ECUACIONES DIOFÁNTICAS

Definición

Sean $a, b, c, x, y \in \mathbb{Z}$. Llamaremos ecuación diofántica a la expresión:

$$ax + by = c$$

¿Cuándo tiene solución una ecuación diofántica?
No siempre tiene solución.
Ejemplo:

$6x + 8y = 3$ no tiene solución como ecuación diofántica, es decir, no existen $x, y \in \mathbb{Z}$ que verifiquen la igualdad.

$$6x + 8y = \underbrace{2(3x + 4y)}_{N^o \text{ par.}} \neq 3$$

Una ecuación diofántica tendrá solución si y sólo si $mcd(a,b)$ divide a c.

Ejemplo. Calcular $x, y \in \mathbb{Z}$ tales que

debemos asegurarnos de que tienen solución.
Para ello vamos a calcular mcd(4763, 1567) aplicando el algoritmo de Euclides

$$4763 = 1567 \cdot 3 + 62 \longrightarrow 62 = 4763 - 1567 \cdot 3$$
$$1567 = 62 \cdot 25 + 17 \longrightarrow 17 = 1567 - 62 \cdot 25$$
$$62 = 17 \cdot 3 + 11 \longrightarrow 11 = 62 - 17 \cdot 3$$
$$17 = 11 \cdot 1 + 6 \longrightarrow 6 = 17 - 11$$
$$11 = 6 \cdot 1 + 5 \longrightarrow 5 = 11 - 6$$
$$6 = 5 \cdot 1 + \boxed{1} \longrightarrow 1 = 6 - 5$$
$$5 = 1 \cdot 5 + 0$$

$$1 = 6 - 5 = 6 - (11 - 6) = 6 \cdot 2 - 11 = (17 - 11) \cdot 2 - 11 =$$
$$= 17 \cdot 2 - 11 \cdot 3 = 17 \cdot 2 - (62 - 17 \cdot 3) \cdot 3 = 17 \cdot 2 - 62 \cdot 3 + 17 \cdot 9 =$$
$$= 17 \cdot 11 - 62 \cdot 3 = (1567 - 62 \cdot 25) \cdot 11 - 62 \cdot 3 =$$
$$= 1567 \cdot 11 - 62 \cdot 275 - 62 \cdot 3 = 1567 \cdot 11 - 62 \cdot 278 =$$
$$= 1567 \cdot 11 - (4763 - 1567 \cdot 3) \cdot 278 = 1567 \cdot 11 - 4763 \cdot 278$$
$$+ 1567 \cdot 834 = 1567 (845) + 4763 (-278)$$

Entonces $1567 \cdot \underbrace{(845)}_{x_0} + 4763 \cdot \underbrace{(-278)}_{y_0} = 1$

Multiplicando la expresión anterior por 7:

Las ecuaciones diofánticas no tienen solución única.

Supongamos que tenemos una solución $x_0, y_0 \in \mathbb{Z}$ de la ecuación

$$ax + by = c$$

Consideremos $K \in \mathbb{Z}$ y $d = mcd(a,b)$

$$ax + by + \frac{ab}{d}K - \frac{ab}{d}K = c$$

$$a\underbrace{\left(x + \frac{b}{d}K\right)}_{x_K} + b\underbrace{\left(y - \frac{a}{d}K\right)}_{y_K} = c$$

Observamos que $x_K = x + \frac{b}{d}K$ e $y_K = y - \frac{a}{d}K$ son solución de mi ecuación inicial.

<u>Ejemplo.</u>

Calcular todas las soluciones de la ecuación

$$1567x + 4763y = 7$$

Ya sabemos que $x = 5915,\ y = -1946$ es una

$$x_k = 5915 - 4763 \cdot k \quad , \quad y_k = -1946 + 1567 \cdot k$$

con $k \in \mathbb{Z}$.

Son todas las soluciones a la ecuación diofántica.

Ejemplo.

Un cajero automático dispone de billetes de 20 y 50 euros. ¿Se pueden sacar 430 euros? En caso afirmativo ¿de cuántas formas posibles?

Si $x \equiv$ nº billetes de 20€ , $y \equiv$ nº billetes de 50€

$$20x + 50y = 430.$$

¿Tiene solución la ecuación? Debemos estudiar si $mcd(20,50) = 10$ divide a 430.

Claramente 10 divide a 430, entonces sí tiene solución.

Para resolver la ecuación debemos recurrir al algoritmo de Euclides:

$$50 = 20 \cdot 2 + \boxed{10} \rightarrow 10 = 50 - 20 \cdot 2$$

$$20 = 10 \cdot 2 + 0$$

$$50\cdot \underbrace{43}_{y_0} + 20(\underbrace{-86}_{x_0}) = 430$$

$x_0 = -86$ e $y_0 = 43$ es solución de la ecuación pero no del problema. Las soluciones válidas para el problema son las positivas.

La solución general es:

$$x_K = -86 + \frac{50}{10}K \quad , \quad y_K = 43 - \frac{20}{10}K$$

$$x_K = -86 + 5K \quad , \quad y_K = 43 - 2K$$

El primer valor de $K \in \mathbb{Z}$ que hace positivo a x_K es $K=18$: $x_{18} = -86+90 = 4$, $y_{18} = 43-36 = 7$

$K=19$: $x_{19} = 9$, $y_{19} = 5$

$K=20$: $x_{20} = 14$, $y_{20} = 3$

$K=21$: $x_{21} = 19$, $y_{21} = 1$

Entonces hay sólo cuatro formas de retirar 430€ en billetes de 20 y 50.

Ejercicio: He comprado entre 50 y 100 artículos a 17€. He vendido unos cuantos por 49 euros

Ejercicio: Un billete de avión vale 700, 550 ó 390 euros según se viaje en primera, negocio ó turista. Si un vuelo de 69 pasajeros ha recaudado 32.740€. ¿Cuántos billetes de cada clase volaron?

CONGRUENCIAS

Recordamos que una relación de equivalencia sobre un conjunto X es una relación "$\equiv$" que verifica:

1) Reflexiva: $a \equiv a \quad \forall a \in X$.
2) Simétrica: $a \equiv b \Rightarrow b \equiv a \quad \forall a, b \in X$.
3) Transitiva: $a \equiv b$ y $b \equiv c \Rightarrow a \equiv c \quad \forall a, b, c \in X$.

Se llama clase de equivalencia de $a \in X$:

$$[a] = \{ b \in X \mid a \equiv b \}$$ (etiquetas)

y el conjunto cociente a:

$$X/_{\equiv} = \{ [a] \mid a \in X \}$$ (Todas las etiquetas)

Intuitivamente una relación de equivalencia

Ejemplo:

Consideramos un conjunto de 12 lápices:

$X = \{1,2,3,4,5,6,7,8,9,10,11,12\}$

Relación de equivalencia: Colores $(\equiv)$

$X/_{\equiv} = \{$ Verde, Azul, Morado $\}$

Verde $= \{1,2,3,4,5\}$ Azul $= \{6,7,8,9\}$

Morado $= \{10,11,12\}$

$[6] = [7] = [8] = [9] \neq [11] \neq [3]$

Definición

Sea $m \in \mathbb{N}$. Se define la relación de congruencia módulo m a la relación de equivalencia sobre $\mathbb{Z}$:

$a \equiv_m b \ (\text{mód } m) \iff \begin{cases} \cdot\ a - b = k \cdot m \text{ con } k \in \mathbb{Z}. \\ \cdot \text{ Si el resto de dividir } a \text{ y } b \\ \text{ entre } m \text{ coinciden.} \end{cases}$

$[a]_m = [b]_m$

Al conjunto cociente lo denotamos por $\mathbb{Z}/_{\equiv_m} \simeq \mathbb{Z}_m$

Ejemplo

Calcular $\mathbb{Z}_4$:

- $[0]_4 = [4]_4 = [8]_4 = [12]_4 = \dots = 4k$
- $[1]_4 = [5]_4 = [9]_4 = [-3]_4 = 1 + 4k$
- $[2]_4 = [6]_4 = [10]_4 = [-2]_4 = 2 + 4k$
- $[3]_4 = [7]_4 = [11]_4 = [-1]_4 = 3 + 4k$

$$\mathbb{Z}_4 = \{ [0]_4 , [1]_4 , [2]_4 , [3]_4 \}$$

Ejercicio: Calcular $\mathbb{Z}_m$.