# *TEMAS DE MATEMÁTICAS*
# *(Oposiciones de Secundaria)*

***TEMA 15***

## ***ECUACIONES DIOFANTICAS***

*TEMA 15*

## *ECUACIONES DIOFANTICAS*

## 1. INTRODUCCIÓN.

**PROP** Sea V un K-espacio vectorial de dimensión n. Sea B = $\{u_1,\ldots..,u_n\}$ base de V. Dados $a_1, a_2,\ldots., a_n \in K$, definimos f: V $\to$ K donde $\vec{v} \in V$ con $\vec{v} = (x_1, x_2, ...., x_n)$ coordenadas respecto de B, $f(\vec{v}) = \sum_{i=1}^{n} a_i x_i$ . Entonces f es una aplicación lineal.

Dem.

$$f(\lambda\vec{v} + \mu\vec{w}) = f(\lambda\cdot(x_1u_1 + ..... + x_nu_n) + \mu(y_1u_1 + ..... + y_nu_n)) =$$

$$= f((\lambda x_1 + \mu y_1)u_1 + ..... + (\lambda x_n + \mu y_n)u_n) =$$

$$= a_1(\lambda x_1 + \mu y_1) + ..... + a_n(\lambda x_n + \mu y_n) =$$

$$= \lambda a_1 x_1 + \mu a_1 y_1 + ..... + \lambda a_n x_n + \mu a_n y_n =$$

$$= \lambda(a_1 x_1 + ..... + a_n x_n) + \mu(a_1 y_1 + ..... + a_n y_n) = \lambda f(\vec{v}) + \mu f(\vec{w})$$

Dada una aplicación lineal f: V $\to$ K con V K-espacio vectorial, nos planteamos la necesidad de conocer que vectores de V, $\vec{x} \in V$ verifican $f(\vec{x}) = c$ siendo $c \in K$ un elemento fijo.

**DEF** Bajo las condiciones anteriores, la expresión $f(\vec{x}) = c$ recibe el nombre de ecuación lineal. Cada $\vec{x} \in V$ que verifique la ecuación anterior es una solución de al ecuación. Los elementos $(x_1, x_2, ....., x_n)$, coordenadas de $\vec{x}$ respecto una base B de V, se llaman incógnitas y los $a_1, a_2,\ldots., a_n \in K$ coeficientes.

**OBS** Aunque sean vectores, es usual representarlos sin la flecha superior, por lo que escribiremos f(x) = c, para simplificar la notación.

**DEF** Una ecuación diofántica es una ecuación algebraica con coeficientes enteros y de la que interesan únicamente las soluciones enteras.

Veremos como resolver las ecuaciones diofánticas, dividiéndolas en diferentes tipos. Nos centraremos más en ecuaciones lineales, aunque también veremos ecuaciones diofánticas no lineales.

## 2. ECUACIONES DIOFÁNTICAS LINEALES.

### 2.1. Ecuaciones con una Incógnita.

Este caso no presenta ninguna dificultad en su resolución, pues una ecuación

$$ax = c$$

con a, c$\in \mathbb{Z}$ tiene solución entera a/c (c es un múltiplo de a).

## 2.2. Ecuaciones con dos Incognitas.

### 2.2.1. La ecuación ax – by = c

**PROP** Sea la ecuación Ax – By = C, siendo $A \neq 0$, $B \neq 0$ y D = mcd (A, B).

Si Ax – By = C admite solución entonces D/C.

Dem.

Como D = mcd (A, B) $\Rightarrow$ A = a · D y B = b · D

La ecuación se puede escribir como aDx – bDy = C y D(ax – by) = C.

Como Ax – By = C tiene solución, la igualdad D(ax – by) = C es cierta y por tanto D/C.

**OBS** Teniendo en cuenta la proposición anterior, basta con resolver la ecuación ax – by = c con mcd (a, b) = 1.

**DEF** Se llama sistema completo de números incongruentes modulo a, a todo conjunto de a números cuyos restos al dividir por a son todos distintos.

Dado a$\in \mathbb{N}$, el conjunto {0, 1,….., a – 1} forma un sistema completo de números incongruentes módulo a.

**PROP** Sea ax – by = c una ecuación diofantica con mcd(a, b) = 1. Sea S = {0, 1,., a – 1} un sistema completo de números incongruentes módulo a. Entonces el conjunto $T = \{b \cdot x + c / x \in S\}$ es un sistema completo de números incongruentes módulo a.

Dem.

Realicemos la demostración por reducción al absurdo.

Sean bi + c y bj + c con i, j$\in$S (es lo mismo que $0 \leq i, j \leq a - 1$), $i \neq j$, dos elementos de T tales que al dividirlos por a dan el mismo resto.

Realizando la división euclidea:

$\exists q, r \in \mathbb{Z}/$ bi + c = aq + r

$\exists q', r \in \mathbb{Z}/$ bj + c = aq´ + r

Restando ambas ecuaciones b(i – j) = a(q – q´)

Y como mcd (a, b) = 1  $i - j/a$

Entonces i y j son congruentes módulo a, lo cual es una contradicción.

**PROP** La ecuación diofantica $ax - by = c$ con mcd (a, b) = 1 tiene solución.

Dem.

Como {0, 1, 2,…., a – 1} es un sistema completo de números incongruentes módulo a, por la proposición anterior tenemos que {c, b + c, 2b + c,…., (a – 1)b + c} es también un sistema completo de números incongruentes módulo a.

Entonces existe un único $b\beta + c$ con $0 \leq \beta \leq a - 1$ tal que al dividir por a obtengamos de resto 0.

$$b\beta + c = a \cdot q \quad \text{con} \quad q \in \mathbb{Z}$$

Llamemos al cociente q por la letra $\alpha$ quedando

$$b\beta + c = a\alpha$$

Y $a\alpha - b\beta = c$

Siendo $(\alpha, \beta)$ una solución particular de $ax - by = c$.

**PROP** Sea la ecuación diofántica $ax - by = c$ con mcd (a, b) = 1 y sea $(\alpha, \beta)$ una solución particular de la misma. Entonces la ecuación tiene infinitas soluciones enteras.

Dem.

Dada la ecuación diofántica $ax - by = c$ con $(x, y)$ solución. Como $(\alpha, \beta)$ es una solución particular $a\alpha - b\beta = c$.

Restando ambas expresiones $a(x - \alpha) - b(y - \beta) = 0$

$$a(x - \alpha) = b(y - \beta)$$

Al ser mcd (a, b) = 1 $\Rightarrow$ $a/y - \beta$ $\Rightarrow$ $y - \beta = at$ con $t \in \mathbb{Z}$.

Sustituyendo $a(x - \alpha) = b \cdot at$ $\Rightarrow$ $x - \alpha = bt$.

Por tanto, la solución completa de la ecuación diofántica es

$$\left.\begin{aligned} x &= \alpha + bt \\ y &= \beta + at \end{aligned}\right\} t \in \mathbb{Z}$$

### 2.2.2. La ecuación ax + by = c.

**PROP** Sea la ecuación $Ax + By = C$, con $A \neq 0$, $B \neq 0$ y $D = \text{mcd}(A, B)$.

Si $Ax + By = C$ admite solución entonces $D/C$.

Dem.

Es igual a la primera proposición del punto 2.2.1.

**OBS** De nuevo consideraremos la ecuación $ax + by = c$ con $mcd(a, b) = 1$.

**PROP** Sea $ax + by = c$ una ecuación diofántica con $mcd(a, b) = 1$. Sea $S=\{0, 1,..,a - 1\}$ un sistema completo de números incongruentes módulo a. Entonces el conjunto $T = \{c - bx / x \in S\}$ es un sistema completo de números incongruentes módulo a.

Dem.

Realicemos la demostración por reducción al absurdo.

Sean $c - ib, c - jb \in T$ con $i, j \in S$ $i \neq j$, tales que al dividirlos por a se obtiene el mismo resto

$\exists q, r \in \mathbb{Z} /$ $c - ib = aq + r$

$\exists q', e \in \mathbb{Z} /$ $c - jb = aq' + r$

Restando ambas ecuaciones $b(j - i) = a(q - q')$

Y como $mcd(a, b) = 1$ $j - i / a$

Entonces i y j son congruentes módulo a, lo cual es una contradicción.

**PROP** La ecuación diofántica $ax + by = c$ con $mcd(a, b) = 1$ tiene solución.

Dem.

Sabemos que $\{c, c - b, c - 2b,\ldots., c - (a - 1)b\}$ es un sistema completo de números incongruentes módulo a.

Entonces existe un único $c - b\beta$ con $0 \leq \beta \leq a - 1$ tal que al dividir por a obtengamos de resto 0.

$\exists \alpha \in \mathbb{Z} /$ $c - b\beta = a \cdot \alpha$

Entonces $a\alpha + b\beta = c$ y $(\alpha, \beta)$ es solución de la ecuación.

**PROP** Sea la ecuación diofántica $ax + by = c$ con $mcd(a, b) = 1$ y sea $(\alpha, \beta)$ una solución particular de la misma. Entonces la ecuación tiene infinitas soluciones enteras.

Dem.

Sea (x, y) una solución general de la ecuación y ($\alpha$, $\beta$) la solución particular.

$$\left.\begin{array}{l} ax+by=c \\ a\boldsymbol{a}+b\boldsymbol{b}=c \end{array}\right\} \Rightarrow a(x-\boldsymbol{a})+b(y-\boldsymbol{b})=0 \Rightarrow a(x-\boldsymbol{a})=b(\boldsymbol{b}-y)$$

Como mcd (a, b) = 1 $\Rightarrow$ a/$\beta$ - y $\Rightarrow$ $\beta$ - y = at t$\in \mathbb{Z}$

Sustituyendo a(x - $\alpha$) = bat $\Rightarrow$ x - $\alpha$ = bt

La solución general tiene la forma

$$\begin{array}{l} x=\boldsymbol{a}+bt \\ y=\boldsymbol{b}-at \end{array} \quad con \quad t\in\mathbb{Z}$$

### 2.2.3. Formas de hallar la solución particular.

Hemos visto en los dos puntos anteriores que una ecuación de la forma ax ± by = c con mcd (a, b) = 1 tiene solución particular. Y a partir de ella hemos encontrado todas las soluciones.

La proposición que nos afirma que existe solución particular nos describe una forma de encontrarla.

1ª Forma:

Consiste en despejar la incógnita de menor coeficiente (supongamos que es a). Eso nos proporciona un conjunto S = {0, 1,…., a – 1} más pequeño. Y probamos secuencialmente los valores de S, siendo solución aquel que al realizar la operación indicada nos da un número entero.

Ejemplo.

Sea la ecuación 39x – 5y = 13

Si despejamos $x=\dfrac{13+5y}{39}$ hemos de ver cual de los números {0, 1,…,38} es solución.

En cambio si despejamos $y=\dfrac{39x-13}{5}$ el conjunto se reduce a {0, 1,…, 4} sólo 5 elementos.

Para x = 2 $\quad y=\dfrac{65}{5}=13$

La solución particular sería (2, 13).

Siendo la solución general $\begin{cases} x = 2 + 5t \\ y = 13 + 39t \end{cases}$

Este método que hemos descrito no se puede utilizar en el caso de que ambos coeficientes de la ecuación tengan un valor elevado. En caso de que suceda esta situación, primero hemos de reducir la ecuación a otra con menores coeficientes.

2ª Forma:

Al encontrarnos con una ecuación con coeficientes altos,

$$ax - by = c$$

despejamos aquella incógnita acompañada de menor coeficiente

$$x = \frac{by + c}{a}$$

Hacemos la división euclidea entre b y a y entre c y a

$\exists q, b' \in \mathbb{Z} /\quad b = aq + b'$

$\exists q', c' \in \mathbb{Z} /\quad c = aq' + c'$

Y sustituimos

$$x = \frac{(aq + b')y + (aq' + c')}{a} = qy + q' + \frac{b'y + c'}{a}$$

Obtenemos la ecuación diofántica

$$ax' - b'y = c'$$

donde el coeficiente de la incógnita no despejada ha sido reducido. En caso de que esta nueva ecuación todavía tenga coeficientes altos, se repite el proceso tantas veces como sea necesario.

Ejemplo.

Sea la ecuación

$$5184x - 625y = 2001$$

que claramente tiene solución ya que mcd (5184, 625) = mcd $(3^4 \cdot 2^6, 5^4) = 1$

Despejamos la incógnita afectada de menor coeficiente:

$$y = \frac{5184x - 2001}{625} = 8x - 3 + \frac{184x - 126}{625} \qquad (1)$$

ya que

$5184 = 625 \cdot 8 + 184$

$2001 = 625 \cdot 3 + 126$

Sea $y' = \dfrac{184x - 126}{625} \Rightarrow 184x - 625y' = 126$

Repetimos el proceso despejando ahora

$$x = \frac{126 + 625y'}{184} = 3y' + \frac{73y'126}{184} \qquad (2)$$

Sea $x' = \dfrac{73y' + 126}{184} \Rightarrow 184x' - 73y' = 126$

Repetimos, despejando

$$y' = \frac{184x' - 126}{73} = 2x' - 1 + \frac{38x' - 53}{73} \qquad (3)$$

Sea $y'' = \dfrac{38x' - 53}{73} \Rightarrow 38x' - 73y'' = 53$

Aplicamos ahora la 1ª forma de resolución para resolver esta ecuación

$$x' = \frac{53 + 73y''}{38}$$

Y es cierta para x´ = 11 y y´´ = 5

Sustituyendo en (3)

$y' = 2 \cdot 11 - 1 + 5 = 26$

Sustituyendo en (1)

$Y = 8 \cdot 89 - 3 + 26 = 735$

Siendo una solución particular

X = 89 y = 735

Y la solución general es:

$$\left.\begin{array}{l} x = 89 + 625t \\ y = 735 + 5184t \end{array}\right\} con \quad t \in \mathbb{Z}$$

3ª Forma.

Dada la ecuación ax ± by = c, como mcd (a, b) = 1, tenemos que por el Algoritmo de Euclides

$\exists \lambda, \mu \in \mathbb{Z} /\ \ \lambda a + \mu b = 1$

Y al multiplicar esa expresión por c

$c\lambda a + c\mu b = c$

$a(\lambda c) + b(\mu c) = c$

que también se puede escribir como

$a(\lambda c) \pm b(\pm \mu c) = c$

siendo $x = \lambda c$ e $y = \pm \mu c$ solución particular de la ecuación.

**OBS** Elegiremos el signo de y según sea el de la ecuación.

## 2.3. Ecuaciones con más de dos incógnitas.

**PROP** Sea la ecuación $A_1x_1 + A_2x_2 + \ldots + A_nx_n = C$ con $A_i \neq 0 \quad \forall i: 1, \ldots, n$.

Sea $D = mcd(A_1, A_2, \ldots, A_n)$. La ecuación tiene solución $\Leftrightarrow$ D/C.

Dem.

Vamos a demostrar el teorema por inducción en el número de incógnitas.

Para n = 1 y n = 2 ya hemos visto que es cierto.

Para n – 1, por hipótesis de inducción, lo suponemos cierto.

Veamos para n.

Sea la ecuación $A_1x_1 + \ldots + A_nx_n = C$

La ecuación

$$A_1x_1 + \ldots + A_{n-1}x_{n-1} = Dy$$

con $D = mcd(a_1, a_2, \ldots, a_{n-1})$ tiene solución, por hipótesis de inducción.

Consideremos la ecuación

$Ay + A_n x_n = C$

El mcd $(D, A_n)$ = mcd $(A_1, \ldots, A_{n-1}, A_n)$ que divide a C.

Entonces, esa ecuación con dos incógnitas tiene solución.

Hemos encontrado solución para la ecuación inicial con n incógnitas.

Esta proposición que acabamos de demostrar nos proporciona un método práctico para hallar la solución de una ecuación con n incógnitas, reduciéndola a otra con una menos hasta llegar a une ecuación con sólo dos incógnitas.

Ejemplo.

Sea $18x_1 + 45x_2 - 20x_3 + 49x_4 = 11$

Sabemos que tiene solución porque mcd (18, 45, 20, 49) = 1 y 1/11.

Sea $18x_1 + 45x_2 - 20x_3 = 1 \cdot y_1$ ya que mcd (18, 45, 20) = 1

Entonces $y_1 + 49x_4 = 11$ con solución particular (60, -1)

Siendo la solución general

$$\left.\begin{array}{l} y_1 = 60 + 49t \\ x_4 = -1 - t \end{array}\right\} t \in \mathbb{Z}$$

Volvamos a reducir la ecuación con tres incógnitas:

Sea $18x_1 + 45x_2 = 9y_2$ ya que mcd (18, 45) = 9

Entonces $9y_2 - 20x_3 = y_1$ con solución particular $(9y_1, 4y_1)$

$$\left.\begin{array}{l} y_2 = 9y_1 + 20t' \\ x_3 = 4y_1 + 9t' \end{array}\right\} \Rightarrow \left.\begin{array}{l} y_2 = 540 + 441t + 20t' \\ x_3 = 240 + 196t + 0t' \end{array}\right\} t' \in \mathbb{Z}$$

Y nos queda $18x_1 + 45x_2 = 9y_2$ que es $2x_1 + 5x_2 = y_2$

Con solución particular $(3y_1, -y_1)$ y la general

$$\left.\begin{array}{l} x_1 = 3y_2 + 5t'' \\ x_2 = -y_2 - 2t'' \end{array}\right\} \Rightarrow \left.\begin{array}{l} x_1 = 1620 + 1323t + 60t' + 5t'' \\ x_2 = -540 - 441t - 20t' - 2t'' \end{array}\right\} t'' \in \mathbb{Z}$$

Siendo la solución final

$$\left.\begin{array}{l} x_1 = 1620 + 1323 + 60t' + 5t'' \\ x_2 = -540 - 441t - 20t' - 2t'' \\ x_3 = 240 + 196t + 9t' \\ x_4 = -1 - t \end{array}\right\} t, t', t'' \in \mathbb{Z}$$

## 3. SISTEMAS DE ECUACIONES DIOFANTICAS LINEALES.

De nuevo, cada ecuación diofántica del sistema de ecuaciones debe verificar que el máximo común divisor de los coeficientes ha de dividir al término independiente. No lo vamos a demostrar, por no reiterarnos en exceso.

En los casos anteriores, esta condición era necesaria y suficiente para garantizar la existencia de solución. Pero en el caso que ahora nos compete, vamos a ver mediante un ejemplo que ya no es suficiente.

Sea el sistema

$$\left.\begin{array}{l} 2x + y + 3z = 7 \\ 8x - 5y - 3z = 11 \end{array}\right\}$$

Aplicando el método de resolución de Gauss, es equivalente a

$$\left.\begin{array}{l} 2x + y + 3z = 7 \\ 10x - 4y = 18 \end{array}\right\} \Rightarrow \left.\begin{array}{l} 2x + y + 3z = 7 \\ 5x - 2y = 9 \end{array}\right\}$$

La segunda ecuación es resoluble ya que mcd (5, 2)/9

$$\left.\begin{array}{l} x = 1 + 2t \\ y = -2 + 5t \end{array}\right\} con \quad t \in \mathbb{Z}$$

Sustituyendo en la 1ª ecuación

$$2(1 + 2t) + (-2 + 5t) + 3z = 7$$

$$2 + 4t - 2 + 5t + 3z = 7$$

$$9t + 3z = 7$$

Y resulta que mcd (9, 3) = 3 y 3 no divide a 7, por lo que la ecuación no tiene solución, y el sistema tampoco.

## 4. ECUACIONES DIOFÁNTICAS NO LINEALES.

### 4.1. Ecuaciones con dos Incógnitas.

#### 4.1.1. La ecuación $x^2 - y^2 = a$.

Dada la ecuación

$$x^2 - y^2 = a$$

con $a \in \mathbb{Z}$, puede escribirse como

$$(x + y)(x - y) = a$$

Si tomamos $m = x + y$
$n = x - y$

Entonces $m \cdot n = a$

Y a cada solución posible le corresponde una descomposición factorial de a.

Al resolver la ecuación $m \cdot n = a$ en $\mathbb{Z}$ podemos deducir que simultáneamente m y n son pares o son impares. Para ello basta tener en cuenta la definición de m y n.

Eso implica que si $a \in \mathbb{Z}$ tiene un factor 2 con multiplicidad 1, no puede haber una descomposición como la indicada en el párrafo anterior. Por tanto la ecuación no tiene solución.

Ejemplos.

1) $x^2 - y^2 = 98$

Como $98 = 2\ 3\ 27^2 \Rightarrow m \cdot n = 2 \cdot 7^2$

Posibilidades:

a) $m = 2 \quad n = 49 \Rightarrow \begin{cases} x + y = 2 \\ x - y = 49 \end{cases} \Rightarrow 2x = 51 \qquad x \notin \mathbb{Z}$ No sirve

b) $m = 14 \quad n = 7 \Rightarrow \begin{cases} x + y = 14 \\ x - y = 7 \end{cases} \Rightarrow 2x = 21 \qquad x \in \mathbb{Z}$ No sirve

Como vemos, no hay solución.

2) $x^2 - y^2 = 36$

Como $36 = 2^2 \cdot 3^2 \Rightarrow m \cdot n = 2^2 \cdot 3^2$

Posibilidades

a) m = 2 n = 18 $\Rightarrow \left.\begin{matrix} x+y=2 \\ x-y=18 \end{matrix}\right\} \Rightarrow x=10 \quad y=-8$

b) m = 4 n = 9 $\Rightarrow$ No puede ser

c) m = 6 n = 6 $\Rightarrow \left.\begin{matrix} x+y=6 \\ x-y=6 \end{matrix}\right\} \Rightarrow x=6 \quad y=0$

d) m = 9 n = 4 $\Rightarrow$ No puede ser

e) m = 18 n = 2 $\Rightarrow \left.\begin{matrix} x+y=18 \\ x-y=2 \end{matrix}\right\} x=10 \quad y=8$

Las soluciones a la ecuación $x^2 - y^2 = 36$ son

(10, -8) (6, 0) (10, 8) y también (-10, 8) (-10, -8)

### 4.1.2. La ecuación de Pell.

La ecuación de Pell es

$$X^2 - dy^2 = N$$

Esta ecuación tiene gran importancia ya que cualquier ecuación cuadrática de dos variables se puede reducir a ella.

Veámoslo:

$ax^2 + bxy + cy^2 + dx + ey + f = 0$ con a, b, c, d, e, f $\in \mathbb{Z}$

Si la escribimos como un polinomio en x tenemos

$ax^2 + (by + d)x + (cy^2 + ey + f) = 0$

y es una ecuación de segundo grado en x. Tendrá solución si el discriminante es un cuadrado perfecto

$(by + d)^2 - 4a(cy^2 + ey + f) = w^2$ con $w \in \mathbb{Z}$

$(b^2 - 4ac)y^2 + (2bd - 4ae)y + (d^2 - 4af - w^2) = 0$

Sea $p = b^2 - 4ac$

$q = 2bd - 4ae$

$r = d^2 - 4af$

Y entonces podemos escribir

$$py^2 + qy + r - w^2 = 0$$

e igualmente es una ecuación de 2º grado en y, que tendrá solución si su discriminante es un cuadrado perfecto

$$q^2 - 4p(r - w^2) = z^2 \qquad \text{con } z \in \mathbb{Z}$$

y la ecuación anterior, escrita como

$$z^2 - 4pw^2 = q^2 - 4pr$$

es una ecuación de Pell con $d = 4p$ y $N = q^2 - 4pr$

En 1768, Lagrange demostró que si N =1 y d no es un cuadrado perfecto con $d > 0$, la ecuación tiene solución no trivial (distinta de $x = 1$ e $y = 0$).

La solución no trivial la calculó mediante fracciones continuas de $\sqrt{d}$ . Veamoslo mediante un ejemplo.

Ejemplo.

$$X^2 - 17y^2 = 1$$

$$\sqrt{17} = 4 + \frac{1}{z} \Rightarrow z = \frac{1}{\sqrt{17} - 4} = \frac{\sqrt{17} + 4}{1} = 4 + \sqrt{17}$$

$$z = 8 + \frac{1}{z} \Rightarrow \sqrt{17} = 4 + \frac{1}{8 + \frac{1}{z}}$$

A partir de aquí, es fácil comprobar que es periódica. La fracción reducida de segundo orden es

$$\sqrt{17} \cong 4 + \frac{1}{8} = \frac{33}{8}$$

Una solución es $x = 33$ $y = 8$

Para hallar todas: Se verifica que

$$\left(19 + 6\sqrt{17}\right)^n = x + \sqrt{17}y$$

Basta desarrollar la potencia y tomar como x los sumandos sin $\sqrt{17}$ y como y los factores que acompañan a $\sqrt{17}$ .

Como $\left(19 + 6\sqrt{17}\right)^n = x + \sqrt{17}y$

$$\left(19-6\sqrt{17}\right)^n = x-\sqrt{17}y$$

Multiplicando ambas expresiones

$19^2 - 17 \cdot 6^2 = x^2 - 17y^2$

Y como $19^2 - 17 \cdot 6^2 = 1$ tenemos que (x, y) es también solución de la ecuación.

### 4.1.3. la ecuación P(x) – by = c con P(x) polinomio.

La ecuación P(x) – by = c con $P(x)=\sum_{i=0}^{n} a_i x^n$ polinomio, no siempre tiene solución.

El método para resolverlas es muy similar al visto para dos variable, siempre que tengan solución.

Despejando en la ecuación la variable y

$$y=\frac{c-P(x)}{b}$$

Si llamamos Q(x) = c – P(x) nos queda

$$y=\frac{Q(x)}{b}$$

Sean m y n dos números enteros tales que dan el mismo resto al dividirlos por b (son congruentes). Entonces

$$m = n + b\cdot s \qquad \text{con} \quad s\in\mathbb{Z}$$

Si $Q(x)=\sum_{i=0}^{n} b_i n^i$ entonces

$$Q(n)=\sum_{i=0}^{n} b_i n^i$$

$$Q(m)=\sum_{i=0}^{n} b_i m^i = \sum_{i=0}^{n} b_i (n+bs)^i = \sum_{i=0}^{n} b_i n^i + s\cdot K = Q(n)+s\cdot K$$

Vemos que Q(n) y Q(m) también son congruentes módulo b. La implicación contraria no es cierta.

Para hallar la solución para y, basta probar {Q(0), Q(1),….., Q(b-1)} y ver cual de ellos, al dividirlo por b, da como resultado un entero.

Supongamos que Q(a) con $0 \le a \le b - 1$ es el múltiplo de b. Entonces la solución general sería:

$$\left.\begin{array}{c} x = a + bt \\ y = \dfrac{Q(a+bt)}{b} \end{array}\right\} \text{con } t \in \mathbb{Z}$$

Ejemplo.

Sea la ecuación $4x^3 - 3x^2 + x - 3y = 3$

$$y = \frac{4x^3 - 3x^2 + x - 3}{3}$$

Q(0) = -3, Q(1) = -1 Q(2) = 19

Entonces

$$\left.\begin{array}{c} x = 3t \\ y = \dfrac{4(3t)^3 - 3(3t)^2 + 3t - 3}{3} = \dfrac{108t^3 - 27t^2 + 3t - 3}{3} \end{array}\right\} t \in \mathbb{Z}$$

$$\left.\begin{array}{c} x = 3t \\ y = 36t^3 - 9t^2 + t - 1 \end{array}\right\} t \in \mathbb{Z}$$

## 4.2. Ecuaciones con más de dos incógnitas.

### 4.2.1. La ecuación Pitagórica $x^2 + y^2 = z^2$

La definición completa de la ecuación pitagórica es

$x^2 + y^2 = z^2$ con x, y, $z \in \mathbb{N} - \{0\}$

Esta ecuación surgió al estudiar el triángulo rectángulo de catetos 3 y 4 e hipotenusa 5. Al ser un triángulo rectángulo verificaba el teorema de Pitágoras

$$3^2 + 4^2 = 5^2$$

Entonces se planteó la posibilidad de hallar más conjuntos de 3 números que correspondiesen a medidas de un triángulo rectángulo, para lo cual había que resolver la ecuación

$x^2 + y^2 = z^2$ con x, y, $z \in \mathbb{N}$

Es claro que si $x_o$, $y_o$, $z_o$ es una solución de la ecuación, entonces $\lambda x_o$, $\lambda y_o$, $\lambda z_o$ con $\lambda \in \mathbb{N}$ también es solución. El recíproco también es cierto.

Entonces, para su resolución, podemos suponer que los tres números x, y, z son coprimos tomados de dos en dos. Las soluciones que verifiquen esta condición reciben el nombre de soluciones primitivas, ya que no son múltiplos de ninguna otra solución.

Teniendo en cuenta lo anterior, los números representados por x e y no pueden ser ambos pares, ya que entonces también lo sería z, y hemos excluido esa situación.

Supongamos entonces que x es impar, y vamos a tratar de resolver la ecuación.

$$x^2 + y^2 = z^2$$

$$x^2 = z^2 - y^2$$

$$x^2 = (z + y)(z - y)$$

$$\text{Sea } u^2 = z + y \quad \text{y} \quad v^2 = z - y \quad \Rightarrow \quad x = u \cdot v$$

$$\left.\begin{array}{l} z + y = u^2 \\ z - y = v^2 \end{array}\right\} \Rightarrow \begin{array}{l} z = \dfrac{u^2 + v^2}{2} \\ y = \dfrac{u^2 - v^2}{2} \end{array}$$

Los factores u y v deben ser impares. Si u y v tuviesen un factor común, entonces z e y también lo tendrían y no serían coprimos, luego u y v además de impares, deben ser coprimos.

| x | 3=3·1 | 5=5·1 | 7=7·1 | 9=9·1 | 11=11·1 | 13=13·1 | 15=15·1 | 15=15·3 | 17=17·1 | 19=19·1 | 21=7·3 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| y | 4 | 12 | 24 | 40 | 60 | 84 | 112 | 8 | 144 | 180 | 20 |
| z | 5 | 13 | 25 | 41 | 61 | 85 | 113 | 17 | 145 | 181 | 29 |

### 4.2.2. La Ecuación de Fermat $x^n + y^n = z^n$.

La ecuación pitagórica dio lugar a intentar resolver

$$x^3 + y^3 = z^3 \quad \text{con} \quad x, y, z \in \mathbb{N}$$

Y posteriormente a

$$x^4 + y^4 = z^4 \quad \text{con} \quad x, y, z \in \mathbb{N}$$

Y en general a

$$X^n + y^n = z^n \quad \text{con} \quad x, y, z, n \in \mathbb{N}$$

llamada ecuación de Fermat por ser este quien la resolvió.

Desde el siglo XVII se ha ido demostrando que para $n = 3$ la ecuación era irresoluble y luego se no para $n = 4$. Un día dijo Fermat que había demostrado que la ecuación era irresoluble para $n \geq 3$, pero nunca dio la demostración.

En 1993, el matemático A. Wiles, publicó la demostración de la irresolubilidad de la ecuación para $n \geq 3$, pero pronto se vio que había cometido un fallo.

Hoy en día es uno de los problemas clásicos de la matemática que sigue sin ser demostrado.

## 5. ECUACIONES DE CONGRUENCIAS.

Recordemos que dos números a y b son congruentes módulo n si al dividirlos por n (mediante la división euclidea) obtenemos el mismo resto. Se representa por

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

y es equivalente a que $a - b = n \cdot t$ con $t \in \mathbb{Z}$.

Podemos plantearnos la resolución de este tipo de expresiones cuando uno de los miembros lo sustituimos por una expresión, que bien puede ser lineal (con una o varias incógnitas) o polinómica. Entonces recibe el nombre de ecuación de congruencias.

Ejemplos.

1) $2x \equiv 5 \pmod{7}$

2) $2x^2 + x + 1 \equiv 3 \pmod{11}$

3) $2x - 3y \equiv 7 \pmod{5}$

Toda ecuación de congruencias puede reducirse a una ecuación diofantica con una incógnita más, y tratar así de resolverla.

Ejemplos.

1) $2x \equiv 5 \pmod{7} \Rightarrow 2x - 5 = 7y \Rightarrow 2x - 7y = 5$

2) $2x^2 + x + 1 \equiv 3 \pmod{11} \Rightarrow 2x^2 + x + 1 - 3 = 11y \Rightarrow 2x^2 + x + 1 - 11y = 3$

3) $2x - 3y \equiv 7 \pmod{5} \Rightarrow 2x - 3y - 7 = 5z \Rightarrow 2x - 3y - 5z = 7$

**Bibliografía Recomendada.**


- Álgebra. Aut: Hungerford. Edit: Springer-Verlag.
- Algèbre. Aut: S. MacLane. Edit: Gauthier-Villars
- Álgebra. Aut: S. Lang. Edit: Aguilar.
- Curso de Álgebra Moderna. Aut. P. Hilton. Edit: Reverté.