Ecuaciones Diofanticas Lineales

Sean a, b, c enteros y $ab \neq 0$, toda ecuación de la forma

$$ax + by = c$$

donde x e y son números enteros, se dice que es una ecuación diofantica lineal en dos variables.

Ejm. Resuelva la ecuación

$$11x + 27y = 4$$

Sol.

Por el algoritmo de Euclides

$$27 = 2 \cdot 11 + 5 \quad (2)$$
$$11 = 2 \cdot 5 + 1 \quad (1)$$
$$5 = 5 \cdot 1 + 0$$

$\Rightarrow (27, 11) = 1$

De donde, de (1) despejamos 1. / $5 = 27 + (-2) \cdot 11$

$$1 = 11 + (-2) \cdot 5$$

$$1 = 11 + (-2)\big(27 + (-2) 11\big)$$

$$1 = 11 + (-2) 27 + 4 \cdot 11$$

$$1 = 5 \cdot 11 + (-2) \cdot 27$$

Así $\quad 11(5) + 27(-2) = 1 \quad // \, 4$

$$\boxed{11(20) + 27(-8) = 4}$$

$$x = 20, \quad y = -8 \in \mathbb{Z}$$

Teorema. Toda ecuación diofantica lineal

$$ax + by = c$$

tiene solución si solo si $g \mid c$, donde $g=(a,b)$

Ejm. Si $2x+4y=7$, existe x, y enteros?

Sol. Como $(2,4)=2$ y $2 \nmid 7$, entonces la ec. no tiene solución.

Teorema Si $g=(a,b)$, $g \mid c$ y x_0 e y_0 es una solución particular de la ecuación diofántica lineal

$$ax+by=c$$

entonces toda solución x e y está dado por las ecuaciones

$$\boxed{x = x_0 + \frac{b}{g}t}, \quad \boxed{y = y_0 - \frac{a}{g}t}, \quad t \in \mathbb{Z}.$$

Ejm. En la ec. $\boxed{11x+27y=4}$, se tiene la solución particular

$x_0=20$, $y_0=-8$ $\quad (g=1,\ a=11,\ b=27)$

de donde la solución general sería.

$$x = x_0 + \frac{b}{g}t \qquad y = y_0 - \frac{a}{g}t$$

$$\boxed{x = 20 + 27 \cdot t} \qquad \boxed{y = -8 - 11 \cdot t}, \quad t \in \mathbb{Z}$$

si $\boxed{t=3}$, $x=101$, $y=-41$

$$11(101)+27(-41)=4$$

Ejm. Determina todas las soluciones de la ec. diofántica lineal.

i) $14x+22y=50$ $\qquad$ ii) $39x+26y=105$

Sol. i) Como $(14,22)=2$ y $2 \mid 50$

entonces la ec. tiene solución.

Luego por el alg. de Euclides

$$22 = (1)\,14 + 8 \qquad ③ \qquad 8 = 22 - 1\cdot 14$$
$$14 = (1)\,8 + 6 \qquad ② \qquad 6 = 14 - 1\cdot 8$$
$$8 = (1)\,6 + 2 \qquad ① \qquad 2 = 8 - 1\cdot 6$$
$$6 = (3)\,2 + 0$$

$$2 = 8 - 1\cdot(14 - 1\cdot 8)$$
$$2 = 8 - 1\cdot 14 + 1\cdot 8$$
$$2 = 2\cdot 8 - 1\cdot 14$$
$$2 = 2(22 - 1\cdot 14) - 1\cdot 14$$
$$2 = 2\cdot 22 - 2\cdot 14 - 1\cdot 14$$
$$2 = 2\cdot 22 - 3\cdot 14$$

$$14x + 22y =$$

Así $\quad 14(-3) + 22(2) = 2 \qquad /\!/ \cdot 25$

$$\boxed{14(-75) + 22(50) = 50}$$

De donde $\quad x_0 = -75 \qquad y_0 = 50$

y la solución general $\quad x = x_0 + \frac{b}{g}t \quad , \quad y = y_0 - \frac{a}{g}t \quad , t \in \mathbb{Z}$

$$x = -75 + \frac{22}{2}t \qquad y = 50 - \frac{14}{2}t \quad , t \in \mathbb{Z}$$

$$\boxed{x = -75 + 11t \quad , \quad y = 50 - 7t \quad , t \in \mathbb{Z}}$$

Congruencias

Se dice que a es congruente a b, módulo n, si $a - b = n\cdot k$.

o $\quad n \mid a-b$

Definición. Si a, b, n son enteros, con $n > 0$, a es congruente con b módulo n sii $a - b = n\cdot k$, $k \in \mathbb{Z}$.

y escribimos. $\qquad a \equiv b \pmod{n}$

Si $n \nmid a-b$, diremos que a no es congruente a b módulo n.

$$a \not\equiv b \pmod{n}$$

Ejm. Determine si cada proposición es V o F.

a) $7 \equiv 2 \pmod{5}$ [V] $\quad 5 \mid 7-2 \quad$ o $\quad 7-2 = 5 \cdot \boxed{1}$

b) $16 \equiv 9 \pmod{4}$ F $\quad 4 \nmid 16-9$

c) $15 \equiv 3 \pmod{4}$ V

d) $7 \equiv -4 \pmod{3}$ F $\quad 3 \nmid 11$

e) $2 \equiv 2 \pmod{7}$ V $\quad \boxed{17 \equiv 9}\ \boxed{(\text{mod } 2)}$

f) $17 \not\equiv 9 \pmod{2}$ F $\quad \equiv \quad =$

g) $x \equiv 3 \pmod{5}$ $\quad x = 8$, V

Teorema La relación de congruencia módulo n, $n > 0$; es una relación de equivalencia en el conjunto de enteros. Es decir.

i) Reflexiva. $\quad a \equiv a \pmod{n}$

ii) Simétrica $\quad a \equiv b \pmod{n}$ entonces $b \equiv a \pmod{n}$

iii) Transitiva $\quad a \equiv b \pmod{n} \wedge b \equiv c \pmod{n}$ entonces

$$a \equiv c \pmod{n}$$

Teoremas sobre congruencias

T.1. Si $a \equiv b \pmod{n}$ y $c \in \mathbb{Z}$ entonces

$$a + c \equiv b + c \pmod{n}$$

T2. Si $a \equiv b \ (\text{mód } n)$ y $c \in \mathbb{Z}$, entonces

$ac \equiv bc \ (\text{mód } n)$

T3. Si $a \equiv b \ (\text{mód } n)$ y $c \equiv d \ (\text{mód } n)$ entonces

$a + c \equiv b + d \ (\text{mod } n)$

T4. Si $a \equiv b \ (\text{mód } n)$ y $c \equiv d \ (\text{mód } n)$ entonces

$a - c \equiv b - d \ (\text{mod } n)$

T5. Si $a \equiv b \ (\text{mód } n)$ y $c \equiv d \ (\text{mód } n)$ entonces

$ac \equiv bd \ (\text{mód } n)$

T6. Si $a \equiv b \ (\text{mód } n)$ y $n \in \mathbb{Z}^+$ entonces

$a^n \equiv b^n \ (\text{mod } n)$

T7. Si $a \equiv b \ (\text{mod } n)$, $c \equiv d \ (\text{mod } n)$ y $r, s \in \mathbb{Z}$ entonces

$ar + cs \equiv br + ds \ (\text{mód } n)$

Encontrar el resto de dividir 2^{30} por 15

$$\begin{array}{l|l} 2^{30} & 15 \\ \hline (r) & \end{array}$$