¿Cómo resolver ecuaciones y sistemas de ecuaciones en congruencias?

Álgebra I – Mayo de 2018

Marcelo Rubio*

Abstract

En estas notas ofrecemos una guía para resolver ecuaciones y sistemas lineales de ecuaciones en congruencia, con algunos ejercicios resueltos a modo de ejemplo. Asumimos que el lector ha revisado previamente la definición y propiedades básicas de la relación de congruencia, así como las nociones de divisibilidad, máximo común divisor y mínimo común múltiplo en $\mathbb{Z}$.

1 Ecuaciones lineales

Nos dedicamos primero a resolver ecuaciones lineales de una variable, que denotamos x. Es decir, buscamos todas las soluciones de

$$ax \equiv b\ (n)\ , \tag{1}$$

donde $a, b \in \mathbb{Z}$, $a \neq 0$ y $n \in \mathbb{N}$ están dados.

En primer lugar, debemos asegurarnos de que (1) admita solución. En el teórico se probó que la condición necesaria y suficiente para la existencia de solución es que $(a, n) \mid b$, donde (a, n) es el máximo común divisor entre a y n; o sea:

$$(1) \text{ admite solución} \quad \Leftrightarrow \quad (a, n) \mid b.$$

Ejemplo. La ecuación $3x \equiv 4\ (9)$ no tiene solución, pues $(3, 9) = 3 \nmid 4$.

Sabemos que si la condición de existencia de solución se cumple, luego tendremos infinitas soluciones. Sin embargo, basta sólo hallar una de ellas para

*merubio@famaf.unc.edu.ar.

caracterizarlas a todas. Esto es, si x_o es solución de (1), luego todas sus soluciones son los elementos del conjunto

$$\mathcal{S} = \left\{ x \in \mathbb{Z} \ : \ x = x_o + \frac{n}{(a,n)} \ k, \ k \in \mathbb{Z} \right\}.$$

Por lo tanto, todo el problema se reduce a hallar una solución *particular*, x_o. Para ello haremos uso de lo que aprendimos sobre números coprimos. Recordemos que $n, m \in \mathbb{Z}$ se dicen *coprimos* si no comparten ningún primo en su factorización, o sea $(n, m) = 1$. Además, se tiene que

$$(n, m) = 1 \quad \Leftrightarrow \quad \exists \, s, t \in \mathbb{Z} \ : \ 1 = sn + tm.$$

Luego, para hallar la solución x_o buscada, primero dividimos ambos miembros de (1) por (a, n), obteniendo (no olvidar dividir también a n)

$$a'x \equiv b' \ (n') \ , \tag{2}$$

donde hemos definido

$$a' = \frac{a}{(a,n)} \ ; \quad b' = \frac{b}{(a,n)} \ ; \quad n' = \frac{n}{(a,n)}.$$

Tres observaciones:

- Se tiene que $(a', n') = 1$ (ejercicio fácil).
- Dado que $(a, n) \mid b$ (pues estamos asumiendo que hay solución), b' *siempre* es entero, y todo está bien definido.
- La ecuación (1) que queríamos resolver originalmente *es equivalente* a la reducción (2). Esto lo probamos en el ejercicio 10 del práctico 5. Por lo tanto los conjuntos de soluciones de ambas ecuaciones son iguales y *basta hallar una solución particular de* (2).

Ahora, como $(a', n') = 1$ por la primer observación, sabemos que existirán enteros s, t tales que

$$1 = s \cdot a' + t \cdot n', \tag{3}$$

los cuales además sabemos calcular por el algoritmo de Euclides. Una vez que los calculamos, multiplicamos ambos miembros de (3) por b' y obtenemos

$$b' = s \cdot b' \cdot a' + n' \cdot t \cdot b'.$$

Tomando congruencia módulo n' como necesitamos para resolver (2), obtenemos que

$$b' \equiv s \cdot b' \cdot a' + n' \cdot t \cdot b' \equiv a' \cdot b' \cdot s \ (n') \ ,$$

pues claramente $n' \cdot t \cdot b' \equiv 0 \ (n')$. Por lo tanto,

$$b' \equiv a' \cdot b' \cdot s \ (n') \ ,$$

y comparando con (2) deducimos que el número $x_o = b' \cdot s$ es una solución particular de (2). Luego, el conjunto de soluciones de (2), que coincide con el conjunto de soluciones de (1) por la tercera observación es $\mathcal{S} = \{x_o + n'k \ : \ k \in \mathbb{Z}\}$, donde *la solución particular puede obtenerse directamente multiplicando a b' por el entero que acompaña a a' en la combinación lineal* (3).

Breve procedimiento para lectores ansiosos I:

Para resolver $ax \equiv b \ (n)$:

1. Chequear que $(a, n) \mid b$. Si esto no pasa, no hay solución. Si se verifica la condición, definir $b' = b/(a, n)$.
2. Cuando hay solución, dividir a toda la ecuación por (a, n) y llevarla a la forma $a'x \equiv b' \ (n')$, con $(a', n') = 1$.
3. Encontrar enteros s, t tales que $1 = sa' + tn'$.
4. Luego, $x_o = b' \cdot s$ es solución particular de la ecuación.
5. Todas las soluciones son $\{x_o + nk/(a, n), \ k \in \mathbb{Z}\}$.

1.1 Ejemplos

Veamos algunos ejemplos donde aplicamos la discusión anterior.

1. *Hallar todas las soluciones de la ecuación*

   $$6x \equiv 10 \ (8).$$

   Solución. Dado que $(6, 10) = 2$ y $2 \mid 10$, tenemos solución única módulo $8/2 = 4$. Para hallar una solución particular, dividimos la ecuación por $(6, 10) = 2$ y obtenemos

   $$3x \equiv 5 \ (4).$$

   Luego, como $(3, 4) = 1$, expresamos a 1 como combinación lineal de 3 y 4. En este caso obtenemos fácilmente

   $$1 = 3 \cdot (-1) + 4 \cdot 1.$$

Multiplicando por 5 ambos miembros se obtiene

$$5 = 3 \cdot (-1) \cdot 5 + 4 \cdot 1 \cdot 5,$$

por lo que $x_o = (-1) \cdot 5 = -5$ es solución particular. Finalmente, todas las soluciones son $\mathcal{S} = \{x = -5 + 4k \ : \ k \in \mathbb{Z}\}$.

2. *Dada la ecuación*

$$-654x \equiv 30 \ (2406),$$

calcular:
(a) La menor solución positiva
(b) todas las soluciones x tales que $-1000 \leq x \leq 313$.

Solución. Usando el algoritmo de Euclides, se ve que $(-654, 2406) = (654, 2406) = 6$ y $6|30$. Por lo tanto, hay solución única módulo $2406/6 = 401$. Si *coprimizamos* la ecuación (es decir, la dividimos por $(654, 2406) = 6$), llegamos a la ecuación equivalente

$$-109x \equiv 5 \ (401). \tag{4}$$

Luego, como $(-109, 401) = 1$, es posible expresar al 1 como combinación lineal de dichos enteros. Nuevamente por el algoritmo de Euclides, obtenemos

$$1 = (-109) \cdot 103 + 401 \cdot 28.$$

Multiplicando ambos miembros de la igualdad anterior por 5, se ve que una solución particular de (4) es $x_o = 103 \cdot 5 = 515$, y todas las soluciones son $\mathcal{S} = \{x = 515 + 401k \ : \ k \in \mathbb{Z}\}$. Ahora respondemos lo que nos pide el problema. La menor solución positiva no es 515, dado que si elegimos $k = -1$, se tiene que $x = 114$ es solución y $114 < 515$. Luego, **(a) La menor solución positiva es 114.** Para responder (b), veamos que si elegimos $k = -4$, la solución es $x = -1089 < -1000$, por lo que nos pasamos. Luego la mínima solución en el intervalo $-1000 \leq x \leq 313$ corresponde a tomar $k = -3$, y es $x_{\min} = -688$. La siguiente es $-688 + 401 = -287$, y la siguiente $-287 + 401 = 114$. La próxima solución claramente supera la cota 313, por lo que **(b) Las soluciones entre $-1000 \leq x \leq 313$ son -688, -287 y 114.**

2 Sistemas de dos ecuaciones

Ahora nos concentraremos en resolver sistemas de (por ejemplo) dos ecuaciones lineales en una variable x, o sea

$$\begin{cases} ax & \equiv b \ (n) \\ cx & \equiv d \ (m) \end{cases} \tag{5}$$

donde $a, b, c, d \in \mathbb{Z}$, $a, c \neq 0$ y $n, m \in \mathbb{N}$. El primer paso será coprimizar al sistema, del mismo modo en el que procedimos en la sección anterior. Es decir, escribimos

$$\begin{cases} a'x & \equiv b' \ (n') \\ c'x & \equiv d' \ (m') \end{cases} \tag{6}$$

donde

$$a' = \frac{a}{(a,n)} \ ; \quad b' = \frac{b}{(a,n)} \ ; \quad n' = \frac{n}{(a,n)} \ ;$$

y

$$c' = \frac{c}{(c,m)} \ ; \quad d' = \frac{d}{(c,m)} \ ; \quad m' = \frac{m}{(c,m)} \ .$$

Si b' o d' no resultan enteros, entonces el sistema no tendrá solución pues alguna de las ecuaciones que lo compone no admite soluciones. Sin embargo, veremos que este no es el único requerimiento que hace falta para garantizar la existencia o no de soluciones.

En efecto, para poder aplicar el teorema de existencia de soluciones visto en el teórico, todavía es preciso llevar al sistema (6) a la forma

$$\begin{cases} x & \equiv b_1 \ (n_1) \\ x & \equiv b_2 \ (n_2) \end{cases} \tag{7}$$

Una vez que obtenemos dicha transformación, sabemos que (7) admite solución sí y sólo sí $(n_1, n_2) \mid (b_1 - b_2)$. O sea

$$(7) \text{ admite solución} \quad \Leftrightarrow \quad (n_1, n_2) \mid (b_1 - b_2).$$

En dicho caso, la solución será única módulo $[n_1, n_2]$ donde $[a, b]$ denota el mínimo común múltiplo entre los enteros a y b.

Ahora, ¿cómo llevamos el sistema (6) a la forma (7)? Para ello, *es necesario encontrar una solución particular de cada ecuación de (6) por separado*, procediendo como en la sección anterior. Sea entonces x_1 solución particular de la primer ecuación en (6), y sea x_2 una particular de la segunda de ellas. Entonces, se tendrá que (6) es completamente equivalente a (convencerse de esto! es fácil)

$$\begin{cases} x & \equiv x_1 \ (n') \\ x & \equiv x_2 \ (m') \end{cases} \tag{8}$$

O sea, simbólicamente se tiene que

$$\begin{cases} a'x & \equiv b' \ (n') \\ c'x & \equiv d' \ (m') \end{cases} \quad \Leftrightarrow \quad \begin{cases} x & \equiv x_1 \ (n') \\ x & \equiv x_2 \ (m') \end{cases}$$

donde x_1 es una solución de $a'x \equiv b' \ (n')$ y x_2 es una solución de $c'x \equiv d' \ (m')$. Una vez llegados a este punto, resolvemos el nuevo sistema (8) del siguiente modo:

- Primero hallamos todas las soluciones de la primera de las ecuaciones, o sea $x \equiv x_1\ (n')$, las cuales son

$$x = x_1 + n' \cdot k\ :\ k \in \mathbb{Z}. \tag{9}$$

- Luego, restando x_1 en ambos miembros de la segunda ecuación de (8) obtenemos

$$x - x_1 \equiv x_2 - x_1\ (m')\ .$$

  Pero como x debe ser además solución de la primer ecuación, tenemos que $x - x_1 = n' \cdot k$. Reemplazando esto en la congruencia anterior se obtiene

$$n' \cdot k \equiv x_2 - x_1\ (m')\ ,$$

  que es una nueva (y de las conocidas) ecuaciones lineales, pero ahora para la incógnita k. Notamos que dicha ecuación admite solución! Pues $(n', m') \mid (x_2 - x_1)$, condición para la existencia de soluciones de (7)!

- Resolvemos la ecuación anterior para k, procediendo como siempre, es decir, hallando una solución particular k_o y generando todas las soluciones sumando a k_o múltiplos enteros de m', y de este modo obtener

$$k = k_o + m' \cdot z,\ z \in \mathbb{Z}. \tag{10}$$

- Finalmente, reemplazando (10) en (9) llegamos a la solución general del sistema (8), que a su vez coincide con la solución del sistema (6) y por ende del sistema que queríamos resolver originalmente:

$$\mathcal{S} = \{x = x_1 + n' \cdot k_o + n' \cdot m' \cdot z\ :\ z \in \mathbb{Z}\}.$$

Si bien pareciera ser todo muy engorroso, veremos en mediante ejemplos que no es tan terrible.

Nota: Este mismo procedimiento puede aplicarse para resolver sistemas de m ecuaciones mónicas de la forma

$$\begin{cases} x & \equiv b_1\ (n_1) \\ x & \equiv b_1\ (n_2) \\ & \vdots \\ x & \equiv b_m\ (n_m) \end{cases}$$

siempre y cuando nos aseguremos de que exista solución, es decir que $(n_i, n_j) \mid (b_i - b_j)$, para todo par con $i \neq j$.

Finalmente, y como es menester,

Breve procedimiento para lectores ansiosos II:

$$\text{Para resolver} \quad \begin{cases} ax & \equiv b\ (n) \\ cx & \equiv d\ (m) \end{cases}$$

1. Chequear que $(a, n) \mid b$ y $(c, m) \mid d$. Si alguna de dichas condiciones no se cumple, no hay solución del sistema.
2. Si estas condiciones se cumplen, proceder como en **Breve procedimiento para lectores ansiosos I** y hallar una solución particular x_1 de la primera ecuación y otra particular x_2 de la segunda.
3. Si $n' = n/(a, n)$ y $m' = m/(c, m)$, chequear que $(n', m') \mid (x_2 - x_1)$. Si esto no pasa, no hay solución del sistema.
4. Encontrar ahora una solución particular k_o de la ecuación $n' \cdot k \equiv x_2 - x_1\ (m')$.
5. El conjunto de soluciones buscado es $\{x_1 + n'k_o + n'm'z,\ z \in \mathbb{Z}\}$.

2.1 Ejemplo

Hallar todas las soluciones, si existen, del sistema

$$\begin{cases} 6x & \equiv 9\ (15) \\ 15x & \equiv 20\ (35) \end{cases}$$

Solución. Como $(6, 9) = 3 \mid 9$ y $(15, 35) = 5 \mid 20$, podemos coprimizar el sistema, obteniendo

$$\begin{cases} 2x & \equiv 3\ (5) \\ 3x & \equiv 4\ (7) \end{cases}$$

Procediendo como en la sección anterior, es fácil ver que una solución de la primer ecuación es $x_1 = -6$, mientras que una solución de la segunda ecuación es $x_2 = -8$, por lo que el sistema anterior es equivalente a

$$\begin{cases} x & \equiv -6\ (5) \\ x & \equiv -8\ (7) \end{cases}$$

La primera de estas ecuaciones admite como solución general a

$$x = -6 + 5k\ :\ k \in \mathbb{Z}. \tag{11}$$

Sumando 6 ambos miembros de la segunda ecuación $x \equiv -8\ (7)$ se obtiene

$$x + 6 \equiv -8 + 6\ (7),$$

es decir,

$$x + 6 \equiv -2\ (7). \tag{12}$$

Pero como x satisface (11), debe ser $x + 6 = 5k$. Reemplazando esto en (12) se llega a una ecuación para k:

$$5k \equiv -2\ (7),$$

cuyo conjunto completo de soluciones es (resolver!)

$$k = 8 + 7z,\ z \in \mathbb{Z}. \tag{13}$$

Si ahora reemplazamos (13) en (11), finalmente llegamos a la solución general buscada:

$$\mathcal{S} = \{x = 34 + 35z\ :\ z \in \mathbb{Z}\}.$$

Notar que la solución general es única módulo $35 = [5, 7]$, como se esperaba.$\square$