

Módulo: Teoría de Números

Sistemas Numéricos Referenciales

RONALD MANRÍQUEZ
HÉCTOR LORCA

Índice general

Introducción	3
1. Máximo Común Divisor (<i>M.C.D.</i>)	4
1.1. Máximo Común Divisor	4
1.2. Algoritmo de la División	4
1.3. Ejercicios Resueltos	5
2. Congruencias Lineales	9
2.1. Conceptos Fundamentales	9
2.2. Propiedades de las Congruencias	10
2.3. Teoremas de Euler y Fermat	10
2.4. Ejercicios Resueltos	11
2.4.1. Ejercicios Propuestos	19
3. Ecuaciones Diofánticas	20
3.1. Ecuaciones Diofánticas	20
3.2. Ejercicios Resueltos	20
3.2.1. Ejercicios Propuestos	34
Bibliografía	35

Introducción

Estos apuntes son elaborados para el curso de *Sistemas Numéricos Referenciales*, de la carrera de Pedagogía en Matemática, de la Universidad de Playa Ancha.

El objetivo de este módulo, es facilitar el aprendizaje de los tópicos relacionados a Teoría de números, en particular, conceptos asociados a el Máximo común Divisor, congruencias lineales y ecuaciones diofánticas. Considerando definiciones esenciales y más de 50 ejercicios resueltos.

Cabe mencionar que la creación de este material nace de la necesidad y la falta de referencias bibliográficas que permitan ver ejercicios resueltos en el área. Si bien existen textos que contienen los tópicos, ninguno de ellos posee tal cantidad de problemas resueltos.

Mayo de 2022

Capítulo 1

Máximo Común Divisor (*M.C.D.*)

1.1. Máximo Común Divisor

Definición 1. *Dado un dominio euclidiano, diremos que un entero positivo d es el M.C.D. entre los enteros a y b , Sí cumple que:*

- i) $d \mid a \quad \wedge \quad d \mid b$*
- ii) Sí $\exists \quad c \in \mathbb{Z}^+$ tal que $c \mid a \quad \wedge \quad c \mid b$ entonces $c \mid d$*

Notación 2. $M.C.D.\{a, b\} = (a, b)$

1.2. Algoritmo de la División

Para buscar el máximo común divisor, así como para deducir sus propiedades principales, se emplea el *algoritmo de la división de Euclides* de la siguiente manera. Sean a y b enteros positivos. Hallamos la serie de igualdades :

$$\left. \begin{array}{l} a = bq_1 + r_2 \quad , \quad 0 < r_2 < b, \\ b = r_2q_2 + r_3 \quad , \quad 0 < r_3 < r_2, \\ r_2 = r_3q_3 + r_4 \quad , \quad 0 < r_4 < r_3, \\ \dots \\ r_{n-2} = r_{n-1}q_{n-1} + r_n \quad , \quad 0 < r_n < r_{n-1} \\ r_{n-1} = r_nq_n, \end{array} \right\} \quad (1)$$

que termina cuando se obtiene cierto $r_{n+1} = 0$. Esto último es indispensable, puesto que la sucesión $b, r_2, r_3, \dots$, como sucesión de enteros decrecientes, no puede contener más de b positivos.

Dados $a, b \in \mathbb{Z}^+, a > b$ entonces $\exists \quad q_i, r_i \in \mathbb{Z}^+$ tales que:

$$\begin{aligned}
 a &= b q_1 + r_1, & 0 < r_1 < b \\
 b &= q_2 \cdot r_1 + r_2, & 0 < r_2 < r_1 \\
 r_1 &= q_3 \cdot r_2 + r_3, & 0 < r_3 < r_2 \\
 r_2 &= q_4 \cdot r_3 + r_4, & 0 < r_4 < r_3 \\
 r_3 &= q_5 \cdot r_4 + r_5, & 0 < r_5 < r_4 \\
 &\cdot \\
 &\cdot \\
 &\cdot \\
 r_{k-1} &= q_5 \cdot r_{k+1} + r_k, & 0 < r_{k+1} < r_k \\
 r_k &= q_{r+2} \cdot r_{k+1} + 0
 \end{aligned}$$

Notar que $r_1, \dots, r_{k+1}$ es una sucesión decreciente de enteros positivos y como solo existe una cantidad finita de enteros menores que b , el proceso terminará.

1.3. Ejercicios Resueltos

1. Encontrar el *M.C.D.* entre $\{11143, 8749\}$

Aplicamos el algoritmo de la división.

$$\begin{aligned}
 11143 &= 8749 \cdot 1 + 2394 \\
 8749 &= 2394 \cdot 3 + 1567 \\
 2394 &= 1567 \cdot 1 + 827 \\
 1567 &= 40 \cdot 1 + 4 \\
 827 &= 740 \cdot 1 + 87 \\
 740 &= 87 \cdot 8 + 44 \\
 87 &= 44 \cdot 1 + 43 \\
 44 &= 43 \cdot 1 + 1 \\
 43 &= 43 \cdot 1 + 0
 \end{aligned}$$

$$M.C.D.\{11143, 8749\} = 43$$

2. Encontrar el *M.C.D.* entre $\{7209, 816\}$

Aplicamos el algoritmo de la división.

$$\begin{aligned} 7209 &= 816 \cdot 8 + 681 \\ 816 &= 681 \cdot 1 + 135 \\ 681 &= 135 \cdot 6 + 6 \\ 135 &= 6 \cdot 22 + 3 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

$$M.C.D.\{7209, 816\} = 3$$

3. Encontrar el *M.C.D.* entre $\{5376, 3402\}$

Aplicamos el algoritmo de la división.

$$\begin{aligned} 5376 &= 3402 \cdot 1 + 1974 \\ 3402 &= 1974 \cdot 1 + 1428 \\ 1974 &= 1428 \cdot 1 + 546 \\ 1428 &= 546 \cdot 2 + 336 \\ 546 &= 336 \cdot 1 + 210 \\ 336 &= 210 \cdot 1 + 126 \\ 210 &= 126 \cdot 1 + 84 \\ 126 &= 84 \cdot 1 + 42 \\ 84 &= 42 \cdot 2 + 0 \end{aligned}$$

$$M.C.D.\{5436, 3401\} = 42$$

4. Encontrar el *M.C.D.* entre $\{1830, 792\}$

Aplicamos el algoritmo de la división.

$$\begin{aligned} 1830 &= (792 \cdot 2) + 246 \\ 792 &= (246 \cdot 3) + 54 \\ 246 &= (54 \cdot 4) + 30 \\ 54 &= (30 \cdot 1) + 24 \\ 30 &= (24 \cdot 1) + 6 \\ 24 &= (6 \cdot 4) + 0 \end{aligned}$$

$$M.C.D.\{1830, 792\} = 6$$

5. Encontrar el *M.C.D.* entre $\{65286, 1283\}$

Aplicamos el algoritmo de la división.

$$\begin{aligned}
 65286 &= (1283 \cdot 50) + 1136 \\
 1283 &= (1136 \cdot 1) + 147 \\
 1136 &= (147 \cdot 7) + 107 \\
 147 &= (107 \cdot 1) + 40 \\
 107 &= (40 \cdot 2) + 27 \\
 40 &= (27 \cdot 1) + 13 \\
 27 &= (13 \cdot 2) + 1
 \end{aligned}$$

$$M.C.D.\{65286, 1283\} = 1$$

6. Encontrar el *M.C.D.* entre $\{1214, 325\}$

Aplicamos el algoritmo de la división.

$$\begin{aligned}
 1214 &= (525 \cdot 3) + 239 \\
 325 &= (239 \cdot 1) + 86 \\
 239 &= (86 \cdot 2) + 67 \\
 86 &= (67 \cdot 1) + 19 \\
 19 &= (10 \cdot 1) + 9 \\
 10 &= (9 \cdot 1) + 1
 \end{aligned}$$

$$M.C.D.\{1214, 325\} = 1$$

7. Encontrar el *M.C.D.* entre $\{723, 420\}$

Aplicamos el algoritmo de la división.

$$\begin{aligned}
 723 &= (420 \cdot 1) + 303 \\
 420 &= (303 \cdot 1) + 117 \\
 303 &= (117 \cdot 2) + 69 \\
 117 &= (69 \cdot 1) + 48 \\
 69 &= (48 \cdot 1) + 21 \\
 48 &= (21 \cdot 2) + 6 \\
 21 &= (6 \cdot 3) + 3 \\
 6 &= (3 \cdot 2) + 0
 \end{aligned}$$

$$M.C.D.\{723, 420\} = 3$$

8. Encontrar el *M.C.D.* entre $\{221, 117\}$

Aplicamos el algoritmo de la división.

$$221 = (117 \cdot 1) + 104$$

$$117 = (104 \cdot 1) + 13$$

$$104 = (13 \cdot 8) + 0$$

$$M.C.D.\{221, 117\} = 13$$

9. Encontrar el *M.C.D.* entre $\{521, 285\}$

Aplicamos el algoritmo de la división.

$$521 = (285 \cdot 1) + 236$$

$$285 = (236 \cdot 1) + 49$$

$$236 = (49 \cdot 4) + 40$$

$$49 = (40 \cdot 1) + 9$$

$$40 = (9 \cdot 4) + 4$$

$$9 = (4 \cdot 2) + 1$$

$$4 = (1 \cdot 4) + 0$$

$$M.C.D.\{521, 285\} = 1$$

10. Encontrar el *M.C.D.* entre $\{666, 514\}$

Aplicamos el algoritmo de la división.

$$666 = (514 \cdot 1) + 152$$

$$514 = (152 \cdot 3) + 58$$

$$152 = (58 \cdot 2) + 36$$

$$58 = (36 \cdot 1) + 22$$

$$36 = (22 \cdot 1) + 14$$

$$22 = (14 \cdot 1) + 8$$

$$14 = (8 \cdot 1) + 6$$

$$8 = (6 \cdot 1) + 2$$

$$6 = (2 \cdot 3) + 0$$

$$M.C.D.\{666, 514\} = 2$$

Capítulo 2

Congruencias Lineales

2.1. Conceptos Fundamentales

Vamos a estudiar los números enteros en relación con los restos de la división de los mismos por un entero positivo m , dado al cual lo llamaremos *módulo*.

A cada número entero le corresponde el resto de su división por m ; si a dos enteros a y b les corresponde un mismo resto r , éstos se llaman *congruentes según el módulo m* , o *respecto del módulo m* , o simplemente, *congruentes módulo m* .

La congruencia de los números a y b respecto del módulo m se escribe así:

$$a \equiv b \pmod{m}.$$

lo cual se lee: a es congruente con b respecto del módulo m .

La congruencia de los números a y b respecto del módulo m es equivalente a:

1. La posibilidad de expresar a en la forma $a = b + mt$, donde t es entero.
2. La divisibilidad de $a - b$ por m . En efecto, de $a \equiv b \pmod{m}$ se deduce que

$$a = mq + r, \quad b = mq_1 + r; \quad 0 \leq r < m,$$

de donde

$$a - b = (q - q_1)m, \quad a = b + mt, \quad t = q - q_1.$$

Recíprocamente, de $a = b + mt$, representando b en la forma

$$b = mq_1 + r, \quad q = q_1 + t.$$

es decir

$$a \equiv b \pmod{m}.$$

2.2. Propiedades de las Congruencias

Sean $a, b, c, d \in \mathbb{Z}$ y $m \in \mathbb{Z}^+$. Entonces se cumplen:

1. Si $a \equiv b \pmod{m}$ y $c \in \mathbb{Z} \Rightarrow a + c \equiv b + c \pmod{m}$
2. Si $a \equiv b \pmod{m}$ y $c \in \mathbb{Z} \Rightarrow ac \equiv bc \pmod{m}$
3. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$
4. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m} \Rightarrow a + c \equiv (b + d) \pmod{m}$
5. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m} \Rightarrow a - c \equiv (b - d) \pmod{m}$
6. Si $a \equiv b \pmod{m}$ y $n \in \mathbb{N} \Rightarrow a^n \equiv b^n \pmod{m}$
7. Si $a \equiv b \pmod{m}$ y $p(x)$ una ecuación polinomial de x con coeficientes enteros

$$\Rightarrow p(a) \equiv p(b) \pmod{m}$$

8. Si $a \equiv b \pmod{m_i}$ con $i = 1, 2, 3, \dots, k$ y $(m_j, m_r) = 1, \forall j \neq r$, entonces

$$a \equiv b \pmod{\prod_{i=1}^k m_i}$$

Demostración: Ejercicio para los estudiantes. ■

2.3. Teoremas de Euler y Fermat

Teorema 3. (Euler)

Si $m > 1$ y $(a, m) = 1$, entonces:

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Demostración: En efecto, si x recorre el sistema reducido de restos

$$x = r_1, r_2, \dots, r_c; \quad c = \phi(m),$$

formado por los restos no negativos mínimos, entonces los restos no negativos mínimos $p_1, p_2, \dots, p_c$ de los números ax también recorren el mismo sistema, pero, generalmente, dispuestos en otro orden.

Multiplicando término a término las congruencias

$$ar_1 \equiv p_1 \pmod{m}, \quad ar_2 \equiv p_2 \pmod{m}, \dots, ar_c \equiv p_c \pmod{m}.$$

obtenemos

$$a^c r_1 r_2 \dots r_c \equiv p_1 p_2 \dots p_c \pmod{m}.$$

de donde dividiendo ambos miembros por el producto $r_1 r_2 \dots r_c = p_1 p_2$, resulta

$$a^c \equiv 1 \pmod{m}.$$

■

Teorema 4. (Fermat)

Si p es primo y a no es divisible por p , entonces

$$a^{p-1} \equiv 1 \pmod{p}. \quad (2.1)$$

Demostración: Este teorema es una consecuencia del teorema *a* para $m = p$. Al último teorema se le puede dar una forma más cómoda. Precizando, si se multiplican ambos miembros de la congruencia por (2.3) por a , se obtiene la congruencia

$$a^p \equiv a \pmod{p}.$$

la cual es válida ya para todos los valores enteros de a , puesto que también es válida si a es múltiplo de p . ■

2.4. Ejercicios Resueltos

1. Encontrar el resto de dividir 3^{40} por 26.

Solución:

Primero debemos identificar la base y el mód .

$$\text{Base} = 3, \quad \text{mód} = 26$$

Ahora decimos que:

$$\begin{aligned} 3^3 &\equiv 1 \pmod{26/()^{13}} && \text{por propiedad 6} \\ (3^3)^{13} &\equiv (1)^{13} \pmod{26} \\ 3^{39} &\equiv 1 \pmod{26/ \cdot 3} && \text{por propiedad 3} \\ 3^{40} &\equiv 3 \pmod{26} \end{aligned}$$

Luego el resto de dividir 3^{40} por 26 es 3.

2. Encontrar el resto de dividir 3^{57} por 26.

Solución:

Primero debemos identificar la base y el mód .

$$\text{Base} = 3, \quad \text{mód} = 26$$

Ahora decimos que:

$$\begin{aligned} 3^3 &\equiv 1 \pmod{26/()}^{19} && \text{por propiedad 6} \\ ((3^3)^{19}) &\equiv 1^{19} \pmod{26} \\ 3^{57} &\equiv 1 \pmod{26} \end{aligned}$$

Luego el resto de dividir 3^{57} por 26 es 1

3. Encontrar el resto de dividir 2^{43} por 31

Solución:

Primero debemos identificar la base y el mód .

$$\text{Base} = 2, \quad \text{mód} = 31$$

Ahora decimos que:

$$\begin{aligned} 2^5 &\equiv 1 \pmod{31/()}^8 && \text{por propiedad 6} \\ (2^5)^8 &\equiv (1)^8 \pmod{31} \\ 2^{40} &\equiv 1 \pmod{31 \cdot 2^3} && \text{por propiedad 3} \\ 2^{40+3} &\equiv 1 \cdot 2^3 \pmod{31} \\ 2^{43} &\equiv 2^3 \pmod{31} \\ 2^{43} &\equiv 8 \pmod{31} \end{aligned}$$

Luego el resto de dividir 2^{43} por 31 es 8

4. Encontrar el resto de dividir 3^{40} por 23

Solución:

Primero debemos identificar la base y el mód .

$$\text{Base} = 3, \quad \text{mód} = 23$$

Ahora decimos que:

$$\begin{aligned}
 3^5 &\equiv 13 \pmod{23} \quad \text{por propiedad 6} \\
 (3^5)^2 &\equiv (13)^2 \pmod{23} \\
 3^{10} &\equiv 169 \pmod{23} \quad \text{por definición} \\
 3^{10} &= 169 + 23k \\
 3^{10} &= 8 + (7 \cdot 23) + 23k \quad \text{por definición} \\
 3^{10} &\equiv 8 \pmod{23} \quad \text{por propiedad 6} \\
 (3^{10})^2 &\equiv (8)^2 \pmod{23} \\
 3^{20} &\equiv 64 \pmod{23} \quad \text{por definición} \\
 3^{20} &= 64 + 23k \\
 3^{20} &= 18 + (2 \cdot 23) + 23k \quad \text{por definición} \\
 3^{20} &\equiv 18 \pmod{23} \quad \text{por propiedad 6} \\
 (3^{20})^2 &\equiv (18)^2 \pmod{23} \\
 (3^{40}) &\equiv 324 \pmod{23} \quad \text{por definición} \\
 3^{40} &= 324 + 23k \\
 3^{40} &= 2 + (23 \cdot 14) + 23k \quad \text{por definición} \\
 3^{40} &= 2 + 23k \\
 3^{40} &\equiv 2 \pmod{23}
 \end{aligned}$$

Luego el resto de dividir 3^{40} por 23 es 2

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

Solución:

Primero debemos identificar la base y el mód .

$$\text{Base} = 2, \quad \text{mód} = 15$$

Ahora decimos que:

$$\begin{aligned}
 2^4 &\equiv 1 \pmod{15} \quad \text{por propiedad 6} \\
 (2^4)^7 &\equiv (1)^7 \pmod{15} \\
 2^{28} &\equiv 1 \pmod{15} \quad \text{por propiedad 3} \\
 2^{28} \cdot 2^2 &\equiv 1 \cdot 2^2 \pmod{15} \\
 2^{30} &\equiv 4 \pmod{15}
 \end{aligned}$$

Luego el resto de dividir 2^{30} por 15 es 4

6. Resolver $3x \equiv 2 \pmod{4}$

Primero notar que $(3, 4) = 1$, entonces por Teorema 3, y como $\phi(4) = \phi(2^2) = (2^2 - 2^1) = 2$, tenemos que:

$$\begin{aligned}
 3x &\equiv 2 \pmod{4} \\
 x &\equiv 3^{\phi(4)-1} \cdot 2 \pmod{4} \\
 x &\equiv 3 \cdot 2 \pmod{4} \\
 x &\equiv 6 \pmod{4} / \text{ por definición} \\
 x &= 6 + 4k \\
 x &= 2 + (4) + 4k \\
 x &= 2 + 4k / \text{ por definición} \\
 x &\equiv 2 \pmod{4}
 \end{aligned}$$

$$S = \{x \in \mathbb{Z} : x = 2 + 4k, k \in \mathbb{Z}\}$$

7. Resolver $3x \equiv 5 \pmod{8}$ Primero notar que $(5, 8) = 1$, entonces por Teorema 3 y como $\phi(8) = \phi(2^3) = (2^3 - 2^1) = 4$, tenemos que:

$$\begin{aligned}
 3x &\equiv 5 \pmod{8} \\
 x &\equiv 3^{\phi(8)-1} \cdot 5 \pmod{8} \\
 x &\equiv 27 \cdot 5 \pmod{8} \\
 x &\equiv 135 \pmod{8} / \text{ por definición} \\
 x &= 135 + 8k \\
 x &= 7 + (16 \cdot 8) + 8k \\
 x &= 7 + 8k / \text{ por definición} \\
 x &\equiv 7 \pmod{8}
 \end{aligned}$$

$$S = \{x \in \mathbb{Z} : x = 7 + 8k, k \in \mathbb{Z}\}$$

8. Resolver $5x \equiv -3 \pmod{8}$

Primero notar que $(5, 8) = 1$, entonces por Teorema 3 y como $\phi(8) = \phi(2^3) = (2^3 - 2^1) = 4$, tenemos que:

$$\begin{aligned}
5x &\equiv -3 \pmod{8} \\
-3x &\equiv 5 \pmod{8} \\
5x &\equiv 5 \pmod{8} \\
x &\equiv 5^{\phi(8)-1} \cdot 5 \pmod{8} \\
x &\equiv 5^3 \cdot 5 \pmod{8} \\
x &\equiv 5^4 \pmod{8} \\
x &\equiv 625 \pmod{8} / \text{por definición} \\
x &= 1 + (78 \cdot 8) + 8k \pmod{8} \\
x &= 1 + 8k \pmod{8} / \text{por definición} \\
x &= 1 \pmod{8}
\end{aligned}$$

$$S = \{x \in \mathbb{Z} : x = 1 + 8k, k \in \mathbb{Z}\}$$

9. Resolver $2x \equiv 1 \pmod{17}$

Primero notar que $(2, 17) = 1$, entonces por Teorema 3 y como $\phi(17) = (17^1 - 17^0) = (17 - 1) = 16$, tenemos que:

$$\begin{aligned}
2x &\equiv 1 \pmod{17} \\
x &\equiv 2^{\phi(17)-1} \cdot 1 \pmod{17} \\
x &\equiv 2^{15} \cdot 1 \pmod{17} \\
x &\equiv 32768 \cdot 1 \pmod{17} / \text{por definición} \\
x &= 9 + (1927 \cdot 17) + 17k \\
x &= 9 + 17k / \text{por definición} \\
x &\equiv 9 \pmod{17}
\end{aligned}$$

$$S = \{x \in \mathbb{Z} : x = 9 + 17k, k \in \mathbb{Z}\}$$

10. Resolver $14x \equiv 11 \pmod{5}$

Primero notar que $(14, 5) = 1$, entonces por Teorema 3 y como $\phi(5) = (5^1 - 5^0) = (5 - 1) = 4$, tenemos que

$$\begin{aligned}
14x &\equiv 11 \pmod{5} \\
x &\equiv 14^{\phi(5)-1} \cdot 11 \pmod{5} \\
x &\equiv 14^3 \cdot 11 \pmod{5} \\
x &\equiv 30184 \pmod{5} / \text{por definición} \\
x &= 4 + (60368 \cdot 5) + 5k \\
x &= 4 + 5k / \text{por definición} \\
x &\equiv 4 \pmod{5}
\end{aligned}$$

$$S = \{x \in \mathbb{Z} : x = 4 + 5k, k \in \mathbb{Z}\}$$

11. Resolver $40x \equiv 777 \pmod{1777}$

$M.C.D.(40, 1777) = 1$, la congruencia lineal tiene exactamente una solución.
Notemos,

$$777 \equiv 2554 \pmod{1777}$$

Por transitividad:

$$\begin{aligned} 40x &\equiv 2554 \pmod{1777} \\ 2 \cdot 20x &\equiv 2 \cdot 1277 \pmod{1777} \\ 20x &\equiv 1277 \pmod{1777} \\ 1277 &\equiv 3054 \pmod{1777} \\ 20x &\equiv 3054 \pmod{1777} \\ 2 \cdot 10x &\equiv 1527 \cdot 2 \pmod{1777} \\ 10x &\equiv 1527 \pmod{1777} \\ 1527 &\equiv -250 \pmod{1777} \\ 10x &\equiv -250 \pmod{1777} \\ 10x &\equiv -25 \cdot 10 \pmod{1777} \\ x &\equiv -25 \pmod{1777} \\ x &\equiv 1752 \pmod{1777} \end{aligned}$$

$$S = \{x \in \mathbb{Z} : x = 1752 + 1777k, k \in \mathbb{Z}\}$$

12. Resolver $4x \equiv 3 \pmod{7}$

$M.C.D.(4, 7) = 1$, entonces son primos Relativos. Por Teorema 3.

$$\begin{aligned} x &\equiv 4^5 \cdot 3 \pmod{7} \\ x &\equiv 4^5 \cdot 3 \pmod{7} \\ x &\equiv 1024 \cdot 3 \pmod{7} \\ x &\equiv 3074 \cdot 3 \pmod{7} \\ x &\equiv (7 \cdot 438) + 6 \pmod{7} \\ x &\equiv 6 \pmod{7} \end{aligned}$$

$$S = \{x \in \mathbb{Z} : x = 6 + 7k, k \in \mathbb{Z}\}$$

13. Resolver $3x \equiv 1 \pmod{17}$

$M.C.D.(3, 17) = 1$, entonces son primos relativos.

Por Teorema 3.

$$\begin{aligned}x &\equiv 3^{(\phi 17)-1} \cdot 1 \pmod{17} \\x &\equiv 3^{15} \cdot 1 \pmod{17} \\x &\equiv 14348907 \pmod{17} \\x &\equiv (17 \cdot 844053) + 6 \pmod{17} \\x &\equiv 6 \pmod{17}\end{aligned}$$

$$S = \{x \in \mathbb{Z}: x = 6 + 17k, k \in \mathbb{Z}\}$$

14. Resolver $3x \equiv 6 \pmod{18}$

M.C.D. (3,18)=3, entonces existen 3 soluciones Incongruentes.

$$3x \equiv 2 \cdot 3 \pmod{18}$$

Donde efectivamente $6 \mid 18$

$$\Rightarrow x \equiv 2 \pmod{6}$$

3 soluciones Incongruentes, de la forma $2 + 6t$, donde $t = \{0, 1, 2\}$

$$S_1 = \{x \in \mathbb{Z}: x = 2 + 6k, k \in \mathbb{Z}\}$$

$$S_2 = \{x \in \mathbb{Z}: x = 8 + 6k, k \in \mathbb{Z}\}$$

$$S_3 = \{x \in \mathbb{Z}: x = 14 + 6k, k \in \mathbb{Z}\}$$

15. Resolver $2x \equiv 1 \pmod{19}$

M.C.D. (2,19)=1, entonces son primos relativos.

Por Teorema 3.

$$\begin{aligned}x &\equiv 2^{\phi(19)-1} \cdot 1 \pmod{19} \\x &\equiv 131072 \pmod{19} \\x &\equiv (19 \cdot 6898) + 10 \pmod{19} \\x &\equiv 10 \pmod{19}\end{aligned}$$

$$S = \{x \in \mathbb{Z}: x = 10 + 19k, k \in \mathbb{Z}\}$$

16. Resolver $3x \equiv 1 \pmod{19}$

M.C.D. $(3,19)=1$, entonces son primos relativos.

Resolvemos a través del Teorema de Euler

$$x \equiv 3^{\phi(19)-1} \cdot 1 \pmod{19}$$

$$x \equiv 3^{16} \pmod{19}$$

$$x \equiv 43046721 \pmod{19}$$

$$x \equiv (19 \cdot 2265616) + 17 \pmod{19}$$

$$x \equiv 17 \pmod{19}$$

$$S = \{x \in \mathbb{Z}: x = 17 + 19k, k \in \mathbb{Z}\}$$

17. Resolver $3x \equiv 1 \pmod{17}$

M.C.D. $(3,17)=1$, entonces son primos relativos.

Por Teorema 3.

$$x \equiv 3^{\phi(17)-1} \cdot 1 \pmod{17}$$

$$x \equiv 3^{15} \cdot 1 \pmod{17}$$

$$x \equiv 14348907 \pmod{17}$$

$$x \equiv (17 \cdot 844053) + 6 \pmod{17}$$

$$x \equiv 6 \pmod{17}$$

$$S = \{x \in \mathbb{Z}: x = 6 + 17k, k \in \mathbb{Z}\}$$

18. Resolver $9x \equiv 4 \pmod{1454}$

M.C.D. $(9, 1454) = 1$, la congruencia lineal tiene exactamente una solución
 $4 \equiv 1548 \pmod{1454}$

$$9x \equiv 1458 \pmod{1454}$$

$$9x \equiv 9 \cdot 162 \pmod{1454}$$

$$x \equiv 162 \pmod{1454}$$

$$S = \{x \in \mathbb{Z}: x = 162 + 1454k, k \in \mathbb{Z}\}$$

19. Resolver $7x \equiv 1 \pmod{10}$

M.C.D. $(7,10)=1$. Entonces son primos relativos.

Entonces por Teorema 3.

$$x \equiv 7^{\phi(10)-1} \cdot 1 \pmod{10}$$

$$x \equiv 7^3 \pmod{10}$$

$$x \equiv 343 \pmod{10}$$

$$S = \{x \in \mathbb{Z}: x = 343 + 10k, k \in \mathbb{Z}\}$$

2.4.1. Ejercicios Propuestos

1. Resolver $7x \equiv 18 \pmod{19}$
2. Resolver $7x \equiv 5 \pmod{11}$
3. Resolver $6x \equiv 8 \pmod{20}$
4. Resolver $8x \equiv 4 \pmod{5}$
5. Resolver $15x \equiv 30 \pmod{60}$

Capítulo 3

Ecuaciones Diofánticas

3.1. Ecuaciones Diofánticas

Estas ecuaciones reciben este nombre en honor a Diofanto, matemático que trabajó en Alejandría a mediados del siglo III a.c.

3.2. Ejercicios Resueltos

1. Resolver $47x + 7y = 5$

Usando el Algoritmo de la División para los enteros $a = 47$ y $b = 7$ se tiene:

$$M.C.D. \quad \{47, 7\}$$

$$\begin{aligned} 47 &= 7 \cdot 6 + 5 \\ 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0 \\ 5 &= 47 + 7(-6) \\ 2 &= 7 + 5(-1) \\ &= 7 + (-1)[47 + 7(-6)] \\ &= 7 + 47(-1) + 7(6) \end{aligned}$$

$$\begin{aligned}
&= 47(-1) + 7(7) \\
1 &= 5 + 2(-2) \\
&= 47 + 7(-6) + (-2)[47(-1) + 7(7)] \\
&= 47 + 7(-6) + 47(2) + 7(-14) \\
1 &= 47(3) + 7(-20) \quad \cdot 5 \\
5 &= 47(15) + 7(-100)
\end{aligned}$$

Donde $x_0 = 15$ e $y_0 = -100$ son soluciones particulares de la Ecuación Diofantica Lineal $47x + 7y = 5$.

2. Resolver $78x + 32y = 2$

Usando el Algoritmo de la División para los enteros $a = 78$ y $b = 32$ se tiene:

$$M.C.D. \quad \{78, 32\}$$

$$\begin{aligned}
78 &= 32 \cdot 2 + 14 \\
32 &= 14 \cdot 2 + 4 \\
14 &= 4 \cdot 3 + 2 \\
4 &= 2 \cdot 2 + 0
\end{aligned}$$

Despejando los restos

$$\begin{aligned}
14 &= 78 + 32(-2) \\
4 &= 32 + 14(-2) \\
&= 32 + (-2)[78 + 32(-2)] \\
&= 32 + 78(-2) + 32(4) \\
&= 32(5) + 78(-2) \\
2 &= 14 + 4(-3) \\
&= 78 + 32(-2) + (-3)[32(5) + 78(-2)] \\
&= 78 + 32(-2) + 32(-15) + 78(6) \\
&= 78(7) + 32(-17)
\end{aligned}$$

Donde $x_0 = 7$ e $y_0 = -17$ son soluciones particulares de la Ecuación Diofantica Lineal $78x + 32y = 2$.

3. Resolver $11x + 34y = 31$

Usando el Algoritmo de la División para los enteros $a = 11$ y $b = 34$ se tiene: $M.C.D. = \{34, 11\}$

$$\begin{aligned} 34 &= 11 \cdot 3 + 1 \\ 11 &= 1 \cdot 11 + 0 \\ 1 &= 34 + 11(-3)/ \quad \cdot 31 \\ 31 &= 34(31) + 11(-93) \end{aligned}$$

Donde $x_0 = 31$ e $y_0 = -93$ son soluciones particulares de la Ecuación Diofantica Lineal $417x + 54y = 8$.

4. Resolver $17x + 54y = 8$ Usando el Algoritmo de la División para los enteros $a = 17$ y $b = 54$ se tiene: $M.C.D. = \{54, 17\}$

$$\begin{aligned} 54 &= 17 \cdot 3 + 3 \\ 17 &= 3 \cdot 5 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

Despejando los restos

$$\begin{aligned} 3 &= 54 + 17(-3) \\ 2 &= 17 + 3(-5) \\ &= 17 + (-5)[54 + 17(-3)] \\ &= 32 + 78(-2) + 32(4) \\ &= 17 + 54(-5) + 17(15) \\ &= 17(16) + 54(-5) \\ 1 &= 3 + 2(-1) \\ &= 54 + 17(-3) + (-1)[17(16) + 54(-5)] \\ &= 54 + 17(-3) + 17(-16) + 54(5)/ \quad \cdot 8 \\ 8 &= 54(78) + 17(-152) \end{aligned}$$

Donde $x_0 = 78$ e $y_0 = -152$ son soluciones particulares de la Ecuación Diofantica Lineal $17x + 54y = 8$.

5. Resolver $5x + 7y = 29$

Usando el Algoritmo de la División para los enteros $a = 5$ y $b = 7$ se tiene:

$$M.C.D. \quad \{5, 7\}$$

$$\begin{aligned} 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0 \\ 2 &= 7 + 5(-1) \\ 1 &= 5 + 2(-2) \\ &= 5 + (-2[7 + 5(2)]) \\ &= 5(3) + 7(-2) / \quad \cdot 29 \\ 29 &= 5(87) + 7(-58) \end{aligned}$$

Donde $x_0 = 87$ e $y_0 = -58$ son soluciones particulares de la Ecuación Diofantica Lineal $5x + 7y = 29$.

6. Resolver $32x + 55y = 771$

Usando el Algoritmo de la División para los enteros $a = 32$ y $b = 55$ se tiene: $M.C.D. \quad \{78, 32\}$

$$\begin{aligned} 55 &= 32 \cdot 1 + 23 \\ 32 &= 23 \cdot 1 + 9 \\ 23 &= 9 \cdot 2 + 5 \\ 9 &= 5 \cdot 1 + 4 \\ 5 &= 4 \cdot 1 + 1 \\ 4 &= 1 \cdot 4 + 0 \end{aligned}$$

Despejando los restos

$$\begin{aligned}
32 &= 55 + 32(-1) \\
9 &= 32 + 23(-1) \\
&= 32 + (-1)[55 + 32(-1)] \\
&= 32 + 55(-1) + 32(1) \\
&= 32(2) + 55(-1) \\
5 &= 23 + 9(-2) \\
&= 55 + 32(-1) + (-2)[32(2) + 55(-1)] \\
&= 55 + 32(-1) + 32(-4) + 55(2) \\
&= 55(3) + 32(-5) \\
4 &= 9 + 5(-1) \\
&= 32(2) + 55(-1) + (-1)[55(3) + 32(-5)] \\
&= 32(2) + 55(-1) + 32(5) + 55(-3) \\
&= 32(7) + 55(-4) \\
1 &= 5 + 4(-1) \\
&= 55(3) + 32(-5) + (-1)[32(7) + 55(-4)] \\
&= 55(3) + 32(-5) + 32(-7) + 55(4) \\
&= 32(-12) + 55(7) / \quad \cdot 771 \\
771 &= 32(-9252) + 55(5397)
\end{aligned}$$

Donde $x_0 = -9252$ e $y_0 = 5397$ son soluciones particulares de la Ecuación Diofantica Lineal $32x + 55y = 771$.

7. Resolver $62x + 11y = 682$

Usando el Algoritmo de la División para los enteros $a = 62$ y $b = 11$ se tiene:

M.C.D. $\{62, 11\}$

$$\begin{aligned}
62 &= 11 \cdot 5 + 7 \\
11 &= 7 \cdot 1 + 4 \\
7 &= 4 \cdot 1 + 3 \\
4 &= 3 \cdot 1 + 1 \\
3 &= 1 \cdot 3 + 0
\end{aligned}$$

Despejando los restos

$$\begin{aligned}
 7 &= 62 + 1(-5) \\
 4 &= 11 + 7(-1) \\
 &= 11 + (-1)[62 + 11(-5)] \\
 &= 11 + 62(-1) + 11(5) \\
 &= 11(6) + 62(-1) \\
 3 &= 7 + 4(-1) \\
 &= 62 + 11(-5) + (-1)[11(6) + 62(-1)] \\
 &= 62 + 11(-5) + 11(-6) + 62(1) \\
 &= 62(2) + 11(-11) \\
 1 &= 4 + 3(-1) \\
 &= 11(6) + 62(-1) + (-1)[62(2) + 11(-11)] \\
 &= 11(6) + 62(-1) + 62(-2) + 11(11) \\
 &= 11(17) + 62(-3) / \quad \cdot 682 \\
 682 &= 62(-2046) + 11(11594)
 \end{aligned}$$

Donde $x_0 = -2046$ e $y_0 = 11594$ son soluciones particulares de la Ecuación Diofántica Lineal $62x + 11y = 682$.

8. Resolver $21x + 312y = 72$

Usando el Algoritmo de la División para los enteros $a = 21$ y $b = 12$ se tiene:

$M.C.D.$ $\{21, 12\}$

$$\begin{aligned}
 21 &= 12 \cdot 1 + 9 \\
 12 &= 9 \cdot 1 + 3 \\
 9 &= 3 \cdot 3 + 0
 \end{aligned}$$

Despejando los restos

$$\begin{aligned}
 9 &= 21 + 12(-1) \\
 3 &= 12 + 9(-1) \\
 &= 12 + (-1)[21 + 12(-1)] \\
 &= 12 + 21(-1) + 12(1) \\
 &= 12(2) + 21(-1) / \quad \cdot 24 \\
 72 &= 12(48) + 21(-24)
 \end{aligned}$$

Donde $x_0 = 48$ e $y_0 = -24$ son soluciones particulares de la Ecuación Diofantica Lineal $21x + 12y = 72$.

9. Resolver $55x + 99y = 77$ Usando el Algoritmo de la División para los enteros $a = 55$ y $b = 99$ se tiene: $M.C.D.$ $\{99, 55\}$

$$99 = 55 \cdot 1 + 44$$

$$55 = 44 \cdot 1 + 11$$

$$44 = 11 \cdot 4 + 0$$

Despejando los restos

$$44 = 99 + 55(-1)$$

$$11 = 55 + 44(-1)$$

$$= 55 + (-1)[99 + 55(-1)]$$

$$= 55 + 99(-1) + 55(1) \quad \cdot 7$$

$$77 = 55(14) + 99(-7)$$

Donde $x_0 = 14$ e $y_0 = -7$ son soluciones particulares de la Ecuación Diofantica Lineal $55x + 99y = 77$.

10. Resolver $85x + 78y = 290$
Usando el Algoritmo de la División para los enteros $a = 85$ y $b = 78$ se tiene:
 $M.C.D.$ $\{85, 78\}$

$$85 = 78 \cdot 1 + 7$$

$$78 = 7 \cdot 11 + 1$$

$$7 = 1 \cdot 7 + 0$$

Despejando los restos

$$\begin{aligned}
7 &= 85 + 78(-1) \\
1 &= 78 + 7(-11) \\
&= 78 + (-11)[85 + 78(-1)] \\
&= 78 + 85(-11) + 78(11)/ \\
&= 78(12) + 85(-11)/ \quad \cdot 290 \\
290 &= 78(3480) + 85(-3190)
\end{aligned}$$

Donde $x_0 = 3480$ e $y_0 = -31190$ son soluciones particulares de la Ecuación Diofántica Lineal $85x + 28y = 290$.

11. Resolver $3x + 7y = 9$ A través del algoritmo de la división en $\mathbb{Z}$ tenemos,
 $M.C.D.\{3, 7\}$:

$$\begin{aligned}
7 &= 3 \cdot 2 + 1 \\
2 &= 1 \cdot 2 + 0
\end{aligned}$$

$$M.C.D.\{7, 3\} = 1$$

Efectivamente $1 \mid 9$. Por lo que la ecuación posee solución. Utilizando el Algoritmo de Euclides se puede expresar,

$$1 = 7 + 3 \cdot (-2)$$

Luego,

$$9 = 3(-18) + 7(9)$$

Donde $x_0 = -18$ e $y_0 = 9$. Cuales representa una solución particular a la ecuación. De aquí la solución general de la ecuación diofántica está dada por las ecuaciones

$$x = -18 + 7t \quad \text{e} \quad y = 9 - 3t$$

Donde $t \in \mathbb{Z}$

12. Resolver $11x + 4y = 5$

A través del algoritmo de la división en $\mathbb{Z}$ tenemos,
 $M.C.D.\{11, 4\}$:

$$\begin{aligned}
11 &= 4 \cdot 2 + 3 \\
4 &= 3 \cdot 1 + 1
\end{aligned}$$

$$M.C.D.\{11, 4\} = 1$$

Efectivamente $1 \mid 5$. Por lo que la ecuación posee solución. Utilizando el Algoritmo de Euclides se puede expresar,

$$3 = 11 + 4 \cdot (-2)$$

Luego,

$$\begin{aligned} 1 &= 4 + 3 \cdot (-1) \\ \Rightarrow &= 4 + \{11 + 4 \cdot (-2)\} \cdot (-1) \\ \Rightarrow &= 4 + \{11 \cdot (-1) + 4 \cdot (2)\} \\ \Rightarrow &= 1 = 4 + \{11 \cdot (-1) + 4 \cdot (2)\} \\ \Rightarrow &= 1 = 4 \cdot (3) + 11 \cdot (-1) / \cdot 5 \\ \Rightarrow &= 5 = 4 \cdot (15) + 11 \cdot (-5) \end{aligned}$$

Donde $x_0 = -5$ e $y_0 = 15$. Cuales representa una solución particular a la ecuación. De aquí la solución general de la ecuación diofántica está dada por las ecuaciones

$$x = -5 + 4t \quad \text{e} \quad y = 15 - 11t$$

Donde $t \in \mathbb{Z}$

13. Resolver $48x + 7y = 5$ A través del algoritmo de la división en $\mathbb{Z}$ tenemos,
 $M.C.D.\{48, 7\}:$

$$48 = 7 \cdot 6 + 6$$

$$7 = 6 \cdot 1 + 1$$

$$6 = 1 \cdot 6 + 0$$

$$M.C.D.\{48, 7\} = 1$$

Efectivamente $1 \mid 5$. Por lo que la ecuación posee solución. Utilizando el Algoritmo de

Euclides se puede expresar,

$$6 = 48 \cdot +7(-6)$$

$$1 = 7 + 6(-1)$$

$$\Rightarrow 1 = 7 + \{48 + 7(-6)\} \cdot (-1)$$

$$\Rightarrow 1 = 48(-1) + 7(7)$$

$$\Rightarrow 1 = 48(-1) + 7(7)/ \cdot 5$$

Luego,

$$5 = 48(-5) + 7(35)$$

Donde $x_0 = -5$ e $y_0 = 35$. Cuales representa una solución particular a la ecuación. De aquí la solución general de la ecuación diofántica está dada por las ecuaciones

$$x = -5 + 7t \quad \text{e} \quad y = 35 - 48t$$

Donde $t \in \mathbb{Z}$

14. Resolver $55x - 99y = 77$ Consideremos $z = -y$, entonces

$$55x + 99z = 77$$

A través del algoritmo de la división en $\mathbb{Z}$ tenemos

$$M.C.D.\{99, 55\}:$$

$$99 = 55 \cdot 1 + 44$$

$$55 = 44 \cdot 1 + 11$$

$$M.C.D.\{99, 11\}: 11$$

Donde Efectivamente $11 \mid 77$

Luego, despejamos los restos

$$44 = 99 + 55(-1)$$

$$11 = 55 + 44(-1)$$

$$11 = 55 + \{99 + 55(-1)\} \cdot (-1)$$

$$11 = 55(2) + 99(-1)$$

$$11 = 55(2) + 99(-1)/ \cdot 7$$

Luego

$$77 = 55(14) + 99(-7)$$

Donde $x_0 = 14$ e $z_0 = -7$. Pero anteriormente establecimos la condición de que $z=-y$ entonces las soluciones son $x_0 = 14$ e $y_0 = 7$ las Cuales representa una solución particular a la ecuación.

De aquí la solución general de la ecuación diofántica está dada por las ecuaciones

$$x = 14 + 9t \quad \text{e} \quad y = 7 - 5t$$

Donde $t \in \mathbb{Z}$

15. Resolver $11x + 34y = 31$ A través del algoritmo de la división en $\mathbb{Z}$ tenemos,
 $M.C.D.\{11, 34\}$:

$$34 = 11 \cdot 3 + 1$$

$$11 = 1 \cdot 11 + 0$$

$$M.C.D.\{34, 11\} = 1$$

Efectivamente $1 \mid 31$. Por lo que la ecuación posee solución. Utilizando el Algoritmo de Euclides se puede expresar,

$$1 = 34 + 11 \cdot (-3)$$

$$1 = 34 + 11 \cdot (-3)/ \cdot 31$$

Luego,

$$31 = 34(31) + 11(-93)$$

Donde $x_0 = -93$ e $y_0 = 31$. Cuales representa una solución particular a la ecuación.
 De aquí la solución general de la ecuación diofántica está dada por las ecuaciones

$$x = -93 + 34t \quad \text{e} \quad y = 31 - 11t$$

Donde $t \in \mathbb{Z}$

16. Resolver $27x + 18y = 72$

A través del algoritmo de la división en $\mathbb{Z}$ tenemos,
 $M.C.D.\{27, 18\}$:

$$27 = 18 \cdot 1 + 9$$

$$18 = 9 \cdot 2 + 0$$

$$M.C.D.\{27, 18\} = 9$$

Efectivamente $9 \mid 18$. Por lo que la ecuación posee solución. Utilizando el Algoritmo de Euclides se puede expresar,

$$9 = 27 + 18 \cdot (-1)$$

$$9 = \{27 + 18 \cdot (-1)\} / \cdot 8$$

Luego,

$$72 = 27(8) + 18(-8)$$

Donde $x_0 = 8$ e $y_0 = -8$. Cuales representa una solución particular a la ecuación. De aquí la solución general de la ecuación diofántica está dada por las ecuaciones

$$x = 8 + 2t \quad \text{e} \quad y = -8 - 2t$$

Donde $t \in \mathbb{Z}$

17. Resolver $44x + 15y = 77$ A través del algoritmo de la división en $\mathbb{Z}$ tenemos

$M.C.D.\{44, 15\}$:

$$44 = 15 \cdot 2 + 14$$

$$15 = 14 \cdot 1 + 1$$

Despejamos los restos

$$14 = 44 + 15(-2)$$

$$1 = 15 + 14(-1)$$

$$\Rightarrow 1 = 15 + (44 + 15(-2))(-1)$$

$$\Rightarrow 1 = 15 + 44(-1) + 15(2)$$

$$\Rightarrow 1 = 44(-1) + 15(3)$$

Luego

$$77 = 15(231) + 44(-77)$$

Donde

$$\left. \begin{array}{l} x_0 = -77 \\ y_0 = 231 \end{array} \right\} \text{ Solución particular de la ecuación}$$

Solución general de la ecuación diofántica

$$x = -77 + 15t \quad y = 231 - 44t$$

con $t \in \mathbb{Z}$

18. Resolver $28x + 36y = 104$ A través del algoritmo de la división en $\mathbb{Z}$ tenemos

$M.C.D.\{36, 32\}:$

$$36 = 28 \cdot 1 + 8$$

$$28 = 8 \cdot 3 + 4$$

Despejamos los restos

$$8 = 36 + 28(-1)$$

$$4 = 28 + 8(-3)$$

$$\Rightarrow 4 = 28 + (36 + 28(-1))(-3)$$

$$\Rightarrow 4 = 28 + 36(-3) + 28(3)$$

$$\Rightarrow 4 = 36(-3) + 28(4)$$

Luego

$$104 = 28(104) + 36(-78)$$

Donde

$$\left. \begin{array}{l} x_0 = 104 \\ y_0 = -78 \end{array} \right\} \text{ Solución particular de la ecuación}$$

Solución general de la ecuación diofántica

$$x = 104 + 36t \quad y = -78 - 28t$$

con $t \in \mathbb{Z}$

19. Resolver $221x + 117y = 20$ A través del algoritmo de la división en $\mathbb{Z}$ tenemos, $M.C.D.\{221, 117\}$:

$$\begin{aligned} 221 &= (117 \cdot 1) + 104 \\ \Rightarrow 117 &= (104 \cdot 1) + 13 \\ \Rightarrow 104 &= (13 \cdot 8) + 0 \end{aligned}$$

$13 \nmid 20$. Por lo que la ecuación no posee solución.

20. Resolver $18x + 5y = 48$

A través del algoritmo de la división en $\mathbb{Z}$ tenemos, $M.C.D.\{18, 5\}$:

$$\begin{aligned} 18 &= 5 \cdot 3 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}$$

$$M.C.D.\{18, 5\} = 1$$

Efectivamente $1 \mid 48$. Por lo que la ecuación posee solución. Utilizando el Algoritmo de Euclides se puede expresar,

$$\begin{aligned} 3 &= 18 + 5 \cdot (-3) \\ 2 &= 5 + (18 + 5 \cdot (-3)) \cdot (-1) \\ \Rightarrow 2 &= 18 \cdot (-1) + 5 \cdot (4) \\ 1 &= 3 + 2 \cdot (-1) \\ \Rightarrow 1 &= (18 + 5 \cdot (-3)) + (18 \cdot (-1) + 5 \cdot (4)) \cdot (-1) \\ \Rightarrow 1 &= 18 \cdot (2) + 5 \cdot (-7) \end{aligned}$$

Luego,

$$48 = 18(96) + 5(-336)$$

Donde $x_0 = 96$ e $y_0 = -336$. Cuales representa una solución particular a la ecuación. De aquí la solución general de la ecuación diofántica está dada por las ecuaciones

$$x = 96 + 5t \quad \text{e} \quad y = -336 - 18t$$

Donde $t \in \mathbb{Z}$

Si t es un entero. Las soluciones positivas se pueden determinar considerando el sistema de desigualdades

$$96 + 5t > 0$$

$$-336 - 18t > 0$$

$$96 + 5t > 0 \quad 336 - 18t > 0$$

$$t > -19,2 \quad t < -18,\bar{6}7$$

entonces

$$-19,2 < t < -18,\bar{6}7$$

Como $t \in \mathbb{Z}$, $t = -19$ y

$$x = 96 + 5(-19) = 1$$

$$y = -336 - 18(-19) = 6$$

$\therefore$ la única solución entera positiva de la ecuación $18x + 5y = 48$ son los valores 1 y 6 para x e y .

3.2.1. Ejercicios Propuestos

1. Resolver $48x + 7y = 5$
2. Resolver $21x - 12y = 72$
3. $32x + 55y = 771$
4. Resolver $66x + 550y = 88$
5. Resolver $23x - 12y = 7$
6. Resolver $36x - 32y = 258$

Bibliografía

- [1] I. Vinogradov, *Fundamentos de la Teoría de los Números*, MIR, Moscú, 1987.
- [2] Pettofrezzo, Anthony and Birkyt, Donald R. *Elements of Number Theory*, Prentice Hall, Inc. United States of America 1970.
- [3] Gauss, Carl Friedrich [1801] (en español), *Disquisitiones arithmeticae*, traducido por Hugo Barrantes, Michael Josephy y Ángel Ruiz, San José, Costa Rica: Centro de Investigaciones Matemáticas y Meta-Matemáticas (CIMM), Universidad de Costa Rica.