Introducción a las ecuaciones diofánticas

¿Cómo se define una Ecuación Diofántica? ¿Cómo se resuelve? ¿Siempre tendrá solución? ¿Hay diferentes tipos de ecuaciones diofánticas?

Comenzaremos por lo tanto ofreciendo una definición y las características principales de las Ecuaciones Diofánticas.

Caracterización de las Ecuaciones Diofánticas

Para comenzar el estudio de las Ecuaciones Diofánticas, le sugerimos reflexionar sobre el siguiente problema.

"Un cajero automático dispone solamente de billetes de 20 y 50 pesos. Un cliente quiere retirar $ 430 de su cuenta. ¿Podrá hacerlo de ese cajero? Si pudiera, ¿cuántos billetes de 20 pesos y cuántos de 50 le daría? ¿Existe para este problema una única respuesta?"

La ecuación relacionada con el problema anterior es $20x + 50y = 430$. Se trata de una **ecuación lineal con dos incógnitas y coeficientes enteros**, de la que sólo nos interesan las **soluciones naturales**.

Las **ecuaciones lineales** con **coeficientes enteros** que exigen **soluciones enteras** se denominan **Ecuaciones Lineales Diofánticas** o **Diofantinas**. En general, cualquier ecuación con coeficientes enteros y soluciones enteras es una Ecuación Diofántica. Dichas ecuaciones reciben su nombre en honor a **Diofanto**, matemático griego que trabajó en Alejandría a mediados del siglo III A.C. Fue uno de los primeros en introducir la notación simbólica en matemáticas y escribió seis libros sobre problemas en los que consideraba la representación de números como suma de cuadrados.

Algoritmo de la División Entera

¿Cuándo un número entero divide a otro? ¿Qué es el Algoritmo de la División Entera? ¿Cuáles son las propiedades fundamentales que derivan de estas definiciones?

Comencemos con la definición de la **relación de la División Entera**, pilar fundamental en la aritmética de los números enteros:

Sean a **y** b dos números enteros tales que $a \neq 0$. Diremos que **a divide a b** si existe un número entero q tal que $b = a \cdot q$.
Suele notarse $a|b$, es decir, $a|b \Leftrightarrow \exists q \in Z \; b = a \cdot q$

Expresiones equivalentes a "a divide a b" son "a es un divisor de b", "b es múltiplo de a" o "b es divisible por a".

Ejemplos:

1) 2 divide a 12 ya que $12 = 2 \times 6$, y 6 es entero. En símbolos, $2|12\ porque\ \exists 6 \in Z\ tal\ que\ 12 = 2 \times 6$

2) 2 no divide a 13 ya que no existe ningún número entero q tal que $13 = 2 \times q$

Teorema de Bezout:

Si a y b ϵ Z (no ambos nulos) y d =(a, b), entonces existen enteros x e y tales que
$d = ax + by$.

Es decir, el Máximo Común Divisor de dos números enteros es una combinación lineal entera de dichos números.

Definición:

Dos enteros a y b se llaman **coprimos** si, y sólo si, su Máximo Común Divisor es 1.

Utilizando la definición anterior, obtenemos un corolario del Teorema de Bezout, que enunciamos a continuación, y que va a ser utilizado en la búsqueda de soluciones de las Ecuaciones Lineales Diofánticas.

Corolario:

Dos enteros a y b son coprimos si, y sólo si, existen enteros x e y tales que
$1 = ax + by$.

Propiedad:

Si (a,b) = d, entonces $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Propiedad:

Si $(a, b) = 1\ \ y\ \ b|a\ q\ \ con\ q \in Z$ entonces $b|q$.

Existencia de soluciones y resolución de Ecuaciones Lineales Diofánticas

TEOREMA:

Sean $a, b, c \in Z$, $a \neq 0$, $b \neq 0$, y sea d el Máximo Común Divisor de a y b. Llamamos $d = (a, b)$. La Ecuación Lineal Diofántica $ax + by = c$ admite soluciones enteras si y sólo si d divide a c (en símbolos,$d|c$).

DEMOSTRACIÓN DEL TEOREMA:

"Sólo si":

Supongamos que los enteros x_0 e y_0 son solución de la ecuación $ax + by = c$.

Entonces $ax_0 + by_0 = c$.

Además, si $d = (a, b)$ entonces:

$d|a \ \wedge \ d|b$ ¿*Por qué*? (1)

$\Rightarrow d|ax_0 + by_0$ ¿*Por qué*? (2)

$\Rightarrow d|c$ ¿*Por qué*? (3)

"Si":

Recíprocamente, supongamos que $d = (a, b)$ divide a c. Entonces:

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \quad \text{¿Por qué?} \quad (4)$$

$$\Rightarrow \exists\, s, t \in Z : \frac{a}{d}s + \frac{b}{d}t = 1 \quad \text{¿Por qué?} \ (5)$$

$$\Rightarrow a\frac{cs}{d} + b\frac{ct}{d} = c \quad \text{¿Por qué?} \quad (6)$$

Basta tomar
$x_0 = \frac{cs}{d}$ e $y_0 = \frac{ct}{d}$ ¿Por qué x_0 e y_o son números enteros? (7)

y resulta que $ax_0 + by_0 = c$.

Es decir, x_0 e $y_o$son soluciones de la ecuación $ax + by = c$.

Solución general

TEOREMA:

Sean $a, b, c \in Z$, $a \neq 0$, $b \neq 0$ tales que el máximo común divisor d de a y b divide a c. Entonces la solución general de la ecuación lineal diofántica $ax + by = c$ es

$$x = x_0 + \frac{b}{d} \cdot k \qquad y = y_0 - \frac{a}{d} \cdot k \qquad , \ k \in Z$$

donde x_0 e y_0 es una solución particular de la misma.

DEMOSTRACIÓN DEL TEOREMA:

Por hipótesis, d divide a c. Luego, el teorema 1.2.1.1. asegura la existencia de una solución particular $x = x_0 \ e \ y = y_o$. Entonces, $ax_0 + by_0 = c$.

Dividiendo ambos miembros de la ecuación por d, resulta

$$\frac{a}{d} x_0 + \frac{b}{d} y_0 = \frac{c}{d}$$

Obsérvese que $\frac{c}{d}$ es un número entero ya que d divide a c , y que por la propiedad anterior, $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Además, como 1 divide a $\frac{c}{d}$, el teorema anterior asegura la existencia de una solución particular de la ecuación

$$\frac{a}{d} x_0 + \frac{b}{d} y_0 = \frac{c}{d}$$

Sea $x = x_1 \ e \ y = y_1$ tal solución. Luego, podemos escribir

$$\frac{a}{d} x_1 + \frac{b}{d} y_1 = \frac{c}{d}$$

Entonces, de

$$\begin{cases} \frac{a}{d} x_1 + \frac{b}{d} y_1 = \frac{c}{d} \\ \frac{a}{d} x_0 + \frac{b}{d} y_0 = \frac{c}{d} \end{cases}$$

se obtiene

$$\frac{a}{d}(x_1 - x_0) + \frac{b}{d}(y_1 - y_0) = 0$$

Luego,

$$\frac{a}{d}(x_1 - x_0) = \frac{b}{d}(y_0 - y_1)$$

$$\Leftrightarrow \frac{b}{d} \mid \frac{a}{d}(x_1 - x_0)$$

Como $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, por propiedad., $\frac{b}{d} \mid (x_1 - x_0)$.

$$\exists k \in Z \; tal \; que \; x_1 - x_0 = \frac{b}{d} \cdot k$$

Luego,

$$x_1 = x_0 + \frac{b}{d} \cdot k$$

Para obtener el valor de y_1, sustituiremos el valor de x_1 recién hallado en la ecuación

$$\frac{a}{d}(x_1 - x_0) + \frac{b}{d}(y_1 - y_0) = 0$$

y resulta

$$\frac{a}{d}\left(x_0 + k.\frac{b}{d} - x_0\right) + \frac{b}{d}(y_1 - y_0) = 0$$

Entonces,

$$\frac{a}{d}\left(k.\frac{b}{d}\right) + \frac{b}{d}(y_1 - y_0) = 0$$

$$\Rightarrow \frac{b}{d}\left(\frac{a}{d} \cdot k + y_1 - y_0\right) = 0$$

$$\Rightarrow \frac{a}{d} \cdot k + y_1 - y_0 = 0$$

Por lo tanto,

$$y_1 = y_0 - \frac{a}{d} \cdot k$$

Luego, la solución general de la ecuación lineal diofántica $ax + by = c$ es

$$x = x_0 + \frac{b}{d} \cdot k \qquad e \qquad y = y_0 - \frac{a}{d} \cdot k \qquad , \quad k \in Z$$

Desarrollo de un ejemplo

Resolver la ecuación diofántica 234x + 126y = 36.

Como (234,126) = 18 |36, la ecuación tiene solución.

Busquemos la solución particular.

$$18 = 126 - 108 \times 1$$

Pero $108 = 234 - 126 \times 1$. Entonces, reemplazando 108 en la igualdad anterior:

$$18 = 126 - (234 - 126 \times 1) \times 1$$

Aplicando propiedad distributiva, $18 = 126 - 234 \times 1 + 126 \times 1$

Sacando a 126 como factor común, $18 = 2 \times 126 - 1 \times 234$

Multiplicando ambos miembros por 2, para obtener c = 36:

$$(-1) \times 2 \times 234 + 2 \times 2 \times 126 = 18 \times 2$$

$$(-2) \times 234 + 4 \times 126 = 36$$

Por lo que resulta que $x_0 = -2 \quad e \quad y_0 = 4$.

Hallemos ahora la solución general. Las soluciones particulares de esta ecuación eran $x_0 = -2 \quad e \quad y_0 = 4$, y el máximo común divisor 18. Por lo tanto, las soluciones generales están dadas por las fórmulas:

$$\boxed{y = y_0 - \frac{a}{d} \cdot k \quad , k \in Z x = x_0 + \frac{b}{d} \cdot k \quad , k \in Z}$$

$$y = 4 - \frac{234}{18} \cdot k \quad , k \in Z . x = -2 + \frac{126}{18} \cdot k \quad , k \in Z$$

Luego, e

Es decir,
$y = 4 - 13 \cdot k \quad , k \in Z x = -2 + 7 \cdot k \quad , k \in Z$ e

son todas las soluciones de la Ecuación Lineal Diofántica 234x + 126y = 36.

Veamos algunas de ellas, reemplazando el valor de k por cualquier número entero.

Con $k = 1, \quad x = 5 \quad e \quad y = -9.$

Con $k = -1, \quad x = -9 \quad e \quad y = 17.$

Con $k = 2, \quad x = 12 \quad e \quad y = -22.$

Las ecuaciones en congruencia

Resolución de ecuaciones en congruencias transformándolas en ecuaciones diofánticas

Una ecuación de congruencia se puede transformar en una ecuación diofántica, de la que sólo nos van a interesar las soluciones incongruentes de x.

TEOREMA

La ecuación en congruencias $a\,x \equiv b\,(m)$ tiene solución entera x si, y sólo si, $(a, m) \mid b$.

DEMOSTRACIÓN DEL TEOREMA

Por definición de congruencia, $ax \equiv b\,(m) \Leftrightarrow m \mid ax - b$. Luego, por definición de divisibilidad, $\exists q \in Z: ax - b = m \cdot q \Leftrightarrow ax - mq = b$.

$ax - mq = b$ es una ecuación diofántica, y por el teorema de la unidad 1 tiene solución si, y sólo si, $(a,m) \mid$ b , que es lo que queríamos demostrar.

En tal caso tiene d $= (a,m)$ soluciones incongruentes módulo m, y son de la forma:

$$x_k = x_0 + \frac{m}{d} \cdot k\,, \qquad k = 0,1,\ldots,d-1$$

Ejemplo:

$10x \equiv 2\ (22)$ tiene 2 soluciones incongruentes módulo 22, ya que $(10,22)=2 \mid 2$ y son $x_0 = 9 \;\; y \;\; x_1 = 20$

EJERCICIOS:

1) Hallar, si existen, las soluciones generales diofánticas (o enteras) de las siguientes ecuaciones:

a) $25x + 35y = 105$ b) $234x - 126y = 36$ c) $115x + 23y = 1$
d) $2x + 6y = 7$ e) $5x + 3y = 8$ f) $110x - 97y = 1042$

2) Hallar. si existen, todas las soluciones incongruentes entre sí de las ecuaciones:

a) $8x \equiv 15\ (9)$ b) $8x \equiv 15\ (6)$ c) $10x \equiv 25\ (5)$

d) $21x \equiv 20\ (7)$ e) $116x \equiv 10\ (14)$ f) $15x \equiv 5\ (25)$

g) $27x \equiv 54\ (12)$ h) $5x \equiv 12\ (13)$