Cuarto Entrenamiento de Teoría de Números

Jesús Liceaga
jose.liceaga@cimat.mx

1 de noviembre de 2021

En esta sesión, aprenderemos a cómo resolver sistemas de congruencias, junto con un resultado muy útil que, si bien no es el mejor para resolverlos, nos permite asegurar su existencia en ciertos casos.

-Liceaga

1. El Teorema Chino del Residuo

A veces, no sólo nos interesa encontrar un número que cumpla con cierta congruencia (por ejemplo, un x tal que $3x + 2 \equiv 0 \pmod 5$), sino encontrar uno que satisfaga varias congruencias a la vez, o bien, ver que no hay ninguno que lo haga.

Por ejemplo, imaginemos que nos gustaría encontrar todos los enteros x tales que $2x \equiv 5 \pmod 7$ y $3x \equiv 4 \pmod 8$. ¿Cómo hacemos esto? En primer lugar, buscamos una solución a alguna de las congruencias, digamos que a $2x \equiv 5 \pmod 7$. A prueba y error, podemos ver rápidamente que la congruencia anterior es equivalente a que $x \equiv 6 \pmod 7$.

Es decir, cualquier número de la forma $x = 7k_1 + 6$ con $k_1 \in \mathbb{Z}$ cumple con la primer congruencia. Entonces, lo que hacemos ahora es sustituir este valor en la segunda:

$$\begin{aligned} 3x &\equiv 4 \pmod 8 \\ \Rightarrow 3(7k_1 + 6) &\equiv 4 \pmod 8 \\ \Rightarrow 21k_1 + 18 &\equiv 4 \pmod 8 \\ \Rightarrow 5k_1 &\equiv 2 \pmod 8 \\ \Rightarrow k_1 &\equiv 2 \pmod 8. \end{aligned}$$

Es decir, $k_1 = 8k_2 + 2$, así que, sustituyendo este valor, obtenemos que $x = 7(8k_2 + 2) + 6 = 56k_2 + 20$. Por lo tanto, las soluciones a nuestro sistema de congruencias son todos los números de la forma $56k_2 + 20$, con k_2 un entero.

En la práctica, ésta es la forma más fácil de obtener las soluciones a un sistema de congruencias: ir sustituyendo y resolviendo las congruencias por separado. Sin embargo, a veces no queremos encontrarlas, sino que nos basta saber que existen, lo cual, bajo ciertas condiciones, podemos asegurar con el Teorema que da nombre a esta sección, sin embargo, antes de probarlo, necesitamos otro resultado:

Lema 1. Sean a y m enteros positivos tales que $mcd(a, m) = 1$. Entonces existe un x tal que $ax \equiv 1 \pmod m$, y este es único módulo m.

Demostración. Como $mcd(a, m) = 1$, entonces existen enteros x, y tales que $ax + my = 1$, de donde $ax = 1 - my$ y, por lo tanto, $ax \equiv 1 - my \equiv 1 \pmod m$. Por otra parte, si suponemos que x_1 y x_2 son tales que $ax_1 \equiv ax_2 \equiv 1 \pmod m$, como $mcd(a, m) = 1$, entonces podemos dividir entre a, obteniendo que $x_1 \equiv x_2 (\bmod m)$, así que nuestra solución es única módulo m.

■

Ya que sabemos esto, estamos en posición de enunciar y probar el siguiente Teorema.

Teorema 1 (Chino del Residuo). Sean $m_1, \ldots, m_n$ enteros positivos primos relativos por parejas y $a_1, \ldots a_n$ enteros cualesquiera. Entonces el sistema de congruencias

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

tiene una solución y esta es única módulo $m = m_1 m_2 \ldots m_n$.

Demostración. Notemos que, para $1 \leq i \leq n$, m/m_i es un entero y que $mcd(m/m_i, m_i) = 1$. Así, por el Lema 1, para cada i existe un entero b_i tal que $(m/m_i)b_i \equiv 1 \pmod{m_i}$. Por otra parte, es claro que $(m/m_i)b_i \equiv 0 \pmod{m_j}$ para $j \neq 1$, pues m_j divide a m/m_i. Entonces, tomemos

$$x_0 = \sum_{i=1}^{n} \frac{m}{m_i} b_i a_i.$$

Así, $x_0 \equiv (m/m_i)a_i b_i \equiv a_i(\pmod{m_i}$ para $1 \leq i \leq n$, donde la primera congruencia se debe a que todos los m/m_j son congruentes a 0 módulo m_i salvo cuando $j = i$ y la segunda a que, por como tomamos a b_i, $(m/m_i)b_i \equiv 1 \pmod{m_i}$. Por lo tanto, x_0 es una solución a nuestro sistema de congruencias.

En cuanto a la unicidad, si x_0 y x_1 son soluciones a nuestro sistema, entonces $x_0 \equiv x_1 \pmod{m_i}$ para $1 \leq i \leq n$, de donde $x_0 \equiv x_1 \pmod{m}$ (¿Por qué?).

■

La demostración anterior puede revolver bastante, es por eso que la "volveremos" a hacer, pero con un ejemplo en particular.

Ejemplo 1. Encuentra el menor entero positivo x tal que $x \equiv 5 \pmod{7}$, $x \equiv 7 \pmod{11}$ y $x \equiv 3 \pmod{13}$.

Solución. En este caso, $a_1 = 5$, $a_2 = 7$, $a_3 = 3$, $m_1 = 7$, $m_2 = 11$, $m_3 = 13$ y $m = 7 \cdot 11 \cdot 13 = 1001$. Ahora, tenemos que encontrar b_1, b_2, b_3 tales que $77b_1 \equiv 1 \pmod{13}$, $91b_2 \equiv 1 \pmod{11}$ y $143b_3 \equiv 1 \pmod{7}$. Simplificando estas congruencias y resolviéndolas por separado, obtenemos que algunas soluciones posibles son $b_1 = -2$, $b_2 = 4$ y $b_3 = -1$. Por lo tanto, al sustituir en la expresión que nos da a x_0, obtenemos que

$$x_0 = 77 \cdot (-1) \cdot 3 + 91 \cdot 4 \cdot 7 + 142 \cdot (-2) \cdot 5 = 887$$

es una solución. Puesto que esta es menor a $1001 = 7 \cdot 11 \cdot 13$, concluimos que es la menor.

■

Ahora, es tu turno de hacer problemas.

1. Sean a, x, y $m_1, \ldots, m_n$ enteros positivos tales que los m_i son primos relativos por parejas. Prueba que si $x \equiv a \bmod m_1$, $\ldots$, $x \equiv a \pmod{m_n}$ entonces $x \equiv a \pmod{m_1 \ldots m_n}$.

2. Sean a, x y m enteros positivos. Prueba que si $x \equiv a \pmod{m}$ y $m'|m$, entonces $x \equiv a \pmod{m'}$.

3. Encuentra el menor entero positivo que deje residuos 1, 2, 3, 4 y 5 cuando lo divides entre 2, 3, 5, 7 y 11, respectivamente.

4. Determina si existe una solución para el sistema $x \equiv 29 \pmod{52}$ y $x \equiv 19 \pmod{72}$.

5. Sea p un entero positivo fijo. Para n positivo, decimos que n es p-seguro si $|n - kp| > 2$ para todo $k \in \mathbb{Z}$. Es decir, si la distancia de n a cualquier múltiplo de p siempre es mayor a 2. ¿Cuántos enteros positivos menores a 10,000 hay que son 7-seguros, 11-seguros y 13-seguros a la vez?

6. Prueba que para todo entero positivo n existen enteros a y b tales que $4a^2 + 9b^2 - 1$ es divisible entre n.

7. Prueba que para todo entero positivo n existen n enteros consecutivos tales que ninguno de ellos es de la forma p^k, donde p es un primo y k un entero positivo.

8. Se tiene que los enteros positivos m, $m+1$, $m+2$ y $m+3$ son divisibles entre los enteros positivos impares n, $n+2$, $n+4$ y $n+6$, respectivamente. Determina el menor valor posible de m en términos de n.

9. Encuentra los últimos 3 dígitos de $1 \times 3 \times 5 \times \cdots \times 2021$.

10. Sean a, b dos enteros positivos primos relativos tales que $a > b$. En un camino recto, en el cual está marcado cada centímetro n, para todo entero n, un saltamontes hará algunos saltos comenzando en la marca de 0 cm y siguiendo las siguientes reglas:

    - Cuando cierto minuto sea múltiplo de a y no de b, saltará a centímetros hacia adelante.
    - Cuando cierto minuto sea múltiplo de b y no de a, saltará b centímetros hacia atrás.
    - Cunado cierto minuto sea múltiplo de a y de b, saltará $a - b$ centímetros hacia adelante.
    - Cuando un minuto no se múltiplo de a ni de b, el saltamontes permanecerá donde está.

    Determina todas las marcas a las que puede llegar el saltamontes.