# Tarea núm. 5 – soluciones

1. Sea $n \in \mathbb{Z}$ con $n > 1$. Demuestra que para todo $a, b \in \mathbb{Z}$ con $a \equiv b \bmod n$, $(a, n) = 1$ si y solo si $(b, n) = 1$. (O sea, la condición $(a, n) = 1$ depende solamente de la clase de congruencia de $a$ mod $n$.)

   ▷ Basta demostrar que $a \equiv b \pmod n \Longrightarrow (a, n) = (b, n)$. Para esto, basta demostrar que $a, n$ y $b, n$ tienen el mismo conjunto de divisores comunes; i.e. para todo entero $d$, $d|a, n \iff d|b, n$.

   Ahora, por definición de $a \equiv b \bmod n$, $b = a + kn$ para algun $k \in \mathbb{Z}$, así que si $d$ es un divisor común de $a, n \Longrightarrow$ existen $a_1, n_1 \in \mathbb{Z}$ tal que $a = da_1, n = dn_1 \Longrightarrow b = a + kn = da_1 + kdn_1 = d(a_1 + kn_1) \Longrightarrow d|b \Longrightarrow d$ es un divisor comun de $b, n$. De manera similar, todo divisor común de $b, n$ es un divisor comun de $a, n$. □

2. Sean $a, b, m, n \in \mathbb{Z}$, donde $m, n > 1$ y $(m, n) = 1$.
   *a*) Existe un $x \in \mathbb{Z}$ tal que $x \equiv a \bmod m$ y $x \equiv b \bmod n$.
   *b*) Tal $x$ es único modulo $mn$. O sea, si $y \in \mathbb{Z}$ entonces $y \equiv a \bmod m$ y $y \equiv b \bmod n$ ssi $x \equiv y \bmod mn$.

   ▷ El conjunto de soluciones a la primera congruencia es la clase de congruencia de $a$ modulo $m$. O sea, los enteros de la forma $x = a + km$, $k \in \mathbb{Z}$. Ahora econtramos los valores de $k$ tal que $x = a + km$ satisface tambien la segunda congruencia: $a + km \equiv b \bmod n \iff km \equiv b - a \bmod n$. Ahora, como $(m, n) = 1$, $m$ tiene un recíproco mod $n$ (problema 1 de la tarea 4), digamos $m' \in \mathbb{Z}$, así que $mm' \equiv 1 \bmod n$. Así que $b - a \equiv km \bmod n \iff (b - a)m' \equiv kmm' \equiv k \bmod n \iff k = (b - a)m' + sn$, $s \in \mathbb{Z}$, y $x = a + km = a + [(b - a)m' + sn]m = x_0 + snm$, donde $x_0 = (b - a)m'm$.

   Es decir, el conjunto de los enteros que satifacen ambas congruencias es toda la clase de congruencia mod $mn$ de la solución particular $x_0 = (b - a)mm'$. □

3. Sean $a_1, \ldots, a_k, n_1, \ldots, n_k \in \mathbb{Z}$, donde $n_1, \ldots, n_k > 1$ y $(n_i, n_j) = 1$ para cada $i \neq j$. Demuestra que existe un $x$, único mod $n_1 \cdots n_k$, tal que $x \equiv a_1 \bmod n_1$, $\ldots$, $x \equiv a_k \bmod n_k$ (son $k$ congruencias que el $x$ debe satisfacer.)

   Nota: este resultado se llama el "Teorema Chino de Resíduos".

   ▷ Por inducción sobre $k$: para $k = 1$ es trivialmente correcto. Suponemos el resultado para $k$ y lo demostramos para $k + 1$. Tenemos entonces $k + 1$ congruencias: $x \equiv a_1 \bmod n_1$, $\ldots$, $x \equiv a_k \bmod n_k$, $x \equiv a_{k+1} \bmod n_{k+1}$, con $(n_i, n_j) = 1$ para todo $i \neq j$. Por inducción, existe una solución $x_0 \in \mathbb{Z}$ al sistema de las primeras $k$ congruencias, y la solución general a estas $k$ congruencias es la clase de congriencia de $x_0$ mod $N$, donde $N = n_1 n_2 \cdots n_k$. Así que la solución al sistema de las $k+1$ ecuaciones es la solución al sistema de dos ecuaciones $x \equiv x_0 \bmod N$, $x \equiv a_{k+1} \bmod n_{k+1}$. Estamos entonces en la situación del problema anterior, si logramos demostrar que $(N, n_{k+1}) = 1$.

   Ahora si $d|N, n_{k+1} \Longrightarrow d|N = n_1 n_2 \cdots n_k \Longrightarrow d$ divide a algunos de los $n_i$, $1 \leq i \leq n$ (ya que son primos relativos en pares) $\Longrightarrow d|n_i, n_{k+1} \Longrightarrow d \leq 1$. Así que $(N, n_{k+1}) = 1$.

   Aplicando entonces el problema anterior concluimos que extiste una solución al sistema de $k + 1$ congruencias, única mod $N \cdot n_{k+1} = n_1 \cdots n_k n_{k+1}$. □

4. Sean $A, B, m, n \in \mathbb{Z}$, donde $m, n > 1$ y $(m, n) = 1$. Entonces $A \equiv B \bmod mn$ si y solo si $A \equiv B \bmod m$ y $A \equiv B \bmod n$.

   ▷ Sea $C = A - B$. Tenemos entonces que $A \equiv B \bmod m$ y $A \equiv B \bmod n$ ssi $C$ es una solución al sistema de dos congruencias $x \equiv 0 \bmod m$, $x \equiv 0 \bmod n$. Ahora, una solución particular a este sistema es $x_0 = 0$. Por el problema 2, sabemos que la solución general al sistema es la clase de congruencia mod $mn$ de una solución particular. Concluimos que $A - B = C \equiv 0 \bmod mn$, es decir, $A \equiv B \bmod mn$ . □

5. Sean $p, q$ dos primos distintos, $n = pq$, $f = (p-1)(q-1)$ y $M, k \in Z$, $k \geq 0$. Demuestra que $M^{1+fk} \equiv M \mod n$.

   ▷ Usando el problema anterior, basta demostrar que $M^{1+fk} \equiv M \mod p$ y mod $q$. Si $p|M$ entonces $M \equiv 0 \mod p$ y $M^{1+fk} \equiv M$ trivialmente. Si $p$ no divide a $M$ entonces $M^{p-1} \equiv 1 \mod p$ (teorema de Fermat), así que $M^{1+fk} = M(M^{p-1})^{k(q-1)} \equiv M \mod p$. De manera similar se demuestra $M^{1+fk} \equiv M \mod q$. □

6. Resolver las siguientes congruencias (encontrar todos los valores enteros de $x$ en cada caso):

   *a*) $3x \equiv 2 \mod 5$.

   ▷ Tenemos que $3 \cdot 2 \equiv 1 \mod 5$ así que $2 \equiv 3x \mod 5 \iff 2 \cdot 2 \equiv 2 \cdot 3x \equiv x \mod 5$. Así que el conjunto de soluciones es la clase de congruencia de 4 mod 5, o sea $x = 4 + 5k$, $k \in \mathbb{Z}$. □

   *b*) $3x \equiv 2 \mod 100$.

   ▷ $3 \cdot 33 = 99 \equiv -1 \mod 100 \implies 3 \cdot (-33) \equiv 1 \mod 100 \implies x \equiv (-33)3x \equiv (-33)2 \equiv -66 \equiv 34 \mod 100$. □

   *c*) $17x \equiv 1 \mod 100$.

   ▷ $17x \equiv 1 \mod 100 \iff 100|17x - 1 \iff$ existe un entero $k$ tal que $17x - 1 = 100k$, lo cual reformulamos un poco más bonito como $17x + 100y = 1$ (poniendo $y = -k$). La idea (como fue explicado en la sugerencia al problema 1 de la tarea 4), es usar el algoritmo de euclides para ir reduciendo esta ecuación, paso a paso, a una ecuación similar con coeficientes cada vez más pequeños.
   Aplicamos entonces el algoritmo de Euclides a $100, 17$. Obtenemos, sucesivamente,

   (1) $100 = 17 \cdot 5 + 15$
   (2) $17 = 15 \cdot 1 + 2$
   (3) $15 = 2 \cdot 7 + 1$.

   Multiplicando la ecuación (2) por 7 y restandole la ecuación (3), obtenemos

   $$17 \cdot 7 - 15 = 15 \cdot 7 - 1,$$

   lo cual da

   (4) $17 \cdot 7 = 15 \cdot 8 - 1$.

   Ahora multiplicando la ecuacion (1) por 8 y restandole la ecuación (4), obtenemos

   $$100 \cdot 8 - 17 \cdot 7 = 17 \cdot 5 \cdot 8 + 1 = 17 \cdot 40 + 1,$$

   lo cual da

   $$100 \cdot 8 = 17 \cdot 47 + 1.$$

   Tomando la última ecuación mod 100, nos da

   $$0 \equiv 17 \cdot 47 + 1 \mod 100,$$

   $$17 \cdot 47 \equiv -1 \mod 100,$$

   $$17 \cdot (-47) \equiv 1 \mod 100.$$

   Tenemos entonces que la solución a nuestra congruencia es $x \equiv -47 \equiv 53 \mod 100$. □

   *d*) $x \equiv 77^{77} \mod 100$.

   ▷ Como $\phi(100) = 40$ y $(100, 77) = 1$ tenemos que $77^{40} \equiv 1 \mod 100$. Además, 77 tiene un recíproco mod 100, digamos $\alpha$, así que $77^{77} \equiv 77^{80}\alpha^3 \equiv \alpha^3 \mod 100$.
   Para enontrar $\alpha$ (el recíproco de 77 mod 100), es más fácil encontrar el recíproco de $-77 \equiv 23 \mod 100$. Tenemos $100 = 23 \cdot 4 + 8$ y $23 = 8 \cdot 3 - 1$. Multiplicamos la primera ecuación por 3 y le restamos la segunda, obtenemos $100 \cdot 3 = 23 \cdot 13 + 1 \implies 23 \cdot 13 + 1 \equiv 0 \mod 100 \implies 23 \cdot (-13) \equiv 1 \mod 100 \implies 77 \cdot 13 \equiv 1 \mod 100 \implies \alpha = 13 \implies 77^{77} \equiv 13^3 \equiv 97 \mod 100$. □

*e*) $x \equiv 14 \bmod 15$ y $x \equiv 16 \bmod 17$.

▷ Es fácil adivinar una solución particular, digamos $x_0 = -1$. Ahora sabemos, por problema 2, que la solución general es $x \equiv -1 \bmod 15 \cdot 17$, o sea $x \equiv 254 \bmod 255$.

*f*) $29 \equiv x^{87} \bmod 55$.

▷ Como 55 es un producto de 2 primos, podemos usar el método de codificación RSA. La manera que lo vimos en clase es descomponer $55 = 11 \cdot 5$, luego definir $f = \phi(55) = 10 \cdot 4 = 40$, luego encontrar el recíproco de 87 mod $f$, digamos $d$. O sea, $87d = 1 + kf$, para algun $k \in \mathbb{Z}$. Luego, como vimos en problema 5, $29^d \equiv (x^{87})^d \equiv x^{87d} \equiv x^{1+kf} \equiv x \bmod 55$, así que el problema se reduce a encontrar $d$, y luego calcular $29^d \bmod 55$. Ahora el recíproco mod 40 de 87 es el recíproco de 7, lo cual es 23 (se puede adivinar o calcular como en los incisos anteriores). Tenemos entonces que $x \equiv 29^{23} \bmod 55$. Ahora $29^{23} \bmod 55$ es un poco desagradable pero también hay trucos. Un truco fuerte es usar el teorema de residuos chinos. Calculamos a $29^{23} \bmod 5$ y 11. Modulo 5 tenemos $29^{23} \equiv (-1)^{23} \equiv -1 \equiv 4$. Modulo 11 es $29^{23} \equiv (-4)^{23} \equiv (-4)^3 \equiv 2$ (ya que $(-4)^{10} \equiv 1$, por Fermat). Tenemos entonces que $x \equiv 4 \bmod 5$ y $x \equiv 2 \bmod 11$. Aquí ya es fácil adivinar una solución particular, digamos 24, así que la solución general es $x \equiv 24 \bmod 55$. □