Sistema de congruencias lineales con módulos coprimos - Métodos para buscar soluciones

Matematica Discreta 2 - IMERL - FIng

Semestre 1 de 2024 - 23/04/24

1 Sistema de congruencias a resolver

Vamos a considerar como ejemplo el Ejercicio 2 del Primer Parcial del segundo semestre de 2023. El ejercicio pide resolver el siguiente sistema de congruencias:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 7 \\ x \equiv 4 \pmod{11} \end{cases}.$$

"Resolver" el sistema significa que debemos hallar **todas** las soluciones del sistema (o argumentar que no tiene solución). Es decir: debemos indicar cuál es el conjunto de soluciones y argumentar por qué esas son todas las soluciones posibles.

2 Existencia de soluciones

Antes de buscar soluciones, vamos a analizar si el sistema tiene solución. Los módulos son coprimos dos a dos. Es decir:

$$mcd(3,7) = 1, \quad mcd(3,11) = 1, \quad mcd(7,11) = 1.$$

Por lo tanto, por el Teorema Chino del Resto (TCR), podemos afirmar que el sistema tiene solución, y que esta es única módulo el producto de los módulos $3 \times 7 \times 11 = 231$. Es decir: el sistema tiene infinitas soluciones, y todas son de la forma:

$$x_k = x_0 + 231k, \ k \in \mathbb{Z};$$

donde x_0 es una solución particular cualquiera a determinar.

Veamos ahora cómo calcular una solución particular x_0. Para esto vamos a considerar varios métodos distintos; todos igual de válidos, aunque cada uno con sus ventajas y

desventajas. Queda a criterio de cada persona la elección del método que le resulte más conveniente.

3 Método de "fuerza bruta"

Este método consiste en hacer una lista de las soluciones de cada ecuación por separado, y luego buscar un valor que sea solución de las tres ecuaciones a la vez (y por lo tanto solución del sistema de ecuaciones).

La primera ecuación es: $x \equiv 1 \pmod 3$. Por definición de congruencia, sus soluciones son de la forma: $x_k = 1 + 3k$, con $k \in \mathbb{Z}$. Si consideramos los valores de $k \geq 0$, obtenemos la siguiente lista de soluciones de la primera ecuación:

$$1, 4, 7, 10, 13, \mathbf{16}, 19, 22, 25, 28, 31, 34, \mathbf{37}, 40, 43, 46, 49, 52, 55, \mathbf{58}, 61, \ldots.$$

La segunda ecuación es: $x \equiv 2 \pmod 7$. Por definición de congruencia, sus soluciones son de la forma: $x_k = 2 + 7k$, con $k \in \mathbb{Z}$. Si consideramos los valores de $k \geq 0$, obtenemos la siguiente lista de soluciones de la segunda ecuación:

$$2, 9, \mathbf{16}, 23, 30, \mathbf{37}, 44, 51, \mathbf{58}, 65, 72, 79, 86, 93, 100, 107, 114, 121, 128, \ldots.$$

A partir de estas dos listas, ya podemos ver que la primera y la segunda ecuación tienen al menos tres soluciones en común: $x = 16$, $x = 37$ y $x = 58$. Veamos si alguno de estos valores también es solución de la tercera ecuación.

La tercera ecuación es: $x \equiv 4 \pmod{11}$. Por definición de congruencia, sus soluciones son de la forma: $x_k = 4 + 11k$, con $k \in \mathbb{Z}$. Es decir (para $k \geq 0$):

$$4, 15, 26, \mathbf{37}, 48, 59, 70, 81, 92, 103, 114, 125, 136, 147, 158, 169, 180, 191, \ldots.$$

Por lo tanto, podemos ver que $x = 37$ es solución de las tres ecuaciones que forman el sistema. Es decir: $x_0 = 37$ es una solución del sistema. Por lo tanto, por el TCR, podemos concluir que todas las soluciones del sistema son de la forma:

$$x_k = x_0 + (3 \times 7 \times 11)\, k = 37 + 231k, \ k \in \mathbb{Z}.$$

En términos de congruencias, podemos decir que las soluciones del sistema son los enteros congruentes con 37 módulo 231: $x \equiv 37 \pmod{231}$.

Observación 1. *El TCR garantiza que las soluciones del sistema difieren en un múltiplo de 231. Esto implica que el sistema tiene una única solución entre 0 y 230. Por lo tanto, una vez que encontramos que $x = 37$ es solución del sistema, podemos parar de buscar*

(porque es la única entre 0 y 230). Si no tuviéramos el resultado del TCR, deberíamos seguir buscando soluciones en común de forma indefinida; por lo que el método de fuerza bruta no sería útil para hallar todas las posibles soluciones del sistema (sí sería útil para hallar soluciones particulares).

4 Método de sustitución y cálculo de inversas

Este método resuelve el sistema de a dos ecuaciones a la vez. Recordemos que el sistema de ecuaciones es:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 7 \\ x \equiv 4 \pmod{11} \end{cases}.$$

4.1 Primer par de ecuaciones

Consideremos el sistema formado por el primer par de ecuaciones del sistema original:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 7 \end{cases}.$$

Como los módulos 7 y 3 son coprimos, sabemos por el TCR que este sistema de dos ecuaciones tiene solución, y que esta es única modulo $7 \times 3 = 21$. Es decir, sabemos que las soluciones de este sistema son de la forma:

$$x = x_0 + 21m,\ m \in \mathbb{Z};$$

siendo x_0 una solución cualquiera del sistema de dos ecuaciones. Vamos a calcular un x_0.

De la segunda ecuación, sabemos que x debe ser de la forma: $x = 2 + 7k$, con $k \in \mathbb{Z}$. Reemplazando en la primera ecuación, se obtiene una nueva ecuación en congruencias, pero en la variable k:

$$2 + 7k \equiv 1 \pmod 3 \Leftrightarrow 7k \equiv -1 \pmod 3.$$

La idea ahora es calcular la inversa de 7 módulo 3, para luego "despejar" k en la ecuación anterior. Por definición, $z \in \mathbb{Z}$ es inversa de 7 módulo 3, si cumple: $7z \equiv 1 \pmod 3$. Esto equivale a la siguiente ecuación diofántica:

$$7z \equiv 1 \pmod 3 \Leftrightarrow 7z = 1 + 3y \Leftrightarrow 7z - 3y = 1,\ z, y \in \mathbb{Z}.$$

Podemos buscar soluciones de esta diofántica con el método de Euclides extendido. Sin embargo, en este caso es más sencillo obtener una solución "a ojo". Por ejemplo, vemos

que el par $z_0 = 1$, $y_0 = 2$ forma una solución de esta diofántica. Por lo tanto, la inversa de 7 módulo 3 es: $z \equiv 1 \pmod 3$. Ahora que tenemos la inversa, podemos despejar k de la ecuación que teníamos. Para esto multiplicamos a ambos lados por la inversa de 7 modulo 3:

$$7k \equiv -1 \pmod 3 \Leftrightarrow 7^{-1}(7k) \equiv 7^{-1}(-1) \pmod 3 \Leftrightarrow k \equiv -1 \pmod 3.$$

Es decir: $k = -1 + 3m$, con $m \in \mathbb{Z}$. Reemplazando k en la expresión de x, se obtienen las soluciones comunes de las primeras dos ecuaciones:

$$x = 2 + 7k = 2 + 7(-1 + 3m) = 2 - 7 + 7(3m) = -5 + 21m,\ m \in \mathbb{Z}.$$

En términos de congruencias, podemos decir que las soluciones del sistema formado por las primeras dos ecuaciones, son los enteros x, tales que: $x \equiv -5 \pmod{21}$.

4.2 Segundo par de ecuaciones

De esta forma logramos convertir las primeras dos ecuaciones en una:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 7 \end{cases} \Leftrightarrow x \equiv -5 \pmod{21}.$$

Por lo tanto, el sistema original es equivalente a:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 7 \\ x \equiv 4 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x \equiv -5 \pmod{21} \\ x \equiv 4 \pmod{11} \end{cases}.$$

Ahora vamos a aplicar el mismo procedimiento para este nuevo sistema de dos ecuaciones. De la primera ecuación tenemos que: $x = -5 + 21k$, con $k \in \mathbb{Z}$. Reemplazando en la segunda ecuación, y simplificando, se obtiene:

$$x \equiv 4 \pmod{11} \Leftrightarrow -5 + 21k \equiv 4 \pmod{11} \Leftrightarrow 21k \equiv 9 \pmod{11}.$$

En este momento deberíamos calcular la inversa de 21 módulo 11, para luego despejar k. Sin embargo, como 21 es mayor al módulo, podemos reducir $21k$ a un número entre 0 y 10 (o entre -10 y 0). En este caso, usando que $21k - 2(11k) = -k$, vemos que: $21k \equiv -k \pmod{11}$. Por lo tanto, la ecuación a resolver es:

$$21k \equiv 9 \pmod{11} \Leftrightarrow -k \equiv 9 \pmod{11} \Leftrightarrow k \equiv -9 \pmod{11}.$$

En este caso tuvimos suerte y pudimos "despejar" el valor de k solamente simplificando la congruencia, y sin necesidad de resolver una diofántica para hallar la inversa.

Obtuvimos entonces que: $k = -9 + 11m$, con $m \in \mathbb{Z}$. Reemplazando k en la expresión de x, se obtiene la solución común de estas dos ecuaciones:

$$x = -5 + 21k = -5 + 21(-9 + 11m) = -5 - 21(9) + 21(11m) = -194 + 231m,\ m \in \mathbb{Z}.$$

Por lo tanto, estas son las soluciones del sistema original. En términos de congruencias, podemos decir que las soluciones del sistema original, son los enteros x, tales que:

$$x \equiv -194 \pmod{231} \equiv (-194 + 231) \pmod{231} \equiv 37 \pmod{231}.$$

5 Método de resolución de diofánticas

Este método resuelve el sistema de a dos ecuaciones a la vez. En este sentido es igual al método anterior. La diferencia es que en el método anterior solamente se resuelven diofánticas para calcular inversas, mientras que en el método de esta sección las diofánticas no necesariamente están asociadas a calcular una inversa modular. Recordemos nuevamente que el sistema de ecuaciones a resolver es:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{7} \\ x \equiv 4 \pmod{11} \end{cases}.$$

5.1 Primer par de ecuaciones

Consideremos el sistema formado por el primer par de ecuaciones del sistema original:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{7} \end{cases}.$$

Ya argumentamos que para este sistema de dos ecuaciones, las soluciones son de la forma: $x = x_0 + 21m$, con $m \in \mathbb{Z}$, y siendo x_0 una solución cualquiera del sistema de dos ecuaciones. Veamos cómo calcular un x_0.

Usando la definición de congruencias, podemos convertir el sistema de dos congruencias a dos ecuaciones en aritmética usual:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{7} \end{cases} \Leftrightarrow \begin{cases} x = 1 + 3k,\ k \in \mathbb{Z} \\ x = 2 + 7m,\ m \in \mathbb{Z} \end{cases}.$$

Usando que $x = x$, las últimas dos ecuaciones implican la siguiente igualdad:

$$1 + 3k = 2 + 7m \Leftrightarrow 3k - 7m = 1,\ k, m \in \mathbb{Z}.$$

De esta forma obtenemos una ecuación diofántica, en las variables k y m. Podemos resolver esta diofántica usando el método de Euclides extendido (para calcular coeficientes de Bezout). Sin embargo, en este caso es más sencillo obtener una solución "a ojo". Por ejemplo, vemos que el par $k_0 = -2$, $m_0 = -1$ forma una solución de esta diofántica. Por lo tanto, las soluciones de la diofántica son de la forma:

$$k = -2 + (-7)n, \quad m = -1 - 3n, \quad n \in \mathbb{Z}.$$

Reemplazando k en la expresión de x, se obtienen las soluciones comunes de las primeras dos ecuaciones:

$$x = 1 + 3k = 1 + 3(-2 - 7n) = 1 - 6 - 7(3n) = -5 - 21n,\ n \in \mathbb{Z}.$$

En términos de congruencias, podemos decir que las soluciones del sistema formado por las primeras dos ecuaciones, son los enteros x, tales que: $x \equiv -5 \pmod{21}$.

5.2 Segundo par de ecuaciones

De esta forma logramos convertir las primeras dos ecuaciones en una:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 7 \end{cases} \Leftrightarrow x \equiv -5 \pmod{21}.$$

Por lo tanto, el sistema original es equivalente a:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 7 \\ x \equiv 4 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x \equiv -5 \pmod{21} \\ x \equiv 4 \pmod{11} \end{cases}.$$

Ahora vamos a aplicar el mismo procedimiento para este nuevo sistema de dos ecuaciones. Usando la definición de congruencia, el nuevo sistema de dos ecuaciones equivale a:

$$\begin{cases} x \equiv -5 \pmod{21} \\ x \equiv 4 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x = -5 + 21k,\ k \in \mathbb{Z} \\ x = 4 + 11m,\ m \in \mathbb{Z} \end{cases}.$$

Esto implica que k y m deben cumplir la siguiente ecuación diofántica:

$$-5 + 21k = 4 + 11m \Leftrightarrow 21k - 11m = 9,\ k, m \in \mathbb{Z}.$$

Ahora debemos buscar soluciones de esta diofántica. Para esto primero debemos hallar coeficientes de Bezout de 21 y 11. Como su mcd es 1, esto equivale a encontrar una solución de la diofántica dada por: $21k - 11m = 1$. Podemos usar el método de Euclides extendido para calcular una solución de esta ecuación. Sin embargo, en este caso resulta sencillo encontrar una solución "a ojo". En efecto, vemos que el par $k_0 = -1$, $m_0 = -2$ es solución. Es decir: $21(-1) - 11(-2) = 1$. Multiplicando por 9 a ambos lados de la igualdad, obtenemos una solución particular de la diofántica que queríamos resolver: $21(-9) - 11(-18) = 9$. Es decir: el par $k_0 = -9$, $m_0 = -18$ es solución particular de $21k - 11m = 9$. Por lo tanto, la solución general es:

$$k = -9 - 11n,\ m = -18 - 21n,\ n \in \mathbb{Z}.$$

Reemplazando el valor de k en la expresión de x, se obtienen las soluciones del sistema de dos ecuaciones en congruencias:

$$x = -5 + 21k = -5 + 21(-9 - 11n) = -5 - 21(9) - 21(11n) = -194 + 231n,\ n \in \mathbb{Z}.$$

Estas son las soluciones del sistema original. En términos de congruencias, las soluciones del sistema original son:

$$x = -194 + 231n,\ n \in \mathbb{Z} \Leftrightarrow x \equiv -194 \pmod{231} \Leftrightarrow x \equiv 37 \pmod{231}.$$

6 Método de combinación lineal

Este método se puede encontrar en el Teórico de OpenFing de 2021, clase 9, "Sistemas de Congruencias 1". El método se introduce junto con el enunciado del TCR (1 hora), y luego se lo aplica en un ejemplo (1 hora y 19 minutos). La notación utilizada es la siguiente:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{7} \\ x \equiv 4 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \end{cases}$$

Luego se definen los siguientes coeficientes:

$$\begin{cases} M_1 = m_2 m_3 = 7 \times 11 = 77 \\ M_2 = m_1 m_3 = 3 \times 11 = 33 \\ M_3 = m_1 m_2 = 3 \times 7 = 21 \end{cases},$$

Se puede probar que una solución particular del sistema original está dada por la siguiente combinación lineal:

$$x_0 = a_1 M_1 M_1' + a_2 M_2 M_2' + a_3 M_3 M_3';$$

donde cada M_i' se define como la inversa de M_i, módulo su respectivo m_i. Es decir:

$$\begin{cases} M_1 M_1' \equiv 1 \pmod{m_1} \Leftrightarrow 77 M_1' \equiv 1 \pmod{3} \\ M_2 M_2' \equiv 1 \pmod{m_2} \Leftrightarrow 33 M_2' \equiv 1 \pmod{7} \\ M_3 M_3' \equiv 1 \pmod{m_3} \Leftrightarrow 21 M_3' \equiv 1 \pmod{11} \end{cases}$$

Antes de calcular las inversas, conviene reducir los coeficientes M_i, módulo cada m_i, para simplificar las ecuaciones en congruencias. Obtenemos:

$$\begin{cases} 77 M_1' \equiv 1 \pmod{3} \\ 33 M_2' \equiv 1 \pmod{7} \\ 21 M_3' \equiv 1 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} 2 M_1' \equiv 1 \pmod{3} \\ 5 M_2' \equiv 1 \pmod{7} \\ 10 M_3' \equiv 1 \pmod{11} \end{cases}$$

En este caso conviene reducir la primera y última ecuación a números negativos, para despejar directamente los valores de M_1' y M_2'. Esto evita tener que resolver las respectivas diofánticas para calcular la inversa:

$$\begin{cases} 2 M_1' \equiv 1 \pmod{3} \\ 5 M_2' \equiv 1 \pmod{7} \\ 10 M_3' \equiv 1 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} -M_1' \equiv 1 \pmod{3} \\ 5 M_2' \equiv 1 \pmod{7} \\ -M_3' \equiv 1 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} M_1' \equiv -1 \pmod{3} \\ 5 M_2' \equiv 1 \pmod{7} \\ M_3' \equiv -1 \pmod{11} \end{cases}$$

Resta calcular la inversa de la segunda ecuación: $5 M_2' \equiv 1 \pmod{7}$. Esto equivale a la diofántica:

$$5 M_2' = 1 + 7k \Leftrightarrow 5 M_2' - 7k = 1,\ M_2', k \in \mathbb{Z}.$$

Es sencillo ver que una solución particular está dada por el par: $M_2' = 3$, $k = 2$. Por lo tanto, la inversa es: $M_2' \equiv 3 \pmod{7}$. Ahora que tenemos las inversas M_i', obtenemos la siguiente solución particular del sistema original:

$$x_0 = a_1 M_1 M_1' + a_2 M_2 M_2' + a_3 M_3 M_3' =$$

$$= 1 \times 77 \times (-1) + 2 \times 33 \times (3) + 4 \times 21 \times (-1) = 37.$$

Por lo tanto, por el TCR, todas las soluciones del sistema están dadas por los x enteros, tales que:

$$x \equiv 37 \pmod{3 \times 7 \times 11} \Leftrightarrow x \equiv 37 \pmod{231}.$$