) = (x, n) = 1$. Pero $d|x, m \implies d|x, mn$ por lo que $(x, m) \leq (x, mn) = 1 \implies (x, m) = 1$ (notamos que $(x, mn) = 1$ ya que $[x]_{mn} \in \mathbb{Z}_{mn}^*$). De manera similar, $(x, n) = 1$.

Segundo, tenemos que demostrar que la definición de $f(c)$ no depende del representante de c que fue elegido para calcular la $f(c) := ([x]_m, [x]_n)$. Esto es, tenemos que demostrar que si x, y son dos representantes de la misma clase c , entonces $([x]_m, [x]_n) = ([y]_m, [y]_n)$. Esto es equivalente a demostrar que $x \equiv y \pmod{mn} \implies x \equiv y \pmod{m}, x \equiv y \pmod{n}$.

Para demostrar esto, tenemos que

$$\begin{aligned} x &\equiv y \pmod{mn} \\ \implies x - y &= kmn \text{ para algun } k \in \mathbb{Z} \\ \implies x - y &= k_1m = k_2n \text{ para } k_1 = kn, k_2 = km \\ \implies x &\equiv y \pmod{m}, x \equiv y \pmod{n}. \end{aligned}$$

Ahora demostramos que f es inyectiva. Esto es: $f([x]) = f([y]) \implies x \equiv y \pmod{nm}$. Tenemos que $f([x]) = f([y]) \implies x \equiv y \pmod{m}, x \equiv y \pmod{n} \implies m, n|x - y \implies x - y = \alpha m = \beta n$ para algunos enteros α, β . Pero $(m, n) = 1$, así que $m|\beta n \implies m|\beta \implies \beta = \gamma m$ para algun entero $\gamma \implies x - y = \beta n = \gamma mn \implies x \equiv y \pmod{nm}$.

Ahora demostramos que f es suprayectiva. Esto es: dado un par de clases $(c_1, c_2) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ existe un $c \in \mathbb{Z}_{mn}^*$ tal que $f(c) = (c_1, c_2)$. Si $c_1 = [a]_m, c_2 = [b]_n$, con $(a, m) = (b, n) = 1$, tenemos que encontrar entonces un entero x tal que $x \equiv a \pmod{m}, x \equiv b \pmod{n}$ y $(x, mn) = 1$. La primera congruencia tiene las soluciones $x = a + ym, y \in \mathbb{Z}$. Subsitiuyendo esto en la segunda congruencia, obtenemos $a + ym \equiv b \pmod{n}$, ó $ym \equiv b - a \pmod{n}$. Como $(m, n) = 1$, tenemos que m tiene un recíproco mod n , o sea un entero m' tal que $mm' \equiv 1 \pmod{n}$. Multiplicamos entonces la congruencia $ym \equiv b - a \pmod{n}$ por m' y obtenemos $y \equiv m'(b - a) \pmod{n}$, por lo que $x := a + mm'(b - a)$ resuelve ambas congruencias. Para ver que este x satisface $(x, mn) = 1$ notamos que $x \equiv a \pmod{m} \implies (x, m) = (a, m) = 1$, y analógamente $(x, n) = 1$. Pero esto implica que $(x, mn) = 1$ ya que $d|x, mn \implies d|mn \implies d|m$ ó $d|n$ (ya que $(m, n) = 1$) $\implies d|m, x$ ó $d|n, x \implies d \leq 1$. \square

4. 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

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

Solución. Por los dos problemas anteriores,

$$\begin{aligned} \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}) &= \phi(p_1^{\alpha_1}) \phi(p_2^{\alpha_2}) \cdots \phi(p_m^{\alpha_m}) = \\ &= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \cdots p_m^{\alpha_m} \left(1 - \frac{1}{p_m}\right) = \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right). \end{aligned}$$

\square