Ecuaciones Diofánticas Lineales y Ecuaciones de Congruencia

Pablo L. De Nápoli

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Álgebra I - Segundo cuatrimestre de 2020

Parte I

Ecuaciones Diofánticas Lineales

Ecuaciones Diofánticas

Una ecuación diofántica es una ecuación en la que interesa encontrar las soluciones enteras (reciben este nombre en honor al matemático Diofanto de Alejandría (siglo III) que las estudió.

Una ecuación diofántica lineal en dos variables es una ecuación de la forma:

$$a \cdot x + b \cdot y = c$$

siendo a, b y c números enteros dados.

Geométricamente, este problema significa que buscamos los puntos en el plano de coordenadas enteras que estén situados sobre una recta.

Criterio para Existencia de soluciones

Teorema (Proposición 5.1.2 del apunte de la profesora Krick)

Llamemos $d = (a : b)$ al máximo común divisor entre los coeficientes a y b. Entonces la ecuación diofántica $a \cdot x + b \cdot y = c$ admite soluciones si y sólo si $d|c$.

La prueba es sencilla: si hay una solución (x, y) entonces

$$d|a \wedge d|b \Rightarrow d|ax \wedge d|by \Rightarrow d|c.$$

Recíprocamente si $d|c$, consideramos $c' = c : d$. Entonces usando el algoritmo de Euclides extendido pordemos encontrar s y t tales que

$$s \cdot a + t \cdot b = d$$

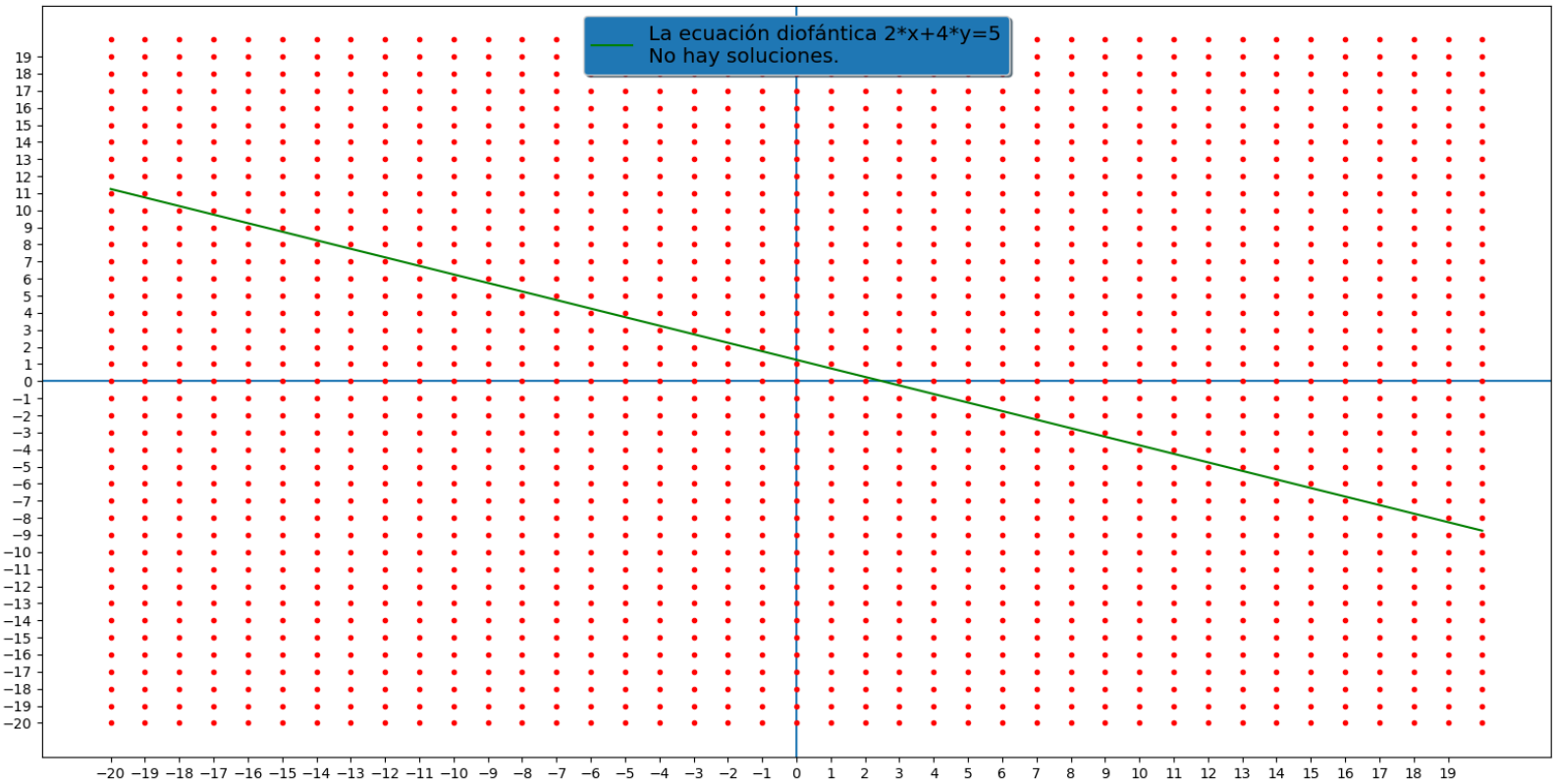
y multiplicando por c' obtenemos:

$$(s \cdot c') \cdot a + (t \cdot c') \cdot b = c$$

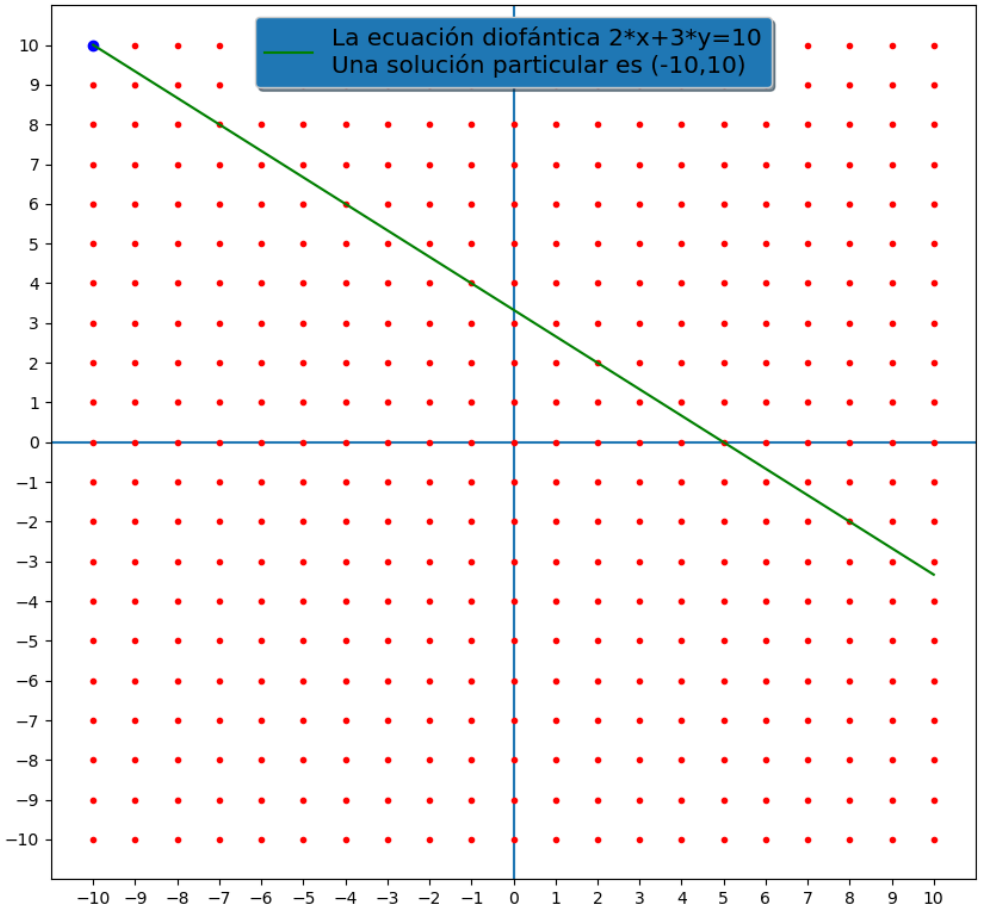
Por lo que $(x_0, y_0) = (s \cdot c', t \cdot c')$ es una solución particular de nuestra ecuación.

Un ejemplo sin soluciones

La ecuación diofántica $2x + 4y = 5$ no tiene soluciones pues en este ejemplo $d = 2$ y d no divide a 5. Esto es evidente en este ejemplo pues si hubiera una solución, el primer miembro sería par mientras que 5 es impar.



Un con soluciones



Aquí $d = 1$ y $s = -1$, $t = 1$.

Dos observaciones clave

- Si estamos en el caso en que $d|c$, llamando $a' = a : d$, $b' = b : d$ (coprimalizando) obtenemos una ecuación equivalente

$$a' \cdot x + b' \cdot y = c'$$

Notemos que ahora a' y b' serán coprimos pues $s \cdot a' + t \cdot b' = 1$.

- Si (x, y) es una solución cualquiera de nuestra ecuación y (x_0, y_0) es la solución particularque encontramos antes

$$a' \cdot (x - x_0) + b' \cdot (y - y_0) = 0$$

así pues la diferencia $(x, y) - (x_0, y_0)$ satisfará la ecuación homogénea (con $c = c' = 0$). Luego: todas las soluciones se obtienen como la suma de una solución particular y una solución de la ecuación homogénea.

Soluciones de la ecuación homogénea

Si tenemos una solución de la ecuación homogénea

$$a' \cdot x + b' \cdot y = 0$$

Podemos escribirla como

$$a' \cdot x = -b' \cdot y$$

Notamos que entonces $b' | a' \cdot x$, pero como $a' \perp b' \Rightarrow b' | x \Rightarrow x = k \cdot b'$. Similarmente $a' | b' \cdot y$, y como $a' \perp b' \Rightarrow a' | y \Rightarrow y = j \cdot a'$. Pero para que se cumpla la ecuación

$$a' \cdot (k \cdot b') + b' \cdot (j \cdot a') = 0$$

debe ser $j = -k$, luego todas las soluciones de la ecuación homogénea son de la forma:

$$(k \cdot b', -k \cdot a')$$

con k entero.

Todas las soluciones

Juntando estas observaciones, podemos completar el enunciado del teorema de la siguiente manera:

Teorema (Proposición 5.1.6 del apunte)

Cuando $d = (a : b) | c$ la ecuación diofántica $a \cdot x + b \cdot y = c$ admite infinitas soluciones. Todas ellas se pueden parametrizarse como

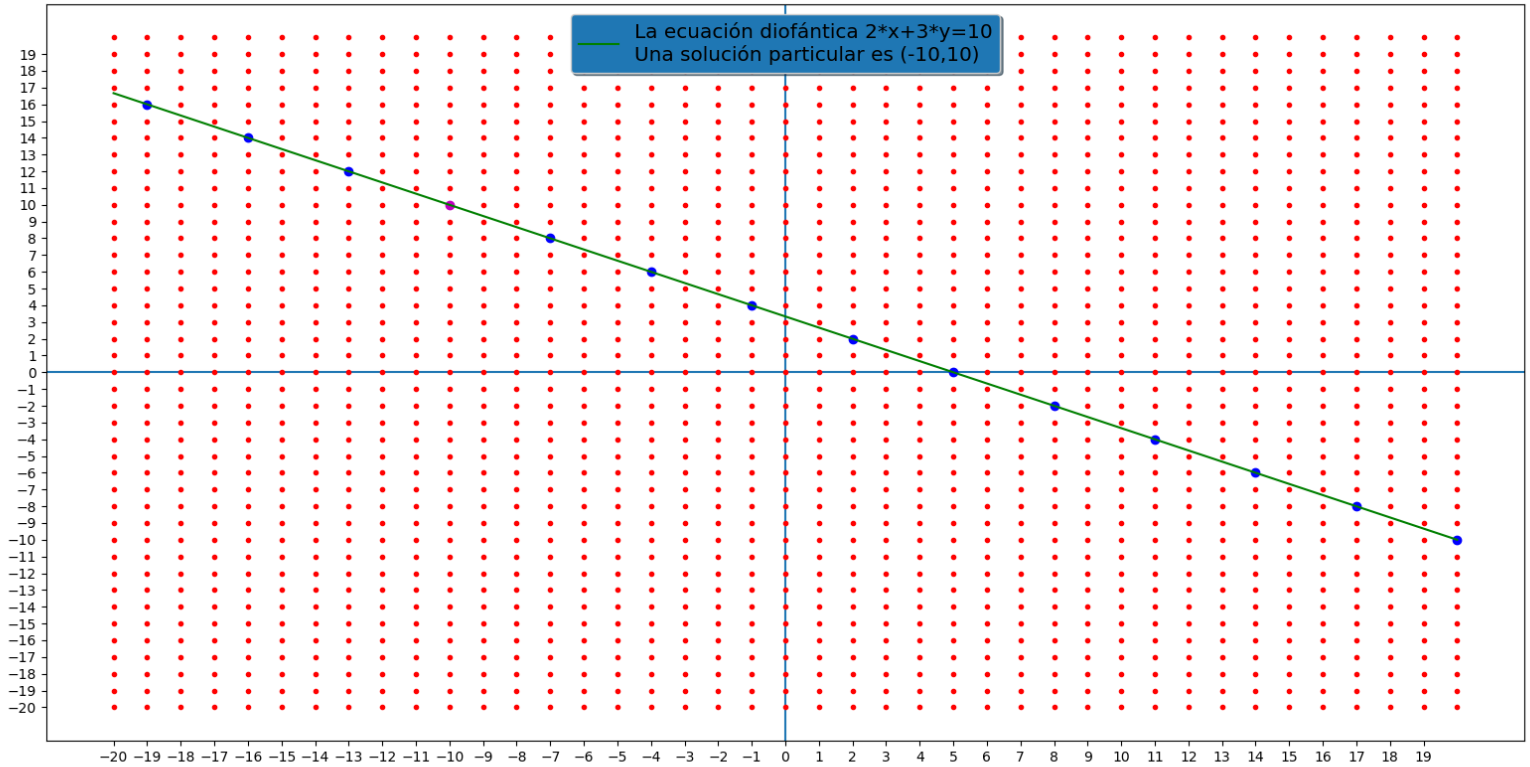
$$\begin{cases} x &= s \cdot c' + k \cdot b' \\ y &= t \cdot c' - k \cdot a' \end{cases} \qquad k \in \mathbb{Z}$$

donde $a' = a : d, b' = b : d, c' = c : d$ y

$$s \cdot a + t \cdot b = d$$

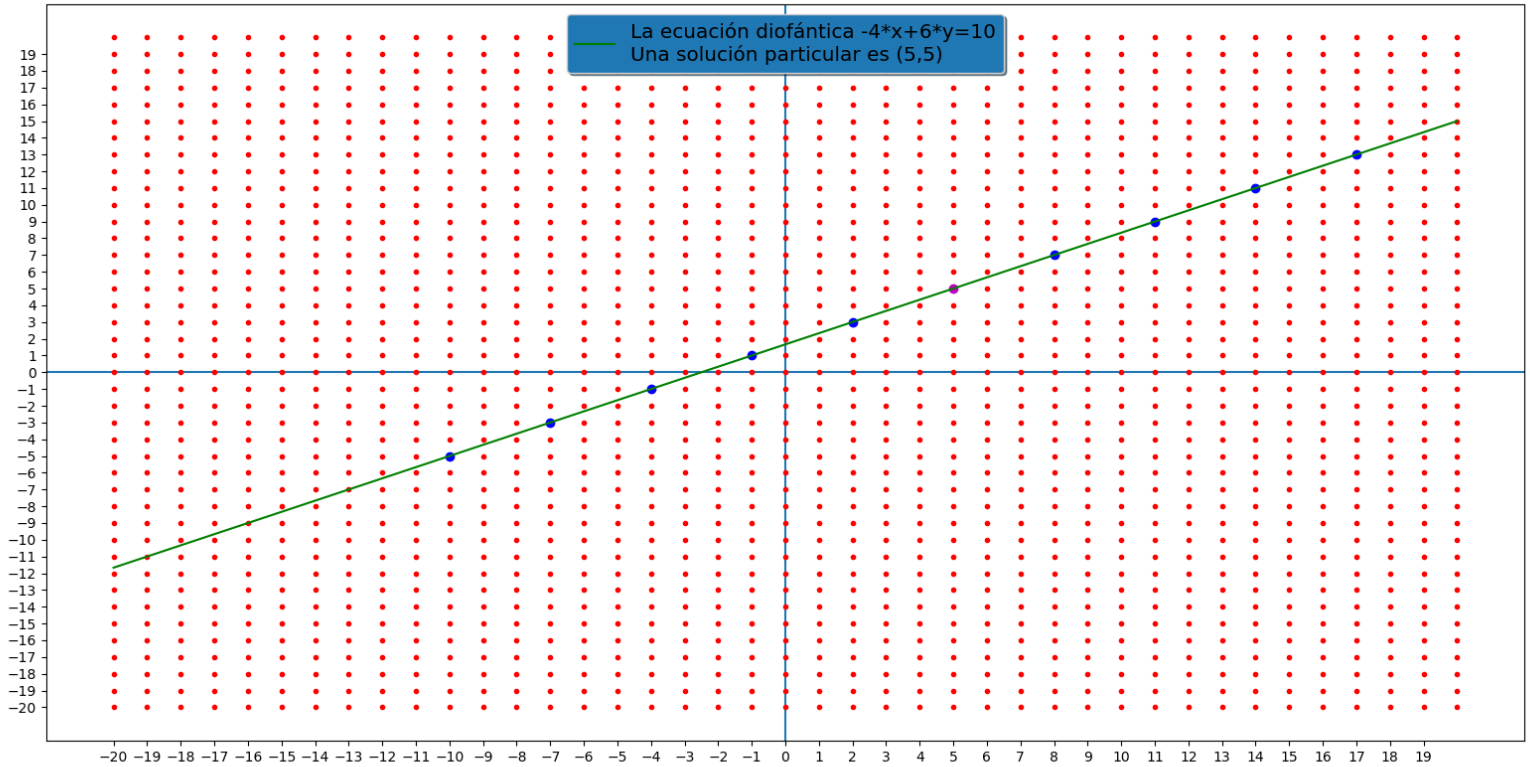
(s y t se encuentran usando el algoritmo de Euclides extendido)

Continuamos el ejemplo de antes..



Aquí $a = a' = 2$, $b = b' = 2$, $c = c' = 10$, $d = 1$, $s = -1$ y $t = 1$. Las soluciones son $(-10 + 3k, 10 + 2k)$ con $k \in \mathbb{Z}$.

Otro ejemplo (con $d = 2$)



Aquí $a - 4, b = 6, c = 10, d = 2, a' = -2, b' = 3, c' = 5, s = -1, t = 1$.
Las soluciones son $(5 + 3k, 5 + 2k)$ con $k \in \mathbb{Z}$.

Algunas cosas para pensar

¿Qué pasa con una ecución diofántica en tres variables?

$$a \cdot x + b \cdot y + c \cdot z = d$$

La noción de máximo común divisor se puede extender a más de dós números, y es una operación asociativa

$$\text{mcd}(a, b, c) = \text{mcd}(\text{mcd}(a, b), c) = \text{mcd}(a, \text{mcd}(b, c))$$

Se deduce que el máximo común divisor de 3 números se puede escribir como una combinación lineal de ellos:

$$\text{mcd}(a, b, c) = s \cdot a + t \cdot b + r \cdot c$$

con s, t, r enteros.
La teoría anterior se puede entonces extender a este caso. La ecuación tendrá solución si y sólo si $\text{mcd}(a, b, c) | d$.

Parte II

Ecuaciones de congruencia lineales

Ecuaciones de congruencia lineales

Un problema íntimamente relacionado con las ecuaciones diofánticas lineales, es la resolución de ecuaciones de congruencia lineales, de la forma:

$$ax \equiv b \pmod{n}$$

Por ejemplo, consideramos la ecuación de congruencia:

$$2x \equiv 3 \pmod{5}$$

Entonces, haciendo una tabla de la función $x \mapsto 2x$ en $\mathbb{Z}_5$ (enteros módulo 5) vemos que la única solución es $x \equiv 4 \pmod{5}$.

$x \pmod 5$	$2x \pmod 5$
0	0
1	2
2	4
3	1
4	3

Puede haber varias soluciones o ninguna

Esta situación, no tiene porqué ocurrir en general: las ecuaciones de congruencia lineales pueden tener varias soluciones o ninguna. Ej; la ecuación

$$2x \equiv 4 \pmod 6$$

posee dos soluciones no congruentes: a saber, $x \equiv 2 \pmod 6$ y $x \equiv 5 \pmod 6$, mientras que la ecución de congruencia

$$2x \equiv 3 \pmod 6$$

no admite ninguna solución.

$x \pmod 6$	$2x \pmod 6$
0	0
1	2
2	4
3	0
4	2
5	4

Reducción a una ecuación diofántica

Obviamente, la resolución de las ecuaciones de congruencia mediante una tabla de restos como hemos hecho en estos ejemplos, sólo resulta practicable cuando el módulo es pequeño. Por ello, resulta deseable desarrollar métodos generales para resolver este problema.
Para ello, observemos que la ecuación de congruencia

$$ax \equiv b \pmod{n}$$

significa que:

$$ax - b = ny \text{ para algún } y \in \mathbb{Z}$$

o sea:

$$ax - ny = b$$

y esta última ecuación, es una ecuación diofántica lineal. Por lo tanto, podemos resolverla por los métodos que vimos antes.

Ejemplo 1

Volvamos a la ecuación de congruencia:

$$2x \equiv 3 \pmod 5$$

Por lo que hemos dicho, esta ecuación significa que:

$$2x - 5y = 3 \text{ para algún } y \in \mathbb{Z} \tag{1}$$

Conforme a la teoría que desarrollamos en la sección anterior, como $\text{mcd}(2, -5) = 1$, esta ecuación admite infinitas soluciones enteras. Para econtrarlas, notamos que 1 se escribe como una combinación lineal de 2 y -5 en la siguiente forma:

$$(-2) \times 2 + (-1) \times (-5) = 1$$

luego

$$(-6) \times 2 + (-3) \times (-5) = 3$$

y por lo tanto: $x_0 = -6$, $y_0 = -3$ es una solución particular de (1).

Ejemplo 1 (continuación)

Todas las soluciones enteras, vendrán entonces dadas por:

$$x = -6 + 5s, \quad y = -3 + 2s$$

En consecuencia, la solución de nuestra ecuación en congruencias será:

$$x \equiv -6 \pmod 5$$

o lo que es equivalente:

$$x \equiv 4 \pmod 5$$

(Notamos que el valor de la variable auxiliar y no interesa al resolver la ecuación de congruencias).

Ejemplo 2

Volvamos a mirar ahora la ecuación de congruencia:

$$2x \equiv 4 (\text{mod } 6)$$

Esta ecuación de congruencia, conduce a la ecuación diofántica lineal:

$$2x - 6y = 4$$

Ahora los coeficientes de la ecuación no son coprimos, por ello dividimos por su máximo común divisor (que es 2), la ecuación:

$$x - 3y = 2$$

Despejando tenemos que,

$$x = 2 + 3y$$

y se obtiene una solución para cada $y \in \mathbb{Z}$.
Por lo tanto, la solucioes se determinan por la condición

$$x \equiv 2 \quad (\text{mód } 3)$$

Ejemplo 2 (continuación)

Nos gustaría expresar esta solución en términos del módulo 6, para ello efectuamos la división entera de y por 2, escribiendo

$$y = 2y' + r$$

donde $r = 0$ o 1. Luego, sustituyendo:

$$x = 2 + 6y' + 3r$$

o sea:

$$x \equiv 2 + 3r \pmod 6$$

Si $r = 0$ obtenemos la solución

$$x \equiv 2 \pmod 6$$

y si $r = 1$ obtenemos la solución:

$$x \equiv 5 \pmod 6$$

que son las que obtuvimos antes.

Ejemplo 3

Finalmente consideremos la ecuación de congruencia:

$$2x \equiv 3 \pmod 6$$

El método anterior conduce a la ecuación diofántica:

$$2x - 6y = 3$$

y como $\text{mcd}(2, 6) = 2$ no divide a 3, concluimos que no existe ninguna solución.

Un teorema general

Teorema

Sean $a, b \in \mathbb{Z}$,$n \in \mathbb{N}$ y $d = mcd(a, n)$. Consideramos la ecuación de congruencia lineal:

$$ax \equiv b \pmod{n}$$

Entonces la ecuación de congruencia lineal admite soluciones si y sólo si $d|b$. En ese caso existen exactamente d soluciones no congruentes módulo n.

Corolario

La ecuación de congruencia lineal:

$$ax \equiv b \pmod{n}$$

tiene solución única si y sólo si $mcd(a, n) = 1$.

Demostración

Como observamos antes, la ecuación de congruencias del enunciado es equivalente a la ecuación diofántica:

$$ax - ny = b \text{ para algún } y \in \mathbb{Z}$$

y esta ecuación tiene solución si y sólo si $d = \text{mcd}(a, n)$ divide a b.
Si esto sucede, llamando $a' = a : d$, $n' = n : d$, $b' = b : d$ y dividiendo por d, obtenemos la ecuación equivalente:

$$a'x - n'y = b'$$

donde ahora a' y b' son coprimos (como en la sección anterior), y todas las soluciones enteras de esta ecuación se pueden expresar en la forma:

$$x = x_0 + n's, \quad y = y_0 - a's \text{ para algún } s \in \mathbb{Z}$$

siendo (x_0, y_0) alguna solución particular. Por lo tanto, x será solución de nuestra ecuación de congruencia, si y sólo si

$$x \equiv x_0 \pmod{n'}$$

Demostración (2)

Para expresar esto en términos del módulo n, como en el ejemplo anterior, efectuamos la división entera de s por d, escribiendo:

$$s = qd + r \text{ con } 0 \leq r < d$$

Entonces, sustituyendo obtenemos

$$x = x_0 + nq + n'r$$

y las soluciones serán

$$x \equiv x_0 + n'r \pmod{n}$$

con $r = 0, 1, 2, \ldots, d - 1$.

Demostración (2)

Finalmente, observemos que estas soluciones no son congruentes módulo n, pues si

$$x \equiv x_0 + n' r_1 \equiv x \equiv x_0 + n' r_2 \pmod{n}$$

entonces

$$n' r_1 \equiv n' r_2 \pmod{n}$$

o sea:

$$n' r_1 - n' r_2 = nk \text{ para algún } k \in \mathbb{Z}$$

Luego multiplicando por d:

$$nr_1 - nr_2 = dnk$$

o sea:

$$r_1 - r_2 = dk$$

o

$$r_1 \equiv r_2 \pmod{d}$$

Pero como $0 \leq r_1, r_2 < d$, concluimos que $r_1 = r_2$.

Otra idea para resolver congruencias lineales

Si tenemos una ecuación lineal con números

$$ax = b$$

(y $a \neq 0$), uno puede obtener la solución multiplicando por el inverso multiplicativo de a, $a^{-1} = \frac{1}{b}$ (lo que equivale a dividir por b), o sea:

$$x = b^{-1}a$$

Como veremos, esta idea puede generalizarse a ecuaciones de congruencia

Inversos Módulo n

El caso $b = 1$ del corolario anterior nos da

Corolario

Sean $a \in \mathbb{Z}$ y $n \in \mathbb{N}$. Si a es coprimo con n entonces existe $\tilde{a}$ (inverso multiplicativo de a módulo n) tal que

$$a \cdot \tilde{a} \equiv 1 \pmod{n}$$

Esta a' es único módulo n (dos soluciones son congruentes módulo n). Recíprocamente si a admite un inverso módulo n, a es coprimo con n.

Ejemplo

Volvamos a mirar la congruencia lineal:

$$2x \equiv 3 \pmod 5$$

Entonces dado que 2 y 5 con coprimos, el 1 se escribe como combinación lineal de ambos:

$$(-2) \times 2 + 1 \times 5 = 1$$

$$\Rightarrow (-2) \times 2 \equiv 1 \pmod 5$$

Es decir que $\overline{2}$ y $\overline{-2} = \overline{3}$ son inversos multiplicativos en $\mathbb{Z}_5$. Entonces, para "pasar dividiendo el 2" en nuestra congruencia lineal, multiplicamos ambos miembros de la congruencia por 3:

$$3 \times 2x \equiv 3 \times 3 \pmod 5$$

y obtenemos nuevamente que: $x \equiv 9 \equiv 4 \pmod 5$.

Parte III

El teorema de Wilson

El teorema de Wilson

Como aplicación de las ideas anteriores, podemos probar el siguiente teorema que proporciona un criterio para saber cuando un número es primo:

Teorema (Teorema de Wilson)

Sea $p \in \mathbb{N}$, $p > 1$. Entonces p es primo si y sólo si p divide a $(p-1)! + 1$, o lo que es equivalente:

$$(p-1)! \equiv -1 \pmod{p}$$

Este teorema aparece en el ejercicio 28 de la práctica 4.

Demostración (1)

Primero probaremos que si p divide a $(p-1)!+1$, entonces p es primo.
Supongamos que por el contrario p no fuera primo, estonces p admitiría un divisor d con $1 < d < p$.
Observemos que entonces $d|(p-1)!$ y como d divide a p, por transitividad también tenemos que $d|(p-1)!+1$. Pero entonces, $d|[(p-1)!+1]-(p-1)!=1$, lo cuál es una contradicción, pues los únicos divisores de 1 son ± 1.
En consecuencia, p debe ser primo.

Demostración (2)

Ahora probemos que si p es primo, entonces $(p-1)! \equiv -1 \pmod{p}$. Para ello observemos que para cada número $1 \leq a < p$, existe un único entero a' con $1 \leq a' < p$ tal que:

$$aa' \equiv 1 \pmod{p}$$

es decir, tal que a' y a son inversos módulo p.
Notamos además que debe ser $a \neq a'$, salvo si $a = 1$ o $a = p-1$. En efecto: si $a = a'$, entonces

$$a^2 \equiv 1 \pmod{p}$$

o también

$$a^2 - 1 \equiv 0 \pmod{p}$$

Factorizando, podemos escribir esto como:

$$(a-1)(a+1) \equiv 0 \pmod{p}$$

pero como a es primo deducimos que:

$$a \equiv 1 \pmod{p} \quad \text{o} \quad a \equiv -1 \pmod{p}$$

Demostración (3)

Entonces, para calcular $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$ módulo p, agrupamos cada factor con su inverso multiplicativo (usando las propiedades asociativa y conmutativa del producto), y resulta:

$$(p-1)! \equiv (p-1) \equiv -1 \pmod{p}$$

Ejemplo

Para mostrar como funciona el proceso de agrupar cada número con su inverso multiplicativo módulo p, veamos un ejemplo.
Sea $p = 7$. Entonces, tenemos la siguiente tabla de inversos módulo 7:

a	a'
1	1
2	4
3	5
4	2
5	3
6	6

Entonces:

$$(p-1)! = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv 6 \equiv -1 \pmod 7$$